kaspersky

Kaspersky Next XDR Expert

© 2026 AO Kaspersky Lab

目录

Kaspersky Next XDR Expert
新增功能
已修复的问题
关于 Kaspersky Next XDR Expert
  硬件和软件要求
    Kaspersky Deployment Toolkit要求
    安装 KUMA 服务的主机的要求
    OSMP Console 要求
    网络代理要求
    虚拟化配置
    常见要求和注意事项
  Kaspersky Next XDR Expert 组件
  兼容的应用程序和解决方案
  基本概念
    管理服务器
    管理服务器层级
    Web 服务器
    网络代理
    管理组
    受管理设备
    未分配的设备
    管理员工作站
    管理 Web 插件
    策略
    策略配置文件
    任务
    关联器
    事件
    警报
    事故
    资源
    任务范围
    本地应用程序设置与政策的关系
    分发点
    连接网关
    Core
    存储库
    收集器
    服务
    KUMA 代理
    关于严重级别
Open Single Management Platform 架构
  SIEM 组件架构

OSMP Console 界面
更改 OSMP Console 界面语言
更改 OSMP 控制台主页
添加和移除书签
授权许可
关于最终用户授权许可协议
关于授权许可密钥
关于激活码
关于密钥文件
授权许可限制
Kaspersky Next XDR Expert授权许可功能
激活 Kaspersky Next XDR Expert
为SIEM组件添加授权许可密钥
查看使用中授权许可密钥的相关信息
撤销对最终用户授权许可协议的同意
续订卡巴斯基应用程序授权许可
移除SIEM组件的授权许可密钥
使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案
关于数据提供
关于数据提供
Kaspersky Unified Monitoring and Analysis Platform 中的数据提供
沙盒中的数据提供
启动
Kaspersky Next XDR Expert 的部署和初始设置
验证 Kaspersky Next XDR Expert 配置的准确性
使用威胁监控、检测和搜索功能
使用 Kaspersky Next XDR Expert 进行事故调查的示例
部署 Kaspersky Next XDR Expert
强化指南
管理 Kaspersky Next XDR Expert 的基础架构
连接安全
账户和身份验证
管理 Kaspersky Next XDR Expert 的保护
管理客户端设备保护
事件传输到第三方系统
配置受管理应用程序的保护
部署方案
多节点部署方案
单节点部署方案
Kaspersky Next XDR Expert 使用的端口
更改用于连接到 OSMP 控制台服务器的端口
更改 Endpoint Agent 用于连接到 agentserver 组件的端口
准备工作和部署
多节点部署：准备管理员和目标主机
单节点部署：准备管理员和目标主机
准备主机以安装 KUMA 服务
安装数据库管理系统

配置 PostgreSQL 或 Postgres Pro 服务器以与 Kaspersky Next XDR Expert 配合使用
准备 KUMA 清查文件，以便在 Kubernetes 集群外部安装 KUMA 服务
多节点部署：指定安装参数
单节点部署：指定安装程序参数
通过代理节点连接 Endpoint Agent
Kaspersky Next XDR Expert 部署向导
Kaspersky Next XDR Expert 安装
为目标主机配置互联网访问
在计算机上同步时间
在Kubernetes集群内安装KUMA服务
在 Kubernetes 集群外部安装 KUMA 服务
部署多个 Kubernetes 集群和 Kaspersky Next XDR Expert 实例
在物理隔离环境中安装或升级 Kaspersky Next XDR Expert
部署前的基础架构就绪度预检查
Kaspersky Next XDR Expert组件的安装前完整性检查
登录 Kaspersky Next XDR Expert
与端点代理的集成
Sandbox 的准备和安装
准备用于 Sandbox 安装的 IT 基础架构
准备用于安装 Sandbox 的虚拟机
准备安装磁盘镜像
安装 Sandbox
步骤 1：查看最终用户授权许可协议和隐私策略
步骤 2：选择用于安装 Sandbox 的磁盘
步骤 3：配置 Sandbox 管理员密码的最小密码长度
步骤 4：创建 Sandbox 管理员账户
步骤 5：配置管理网络接口
步骤 6：分配主机名并添加 DNS 服务器地址
步骤 7：配置静态网络路由
与沙盒集成
Kaspersky Next XDR Expert的高可用性部署
Kaspersky Next XDR Expert 的高可用性配置
恢复Kubernetes集群中的故障节点
Kaspersky Next XDR Expert 的高可用性多站点部署
多站点部署：准备管理员主机和目标主机
多站点部署：指定安装参数
标准 Ubuntu Server 24.04 LTS 虚拟机上的跨数据中心多站点部署
Kaspersky Next XDR Expert 维护
更新 Kaspersky Next XDR Expert 组件
检查已安装的Kaspersky Next XDR Expert组件的完整性
无需重新安装即可更改 Kaspersky Next XDR Expert 参数
添加和删除Kubernetes集群的主节点和工作线程节点
配置文件的版本控制
卸载 Kaspersky Next XDR Expert
手动卸载 Kaspersky Next XDR Expert 组件
安装失败后重新安装 Kaspersky Next XDR Expert
重新安装 Kaspersky Next XDR Expert 组件

- 备份 Kaspersky Next XDR Expert 数据的副本和数据恢复
  - 配置 Kaspersky Next XDR Expert 备份副本的存储
  - 配置和管理备份计划
  - 手动创建 Kaspersky Next XDR Expert 数据备份副本
  - 查看 Kaspersky Next XDR Expert 数据的备份
  - 从备份副本恢复 Kaspersky Next XDR Expert 数据
- 停止 Kubernetes 集群节点
- 使用证书访问公共 Kaspersky Next XDR Expert 服务
- 计算和更改用于存储管理服务器数据的磁盘空间
- 查看和更改 KUMA Core 和 Metrics 服务的磁盘空间
- 查看和更改对象存储大小
- 增加可观测性存储大小
- Kubernetes集群证书轮换
- 注册表访问凭证轮换
- DBMS 凭证和证书轮换
- 添加用于安装附加 KUMA 服务的主机
- 更换使用 KUMA 存储的主机
- 使用部署在虚拟机上的 Kaspersky Next XDR Expert
- Kaspersky Next XDR Expert 的演示部署
  - 准备管理员主机和目标主机
  - 指定安装参数
- 将 Kaspersky Next XDR Expert 从版本 2.2 升级到 2.3
- 迁移到 Kaspersky Next XDR Expert
- 关于从 Kaspersky Security Center Windows 迁移
  - 从 Kaspersky Security Center Windows 导出组对象
  - 将导出文件导入 Kaspersky Next XDR Expert
  - 将受管理设备切换至 Kaspersky Next XDR Expert 都管理下
- 关于从KEDR 7.1迁移
- 设置和使用SIEM组件
- KUMA 服务
  - 服务工具
    - 获取服务标识符
    - 停止、启动、检查服务状态
    - 重启服务
    - 删除服务
    - 查看活动查询表
    - 分区窗口
    - 搜索相关事件
  - 服务资源集
  - 创建存储
    - ClickHouse 集群结构
    - ClickHouse 集群节点设置
    - 事件冷存储
      - 移除冷存储磁盘
      - 分离、存档和附加分区
    - 为存储创建资源集
    - 在 OSMP 中创建存储服务

- 在 OSMP 网络基础设施中安装存储
- 备份、恢复和导入分区
  - 计划分区备份
  - 手动备份分区
  - 从外部 OSMP 实例导入分区
  - 从备份恢复分区
- 创建关联器
  - 启动关联器安装向导
    - 步骤 1：关联器常规设置
    - 步骤 2：全局变量
    - 步骤 3：关联
    - 步骤 4：增强
    - 步骤 5：响应
    - 步骤 6：路由
    - 步骤 7：设置验证
  - 在 OSMP 网络基础设施中安装关联器
  - 验证关联器安装
  - 创建 correlator-ng 关联器
    - 配置关联器correlator-ng
    - correlator-ng 支持的数据类型
    - 关联规则选择器和表达式
    - 标准关联规则的属性
    - correlator-ng中的数据函数
- 创建事件路由器
  - 启动事件路由器安装向导
    - 步骤 1：事件路由器的常规设置
    - 步骤 2：路由
    - 步骤 3：设置验证
  - 在服务器上安装事件路由器
- 创建收集器
  - 启动收集器安装向导
    - 步骤 1：连接事件源
    - 步骤 2：传输
    - 步骤 3：事件解析
    - 步骤 4：筛选事件
    - 步骤 5：事件聚合
    - 步骤 6：事件增强
    - 步骤 7：路由
    - 步骤 8：设置验证
  - 在 KUMA 网络基础设施中安装收集器
  - 验证收集器安装
  - 确保收集器运行不间断
    - 使用 rsyslog 控制事件流
    - 使用 nginx 控制事件流
  - 预定义收集器

- 创建代理
  - 为代理创建资源集
  - 在 OSMP 中创建代理服务
  - 在 OSMP 网络基础设施中安装代理
    - 在 Linux 资产上安装 KUMA 代理
    - 在 Windows 资产上安装 KUMA 代理
  - 自动创建的代理
  - 更新代理
  - 将事件从隔离网段传输到 KUMA
    - 二极管代理配置文件
    - 密钥字段描述
    - 在隔离网段中安装 Linux 代理
    - 在隔离网段中安装 Windows 代理
  - 将事件从 Windows 计算机传输到 OSMP
  - 配置代理以接收来自隔离网段的 Netflow 事件
- AI 服务
  - 使用 KIRA 分析警报和事故
    - 透过LLM提供商配置与KIRA的集成
    - 使用 KIRA 进行分析
    - “使用 KIRA 进行分析”任务可能出现的错误
  - 使用KIRA以自然语言创建搜索查询
    - 使用KIRA创建自然语言搜索查询并将其转换为SQL查询
    - 使用自然语言构建查询时可能出现的错误
  - 配置 DLL 劫持检测
  - AI资产评分和状态。
    - 安装AI资产评分和状态服务
    - 重新签发AI服务证书
    - AI资产评分和状态服务的设置
- 配置事件通知
  - 配置 Auditd 事件的接收
    - 安装 KUMA 收集器以接收 Auditd 事件
    - 配置事件源服务器
  - 配置 KATA/EDR 事件的接收
    - 配置将 KATA/EDR 事件导出到 KUMA
    - 创建用于接收 KATA/EDR 事件的 KUMA 收集器
    - 安装用于接收 KATA/EDR 事件的 KUMA 收集器
  - 配置 Open Single Management Platform 以将事件导出到 KUMA SIEM 系统
    - 配置 KUMA 收集器以收集 Open Single Management Platform 事件
    - 安装 KUMA 收集器以收集 Open Single Management Platform 事件
  - 配置从 MS SQL 接收 Open Single Management Platform 事件
    - 在 MS SQL 数据库中创建账户
    - 配置 SQL Server Browser 服务
    - 在 KUMA 中创建密钥
    - 配置连接器
    - 配置 KUMA 收集器以从 MS SQL 数据库接收 Kaspersky Security Center 事件
    - 安装 KUMA 收集器以从 MS SQL 数据库接收 Kaspersky Security Center 事件

使用 KUMA 代理 (WEC) 配置从 Windows 设备接收事件
配置来自 Windows 设备的事件审计
在 Windows 设备上配置审计策略
使用组策略配置审计
使用 Windows 事件收集器服务配置从 Windows 设备集中接收事件
配置从事件源服务器的数据传输
配置 Windows 事件收集器服务
授予查看 Windows 事件的权限
授予作为服务登录的权限
配置 KUMA 收集器以接收来自 Windows 设备的事件
安装 KUMA 收集器以从 Windows 设备接收事件
使用 KUMA 代理 (WEC) 配置从 Windows 设备到 KUMA 的事件转发
使用 KUMA 代理 (WMI) 配置从 Windows 设备接收事件
配置用于管理 KUMA 的审计设置
使用本地策略配置审计
使用组策略配置审计
配置从事件源服务器的数据传输
授予查看 Windows 事件的权限
授予作为服务登录的权限
配置 PostgreSQL 事件的接收
安装 pgAudit 插件
配置 Syslog 服务器以发送事件
配置 IVK Kolchuga-K 事件的接收
配置将 IVK Kolchuga-K 事件导出到 KUMA
配置 CryptoPro NGate 事件的接收
配置将 CryptoPro NGate 事件导出至 KUMA
配置 Ideco UTM 事件的接收
配置将 Ideco UTM 事件导出至 KUMA
配置 KWTS 事件的接收
配置将 KWTS 事件导出至 KUMA
配置 KLMS 事件的接收
配置将 KLMS 事件导出至 KUMA
配置 KSMG 事件的接收
配置将 KSMG 事件导出至 KUMA
配置 PT NAD 事件的接收
配置将 PT NAD 事件导出至 KUMA
使用 MariaDB 审计插件配置事件的接收
配置 MariaDB 审计插件以发送 MySQL 事件
配置 MariaDB 审计插件以发送 MariaDB 事件
配置 Syslog 服务器以发送事件
配置 Apache Cassandra 事件的接收
在 KUMA 中配置 Apache Cassandra 事件日志记录
配置 FreeIPA 事件的接收
配置将 FreeIPA 事件导出到 KUMA
配置 VipNet TIAS 事件的接收
配置将 ViPNet TIAS 事件导出到 KUMA

配置 Nextcloud 事件的接收
配置 Nextcloud 事件审计
配置 Syslog 服务器以发送 Nextcloud 事件
配置 Snort 事件的接收
配置 Snort 事件的日志记录
配置 Suricata 事件的接收
配置 Suricata 事件的日志记录。
配置 FreeRADIUS 事件的接收
配置 FreeRADIUS 事件审计
配置 Syslog 服务器以发送 FreeRADIUS 事件
配置 VMware vCenter 事件接收
配置与 VMware vCenter 的连接
配置 zVirt 事件的接收
配置 zVirt 事件的导出
配置 Zeek IDS 事件的接收
转换 Zeek IDS 事件日志格式
使用 ETW 连接器配置 DNS 服务器事件接收
Windows 端配置
使用 Kaspersky Endpoint Security for Windows 配置 Windows 事件接收
Codemaster Mirada
配置 Codemaster Mirada 事件的接收
配置 Postfix 事件的接收
配置 Postfix 以发送事件
配置 KUMA 收集器以接收和处理 Postfix 事件
配置 CommuniGate Pro 事件的接收
配置 CommuniGate Pro 以发送事件
配置 KUMA 收集器以接收和处理 CommuniGate Pro 事件
配置 Yandex Cloud 事件的接收
配置 Yandex Cloud 事件的审计
配置 Yandex Cloud 事件的导出
配置 Microsoft 365 事件的接收
配置 Kontinent 加密系统事件的接收
准备接收 Kontinent 事件
配置 kuma-kont 实用程序
启动和管理 kuma-kont 服务
kuma-kont-config.yaml 配置文件中的设置
与其他解决方案集成
与 Kaspersky Security Center 集成
配置 Kaspersky Security Center 资产的数据刷新间隔
按计划导入 Kaspersky Security Center 资产
手动导入 Kaspersky Security Center 资产
查看 Kaspersky Security Center 服务器的层次结构
从 Kaspersky Security Center 数据库导入事件
Kaspersky Endpoint Detection and Response 集成
使用 kafka 连接器导入 Kaspersky Endpoint Detection and Response 事件
使用 kata/edr 连接器导入 Kaspersky Endpoint Detection and Response 事件
配置在 KUMA 警报中显示指向 Kaspersky Endpoint Detection and Response 检测的链接

与 Kaspersky CyberTrace 集成
集成 CyberTrace 指标搜索
配置 CyberTrace 以接收和处理请求
创建事件增强规则
集成 CyberTrace 界面
LDAP 连接
启用和禁用 LDAP 集成
将租户添加到 LDAP 服务器集成列表
创建 LDAP 服务器连接
创建 LDAP 服务器连接的副本
更改 LDAP 服务器连接
更改数据更新频率
更改数据存储期限
启动账户数据更新任务
删除 LDAP 服务器连接
Kaspersky Industrial CyberSecurity for Networks 集成
在 KICS for Networks 中配置集成
在 KUMA 中配置集成
启用和禁用与 KICS for Networks 的集成
更改数据更新频率
从 KICS for Networks 导入资产信息时的特殊注意事项
更改 KICS for Networks 资产的状态
与 Neurodat SIEM IM 集成
Kaspersky Automated Security Awareness Platform
在 KASAP 中创建令牌并获取 API 请求的链接
在 KUMA 中配置集成
查看有关 KASAP 用户的信息并更改学习组
向 Telegram 发送通知
创建和配置 Telegram 机器人
创建用于发送通知的脚本
在 KUMA 中配置通知
UserGate 集成
在 UserGate 中配置集成
准备用于与 UserGate 集成的脚本
配置用于与 UserGate 集成的响应规则
与 Kaspersky Web Traffic Security 集成
在 KWTS 中配置集成
准备与 KWTS 集成的脚本
配置与 KWTS 集成的响应规则
与 Kaspersky Secure Mail Gateway 集成
在 KSMG 中配置集成
准备与 KSMG 集成的脚本
从 RedCheck 导入资产信息
配置 Sendmail 事件的接收
配置 Sendmail 日志记录
配置 Sendmail 事件的导出
配置与外部SIEM系统的集成

管理 KUMA
配置 KUMA Core
代理
连接到 SMTP 服务器
操作 Kaspersky Security Center 任务
在 Kaspersky Security Center 中创建 KUMA 任务
手动启动 Kaspersky Security Center 任务
自动启动 Kaspersky Security Center 任务
检查 Kaspersky Security Center 任务的状态
KUMA 日志
KUMA 通知
编辑 KUMA 用户配置文件
处理租户
管理证书
下载证书
修改自签名 Web 界面证书
重新颁发内部 CA 证书
重新颁发特定服务的证书
处理地理数据
地理数据格式
将地理数据从 MaxMind 转换为 IP2Location
导入和导出地理数据
地理数据的默认映射
使用知识库
查看包详细信息
查看资源详细信息
安装和更新包及资源
KUMA 资源
资源操作
创建、重命名、移动和删除资源文件夹
创建、复制、移动、编辑和删除资源
将资源与服务链接起来
更新资源
使用卡巴斯基更新实用程序配置自定义源
导出资源
导入资源
标签管理
规范化器
事件解析设置
扩展事件模式
添加扩展事件模式字段
编辑扩展事件模式字段
导入和导出扩展事件模式字段
删除扩展事件模式字段
在规范化器中使用扩展事件模式字段
使用 KIRA 生成正则表达式
规范化器中的增强操作

- 将数据发送到额外规范化器的条件
- 支持的事件源
- 连接器
  - 查看连接器设置
  - 添加连接器
  - 连接器设置
    - Tcp 类型
    - Udp类型
    - Netflow 类型
    - Sflow 类型
    - Nats-jetstream 类型
    - 连接器，Kafka 类型
    - kata/edr 类型
    - 连接器，HTTP 类型
    - SQL 类型
    - 文件类型
    - 类型 1c-xml
    - 类型 1c-log
    - 二极管类型
    - Ftp 类型
    - Sftp 类型
    - smb 类型
    - Nfs 类型
    - vmware 类型
    - Wmi 类型
    - Wec 类型
    - SNMP 类型
    - SNMP 陷阱类型
      - 配置 Windows 的 SNMP 陷阱消息源
        - 配置和启动 SNMP 和 SNMP 陷阱服务
        - 配置"事件转陷阱转换器"服务
    - elastic 类型
    - etw 类型
    - universalAPI类型
    - promtail类型
    - http-streaming 类型
    - 预定义连接器
- 目标位置
  - 目标位置，"内部"类型
  - Nats-jetstream 类型
  - Tcp 类型
  - Udp类型
  - Http 类型
  - 二极管类型
  - Kafka 类型
  - 文件类型
  - 存储类型

- 关联器类型
- 目标位置，“事件路由器”类型
- 预定义目标位置

过滤器

活动列表

- 查看活动列表的表格
- 添加活动列表
- 查看活动列表的设置
- 更改活动列表的设置
- 复制活动列表的设置
- 删除活动列表
- 查看活动列表中的记录
- 搜索活动列表中的记录
- 将记录添加到活动列表
- 复制活动列表中的记录
- 更改活动列表中的记录
- 从活动列表中删除记录
- 将数据导入活动列表
- 从活动列表中导出数据
- 预定义活动列表

词典

密钥

上下文表

- 查看上下文表列表
- 添加上下文表
- 查看上下文表设置
- 编辑上下文表设置
- 复制上下文表设置
- 删除上下文表
- 查看上下文表记录
- 搜索上下文表记录
- 添加上下文表记录
- 编辑上下文表记录
- 删除上下文表记录
- 将数据导入上下文表
- 从上下文表中导出数据

关联规则

- 标准关联规则
- 简单关联规则
- 操作关联规则
- 关联器中的变量
  - 相同和唯一字段中的局部变量
  - 选择器中的局部变量
  - 事件增强中的局部变量
  - 活动列表增强中的局部变量
  - 变量的属性
  - 变量的要求

变量函数
声明变量
预定义关联规则
为关联规则添加临时排除列表
Sigma 规则转换器
准备 Sigma 规则
支持的 Sigma 规则转换示例
MITRE ATT&CK 矩阵覆盖范围
聚合规则
增强规则
响应规则
Kaspersky Security Center 的响应规则
自定义脚本的响应规则
KICS for Networks 的响应规则
Kaspersky Endpoint Detection and Response 的响应规则
Active Directory 响应规则
数据收集和分析规则
虚拟管理服务器
构建 OSMP 实例层次结构
将子实例连接到父实例
在 OSMP 实例层次结构中分配从属管理服务器
将子实例与父实例断开连接
层次结构中关联规则的分布
分发全局关联器配置以及全局关联规则
分发全局关联规则以供本地使用
复制继承的关联规则以供本地使用
查看在 OSMP 子实例中创建的资源和服务
在层次结构中分发资源时的文件夹行为
将 OSMP 实例组合成层次结构
证书轮换后修复实例层次结构
与其他解决方案集成
Kaspersky Automated Security Awareness Platform
Создание токена в KASAP и получение URL для API-запросов
配置与 Kaspersky Threat Intelligence Portal 的集成
与 KATA/KEDR 集成
配置 Kaspersky Next XDR Expert 与脚本启动服务的集成
威胁检测
处理警报
关于警报
警报数据模型
查看警报表
查看警报详情
向分析师分配警报
更改警报状态
手动创建警报
将警报添加到事故
解除警报与事故的关联

- 将事件关联到警报
- 解除事件与警报的关联
- 在调查图上处理警报
- 将IOA规则添加到排除项
- 管理聚合规则
  - 创建聚合规则
  - 编辑聚合规则
  - 将聚合规则复制到另一个租户
  - 删除聚合规则

处理事故

- 关于事故
- 事故数据模型
- 创建事故
- 创建子事故
- 查看事故表格
- 查看事故详情
- 将事故分配给分析师
- 更改事故状态
- 更改事故优先级
- 合并事故
- 将事故导出到文件
- 从 XDR 事故创建 Managed Detection and Response 事故
- 调查图
  - 进程树状图
    - 构建进程树状图
    - 删除进程树状图
    - 对进程树状图进行备注
- 分段规则
- 将分段规则复制到另一个租户
- 管理服务水平协议 (SLA)
  - 创建服务水平协议 (SLA) 条目
  - 删除服务水平协议 (SLA) 条目
- 管理事故类型
  - 查看事故类型表
  - 创建事故类型
  - 编辑事故类型
  - 删除事故类型
- 管理事故工作流
  - 查看事故工作流表
  - 预定义事故工作流
  - 创建事故工作流
  - 编辑事故工作流和状态
  - 删除事故工作流
- 管理事故工作量
  - 添加事故工作量
  - 编辑事故工作量

删除事故工作量
生成和导出事故报告
配置警报和事故的保留期
配置警报和事故的自动分配
查看资产详情
通过远程终端进行调查和响应
管理远程终端连接
通过远程终端执行响应操作
威胁搜索
处理事件
事件数据模型
Process
Registry Create
File Create
File Modify
File Rename
File Read
File Delete
File Attributes Modify
File Creation Time Modify
File Hardlink Created
File Symlink Created
Module
Registry Create
Registry Delete
Registry Modify
Registry Rename
Registry Query
Registry Save
Connection
Port Listen
AMSI Scan
Process Console Input
Driver
Process Interpreted File Run
DNS
Pipe Create
Pipe Connect
LDAP
WMI Activity
WMI Consumer Register
Code Injection
Process Access
Threat Detect
Threat Detect Processing Result
Linux Event Log
Windows Event Log

Blocked Document
Applock
Process Terminated
Device
File System Mount
File System Unmount
Bits Job Create
Bits Job Complete
Bits Job Start
Bits Job Stop
Bits Job Add File
Bits Job Error
Service Create
Service Modify
Service Delete
Scheduled Task Create
Scheduled Task Modify
Scheduled Task Delete
File Owner Change
File ACL Change
Registry Owner Change
Registry ACL Change
Executable Memory Mapped
Agent Start
Agent Stop
Agent Install
Agent Uninstall
Agent Action
System Startup
System Shutdown
Connection Close
事件的细粒度访问
查看事件表
搜索和筛选事件
手动创建 SQL 查询
使用构建器生成 SQL 查询
使用 KUMA SQL 函数生成 SQL 查询
在 SQL 查询中使用“enrich”函数集
在 SQL 查询中使用“lookup”函数集
查看事件详情
保存和选择事件过滤器配置
按时间段筛选事件
导出事件
查看审计事件和配置通知
审计事件
回溯扫描
获取事件表统计信息

威胁响应
响应操作
终止进程
将设备移动至其他管理组
更新数据库
更改设备的授权状态
将文件移动至隔离区
从隔离区恢复文件
从隔离区获取文件
从隔离区删除文件
查看有关 KASAP 用户的信息并更改学习组
启用和禁用网络隔离
执行“添加预防规则”和“删除预防规则”响应操作
运行程序
管理服务
通过 Kaspersky NGFW 阻止 IP 地址
获取文件以供进一步分析
获取文件
获取注册表键
获取 NTFS 元文件
获取取证信息
获取磁盘映像
获取内存转储
获取进程内存转储
扫描设备以检测威胁
运行恶意软件扫描
YARA 扫描
IOC 扫描
扫描从设备中获取的文件
删除文件
通过 Active Directory 响应
使用第三方脚本进行响应
通过 UserGate 响应
通过 Ideco NGFW 响应
通过 Ideco UTM 响应
通过 Redmine 响应
通过 Check Point NGFW 响应
通过 Sophos Firewall 响应
通过 Continent 4 响应
通过 SKDPU NT 响应
通过 FortiGate 响应
通过 Palo Alto NGFW 进行响应
通过 Jira 响应
查看警报或事故详细信息中的响应历史记录
查看恶意软件扫描结果
处理因响应操作而获得的文件

使用阻止规则表
创建防止规则
导入阻止规则
使用IOC规则表
使用YARA规则表
行动手册
查看行动手册列表
创建行动手册
在可视化编辑器中配置行动手册执行步骤
编辑行动手册
自定义行动手册
查看行动手册属性
终止行动手册
删除行动手册
管理行动手册版本
比较行动手册版本
恢复行动手册版本
在测试模式下启动行动手册
启动行动手册和响应操作
手动启动行动手册
为用户指定的对象启动行动手册
以“训练”操作模式启动行动手册
配置响应操作的手动审批
审批行动手册或响应操作
通过行动手册进行数据增强
查看响应历史记录
预定义行动手册
[KL] P001“办公应用程序创建可执行文件”
[KL] P002“Windows 事件日志已被清除”
[KL] P003“来自 wmiprvse.exe 的可疑子进程”
[KL] P004 “沙盒中等检测”
[KL] P005 “沙盒高等检测”
[KL] “检查外部IP地址的行动手册”
[KL] “检测到受感染文件时隔离设备的行动手册”
[KL][EDR]“删除通过告警传输到主机的恶意文件”
[KL][EDR]“删除从事故传输到主机的恶意文件”
[KL][EDR]“检测到警报中的发现活动时隔离主机”
[KL][EDR]“从事故中检测到发现活动时隔离主机”
[KL][EDR]“检测到数据渗出活动时隔离主机”
[KL][EDR]“从警报中检测到反向 shell 活动时隔离主机”
[KL][EDR]“当检测到事故中的反向 Shell 活动时隔离主机”
[KL][EDR]“根据警报缓解电子邮件附件中的恶意活动”
[KL][EDR]“缓解事故中电子邮件附件引发的恶意活动”
[KL][EDR]“缓解告警中的内存转储活动”
[KL][EDR]“缓解事故中的内存转储活动”
行动手册触发规则

- 行动手册算法
  - 行动手册参数
  - 执行步骤参数
    - 循环
    - 并行
    - 决定
    - 更新数据
  - 响应函数参数
- 使用行动手册编辑事故
- 使用行动手册编辑警报

管理 Sandbox

- 初始 Sandbox 设置
  - 为 Sandbox 配置数据库更新
  - Sandbox 网络接口
    - 配置 DNS 设置
    - 配置管理网络接口
    - 配置已处理对象的互联网访问
    - 添加静态网络路由
  - 更改 Sandbox 管理员账户密码
  - 沙盒身份验证政策
    - 终止不活动的 Sandbox 会话
    - 关于 Sandbox 身份验证尝试失败的通知
  - 设置将已检测到的对象发送到KPSN拒绝列表
- 准备虚拟机以供使用
  - 将镜像上传到存储
  - 导入模板
  - 创建自定义虚拟机模板
  - 配置操作系统和软件
  - 创建虚拟机
  - 安装虚拟机
  - 下载调试符号

配置 OSMP 以使用检测技术

- 更新沙盒和反恶意软件引擎的反病毒数据库
- 创建受密码保护的存档的密码列表
- 在 Sandbox 中选择用于扫描对象的操作系统
- 创建自定义 Sandbox 规则
- 配置从 Endpoint Agent 向 Sandbox 发送文件
- 关于入侵指标、 IOC 文件和 IOC 规则
- 导入 IOC 规则
- 导入 YARA 规则

Kaspersky Next XDR Expert API

- 创建令牌
- 授权 API 请求

使用 Open Single Management Platform

- 配置管理服务器
  - 配置管理服务器连接地址
  - 配置 OSMP 控制台与管理服务器的连接

- 配置互联网访问设置
- 用于在 Open Single Management Platform 操作的证书
  - 关于 Open Single Management Platform 证书
  - Open Single Management Platform 中使用的自定义证书的要求
  - 重新颁发 OSMP 控制台证书
  - 替换 OSMP 控制台的证书
  - 将 PFX 证书转换为 PEM 格式
  - 场景：指定自定义管理服务器证书
  - 使用 klsetsrvcert 实用程序替换管理服务器证书
  - 使用 klmover 实用程序将网络代理连接到管理服务器
- 管理服务器层级
- 创建管理服务器层级：添加从属管理服务器
- 查看从属管理服务器列表
- 管理虚拟管理服务器
  - 创建虚拟管理服务器
  - 启用或禁用虚拟管理服务器
  - 为虚拟管理服务器分配管理员
  - 更改客户端设备的管理服务器
  - 删除虚拟管理服务器
- 配置管理服务器连接事件记录
- 设置事件存储库中的最大事件数量
- 更改 DBMS 凭据
- 管理服务器数据的备份复制与恢复
  - 配置管理服务器备份任务
  - 使用 KDT 实用程序来恢复管理服务器数据
- 删除管理服务器层级
- 访问公共 DNS 服务器
- 配置界面
- 使用 TLS 的加密通信

发现网络设备

- 情景：发现网络设备
- Windows 网络轮询
- IP 范围轮询
- 域控制器轮询
- 配置 Samba 域控制器
- 在客户端设备上使用 VDI 动态模式
  - 在网络代理安装包属性中启用 VDI 动态模式
  - 将组成 VDI 的设备移至管理组

管理客户端设备

- 受管理设备设置
- 检查客户端设备与管理服务器之间的连接。klnagchk 实用程序
- 创建管理组
- 设备移动规则
  - 创建设备移动规则
  - 复制设备移动规则
  - 设备移动规则的条件
- 手动将设备添加到管理组

手动将设备或者集群移动至管理组
关于集群和服务器阵列
集群或服务器阵列的属性
分发点和连接网关的调整
  分发点的标准配置：单一办公室
  分发点的标准配置：多个小远程办公室
  计算分发点的数量和配置
  自动分配分发点
  手动分配分发点
  修改管理组的分发点列表
  启用推送服务器
关于设备状态
配置设备状态切换
设备分类
  从设备分类中查看设备列表
  创建设备分类
  配置设备分类
  从设备分类中导出设备列表
  在分类中从管理组中删除设备
设备标签
  设备标签
  创建设备标签
  重命名设备标签
  删除设备标签
  查看分配了标签的设备
  查看分配到设备的标签
  手动标记设备
  从设备上删除分配的标签
  查看自动标记设备规则
  编辑自动标记设备规则
  创建自动标记设备规则
  为自动标记设备运行规则
  删除自动标记设备规则
数据加密和保护
  查看加密驱动器列表
  查看加密事件列表
  创建和查看加密报告
  授予对处于离线模式的加密驱动器的访问权限
  在管理服务器之间传输加密密钥
更改客户端设备的管理服务器
当设备显示不活动时查看和配置操作
远程访问受管理设备
  使用 OSMP 控制台从基于 Linux 的设备远程访问基于 Linux 的受管理设备
  使用 OSMP 控制台从基于 Linux 的设备远程访问基于 Windows 的受管理设备
  使用 OSMP 控制台从基于 Windows 的设备远程访问基于 Linux 的受管理设备
  使用 OSMP 控制台从基于 Windows 的设备远程访问基于 Windows 的受管理设备

管理资产
添加资产类别
配置资产表
搜索资产
导出资产数据
查看资产详情
添加资产
在OSMP中添加资产信息
从 Kaspersky Security Center 导入资产信息
从 MaxPatrol 导入资产信息
从 MaxPatrol VM 导入资产信息
kuma–ptvm–config.yaml 配置文件设置
从 KICS for Networks 导入资产信息
导入过程中的资产字段比对示例
kuma-ptvm-config.yaml 配置文件的设置
将类别分配给资产
编辑资产参数
归档资产
删除资产
删除资产类别
批量删除资产
更新 Kaspersky Security Center 资产中的第三方应用程序并修复漏洞
将资产移动到所选管理组
资产审计
配置资产审计
存储和搜索资产审计事件
启用和禁用资产审计
自定义资产字段
关键信息基础设施资产
部署 Kaspersky 应用程序
方案：Kaspersky 应用程序部署
保护部署向导
步骤 1：开始保护部署向导
步骤 2：选择安装包
步骤 3：选择分发密钥文件或激活码的方法
步骤 4：选择网络代理版本
步骤 5：选择设备
步骤 6：指定远程安装任务设置
步骤 7：重启管理
步骤 8：安装前删除不兼容的应用程序
步骤 9：移动设备到受管理设备
步骤 10：选择访问设备的账户
步骤 11：开始安装
添加卡巴斯基应用程序的管理插件
卸载管理 Web 插件
查看集成到 Open Single Management Platform 中的组件列表
查看 Kaspersky Next XDR Expert 组件的名称、参数和自定义操作

- 下载和创建卡巴斯基应用程序的安装包
- 从文件创建安装包
- 创建独立安装包
- 更改自定义安装包数据大小的限制
- 准备 Linux 设备以安装网络代理
- 准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理
- 为远程安装准备 Windows 设备
- 准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理
- 以静默模式安装 Linux 网络代理（使用应答文件）
- 查看独立安装包列表
- 将安装包分发至从属管理服务器
- 将 Kaspersky Next XDR Expert 与 Kaspersky Endpoint Security for Linux 一起部署
- 使用远程安装任务安装应用程序
  - 远程安装应用程序
  - 在从属管理服务器上安装应用程序
- 指定 Unix 设备上的远程安装设置
- 启动和停止卡巴斯基应用程序
- 替换第三方安全应用程序
- 远程删除应用程序或软件更新

配置卡巴斯基应用程序

- 方案：配置网络保护
- 关于以设备为中心和以用户为中心的安全管理方法
- 策略设置和传播：以设备为中心的方法
- 策略设置和传播：以用户为中心的方法
- 关于将网络代理切换到其他管理服务器
- 为漫游用户创建连接配置文件
- 策略和策略配置文件
  - 关于策略和策略配置文件
  - 关于“锁定”和锁定的设置
  - 策略继承和策略配置文件
    - 策略层级
    - 策略层级中的策略配置文件
    - 如何在受管理设备上实施设置
  - 管理策略
    - 查看策略列表
    - 创建新策略
    - 常规策略设置
    - 修改策略
    - 启用和禁用策略继承选项
    - 复制策略
    - 移动策略
    - 导出策略
    - 导入策略
    - 强制同步
    - 查看策略分发状态图
    - 在出现病毒爆发事件时自动激活策略
    - 删除策略

- 管理策略配置文件
  - 查看策略配置文件
  - 更改策略配置文件优先级
  - 创建策略配置文件
  - 复制策略配置文件
  - 创建策略配置文件激活规则
  - 删除策略配置文件
  - 导出和导入政策配置文件
- 网络代理程序政策设置
- Windows、Linux 和 macOS 网络代理的使用：比较
- 按操作系统比较网络代理设置
- 配置受管理应用程序的保护
- Kaspersky Endpoint Security 更新组任务的手动设置
- 卡巴斯基安全网络和卡巴斯基私人安全网络
  - 关于 KSN
  - 设置对 KSN 的访问
  - 启用和禁用 KSN 的使用
  - 配置与KPSN本地信誉数据库的连接
  - 查看已接受的 KSN 声明
  - 接受更新的 KSN 声明
  - 检查分发点是否充当 KSN 代理服务器
  - 查看 KSN 代理服务器的统计信息
- 管理端点保护任务
  - 关于任务
  - 关于任务范围
  - 创建任务
  - 手动启动任务
  - 为选择的设备执行任务
  - 查看任务列表
  - 常规任务设置
  - 导出任务
  - 导入任务
  - 启动更改任务密码向导
    - 步骤 1：指定凭证
    - 步骤 2：选择要采取的操作
    - 步骤 3：查看结果
  - 浏览保存在管理服务器中的任务运行结果
  - Kaspersky Endpoint Security 设备扫描组任务的手动设置
- 管理检测和响应任务
  - 查看任务表
  - 查看任务运行结果
  - 重新启动任务
- 应用程序标签
  - 创建应用程序标签
  - 重命名应用程序标签
  - 分配标签到应用程序

从应用程序上删除分配的标签
删除应用程序标签
在 OSMP 控制台中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序
管理用户和用户角色
关于用户账户
关于用于角色
配置对应用程序功能的访问权限。基于角色的访问控制
应用程序功能的访问权限
预定义用户角色
分配对特定对象的访问权限
分配权限到用户和组
添加内部用户账户
创建安全组
编辑内部用户账户
更改用户工作状态
编辑安全组
为用户或安全组分配角色
添加用户账户到内部安全组
指派用户作为设备所有者
配置双重身份验证
关于账户的双重身份验证
在OSMP云控制台登录时配置双重身份验证密钥
允许用户配置双重身份验证
重置和删除双重身份验证密钥
从双重身份验证中排除账户
编辑安全码签发者的名称
允许的密码输入尝试次数
配置用户 SSO 会话和身份验证令牌的生命周期
删除用户或安全组
更改用户账户密码
在登录页面添加自定义消息区块
创建用户角色
编辑用户角色
编辑用户角色范围
删除用户角色
关联策略配置文件到角色
配置 Kerberos 域身份验证
更新 Kaspersky 数据库和应用程序
方案：定期更新 Kaspersky 数据库和应用程序
关于更新 Kaspersky 数据库、软件模块和应用程序
创建"将更新下载至管理服务器存储库"任务
浏览已下载的更新
验证已下载的更新
创建"将更新下载至分发点存储库"任务
添加"将更新下载至管理服务器存储库"任务的更新源
批准和拒绝软件更新
自动安装 Kaspersky Endpoint Security for Windows 的更新

关于使用 diff 文件更新 Kaspersky 数据库和软件模块
启用下载 diff 文件功能
通过分发点下载更新
更新离线设备上的 Kaspersky 数据库和软件模块
客户端设备的远程诊断
打开远程诊断窗口
启用和禁用应用程序跟踪
下载应用程序的跟踪文件
删除跟踪文件
下载应用程序设置
从客户端设备下载系统信息
下载事件日志
启动、停止和重新启动应用程序
运行 Kaspersky Security Center 网络代理的远程诊断并下载结果
在客户端设备上运行应用程序
为应用程序创建内存转储文件
在基于 Linux 的客户端设备上运行远程诊断
管理客户端设备上的第三方应用程序和可执行文件
使用应用程序控制来管理可执行文件
应用程序控制模式和类别
获取并查看客户端设备上安装的应用程序列表
获取并查看客户端设备上存储的可执行文件列表
创建含有手动添加内容的应用程序类别
创建包括选定设备中的可执行文件的应用程序类别
创建包括选定文件夹中的可执行文件的应用程序类别
查看应用程序类别列表
在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”
添加事件相关的可执行文件到应用程序类别
创建“安装所需更新并修复漏洞”任务
“查找漏洞和所需更新”任务设置
关于授权许可
OPENAPI 参考指南
监控和报告
方案：监控和报告
关于监控和报告的类型
智能培训模式中的规则触发
查看并确认使用自适应异常控制规则执行的检测
从自适应异常控制规则添加排除
仪表板和小部件
使用仪表板
管理和保护小部件
添加小部件到仪表板
从仪表板隐藏小部件
移动小部件到仪表板
更改小部件尺寸或样子
更改小部件设置

检测和响应小部件
有关管理小部件的基础操作
在小部件中显示数据的特殊注意事项
创建小部件
编辑小部件
删除小部件
小部件设置
事件小部件
“活动列表”小部件
上下文表小部件
资产自定义小部件
其他小部件
过滤小部件数据
过滤单个小部件上的数据
过滤多个小部件中的数据
深层探究到相关控制板
在活动列表类型小部件中显示租户名称
检测和响应控制板
创建仪表板布局
选择仪表板布局
将某个仪表盘布局设置为默认布局
编辑仪表板布局
删除仪表板布局
启用和禁用 TV 模式
预配置仪表板布局
关于仅仪表板模式
配置仅仪表板模式
管理和防护报告
使用报告
报告模板
创建报告模板
查看和编辑报告模板属性
删除报告模板
通用报告模板
导出报告到文件
生成和浏览报告
创建报告发送任务
检测和响应报告
报告模板
创建报告模板
配置报告计划
编辑报告模板
复制报告模板
删除报告模板
导出或导入报告模板
通用报告模板

- 生成的报告
  - 查看报告
  - 生成报告
  - 保存报告
  - 更新报告
  - 删除报告
- 事件和事件分类
  - 关于 Kaspersky Next XDR Expert 中的事件
  - Kaspersky Next XDR Expert 组件事件
    - 事件类型描述的数据结构
    - 管理服务器事件
      - 管理服务器严重事件
      - 管理服务器功能失败事件
      - 管理服务器警告事件
      - 管理服务器信息事件
    - 网络代理事件
      - 网络代理警告事件
      - 网络代理信息事件
  - 使用事件分类
  - 创建事件分类
  - 编辑事件分类
  - 查看事件分类列表
  - 导出事件分类
  - 导入事件分类
  - 查看事件详情区域
  - 导出事件到文件
  - 从事件查看对象历史
  - 删除事件
  - 删除事件分类
  - 设置事件存储期限
  - 阻止频繁事件
    - 关于阻止频繁事件
    - 管理频繁事件阻止
    - 移除对频繁事件的阻止
  - 在管理服务器上的事件处理和存储
- 回溯扫描
- 通知和设备状态
  - 使用通知
  - 查看屏幕通知
  - 关于设备状态
  - 配置设备状态切换
  - 配置通知传送
  - 测试通知
  - 用于描述事件的参数和环境变量

监控事件源
源状态
事件源列表
监控策略
卡巴斯基公告
关于 Kaspersky 公告
禁用 Kaspersky 公告
Cloud Discovery
使用小部件启用 Cloud Discovery
将 Cloud Discovery 小部件添加到仪表板
查看有关云服务使用的信息
云服务的风险级别
阻止对不需要的云服务进行的访问
导出事件到 SIEM 系统
配置导出事件到 SIEM 系统
先决条件
关于事件导出
关于配置 SIEM 系统中的事件导出
标记要以 Syslog 格式导出到 SIEM 系统的事件
关于标记要以 Syslog 格式导出到 SIEM 系统的事件
标记要以 Syslog 格式导出的 Kaspersky 应用程序事件
标记要以 Syslog 格式导出的常规事件
关于使用 Syslog 格式导出事件
关于使用 CEF 和 LEEF 格式导出事件
将事件转换为 CEF 或 LEEF 格式
配置 Kaspersky Next XDR Expert 以将事件导出到 SIEM 系统
监控策略和策略配置文件的更改
直接从数据库导出事件
使用 klsql2 实用工具执行 SQL 查询
klsql2 实用工具中的 SQL 查询例子
查看 Kaspersky Next XDR Expert 数据库名称
查看导出结果
将事件从 OSMP 收集器发送到外部 SIEM 系统收集器
管理对象修订
查看并保存策略修订
比较策略修订
回滚对象到先前修订
对象删除
从隔离区和文件备份下载和删除文件
从隔离区和文件备份区下载文件
关于从隔离区、文件备份区或活动威胁存储库中删除对象
上传文件进行扫描
手动扫描存储库中的文件
查看扫描状态和扫描结果

- Kaspersky Next XDR Expert 组件的运行诊断
  - 获取 Kaspersky Next XDR Expert 组件的日志文件
  - 查看 OSMP 指标
    - 监控 Kaspersky Next XDR Expert 组件的状态
    - 配置有关Kubernetes集群运行状况事件的电子邮件通知
    - 管理Kubernetes集群运行状况事件的电子邮件通知收件人
    - 在不重新安装Kaspersky Next XDR Expert的情况下，将SMTP服务器连接参数添加到配置文件
    - 查看 Longhorn 指标
    - 查看EDR控制板和指标
    - 查看Node Exporter完整版控制板
  - 服务监控
    - 查看 KUMA 指标
    - KUMA指标警报触发条件
  - 存储有关 Kaspersky Next XDR Expert 组件的诊断信息
  - 获取跟踪文件
  - 记录自定义操作的启动
- 多租户
  - 关于将管理服务器绑定到租户
  - 配置与 Open Single Management Platform 的集成
  - 查看和编辑租户
  - 添加租户
  - 为租户中的用户和用户组分配角色
  - 删除租户
  - 配置邮件通知
  - 创建通知模板
  - 编辑和删除通知模板
  - 配置用于访问共享网络资源的凭证存储
  - 配置定期IOC扫描
  - 配置文件存储库中文件的自动轮换
- 联系技术支持
  - 如何获取技术支持
  - 通过 Kaspersky CompanyAccount 获得技术支持
- 已知问题和限制
- 故障排除
- 附录
  - 组件手动启动和安装命令
  - KUMA 文件的完整性检查
  - 规范化事件数据模型
  - 配置来自 KATA EDR 的规范化事件的数据模型
  - 资产数据模型
  - 用户账户数据模型
  - 审计事件
    - 用户已编辑字段集设置来定义来源
    - 密钥文件已添加
    - 备用授权许可密钥已添加
    - 备用授权许可密钥已删除
    - 应用程序已使用激活码激活。

授权许可已续期。
无效的激活码
激活码已被阻止
激活码或密钥文件已删除
EPS已超限
授权许可已到期，宽限期已开始
宽限期结束
已添加过期的激活码或密钥文件
用于区分事件访问权限的空间集已更改
服务监控阈值已更改
KUMA Core设置已修改
GeoIP数据库已导入
服务已创建
服务已删除
服务已重新加载
服务已重新启动
服务已启动
服务已配对
任务状态已更改
分区已被用户删除
分区将在保留期结束后自动删除
分区已按绝对保留期删除
分区已按相对保留期删除
分区已移至冷存储
将分区移至冷存储时出错
活动列表清除成功或操作失败
活动列表项更改成功或操作失败
活动列表项删除成功或操作失败
活动列表导入成功或操作失败
活动列表已导出
上下文表已导出
上下文表导入成功或操作失败
上下文表项修改成功或操作失败
上下文表项已修改或操作失败
上下文表清除成功或操作失败
资源已添加
资源已删除
资源已更新
导入资源
设置已更新
已成功在服务上更新字典或操作失败
字典条目已添加
字典条目删除成功或操作失败
扩展事件模式字段已创建
扩展事件模式字段已编辑
扩展事件模式字段已导入
带有扩展事件模式字段的规范化器已导入

- 扩展事件模式字段已删除
- 发送至 KIRA 的请求
- KICS/KATA响应
- Kaspersky Automated Security Awareness Platform 响应
- KEDR response
- 导入MITRE ATT&CK技术和策略
- 指标警报已注册服务或操作失败
- Active Directory 中的响应
- 备份分区、从备份中还原、从外部安装的KUMA导入分区
- 使用KIRA将自然语言查询转换为SQL查询。
- 事件读取尝试
- 搜索请求已取消
- KEDR资源已更新
- KEDR资源更新任务已完成
- KEDR事件字段已更新
- 文件localizations.json已导入
- 规则已链接到收集器
- 规则已与收集器取消关联
- 规则已关联到关联器
- 规则已与关联器解除关联
- 从 KUMA 导出的资源
- 从隔离网段接收有关事件的服务数据

- 关联规则
- 时间格式
- 映射预定义规范化器的字段

词汇表

- Bootstrap
- EPP 应用程序
- IOA规则
- IOC 文件
- Kubernetes 集群
- KUMA 服务
- KUMA 清查文件
- Observables
- 上下文
- 事件
- 事件路由器
- 事故
- 代理
- 传输存档文件
- 关联器
- 关联规则
- 分发包
- 分段规则
- 卡巴斯基部署工具包
- 取证信息
- 响应操作

- 多租户
- 威胁发展链
- 存储
- 收集器
- 注册表
- 目标主机
- 租户
- 管理员设备
- 网络代理
- 网络位置识别 (NLA)
- 自定义操作
- 节点
- 行动手册
- 行动手册算法
- 规范化事件
- 警报
- 调查图
- 资产
- 轻量级 Nagent（LWNGT）
- 配置文件

有关第三方代码的信息

商标声明

The MITRE Corporation Terms of Use

Kaspersky Next XDR Expert

新功能

- Kaspersky Next XDR Expert 中的新功能

主要功能

- 管理警报和安全事故
- 威胁搜索工具
- 调查图表
- 预定义和自定义行动手册
- 手动威胁响应操作
- 仪表板和小部件

兼容性及硬件和软件要求

- 硬件和软件要求
- 兼容的应用程序和解决方案
- 与其他解决方案和第三方系统集成

启动

- Kaspersky Next XDR Expert 的部署、激活和初始配置的演练场景
- 部署 Kaspersky Next XDR Expert
- 迁移到 Kaspersky Next XDR Expert
- 使用威胁监控、检测和搜索功能
- 使用 Kaspersky Next XDR Expert 进行事故调查的示例

使用 Open Single Management Platform

- 在公司网络中的设备上安装卡巴斯基安全应用程序
- 远程运行扫描和更新任务
- 管理受管理应用程序的安全策略

新闻

Kaspersky Next XDR Expert 2.3

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 在包含警报详情和事故详情的窗口中，您可以在**可观察对象**部分中根据**值**列中的数据搜索可观测对象表。
- 向状态为**新建**的事故添加警报或从中删除警报时，系统会自动重新评估事故优先级。优先级将设置为**事故严重性**的值。
- 现已提供新的预定义行动手册：
  - [KL][EDR]“缓解警报中电子邮件附件引发的恶意活动”行动手册
  - [KL][EDR]“缓解事故中电子邮件附件引发的恶意活动”行动手册
  - [KL][EDR]“缓解警报中的内存转储活动”行动手册
  - [KL][EDR]“缓解事故中的内存转储活动”行动手册
  - [KL][EDR]“根据警报检测到发现活动时隔离主机”行动手册
  - [KL][EDR]“根据事故检测到发现活动时隔离主机”行动手册
  - [KL][EDR]“检测到数据渗出活动时隔离主机”行动手册
  - [KL][EDR]“删除警报中传输到主机的恶意文件”行动手册
  - [KL][EDR]“删除事故中传输到主机的恶意文件”行动手册
  - [KL][EDR]“根据警报检测到反向 shell 活动时隔离主机”行动手册
  - [KL][EDR]“根据事故检测到反向 shell 活动时隔离主机”行动手册

Kaspersky Next XDR Expert 2.2

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 可以在首次登录后强制要求用户账户更改密码，或在经过指定天数后强制要求更改。
- 分段和聚合规则的改进：
  - 现在支持继承。
  - 现在可以在 **监控** → **资源和服务** 部分配置规则。
- 新增了两个连接器，用于通过 SMB 和 SFTP 协议接收日志文件。
- 新的可选参数 `--pair.fingerprint` 有助于提高服务与 KUMA Core 连接的安全性。从 Kaspersky Next XDR Expert 2.2 开始，创建服务时，安装向导默认会在安装命令中包含 CA 证书指纹。例如：`/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:7210 --pair.fingerprint XXXX --id YYYY --api.port ZZZZ --install`。如果您不想使用指纹进行身份验证，可以输入 `insecure` 作为该选项的值。从 Kaspersky Next XDR Expert 2.1 升级到 2.2 时，无需执行任何其他操作。在 Kaspersky Next XDR Expert 2.2 之前安装的服务升级后默认使用 `insecure` 值。如果将 CA 证书指纹 ID 用于 `--pair.fingerprint` 选项，则在重新颁发 CA 证书后，您需要从 Web 界面复制新的指纹 ID，在 systemd 配置中将该选项更新为新值，然后重新启动服务。
- 新增了一种**转换类型 unicodeUnescape**，用于在将原始事件字段的值写入 OSMP 事件字段之前，将其从 Unicode 字符串转换为人类可读的文本。

  转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

  可用转换：
  - **lower** — 用于将值的所有字符变为小写
  - **upper** — 用于将值的所有字符变为大写
  - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
  - **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
  - **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
    - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
    - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
  - **trim** — 用于同时从值的开始和结束位置删除“**字符**”字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
  - **append** 用于将“**常量**”字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。

- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

- 现在，您可以使用安装在隔离网络段内的代理，将来自该网络段的事件服务数据发送到收集器。
- 现在可以为 XDR 功能区域配置更精细的租户访问权限。

- Kaspersky Deployment Toolkit 的改进和新增功能：
  - 引入了 **XDR Deployer**，这是一个分步交互式向导，可自动执行操作系统准备、预检查和应用程序部署。
  - 现在可以配置访问令牌、刷新令牌和 SSO 会话的生命周期。可在部署前通过配置文件参数进行配置，也可在部署后使用自定义操作进行配置。
  - 除了日志文件中记录外，严重部署错误现在还会直接显示在控制台窗口中。
  - 新增了 `./kdt metrics export` 命令，该命令可用于获取关键 OSMP 指标的压缩文件，以便进一步导入和分析。
- 用户体验改进：
  - 在资产详细信息中，现在可以搜索已安装软件列表。
  - 现在，您可以更改用于 EDR 代理连接到代理服务器的默认端口，以及用于通过浏览器访问 OSMP Console 服务器的默认端口。
  - 改进了不包含 `ProcessUniqueId` 字段的事件的调查图节点之间的链接。
  - 新增了从事故详情和警报详情到 Kaspersky TIP 的导航，以便查看有关 MITRE ATT&CK 战术和技术的详细信息。
  - 警报表和事故表现在包含 **外部引用** 列。
  - 新增了编辑和删除警报及事故评论的时间限制。现在可以将这些操作设置为在警报或事故创建后的指定时间段过后不再可用。
- 以下功能继承自 Kaspersky Security Center Linux：
  - 增强了**任务**和**策略**表的筛选功能。现在，您可以使用“或”逻辑添加多个条件，还可以使用新的操作符，该操作符允许您为单个属性选择多个值，并显示至少符合一个指定条件的记录。
  - 分发点分配功能已改进：列表现在仅显示未分配的分发点。
  - 现在，您可以一次性为多个虚拟管理服务器分配管理员。
  - 在主菜单中：
    - 新增了**软件管理**部分。以下部分现在已移至 **软件管理**：**安装包**、**卡巴斯基应用程序**、**第三方应用程序**、**当前应用程序版本**和**补丁管理**。
    - **未分配的设备**和**硬件**部分现已移至**资产管理**。
    - **任务**和**存储库**部分已移至菜单第一级。
    - “Web 插件备份”部分已不再使用，并已从 Web Console 中移除。
- Kaspersky Deployment Toolkit现在支持以下操作系统版本：
  - Ubuntu Server 26.04 LTS
  - Astra Linux 特别版 RUSB.10015-01（操作更新 1.8.5）

- Kaspersky Next XDR Expert现在支持以下操作系统版本：
  - Ubuntu Server 26.04 LTS
  - Astra Linux 特别版 RUSB.10015-01（操作更新 1.8.5）
- 现在支持以下虚拟化平台：
  - Microsoft Hyper-V Server 2022
  - Nutanix 7.3
- Kaspersky Next XDR Expert现在支持使用以下DBMS：
  - PostgreSQL 18.4 64 位
  - Postgres Pro 18 Enterprise 64 位（集群内置高可用性）
- 新增了在事件卡中对 `DeviceCustom*` 和 `Flex*` 字段使用紧凑显示模式的功能，其中 `Label*` 字段值显示为字段名称。
- 新增了知识库部分，用于处理 KUMA 软件包和资源。用户可以在该区域中搜索和筛选软件包和资源、查看其相关信息、安装整个软件包或单个资源、更新资源，以及查看它们之间的依赖关系。
- 新增了hexToDecimal转换类型，用于在将源事件字段值存储到 KUMA 事件字段之前，将其从十六进制转换为十进制。
- 使用 **regexp** 解析方法的规范化器现在支持使用 KIRA 根据已添加的示例生成正则表达式。在这种情况下，生成的正则表达式会自动添加到**规范化**字段。
- 新增了在创建 SQL 查询时提供函数建议的功能。在 SQL 查询字段中输入函数名称时，系统会显示可用函数列表，并显示所选函数的用法示例。
- 附加规范化现在可用于以 sFlow 格式接收的事件。
- 在 DNS 扩充期间降低了 DNS 服务器的负载：发生事件时，解决方案会进行两次扩充尝试。联系 DNS 服务器后，收集器会将有关 IP 地址和主机名的信息缓存到磁盘上。该数据会在缓存记录的整个保留期内使用。事件记录会存储在磁盘上，直到从 DNS 服务器中删除缓存或记录为止。
- 为了从隔离的网段接收 NetFlow 事件，需要使用安装在该网段内的专用代理。该代理充当中间节点：它在本地接收 NetFlow 事件，并将其转发到配置了 NetFlow 连接器的收集器。
- 新增了用于测试与 SMTP 服务器的连接的按钮。为了测试连接，Kaspersky Next XDR Expert 会向当前用户配置文件中指定的电子邮件地址发送测试消息。
- 从存储库导入资源时，会使用KUMA Core 设置区域中 KUMA 资源本地化设置所指定的语言。
- 在 Kaspersky Next XDR Expert 2.1 中作为 Beta 版本添加的两项功能（周期类型的关联规则和未经授权使用账户的检测）在 Kaspersky Next XDR Expert 2.2 中不可用。计划在 Kaspersky Next XDR Expert 的下一个版本中重新设计并发布这些功能。
- 新增了对使用 ODBC 驱动程序的SQL 连接器的支持。
- 新增了http-streaming 类型的连接器，用于通过 HTTP 接收流式事件。

Kaspersky Next XDR Expert 2.1

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 用户活动审计事件现位于**威胁搜索**部分。这些事件提供了有关用户操作的详细信息，并在**EventType**字段中标记了`Audit`值。
- 在威胁搜索**威胁搜索事件搜索**时，对于手动运行的查询，会生成一个审计事件。
- [OOTB] Kaspersky OSMP 收集器用于从 OSMP 组件接收审计事件（审计事件、审计事件）。该收集器会在OSMP部署期间自动安装。审计事件发送到审计空间，该空间在存储中自动创建。
- 资产筛选选项包括：**仅显示子实例**和**仅显示父实例**。这些选项允许您根据资产属于子实例还是父实例来筛选资产。所选筛选条件将直接应用于资产表，并立即更新显示结果。
- 删除资产类别分两个阶段进行：归档和永久删除。归档允许您在从系统中永久删除之前验证该类别是否仍然被任何资源引用。
- 新增调查和响应功能：
  - 在您指定延迟原因之前，针对违反SLA的事件的操作将被阻止。
  - 现在警报和事件详情的加载速度更快。
  - 现在可以通过API导出和导入行动手册。您可以使用它轻松地在租户和实例之间传输行动手册。
  - 增加了比较行动手册不同版本的功能，以跟踪更改并简化版本管理。
  - 现在可以查看行动手册和响应操作执行的详细结果。您可以通过单击**行动手册状态**或**操作状态**值在**响应历史**部分中查看它们，这将打开执行详细信息面板。
  - 现在您可以在Kaspersky TIP中查看IOA规则的详细信息。为此，请在警报或事件详情或IOA规则详情中，单击**在 Kaspersky TIP 中查找**按钮。
  - 新的预定义行动手册现已可用：
    - 检查外部IP地址的行动手册。
    - 用于隔离检测到受感染文件的设备的行动手册。
- 现在打开运行状况监控控制板更加便捷。您无需再输入URL，只需在Kaspersky Next XDR Expert中单击按钮即可。
- 文件管理功能改进：
  - 文件上传进度现在显示在文件部分。您可以将文件直接上传到**文件**部分，也可以将其附加到警报或事件。上传进度只能在**文件**部分跟踪，所有已上传的文件都会自动显示在此处。
  - 您现在可以在**文件**部分启用自动文件轮换。启用此功能后，系统会删除最旧的文件以释放空间，方便上传新文件。与检测到的威胁关联的文件不会被删除，并会继续关联到相应的警报。

- 对OSMP实例层次结构的改进：
  - 现在您可以将阻止规则分配到整个层次结构中。
  - 现在您可以将YARA和IOC规则分配到整个层次结构中。
- 改进了进程树状图可视化功能。现在，进程树状图数据按需加载，而不是一次性检索所有相关事件。
- 改进了沙盒中用户活动的日志记录：
  - 沙盒中已扩展了已记录用户操作的集合。
  - 现在可以在沙盒中查看用户活动日志。
- OSMP可以使用Syslog协议将应用程序网页界面中的用户操作信息以及警报导出到外部SIEM系统。SIEM系统可以是KUMA（独立解决方案）或第三方SIEM系统。
- OSMP分发包包含一个预定义的关联规则，该规则会在三次身份验证失败后生成关联事件。
- 已将`DeviceEventCategory`参数添加到在按相对保留期删除分区时生成的审计事件中。
- 现在可以指定最大EPS值来确定回溯扫描中的最大负载。
- 现在支持在 extract_from_timestamp 函数中使用 `$timezone` 变量。时区可以动态设置，包括通过关联规则的局部变量中定义的字典变量。
- 现在，使用 Kaspersky Investigation and Response Assistant 分析警报和事故时，您可以使用**自定义**模式。在**自定义**模式下，请求将直接发送到指定的第三方LLM提供商的API。
- 以下功能继承自 Kaspersky Security Center Linux：
  - 您可以比较政策修订版本。此选项适用于管理服务器、网络代理程序、 Kaspersky Endpoint Security for Windows （从14.0网页插件版本开始）以及 Kaspersky Endpoint Security for Mac（从12.2.1 Patch A网页插件版本开始）的政策。未来版本将扩展支持此功能的卡巴斯基应用程序列表。
  - 您可以将事件以CEF或LEEF格式导出到SIEM系统。
  - 改进了 Linux 设备上用于保留网络代理设备标识符（`Device ID` 参数）的算法。如果设备的 BIOS 序列号、主板序列号、存储磁盘标识符或 MAC 地址与之前已知的值匹配，则在操作系统更新或 MAC 地址更改后，管理服务器能够正确识别该设备，将其视为之前已发现的设备。
  - 网络代理现支持 Windows ARM 64 位架构。与受管理应用程序的兼容性可以在相应的帮助文档中进行验证。
  - 现在提供适用于 Linux 的网络代理的单一安装包。此安装包包含适用于不同软件包管理器和 CPU 架构的版本。安装过程中，系统会自动检测环境并安装相应的网络代理软件包。
  - 在隔离网络中，为Windows设备创建安装套件现在需要从卡巴斯基网站下载其他模块。
  - Linux网络代理程序现在支持无法解析本地主机的环境。
  - 您现在可以一次性删除事件分类和设备事件列表中的所有事件。
    事件分类选择和设备事件列表中均提供**全部选择**和**在当前页面上全选**。

    - 您现在可以手动指定移动规则优先顺序。
      选择移动规则后， **更改优先级**按钮将变为可用状态，允许您指定新的优先级。

- Kaspersky Deployment Toolkit现在支持以下操作系统版本：
    - Astra Linux特别版RUSB.10015-01（操作更新1.8.2）
    - Oracle Linux 9.7
- 网络代理现在支持与以下新操作系统版本配合使用：
    - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM
    - Platform V SberLinux OS Server (SLO) 9.6
- Kaspersky Next XDR Expert现在支持以下操作系统版本：
    - Astra Linux特别版RUSB.10015-01（操作更新1.8.2）
- 现在支持以下虚拟化平台：
    - VMware vSphere 9
- Kaspersky Next XDR Expert现在支持使用以下DBMS：
    - PostgreSQL 17.9 64 位
    - PostgreSQL 18.3 64 位
    - Postgres Pro 17.7.1 Enterprise 64 位（集群内置高可用性）

Kaspersky Next XDR Expert 2.0

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 统一 OSMP 控制台：您现在可以在 Kaspersky Next XDR Expert 中管理 Kaspersky Unified Monitoring and Analysis Platform 和 Kaspersky Endpoint Detection and Response 场景。
- Kaspersky Endpoint Detection and Response 已推出新的响应操作：
    - 管理服务
    - 删除文件
    - 获取文件
    - 从隔离区获取文件
    - 扫描从设备获取或用户上传的文件
    - 获取内存转储

    - 获取进程内存转储
    - 获取磁盘映像
    - 获取取证信息
    - 获取注册表键
    - 获取 NTFS 元文件
    - YARA 扫描
    - IOC 扫描
    - 从隔离区恢复文件
    - 从隔离区删除文件
- 新增 AI 功能：
    - 使用KIRA生成警报和事故的简要报告，以提高分析效率。
    - AI 会分析账户行为，并在检测到可疑活动或账户被入侵迹象时生成警报。
    - AI 会检测合法应用程序加载恶意的 DLL 并替换原始 DLL 的攻击。
    - AI 现在可以帮助您在**威胁搜索**部分生成 SQL 查询。
- 所有账户现在都需要双重身份验证以增强安全性。
- 您现在可以在测试模式下启动行动手册，以便在执行前检查其功能。
- 您现在可以从**资产(设备)**和**响应历史**部分以及**事件详情**中启动响应操作。
- 现在可以使用更新后的参数重新运行响应操作；
- 新增远程终端访问功能，用于直接进行设备调查和响应操作。
- 调查图改进：
    - 现在您可以根据时间线将事件放置在调查图上。较早的事件显示在左侧，较晚的事件显示在右侧。
    - 事件树现在显示在专用面板中，而不是直接显示在图上。
    - 图表上的事件现在按照时间线排列：较早的事件显示在左侧，较晚的事件显示在右侧。
    - 现在您可以为整个流程树和单个节点添加注释。
    - 缩放图表时，节点可以分组到集群中，您可以展开集群以在优化比例下查看底层节点。
- 针对事件实施了新的数据模型。

- 新增了以下警报类型：
  - 基于文件扫描结果生成的警报。
  - 当文件在之前的警报中未被分析后再次扫描时，系统会创建重新扫描警报。
  - 由 TAA (IOA) 检测技术生成的警报。
  - 由 IOC 检测技术生成的警报。
  - 由 YARA 检测技术生成的警报。
- 现在可以在Kaspersky Endpoint Security for Windows策略中配置IOA排除项设置，可以直接在策略中配置，也可以从警报或事件详细信息中进行配置；
- 现在您可以配置用户身份验证策略，包括密码有效期和用户会话终止前允许的非活动时间。
- 增加了对分层多租户的支持。安装程序可以组织成父实例和子实例，并且可以从父实例连接到子实例。
- "**资产(设备)**"部分现在包含两个选项卡：
  - "**资产(设备)**"，您可以在其中管理和分类设备；
  - "**分析和响应**"，您可以在其中对列出的资产启动响应操作并通过远程终端连接到它们。
- 您现在可以创建和管理以下自定义规则：
  - 防御规则
  - IOC 规则
  - YARA 规则
  - 沙盒规则
- 现在，当启用与卡巴斯基沙盒的集成时， Kaspersky Endpoint Security for Windows和Kaspersky Endpoint Security for Linux均可自动和手动向沙盒发送文件。
- 现在支持物理隔离部署：
  - 在具备辅助功能的互联网管理主机上准备软件包存档。
  - 将该软件包存档传输到隔离环境。
  - 在无法访问互联网的目标主机上安装Kaspersky Next XDR Expert。
- 增加了对上传服务器和端点代理程序凭证的支持，以在它们之间建立安全连接。
- 增加了上传用于连接到沙盒的凭证的功能。
- 现在支持 FreeIPA 和 ALD Pro 域控制器。
- 您的账户菜单现已从主菜单移至顶部窗格。
- 新增语言支持：Kaspersky Next XDR Expert 现已支持简体中文和繁体中文。

- SIEM 组件 (KUMA) 中引入的新功能和改进：
  - 指标服务可以安装在任意主机上。只能存在一个指标服务。从头开始安装 KUMA 时，您必须在清查文件的“`kuma_metrics`”部分指定用于安装指标服务的主机。将 KUMA 升级到 4.2 版本时，您必须在清查文件的“`kuma_metrics`”部分指定安装了活动指标服务的主机。例如，如果在 KUMA 4.0 中，指标服务安装在主机 kuma-core.example.com 上，那么在升级到 4.2 版本之前，需要在清查文件的 kuma_metrics 部分中指定 kuma-core.example.com 主机。如果要将指标服务迁移到另一台主机，可以使用 expand.sh 安装程序和 expand.inventory.yml 清查文件来完成此操作。

    将 KUMA Core 迁移到 Kubernetes 集群时，必须首先使用 expand.sh 安装程序和 expand.inventory.yml 清查文件将指标服务迁移到与 KUMA Core 相同的主机。将 KUMA Core 迁移到 Kubernetes 集群时，会检查指标服务是否在此主机上运行。如果找不到指标服务，则会返回错误并停止迁移。当您将 KUMA Core 迁移到 Kubernetes 集群时，指标数据也会迁移到集群中。
  - 您可以按计划备份分区、手动备份分区、从备份恢复分区，或者从外部 KUMA 安装导入分区。
  - 现在您可以使用 Web 界面备份和恢复 KUMA Core。
  - 对于冷存储， ClickHouse 集群中的数据现在可以传输到 S3 云存储。
  - Kafka 连接器现在使用 SCRAM-SHA-256 和 SCRAM-SHA-512 安全连接机制进行授权。
  - 新增了 universalAPI 连接器，用于从任意 REST API 获取数据，支持 JSON、按 IDS 筛选和迭代模式。
  - 现在，您可以以较低的优先级在后台运行 SQL 请求，并在执行完成后查看结果。
  - 使用主管理员帐户时，您现在可以查看和管理其他用户的活动请求。
  - 新增了周期性关联规则类型，用于通过检测可能表明账户已泄露的异常用户活动，检测未经授权的账户使用情况。只有在使用 correlator-ng 关联器时，才能创建此规则。
  - 现在，您可以在用户帐户中配置时区和 ISO 8601 格式，还可以为整个 KUMA 实例自定义每周的第一天（仅主管理员可用）。
  - 现在，您可以将资源（关联规则、丰富规则、响应规则、聚合规则和目标）关联到收集器、关联器和事件路由器等服务。可用服务取决于所选资源的类型。
  - 新增的 UDP 目标类型允许通过 UDP 从收集器和关联器传输规范化事件。
  - 现在，您可以在上下文表中以 CSV 和 TSV 格式导出数据。
- Kaspersky Security Center for Linux 16.1 增加了新功能并进行了改进。

Kaspersky Next XDR Expert 1.4

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 升级 Kaspersky Next XDR Expert 时，您可能需要更新 Bootstrap，具体取决于您要升级的版本。

  - **需要更新 Bootstrap 的升级**

    对于 Kaspersky Next XDR Expert 的以下升级，更新 Bootstrap：

    - 版本 1.3 → 版本 1.4 Hotfix 6 或更高版本
    - 版本 1.4 → 版本 1.4 Hotfix 6 或更高版本
    - 版本 1.4 Hotfix 1 → 版本 1.4 Hotfix 6 或更高版本
    - 版本 1.4 Hotfix 2 → 版本 1.4 Hotfix 6 或更高版本

    要更新 Bootstrap，请运行以下命令：

    ```
    ./kdt apply -k <XDR 更新存档路径> -i <配置文件路径> --force-bootstrap
    ```

    然后，运行以下命令来升级 Kaspersky Next XDR Expert：

    ```
    ./kdt apply -k <XDR 更新存档路径>
    ```

  - **不需要更新 Bootstrap 的升级**

    对于 Kaspersky Next XDR Expert 的以下升级，不要更新 Bootstrap：

    - 版本 1.4 Hotfix 3 → 版本 1.4 Hotfix 6 或更高版本
    - 版本 1.4 Hotfix 4 → 版本 1.4 Hotfix 6 或更高版本

    要升级 Kaspersky Next XDR Expert，运行以下命令：

    ```
    ./kdt apply -k <XDR 更新存档路径>
    ```

- 您现在可以为处理事故设置固定响应时间 (SLA)。SLA 指标包括完全解决事故花费的时间、首次响应花费的时间以及确认事故花费的时间。
- 现在支持 Postgres Pro 内置高可用性集群。此 DBMS 集群的节点在安装 Kaspersky Next XDR Expert 时在连接字符串中指定。
- 您现在可以保存 Kaspersky Next XDR Expert 数据的备份副本，然后从创建的副本中恢复数据。
- 您现在可以添加或删除包含在 Kubernetes 集群中的工作节点，而无需重新启动集群节点。
- 支持将行动手册保存为草稿。行动手册草稿无法启动，但可以在行动手册所属的租户中进行编辑。要启动行动手册草稿，您需要先将其发布。
- 您现在可以针对任何图节点或链接留下评论。

- 支持将事故导出为 PDF。
- 您现在可以将警报或事故所影响或所涉及资产的相关信息以及当前事故关联警报的相关可观察对象的信息导出为 CSV 文件。
- 您可以手动或使用行动手册将警报和事故分配给用户组。如果您要根据组内用户的工作量和可用性状态自动分配警报和事故，则可以启用自动分配功能。
- 行动手册可视化编辑器现在可用于创建行动手册。行动手册可视化编辑器允许您构建和可视化行动手册执行流程，以及行动手册算法步骤之间的关系。
- 将警报关联到事故时，会显示警报和事故的名称。该操作可以按名称过滤警报和事故。
- 警报和事故的过滤功能已加以改进。
- 如果有多条聚合规则应用于该警报，这些聚合规则将按指定优先级依次处理，而非仅处理找到的第一条规则。
- 现在可以使用 Linux 设备漫游用户的连接配置文件。使用连接配置文件，您可以为 Linux 设备上的网络代理配置规则，以连接到相同或不同的管理服务器，具体取决于设备位置。
- 现在可以在管理服务器之间传输加密密钥。
- "**扫描**"按钮已从"**隔离**"部分删除。

Kaspersky Next XDR Expert 1.3

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 应用程序中使用了更新版本的 Bootstrap。在安装新版本的 Kaspersky Next XDR Expert 之前，请运行以下命令来更新 Bootstrap：

  ```
  ./kdt apply -k <XDR 更新存档路径> -i <配置文件路径> --force-bootstrap
  ```

- 您现在可以创建子事故。您可以根据子事故来调查不同租户中的事故并做出响应。
- Kaspersky NGFW 可用于事故响应方案。您可以使用 KUMA 清查文件为 Kaspersky NGFW 创建服务。Kaspersky NGFW 提供以下功能：
  - 通过 Kaspersky NGFW 阻止 IP 地址。
  - Kaspersky NGFW 的新仪表板。
- 您现在无需重新安装，即可借助卡巴斯基部署工具包来更改 Kubernetes 集群 IP 地址和服务的 FQDN。
- 预验证配置文件中的参数。在开始安装或更新 Kaspersky Next XDR Expert 之前，卡巴斯基部署工具包会验证配置文件中是否存在参数以及这些参数的值。该功能适用于单节点和多节点部署。
- 您现在可以在 Kaspersky Next XDR Expert 的用户界面中管理聚合规则。
- 新增了"**按类型分组的事故**"小部件。

- 以下仪表板小部件现在显示未关闭事故的信息：
  - 活动事故
  - 按租户分组的活动事故
  - 按严重级别分组的事故
  - 事故中受影响的资产
  - 事故中受影响的资产类别
  - 最新事故
- 您可以合并的与事故关联的警报数量限制已提高。可合并的与事故关联的警报数量上限为 1000。合并事故时，与这些事故关联的警报数量将显示在“**合并事故**”窗口中。
- 私有 IP 地址不再包含在与警报或事故相关的可观察对象中。
- Kaspersky Next XDR Expert 现在支持新版本的 EPP 应用程序。

Kaspersky Next XDR Expert 1.2

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 应用程序中使用了更新版本的 Bootstrap。在安装新版本的 Kaspersky Next XDR Expert 之前，请运行以下命令来更新 Bootstrap：

  ```
  ./kdt apply -k <XDR 更新存档路径> -i <配置文件路径> --force-bootstrap
  ```

- Kaspersky Next XDR Expert 从 1.1 版升级到 1.2 版。
- 优化了 Kaspersky Next XDR Expert 的部署：改进的配置文件和快速启动向导，便于输入安装参数。
- 部署初步检查。您现在可以在部署 Kaspersky Next XDR Expert 之前，检查是否满足系统要求。卡巴斯基部署工具包 (KDT) 会检查您的硬件、操作系统、软件和网络环境。如果至少有一项要求未满足，KDT 将中断部署并向您提供详细报告。
- 灵活的事故工作流。您可以配置事故工作流并在可视化编辑器中查看。
- 您现在可以为警报或事故附加文件。如有必要，您可以删除或下载附加的文件。
- 根据事故类型自定义事故处理流程。
- 创建行动手册时，您可以配置行动手册算法来编辑事故属性或警报属性。
- 您可以将事故表中显示的所有事故的信息导出为 JSON 文件。当必须将此信息提供给第三方时，可能需要进行此操作。
- 基于 AI 的资产评分。基于机器学习的引擎可帮助您评估资产上运行的流程，并判断特定流程属于正常，还是异常，需要 SOC 分析师介入处理。
- 改进了 Kaspersky Next XDR Expert 中所发生事件的电子邮件通知模板的配置过程。

- 您可以根据需要缩短或延长警报和事故的保留期。默认情况下，警报和事故的保留期为 360 天。
- 卸载 Kaspersky Next XDR Expert。所有创建的数据也将被删除。
- 现在，您可以从警报详情窗口或事故详情窗口中的快捷菜单中，在新浏览器标签页上打开“**威胁搜索**”页面。
- 您现在可以在警报详情窗口或事故详情窗口中，搜索受影响的资产和可观察对象。
- 能够通过 REST API 配置警报聚合规则。
- 当您从警报详情窗口或事故详情窗口打开“**威胁搜索**”页面时，现在可以基于警报或事故的第一个事件和最后一个事件之间的时间段执行搜索，而不是过去 24 小时。
- 部署初步检查。您现在可以在部署 Kaspersky Next XDR Expert 之前，检查是否满足系统要求。卡巴斯基部署工具包 (KDT) 会检查您的硬件、操作系统、软件和网络环境。如果至少有一项要求未满足，KDT 将中断部署并向您提供详细报告。
- Kaspersky Next XDR Expert 现在可以安装在 Nutanix AHV 虚拟化平台上。
- OSMP 控制台优化：控制台窗口、登录页面和仪表板的加载速度现已提升。
- 您现在可以从事故详情窗口切换到“**威胁搜索**”页面上的事故相关事件。
- Kaspersky Next XDR Expert 现支持以下 EPP 应用程序：
  - Kaspersky Endpoint Security for Windows（版本 12.5、12.6、12.7）
  - Kaspersky Endpoint Security 12.1 for Linux
  - Kaspersky Endpoint Security 12.1 for Mac
  - Kaspersky Industrial CyberSecurity for Nodes 4.0
  - Kaspersky Endpoint Agent 4.0
- Kaspersky Next XDR Expert 现在可兼容 Kaspersky Anti Targeted Attack Platform 7.0。
- 您现在可以通过单击刷新图标来刷新警报详情窗口和事故详情窗口中的信息。

Kaspersky Next XDR Expert 1.1

Kaspersky Next XDR Expert 具有多个新功能和改进：

- 应用程序中使用了更新版本的 Bootstrap。在安装新版本的 Kaspersky Next XDR Expert 之前，请运行以下命令来更新 Bootstrap：

  ```
  ./kdt apply -k <XDR 更新存档路径> -i <配置文件路径> --force-bootstrap
  ```

- 全新设计的用户界面。
- 降低了硬件和软件要求。
- 提高了应用程序的稳定性。

- 新的部署向导简化了安装参数的配置。
- 添加了预定义的行动手册。
- Kaspersky Next XDR Expert 现支持以下 EPP 应用程序：
  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Industrial CyberSecurity for Nodes 3.2
  - Kaspersky Endpoint Agent 3.16
- 新的仪表板小部件用于监控通过行动手册执行的响应。
- 从 Kaspersky Security Center 迁移到 Kaspersky Next XDR Expert，包括用户和租户的迁移，以及租户与 Kaspersky Security Center 管理服务器的绑定。
- Kaspersky Next XDR Expert 现可兼容 Kaspersky Anti Targeted Attack Platform 6.0。
- Kaspersky Unified Monitoring and Analysis Platform 在 2024 年 8 月发布的更新中引入的新功能和改进。

已修复的问题

下表列出了在Kaspersky Next XDR Expert的先前版本中发现并在当前版本中修复的所有问题。

Kaspersky Next XDR Expert 2.3中已修复问题列表

受感染的首个版本	问题 ID	问题描述
2.2	10682804	选择某些部分（例如 **来源状态**）作为主页后，重新登录 OSMP 控制台时会显示空白页面。
2.1	10699357	登录 OSMP 控制台时，可能会显示消息 Kaspersky Next XDR Expert 配置错误。
2.1	10684421	从事故卡片下钻到相关警报和其他事故的警报详情后，卡片停止加载。
2.1	10664845	将设备添加到 Kaspersky Endpoint Security for Windows 策略的受信任区域时，显示的可用设备列表可能会包含已添加到受信任区域的设备。
2.2	10644898	如果在**远程网络地址**选项卡上指定了 IP 地址范围，则在策略属性（**应用程序设置** → **防火墙**）中添加的网络数据包规则不会保存。
2.1	10563335	Kaspersky Endpoint Security for Windows 策略的安装在 MDR 配置步骤后停止。
2.1	10563321	修复了在 Kaspersky Endpoint Security for Windows 策略属性（**应用程序设置** → **常规设置** → **遥测设置**）中编辑排除规则时出现的问题：如果排除规则包含格式为"EventType = *value*"的条件，将"="运算符替换为"等于"会导致出现"带有此名称的规则已存在"错误。
1.4	9934440	安装 OSMP 时，不会在安装主机上检查是否可以通过 `resolv.conf` 文件中指定的 DNS 服务器正确解析平台组件（OSMP 控制台、管理服务器、DBMS）的 FQDN。

Kaspersky Next XDR Expert 2.2.1 中修复的问题列表

受感染的首个版本	问题 ID	问题描述
2.2	10563365	新增 HTTP 流式传输连接器。
2.1	10624497 10634081	已正确创建 Kaspersky Next XDR Expert 数据的备份副本。

Kaspersky Next XDR Expert 2.2中已修复问题列表

受感染的首个版本	问题 ID	问题描述
2.1	10355947	URL 未显示在警报或事故详细信息的 **可观察对象** 部分中。
2.1	10137933	`/api/v1/alerts` 端点返回的错误响应为文本格式，而不是 JSON 格式。
2.0	10135653	如果密钥位于中间证书文件的开头，则应用配置文件失败，并显示 `intermediate_bundle: parameter is not PEM encoded` 错误。
2.1	10014033	在 **响应历史** 部分中，应用"**行动手册名称** != <playbook name>"筛选器时，手动响应条目被错误地包含在搜索结果中。

2.1	10091214	再次单击当前活动的主菜单部分会导致显示空白页面。
2.1	9726211	比较两个行动手册版本时，先选择最新版本，然后再选择早期版本后，比较视图出现颠倒：较新的版本显示在左侧，更改以红色突出显示，而较旧的版本显示在右侧，更改以绿色突出显示。

Kaspersky Next XDR Expert 2.1.3中已修复问题列表

受感染的首个版本	问题 ID	问题描述
2.1	10119212	将Kaspersky Next XDR Expert 2.0.1 HF4升级到 2.1 HF2 时，如果使用了超过五个工作节点，则无法迁移到NATS。
2.1	10129716	无法从警报详情导航到关联的CEF事件，并且CEF事件导出不可用。
2.1	10132483	无法配置警报和事故列表的自动刷新间隔。
2.1	10132891	导出特定租户的事件时，导出的文件包含所有租户的事件，而不是仅包含所选租户的事件。
2.1	10133000	内部连接器的Auditd参数运行不正确。
2.1	10133396	在SQL查询中使用EDR和CEF字段时，字段别名处理不正确，导致countIf函数和嵌套查询失败。
2.1	10133457	存在大量活动服务时，**资源和服务**部分加载缓慢。
2.1	10135956	存在大量警报或事故时，无法按警报或事故ID搜索表。
2.1	10145872	无法通过OSMP控制台界面或API删除SMTP设置中包含的密钥。此外，即使在不需要密钥的情况下，也必须在SMTP设置中指定密钥。
2.1	10146680	当本地用户导航到**监控** → **CyberTrace**部分时，即使CyberTrace集成配置正确，也会发生`bad token response`错误。
2.1	10152245	KUMA资源文件夹加载缓慢。
2.1	10159009	租户属性中未显示警报和事故设置部分。
2.1	10084426	轮询 Active Directory 域后，重新启动 Kaspersky Security Center 组件时，所有信息都被重新发布到 NATS，而不是仅发送新的或修改后的数据。
2.1	10091301	轮询 Active Directory 域后，Kaspersky Security Center 组件向 NATS 发送了 `tenant_id` 参数的错误值。

Kaspersky Next XDR Expert 2.1.2中已修复问题列表

受感染的首个版本	问题 ID	问题描述
2.1	9987559	9987559：在**资产(设备)**部分的**分析和响应**选项卡中，**打开远程终端**按钮未显示。
2.1	9987778	由于 k0s 文件传输期间出现 `MSCP` 错误，在虚拟接口上执行 Bootstrap 安装失败，并显示 `ssh_verify_known_hosts failed` 错误。
2.1	9986780	由于事件时间戳的时区不正确，事件时间表不完整。
2.1	9818418	当根租户设置的**证书**部分中没有证书时，证书导入按钮不可用。
2.1	9952850	当包含旧版本（旧于2.0版本）EDR事件时，调查图表显示为空（500错误）。
2.1	9970495	如果文件之前曾通过**移动到隔离区**响应进行过隔离，则文件在恢复后仍处于隔离状态。
2.1	9973357	在创建或更改密码时，密码验证只允许来自3个必填类别的字符，而不是4个字符。
2.1	9989267	从**威胁搜索**事件手动创建的警报错误地触发了**创建事故：同一主机资产**和**关联到现有事故：同一主机资产**分段规则。
2.1	9989284	在将警报与事件解除关联后，无法更改警报中的分析人员。
2.1	9996452	如果在沙盒规则中指定了最小和最大文件大小，**获取文件**和**文件扫描**响应无法启动。

2.1	9992321	警报中资产卡片的**关联至类别**按钮不可用。
2.1	10037395	事故卡片中的**在威胁搜索中搜索**按钮返回的事件列表为空。
2.1	10042351	**获取进程内存转储**响应未能完成，并一直卡在**已推出**状态。
2.1	10026313	根租户授权许可的活动设备数错误地显示为0。
2.1	10055774	在时间线模式下，调查图表中未显示垂直时间戳。
2.1	9986186	在 Kaspersky Security Center 安装阶段，XDR 从 2.0.1 升级到 2.1 失败（`invocation image launch is completed with an error`）。
2.1	9997088	在 irp-licensing-policy 迁移阶段，XDR 从 2.0.1 升级到 2.1 失败，并出现 `create storage: check migrations: missing migration` 错误。

Kaspersky Next XDR Expert2.1.1中已修复问题列表

受感染的首个版本	问题 ID	问题描述
2.1	9940726	未收到触发的关联规则的统计信息。
2.1	9961307	添加Kaspersky Endpoint Detection and Response授权许可密钥时，无法通过远程终端连接到资产。
2.1	9995015	无法重新接受更新后的KSN声明。
2.1	9935812	**运行 YARA 扫描**响应操作的**目录的完整路径**字段不接受带掩码的路径。
2.1	9942685	无法从IOC规则生成的警报打开IOC报告。
2.1	9942527, 9942530	从OSMP关联器事件中的`ThreatVerdictname`字段导航到Kaspersky Threats时，打开了错误的URL。
2.1	9941545, 9941548	从事件、警报或事故中的`DeviceAdress`字段导航到Kaspersky 威胁情报门户时，打开了错误的URL。
2.1	9942427	从遥测事件中的哈希值字段导航到VirusTotal服务时，打开了错误的URL。
2.1	9951714	由于默认时间筛选器不正确，并非所有与事故相关的事件都显示在**威胁搜寻**部分。
2.1	9959926	AMSI 扫描事件中的"`AmsiContentData`"字段显示不正确，并且不支持上下文菜单操作。
2.1	9960056	在具有EDR模块的授权许可下，在**更新设置**部分更改更新源未保存。
2.1	9964882	从报告编辑视图返回报告模板列表不起作用，导致页面空白。
2.1	9967180	单击**监控政策**选项选项卡（**来源**列）上的**显示**按钮导致页面空白。
2.1	9959327	资源2.0值出现在**资源和服务**列表的**资源和服务**筛选下拉列表中。

Kaspersky Next XDR Expert2.1中已修复问题列表

受感染的首个版本	问题 ID	问题描述
2.0	9662328	在刷新警报或事件详细信息后，可观察对象的增强结果已被清除。
2.0	9714816	由相同的IOA规则生成的警报没有在整个24小时内汇总。
2.0	9652409 9636329	在将辅助管理服务器添加到群组后，设备未出现在管理群组层次结构中的**受管理设备**下。
2.0	9696104	在导出和导入IOA排除项时引号没有转义，这导致SQL解析器错误，并阻止一些排除项在KES政策中正常运行。
2.0	9544457	**威胁搜寻**部分使用的默认预设不适用于EDR事件。
2.0	9757637	无法导入卡巴斯基安全管理中心资产。

2.0	9702974	在将控制台语言切换到中文后，**Detection and Response**选项卡（**资产管理→资产(设备)→Detection and Response**）上的内容仍为英语。
2.0	9708837 9474866	在单节点部署期间，内部DBMS帐户密码中的特殊字符阻止OSMP扫描器安装程序和沙盒配置。
2.0	9577657	无法使用配置文件自定义代理服务器和更新程序。
2.0	9499714	**事故**部分无法打开，并显示由于内存使用过多，获取事故类型列表失败错误。
2.0	9660585	将OSMP控制台语言切换到简体中文后，Kaspersky Managed Detection and Response插件本地化无法正确应用。
1.4	8773796	调查图表上的**撤销**和**重做**按钮在某些情况下无法正常工作。
1.3	8452910	将Kaspersky Next XDR Expert从1.2版本升级到1.3版本时，如果自动执行特定组件的某些配置步骤而不是手动执行，则可能导致资源溢出和Kaspersky Next XDR Expert无法正常运行。
1.2	7323982	在支持版本管理的对象属性窗口中，**修订历史**部分的**Web Console IP 地址**字段显示不正确的IP地址。

关于 Kaspersky Next XDR Expert

Kaspersky Next XDR Expert (XDR) 是一款强大的网络安全解决方案，可保护您的企业 IT 基础设施免受复杂的网络威胁，包括那些无法被安装在企业资产上的 EPP 应用程序检测到的威胁。该解决方案提供了全面的可见性、相关性和自动化，利用了多种响应工具和数据源，包括端点资产、网络和云数据。为了有效保护您的 IT 基础设施，Kaspersky Next XDR Expert 会分析来自这些来源的数据，以识别威胁、创建潜在事故警报并提供响应工具。Kaspersky XDR 依赖于先进的分析能力和丰富的安全专业技术积累。

该解决方案通过集成组件和单一界面中的整体场景提供统一的检测和响应流程，从而提高安全专业人员的效率。Kaspersky Next XDR Expert 组件部署在一个名为 Open Single Management Platform 的单一平台上。

检测工具包括：

- 威胁搜索工具，通过分析事件主动搜索威胁和漏洞。
- 高级威胁检测和跨源关联：实时关联来自不同来源的事件，提供适用于不同场景的开箱即用的关联规则，并支持 MITRE ATT&CK 矩阵映射，能够创建新规则和自定义现有规则，以及支持用于检测零日漏洞的回顾性扫描。
- 调查图，用于可视化和促进事故调查并确定警报的根本原因。
- 通过使用 Kaspersky 威胁情报门户，可以获取最新的详细威胁情报，例如有关网址、域名、IP 地址、文件哈希、统计和行为数据以及 WHOIS 和 DNS 数据的详细威胁情报。

响应工具包括：

- 手动响应操作：资产隔离、运行命令、添加和删除阻止规则、在资产上启动任务、Kaspersky Threat Intelligence Portal声誉增强以及对用户分配培训。
- 预定义和用户创建的行动手册，用于自动执行典型的响应操作。
- 第三方应用程序响应操作和跨应用程序响应场景。

Kaspersky Next XDR Expert包含端点威胁检测和响应功能（来自Kaspersky Endpoint Detection and Response）：

- 全面了解整个企业基础设施中的端点；
- 基于入侵指标（IOC）、YARA规则和独特的攻击指标（IOA）检测威胁；
- 保护邮件服务器以及传入和传出电子邮件免受有害对象、垃圾邮件和钓鱼的侵害。
- 沙盒用于安全地分析可疑文件和程序，并在隔离环境中提供有关对象行为的信息。

Kaspersky Next XDR Expert 还使用 Open Single Management Platform 组件进行资产管理以及集中运行安全管理和维护任务：

- 在公司网络中的资产上部署卡巴斯基应用程序。
- 远程启动扫描和更新任务。
- 获取有关资产保护的详细信息。
- 使用卡巴斯基应用程序配置所有安全组件。

Kaspersky Next XDR Expert 支持租户层次结构。

Kaspersky Next XDR Expert 与 Active Directory 集成（包含 API），并支持与卡巴斯基应用程序和第三方解决方案的广泛集成以进行数据获取和响应。有关 Kaspersky Next XDR Expert 支持的应用程序和解决方案的信息，请参阅“兼容的 Kaspersky Next 应用程序”和“与其他解决方案集成”部分。

Kaspersky Next XDR Expert 组件

	Open Single Management Platform		Kaspersky Industrial CyberSecurity for Networks
	Kaspersky Anti Targeted Attack Platform		Kaspersky Industrial CyberSecurity for Nodes
	Kaspersky Security for Linux Mail Server		Kaspersky CyberTrace
	Kaspersky Endpoint Security for Business		Kaspersky Automated Security Awareness Platform
	卡巴斯基混合云安全		

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

硬件和软件要求

本文介绍了单节点部署方案和多节点部署方案的硬件要求、Kaspersky Next XDR Expert 的软件要求，以及 Kaspersky Deployment Toolkit 和 Open Single Management Platform 组件的硬件和软件要求。

由于Kaspersky Next XDR Expert及其组件需要快速数据传输，我们强烈建议您使用直连式存储。推荐使用以下存储接口：SAS v3.5及更高版本、SATA Express。

单节点部署：硬件要求

单节点部署需要较少的资源（参见下表），但应考虑以下事项：

- 单节点方案仅支持网络中最多存在 10,000 台设备。
- 数据库位于集群外的主工作节点上。

  在单节点部署的情况下，强烈推荐您首先在将充当主节点的主机上手动安装 DBMS。之后，您可以在同一主机上部署 Kaspersky Next XDR Expert。

- 为了正确部署解决方案，请确保目标主机的 CPU 支持 BMI、AVX 和 SSE 4.2 指令集。

最小硬件条件

单节点部署方案的硬件要求

解决方案	250 台设备	1,000 台设备	3,000 台设备	5,000 台设备	10,000 台设备
包含以下应用程序的解决方案： • Open Single Management Platform • Kaspersky Unified Monitoring and Analysis Platform • 沙盒	1 个 XDR 主工作节点： • CPU：10核；工作频率：2.5GHz • RAM：44 GB • 可用固态硬盘空间： • 第一个磁盘子系统：400 GB • 第二个磁盘子系统：500GB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。	1 个 XDR 主工作节点： • CPU：16核；工作频率：2.5GHz • RAM：48 GB • 可用固态硬盘空间： • 第一个磁盘子系统：400 GB • 第二个磁盘子系统：600GB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。	1 个 XDR 主工作节点： • CPU：22核；工作频率：2.5GHz • RAM：54 GB • 可用固态硬盘空间： • 第一个磁盘子系统：600 GB • 第二个磁盘子系统：1TB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。	1 个 XDR 主工作节点： • CPU：32核；工作频率：2.5GHz • RAM：62 GB • 可用固态硬盘空间： • 第一个磁盘子系统：800 GB • 第二个磁盘子系统：1.4 TB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。	1 个 XDR 主工作节点： • CPU：36核；工作频率：2.5GHz • RAM：74 GB • 可用固态硬盘空间： • 第一个磁盘子系统：1.5TB • 第二个磁盘子系统：2.4TB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。

多节点部署：硬件要求

多节点部署需要更多资源（参见下表）。对于此方案，应考虑以下事项：

- 对于超过 10,000 个设备的网络，推荐采用多节点集群部署方案。
- 数据库位于集群外的独立主机上。
- 为了正确部署解决方案，请确保目标主机的 CPU 支持 BMI、AVX 和 SSE 4.2 指令集。

最小硬件条件

多节点部署方案的硬件需求

解决方案	20,000 台设备	30,000 台设备	50,000 台设备
包含以下应用程序的解决方案： • Open Single Management Platform • Kaspersky Unified Monitoring and Analysis Platform • 沙盒	12 个节点： • 1 个 XDR 主节点 • 3 个 XDR 工作节点 • 1 个 XDR 数据库节点 • 1 个 KUMA 收集器 • 1 个 KUMA 关联器 • 3 个 KUMA 协调器 • 2 个 KUMA 存储	12 个节点： • 1 个 XDR 主节点 • 3 个 XDR 工作节点 • 1 个 XDR 数据库节点 • 1 个 KUMA 收集器 • 1 个 KUMA 关联器 • 3 个 KUMA 协调器 • 2 个 KUMA 存储	12 个节点： • 1 个 XDR 主节点 • 3 个 XDR 工作节点 • 1 个 XDR 数据库节点 • 1 个 KUMA 收集器 • 1 个 KUMA 关联器 • 3 个 KUMA 协调器 • 2 个 KUMA存储
	1 个 XDR 主节点： • CPU：4 核 • RAM：8 GB • 可用 SSD 磁盘空间：500 GB 3 个 XDR 工作节点： • CPU: +10核。 • RAM：20 GB • 可用 SSD 磁盘空间：1 TB 1 个 XDR 数据库节点： • CPU: +10核。 • RAM：22 GB • 可用 SSD 磁盘空间：1,6 TB 1 个 KUMA 收集器节点： • CPU: +8核。 • RAM：16 GB • 可用 SSD 磁盘空间：500 GB 1 个 KUMA 关联器节点： • CPU: +8核。 • RAM：32 GB • 可用 SSD 磁盘空间：500 GB 3 个 KUMA 协调器节点： • CPU: +6核。 • RAM：12 GB • 可用 SSD 磁盘空间：200 GB 2 个 KUMA 存储节点： • CPU：24 核 • RAM：64 GB • 可用 SSD 磁盘空间：4.7 TB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。 网络带宽：每个节点 10 Gbps	1 个 XDR 主节点： • CPU：4 核 • RAM：8 GB • 可用 SSD 磁盘空间：500 GB 3 个 XDR 工作节点： • CPU: +12核。 • RAM：24 GB • 可用 SSD 磁盘空间：1 TB 1 个 XDR 数据库节点： • CPU: +12核。 • RAM：24 GB • 可用 SSD 磁盘空间：2,7 TB 1 个 KUMA 收集器节点： • CPU: +8核。 • RAM：16 GB • 可用 SSD 磁盘空间：500 GB 1 个 KUMA 关联器节点： • CPU: +8核。 • RAM：32 GB • 可用 SSD 磁盘空间：500 GB 3 个 KUMA 协调器节点： • CPU: +6核。 • RAM：12 GB • 可用 SSD 磁盘空间：200 GB 2 个 KUMA 存储节点： • CPU：24 核 • RAM：64 GB • 可用 SSD 磁盘空间：7 TB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。 网络带宽：每个节点 10 Gbps	个 XDR 主节点： • CPU：4 核 • RAM：8 GB • 可用 SSD 磁盘空间：500 GB 3 个 XDR 工作节点： • CPU: +14核。 • RAM：30 GB • 可用 SSD 磁盘空间：1 TB 1 个 XDR 数据库节点： • CPU: +16核。 • RAM：32 GB • 可用 SSD 磁盘空间：4,3 TB 1 个 KUMA 收集器节点： • CPU: +8核。 • RAM：16 GB • 可用 SSD 磁盘空间：500 GB 1 个 KUMA 关联器节点： • CPU: +8核。 • RAM：32 GB • 可用 SSD 磁盘空间：500 GB 3 个 KUMA 协调器节点： • CPU: +6核。 • RAM：12 GB • 可用 SSD 磁盘空间：200 GB 2 个 KUMA 存储节点： • CPU：24 核 • RAM：64 GB • 可用 SSD 磁盘空间：12 TB 1个沙盒节点： • CPU: +32核。 • RAM：80 GB • 磁盘子系统：2个硬盘，每个600GB，10,000RPM。 网络带宽：每个节点 10 Gbps

Kaspersky Next XDR Expert：软件要求

软件要求以及支持的系统和平台

操作系统	支持以下操作系统的 64 位版本： Ubuntu Server 24.04 LTS Ubuntu Server 26.04 LTS Astra Linux® 特别版 RUSB.10015-01（操作更新 1.8.5）
包	Python® 3.8 或更高版本

<table>
<tr><td>虚拟化平台</td><td>Kaspersky Next XDR Expert 支持此处列出的所有虚拟化平台。但是，Kaspersky Next XDR Expert 组件存在一些限制。下表列出了差异。
<table>
<tr><th>虚拟化平台名称</th><th>Kaspersky Next XDR Expert</th><th>KUMA</th><th>沙盒</th></tr>
<tr><td>VMware ESXi 7.0.3</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Microsoft Hyper-V® Server 2022</td><td>✓</td><td>✓</td><td>—</td></tr>
<tr><td>基于内核的虚拟机 (KVM)</td><td>✓</td><td>✓</td><td>—</td></tr>
<tr><td>Brest 3.3 虚拟化软件</td><td>✓</td><td>—</td><td>✓</td></tr>
<tr><td>RED Virtualization 7.3</td><td>✓</td><td>—</td><td>✓</td></tr>
<tr><td>Proxmox Virtual Environment 9.1、9.2</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Nutanix 7.5</td><td>✓</td><td>✓</td><td>—</td></tr>
<tr><td>zVirt Node 4.5</td><td>✓</td><td>—</td><td>✓</td></tr>
</table></td></tr>
<tr><td>数据库管理系统 (DBMS)</td><td>PostgreSQL 17.9 64 位
PostgreSQL 18.4 64 位
Postgres Pro 18 Enterprise 64 位（集群内置高可用性）
所有列出的 PostgreSQL 版本均支持 Corosync/Pacemaker</td></tr>
<tr><td>集群节点（控制器和工作节点）上的文件系统</td><td>ext4
XFS</td></tr>
</table>

Kaspersky Next XDR Expert 组件

要查看 Kaspersky Next XDR Expert 组件的硬件和软件要求，请单击其名称：

- OSMP Console
- Kaspersky Unified Monitoring and Analysis Platform（以下简称 KUMA）
- Kaspersky Security Center 从属管理服务器
- Kaspersky Security Center 网络代理
- Kaspersky Endpoint Security for Windows
- Kaspersky Anti Targeted Attack Platform（以下简称 KATA）
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky CyberTrace
- 卡巴斯基威胁情报门户
- Kaspersky Automated Security Awareness Platform（以下简称 KASAP）

Kaspersky Deployment Toolkit安装要求

所有 Kaspersky Next XDR Expert 组件均使用 Kaspersky Deployment Toolkit 实用程序（以下简称 KDT）进行安装。

KDT的硬件和软件要求如下：

规格	系统要求
硬件	CPU：4 核，工作频率 2.5 GHz RAM：8 GB 可用磁盘空间：至少100GB，包括： • Docker 数据存储目录（默认：`/var/lib/docker`）：至少 60 GB • KDT 的临时文件目录（默认：`/tmp`）：至少 15 GB
系统	支持以下操作系统的 64 位版本： • Astra Linux 特别版 RUSB.10015-01（操作更新 1.8.5） • Ubuntu Server 24.04 LTS • Ubuntu Server 26.04 LTS

安装 KUMA 服务的主机的要求

KUMA 服务（收集器、关联器和存储）既可以安装在 Kubernetes 集群之外的专用主机上，也可以作为 Kaspersky Next XDR Expert 部署的一部分，以工作负载形式安装在 Kubernetes® 集群内。

当KUMA服务部署在Kubernetes集群之外时，本文中定义的硬件、软件和安装要求直接适用于安装这些服务的主机。

当KUMA服务部署在Kubernetes集群内部时，它们会在Kubernetes工作线程节点上运行，并根据本文中定义的KUMA硬件、软件和安装要求消耗集群资源。在这种情况下，Kubernetes工作线程节点必须提供足够的容量来满足这些要求。

常规应用程序安装要求

您可以在以下操作系统上安装应用程序：

- Oracle Linux
- Astra Linux
- Ubuntu

  支持的操作系统版本列于“硬件和软件要求”部分。

  支持的配置包括服务器和带 GUI 支持的服务器。在带 GUI 支持的服务器配置中，无需安装其他报告安装包。

部署应用程序之前，请确保满足以下条件：

- 要安装组件的服务器满足硬件和软件要求；
- 已安装的 KUMA 实例所使用的端口可用；

- KUMA 组件使用主机的完全限定域名(FQDN) 进行寻址，格式为 hostname.example.com。安装应用程序之前，请确保运行以下命令时，将返回正确的主机 FQDN：

  ```
  hostname -f
  ```

- 运行安装程序的服务器名称不得为 `localhost` 或 `localhost.<domain>`；
- 您要安装 KUMA Core 的服务器名称不以数字开头。
- 所有带有 KUMA 服务的服务器上都配置了基于网络时间协议 (NTP) 的时间同步功能。

安装 Sigma 规则转换器的要求

该转换器支持以下操作系统：

- Ubuntu 2024
- Windows 10
- Windows 11
- RED OS 7
- RED OS 8
- Oracle Linux 8.3
- Oracle Linux 9.3

硬件和软件推荐配置要求

本部分列出了每秒处理事件数 (EPS) 高达 40,000 的数据流所需的硬件与软件要求。KUMA 负载值取决于所解析的事件类型和规范化器的效率。

对于事件处理效率，CPU 核心数比时钟频率更重要。例如，具有中等时钟频率的 8 个 CPU 核心处理事件的效率高于具有高时钟频率的 4 个 CPU 核心。下表列出了 KUMA 组件的硬件和软件要求。

收集器占用的 RAM 量取决于配置的数据增强方法（DNS、账户、资产、使用来自 Kaspersky CyberTrace 的数据进行增强）以及是否使用聚合。RAM 的消耗受数据聚合窗口设置、用于数据聚合的字段数量以及聚合字段的数据量的影响。

例如，假设事件流为 1000 EPS，且禁用了事件增强功能（禁用事件增强功能和事件聚合功能，每个租户含 5000 个账户和 5000 个资产），则一个收集器需要配置以下资源：

- 1 个 CPU 核心或 1 个虚拟 CPU
- 512 MB RAM
- 1 GB 磁盘空间（不包括事件缓存的占用量）

例如，要支持 5 个不执行事件增强功能的收集器，您必须分配以下资源：5 个 CPU 核心、2.5 GB RAM 和 5 GB 可用磁盘空间。

安装 KUMA 服务的硬件和软件推荐配置要求

	收集器	关联器	存储库
CPU数	支持 SSE 4.2 的 Intel 或 AMD™ 处理器： 至少 4 核/8 线程或 8 个虚拟 CPU。	支持 SSE 4.2 的 Intel 或 AMD： 至少 4 核/8 线程或 8 个虚拟 CPU。	支持 SSE 4.2 的 Intel 或 AMD： 至少 12 核/24 线程或 24 个虚拟 CPU。
RAM	16 GB	16 GB	48 GB
剩余磁盘空间	/opt 目录大小：至少 500 GB。	/opt 目录大小：至少 500 GB。	/opt 目录大小：至少 500 GB。
操作系统	• Ubuntu Server 24.04 LTS • Oracle Linux 8.6、8.7、9.2、9.4。 • Astra Linux特别版RUSB.10015-01（操作更新1.8.2）		
网络带宽	100 Mbps	100 Mbps	如果数据流超过 20,000 EPS，ClickHouse 节点之间的传输速率必须至少为 10 Gbps。

以下虚拟环境支持安装 KUMA：

- VMware 6.5 或更高版本
- 适用于 Windows® Server 2012 R2 或更高版本的 Hyper-V
- QEMU-KVM 4.2 或更高版本

卡巴斯基对存储服务器的建议

对于存储服务器，卡巴斯基专家建议如下：

- 将 ClickHouse 部署到固态硬盘 (SSD) 上。SSD 有助于提高数据访问速度。硬盘可用于通过 HDFS 技术存储数据。
- 要将数据存储系统连接到存储服务器，请使用高速协议，例如光纤通道或 iSCSI 10G。不建议使用 NFS 和 SMB 等应用程序级协议连接数据存储系统。
- 在 ClickHouse 集群服务器上使用 ext4 文件系统。
- 若使用 RAID 阵列，追求高性能可采用 RAID 0，需兼顾高性能与容错性则采用 RAID 10。
- 为确保数据存储子系统的容错能力和性能，请确保 ClickHouse 节点严格部署在不同的磁盘阵列上。
- 如果您使用虚拟化基础架构来托管系统组件，请在不同的虚拟机管理程序上部署 ClickHouse 集群节点。在这种情况下，需要防止两个运行 ClickHouse 的虚拟机在同一个虚拟机管理程序上运行。
- 对于高负载的 KUMA 安装场景，请在物理服务器上安装 ClickHouse。

代理设备要求

要将数据发送到 KUMA 收集器，必须在网络基础设施的设备上安装代理。下表列出了硬件和软件要求。

安装代理的推荐硬件和软件配置要求

	Windows 设备	Linux 设备
CPU	单核，1.4 GHz 或更高	单核，1.4 GHz 或更高
RAM	512 MB	512 MB
剩余磁盘空间	1 GB	1 GB
操作系统	• Microsoft Windows® 2012 • Microsoft Windows Server® 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows 10 20H2、21H1	• Astra Linux 特别版 RUSB.10015-01（2023-0426SE17 更新 1.7.4） • Ubuntu 22.04 LTS (Jammy Jellyfish) • Debian 11.7 (Bullseye)

Oracle Linux、Astra Linux、Ubuntu 22.04 LTS 操作系统的安装要求

	Oracle Linux	Astra Linux	Ubuntu 22.04 LTS
Python 版本	从 3.6 到 3.11。不支持 3.12 及更高版本。	从 3.6 到 3.11。不支持 3.12 及更高版本。	从 3.6 到 3.11。不支持 3.12 及更高版本。
SELinux 模块	已禁用	已禁用	已禁用

	Oracle Linux	Astra Linux	Ubuntu 22.04 LTS
包管理器	pip3	pip3	pip3

基本包	• netaddr
	• firewalld
	• compat-openssl11
	您需要在 KUMA Core 将部署在集群外部的 Oracle Linux 9 主机上安装此安装包。
	关于从 Oracle Linux 8.x 升级到 Oracle Linux 9.x 的更多信息。
	要安装这些安装包，请运行以下命令：
	`pip3 install netaddr`
	`yum install firewalld`
	`yum install compat-openssl11`
		• python3-apt
		• curl
		• libcurl4
		要安装这些安装包，请运行以下命令：
		`apt install python3-apt curl libcurl4`
			• python3-apt
			• curl
			• libcurl4
			• openssl 1.1.1
			• acl
			要安装这些安装包，请运行以下命令：
			`apt install python3-apt curl libcurl4 acl`
			您可以从 Ubuntu 官方网站下载 openssl1.1.1 软件包，并使用以下命令进行安装：
			`dpkg -i libssl1.1_1.1.1f-1ubuntu2_amd64.deb`

依赖包	没有值。	• netaddr • python3-cffi-backend 要安装这些安装包，请运行以下命令： `apt install python3-netaddr python3-cffi-backend` 如果您计划从 KUMA 查询 Oracle DB 数据库，则需要安装 Astra Linux libaio1 包。	• netaddr • python3-cffi-backend 要安装这些安装包，请运行以下命令： `apt install python3-netaddr python3-cffi-backend`
为了正确生成和下载报告，必须在带有 KUMA Core 的设备上安装的软件包	• nss • gtk2 • atk • libnss3.so • libatk-1.0.so.0 • libxkbcommon • libdrm • at-spi2-atk • mesa-libgbm • alsa-lib • cups-libs • libXcomposite • libXdamage • libXrandr 要安装这些安装包，请运行以下命令： `yum install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr`	• libgtk2.0.0 • libnss3 • libatk-adapter • libdrm-common • libgbm1 • libxkbcommon0 • libasound2 要安装这些安装包，请运行以下命令： `apt install libgtk2.0.0 libnss3 libatk-adaptor libdrm-common libgbm1 libxkbcommon0 libasound2`	• libatk1.0-0 • libgtk2.0-0 • libatk-bridge2.0-0 • libcups2 • libxcomposite-dev • libxdamage1 • libxrandr2 • libgbm-dev • libxkbcommon-x11-0 • libpangocairo-1.0-0 • libasound2 要安装这些安装包，请运行以下命令： `apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2 libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2`
安装应用程序所需的用户权限	没有值。	您需要为将要安装应用程序的用户分配所需的权限： `sudo pdpl-user -i 63 <将要安装应用程序的用户>`	没有值。

OSMP Console 要求

OSMP Console Server

有关硬件和软件要求，请参阅工作节点要求。

客户端设备

要使用 OSMP Console，客户端设备仅需安装浏览器。

最小屏幕分辨率为 1366x768 像素。

设备的硬件和软件要求与 OSMP Console 所使用的浏览器的要求一致。

浏览器：

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

网络代理要求

最小硬件条件：

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

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

网络代理。支持的平台

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

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

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

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

	M OS (Moscow Electronic School) 12 Server 64 位 Mostech 64 位 Mostech Server 64 位 Fedora® Linux Server 41 64 位 Fedora Linux Workstation 41 64 位
操作系统。macOS	有关受支持的操作系统列表，请参阅 Kaspersky Endpoint Security for Mac 帮助。 ™
虚拟化平台	有关受支持的虚拟化平台的信息，请参阅Kaspersky Security for Virtualization Light Agent在线帮助。

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

- 更新重译（分发点使用）
- KSN代理（分发点使用）
- 漏洞扫描任务

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

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

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

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

建议您安装与 Open Single Management Platform 相同版本的 Linux 网络代理。

Open Single Management Platform 完全支持相同或更高版本的网络代理。

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

虚拟化配置

在 Hypervisor 主机上，必须禁用 BIOS/UEFI 中的所有节能优化（C 状态、P 状态、睿频加速和类似功能）。

如果 Hypervisor 主机上的 BIOS/UEFI 支持 CPU 性能设置，则必须将其配置为最高性能。参考硬件供应商文档以获取指导。

在 Hypervisor 主机上，必须在 BIOS/UEFI 中启用虚拟化支持（Intel VTx/VTd、AMD-V/ AMD-Vi 等）。

必须启用透明大页面（THP）。

I/O 调度程序必须设置为“`noop`”。

建议您增加“`max_io_threads`”参数。

NUMA（非统一内存访问）

在具有单插槽或低内存的主机上，应禁用 NUMA。

在多插槽系统上，应启用 NUMA（建议在 XDR 推荐规格的基础上至少增加 20% 的额外内存，以应对 NUMA 开销）。

VMware 配置

启用“`Reserve all guest memory`”选项。

设置共享资源参数（例如 CPU 和内存份额）的最小值，以确保每个虚拟机都能获得专用资源。

使用 VMXNET3 网络适配器优化虚拟机的网络性能。

基于 Kernel、Proxmox、Nutanix、RED Virtualization、zVirt Node 的虚拟机配置

将 Hypervisor 配置为主机模式或主机直通模式。

存储子系统应使用 SCSI 驱动程序，而不是块 (blk) 驱动程序。

不要使用共享资源，以确保专用资源分配。

HYPER-V 配置

vCPU 与 pCore 的比例应配置为 1:1。

请遵循以下文章中的建议：

- https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-for-deploying-devices-using-discrete-device-assignment
- https://www.vinchin.com/vm-tips/hyper-v-performance-tuning.html

常见要求和注意事项

如果使用虚拟化，则需要 100% vCPU 分配。

对于超过 40,000 个设备的网络，请使用从属管理服务器。

确保 DNS 服务器在网络上可用。

单节点部署无法升级到多节点部署。如果预计基础设施扩展，则建议采用多节点安装程序。

有效设备和 EPS 计算

硬件要求可能因端点设备上运行的操作系统而异。使用以下公式估算您网络中的有效设备：

```
< 设备数量 > = < Windows 端点 > + 3* < Linux 和 macOS 端点 > + 20 * < 服务器 >
```

在默认设置下，有效设备预计贡献 0.5 EPS（每秒事件数）。总 EPS 使用以下公式计算：

```
< 总 EPS > = < 有效设备 EPS > + < 第三方 EPS >
```

您可以使用以下公式将总 EPS 转换为有效设备：

```
< 有效设备总数 > = < 总 EPS > *2
```

节点配置

如果 BIOS/UEFI 支持 IOMMU（输入/输出内存管理单元），则必须启用它。

必须禁用 BIOS/UEFI 中的所有节能优化，例如 C 状态、P 状态和睿频加速。

如果 BIOS/UEFI 支持 CPU 性能设置，则必须将其配置为最高性能。有关更多信息，请参阅硬件供应商的文档。

磁盘/存储要求

最低输入/输出性能：

- 对于单节点部署： 12,000 IOPS（顺序读写，8 KB 块大小）。
- 对于多节点部署： 8,000 IOPS（顺序读写，8 KB 块大小）。

RAID 阵列的条带大小必须至少为 16 KB。

SSD/NVMe 驱动器必须支持 TRIM 功能。

不推荐丢弃挂载选项。相反，必须配置定期清理未使用块以保持性能。

fsync 延迟不应超过最佳值：

- 单节点部署和控制平面节点为 2 毫秒。
- EPS 高于 1000 的计算节点为 3 毫秒。
- EPS 低于 1000 的计算节点为 10 毫秒。

NUMA（非统一内存访问）

在具有单插槽或低内存的主机上，应禁用 NUMA。

在多插槽系统上，应启用 NUMA。建议您在 XDR 推荐的内存规格基础上至少增加 20% 的内存，以应对 NUMA 开销。

Kaspersky Next XDR Expert 组件

下表列出了Kaspersky Next XDR Expert包含的组件。

Kaspersky Next XDR Expert 组件

组件名称	描述
agentserver	该组件允许通过代理程序集成对资产执行响应操作。
asset-manager	该组件用于集中式资产管理。
backup-operator	该自动化工具通过自定义资源和标签管理数据备份和恢复。
bootstrap	基本执行环境，包括Kubernetes集群和用于运行Kaspersky Next XDR Expert的基础设施组件。
cp	该通讯平台支持系统组件之间的数据交换和交互。
openbao-csi-provider	该组件允许通过容器存储接口（CSI）访问外部存储的集群。
database-cluster	该组数据库服务器协同工作，以实现高可用性和可扩展性。
database-operator	CloudNativePG Kubernetes控制器，用于管理内部数据库连接配置、数据库资源、密钥和凭证轮换。
gateway	Kubernetes集群网关。
hierman	该组件管理层级操作。
iam	该OSMP平台组件提供身份验证和授权。
irp	该组件可自动处理警报和事件并执行响应操作。
istio	该服务网格用于管理Kubernetes集群中的服务通讯。
keswin_web_plugin_xdr	该 Web 插件用于在 Kaspersky Next XDR Expert 中管理 Kaspersky Endpoint Security for Windows，支持安全策略配置、事故监控和平台组件集成。
ksb-facade	该组件通过使用mixin和部署模板来执行操作。
ksc	Kaspersky Security Center 管理服务器
ksn-proxy-facade	该组件通过Porter、外部KSN服务集成和统计处理管理KSN代理部署。
kuma-migrator	该组件可自动迁移KUMA版本之间的配置、数据和设置。
loadbalancer	该组件将请求路由到集群中的容器或进程，并提供跨节点的审计、身份验证和会话同步。

组件名称	描述
nsqlookupd	该服务发现NSQ生产者并引导集群内的客户端。
nwc	OSMP Console。
objectstorage	该组件用于存储临时行动手册数据、警报和事件文件，并支持S3 API进行外部集成。
observability	该组件提供对事件、威胁和资产的集中可见性，并通过与KUMA平台集成来支持响应自动化。
orchestra	自动化平台。该通用组件协调工作流程和执行行动手册，以支持自动响应事件并简化安全操作。
osmp-ksn-proxy	该组件通过 KSN 代理 API 和路由数据将检测和警报统计数据传输到 KSN 或 KPSN。
osmp-scanner	该组件使用反恶意软件、YARA和沙盒扫描文件、发送文件进行分析并生成报告。
plugin-admin-agent	该组件管理网络代理策略。
plugin-admin-server	该组件管理管理服务器。
plugin-agent-server	该组件管理Kaspersky Endpoint Detection and Response的各项功能。
plugin-asset-management	该组件管理资产，包括设备、用户和其他资源。
plugin-enterprise	该组件与其他卡巴斯基解决方案集成，并通过网页界面和API提供资产管理、监控、响应自动化和多租户支持。
plugin-kata	该组件与KATA/EDR集成，用于响应操作、事件数据扩展以及高可用性和可扩展性支持。
plugin-kuma	该组件将KUMA功能集成到Kaspersky Next XDR Expert中。
plugin-osmp-scanner	该组件提供扫描交互，与反恶意软件、YARA和沙盒集成，将结果发送到ObjectStorage、Proxy和Disaster Recovery，并支持自动和手动响应操作。
plugin-public-api-token-settings	该组件通过公共API管理API令牌设置，以支持Kaspersky Next XDR Expert组件和外部系统的身份验证和授权。
plugin-tenant-roles	该组件管理租户内用户和群组角色分配，并与IAM集成，以实现角色模型和多租户支持。
spp_web_plugin_xdr	该组件与卡巴斯基单一产品插件集成，可通过OSMP控制台管理其他卡巴斯基产品。
secrets-manager	该组件管理密钥，确保其在服务部署和配置期间的安全存储和正确使用。
tenant-registry	该组件管理租户生命周期、身份数据，并与Kaspersky Security Center服务器和外部系统集成。
plugin-kessw	该组件用于在Kaspersky Next XDR Expert中管理Kaspersky Embedded Systems Security for Windows（KESS）。
plugin-kes-linux	该组件管理Kaspersky Endpoint Security for Linux
plugin-kesw	该组件管理Kaspersky Endpoint Security for Windows
plugin-spp	卡巴斯基单一产品插件，用于通过OSMP控制台管理其他卡巴斯基产品。

兼容的应用程序和解决方案

本文列出了应用程序已测试并保证正常运行的软件版本。应用程序也可能兼容其他软件版本，但这些配置尚未经过完整的测试流程，因此未包含在保证支持的版本列表中。

Kaspersky Next XDR Expert 可与以下版本的应用程序和解决方案集成：

- Kaspersky Security Center Linux 16.3（作为从属管理服务器）
- Kaspersky Security Center Windows 15.1 或更高版本（作为从属管理服务器）

- Kaspersky Anti Targeted Attack Platform 7.1

  周三强烈建议迁移到 Open Single Management Platform (OSMP) 架构。在该架构中，Kaspersky Endpoint Security 应用程序无需中环节点服务器参与即可直接连接到 OSMP。
  如果您尚未在所有受管理设备上将安全应用程序升级到新版本，则在升级完成之前，威胁响应仍通过与 Kaspersky Anti Targeted Attack Platform (KATA) 的集成进行管理。这意味着事故响应平台会向 KATA 发送请求，然后 KATA 会向安全应用程序发送请求。
  只有在因某种原因无法迁移到 OSMP 架构的异常情况下，才允许使用此方案。

- Kaspersky Endpoint Security for Windows 14.0、14.1（支持文件服务器）
- Kaspersky Endpoint Security for Linux 12.4、12.5
- Kaspersky Endpoint Security for Mac 12.2.1、12.2.1 补丁 A
- Kaspersky CyberTrace 5.0（只能在 KUMA 控制台中配置集成）
- Kaspersky Industrial CyberSecurity for Nodes 5.0
- Kaspersky Industrial CyberSecurity for Networks 4.0（只能在 KUMA 控制台中配置集成）
- Kaspersky Secure Mail Gateway 2.0 或更高版本（只能在 KUMA 控制台中配置集成）
- Kaspersky Security for Linux Mail Server 10 或更高版本（只能在 KUMA 控制台中配置集成）
- Kaspersky Web Traffic Security 6.0 或更高版本（只能在 KUMA 控制台中配置集成）
- Kaspersky Automated Security Awareness Platform
- 卡巴斯基威胁情报门户
- Kaspersky NGFW 1.2
- Kaspersky Managed Detection and Response
- Kaspersky SIEM 4.2、4.6
- Kaspersky Security for Virtualization Light Agent 6.3.1、6.4

  Kaspersky Security for Virtualization Light Agent 支持 Kaspersky Next XDR Expert，但存在一些限制。Web 插件、安全虚拟机 (SVM) 和 Integration Server 只能通过充当从属管理服务器的 Kaspersky Security Center 进行管理。

有关受支持应用程序版本的最新信息，请参阅应用程序支持生命周期网页。

已知问题和限制

Kaspersky Next XDR Expert 支持管理 Kaspersky Endpoint Security for Windows，但存在以下限制：

- 不支持自适应异常控制组件。Kaspersky Next XDR Expert 不支持自适应异常控制规则。
- Kaspersky Sandbox 组件不受支持。

基本概念

本节介绍与 Kaspersky Next XDR Expert 相关的基本概念。

管理服务器

Kaspersky Next XDR Expert 组件支持远程管理安装在客户端设备上的 Kaspersky 应用程序。

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

管理服务器作为服务安装在设备上，且拥有以下属性集：

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

有关安装设置的完整列表，请参阅以下文章：安装 Open Single Management Platform。

管理服务器执行以下功能：

- 存储管理组结构
- 存储有关客户端设备配置的信息
- 应用程序分发包的存储结构
- 将应用程序远程安装至客户端设备和远程卸载应用程序
- 更新卡巴斯基应用程序的应用程序数据库和软件模块
- 管理客户端设备上的策略和任务
- 存储有关客户端设备上已发生事件的信息
- 生成有关卡巴斯基应用程序操作的报告

- 向客户端设备部署授权许可密钥并存储授权许可密钥信息
- 转发有关任务进度的通知（例如在客户端设备上检测到病毒）

在应用程序界面中命名管理服务器

在 OSMP 控制台的界面中，管理服务器可以采用以下名称：

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

您可以使用 OSMP 控制台连接到管理服务器。

管理服务器层级

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

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

*虚拟管理服务器*是从属管理服务器的一个特例。

您可以使用管理服务器的层次结构执行以下操作：

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

管理组层次结构中包括的每台设备都只能连接到一台管理服务器。您必须独立监控设备到管理服务器的连接。使用这些功能可以根据网络属性在不同服务器的管理组中搜索设备。

Web 服务器

Kaspersky Next XDR Expert *Web 服务器*（以下简称 *Web 服务器*） 是 Kaspersky Next XDR Expert 的一个组件，与管理服务器一起安装。Web 服务器用于通过网络传输独立安装包。

当您创建独立安装包时，它会自动发布在 Web 服务器上。已创建的独立安装包列表中会显示用于下载独立包的链接。必要时，您可以取消发布独立包或在 Web 服务器上重新发布。您可以通过电子邮件等便捷的方式，将链接发送给用户。通过使用此链接，用户可将安装包下载至本地设备。

网络代理

管理服务器与设备之间的交互由 Kaspersky Next XDR Expert 的*网络代理*组件执行。必须在所有使用 Kaspersky Next XDR Expert 管理 Kaspersky 应用程序的设备上安装网络代理。

安装了网络代理的设备被称为*受管理设备*或*设备*。

Linux 网络代理作为服务安装在设备上，且具有以下属性集：

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

Windows 网络代理作为服务安装在设备上，且具有以下属性集：

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

macOS的网络代理程序作为服务安装在设备上，且具有以下属性集：

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

服务进程的名称：

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

- 对于 Windows：
  - klnagent
- 对于 macOS：
  - com.kaspersky.klnagent

默认情况下，网络代理安装程序在以下位置：

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

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

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

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

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

管理组

一个*管理组*（以下也称为*组*）是根据特定特征组合而成的受管理设备逻辑集合，旨在 Kaspersky Next XDR Expert 中将组内设备作为一个整体进行管理。

管理组内的所有受管理设备都被配置以做如下事情：

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

受管理设备只能属于一个管理组。

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

受管理设备

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

您可以让受管理设备作为分发点和连接网关来运行。

设备仅可以被一个管理服务器管理。一台管理服务器能够管理的设备数量取决于托管管理服务器的设备的配置和 DBMS 限制。

未分配的设备

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

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

管理员工作站

安装了 OSMP 控制台服务器的设备称作*管理员工作站*。管理员可以使用这些设备来远程集中管理客户端设备上安装的卡巴斯基应用程序。

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

您可以将管理员的工作站作为客户端设备包括在管理组中。

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

管理 Web 插件

作为特殊组件的*管理 Web 插件*通过 OSMP 控制台对 Kaspersky 软件进行远程管理。在下文中，管理 Web 插件也称为*管理插件*。管理插件是 OSMP 控制台与特定卡巴斯基应用程序之间的接口。使用管理插件，您可以配置应用程序任务和策略。

管理插件提供以下：

- 创建和编辑应用程序任务和设置的界面
- 用于创建和编辑策略和策略配置文件以便远程集中配置卡巴斯基应用程序和设备的界面

- 应用程序事件传输
- OSMP 控制台可以显示应用程序的运行数据和事件，以及从客户端设备转发的统计信息

政策

*政策*是应用于一个管理群组和其子群组的卡巴斯基应用程序设置集。您可以在管理组的设备上安装多个卡巴斯基应用程序。Kaspersky Next XDR Expert 为管理组中的每个卡巴斯基应用程序提供一个策略。策略具有以下状态之一：

策略的状态

状态	描述
活动	应用于设备的当前策略。对于每个管理组中的卡巴斯基应用程序，只能有一个策略处于活动状态。设备对卡巴斯基应用程序应用活动策略的设置值。
非活动	当前未应用于设备的策略。
漫游	如果选择该选项，策略将在设备离开企业网络时变为活动状态。

策略根据以下规则发挥作用：

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

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

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

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

策略配置文件根据以下规则发挥作用：

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

策略配置文件

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

为了帮助您避免创建同一策略的多个实例，Kaspersky Next XDR Expert 允许您创建*策略配置文件*。策略配置文件用于在单一管理组中的设备在不同策略设置下运行时。

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

任务

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

特定应用程序的任务仅在安装了该应用程序的管理插件时可以被创建。

任务可以在管理服务器和设备上执行。

以下任务在管理服务器上执行：

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

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以被管理员通过管理控制台工具修改，或者被远程设备用户修改（例如，通过安全应用程序界面）。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

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

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

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务结果保存在 Syslog 事件日志和 Kaspersky Next XDR Expert 事件日志中，既集中保存在管理服务器上，也本地保存在每台设备上。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

关联器

*关联器*是一个用于分析规范化事件的程序组件。在关联过程中，可将事件与活动列表和/或字典中的信息进行关联。

经分析获取的数据可用于执行以下任务：

- 活动列表内容管理。
- 将关联事件发送到配置的目标位置

事件会实时进行关联。

关联器的工作原理基于对事件的签名分析。这意味着每个事件都会按照用户设置的关联规则进行处理。当程序检测到满足关联规则条件的事件序列时，会创建一个关联事件并将其发送到存储。关联事件也可以发送到关联器进行重新分析，从而允许您自定义关联规则，使其基于先前分析的结果触发。一个关联规则的结果可以被其他关联规则使用。

您可以在各个关联器之间分配关联规则及其使用的活动列表，从而平衡服务负载。在这种配置下，收集器会将规范化事件发送到所有可用的关联器。

关联器循环执行以下步骤：

1. **获取事件**

   关联器从收集器或其他服务接收规范化的事件。

2. **应用关联规则**

   您可以将关联规则配置为由单个事件或事件序列触发。如果关联规则未检测到警报，事件处理到此结束。

3. **响应警报**

   您可以指定程序在检测到警报时必须执行的操作。该程序中提供以下操作：

   - 事件增强
   - 与活动列表相关的操作
   - 发送通知
   - 保存关联事件

4. **发送关联事件**

   当程序检测到满足关联规则条件的事件序列时，会创建一个关联事件并将其发送到存储。至此，关联器完成事件处理。

事件

*事件*是记录在组织 IT 基础设施受监控元素上的信息安全事件。例如，事件包括登录尝试、与数据库的交互以及传感器信息广播。每个单独的事件可能看似毫无意义，但综合来看，它们会构成一个更全面的网络活动图景，从而帮助识别安全威胁。这是 KUMA 的核心功能。

KUMA 从日志中接收事件，并通过将来自异构源的数据转换为统一格式来重构这些事件（此过程称为规范化）。然后对事件进行筛选和聚合，并将其发送到关联器服务进行分析，以及发送到存储服务进行保留。当 KUMA 识别出特定事件或事件序列时，它会创建*关联事件*，这些事件也会被分析和保留。如果某个事件或一系列事件表明存在潜在的安全威胁，KUMA 会创建警报。此警报包含有关威胁的警告以及安全官应调查的所有相关数据。

在整个生命周期中，事件会经历转换，并可能获得不同的名称。以下是典型事件生命周期的描述：

初始步骤在收集器中执行。

1. 原始事件。KUMA 使用连接器从事件源接收的原始消息称为“*原始事件*”。这是一条未处理的消息，KUMA 还不能使用该消息。为了使其可用，必须对其进行规范化，以符合 KUMA 数据模型。这发生在下一阶段。

2. 规范化事件。规范化器根据 KUMA 数据模型转换“原始”事件数据。经过转换后，原始消息成为*规范化事件*，可供 KUMA 进行分析。此后，KUMA 仅处理规范化事件。原始事件不再使用，但它们可以作为规范化事件的一部分保留在 `Raw` 字段内。

   该程序采用以下规范化器：

   - JSON
   - CEF
   - Regexp
   - Syslog （遵循 RFC3164 和 RFC5424 标准）
   - CSV/TSV
   - Key-value
   - XML
   - Netflow v5、v9、IPFIX（v10）、sFlow v5
   - SQL

   此时，已规范化的事件已经可以用于分析。

3. 事件目标位置。收集器服务处理完事件后，它就可以被其他 KUMA 服务使用，并发送到 KUMA 关联器和/或存储。

事件生命周期的后续步骤在关联器中完成。

事件分为以下类型：

1. 基础事件。已规范化的事件。

2. 聚合事件。处理大量类似事件时，您可以将它们“合并”为单个事件，以节省处理时间和资源。这些事件充当基础事件并以相同方式处理；但除了父事件（已“合并”的事件）的所有参数之外，聚合事件还包含一个计数器，用于指示其代表的父事件数量。聚合事件还会存储收到第一个和最后一个父事件的时间。

3. 关联事件。当检测到满足关联规则条件的一系列事件时，程序会创建*关联事件*。这些事件可以进行筛选、增强和聚合处理。它们还可以发送到存储空间或循环送入关联器管道。

4. 审计事件。在 Kaspersky Security Center 中执行某些安全相关操作时，会创建审计事件（审计事件、审计事件）。这些事件用于确保系统完整性。这些事件会自动放入单独的存储空间，并至少保存 365 天。

5. 监控事件。这些事件用于跟踪 KUMA 接收的数据量的变化。

警报

在 KUMA 中，当收到触发关联规则的一系列事件时会创建警报。KUMA 分析师会创建关联规则，以检查传入事件是否存在潜在安全威胁。因此，当关联规则被触发时，系统会显示有关潜在恶意活动的警告。负责数据保护的安全官必须调查这些警报，并在必要时做出响应。

KUMA 会自动为每个警报分配严重级别。该参数显示触发关联规则的进程的重要程度或数量。应优先处理严重级别较高的警报。收到新的关联事件时，严重级别的值会自动更新，但安全官也可以手动设置。在这种情况下，警报严重级别不再自动更新。

相关事件会链接到警报，从而可以使用这些事件的数据丰富警报。KUMA 还提供了用于警报调查的下钻功能。

您可以根据警报创建事故。

本部分介绍了 KUMA 中的警报管理。

事故

如果 KUMA 收到的数据的性质或生成的关联事件和警报表明可能存在攻击或漏洞，则可以将此类事故的特征组合成一个*事故*。这使安全专家可以全面分析威胁的表现形式并有助于做出高效的响应。

您可以为事故分配类别、类型和严重级别，并将事故分配给数据保护官进行处理。

事故可以导出到 NCIRCC 和 MDR。

资源

*资源*是 KUMA 组件，包含用于实现各种功能的参数：例如，与给定的网址建立连接或根据某些规则转换数据。这些模块化组件组合成服务资源集，而服务资源集又用于创建 KUMA 服务。

任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

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

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

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

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

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

- 指定设备分类。

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

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

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

本地应用程序设置与策略的关系

您可以使用策略为组中的所有设备设置完全相同的应用程序设置值。

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

应用程序在客户端设备上使用的设置的值由策略中该设置的锁定位置（🔒）确定：

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

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

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

在首先根据策略设置应用策略之后，才会更改本地应用程序设置。

分发点

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

安装在作为分发点的设备上的网络代理的功能和用例因操作系统而异。

分发点可执行以下功能：

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

  分发点加速更新发布并释放管理服务器资源。

- 使用 UDP 通过多点传送分发策略和组任务。

- 用作管理组中的设备与管理服务器的连接网关。

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

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

- 轮询网络以检测新设备并更新现有设备的信息。分发点应用与管理服务器相同的设备发现方法。

- 执行卡巴斯基和其他软件供应商的应用程序的远程安装，包括在没有网络代理的客户端设备上安装。

  此功能允许将网络代理的安装包远程传输到位于管理服务器无直接访问权限的网络上的客户端设备。

- 作为代理服务器加入卡巴斯基安全网络 (KSN)。

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

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

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

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

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

如果管理员手动分配分发点，则可以将它们分配给管理组或网络位置。

带有活动连接配置文件的网络代理不参与广播域检测。

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

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

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

一个分发点需要至少 4 GB 的可用磁盘空间。如果分发点的可用磁盘空间小于 2 GB，Kaspersky Next XDR Expert 将创建一个重要级别为*警告*的安全问题。安全问题将被发布在设备属性的“**安全问题**”部分中。

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

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

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

连接网关

*连接网关*是以特殊模式运行的网络代理。连接网关接受来自其他网络代理的连接，并通过其自身与服务器的连接将它们与管理服务器建立隧道连接。与普通的网络代理不同，连接网关等待来自管理服务器的连接，而不是建立与管理服务器的连接。

一个连接网关最多可以接收 10,000 台设备的连接。

使用连接网关有两种选择：

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

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

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

  所有连接网关都包含在管理服务器属性的分发点列表中。

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

Core

Core 是 KUMA 的核心组件，它是所有其他服务和组件的基础。Core 的控制台提供了一个图形用户界面，供操作员/分析师日常使用以及配置整个系统。

Core 允许您：

- 创建和配置程序的服务或组件，以及将必要的软件集成到系统中；
- 集中管理程序服务和用户账户；
- 可视化程序的统计数据；
- 根据接收到的事件调查安全威胁。

存储

KUMA *存储*用于存储规范化事件，并确保 KUMA 能够快速可靠地访问这些事件以提取分析数据。ClickHouse 技术可实现快速访问和高可用性。这意味着*存储*是一个绑定到 KUMA 存储服务的 ClickHouse 集群。ClickHouse 集群可补充冷存储磁盘。

选择 ClickHouse 集群配置时，需考虑组织对事件存储的特定需求。有关更多信息，请参阅“ClickHouse 文档”。

在存储库中，您可以创建*空间*。空间可用于组织集群中的数据，例如，将特定类型的事件存储在一起。

收集器

*收集器*是一个应用程序组件，该组件从事件源接收和处理消息，并将它们传输到存储、关联器和/或第三方服务以识别警报。

对于每个收集器，您需要配置一个连接器和一个规范化器。您还可以配置无限数量的附加规范化器、过滤器、增强规则和聚合规则。要使收集器将规范化事件发送到其他服务，您必须添加目标。通常使用两个目标：存储和关联器。

收集器循环执行以下步骤：

1. **从事件源接收消息**

   要接收消息，必须配置主动或被动连接器。被动连接器仅侦听来自事件源的消息，而主动连接器会主动轮询事件源，例如数据库管理系统。

   连接器可以有不同的类型。连接器类型的选择取决于消息传递所使用的传输协议。例如，如果您的事件源通过 TCP 发送消息，则必须安装 TCP 类型的连接器。

   有下述连接器类型可用：

   - 内部
   - TCP
   - UDP

- netflow
- sflow
- nats-jetstream
- kafka
- http
- sql
- file
- diode
- ftp
- nfs
- wmi
- wec
- SNMP
- elastic
- etw

2 事件解析和规范化

连接器接收的事件将使用用户设置的规范化器和规范化规则进行处理。规范化器的选择取决于事件源所发送消息的格式。例如，如果事件源以 CEF 格式发送消息，则必须选择 CEF 类型的规范化器。

以下规范化器可用：

- JSON
- CEF
- Regexp
- Syslog （遵循 RFC3164 和 RFC5424 标准）
- CSV
- Key-value
- XML
- NetFlow v5
- NetFlow v9
- IPFIX (v10)
- SQL

3 规范化事件的过滤

您可以配置过滤器，以选择符合指定条件的事件进行进一步处理。

4 规范化事件的增强和转换

增强规则允许您向事件中添加来自内部和外部数据源的补充信息。

可用的增强数据源如下：

- constants
- cybertrace
- 字典
- dns
- events
- ldap
- templates
- timezone data
- geographic data

转换规则允许您根据特定条件转换事件字段的值。

以下转换方式可用：

- lower：将所有字符转换为小写。
- upper：将所有字符转换为大写。
- regexp：使用 RE2 正则表达式提取子字符串。
- substring：通过指定首字符和尾字符来提取子字符串。
- replace：将部分文本替换为字符串。
- trim：删除指定的字符。
- append：在字段值末尾添加字符。
- prepend：在字段值开头添加字符。

5 聚合规范化事件

您可以配置聚合规则以减少传输到存储和/或关联器的类似事件的数量。聚合规则可将多个事件合并为一个事件。这有助于减轻负责后续事件处理的服务的负载，并节省存储空间和许可证的每秒事件数 (EPS) 配额。例如，如果有许多事件涉及两个 IP 地址之间使用相同传输层和应用层协议的网络连接，则可将在特定时间段内发生的此类事件汇总为一个大型事件。

6 传输规范化事件

完成所有处理阶段后，事件将被发送到所配置的目标位置。

服务

*服务*是KUMA 的主要组件，用于接收、处理、分析和存储事件。每个服务由协同工作的两部分组成：

- 其中的一个部分是在 KUMA 控制台中基于服务资源集创建的。
- 服务的另一部分作为 KUMA 组件之一，安装在部署 KUMA 的网络基础设施中。服务的服务器部分可包含多个实例：例如，同一代理或存储的服务可以同时安装在多台设备上。

服务的两个部分通过服务 ID相互关联。

KUMA 代理

KUMA *代理*是将服务器和工作站中的原始事件转发到 KUMA 目标的服务。

提供以下类型的代理：

- wmi 代理用于使用 Windows Management Instrumentation 从远程 Windows 设备接收数据。它们安装到 Windows 资产中。
- WEC 代理用于使用 Windows Event Collector 从本地设备接收 Windows 日志。它们安装到 Windows 资产中。
- TCP 代理用于通过 TCP 协议接收数据。它们安装到 Linux 和 Windows 资产中。
- UDP 代理用于通过 UDP 协议接收数据。它们安装到 Linux 和 Windows 资产中。
- NATS 代理用于 NATS 通讯。它们安装到 Linux 和 Windows 资产中。
- Kafka 代理用于 Kafka 通讯。它们安装到 Linux 和 Windows 资产中。
- HTTP 代理用于通过 HTTP 协议进行通讯。它们安装到 Linux 和 Windows 资产中。
- 文件代理用于从文件获取数据。它们安装到 Linux 资产中。
- FTP 代理用于通过文件传输协议接收数据。它们安装到 Linux 和 Windows 资产中。
- NFS 代理用于通过网络文件系统协议接收数据。它们安装到 Linux 和 Windows 资产中。
- SNMP 代理用于通过简单网络管理协议接收数据。它们安装到 Linux 和 Windows 资产中。
- 二极管代理与数据二极管配合使用，从隔离网段接收事件。它们安装到 Linux 和 Windows 资产中。
- ETW 代理用于接收 Windows 事件跟踪数据。它们安装到 Windows 资产中。

关于严重级别

*严重级别*反映了 KUMA 关联器检测到的安全敏感活动的相对重要性。它显示了多个警报的处理顺序，并指示是否应该让高级安全官参与。

关联器会根据关联规则设置，自动为关联事件和警报分配严重级别值。警报的严重级别还取决于与已处理事件相关的资产，因为关联规则会考虑相关资产类别的严重级别。如果警报或关联事件没有任何具有严重级别值的关联资产，或者根本没有任何关联资产，则该警报或关联事件会继承生成它的关联规则的严重级别。警报或关联事件的严重级别始终等于或高于生成它的关联规则的严重级别。

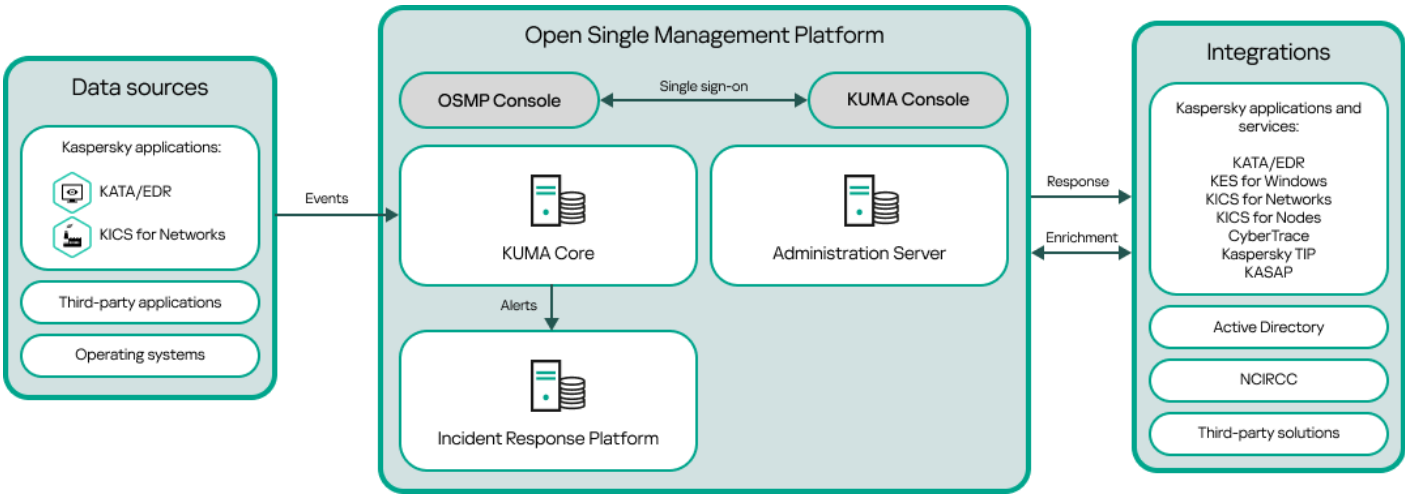
可以手动更改警报的严重级别。手动修改的严重级别不再由关联规则自动更新。

可能的严重级别值：

- 低
- 中
- 高
- 严重

Open Single Management Platform 架构

本部分提供了对 Open Single Management Platform 组件及其交互的描述。



Open Single Management Platform 架构

Open Single Management Platform 包含以下主要组件：

- **Open Single Management Platform** (OSMP)。Kaspersky Next XDR Expert 所基于的技术基础。OSMP 集成了所有解决方案组件，并提供组件之间的交互。OSMP 是可扩展的，支持与卡巴斯基应用程序和第三方解决方案的集成。
- **OSMP Console**。为 OSMP 提供 Web 界面。
- KUMA Core。KUMA 的核心组件。KUMA 接收、处理和存储信息安全事件，然后使用关联规则分析这些事件。分析结果显示，如果满足关联规则的条件，KUMA 将创建警报并将其发送至事故响应平台。
- **事故响应平台**。这是一个 Open Single Management Platform 组件，支持自动或手动创建事故、管理警报和事故生命周期、将警报和事故分配给 SOC 分析师，以及自动或手动响应事故（包括通过行动手册进行响应）。
- Administration Server（简称*服务器*）。客户端组织端点保护的关键组件。管理服务器通过 EPP 应用程序提供端点保护的集中部署和管理，并允许您监控端点保护状态。
- **数据源**。生成事件的信息安全硬件和软件。将 Kaspersky Next XDR Expert 与所需数据源集成后，KUMA 会接收事件并进行存储和分析。
- **集成**。卡巴斯基应用程序和第三方解决方案与 OSMP 集成。通过集成解决方案，SOC 分析师可以丰富事故调查所需的数据，然后对事故做出响应。

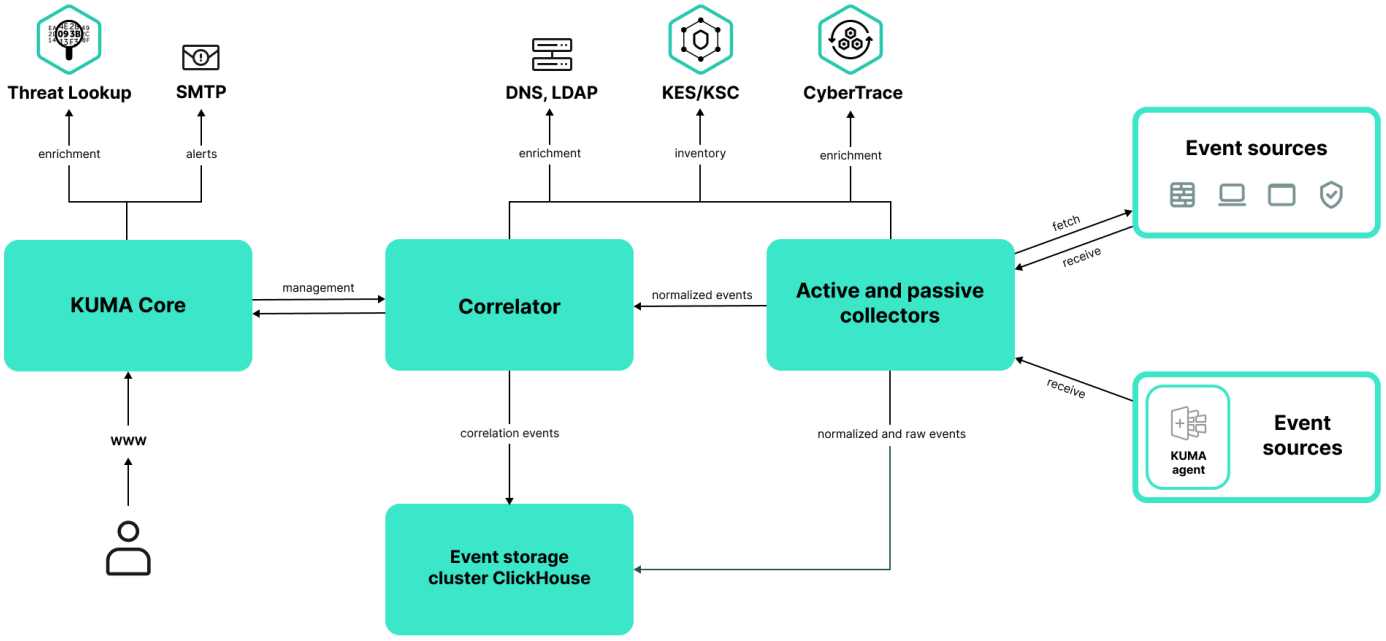
SIEM 组件架构

标准程序安装包含以下组件：

- *核心*，其中包含用于监控和管理系统组件设置的图形界面。
- 一个或多个*收集器*，用于接收来自事件源的消息，并对其进行解析、规范化以及（如需要）过滤和/或聚合。

- *关联器*，用于分析从收集器接收的规范化事件，使用活动列表执行必要操作，并根据关联规则创建警报。
- *存储*，用于保存规范化事件和已注册的警报。

事件通过可选加密的可靠传输协议在组件之间传输。您可以配置负载均衡以在服务实例之间分配负载，还可以启用自动切换功能，以便在主组件不可用时切换到备份组件。如果所有组件都不可用，事件将保存到硬盘缓冲区，以便稍后发送。文件系统中用于临时存储事件的缓冲区大小可以更改。



KUMA 架构

OSMP Console 界面

Kaspersky Next XDR Expert通过OSMP控制台界面进行管理。

OSMP Console 窗口包含以下项：

- 主菜单位于窗口左侧
- 窗口上部区域中的上方窗格
- 工作区在窗口右侧

主菜单

主菜单包含以下部分：

- **管理服务器**。显示您当前连接到的管理服务器的名称。您可以通过单击管理服务器名称来打开管理服务器属性。
- **控制台导航**。显示主菜单地图。大部分显示的部分可以被添加到书签或设置为主页。默认**控制台导航**被设为主页。您可以更改这些设置。
- **监控**。提供有关您的基础设施、保护状态和统计信息的概览，包括威胁搜索、警报和事故以及行动手册。此外，您还可以在此部分添加和配置 KUMA 资源和服务。
- **资产管理**。包含用于资产和硬件管理以及卡巴斯基应用程序策略的工具。
- **任务**。包含用于创建和运行任务的工具。
- **用户和角色**。可让您管理用户和角色，通过为用户分配角色来配置用户权限，以及将策略配置文件与角色关联。
- **存储库**。可让您访问应用程序存储库。
- **软件管理**。可让您管理卡巴斯基和第三方应用程序，以及安装包和补丁。
- **操作**。包含多种操作，包括应用程序授权许可、查看和管理加密驱动器和加密事件。
- **发现和部署**。可让您轮询网络以发现客户端设备，以及手动或自动将设备分发到管理组。此部分还包含保护部署向导。
- **市场**。包含有关全系列卡巴斯基业务解决方案的信息，可让您选择所需的解决方案，然后继续在卡巴斯基网站上购买这些解决方案。
- **设置**。包含将Kaspersky Next XDR Expert与其他卡巴斯基应用程序集成的设置，并允许您创建API令牌。还包含与根据所使用的功能显示界面元素以及界面语言相关的设置。此外，您还可以从此部分打开 KUMA 设置窗口，其中包含 KUMA 配置参数，包括 KUMA 配置设置、KUMA 集成设置、授权许可密钥管理和访问选项。

如有需要，可单击屏幕底部的 V 形符号 (‹‹)，将主菜单最小化为图标形式。

上方窗格

上方窗格始终显示在所有控制台区域中，且无法隐藏。

窗格左侧包含应用程序名称和徽标。如果单击应用程序名称或徽标，会打开 OSMP Console 主页。

窗格右侧显示以下设置：

- 通知图标 (🔔)。如果单击该图标，将打开一个包含通知的窗格。
- 您账户的菜单。包含指向 Kaspersky Next XDR Expert 帮助的链接。您还可以退出 Kaspersky Next XDR Expert，查看您的工作状态、OSMP Console 版本和已安装的管理 Web 插件列表。

工作区域

工作区显示您选择在 OSMP Console 界面窗口的各个部分中查看的信息。它还包含可用于配置信息显示方式的控制元素。

更改 OSMP Console 界面语言

您可以选择 OSMP Console 的界面语言。

要更改界面语言：

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

更改 OSMP 控制台主页

登录 OSMP 控制台后，主页将显示。

默认**控制台导航部分**被设为主页。如果需要的话，您可以更改主页。

更改主页：

1. 在**控制台导航**部分，将鼠标光标悬停在您想要设置为主页的项目上。
2. 主页 (⌂) 图标显示后，单击图标。

   主页已更改。屏幕上会显示相应消息。被选为主页的项目标有主页 (⌂) 图标。

无法将**市场**和**设置**部分设为主页。

添加和移除书签

您可以将 OSMP 控制台中常用的部分添加到主菜单的“**书签**”部分，以便快速访问。

如果您没有向书签添加如何元素，**书签**部分将不显示在主菜单中。

您只能向书签添加显示页面的部分。例如，如果您转到**资产管理 → 资产(设备)**，一个包含设备表的页面会打开，意味着您可以将该部分添加到书签。如果在主菜单中选择该部分后显示一个窗口或者没有显示任何元素，则您无法将该部分添加到书签。

要将一个部分添加到书签：

1. 在主菜单中，将鼠标光标悬停在要固定的部分上。
2. 书签 (🔖) 显示后，单击图标。

   该部分显示在**书签**部分。

要从书签移除一个部分：

1. 在主菜单中，转到“**书签**”部分。
2. 将鼠标光标悬停在要移除的部分上，然后单击书签 (🔖) 图标。

   该部分被从书签中移除。

您也可以在“**控制台导航**”部分中通过将鼠标光标悬停在上面并单击书签 (🔖) 图标添加或将其从书签中移除。所选项将用书签 (🔖) 图标进行标记并显示在主菜单的“**书签**” 部分。如果您想将该项从书签中移除，请单击书签 (🔖) 图标。

书签 部分仅显示在主菜单中。它从不显示在**控制台导航**页面上。

授权许可

本节介绍 Kaspersky Next XDR Expert 授权许可的主要方面。

关于最终用户授权许可协议

最终用户授权许可协议（简称"授权许可协议"）是您与 AO Kaspersky Lab 之间具有约束力的协议，其中规定了您使用该应用程序应遵守的条款。

在您开始使用应用程序之前请认真阅读授权许可协议。

您可以使用以下方法浏览最终用户授权许可协议的条款：

- 在安装 Open Single Management Platform 期间。
- 通过阅读 license.txt 文档。该文档包含在应用程序分发包中。

当您安装应用程序时同意了最终用户授权许可协议，这表明您接受了最终用户授权许可协议的条款。如果您不接受授权许可协议的条款，请取消应用程序安装且不得使用该应用程序。

关于授权许可密钥

*授权许可密钥*由一系列数位组成，您可以依据最终用户授权许可协议的条款使用它们激活并使用应用程序。授权许可密钥由 Kaspersky 专家生成。

您可以使用下面的方法添加一个授权许可密钥到应用程序：通过应用*密钥文件*或输入*激活码*。为应用程序添加授权许可后，将在应用程序界面中显示该授权许可密钥的唯一字母数字序列。

如果违反授权许可协议的条款，Kaspersky 可能会阻止授权许可密钥。如果授权许可已被阻止，要使用应用程序，您需要添加另外一个授权许可密钥。

授权许可密钥可以是活动密钥或附加（备用）密钥。

*活动授权许可密钥*是应用程序当前使用的授权许可密钥。活动授权许可密钥可以被添加为商业授权许可。应用程序只能拥有一个活动授权许可密钥。

*附加（或备用）授权许可密钥*是允许用户使用应用程序，但是当前未使用的授权许可密钥。与当前授权许可密钥相关联的授权许可过期时，附加授权许可密钥将自动成为当前活动授权许可密钥。只有在添加了活动授权许可密钥之后，才可以添加附加授权许可密钥。

试用授权许可密钥仅可以被当作活动授权许可密钥添加。试用授权许可密钥不可以被当作附加授权许可密钥添加。

关于激活码

*激活码*是由 20 个拉丁字母和数字组成的唯一序列。您必须输入激活码才能添加用于激活 Open Single Management Platform 的授权许可密钥。激活码会发送到您在购买 Open Single Management Platform 或请求 Open Single Management Platform 试用版本时提供的电子邮件地址上。

要使用激活码来激活应用程序，您需要访问互联网以连接到卡巴斯基激活服务器。

如果您在安装应用程序后丢失了激活码，请联系向其购买授权许可的卡巴斯基合作伙伴。

关于密钥文件

*密钥文件*是 Kaspersky 提供的 .key 扩展名的文件。密钥文件设计用于通过添加授权许可密钥激活应用程序。

密钥文件会发送到您在购买 Open Single Management Platform 或订购试用版本的 Open Single Management Platform 时提供的电子邮件地址。

您不需要连接到 Kaspersky 激活服务器以使用密钥文件激活应用程序。

如果密钥文件被意外删除，您可以恢复它。您可能需要密钥文件来注册 Kaspersky CompanyAccount。

若要恢复您的密钥文件，执行下面任何的操作：

- 联系授权许可销售商。
- 使用您有效的激活码，通过卡巴斯基网站接收密钥文件。

授权许可限制

购买 Kaspersky Next XDR Expert 授权许可时，您可以设定要保护的用户数量。您最多可以超过授权许可限制的 5%。如果超过授权许可限制的 5% 以上，则额外的设备和额外的账户将添加到“**受限制资产**”列表中。

如果超过授权许可限制，OSMP 控制台顶部会出现一条通知。

无法启动受限资产的响应操作或行动手册。

要查看受限资产的列表：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 在“**租户**”部分中，单击根租户。
   根租户的属性窗口将打开。

3. 选择“**授权许可**”选项卡。

4. 单击包含受限资产数量的链接。

“**受限制资产**”窗口打开。

列表最多显示 2000 个受限资产（前 1000 个设备和前 1000 个账户）。

Kaspersky Next XDR Expert授权许可功能

Kaspersky Next XDR Expert授权许可扩展了Kaspersky EDR Expert授权许可的功能，增加了用于自动响应和事故管理的高级工具。

Kaspersky Next XDR Expert授权许可包含以下附加功能：

- **高级响应** — 通过自定义脚本或UserGate自动响应警报和事故。
- **XDR响应** — 扩展的XDR响应操作目录。
- **高级案例管理** — 服务级别协议（SLA）、配置警报和事故的自动分配以及跨租户子事故支持。

Kaspersky Next XDR Expert授权许可提供更灵活、可扩展的事故管理，支持集成到复杂的基础架构中，并实现响应流程的高级自动化。

激活 Kaspersky Next XDR Expert

安装 Kaspersky Next XDR Expert 后，您必须在管理服务器属性中激活该应用程序。

要激活 Kaspersky Next XDR Expert：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**授权许可密钥**”区域。
3. 在**当前授权许可**下，单击**选择**按钮。
4. 在打开的窗口中，选择要用于激活 Kaspersky Next XDR Expert 的授权许可密钥。如果未列出授权许可密钥，请单击**添加新授权许可密钥**按钮，然后指定新的授权许可密钥。
5. 如有必要，您还可以添加备用授权许可密钥。为此，请在**备用授权许可密钥**下，单击**选择**按钮，然后选择现有授权许可密钥或添加新授权许可密钥。请注意，如果没有活动授权许可密钥，则无法添加备用授权许可密钥。
6. 单击“**保存**”按钮。

为SIEM组件添加授权许可密钥

可以在 OSMP 控制台中添加应用程序授权许可密钥。如果您使用密钥文件激活应用程序，则可能同时存在两个许可证密钥：一个活动密钥和一个备用密钥。如果您使用激活码，则只有一个授权许可密钥。在KUMA中，一个活动授权许可密钥、一组备用授权许可密钥或一个激活码组成的群组称为*授权许可群组*。因此，您可以使用两个密钥文件或激活码添加授权许可群组。

如果向KUMA实例添加了多个授权许可群组，则所有授权许可群组的活动授权许可密钥将自动合并。这将创建一个*合并授权许可*。此类授权许可的授权许可密钥将按照以下规则合并：

- 将所有活动授权许可密钥的**EPS可用**值相加。合并后的授权许可中会指定最终的EPS值，并且所有租户都可以使用该值。

  如果合并授权许可中包含的任何授权许可密钥过期，则该授权许可密钥的EPS限制值将自动从合并授权许可的EPS总配额中减去。因此，当向合并授权许可中添加新的活动授权许可密钥时，该授权许可密钥的EPS限制值会自动添加到EPS总配额中。

- 租户授权许可中可用的模块集必须相同。如果某个授权许可包含其他授权许可中没有的模块，则合并授权许可中将不包含该模块。因此，任何租户都无法使用该模块。

  向合并授权许可添加新的授权许可密钥时，也适用同样的规则。如果某个模块在新授权许可密钥中可用，但在合并授权许可中不可用，则该模块在合并授权许可下不可用。如果合并授权许可中提供的某个模块在新授权许可密钥中不可用，则该模块在合并授权许可下将不可用。当添加的授权许可密钥与模块集不匹配时，KUMA会显示警告信息，并且只有在您确认后才会添加此类授权许可密钥。

- 合并授权许可最多可以包含50个活动密钥。

只有具有主管理员角色的用户才能添加授权许可密钥。

新增授权许可群组

若要新增授权许可群组：

1. 在应用程序主窗口中，转到**设置**→KUMA→ **打开** KUMA **设置**部分。

   这将打开 KUMA 设置窗口。

2. 在**其他**下，单击**授权许可**。

3. 点击**添加授权许可密钥**。

4. 这将打开一个窗口；在该窗口中，输入新授权许可群组的名称。

5. 单击“**添加**”。

6. 单击新增的授权许可群组的名称。

7. 在打开的窗口中， 选择要添加授权许可密钥的方式：

   - 使用激活码。

     1. 输入激活码。

     2. 如果贵企业使用代理服务器连接到互联网，请输入代理服务器的信息。激活应用程序需要互联网连接。

   - 使用密钥文件。

     1. 在**激活的授权许可密钥**部分，点击**上传**按钮，然后选择密钥文件（扩展名为.KEY的文件）。

     2. 在**备用授权许可密钥**部分，以相同方式添加备用授权许可密钥。

8. 单击“**添加**”。

授权许可群组随即添加到列表中，应用程序将被激活。

添加备用授权许可密钥

若要将备用授权许可密钥添加到授权许可群组：

1. 在应用程序主窗口中，转到**设置**→KUMA→ **打开** KUMA **设置**部分。
   这将打开 KUMA 设置窗口。

2. 在**其他**下，单击**授权许可**。

3. 点击要添加备用授权许可密钥的授权许可群组名称。

4. 这将打开一个窗口；在该窗口的**备用授权许可密钥**部分，点击**上传**按钮，然后选择密钥文件（扩展名为.KEY的文件）。

5. 单击“**添加**”。

替换活动授权许可密钥

如果要添加一个活动授权许可密钥来替换已添加的密钥，请先删除当前授权许可密钥。然后再添加新的授权许可密钥。

查看使用中授权许可密钥的相关信息

要查看活动和备用授权许可密钥：

1. 在主菜单中，转到“**设置**” → “**租户**”。

2. 在“**租户**”部分中，单击根租户。
   根租户的属性窗口将打开。

3. 选择“**授权许可**”选项卡。

   显示活动和备用授权许可密钥。

显示的授权许可密钥应用于根租户的所有子租户。无法为子租户指定单独的授权许可密钥。子租户的属性窗口不包含“**授权许可**”选项卡。

如果超出授权许可密钥限制，则会显示通知，并且有关授权许可密钥的信息会显示警告。

您可以单击“**转到管理服务器**”按钮来管理 Kaspersky Next XDR Expert 授权许可密钥。

在“**授权许可**”选项卡上，您还可以查看授权许可对象的列表。要执行此操作，请单击 ⓘ 按钮。

授权许可对象的可用性取决于购买的授权许可类型。

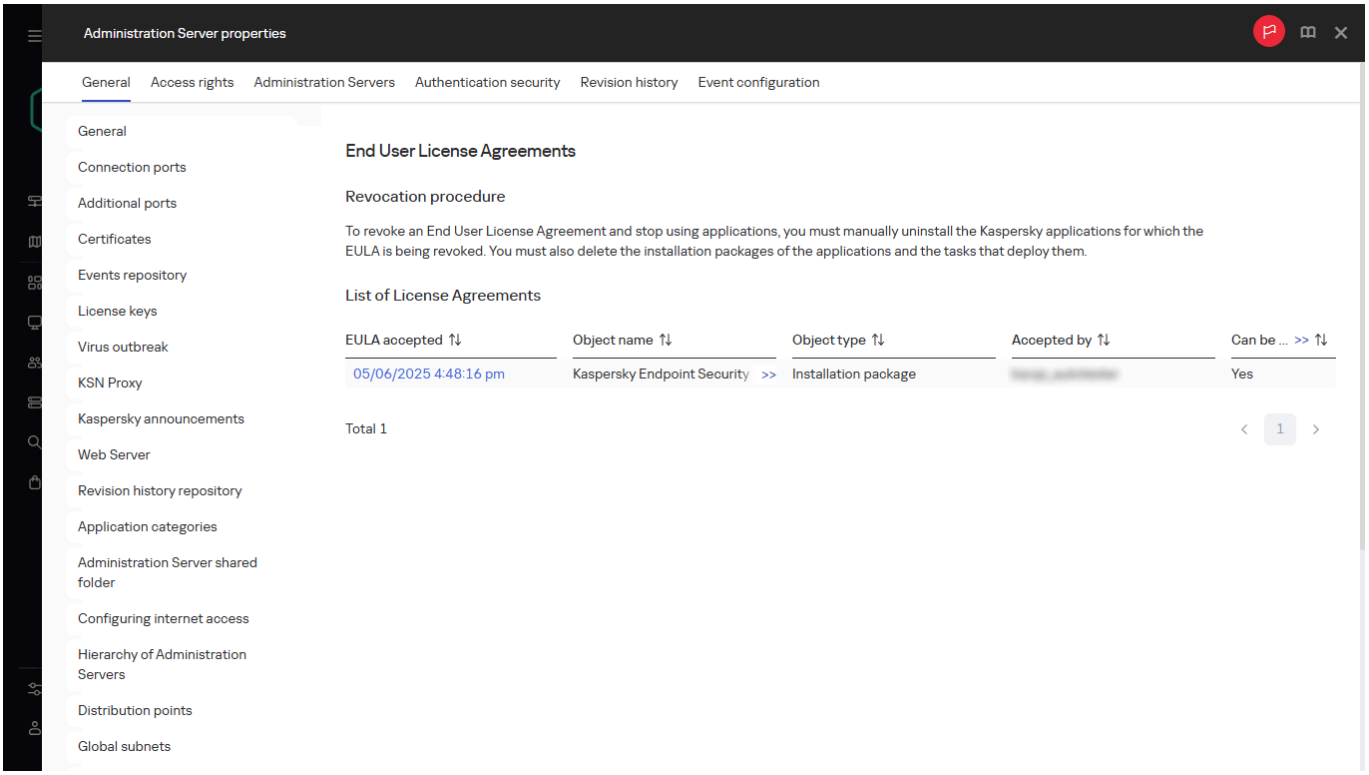
撤销对最终用户授权许可协议的同意

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

要撤销受管理 Kaspersky 应用程序的 EULA：

1. 打开管理服务器属性窗口，然后在**常规**选项卡上选择**最终用户授权许可协议**部分。

   将显示在创建安装包时、无缝安装更新时或部署 Kaspersky Security for Mobile 时接受的 EULA 列表。



EULA 列表

2. 在该列表中，选择要撤销的 EULA。

   您可以查看 EULA 的以下属性：

   - EULA 的接受日期
   - 接受 EULA 的用户名

3. 单击任意 EULA 的接受日期以打开其属性窗口，其中显示以下数据：

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

4. 在 EULA 属性窗口的下部，单击“**撤回授权许可协议**”按钮。

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

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

5. 单击按钮以确认撤销。

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

续订 Kaspersky 应用程序授权许可

您可以续订 Kaspersky Next XDR Expert 的授权许可，也可以续订其中所含 Kaspersky 应用程序（例如 Kaspersky Unified Monitoring and Analysis Platform）的授权许可。您可以续订已过期或将在 30 天内过期的授权许可。

购买新的 Kaspersky Next XDR Expert 授权许可后，将向您的电子邮件地址发送一封电子邮件，包含新授权许可密钥的压缩包。

要续订 Kaspersky Next XDR Expert 的授权许可：

1. 从发送到您电子邮件地址的压缩包中提取新的授权许可密钥。
2. 按照“激活 Kaspersky Next XDR Expert”中描述的步骤操作。

   授权许可即被续订。

如果需要续订随附的卡巴斯基应用程序的授权许可，则必须将新的授权许可密钥添加到这些解决方案的 Web 界面。

有关如何续订 Kaspersky Unified Monitoring and Analysis Platform 授权许可的信息，请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助中的“将授权许可密钥添加到程序 Web 界面”部分。

在 OSMP Console 中，授权许可即将到期时，会按照以下计划显示通知：

- 到期前 30 天
- 到期前 7 天
- 到期前 3 天
- 到期前 24 小时
- 授权许可到期后

移除SIEM组件的授权许可密钥

在 OSMP 控制台中，您可以从程序中移除已添加的授权许可密钥（例如，需要将当前授权许可密钥替换为其他授权许可密钥时）。授权许可密钥移除后，收集器立即停止接收和处理事件。以往的事件仍然可用。创建和修改资源不可用，创建和运行服务也不可用。添加授权许可密钥后，此功能将重新激活。

只有具有主管理员角色的用户才能删除授权许可密钥。

若要删除已添加的授权许可密钥：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**其他**下，单击**授权许可**。
3. 选中要删除的授权许可密钥对应的复选框，然后单击垃圾桶图标（ ）。
4. 这将打开一个确认窗口；在该窗口中，单击**删除**。

   授权许可密钥将从应用程序中移除。

使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案

市场 是主菜单中的一个区域，可让您查看整套 Kaspersky 商业解决方案，选择您需要的解决方案，并在 Kaspersky 网站上进行购买。您可以使用筛选功能，以便仅查看适合您的组织和信息安全系统要求的解决方案。选择解决方案后，Kaspersky Security Center会将您重定向到卡巴斯基网站上的相关网页，以了解有关该解决方案的更多信息。每个网页都可让您继续购买或包含有关购买过程的说明。

在“**市场**”区域中，可以使用以下条件筛选 Kaspersky 解决方案：

- 要保护的设备（端点、服务器和其他类型的资产）数量：
  - 50–250
  - 250–1000
  - 大于 1000
- 组织的信息安全团队的成熟度：
  - **基础**
    这是只有一个 IT 团队的企业的典型成熟度。自动阻止最大可能数量的威胁。
  - **最佳**
    这是在 IT 团队内具有特定 IT 安全功能的企业的典型成熟度。在此级别，所需的解决方案使公司能够应对商品威胁以及绕过现有预防机制的威胁。
  - **专家**
    这是具有复杂和分布式 IT 环境的企业的典型成熟度。IT 安全团队成熟或者公司拥有 SOC（安全运营中心）团队。所需的解决方案使公司能够应对复杂威胁和针对性攻击。
- 您要保护的资产类型：
  - **端点**：员工的工作站、物理机和虚拟机、嵌入式系统
  - **服务器**：物理和虚拟服务器
  - **云**：公有、私有或混合云环境；云服务
  - **网络**：局域网、IT 基础设施
  - **服务**：Kaspersky 提供的安全相关服务

要查找和购买 Kaspersky 商业解决方案：

1. 在主菜单中，转到“**市场**”。
   默认情况下，该区域显示所有可用的 Kaspersky 商业解决方案。
2. 要仅查看适合您组织的解决方案，请在筛选器中选择所需的值。
3. 点击您要购买或想要了解更多信息的解决方案。

   您将被重定向到解决方案网页。您可以按照屏幕上的说明进行购买。

关于数据提供

Kaspersky Next XDR Expert处理以下数据：

- Open Single Management Platform
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Security Center Linux
- 沙盒
- 端点代理程序
  有关端点代理程序传输的数据的详细信息，请参阅相应应用程序的在线帮助文档：
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Mac

关于数据提供

本地处理的数据

Kaspersky Next XDR Expert 旨在实时优化威胁检测、事故调查、威胁响应（包括自动响应）和主动威胁搜索。

Kaspersky Next XDR Expert 执行以下主要功能：

- 接收、处理和存储信息安全事件
- 分析和关联传入的数据
- 事故和警报调查，手动响应。
- 使用预定义和自定义行动手册进行自动响应。
- 基于事件的实时威胁搜索。

为执行其主要功能，Kaspersky Next XDR Expert 可以接收、存储和处理以下信息：

- 有关在所有设备上安装 Kaspersky Next XDR Expert 组件的信息：
  - 设备名称、MAC 地址、操作系统供应商、操作系统内部版本号、操作系统内核版本、所需的已安装软件包、账户权限、服务管理工具类型和端口状态。这些数据由 Kaspersky 部署工具包在安装过程中获取。
  - IPv4 地址。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。

- 用于访问安装了 Kaspersky Next XDR Expert 组件的设备的账户名称和 SSH 密钥。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。
- Kaspersky Next XDR Expert 账户名称和密码。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。
- 数据库访问数据：IP/DNS 名称、端口、用户名和密码。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。
- KUMA 资产清查文件和授权许可密钥。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。
- DNS 区域。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。
- 用于受管理设备与 Open Single Management Platform 组件建立安全连接的证书。这些数据由用户在 Kaspersky 部署工具包配置文件中指定。
- 信息保存在安装日志中，该日志存储在 Kaspersky 部署工具包数据库中。初始基础架构的安装日志保存到用户设备上的文件中。初始基础架构的安装日志保存到用户设备上的文件中。存储期限不设限制；卸载解决方案时将删除安装日志文件。用户名和密码以加密格式存储。
- 事故状态模型信息，包括预定义模型。
- 有关事故类型的信息：事故类型名称、描述和其他常规信息。
- 有关用户账户的信息：全名和电子邮件地址。用户在OSMP控制台中输入数据。数据存储在数据库中，直到用户将其删除。
- 集成令牌数据。
- 有关租户的信息：租户名称、父租户名称、描述。用户在OSMP控制台中输入数据。数据存储在数据库中，直到用户将其删除。
- 证书信息：作为端点代理的应用程序的客户端证书、OSMP服务器证书、KUMA收集器服务器证书。
- 组织网络中的设备信息。
  - 配置相关集成后，OSMP将接收数据。您可以通过以下方式添加资产：
    - 导入资产：
      - On demand from MaxPatrol VM.
      - 定期从卡巴斯基安全管理中心和Kaspersky Industrial CyberSecurity for Networks导入。
    - 通过OSMP控制台或API手动创建资产。
  - OSMP存储以下设备信息：
    - 技术特性（一般属性、操作系统、硬件详细信息和已安装的卡巴斯基应用程序）。
    - 检测到的漏洞和设备防护状态。
    - 特定来源的数据。
    - 设备类别及其严重级别。
    - AI评分和状态。

- 警报和事故数据：
  - 警报信息：触发的规则、与 MITRE 矩阵的对应关系、警报状态、解决结果、分配的操作员或组、受影响的资产（设备和账户）、可观察对象（IP、MD5、SHA256、URL、DNS 域或 DNS 名称、用户名、主机名）、警报涉及 CII 设备的情况、注释和更改日志、文件。这些信息是根据从 Kaspersky Unified Monitoring and Analysis Platform 获取的关联事件在 OSMP Console 中自动生成的。
    - 此外，还会根据警报类型存储其他数据：
      - 对于基于文件扫描结果生成的警报：扫描文件的名称和哈希值；反恶意软件和沙盒判定结果；有关本地文件操作和沙盒分析期间由文件触发的网络活动的信息；包含扫描文件对象的受密码保护的存档；
      - 对于卡巴斯基TAA（IOA）规则生成的警报：有关触发的IOA规则、 IOA规则描述、响应建议以及误报的可能原因的信息（规则信息不由用户提供，而是由卡巴斯基分发）；
      - 对于IOC检测技术生成的警报：触发的IOC规则的名称和严重级别；IOC设备扫描期间已检测到的对象，包括IP地址、DNS记录、注册表项和值、路由表项、进程和文件信息、服务详细信息以及用户名和ID；
      - 对于YARA检测技术生成的警报：触发的YARA规则的名称和严重级别；YARA设备扫描期间已检测到的对象，包括文件和进程信息。
  - 事故信息：关联的警报、子事故、触发的规则、与 MITRE 矩阵的对应关系、事故状态、解决结果、分配的操作员或组、受影响的资产（设备和账户）、可观察对象（来自警报）、事故涉及 CII 设备的情况（包括调查图中的注释）、更改日志、文件、事故类型、事故排序、响应和解决指标，以及触发的 IOA 规则的详细信息，包括其名称、描述、响应建议和可能的误报原因。这些信息由 OSMP Console 根据规则自动生成，或由用户手动生成。
  - 有关配置从警报生成事故的分段规则的数据：名称和规则触发条件、新事故名称的模板、规则描述、规则启动优先级、继承选项和继承范围。用户在OSMP控制台中输入数据。
  - 通知模板信息：模板名称、消息主题、消息正文模板、模板描述、触发时发送通知的检测规则、选定的需向用户发送通知的检测技术，以及警报和事故的严重级别。用户在OSMP控制台中输入数据。
- 警报和事故的到期日期设置。
- 事故调查图和进程树。OSMP存储以下用户定义的关于为事件构建的进程树的信息：已创建进程树的名称和备注；
- 行动手册数据：
  - 行动手册操作数据，包括响应操作参数的数据：名称、描述、标签、触发器和算法。用户在OSMP控制台中输入数据。
  - 行动手册中执行响应操作的数据：来自集成系统的数据和来自设备的数据。
  - 所有警报和事故的完整响应历史记录，包括未与警报或事故关联的响应操作。

  上面列出的数据将在数据库中存储三天，然后删除。卸载Kaspersky Next XDR Expert时，数据将被完全删除。
- 访问共享资源的凭证。这些凭证以加密形式存储，并分发到设备以支持响应操作，例如获取内存转储和磁盘镜像。
- 有关通过响应操作从设备获取或由用户手动上传的文件的信息，包括文件名或文件的完整路径、大小、哈希值、租户、源设备或上传用户、描述、扫描状态（防病毒、YARA、沙盒）和扫描结果。

- 关于应用于设备的防御规则的信息。包括规则名称、哈希值、租户、规则适用的设备、规则状态（启用或禁用）以及在执行与防御规则匹配的文件时通知端点用户的选项。

- 关于用于扫描设备的YARA规则的信息。包括规则名称、租户、描述以及文件扫描选项（启用或禁用），该选项决定此规则是否应用于服务器端扫描从设备获取或用户上传的文件。规则以文件的形式存储在OSMP对象存储中，并在执行YARA扫描响应操作时发送到端点。

- 关于用于设备扫描的IOC规则信息。包括规则名称、严重级别、租户以及定期扫描选项（启用或禁用）。规则以文件的形式存储在OSMP对象存储中，并在执行IOC扫描响应操作时发送到终端。对于定期扫描，扫描时间表也会发送到终端，包括启用和禁用选项、扫描开始时间和最大扫描持续时间。

- 文件对象扫描设置，包括用于存档解密的常用客户端密码目录以及资产管理和沙盒数据库的更新来源。这些设置由用户在OSMP控制台中配置。

- 在OSMP中使用KPSN时，将处理以下数据：部署KPSN API的服务器的名称或IP地址，以及用于连接到API的证书。

- 集成设置数据（Kaspersky 解决方案或服务，以及参与 Kaspersky Next XDR Expert 场景的第三方解决方案）：

  - Kaspersky 威胁情报门户集成：用于连接到 Kaspersky 威胁情报门户的 API 访问令牌、缓存保留期、连接是否通过代理或服务类型。用户在OSMP控制台中输入数据。

  - KATA 和 KEDR 集成：KATA 和 KEDR 服务器地址：IP 地址或主机名、端口、用于连接到 KATA 和 KEDR 的唯一 ID、证书文件以及用于连接到 KATA 和 KEDR 的私钥。用户在OSMP控制台中输入数据。

  - 连接到将运行自定义脚本的主机：IP 地址或主机名、端口、用户名和 SSH 密钥以及密码或密钥。用户在OSMP控制台中输入数据。

  - OSMP 管理服务器集成：管理服务器名称，层次结构中管理服务器的完整路径。用户在OSMP控制台中输入数据。

  - Kaspersky CyberTrace 集成：Kaspersky CyberTrace 可用的 IPv4 地址或主机名和端口、名称和密码。用户在OSMP控制台中输入数据。

  - Kaspersky Automated Security Awareness Platform（KASAP）集成：用于连接到KASAP的API访问令牌、KASAP门户URL、KASAP管理员电子邮件地址以及连接是否通过代理。用户在OSMP控制台中输入数据。

  - Active Directory 集成：域控制器的地址、用于连接到域控制器的用户名和密码以及证书。用户在OSMP控制台中输入数据。

  - 外部系统集成（例如 UserGate）：用于远程访问客户端设备的账户名称和 SSH 密钥或密码。

  - 卡巴斯基沙盒的集成：部署沙盒的虚拟机操作系统的参考配置、沙盒服务器IP地址、沙盒服务器证书、OSMP控制台中显示的服务器名称以及用于文件分析的沙盒规则。用户在OSMP控制台中输入数据。

- 用户连接到OSMP控制台时使用的IP地址由控制台自动记录，并一直存储到该用户编辑过的对象修订版本的保留期结束。

- 有关OSMP安装程序层次结构配置的信息。

有关为执行Kaspersky Next XDR Expert的主要功能而接收、存储和处理的其他数据的详细信息，请参阅应用程序帮助：

- Kaspersky Security Center 15.4 Linux
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky EDR Expert

上述数据存储在数据库中，直到用户将其删除。与警报或事故相关的数据将存储至警报或事故的整个保留期结束。所有其他数据将无限期存储，直至用户删除数据或删除与数据关联的租户。卸载Kaspersky Next XDR Expert时，数据将被完全删除。

上述所有数据只能通过Kaspersky Next XDR Expert组件的转储文件、跟踪文件或日志文件传输给卡巴斯基，包括安装程序和实用程序创建的日志文件。Kaspersky Next XDR Expert 组件的转储文件、跟踪文件或日志文件包含个人或机密数据。转储文件、跟踪文件或日志文件以明文形式存储在设备上。转储文件、跟踪文件或日志文件不会自动传输到卡巴斯基，但管理员可以根据技术支持的请求手动将这些文件传输到卡巴斯基，以解决与 Kaspersky Next XDR Expert 性能相关的问题。卡巴斯基将根据适用法律和卡巴斯基策略保护所有收到的数据。数据均通过安全通讯渠道传输。此类信息的默认存储期限（轮换期）为 7 天。

传输到 AO Kaspersky Lab 的数据

通过 OSMP 控制台中的链接访问 Kaspersky Next XDR Expert 帮助时，用户同意将以下数据自动传输给卡巴斯基：Kaspersky Next XDR Expert 代码、Kaspersky Next XDR Expert 版本和 Kaspersky Next XDR Expert 本地化信息。

为了向员工分配培训课程，Kaspersky Next XDR Expert 会将以下数据传输到 Kaspersky Automated Security Awareness Platform：用户电子邮件地址、Kaspersky Automated Security Awareness Platform ID 和培训组 ID。

为了获取其他警报数据，Kaspersky Next XDR Expert 会将与警报、事故和事件相关的可观察对象的类型和值传输到 Kaspersky 威胁情报门户。

为了获取有关通过警报、事故或事故卡片中的链接访问检测到的威胁的评估信息，Kaspersky Next XDR Expert会将以下数据传输到Kaspersky Threats服务：名称。

为了接收事故检测和响应服务，Kaspersky Next XDR Expert将以下数据传输到“卡巴斯基托管检测和响应”服务：

- 启用与Kaspersky Managed Detection and Response的集成后，OSMP会临时存储以下数据，直到成功传输并将其传输到Kaspersky Managed Detection and Response基础设施：接收规则触发事件的设备标识符、用户标识符和Kaspersky Managed Detection and Response客户端标识符。
- 使用OSMP中的卡巴斯基托管检测与响应解决方案时，警报中的以下额外信息会传输到“卡巴斯基托管检测与响应基础”设施：扫描文件的名称和哈希值；反恶意软件和沙盒检测结果；有关沙盒分析期间文件生成的本地文件操作和网络活动的信息；包含扫描文件对象的受密码保护的容器；以及触发IOA规则的事件，其中可能包括设备上的文件和应用程序名称、注册表密钥名称和值以及用户名。
- 使用OSMP的Kaspersky Managed Detection and Response解决方案时，用户请求会将以下事故相关信息传输到Kaspersky Managed Detection and Response基础设施：事故名称；创建日期和时间以及上次更新日期和时间；有关触发规则和相关MITRE策略和技术的信息；分配给该事故的运算符名称；受影响设备的名称和标识符；以及警报中包含的事件。这些事件可能包括客户设备上的文件名、注册表项名称、应用程序名称和用户名。

  所有这些数据仅在用户接受“卡巴斯基托管检测与响应”数据处理协议（DPA）后才会传输到“卡巴斯基托管检测与响应”。在“卡巴斯基托管检测与响应”界面中激活该服务时，系统会确认该协议。

为了增强信息保护能力，Kaspersky Next XDR Expert会将OSMP运行期间生成的KSN统计数据传输到“卡巴斯基安全网络”服务。传输的数据范围在 KSN 声明中规定，该声明包含在应用程序分发包中。参与KSN是可选的，由OSMP用户自行控制。传输前，KSN统计数据会临时缓存在托管OSMP组件的服务器上。

使用“卡巴斯基专用安全网络”时，KSN统计数据会缓存在托管OSMP组件的服务器上，其范围与使用“卡巴斯基安全网络”时相同。如果“卡巴斯基专用安全网络”服务器位于组织外部，缓存的KSN统计数据可能会传输到组织外部。“卡巴斯基专用安全网络”管理员有责任确保此数据的安全。

提供给第三方的数据

通过访问警报或事故详情中的链接以获取有关 MITRE 战术或技术的信息，以下有关 MITRE 战术或技术的信息将被传输到 MITRE 网站：ID 和类型。

为了通过在远程客户端设备上执行第三方脚本，利用外部系统（例如UserGate）执行响应操作，Kaspersky Next XDR Expert会将以下信息传输到外部系统：警报和事故中可观察对象的类型和值。

为了在从事件卡中点击链接时检查文件和URL的声誉，Kaspersky Next XDR Expert将以下信息传输到VirusTotal服务：文件哈希值（FileMd5和FileSha256）；远程主机名（NetUrlHostname）；HTTP请求的目标URI（NetUri）；目标IPv4或IPv6地址（NetDstIp）；DNS查询中请求的URL（DnsResourceName）；以及请求的DNS服务器（DnsServerIp）。

Kaspersky Unified Monitoring and Analysis Platform 中的数据提供

提供给第三方的数据

KUMA 功能不涉及自动向第三方提供用户数据。

本地处理的数据

Kaspersky Unified Monitoring and Analysis Platform（以下简称 KUMA 或“程序”）是一个集成软件解决方案，包括以下主要功能：

- 接收、处理和存储信息安全事件
- 分析和关联传入的数据
- 在接收到的事件中搜索
- 检测到信息安全威胁的症状时创建通知。
- 创建警报和事故以处理信息安全威胁。
- 在仪表板和报告中显示有关客户基础设施状态的信息。

- 监控事件源。
- 设备（资产）管理–查看、搜索、添加、编辑和删除资产，以及将资产信息导出到 CSV 文件。

为了执行其主要功能，KUMA 可能会接收、存储和处理以下信息：

- 企业网络上的设备信息。

  如果配置了相应集成，KUMA Core 服务器将接收数据。您可以通过以下方式将资产添加到 KUMA：

  - 导入资产：
    - 根据需要从 MaxPatrol VM 导入。
    - 按计划从 Open Single Management Platform 和 KICS for Networks 导入。
  - 通过 Web 界面或 API 手动创建资产。

  KUMA 存储以下设备信息：

  - 设备的技术特性。
  - 在资产上检测到的漏洞。
  - 特定于资产来源的信息。
- 用户指定用于向 NCIRCC 发送事故的企业网络中设备的其他技术属性：IP 地址、域名、URI、受监控对象的电子邮件地址、遭受攻击的网络服务以及端口/协议。
- 组织信息：名称、税号、地址、用于发送通知的电子邮件地址。
- 通过查询 Active Directory 网络而获得的有关组织单位、域、用户和组的 Active Directory 信息。

  如果配置了相应的集成，KUMA Core 服务器将收到此信息。为确保与 LDAP 服务器的连接安全性，用户必须在 KUMA 控制台中输入服务器 URL、基本 DN、连接凭证和证书。
- KUMA 中用于用户域身份验证的信息包括：用于在 Active Directory 目录服务中搜索访问组的根 DN、域控制器的 URL、证书（用于签署 AD 证书的根公钥）、Active Directory 中用户访问组的完整路径（区分名称）。
- 来自已配置来源的事件中包含的信息。

  在收集器中，事件源完成配置后，会生成 KUMA 事件并将其发送到其他 KUMA 服务。有时事件可能首先到达代理服务，再由代理服务将事件从来源转发至收集器。此外，您可以配置保存聚合事件服务器的地址或主机名。

  此外，端点代理程序会根据事件数据模型向OSMP发送有关事件的信息。
- KUMA 与其他应用程序集成所需的信息（涉及的应用程序包括：Kaspersky Threat Lookup、Kaspersky CyberTrace、Open Single Management Platform、Kaspersky Industrial CyberSecurity for Networks、Kaspersky Automated Security Awareness Platform、Kaspersky Endpoint Detection and Response、Security Orchestration, Automation and Response、AI 服务：AI 资产评分和状态、Kaspersky Investigation and Response Assistant）。

  该信息包括用于与其他应用程序建立连接的证书、令牌、URL 或凭据，以及 KUMA 基本功能运行所需的必要数据（例如电子邮箱）。用户在 KUMA 控制台中输入此数据
- 已配置事件接收的来源相关信息。

  该信息包括源名称、主机名、IP 地址，以及分配给事件源的监控策略。监控策略指定了负责人的电子邮件地址，如果违反策略，将向其发送通知。

- 用户账户：姓名、用户名、电子邮件地址。用户可以在 KUMA 控制台中查看自己的个人资料数据。
- 用户个人资料设置：
  - KUMA 中的用户角色。用户可以看到分配给自己的角色。
  - 本地化语言、通知设置、不可打印字符的显示。
    用户在 KUMA 界面中输入此数据。
  - **资产**部分的资产类别列表、默认仪表板、仪表板的电视模式标识、默认事件的 SQL 查询语句、默认预设配置。
    用户在 KUMA 控制台的相应部分中指定这些设置。
- KUMA 中用户域身份验证所需数据：
  - Active Directory：用于在 Active Directory 目录服务中搜索访问组的根 DN、域控制器的 URL、证书（用于 AD 证书签名的根公钥）、AD 中用户访问组的完整路径（专有名称）。
  - Active Directory Federation Services：信任方 ID（AD FS 中的 KUMA ID）、用于获取 Connect 元数据的 URL、用于从 AD FS 重定向的 URL 以及 AD FS 服务器证书。
  - FreeIPA：基本 DN、URL、证书（用于 FreeIPA 证书签名的根公钥）、自定义集成凭证、连接凭证。
- 审计事件
  KUMA 自动记录审计事件。
- KUMA 日志
  用户可以在 KUMA 控制台中启用扩展日志功能。日志条目存储在用户的设备上，不会自动传输任何数据。
- 有关用户接受卡巴斯基法律协议条款和条件的信息。
- 用户在 KUMA 界面中输入的任何信息。

上述列出的信息可以通过以下方式录入 KUMA：

- 用户在 KUMA 控制台中输入信息。
- 如果用户配置了与事件源的连接，KUMA 服务（代理或收集器）会接收相关数据。
- 通过 KUMA REST API。
- 可使用 MaxPatrol VM 的实用程序获取设备信息。

列出的信息存储在 KUMA 数据库（MongoDB、ClickHouse、SQLite）中。密码以加密形式存储（存储密码的哈希值）。

上述列出的所有信息仅能通过以下形式传输到卡巴斯基：转储文件、跟踪文件，或 KUMA 组件的日志文件（包括安装程序和实用程序创建的日志文件）。

转储文件、跟踪文件以及 KUMA 组件的日志文件可能包含个人信息和机密信息。转储文件、跟踪文件和日志文件以非加密形式存储在设备上。转储文件、跟踪文件和日志文件不会自动提交给卡巴斯基，但管理员可以按照技术支持部门的请求手动将这些信息提交给卡巴斯基，以帮助对 KUMA 进行故障排查。

卡巴斯基以匿名形式使用收集的数据，且仅用于一般统计目的。汇总统计数据根据接收到的原始数据自动生成，不包含任何个人信息或其他机密信息。当新数据累积时，旧数据会被删除（每年一次）。汇总统计数据将无限期保存。

卡巴斯基将根据适用法律和卡巴斯基策略保护所有收到的数据。数据均通过安全通讯渠道传输。

沙盒中的数据提供

存储在具有沙盒组件的服务器上的数据

- 扫描的文件：`/var/opt/kaspersky/sandbox/library/`。
- 文件扫描结果：`/var/opt/kaspersky/sandbox/library/`和`/tmp/`。
- 任务设置：`/var/opt/kaspersky/sandbox/library/`以及 Sandbox 组件数据库。
- 跟踪文件：`/var/log/kaspersky/sandbox/`。
- 更新源设置：`/var/opt/kaspersky/apt-updater`。
- 最短密码长度设置：`/var/opt/kaspersky/apt-config-ram-common/validator.conf`。
- 虚拟机：`/vm`。
- 已下载的 iso 格式操作系统和应用程序镜像：`/var/opt/kaspersky/sandbox/custom_images/iso`。

启动

以下场景展示了从购买 Kaspersky Next XDR Expert 到执行事故调查和威胁搜索的分步操作。

首先完成 Kaspersky Next XDR Expert 安装和初始配置，然后探索 Kaspersky Next XDR Expert 威胁检测和搜索功能，最后查看事故调查工作流程的示例。

Kaspersky Next XDR Expert 的部署和初始设置

按照此方案，您可以部署 Open Single Management Platform 并包含运行 Kaspersky Next XDR Expert 解决方案所需的所有组件，然后执行所需的初步配置和集成。

先决条件

在开始之前，请确保：

- 您拥有 Kaspersky Next XDR Expert 和兼容 EPP 应用程序的授权许可密钥。
- 您的基础架构满足硬件和软件要求。

阶段

主要安装方案和初始配置场景分阶段进行：

1. **部署**

   准备好部署 Open Single Management Platform 以及部署 Kaspersky Next XDR Expert 所需所有组件的基础架构，然后使用 Kaspersky 部署工具包实用程序部署该解决方案。

2. **激活**

   使用您的授权许可激活 Kaspersky Next XDR Expert 解决方案。

3. **多租户配置**

   如需要，您可以使用多租户功能：

   1. 规划和创建所需的租户层次结构。
   2. 在 Open Single Management Platform 中创建匹配的管理服务器层级结构。
   3. 将租户绑定到相应的管理服务器。
   4. 为所有 Kaspersky Next XDR Expert 用户创建用户账户，然后分配角色。

4 添加资产

在 Kaspersky Next XDR Expert 中，您的基础设施中必须受保护的设备会被标识为资产。Open Single Management Platform 允许您发现网络中的设备并管理其保护策略。您也可以在第 8 阶段手动添加资产或从其他来源导入资产。

用户账户在 Kaspersky Next XDR Expert 中也被标识为资产。确保在第 9 阶段配置与 Active Directory 的集成，以便在相关事件、警报和事故中显示受影响的用户账户。

5 添加用户和分配角色

为用户账户分配角色，以根据任务定义用户对各种 Kaspersky Next XDR Expert 功能的访问权限。

6 连接到 SMTP 服务器

配置与 SMTP 服务器的连接，以便通过电子邮件通知有关 Kaspersky Next XDR Expert 中发生的事件。

7 安装端点保护应用程序和解决方案

Kaspersky Next XDR Expert 的运行，有赖于从资产所安装安全应用程序接收到的事件。检查兼容的卡巴斯基应用程序和解决方案列表。您可以使用 Open Single Management Platform 在您基础架构的设备上部署卡巴斯基应用程序。

确保端点保护应用程序与 Kaspersky Anti Targeted Attack Platform 集成。例如，如果您在资产上使用 Kaspersky Endpoint Security，请参阅以下帮助文档之一，了解如何配置与 KATA 的集成：

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

8 配置事件源、存储和关联

指定事件的接收来源以及事件的存储和处理方式：

1. 登录 KUMA 控制台。
2. 设置 Kaspersky Unified Monitoring and Analysis Platform 与 Kaspersky Security Center 的集成。
3. **从 Open Single Management Platform 导入资产**。

   受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

   KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

   - 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
   - 资产属性信息：漏洞；软件，包括操作系统；资产所有者

   若要导入卡巴斯基安全管理中心资产信息：

   1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
   2. 点击**导入**，然后选择以下操作之一：

      - 如要导入资产基本属性信息，请点击**导入KSC资产**。

        这将打开**导入KSC资产**窗口。

- 若要导入资产其他属性信息，请点击**导入KSC资产属性**。

  这将打开**导入KSC资产属性**窗口。

3. 在下拉列表中，选择要为其执行导入操作的租户。

   在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。

   如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。

4. 单击“**导入**”按钮。

将导入资产信息。

此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

4. 手动添加资产或从其他来源导入资产（可选）。

5. 配置事件源以指定您想要从中接收事件的位置。

6. 为事件创建存储。

7. 创建收集器以接收、处理（规范化）和传输事件。

8. 创建关联器，以对规范化事件进行初步分析和进一步处理。

   在创建关联器时，您可以创建关联规则来定义处理和响应事件的规则。您也可以导入之前保存的关联规则，或者使用 Kaspersky Next XDR Expert 解决方案提供的现成关联规则集。创建关联器后，您可以根据需要将关联规则链接到关联器。

   建议在此阶段配置排除项，以避免误报和无关数据。

9 配置集成

配置 Kaspersky Next XDR Expert 与 Active Directory 以及其他 Kaspersky 解决方案的集成，以扩展功能范围并丰富事故调查所需数据。

1. 与 Active Directory 集成（强烈推荐）。

2. 与 KATA/EDR 集成（需要授权许可）。

3. 与 Kaspersky CyberTrace 集成（可选集成；需要授权许可）。

4. 与 Kaspersky TIP 集成（可选集成；需要授权许可）或 Kaspersky Open TIP 集成。

5. 与 Kaspersky Automated Security Awareness Platform 集成（可选集成；需要授权许可）。

10 配置更新

创建“下载更新至管理服务器存储库”任务。

11 验证配置准确性

在其中一个资产上使用 EICAR 测试文件。若初始设置正确执行且已配置必要的关联规则，则该事件将触发在警报列表中创建警报的动作。

初始设置完成后，Kaspersky Next XDR Expert 将接收并处理来自受保护资产的事件，并在触发关联规则时创建警报。

验证 Kaspersky Next XDR Expert 配置的正确性

您可以在其中一个资产上使用 EICAR 测试病毒，确保 Kaspersky Next XDR Expert 已正确部署和配置。如果初始设置正确执行并且配置了必要的关联规则，则关联事件将触发在警报列表中创建警报。

要验证 Kaspersky Next XDR Expert 配置的正确性：

1. 在 OSMP Console 的 KUMA 部分中创建一个新的关联器。
   创建关联器时，请勿在“**关联**”部分指定参数。
2. 从 SOC 内容包中导入关联规则，以获取用于检测 EICAR 测试病毒的预定义关联规则。
3. 为创建的关联器指定关联规则。
   您可以使用以下方法之一来指定关联规则：
   - 将预定义的关联规则关联到创建的关联器：
     a. 转到“**资源**”，单击“**关联规则**”，然后选择将应用关联规则的租户。
     b. 在预定义关联规则列表中，选择“**R077_02_KSC.Malware detected**”规则以检测来自 Kaspersky Security Center 的事件。
     c. 单击“**关联到关联器**”，然后选择创建的关联器以将所选的关联规则关联到关联器。
   - 使用预定义过滤器手动创建关联规则：
     a. 打开创建的关联器设置，转到**“关联”部分**，然后单击“**添加**”。
     b. 在“**创建关联规则**”窗口的“**常规**”选项卡上，设置以下参数以及其他规则参数：
        - **类型**：简单。
        - **传播的字段**：DestinationAddress、DestinationHostName、DestinationAccountID、DestinationAssetID、DestinationNtDomain、DestinationProcessName、DestinationUserName、DestinationUserID、SourceAccountID、SourceUserName。
     c. 转到“**选择器**” → “**设置**”，然后指定表达式来过滤所需的事件：
        - 在构建器模式下，使用“AND”运算符添加“**f: KSC 事件**”、“**f: KSC 病毒检测**”和“**f: 基础事件**”过滤条件。
        - 或者，您也可以在源代码模式下按如下方式指定此表达式：

          ```
          filter='b308fc22-fa79-4324-8fc6-291d94ef2999'
          AND filter='a1bf2e45-75f4-45c1-920d-55f5e1b8843f'
          AND filter='1ffa756c-e8d9-466a-a44b-ed8007ca80ca'
          ```

     d. 在关联规则设置的“**操作**”部分，仅选中“**输出**”复选框（必须取消选中“**循环到关联器**”和“**无警报**”复选框）。在这种情况下，当检测到 EICAR 测试病毒时，将创建关联事件，并在 Kaspersky Next XDR Expert 的警报列表中创建警报。
     e. 单击“**新建**”以保存与关联器相关的关联规则设置。

4. 在 OSMP Console 的 KUMA 部分中创建并配置一个收集器，用于从 MS SQL 数据库接收有关管理服务器事件的信息。

   或者，您可以使用预定义的 [OOTB] KSC SQL 收集器。

5. 在收集器设置的“**路由**”部分中，将“**类型**”设置为“**关联器**”，然后在“**URL**”字段中指定创建的关联器，以将处理后的事件转发至该关联器。

6. 在组织网络的资产上安装网络代理和端点保护应用程序（例如，Kaspersky Endpoint Security）。确保资产已连接到管理服务器。

7. 将 EICAR 测试文件放置在资产上，然后使用端点保护应用程序检测测试病毒。

之后，管理服务器将收到有关资产相关事件的通知。此事件将被转发到 KUMA 组件，转换为关联事件，然后此事件将触发在 Kaspersky Next XDR Expert 的警报列表中创建警报。如果已创建警报，则表示 Kaspersky Next XDR Expert 运行正常。

使用威胁监控、检测和搜索功能

安装和配置 Kaspersky Next XDR Expert 后，您可以使用 Kaspersky Next XDR Expert 功能监控基础架构的安全性、调查安全事故、自动化工作流程和主动搜索威胁：

- **使用仪表板和自定义小部件**

  仪表板的“**检测和响应**”选项卡可以包含小部件，这些小部件可显示有关检测到和已注册警报和事故以及对其所采取响应操作的信息。您可以使用和自定义仪表板中预配置的小部件布局，或者创建新的布局和小部件。

  Open Single Management Platform 还提供各种安全监控和报告工具。

- **使用报告**

  您可以在 Kaspersky Unified Monitoring and Analysis Platform 中配置报告生成，以根据指定的时间计划接收所需的汇总数据。

- **使用威胁搜索**

  您可以使用威胁搜索工具分析事件，以搜索尚未自动检测到的威胁和漏洞。威胁搜索既可用于警报和事故调查，也可用于主动搜索威胁。

- **使用行动手册**

  您可以使用行动手册根据指定的算法自动响应警报和事故。您可以在各种操作模式下启动一系列预定义的行动手册。您可以创建自定义行动手册。

使用 Kaspersky Next XDR Expert 进行事故调查的示例

此场景展示了事故调查的工作流程示例。

事故调查分阶段进行：

1. **向用户分配警报**

   您可以将警报分配给自己或其他用户。

2. **检查触发的关联规则是否与警报事件的数据匹配**

   查看有关警报的信息，并确保警报事件数据与触发的关联规则匹配。如果警报为误报，请编辑关联规则。

3. **分析警报信息**

   分析有关警报的信息，以确定进一步分析警报所需的数据。

4. **手动增强**

   启动可用的解决方案，以进一步增强事件数据（例如，Kaspersky TIP）。

5. **误报检查**

   确认触发关联规则的活动对于组织 IT 基础设施而言是否属于异常活动。

6. **事故创建**

   如果步骤 3 到 5 表明该警报需要调查，您可以创建事故或将警报链接到现有事故。

   您也可以合并事故。

7. **事故管理**

   您可以通过更改事故状态和优先级以及将其分配给其他分析师来管理事故。

   您还可以管理事故 SLA、类型和工作流。此外，您还可以跟踪事故相关工作所花费的精力。

8. **调查**

   此步骤包括查看与事故相关的资产、用户账户以及警报的信息。您可以使用调查图和威胁搜索工具来获取更多信息。

9. **搜索相关资产**

   您可以查看与事故相关的资产上所发生的警报。

10. **搜索相关事件**

    您可以通过搜索相关警报的事件来扩展调查范围。

11. **查看事故历史记录**

    您可以查看事故的变更日志和响应历史记录。

12. **注释**

    您可以留下注释，其中包含调查事故相关的必要信息。

13. **响应**

    您可以手动执行响应操作。

14. **使用行动手册进行响应**

    您可以手动启动行动手册来响应事故。

15. **关闭事故**

    在采取措施清除攻击者在组织 IT 基础设施中存在的痕迹后，您可以关闭事故。

部署 Kaspersky Next XDR Expert

按照此应用场景，您可以为部署Open Single Management Platform和Kaspersky Next XDR Expert（包括Kaspersky Endpoint Detection and Response功能）的所有必要组件准备基础设施，准备包含安装参数的配置文件，并使用卡巴斯基部署工具包实用程序（以下简称KDT）部署解决方案。

在部署 Open Single Management Platform 和 Kaspersky Next XDR Expert 组件之前，建议先阅读强化指南。

部署方案分阶段进行：

1. **选择部署 Kaspersky Next XDR Expert 的选项**

   选择最适合您组织的 Kaspersky Next XDR Expert 配置。多节点部署和单节点部署都可用。

2. **下载包含 Kaspersky Next XDR Expert 组件的分发包**

   分发包中包含以下组件：

   - 包含Kaspersky Next XDR Expert 组件以及Kaspersky Next XDR Expert和KDT最终用户授权许可协议的传输存档文件

     组件使用RSA密钥和GOST R 34.11-2012密钥签名。您可以验证Kaspersky Next XDR Expert组件的真实性和完整性。

   - 包含KDT实用程序、配置文件和KUMA清查文件模板的存档文件

3. **安装数据库管理系统（DBMS）**

   对于多节点部署，请在不包含在Kubernetes集群的独立服务器上手动安装DBMS。

   对于单节点部署，请在部署Kaspersky Next XDR Expert之前在目标主机上手动安装DBMS。在这种情况下，DBMS 和 Kaspersky Next XDR Expert 组件安装在同一目标主机上，但 DBMS 不包含在 Kubernetes 集群中。

4. **准备管理员主机和目标主机**

   根据所选的部署方案，定义将在其上部署 Kubernetes 集群以及该集群中包含的 Kaspersky Next XDR Expert 组件的目标主机数量。准备所选的管理员主机和目标主机以部署 Kaspersky Next XDR Expert。

   说明：

   - 多节点部署：准备管理员和目标主机
   - 单节点部署：准备管理员和目标主机

5. **准备 KUMA 主机以在 Kubernetes 集群外部安装 KUMA 服务（可选）**

   KUMA服务（收集器、关联器和存储）可以完全安装在Kubernetes集群内，完全安装在集群外的单独主机上，或者部分安装在集群内，部分安装在集群外。

   如果您希望将 KUMA 服务完全安装在 Kubernetes 集群外部的独立主机上，或者部分安装在集群内部，部分安装在集群外部，请准备 KUMA 目标主机以安装 KUMA 服务。

   操作指南：准备 KUMA 主机以在 Kubernetes 集群外部通过安装程序安装 KUMA 服务

6 准备 KUMA 清查文件以在 Kubernetes 集群外部安装 KUMA 服务（可选）

如果您希望将 KUMA 服务完全安装在 Kubernetes 集群外部的独立主机上，或者部分安装在集群内部，部分安装在集群外部，请准备 YAML 格式的 KUMA 清查文件。KUMA 清查文件包含用于在 Kubernetes 集群外部安装 KUMA 服务的参数。

操作指南：准备 KUMA 清查文件以在 Kubernetes 集群外部安装 KUMA 服务

7 准备配置文件

以 YAML 格式准备配置文件。该配置文件包含要部署的目标主机列表以及 Kaspersky Next XDR Expert 组件的一组安装参数。

如果您在单节点上部署Kaspersky Next XDR Expert，请使用包含特定于单节点部署的安装参数的配置文件。

说明：

- 多节点部署：指定安装参数
- 单节点部署：指定安装程序参数

您可以手动填写配置文件模板；或者使用“部署向导”来指定 Kaspersky Next XDR Expert 部署所需的安装参数，然后生成配置文件。

操作指南：使用“部署向导”指定安装参数

8 部署 Kaspersky Next XDR Expert

使用 KDT 部署 Kaspersky Next XDR Expert。KDT 会自动部署 Kubernetes 集群，Kaspersky Next XDR Expert 组件和其他基础架构组件均安装于该集群中。

操作说明：安装 Kaspersky Next XDR Expert

9 安装 KUMA 服务

安装 KUMA 服务（收集器、关联器和存储）。

KUMA服务可以完全安装在Kubernetes集群内，完全安装在集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。

操作指南：在Kubernetes集群外部安装KUMA服务

操作说明：在Kubernetes集群内安装KUMA服务

10 添加从属管理服务器

如需进一步集成端点代理程序，必须部署从属管理服务器。

操作说明：添加从属管理服务器

11 安装和集成端点代理

按照端点代理文档中的说明来安装端点代理：

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

配置与端点代理的集成。

12 安装和集成 Sandbox

安装 Sandbox，进行配置，然后在其中安装虚拟机。

配置与 Sandbox 的集成。

强化指南

The Hardening Guide is intended for professionals who deploy and administer Kaspersky Next XDR Expert, as well as for those who provide technical support to organizations that use Kaspersky Next XDR Expert.

强化指南描述了配置 Kaspersky Next XDR Expert 及其组件的建议和功能，旨在降低其被损害的风险。

强化指南包含以下信息：

- 准备 Kaspersky Next XDR Expert 部署的基础架构
- 配置与 Kaspersky Next XDR Expert 的安全连接
- 配置用于访问 Kaspersky Next XDR Expert 的账户
- 管理 Kaspersky Next XDR Expert 的保护
- 管理客户端设备保护
- 配置受管理应用程序的保护
- 将信息传输到第三方应用程序

在开始部署 Kaspersky Next XDR Expert 之前，建议您阅读强化指南。

管理 Kaspersky Next XDR Expert 的基础架构

本部分介绍了操作系统及 Kaspersky Next XDR Expert 正常运行所需的核心原则 — 仅使用满足功能需求的最少应用程序。本部分还介绍了最小特权原则，可归结为零信任的概念。

管理操作系统账户

要使用 KDT 与 Kubernetes 集群协作，建议创建一个具有最小权限的单独用户。最佳方法是使用 LDAP 来实现对操作系统用户账户的管理，并能够通过 LDAP 撤销用户权限。有关用户撤销和阻止的具体实施，请参阅 LDAP 解决方案中的用户/管理员指南。建议使用至少 18 个字符的密码或包含任意分隔符、至少 4 个单词的密码短语来验证用户身份。您也可以使用物理身份验证方式（例如，令牌）。

有关更多信息，请参阅OpenLDAP软件说明文档。

示例

分发包	用户创建命令	最少的群组/权限集
Ubuntu/Debian/Astra/Atlant	`useradd "$1" --shell /bin/bash --create-home --password "$(openssl passwd -1 "$2")"`	`usermod -aG sudo,root "$1"` 添加到 `sudo` 群组可让用户在没有密码的情况下执行 `sudo`。

此外还建议保护用户主目录和所有嵌套目录，以便只有用户可以访问它们。其他用户和用户组不得拥有对主目录的访问权限。

示例

在此示例中，`example_user`用户的文档目录位于`~/Documents`。默认情况下（通过`useradd/adduser`和`umask 022`命令创建用户时），目录的权限为`755`。为确保只有该用户才能访问根文件夹和所有子文件夹，`umask`已更改为`077`，权限已明确设置为`700`。下面是一个命令示例，可用于验证权限是否已正确设置（只有所有者有访问权限）。

```
要显示目录的权限、所有者和群组：
stat -c "%A %U %G" /home/example_user/Documents
如果权限授予正确，则预期命令输出如下：
drwx------ example_user example_user
如果权限不符合要求，请将根目录及其所有子目录的权限设置为700：
chmod -R 700 /home/example_user/Documents
请确保所有者是正确的用户：
chown -R example_user:example_user /home/example_user/Documents
```

建议不要授予用户主目录中 .ssh、.kube、.config 和 .kdt 目录以及这些目录中包含的所有文件的执行权限。

示例

显示最敏感目录的权限—显示每个指定目录的模式、所有者和路径：

```
find ~/Documents -type d \( -name .ssh -o -name .kube -o -name .config -o -name .kdt \) \

-exec stat -c "%A %U %G %n" {} \;
```

预期命令输出：

```
drwx------ example_user example_user /home/example_user/Documents/.ssh

drwx------ example_user example_user /home/example_user/Documents/.kube

drwx------ example_user example_user /home/example_user/Documents/.config

drwx------ example_user example_user /home/example_user/Documents/.kdt
```

`drwx------`表示权限`700`：只有所有者才能读取、写入和执行（对于目录，“执行”是指进入目录的权限，而不是运行软件的权限）。

如果检测到额外的执行位，请将其从文件中删除：

```
find ~/Documents -type f \( -path "*/.ssh/*" -o -path "*/.kube/*" -o -path "*/.config/*"
-o -path "*/.kdt/*" \) -exec chmod a-x {} \;
```

如果需要，请设置更严格的权限（例如，`600`）：

```
find ~/Documents -type f \( -path "*/.ssh/*" -o -path "*/.kube/*" -o -path "*/.config/*"
-o -path "*/.kdt/*" \) -exec chmod 600 {} \;
```

操作系统的包管理

建议使用 KDT 和 Kaspersky Next XDR Expert 正常运行所需的最少应用程序集。例如，您不需要使用图形用户界面在 Kubernetes 集群中进行操作，因此建议不要安装图形软件包。如果已经安装了软件包，建议删除这些包，包括 Xorg 或 Wayland 等图形服务器。

建议定期为系统软件和 Linux 内核安装安全更新。此外还建议启用自动更新，如下所示：

- 对于使用atp软件包管理器的操作系统：

```
/etc/apt/apt.conf.d/50unattended-upgrades
```

```
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}-security";
    "${distro_id}ESMApps:${distro_codename}-apps-security";
    "${distro_id}ESM:${distro_codename}-infra-security";
};
```

- 对于使用 rpm、dnf 和 yum 软件包管理器的操作系统：

```
/etc/dnf/automatic.conf
```

```
[commands]
#  要执行何种类型的升级：
# default                            = 所有可用升级
# security                           = 仅安全升级
upgrade_type = default
# 当更新可用时是否应下载更新，由
# dnf-automatic.timer 控制。notifyonly.timer、download.timer 和
# install.timer 会覆盖此设置。
download_updates = yes
# 当更新可用时是否应应用更新，由
# dnf-automatic.timer 控制。notifyonly.timer、download.timer 和
# install.timer 会覆盖此设置。
apply_updates = no
```

操作系统安全设置

可以在 `/etc/sysctl.conf` 文件中或使用 `sysctl` 命令启用 Linux 内核安全设置。建议使用的 Linux 内核安全设置列在 `/etc/sysctl.conf` 文件片段中：

```
/etc/sysctl.conf
```

```
# 禁用 execshield
kernel.randomize_va_space=2
# 启用 IP 欺骗保护
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
# 忽略广播网络请求
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_responses=1
# 启用网络欺骗包的日志记录
net.ipv4.conf.all.log_martians=1
# 隐藏内核指针
kernel.kptr_restrict=1
# 限制对内核日志的访问
kernel.dmesg_restrict = 1
# 禁止非特权用户进行内核性能分析
kernel.perf_event_paranoid=3
# 增加 ASLR 熵位
```

```
vm.mmap_rnd_bits=32
vm.mmap_rnd_compat_bits=16
```

建议限制对 PID 的访问。这将降低一个用户跟踪另一个用户进程的可能性。例如，您可以在挂载 `/proc` 文件系统时，通过将以下行添加到 `/etc/fstab` 文件来限制对 PID 的访问：

```
proc /proc proc nosuid,nodev,noexec,hidepid=2,gid=proc 0 0
```

如果操作系统进程通过使用 `systemd` 系统进行管理，`systemd-logind` 服务仍然可以监控其他用户的进程。为了使用户会话在 `systemd` 系统中正常工作，您需要创建 `/etc/systemd/system/systemd-logind.service.d/hidepid.conf` 文件，然后向其中添加以下行：

```
[Service]
SupplementaryGroups=proc
```

> 由于某些系统可能没有 `proc` 组，建议提前添加 `proc` 组。

建议使用 `systemctl mask ctrl-alt-del.target` 命令关闭 **`ctrl`**+**`alt`**+**`del`** 组合键，以防止操作系统意外重启。

建议禁止特权用户（根用户）通过身份验证来建立远程用户连接。

示例

以下是一组同时阻止root通过网络登录并将其排除在LDAP身份验证之外的命令。

```
# 1&period; SSH

sudo sed -i 's/^#\?PermitRootLogin .*/PermitRootLogin no/' /etc/ssh/sshd_config

sudo systemctl restart sshd

# 2&period; Local account

sudo passwd -l root

sudo usermod -s /usr/sbin/nologin root

# 3&period; Example of LDAP bind, the file path may differ

LDAP_CONF="/etc/ksc/ldap_connection.json"

if [ -f "$LDAP_CONF" ]; then

sudo jq '.ldap.bindDn = "cn=admin,dc=example,dc=com"' "$LDAP_CONF" | sudo tee
"$LDAP_CONF" > /dev/null

sudo systemctl restart ksc-orchestrator

fi

# 4&period; Sudo without NOPASSWD
```

```
sudo sed -i '/^root.*NOPASSWD/d' /etc/sudoers
```

建议使用防火墙来限制网络活动。有关所用端口和协议的更多信息，请参阅“Kaspersky Next XDR Expert 使用的端口”。

示例

操作	ufw (Ubuntu/Debian)	firewalld (RHEL/CentOS)	iptables
检查状态	ufw status	firewall-cmd --list-all	iptables -L -n
检查端口	ss -tuln | grep 443	ss -tuln | grep 443	ss -tuln | grep 443
外部审计	nc -zv IP 443	nc -zv IP 443	nc -zv IP 443
打开端口	ufw allow 443/tcp	firewall-cmd --add-port=443/tcp --permanent + --reload	iptables -A INPUT -p tcp --dport 443 -j ACCEPT
关闭端口	ufw deny 443/tcp	firewall-cmd --remove-port=443/tcp --permanent + --reload	iptables -A INPUT -p tcp --dport 443 -j DROP
保存规则	Auto	Auto	iptables-save > /etc/iptables/rules.v4

建议启用`auditd`，以简化安全事故的调查。有关启用遥测重定向的更多信息，请参阅 Auditd 事件接收设置。

建议定期备份以下配置和数据目录：

- 管理主机：`~/kdt`
- 目标主机：`/etc/k0s/`、`/var/lib/k0s`

建议对这些备份进行加密。

各种操作系统和 DBMS 的强化指南

如果您需要配置操作系统和软件的安全设置，可以参阅“互联网安全中心 (CIS) 提供的建议”。

如果您使用的是 Astra Linux 操作系统，请参阅适用于您的 Astra Linux 版本的安全建议。

如果您需要配置 PostgreSQL 的安全设置，请使用官方 PostgreSQL 文档中的服务器管理建议。

连接安全

严格的 TLS 设置

建议使用 1.2 及以后版本的 TLS 协议，限制或禁止不安全的加密算法。

您可以配置管理服务器使用的加密协议 (TLS)。请注意，在发布 Kaspersky Next XDR Expert 版本时，默认已配置加密协议设置以确保安全的数据传输。

限制对 Kaspersky Next XDR Expert 数据库的访问

建议限制对 Kaspersky Next XDR Expert 数据库的访问。例如，仅对部署了 Kaspersky Next XDR Expert 的设备授予访问权限。这可降低 Kaspersky Next XDR Expert 数据库因已知漏洞而受到损害的可能性。

您可以根据使用的数据库的操作说明配置参数，也可以在防火墙上提供关闭的端口。

账户和身份验证

使用 Kaspersky Next XDR Expert 的两步验证

Kaspersky Next XDR Expert 提供基于 RFC 6238 标准（基于时间的一次性密码 (TOTP) 算法）的用户**双重身份验证**。

为您自己的账户启用双重身份验证后，每次通过浏览器登录 Kaspersky Next XDR Expert 时，您都需要输入用户名、密码和额外的一次性安全码。要接收一次性安全码，您的计算机或移动设备上必须安装认证应用。

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

我们强烈建议不要在与 Kaspersky Next XDR Expert 建立连接的同一台设备上安装认证应用。您可以在移动设备上安装认证应用。

对操作系统使用双重身份验证

我们建议在部署了 Kaspersky Next XDR Expert 的设备上使用多重身份验证 (MFA)，例如使用令牌、智能卡或其他方法（如果可能）。

禁止保存管理员密码

如果您通过浏览器使用 Kaspersky Next XDR Expert，我们不建议在用户设备上安装的浏览器中保存管理员密码。

内部用户账户的身份验证

默认情况下，Kaspersky Next XDR Expert 内部用户账户的密码必须遵守以下规则：

- 密码长度必须为10到256个字符。

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

默认下，允许的最大密码输入尝试次数是 3。此数值是固定的，无法更改。

用户可以在有限次数内输入无效的密码。达到限制后，用户账户被锁定一小时。

限制分配主管理员角色

该用户在 Kaspersky Next XDR Expert 的访问控制列表 (ACL) 中被分配了主管理员角色。我们不建议将主管理员角色分配给大量用户。

配置对应用程序功能的访问权限

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

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

基于角色的访问控制模型的主要优点：

- 易于管理
- 角色层级
- 最小特权方法
- 职责分离

您可以根据职位为某些员工分配内置角色，或创建全新的角色。

配置角色时，请注意与 Kaspersky Next XDR Expert 设备保护状态更改以及第三方软件远程安装相关的权限：

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

使用单独的账户进行远程安装应用程序

除了对访问权限进行基本区分之外，我们建议限制所有账户（主管理员或其他专用账户除外）远程安装应用程序。

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

定期审核所有用户和用户的操作

我们建议对部署了 Kaspersky Next XDR Expert 的设备上的所有用户进行定期审核。这使您能够应对与设备可能遭受损害相关的某些类型的安全威胁。

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

管理 Kaspersky Next XDR Expert 的保护

选择 Kaspersky Next XDR Expert 的保护软件

根据 Kaspersky Next XDR Expert 的部署类型和常规保护策略，选择应用程序来保护部署了 Kaspersky Next XDR Expert 的设备和管理员主机。

如果您在专用设备上部署了 Kaspersky Next XDR Expert，我们建议选择 Kaspersky Endpoint Security 应用程序来保护部署了 Kaspersky Next XDR Expert 的设备和管理员主机。这可让您应用所有可用技术来保护这些设备，包括行为分析模块。

如果 Kaspersky Next XDR Expert 部署在基础设施中存在的设备上并且之前曾用于其他任务，我们建议考虑以下保护软件：

- Kaspersky Industrial CyberSecurity for Nodes。我们建议在包含在工业网络中的设备上安装此应用程序。Kaspersky Industrial CyberSecurity for Nodes 是一个应用程序，具有与各种工业软件制造商的兼容性证书。
- 推荐的安全应用程序。如果 Kaspersky Next XDR Expert 安装在装有其他软件的设备上，我们建议考虑该软件供应商关于安全应用程序兼容性的建议（可能已有选择安全解决方案的建议，您可能需要配置受信任区域）。

保护模块

如果与 Kaspersky Next XDR Expert 安装在相同设备上的第三方软件的供应商没有特别建议，我们建议激活并配置所有可用的保护模块（在检查这些保护模块的运行一段时间后）。

为装有 Kaspersky Next XDR Expert 的设备配置防火墙

在部署了 Kaspersky Next XDR Expert 的设备上，我们建议配置防火墙，以限制管理员通过浏览器连接到 Kaspersky Next XDR Expert 的设备数量。

默认情况下，

Kaspersky Next XDR Expert 使用端口 443 通过浏览器登录。我们建议限制可以使用该端口管理 Kaspersky Next XDR Expert 的设备数量。

管理客户端设备保护

限制将授权许可密钥添加到安装包

安装包可以通过包含在 Kaspersky Next XDR Expert 中的 Web 服务器发布。如果您将授权许可密钥添加到在 Web 服务器中发布的安装包，则所有用户都可以读取该授权许可密钥。

为避免泄露授权许可密钥，我们不建议将授权许可密钥添加到安装包中。

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

在管理组之间移动设备的自动规则

我们建议限制使用自动规则在管理组之间移动设备。

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

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

此建议不适用于将设备一次性初始分配给管理组。

分发点和连接网关的安全要求

安装了网络代理的设备可以充当分发点并执行以下功能：

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

在组织的网络上放置分发点用于：

- 减少 Kaspersky Next XDR Expert 的负载
- 流量优化
- 让 Kaspersky Next XDR Expert 能够访问网络中难以到达的设备

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

限制自动分配分发点

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

对于工业网络和小型网络，您可以手动分配设备作为分发点。

您还可以查看分发点活动报告。

事件传输到第三方系统

本部分介绍了将客户端设备上发现的安全问题传输到第三方系统的具体方法。

监控和报告

为了及时响应安全问题，我们建议配置监控和报告功能。

导出事件到 SIEM 系统

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

审计事件的电子邮件通知

为了及时响应紧急情况，我们建议配置管理服务器以发送有关其发布的审计事件、关键事件、故障事件和警告的通知。

由于这些事件是系统内事件，因此可以预期它们的数量很少，这非常适用于邮件。

配置受管理应用程序的保护

受管理应用程序策略

我们建议为所使用的每类应用程序和 Kaspersky Next XDR Expert 的所有组件（网络代理、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Agent 等）创建一个策略。此组策略必须应用于所有受管理设备（根管理组）或根据配置的移动规则新的受管理设备将自动移动到其中的单独组。

指定用于禁用保护和卸载应用程序的密码

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

使用卡巴斯基安全网络

不允许使用 KSN，因为这会导致应用程序失去认证状态。

定期扫描受管理设备

对于所有设备组，我们建议创建一个定期运行完整设备扫描的任务。

发现新设备

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

出于安全目的，您可以使用包含所有新设备的默认管理组和影响该组的默认策略。

部署方案

部署Kaspersky Next XDR Expert（包括Kaspersky Endpoint Detection and Response功能）有两种选择：在Kubernetes集群内进行多节点或单节点部署。在开始之前，建议您先了解可用的部署方案，然后选择最符合您组织要求的方案。您还可以参考容量大小指南，其中概述了硬件要求，并根据您企业中的设备数量推荐部署选项。

根据您选择的部署选项，Kaspersky Next XDR Expert可能需要以下主机才能正常运行：

- **管理员设备**

  管理员主机是用于部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert 的物理机或虚拟机。由于 KDT 在管理员主机上运行，因此该主机必须满足 KDT 的要求。

  如果管理员主机不包含在集群中，它将仅用于部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert。如果管理员主机包含在集群中，它还将充当用于运行 Kaspersky Next XDR Expert 组件的目标主机。在这种情况下，主机必须满足目标主机的要求。

- **目标主机**

  目标主机是用于部署Kaspersky Next XDR Expert的物理机或虚拟机。将使用以下目标主机：

  - 用于在集群内部安装 Kaspersky Next XDR Expert 组件的目标主机

    包含在 Kubernetes 集群中且工作负载分布在其中的各主机。目标主机必须满足所选部署方案（多节点部署或单节点部署）的要求。

    KUMA 服务（收集器、关联器和存储）可以完全安装在集群内，完全安装在集群外的单独主机上，或者部分安装在 Kubernetes 集群内，部分安装在 Kubernetes 集群外。此种情况下，主机必须满足安装 KUMA 服务所需的硬件、软件和安装要求。

    您可以将其中一个目标主机用作管理员主机来运行 Kaspersky Next XDR Expert 部署。在这种情况下，该主机还必须满足 KDT 的要求。

  - 用于安装 KUMA 服务的 KUMA 目标主机（可选）

    KUMA 服务（收集器、关联器和存储）可以安装在集群外部独立主机的目标主机上。KUMA目标主机的数量取决于Kaspersky Next XDR Expert需要处理的事件数量。

    KUMA目标主机必须满足安装KUMA服务所需的硬件、软件和安装要求。

- **DBMS主机（仅限多节点部署）。**

  用于安装DBMS的主机位于Kubernetes集群之外的独立服务器。此主机必须满足数据库节点的要求。

多节点部署

在多节点部署中，Kaspersky Next XDR Expert组件安装在Kubernetes集群中的多个工作线程节点上。如果一个节点发生故障，集群可以在另一个节点上恢复组件运行。

在此配置中，您至少需要五台主机：

- 一台主机，用于DBMS
- 四台目标主机，用于Kubernetes集群和Kaspersky Next XDR Expert组件：
  - 一台主机同时充当管理员主机和目标主机
  - 三台目标主机

  若想使用位于集群之外的管理员主机，则需要额外分配一台主机用于部署。

  要在集群之外安装KUMA服务，您必须额外分配至少一台KUMA目标主机。

单节点部署

在单节点部署环境中，所有Kaspersky Next XDR Expert组件都安装在Kubernetes集群内的单个节点上。此选项适用于计算资源需求较低的解决方案。

在此配置中，至少需要一台目标主机来安装Kubernetes集群、Kaspersky Next XDR Expert组件和DBMS。该主机同时充当管理员主机和目标主机。若要使用位于集群外部的管理员主机，则必须额外分配一台主机用于部署。

若要在集群外部安装KUMA服务，必须额外分配至少一台KUMA目标主机。

在此配置中，DBMS不需要单独的节点。但是，在部署Kaspersky Next XDR Expert之前，应将其手动安装在目标主机上。

部署单节点的层次结构

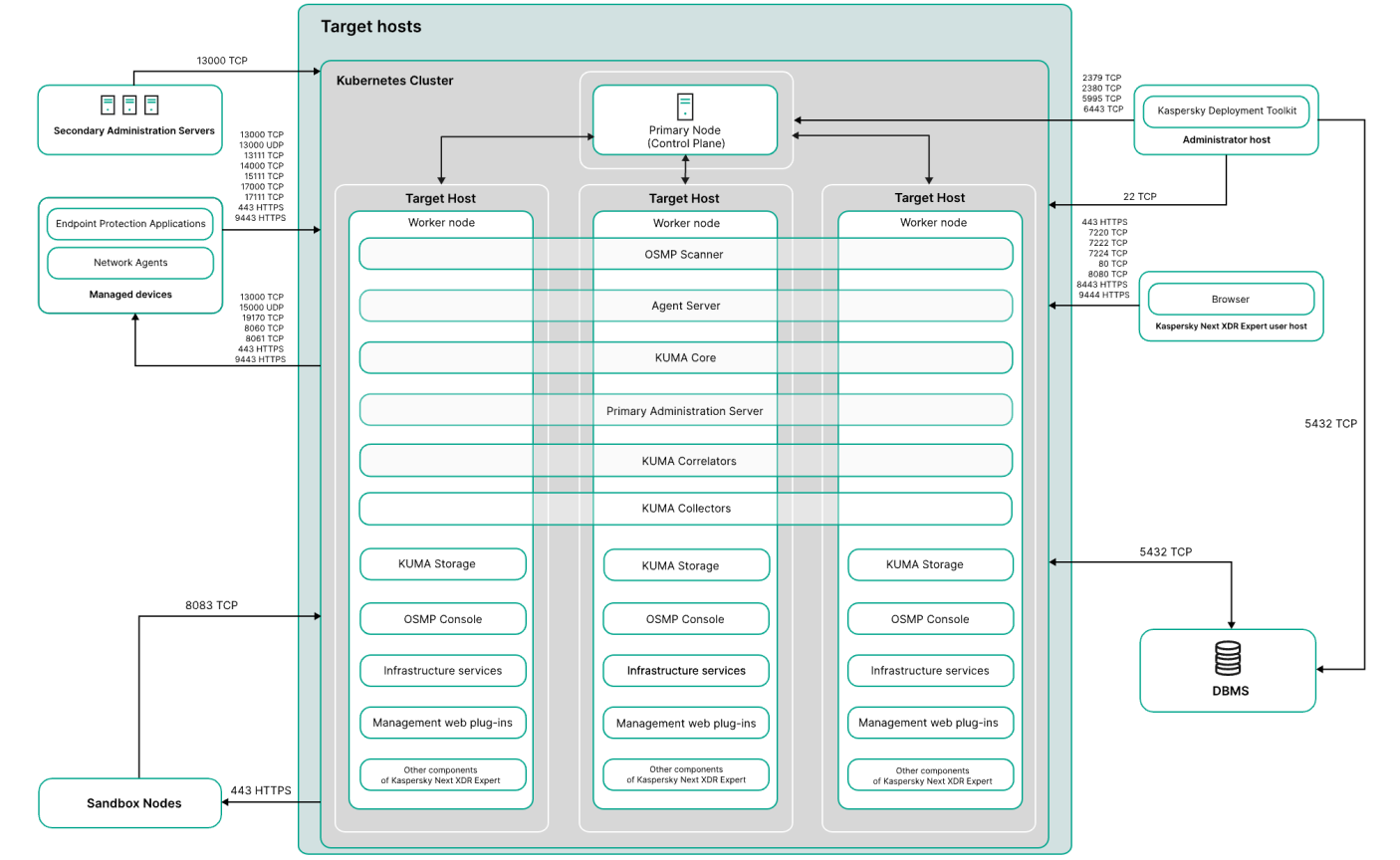
在分层部署中，会部署多个单节点。所有单节点部署完成后，系统会选择一个节点作为父实例。通常，性能最强的节点会根据计算结果成为父实例。然后，其余节点会连接到父实例。

如果您在计算部署所需资源方面需要帮助，请联系技术支持。

多节点部署方案

下图展示了 Kaspersky Next XDR Expert 的多节点部署方案。

在该方案中，Kaspersky Next XDR Expert 组件在工作节点之间的分布仅作为示例显示。实际的组件分布可能有所不同。



Kaspersky Next XDR Expert 的多节点部署方案

Kaspersky Next XDR Expert 的多节点部署方案包含以下主要组件：

- **管理员主机**。在此主机上，管理员使用Kaspersky Deployment Toolkit来部署和管理Kubernetes集群和Kaspersky Next XDR Expert。管理员主机可以位于Kubernetes集群外部，也可以位于集群内部。如果管理员主机包含在集群中，它还将充当用于运行Kaspersky Next XDR Expert组件的目标主机。

- **DBMS 服务器**。Kaspersky Next XDR Expert 组件要正常运行，需要一台已安装数据库管理系统的服务器。DBMS 服务器不包含在 Kubernetes 集群中。管理员在 Kubernetes 集群之外的独立服务器上手动安装 DBMS。

- **Kubernetes 集群**。Kubernetes集群包括控制节点（在部署过程中也称为主节点）和至少三个工作线程节点。主节点和工作线程节点的数量可能会有所不同。所有Kaspersky Next XDR Expert组件都部署在工作线程节点上：

  - **主管理服务器**。客户端组织端点保护的关键组件。管理服务器通过EPP应用程序提供端点防护的集中部署和管理，并允许您监控端点防护状态。

    此组件部署在其中一个工作线程节点上，不具有节点亲和性。Kubernetes调度器会根据可用资源选择工作线程节点。

  - **OSMP扫描器**。该组件使用反恶意软件引擎、YARA和沙盒扫描文件、发送文件进行分析并生成报告。

    此组件部署在其中一个工作线程节点上，不具有节点亲和性。Kubernetes调度器会根据可用资源选择工作线程节点。

  - **代理程序服务器**。此组件负责OSMP和端点代理程序之间的交互。

    此组件部署在其中一个工作线程节点上，不具有节点亲和性。Kubernetes调度器会根据可用资源选择工作线程节点。

  - KUMA Core。SIEM组件的核心组成部分，是所有其他服务和组件的基础。

    此组件部署在其中一个工作线程节点上，不具有节点亲和性。Kubernetes调度器会根据可用资源选择工作线程节点。

  - **OSMP控制台**。此组件为OSMP提供网页界面。

    此组件部署在所有集群节点上。

  - **管理网页插件**。该组件用于通过OSMP控制台远程管理卡巴斯基软件。

    这些组件部署在所有集群节点上。

  - **Kaspersky Next XDR Expert的基础设施服务和其他组件**。其他组件，可提供集中式资产管理、数据交换、层级构建、身份验证和授权；以及其他功能，例如操作审计、安全政策管理和更新分发。这些组件部署在所有集群节点上。

- **KUMA服务**。KUMA服务（收集器、关联器和存储）可以完全安装在集群内的工作线程节点上，完全安装在Kubernetes集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。KUMA服务的目标主机数量可能有所不同。KUMA服务由管理员手动创建。

  在该方案中，KUMA服务完全安装在集群内的工作线程节点上。在这种情况下，KUMA收集器和KUMA关联器由管理员手动创建，并且默认情况下，在没有节点亲和性的情况下部署。在每个节点上手动创建多个KUMA存储。

- **Kaspersky Next XDR Expert 用户主机**。用于登录OSMP控制台的用户设备。

- **从属管理服务器**（可选）。辅助管理服务器用于创建服务器层次结构，并用于与端点代理城市的进一步集成。

- **受管理设备**。受 Kaspersky Next XDR Expert 保护的客户端设备。每个受管理设备都安装了网络代理程序和EPP应用程序。

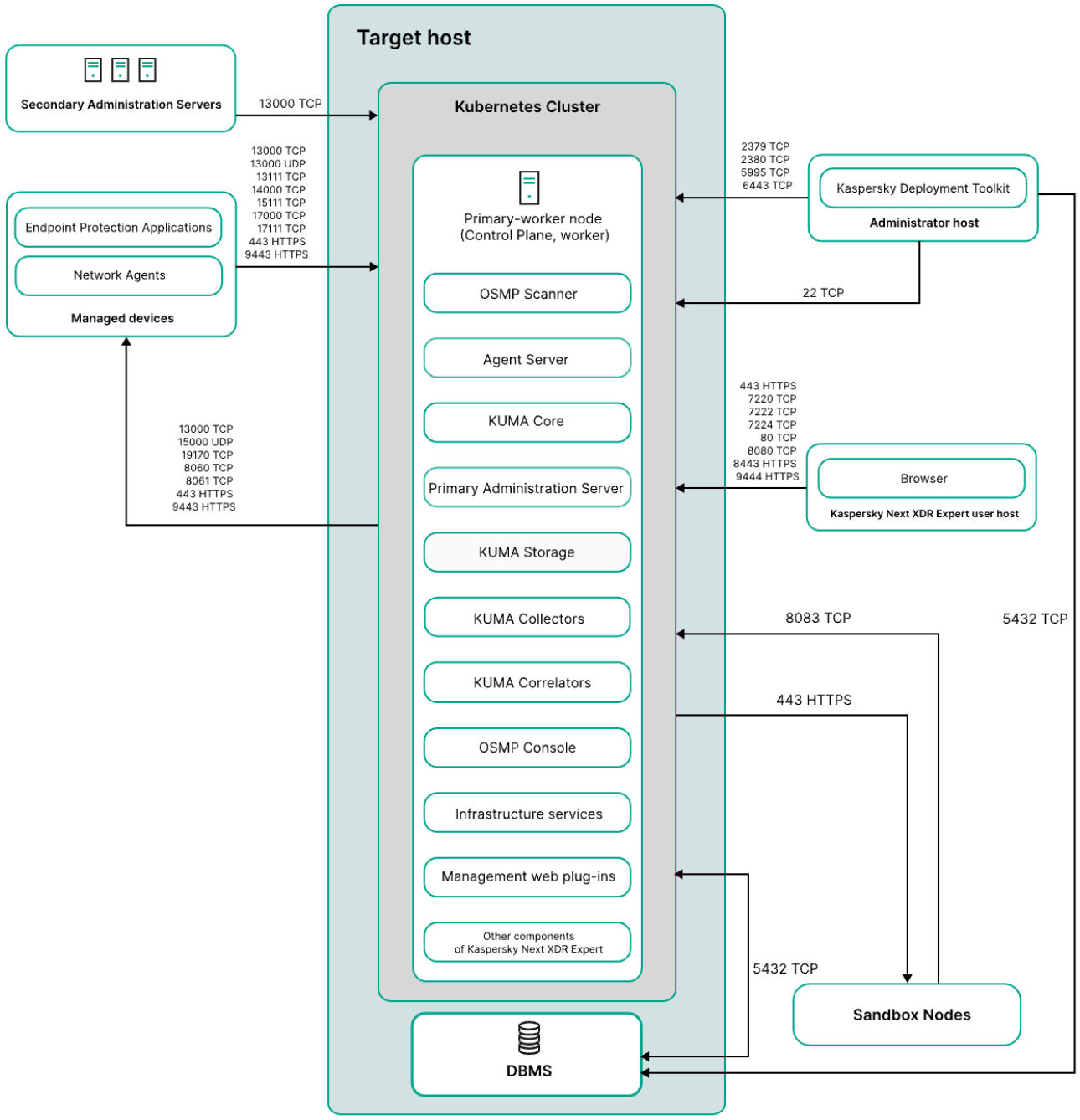
- **沙盒节点**。沙盒节点可以包含一个或多个运行沙盒组件实例的服务器。一种用于托管隔离执行环境和辅助服务的专用计算资源。此节点负责分析和处理进入受保护系统的文件、链接、URL和其他对象。沙盒节点独立于Kubernetes集群运行。

  沙盒服务器的数量可能因工作负载而异。管理员在每台服务器上手动安装沙盒。

该方案不提供成功部署所需的所有端口。有关端口的完整列表，请参阅Kaspersky Next XDR Expert使用的端口。

单节点部署方案

下图展示了 Kaspersky Next XDR Expert 的单节点部署方案。



Kaspersky Next XDR Expert 的单节点部署方案

Kaspersky Next XDR Expert 的单节点部署方案包含以下主要组件：

- **管理员主机**。在此主机上，管理员使用Kaspersky Deployment Toolkit来部署和管理Kubernetes集群和Kaspersky Next XDR Expert。管理员主机可以位于Kubernetes集群外部，也可以位于集群内部。如果管理员主机包含在集群中，它还将充当用于运行Kaspersky Next XDR Expert组件的目标主机。

- **DBMS 服务器**。Kaspersky Next XDR Expert 组件要正常运行，需要一台已安装数据库管理系统的服务器。DBMS 服务器不包含在 Kubernetes 集群中。管理员在部署 Kaspersky Next XDR Expert 之前，在将充当主工作节点的目标主机上手动安装 DBMS。

- **Kubernetes 集群**。Kubernetes集群包括同时充当控制平面节点（在部署过程中也称为主节点）和工作线程节点的目标主机。所有Kaspersky Next XDR Expert组件都部署在此主要工作线程节点上：

  - **主管理服务器**。客户端组织端点保护的关键组件。管理服务器通过EPP应用程序提供端点防护的集中部署和管理，并允许您监控端点防护状态。

  - **OSMP扫描器**。该组件使用反恶意软件引擎、YARA和沙盒扫描文件、发送文件进行分析并生成报告。

  - **代理程序服务器**。此组件负责OSMP和端点代理程序之间的交互。

  - KUMA Core。SIEM组件的核心组成部分，是所有其他服务和组件的基础。

  - **OSMP控制台**。此组件为OSMP提供网页界面。

  - **管理网页插件**。该组件用于通过OSMP控制台远程管理卡巴斯基软件。

  - **Kaspersky Next XDR Expert的基础设施服务和其他组件**。其他组件，可提供集中式资产管理、数据交换、层级构建、身份验证和授权；以及其他功能，例如操作审计、安全政策管理和更新分发。

- **KUMA服务**。KUMA服务（收集器、关联器和存储）可以完全安装在集群内的工作线程节点上，完全安装在Kubernetes集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。KUMA服务的目标主机数量可能有所不同。KUMA服务由管理员手动创建。在该方案中，KUMA服务完全安装在集群内的工作线程节点上。

- **Kaspersky Next XDR Expert 用户主机**。用于登录OSMP控制台的用户设备。

- **从属管理服务器**（可选）。辅助管理服务器用于创建服务器层次结构，并用于与端点代理城市的进一步集成。

- **受管理设备**。受 Kaspersky Next XDR Expert 保护的客户端设备。每个受管理设备都安装了网络代理程序和EPP应用程序。

- **沙盒节点**。沙盒节点可以包含一个或多个运行沙盒组件实例的服务器。一种用于托管隔离执行环境和辅助服务的专用计算资源。此节点负责分析和处理进入受保护系统的文件、链接、URL和其他对象。沙盒节点独立于Kubernetes集群运行。

  沙盒服务器的数量可能因工作负载而异。管理员在每台服务器上手动安装沙盒。

该方案不提供成功部署所需的所有端口。有关端口的完整列表，请参阅Kaspersky Next XDR Expert使用的端口。

Kaspersky Next XDR Expert 使用的端口

为了使管理员主机和目标主机之间正确交互，必须通过下表所列端口，提供从管理员主机到目标主机的连接访问权限。这些端口无法更改。

为了使管理员主机与用于安装 KUMA 服务且位于 Kubernetes 集群之外的主机进行交互，必须仅通过 TCP 22 端口提供访问权限。

用于管理员主机和目标主机之间交互的端口

端口	协议	方向	来源	目标	端口目的
22	TCP	入站	管理员设备	目标主机	提供从管理员主机到目标主机的 SSH 连接。 提供从管理员主机到用于安装外部 KUMA 服务的主机的 SSH 连接。
2379、2380	TCP	入站	管理员设备	目标主机（主节点）	连接到 Kubernetes 存储 (ETCD)。
5995	TCP	入站	管理员设备	目标主机（主节点）	连接到 Docker 注册表。
6443	TCP	入站	管理员设备	目标主机（主节点）	连接到 Kubernetes API。

为确保 Kaspersky Next XDR Expert 组件正常运行，目标主机必须位于同一广播域中。

下表列出了集群中所有目标主机的防火墙上必须打开的端口。这些端口无法更改。

如果您在目标主机上使用 firewalld 或 UFW 防火墙，KDT 会自动在防火墙上打开所需的端口。否则，您可以在部署 Kaspersky Next XDR Expert 之前手动打开列出的端口。

Kaspersky Next XDR Expert 组件使用的必需端口

端口	协议	方向	来源	目标	端口目的
80、8080	TCP (HTTP)	入站	浏览器	集群目标主机	从浏览器接收连接。重定向到 443 TCP (HTTPS) 端口。
443、8443	TCP (HTTPS)	入站	浏览器	集群目标主机	从浏览器接收连接。 通过 OpenAPI™ 接收与管理服务器的连接。用于实现与管理服务器交互场景的自动化。
13000	TCP	入站	网络代理或从属管理服务器	集群目标主机	接收来自网络代理和从属管理服务器的连接。
13000	UDP	入站	网络代理	集群目标主机	接收从网络代理关闭的设备的信息。
14000	TCP	入站	网络代理	集群目标主机	接收从网络代理的连接。
17000	TCP	入站	受管理设备	集群目标主机	接收从受管理设备的应用程序激活连接（除了从移动设备）。
19170	TCP (HTTPS)	出站	集群目标主机	受管理设备	使用 OSMP Console 远程访问受管理设备。
7210	TCP	入站	KUMA 目标主机	集群目标主机	从 KUMA Core 服务器接收 KUMA 配置。
7220	TCP	入站	浏览器	集群目标主机	从浏览器接收连接。
7222	TCP	入站	浏览器	集群目标主机	CyberTrace 系统中的反向代理。
7224	TCP	入站	浏览器	集群目标主机	身份和访问管理器 (IAM) 的回调。
8429	TCP	入站	KUMA 代理	集群目标主机	记录 KUMA 代理性能指标。

下表包含在 Kaspersky Next XDR Expert 部署期间防火墙上默认未打开的端口。这些端口无法更改。

如果您需要执行下表“**端口用途**”列中列出的操作，则可以手动在所有目标主机的防火墙上打开相应的端口。

Kaspersky Next XDR Expert 组件使用的防火墙可选端口

端口	协议	方向	来源	目标	端口目的
8060	TCP	出站	集群目标主机	受管理设备	将发布的安装包传输到受管理设备。
8061	TCP	出站	集群目标主机	受管理设备	将发布的安装包传输到受管理设备。

端口	协议	方向	来源	目标	端口目的
8083	HTTP	入站	沙盒	集群目标主机	在沙盒中更新病毒数据库。
13111	TCP	入站	受管理设备	集群目标主机	接收受管理设备向 KSN 代理服务器发送的请求。
15111	UDP	入站	受管理设备	集群目标主机	接收受管理设备向 KSN 代理服务器发送的请求。
17111	TCP	入站	受管理设备	集群目标主机	接收受管理设备向 KSN 代理服务器发送的请求。
5432	TCP	入站	DBMS (PostgreSQL)	集群目标主机	与 DBMS (PostgreSQL) 的交互。仅当您执行演示部署并在 Kubernetes 集群内的目标主机上安装 DBMS 时才使用此端口。

下表列出了与 Sandbox 交互的主机防火墙上必须打开的端口。

用于与 Sandbox 交互的端口

端口	协议	方向	来源	目标	端口目的
22	TCP	入站	管理员设备	Sandbox 节点	通过 SSH 连接到 Sandbox 服务器。
443	TCP	入站	OSMP	Sandbox 节点上的目标组件	来自 OSMP 组件的传入连接。
8443	TCP	入站	浏览器	Sandbox 节点上的目标组件	访问 Sandbox Web 界面。
80 或 443	TCP	出站	Sandbox 节点上的目标组件	目标更新服务器	从卡巴斯基更新服务器获取更新。
任何	任何	出站和相应的入站	Sandbox 节点上的目标组件	互联网上的目标资源	访问互联网以分析已处理对象的网络行为。

下表包含必须打开才能使 Kubernetes 集群和基础架构组件正常运行的端口。这些端口无法更改。

如果您在目标主机上使用 firewalld 或 UFW 防火墙，KDT 会自动在防火墙上打开所需的端口。否则，您可以在部署 Kaspersky Next XDR Expert 之前手动打开列出的端口。

Kubernetes 集群和基础架构组件使用的端口

端口	协议	节点
80	TCP	主节点
443	TCP	主节点
10250	TCP	主节点
9443	TCP	主节点
6443	TCP	主节点
8132	TCP	主节点
5995	TCP	主节点
80	TCP	工作节点
443	TCP	工作节点
179	TCP	工作节点
10250	TCP	工作节点
10255	TCP	工作节点
9443	TCP	工作节点
6443	TCP	工作节点
9500	TCP	工作节点
9501	TCP	工作节点
9502	TCP	工作节点

端口	协议	节点
9503	TCP	工作节点
8500	TCP	工作节点
8501	TCP	工作节点
3260	TCP	工作节点
8000	TCP	工作节点
8002	TCP	工作节点
2049	TCP	工作节点
3370	TCP	工作节点
179	UDP	工作节点
51820	UDP	工作节点
51821	UDP	工作节点

为了使 Kubernetes 集群中未包含的 KUMA 服务正常运行，您必须打开下表列出的端口。下表显示了默认网络端口值。这些端口在 KUMA 安装期间自动打开。

用于与外部 KUMA 服务交互的端口

端口	协议	方向	来源	目标	端口目的
8123	HTTPS	入站	存储服务	ClickHouse 集群节点	在 ClickHouse 集群中写入和接收规范化事件。
9009	HTTPS	入站/出站	ClickHouse 群集副本	ClickHouse 群集副本	ClickHouse 集群副本之间的内部通讯，用于传输集群数据。
2181	TCP	入站	ClickHouse 集群节点	ClickHouse 管家复制协调服务	ClickHouse 服务器副本接收和写入复制元数据。
2182	TCP	入站/出站	ClickHouse 管家复制协调服务	ClickHouse 管家复制协调服务	复制协调服务之间为达成仲裁共识的内部通讯。
8001	TCP	入站	Victoria Metrics	ClickHouse 服务器	接收 ClickHouse 服务器操作指标。
9000	TCP	入站	ClickHouse 客户端	ClickHouse 集群节点	在 ClickHouse 集群中写入和接收数据。

如果在服务器上创建额外的 KUMA 服务（收集器、关联器或存储），则需要手动打开与服务器上创建的服务相对应的端口。您可以使用 TCP 端口 7221 或用于服务安装的其他端口。

如果使用开箱即用的示例服务，则在 Kaspersky Next XDR Expert 部署期间会自动打开以下端口：

- 7230 TCP
- 7231 TCP
- 7232 TCP
- 7233 TCP
- 7234 TCP
- 7235 TCP
- 7236 TCP
- 5140 TCP
- 5140 UDP

- 5141 TCP
- 5144 UDP
- 5150 UDP

更改用于连接到 OSMP 控制台服务器的端口

默认情况下，当管理员通过浏览器连接到 OSMP 控制台服务器，以及 Endpoint Agent 连接到 agentserver 组件时，二者使用相同的节点和相同的端口 (443)，但各自使用不同的 FQDN。如有必要，可以在安装 Kaspersky Next XDR Expert 期间，或在解决方案已安装后，为这些组件配置两个不同的端口。

要更改所需端口，您必须有权访问 KDT 实用程序所在的管理员主机。

更改 OSMP 控制台端口的过程存在以下限制：

- 如果将端口号指定为无效值（超出范围、包含无效字符或值为空），解决方案安装将失败。
- 更改端口后，连接到 OSMP 控制台时，务必在浏览器的地址栏中指定新的端口号。

要在 Kaspersky Next XDR Expert 已安装的情况下更改 OSMP 控制台端口：

1. 选择 1–65535 范围内的新端口号。
2. 如果使用防火墙或其他网络访问限制工具，请配置这些工具以确保所选端口可访问。
3. 运行以下命令以更改端口：

   ```
   ./kdt invoke foreach -a setConsolePort --param console_port="<port_number>"
   ```

   其中，使用您选择的端口号替换 `<port_number>`。

   如果命令成功完成，当前 OSMP 控制台连接会话将被终止。
4. 重新连接到 OSMP 控制台服务器。为此，请在浏览器的地址栏中输入 配置文件 中指定的 Web Console 服务 FQDN 以及新的端口号。

用于连接到 OSMP 控制台的端口已更改。默认端口 443 不再接受与 OSMP 控制台的连接。

要在安装 Kaspersky Next XDR Expert 期间更改 OSMP 控制台端口：

1. 选择 1–65535 范围内的新端口号。
2. 在配置文件中指定新的端口号。

   为此，请在配置文件中添加用于新 OSMP 控制台端口的安装参数，然后按如下方式指定所选端口号：

   ```
   parameters:
     - name: console_port
       source:
         value: "<port_number>"
   ```

其中：

- `console_port` 指定新的端口号。
- `<port_number>` 替换为您已选择的端口号。

3. 如果使用防火墙或其他网络访问限制工具，请配置这些工具以确保所选端口可访问。
4. 安装 Kaspersky Next XDR Expert。
   有关详细信息，请参阅部署 Kaspersky Next XDR Expert部分。
5. 成功安装后，连接到 OSMP 控制台服务器。
   为此，请在浏览器的地址栏中输入 Web Console 服务的 FQDN 以及配置文件中指定的新端口号。

用于连接到 OSMP 控制台的端口已更改。默认端口 (443) 不再用于连接到 OSMP 控制台。

更改 Endpoint Agent 用于连接到 agentserver 组件的端口

默认情况下，当管理员通过浏览器连接到 OSMP 控制台服务器，以及 Endpoint Agent 连接到 agentserver 组件时，二者使用相同的节点和相同的端口 (443)，但各自使用不同的 FQDN。如有必要，可以在安装 Kaspersky Next XDR Expert 期间，或在解决方案已安装后，为这些组件配置两个不同的端口。

> 要更改所需端口，您必须能够访问 KDT 实用程序所在的管理员主机，并且具有修改 Endpoint Agent 策略的权限。

更改 Endpoint Agent 所用端口的过程存在一项限制。如果将端口号指定为无效值（超出范围、包含无效字符或值为空），则在第一种操作流程中，更改端口的命令会执行失败。在第二种操作流程中，解决方案安装会失败。

要在 Kaspersky Next XDR Expert 安装后更改 Endpoint Agent 使用的端口：

1. 选择 1–65535 范围内的新端口号。
2. 如果使用防火墙或其他网络访问限制工具，请配置这些工具以确保所选端口可访问。
3. 运行以下命令，以更改 Endpoint Agent 用于连接到 agentserver 组件的端口（第一个命令）以及用于发送遥测数据的端口（第二个命令）：

   ```
   ./kdt invoke foreach -a changeAgentServerSmpPort --param as_smp_port="<port_number>"
   ./kdt invoke foreach -a setKumaTelemetryPort --param kuma_gateway_telemetry_listener_port="<port_number>"
   ```

   其中，使用您选择的端口号替换 `<port_number>`。
   如果这些命令成功完成，Endpoint Agent 与 agentserver 组件之间的当前连接会话将终止。agentserver 组件不再接收来自 Endpoint Agent 的数据。
4. 如果来自 Endpoint Agent 的数据通过代理节点路由，请执行以下操作：
   a. 在 Nginx 配置文件中，在字符串 `listen <port_number> ssl http2;` 中指定新的端口号
   b. 运行命令 `nginx -s reload` 以重启 Nginx 并应用配置文件中的更改。
5. 在 OSMP Console 的主菜单中，转到 **资产管理** → **策略**。

6. 在列表中单击所需的端点安全应用程序策略，然后转到“**应用程序设置** → **内置代理配置** → **Endpoint Detection and Response Expert (on-premises)** → **连接到响应服务器**”。

7. 在 **连接设置** 下，选中服务器旁边的复选框，然后单击 **删除** 按钮。
   使用旧端口的所需服务器已删除。

8. 单击窗格中的 **添加** 按钮，然后单击 **选择服务器** 按钮。

9. 在打开的窗口中，选择使用新端口的服务器，然后确认操作。

Endpoint Agent 用于连接到 agentserver 组件的端口已更改。agentserver 组件开始使用新端口接收来自 Endpoint Agent 的数据。策略应用到 Endpoint Agent 后，Endpoint Agent 将通过新端口重新连接到 OSMP 组件。默认端口 (443) 不再用于连接到 agentserver 组件。

要在安装 Kaspersky Next XDR Expert 时更改 Endpoint Agent 使用的端口：

1. 选择 1–65535 范围内的新端口号。

2. 在配置文件中，指定 Endpoint Agent 用于连接到 agentserver 组件的新端口以及用于发送遥测数据的端口。
   为此，请在配置文件中添加新端口的安装参数，如下所示：

```
parameters:
- name: as_smp_port
  source:
    value: "<port_number>"
- name: kuma_gateway_telemetry_listener_port
  source:
    value: "<port_number>"
```

   其中：

   - `as_smp_port` 指定 Endpoint Agent 使用的新端口号。
   - `kuma_gateway_telemetry_listener_port` 指定用于发送遥测数据的新端口号。
   - `<port_number>` 替换为您已选择的端口号。

3. 如果使用防火墙或其他网络访问限制工具，请配置这些工具以确保所选端口可访问。

4. 安装 Kaspersky Next XDR Expert。
   有关详细信息，请参阅部署 Kaspersky Next XDR Expert部分。

5. 如果来自 Endpoint Agent 的数据通过代理节点路由，请执行以下操作：

   a. 在 Nginx 配置文件中，在字符串 `listen <port_number> ssl http2;` 中指定新的端口号

   b. 运行命令 `nginx -s reload` 以重启 Nginx 并应用配置文件中的更改。

Endpoint Agent 使用的端口已更改。agentserver 组件开始使用新端口接收来自 Endpoint Agent 的数据。默认端口 443 无法用于连接到 agentserver 组件。

准备工作和部署

本部分介绍如何为部署 Kaspersky Next XDR Expert 来准备基础架构，设置多节点或单节点部署专用的安装参数，以及如何使用部署向导来生成配置文件。

您将了解如何根据多节点和单节点部署方案来安装 Kaspersky Next XDR Expert。此外，本部分还包含有关如何使用 Kaspersky Next XDR Expert 实例部署多个 Kubernetes 集群以及如何使用 KDT 在它们之间切换的信息。

多节点部署：准备管理员和目标主机

准备多节点部署包括配置管理员主机和目标主机。准备好主机并指定配置文件后，您将能够使用 KDT 在目标主机上部署 Kaspersky Next XDR Expert。

准备管理员主机

首先需要准备一个设备作为管理员主机，KDT 将从该设备启动。该主机既可以纳入部署期间由 KDT 创建的 Kubernetes 集群，也可以不纳入。如果管理员主机不包含在集群中，它将仅用于部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert。如果管理员主机包含在集群中，它还将充当用于运行 Kaspersky Next XDR Expert 组件的目标主机。

> 分配给管理员主机的所有虚拟 CPU 必须位于同一个 NUMA 节点上。在 Hypervisor 上配置管理员主机的虚拟机时，请确保 CPU 和内存资源分配自同一个 NUMA 节点。这样可以防止跨节点内存访问，因为跨节点内存访问可能导致安装期间内存分配失败。

要准备管理员主机：

1. 确保管理员主机上的硬件和软件满足要求。

   如果管理员主机未包含在 Kubernetes集群中，请使用KDT要求。

   如果管理员主机包含在集群中，请使用多节点部署的硬件要求和OSMP的软件要求。

2. 在临时文件目录（默认情况下，`/tmp`）中为 KDT 分配至少 15 GB 的可用空间。如果此目录中没有足够的可用空间，请运行以下命令指定另一个目录的路径：

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. 配置容器运行时。使用以下容器运行时之一：

   - KDT 内置容器运行时（基于 runc）。

     要安装该运行时，请运行以下命令：

     ```
     sudo ./kdt init
     ```

     如果内置容器运行时不适合您的环境，您可以改用 Docker 容器运行时。

   - Docker 容器运行时。

安装适用于Docker 25或更高版本的套件。请勿从操作系统维护者的存储库中安装非官方的 Docker 软件包分发版。

如果 Docker 密钥环无法自动下载，请手动下载：

a. 在浏览器中开放 https://download.docker.com/linux/ubuntu/gpg 链接，将密钥保存为 docker.asc。

b. 执行以下命令：

```
sudo mv docker.asc /etc/apt/keyrings/docker.asc
```

用于 Docker 数据存储的磁盘分区（默认情况下为 `/var/lib/docker`）必须至少有 60 GB 的可用空间。

执行安装后步骤，配置管理主机以确保Docker正常运行：

```
sudo groupadd docker
sudo usermod -aG docker $USER
newgrp docker
sudo systemctl enable docker.service
sudo systemctl enable containerd.service
sudo systemctl status docker.service
```

4. 对于将被纳入该集群的管理员主机，请执行额外的准备操作：

a. 由于该设备将充当管理员主机和目标主机，请确保其满足多节点部署的要求。

b. 确保管理员主机支持 cgroup v2 技术。

a. 由于设备将充当管理员主机和目标主机，需要确保其满足单节点部署的要求（因为演示部署和单节点部署的方案类似）。

b. 确保管理员主机支持 cgroup v2 技术。

Linux 内核版本 2.6.24 或更高版本支持 cgroup v2 技术。

c. 在管理员主机上安装 uidmap 软件包。

检查 /etc/subgid 和 /etc/subuid 文件包含将用于启动 KDT 的用户账户。为此，请运行以下命令：

```
getsubids USER
```

如果此命令未返回结果，则必须按以下格式，手动将用户账户添加到 /etc/subgid 和 /etc/subuid 文件中：

```
<username>:<min_subid>:<range_length>
```

where：

- `<username>` — 启动 KDT 的账户的用户名。
- `<min_subid>` — 最小 subuid 值。
- `<range_length>` — 为用户 `<username>` 分配的 subuid 数量。

准备目标主机

目标主机是用于部署 Kaspersky Next XDR Expert 的物理机或虚拟机，并包含在 Kubernetes 集群中。Kaspersky Next XDR Expert 组件在这些主机上运行。

其中一个目标主机可用作管理员主机。在这种情况下，您必须按照前面的步骤将此主机配置为管理员主机，然后执行目标主机的准备工作。

多节点部署的最小集群配置包括四个节点：

- 一个主节点

  主节点用于管理集群、存储元数据和分配工作负载。

- 三个工作节点

  工作节点用于执行 Kaspersky Next XDR Expert 组件的工作负载。

集群中的主节点和工作线程节点的数量可能会有所不同。为了在节点之间实现最佳工作负载分配，推荐使用性能大致相同的节点。

KUMA服务（收集器、关联器和存储）可以完全安装在集群内的工作节点上，完全安装在Kubernetes集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。

如果您有多个主节点，则需要负载均衡器来在主节点之间分配传入的请求，并确保工作负载均匀。如果您想使用外部负载平衡器，请在Kubernetes集群之外分配一个单独的主机，并在配置文件中指定其参数。如果您不想使用外部负载平衡器，工作线程节点将充当负载平衡器。

要准备目标主机：

1. 确保目标主机上的硬件和软件满足多节点部署的要求，并且目标主机位于同一个广播域中。

   如果 KUMA 服务安装在集群内，目标主机必须满足安装 KUMA 服务所需的硬件、软件和安装要求。

   为了使 Kaspersky Next XDR Expert 正常运行，目标主机上 Ubuntu 系列操作系统的 Linux 内核版本必须为 5.15.0.107 或更高版本。

   为确保 Kubernetes 集群及其组件正常运行，必须在所有集群节点上禁用交换分区。如果节点上启用了交换分区，KDT 将在部署期间自动将其禁用。

   目标主机上不得安装 Docker，除非目标主机将用作管理员主机。KDT 将在部署期间安装所有必要的软件和依赖项。

2. 确保挂载在 `/var` 的文件系统在每个目标主机上至少有 700 GB 的可用空间。

   周三建议将 `/opt/lvp/hot` 目录放置在专用的高性能磁盘子系统上，并将 `/opt/lvp/cold` 目录放置在单独的高容量磁盘子系统上。

3. 在每个目标主机上，安装 sudo 包（如果尚未安装）。对于 Debian 系列操作系统，请在目标主机上安装 UFW 包。

4. 在每个目标主机上，配置 /etc/environment 文件。如果您组织的基础设施使用代理服务器来访问互联网，请使用目标主机上的代理服务器来配置互联网访问。

5. 在具有UFW配置的主节点上，允许IP转发。在 `/etc/default/ufw` 文件中，将 `DEFAULT_FORWARD_POLICY` 设置为 `ACCEPT`。

6. 提供对软件包存储库的访问权限，该存储库中存储了 Kaspersky Next XDR Expert 所需的以下软件包：

   - nfs-common
   - containerd
   - cron
   - cryptsetup
   - cryptsetup-bin
   - netcat-traditional
   - nfs-common
   - open-iscsi
   - python3-cffi-backend
   - python3-cryptography
   - python3-netaddr
   - python-apt-common
   - systemd
   - tar

   KDT 将在部署期间尝试从软件包存储库安装这些包。您也可以手动安装这些软件包。

7. 确保安装了以下软件包：

   - 在每个目标主机上：python3-apt
   - 在主节点上：curl

   在使用KDT从软件包存储库部署期间，这些软件包不会安装。如果尚未安装这些软件包，则必须手动安装。

8. 对于目标主机，请在虚拟机监控程序、虚拟交换机或网络基础设施级别禁用ARP/MAC欺骗保护机制。

   对于 VMware，请启用**伪造传输**和**MAC 地址更改**。对于 Hyper-V，请启用**MAC 地址欺骗**。对于网络设备，请禁用**动态 ARP 检测 (DAI)**，或将端口配置为受信任端口。

   有关检查 ARP 请求是否到达节点的示例，请参阅MetalLB 故障排除指南。

9. 为目标主机和 Kubernetes 集群网关预留静态 IP 地址。

   Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。网关 IP 地址是 IPv4 地址（例如，10.80.23.182）。它在配置文件中指定（“`ingress_ip`”参数）。

确保目标主机、Kubernetes 集群网关和 DBMS 主机位于同一广播域中。

> Kubernetes 集群网关和目标主机需要 IPv4 地址。如果您的环境需要 IPv6 连接，请配置目标主机和 Kubernetes 集群网关上的操作系统，以将 IPv6 流量路由到 IPv6 网关 (NAT64) 或 IPv6 隧道。此配置可使集群在 IPv4 上运行，同时提供与 IPv6 网络的互操作性。

10. 在您的 DNS 服务器上，注册服务 FQDN 以连接到 Kaspersky Next XDR Expert 服务。

    默认情况下，Kaspersky Next XDR Expert 服务可通过以下地址访问：

    - <console_host>.<smp_domain> — 访问 OSMP 控制台界面。
    - <ksc_host>.<smp_domain> — 与管理服务器交互。
    - <kuma_host>.<smp_domain>—访问SIEM组件。
    - <api_host>.<smp_domain> — 访问 Kaspersky Next XDR Expert API。
    - <monitoring_host>.<smp_domain> — 访问 OSMP 指标。

      其中 <console_host>、<ksc_host>、<kuma_host>、<api_host> 和 <monitoring_host> 是服务主机名，<smp_domain> 是服务域名。这些参数是服务 FQDN 的一部分，您可以在配置文件中指定。如果您未指定服务主机名的自定义值，则使用默认值：`console_host` — “`console`”、`ksc_host` — “`admsrv`”、`kuma_host` — “`kuma`”、`api_host` — “`api`”、`monitoring_host` — “`monitoring`”。

    列出的服务 FQDN 必须解析为 Kubernetes 集群的 IP 地址。例如，如果 Kubernetes 集群地址为 10.80.23.182，则服务 FQDN 将按如下方式解析为 IP 地址：

    - <console_host>.<smp_domain>—10.80.23.182
    - <ksc_host>.<smp_domain>—10.80.23.182
    - <kuma_host>.<smp_domain>—10.80.23.182
    - <api_host>.<smp_domain>—10.80.23.182
    - <monitoring_host>.<smp_domain>—10.80.23.182

11. 在目标主机上，创建将用于 Kaspersky Next XDR Expert 部署的账户。

    这些账户用于 SSH 连接，并且必须能够在不输入密码的情况下提升权限 (sudo)。为此，将创建的用户账户添加到 `/etc/sudoers` 文件。

    查看详情

    要将创建的用户账户添加到 `/etc/sudoers` 文件：

    1. 运行以下命令：

       ```
       sudo useradd -m -s /bin/bash <user_name>
       sudo usermod -aG sudo <user_name>
       ```

    2. 使用以下命令打开 `/etc/sudoers` 文件：

       ```
       sudo visudo
       ```

3. 在 `# Allow members of group sudo to execute any command` 部分的末尾添加以下行：

   ```
   <user_name> ALL=(ALL) NOPASSWD: ALL
   ```

   其中，`<user_name>` 是所创建用户的名称。

4. 保存并关闭 `/etc/sudoers` 文件。

12. 配置管理员和目标主机之间的 SSH 连接：

    a. 在管理员主机上，使用 ssh-keygen 实用程序生成 SSH 密钥，不设置密码短语。

    b. 使用 ssh-copy-id 实用程序将公钥复制到每个目标主机；如果使用负载均衡器，还要复制到负载均衡器主机（例如，复制到 `/home/<user_name>/.ssh` 目录）。

    如果使用目标主机作为管理员主机，则还必须将公钥复制到该主机。

13. 为了确保 Kaspersky Next XDR Expert 组件正常运行，请在目标主机之间提供网络访问，并在必要时在管理员主机和目标主机的防火墙上打开所需端口。

14. 在管理员主机和目标主机上通过网络时间协议 (NTP) 配置时间同步。

15. 如有必要，请准备自定义证书以便使用 Kaspersky Next XDR Expert 公共服务。

    您可以为每项服务使用一个基于组织根证书或叶证书颁发的中间证书。准备好的自定义证书将代替自签名证书。

单节点部署：准备管理员和目标主机

准备单节点部署包括配置管理员主机和目标主机。在单节点配置中，Kubernetes 集群和 Kaspersky Next XDR Expert 组件安装在一个目标主机上。准备好目标主机并指定配置文件后，您将能够使用 KDT 在目标主机上部署 Kaspersky Next XDR Expert。

准备管理员主机

首先需要准备一个设备作为管理员主机，KDT 将从该设备启动。该主机既可以纳入部署期间由 KDT 创建的 Kubernetes 集群，也可以不纳入。如果管理员主机不包含在集群中，它将仅用于部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert。如果管理员主机包含在集群中，它还将充当用于运行 Kaspersky Next XDR Expert 组件的目标主机。在这种情况下，只有一台主机用于部署和运行该解决方案。

> 分配给管理员主机的所有虚拟 CPU 必须位于同一个 NUMA 节点上。在 Hypervisor 上配置管理员主机的虚拟机时，请确保 CPU 和内存资源分配自同一个 NUMA 节点。这样可以防止跨节点内存访问，因为跨节点内存访问可能导致安装期间内存分配失败。

要准备管理员主机：

1. 确保管理员主机上的硬件和软件满足要求。

   如果管理员主机未包含在 Kubernetes集群中，请使用KDT要求。

   如果管理员主机包含在集群中，请使用单节点部署的硬件要求和 OSMP的软件要求。

2. 在临时文件目录（默认情况下，`/tmp`）中为 KDT 分配至少 15 GB 的可用空间。如果此目录中没有足够的可用空间，请运行以下命令指定另一个目录的路径：

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. 配置容器引擎。使用以下容器引擎之一：

   - KDT 内置容器引擎（基于 runc）

     运行以下命令安装内置容器引擎：

     ```
     sudo ./kdt init
     ```

     如果内置容器引擎不适合您的环境，您可以改用 Docker 容器引擎。

   - Docker 容器引擎

     安装适用于Docker 25 或更高版本的套件。请勿从操作系统维护者的存储库中安装非官方的 Docker 软件包分发版。

     如果 Docker 密钥环无法自动下载，请手动下载：

     a. 在浏览器中开放 https://download.docker.com/linux/ubuntu/gpg 链接，将密钥保存为 docker.asc。

     b. 执行以下命令：

     ```
     sudo mv docker.asc /etc/apt/keyrings/docker.asc
     ```

     用于 Docker 数据存储的磁盘分区（默认情况下为 `/var/lib/docker`）必须至少有 60 GB 的可用空间。

     执行安装后步骤，配置管理主机以确保Docker正常运行：

     ```
     sudo groupadd docker
     sudo usermod -aG docker $USER
     newgrp docker
     sudo systemctl enable docker.service
     sudo systemctl enable containerd.service
     sudo systemctl status docker.service
     ```

4. 对于将被纳入该集群的管理员主机，请执行额外的准备操作：

   a. 由于该设备将充当管理员主机和目标主机，请确保其满足单节点部署的要求。

   b. 确保管理员主机支持 cgroup v2 技术。

      a. 由于设备将充当管理员主机和目标主机，需要确保其满足单节点部署的要求（因为演示部署和单节点部署的方案类似）。

      b. 确保管理员主机支持 cgroup v2 技术。

         Linux 内核版本 2.6.24 或更高版本支持 cgroup v2 技术。

      c. 在管理员主机上安装 uidmap 软件包。

         检查 /etc/subgid 和 /etc/subuid 文件包含将用于启动 KDT 的用户账户。为此，请运行以下命令：

         ```
         getsubids USER
         ```

         如果此命令未返回结果，则必须按以下格式，手动将用户账户添加到 /etc/subgid 和 /etc/subuid 文件中：

`<username>:<min_subid>:<range_length>`

where:

- `<username>` — 启动 KDT 的账户的用户名。
- `<min_subid>` — 最小 subuid 值。
- `<range_length>` — 为用户 `<username>` 分配的 subuid 数量。

准备目标主机

目标主机是用于部署 Kaspersky Next XDR Expert 并包含在 Kubernetes 集群中的物理机或虚拟机。目标主机管理 Kubernetes 集群以及运行在该主机上的 Kaspersky Next XDR Expert 组件，并存储元数据。

单节点部署的最小集群配置包括一台充当主节点和工作节点的目标主机。Kubernetes 集群和 Kaspersky Next XDR Expert 组件安装在此主工作节点上。

KUMA 服务（收集器、关联器和存储）可以完全安装在集群内部的主要工作节点上，也可以完全安装在 Kubernetes 集群外部的独立主机上，或者部分安装在 Kubernetes 集群内部，部分安装在 Kubernetes 集群外部。

如果要从目标主机运行 Kaspersky Next XDR Expert 部署程序，则必须按照前面的步骤将此主机配置为管理员主机，然后执行目标主机的准备工作。

要准备目标主机：

1. 确保目标主机上的硬件和软件满足单节点部署的要求。

   如果KUMA服务安装在集群内部，则目标主机必须满足安装KUMA服务所需的硬件、软件和安装要求。

   由于 DBMS 将安装在目标主机上，因此您还需要确保目标主机满足 DBMS 的要求。

   为确保 Kaspersky Next XDR Expert 正常运行，搭载 Ubuntu 系列操作系统的目标主机，其 Linux 内核版本必须为 5.15.0.107 或更高版本。

   为确保 Kubernetes 集群及其组件正常运行，必须在所有集群节点上禁用交换分区。如果节点上启用了交换分区，KDT 将在部署期间自动将其禁用。

   除非目标主机将用作管理员主机，否则请勿在目标主机上安装 Docker。KDT 将在部署期间安装所有必要的软件和依赖项。

2. 确保挂载在 `/var` 的文件系统在目标主机上至少有 360 GB 的可用空间。

   周三建议将 `/opt/lvp/hot` 目录放置在专用的高性能磁盘子系统上，并将 `/opt/lvp/cold` 目录放置在单独的高容量磁盘子系统上。

3. 在目标主机上安装 DBMS。

   在部署 Kaspersky Next XDR Expert 之前，您必须安装 DBMS，因为在这种情况下，DBMS 和 Kaspersky Next XDR Expert 组件将安装在同一目标主机上，并且 DBMS 不包含在 Kubernetes 集群中。

4. 如果尚未安装 sudo 软件包，请安装此包。对于 Debian 系列操作系统，请安装 UFW 软件包。

5. 配置 /etc/environment 文件。如果您组织的基础设施使用代理服务器来访问互联网，请使用目标主机上的代理服务器来配置互联网访问。

6. 如果主工作线程节点具有 UFW 配置，则允许 IP 转发。在 `/etc/default/ufw` 文件中，将 `DEFAULT_FORWARD_POLICY` 设置为 `ACCEPT`。

7. 提供对软件包存储库的访问权限，该存储库中存储了 Kaspersky Next XDR Expert 所需的以下软件包：

   - nfs-common
   - containerd
   - cron
   - cryptsetup
   - cryptsetup-bin
   - netcat-traditional
   - nfs-common
   - open-iscsi
   - python3-cffi-backend
   - python3-cryptography
   - python3-netaddr
   - python-apt-common
   - systemd
   - tar

   KDT 将在部署期间尝试从软件包存储库安装这些包。您也可以手动安装这些软件包。

8. 确保以下软件包安装在主工作线程节点上：

   - python3-apt
   - curl

   在使用KDT从软件包存储库部署期间，这些软件包不会安装。如果尚未安装这些软件包，则必须手动安装。

9. 对于目标主机，请在虚拟机监控程序、虚拟交换机或网络基础设施级别禁用ARP/MAC欺骗防护机制。

   对于 VMware，请启用**伪传输**和**MAC 地址更改**。对于 Hyper-V，请启用**MAC 地址欺骗**。对于网络设备，请禁用**动态 ARP 检测 (DAI)**，或将端口配置为受信任端口。

   有关检查 ARP 请求是否到达节点的示例，请参阅MetalLB 故障排除指南。

10. 为目标主机和 Kubernetes 集群网关预留静态 IP 地址。

Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。网关 IP 地址是 IPv4 地址（例如，10.80.23.182）。它在配置文件中指定（“`ingress_ip`”参数）。

确保目标主机和 Kubernetes 集群网关位于同一广播域中。

> Kubernetes 集群网关和目标主机需要 IPv4 地址。KDT 会自动在集群节点上禁用 IPv6。

11. 在您的 DNS 服务器上，注册服务 FQDN 以连接到 Kaspersky Next XDR Expert 服务。

    默认情况下，Kaspersky Next XDR Expert 服务可通过以下地址访问：

    - <console_host>.<smp_domain> — 访问 OSMP 控制台界面。
    - <ksc_host>.<smp_domain> — 与管理服务器交互。
    - <kuma_host>.<smp_domain>—访问SIEM组件。
    - <api_host>.<smp_domain> — 访问 Kaspersky Next XDR Expert API。
    - <monitoring_host>.<smp_domain> — 访问 OSMP 指标。

      其中 <console_host>、<ksc_host>、<kuma_host>、<api_host> 和 <monitoring_host> 是服务主机名，<smp_domain> 是服务域名。这些参数是服务 FQDN 的一部分，您可以在配置文件中指定。如果您未指定服务主机名的自定义值，则使用默认值：`console_host` — “`console`”、`ksc_host` — “`admsrv`”、`kuma_host` — “`kuma`”、`api_host` — “`api`”、`monitoring_host` — “`monitoring`”。

    列出的服务 FQDN 必须解析为 Kubernetes 集群的 IP 地址。例如，如果 Kubernetes 集群地址为 10.80.23.182，则服务 FQDN 将按如下方式解析为 IP 地址：

    - <console_host>.<smp_domain>—10.80.23.182
    - <ksc_host>.<smp_domain>—10.80.23.182
    - <kuma_host>.<smp_domain>—10.80.23.182
    - <api_host>.<smp_domain>—10.80.23.182
    - <monitoring_host>.<smp_domain>—10.80.23.182

12. 创建将用于部署 Kaspersky Next XDR Expert 的用户账户。

    这些账户用于 SSH 连接，并且必须能够在不输入密码的情况下提升权限 (sudo)。为此，将创建的用户账户添加到 `/etc/sudoers` 文件。

    查看详情

    要将创建的用户账户添加到 `/etc/sudoers` 文件：

    1. 运行以下命令：

       ```
       sudo useradd -m -s /bin/bash <user_name>
       sudo usermod -aG sudo <user_name>
       ```

    2. 使用以下命令打开 `/etc/sudoers` 文件：

       ```
       sudo visudo
       ```

3. 在 `# Allow members of group sudo to execute any command` 部分的末尾添加以下行：

   ```
   <user_name> ALL=(ALL) NOPASSWD: ALL
   ```

   其中，`<user_name>` 是所创建用户的名称。

4. 保存并关闭 `/etc/sudoers` 文件。

13. 配置管理员和目标主机之间的 SSH 连接：

    a. 在管理员主机上，使用 ssh-keygen 实用程序生成 SSH 密钥，不设置密码短语。

    b. 使用 ssh-copy-id 实用程序将公钥复制到目标主机（例如，复制到 `/home/<user_name>/.ssh` 目录）。

    如果使用目标主机作为管理员主机，则还必须将公钥复制到该主机。

14. 为确保 Kaspersky Next XDR Expert 组件正常运行，请在管理员主机和目标主机的防火墙上打开所需的端口（如有必要）。

15. 在管理员主机和目标主机上通过网络时间协议 (NTP) 配置时间同步。

16. 如有必要，请准备自定义证书以便使用 Kaspersky Next XDR Expert 公共服务。

    您可以为每项服务使用一个基于组织根证书或叶证书颁发的中间证书。准备好的自定义证书将代替自签名证书。

准备主机以安装 KUMA 服务

KUMA 服务（收集器、关联器和存储）安装在位于 Kubernetes 集群之外的 KUMA 目标主机上。

使用 KUMA 目标主机 FQDN 访问 KUMA 服务。管理员主机必须能够通过其 FQDN 访问 KUMA 目标主机。

如果您计划在基础设施中使用多个租户，请为每个租户创建一个单独的收集器。

要准备 KUMA 目标主机以安装 KUMA 服务：

1. 确保满足硬件、软件和安装要求。

2. 指定主机名。

   必须指定 FQDN，例如：kuma1.example.com。

   不建议在安装后更改 KUMA 主机名。这将无法验证证书的真实性，并会中断应用程序组件之间的网络通讯。

3. 运行以下命令：

   ```
   hostname -f
   ```

   ```
   hostnamectl status
   ```

   比较 `hostname -f` 命令的输出与 `hostnamectl status` 命令输出中 `Static hostname` 字段的值。这些值必须与设备的 FQDN 匹配。

4. 配置管理员主机和 KUMA 目标主机之间的 SSH 连接。

   使用为目标主机创建的 SSH 密钥。使用 ssh-copy-id 实用程序将公钥复制到 KUMA 目标主机。

5. 在组织的 DNS 区域中注册 KUMA 目标主机，以允许将主机名转换为 IP 地址。

6. 确保所有 KUMA 目标主机上都配置了基于网络时间协议 (NTP) 的时间同步功能。KUMA 服务（收集器、关联器和存储）安装在位于 Kubernetes 集群之外的 KUMA 目标主机上。

主机已准备好安装 KUMA 服务。

安装数据库管理系统

Kaspersky Next XDR Expert 支持 PostgreSQL 或 Postgres Pro 数据库管理系统 (DBMS)。有关受支持的 DBMS 的完整列表，请参阅“硬件和软件要求”。

以下每个 Kaspersky Next XDR Expert 组件都需要一个数据库：

- 管理服务器
- 自动化平台
- 事故响应平台 (IRP)
- Identity and Access Manager (IAM)

每个组件都必须在同一个 DBMS 实例中有一个单独的数据库。DBMS实例必须安装在Kubernetes集群之外的独立服务器上。建议您在 Kubernetes 集群之外安装 DBMS 实例。

对于 DBMS 安装，KDT 需要一个特权 DBMS 账户，该账户需拥有创建数据库及其他 DBMS 账户的权限。KDT 使用具有超级用户权限的默认 DBMS 账户或具有相同权限的其他 DBMS 账户来创建数据库以及 Kaspersky Next XDR Expert 组件所需的其他 DBMS 账户。

对于多节点部署，您必须在不包括Kubernetes集群的独立服务器上手动安装DBMS。

对于单节点部署，您必须在部署 Kaspersky Next XDR Expert 之前在目标主机上手动安装 DBMS。在这种情况下，DBMS 和 Kaspersky Next XDR Expert 组件安装在同一目标主机上，但 DBMS 不包含在 Kubernetes 集群中。

对于如何安装所选 DBMS 的信息，请参考其文档。

PostgreSQL安装程序命令示例

要安装PostgreSQL，请运行以下命令：

```
sudo apt install -y postgresql-<版本>
sudo systemctl start postgresql
sudo systemctl enable postgresql
```

其中，<版本> 是受支持的 PostgreSQL 版本之一。

安装DBMS后，您需要配置DBMS服务器参数，以确保DBMS与Open Single Management Platform的正常运行。

配置 PostgreSQL 或 Postgres Pro 服务器以与 Kaspersky Next XDR Expert 配合使用

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

Kaspersky Next XDR Expert 支持 PostgreSQL 或 Postgres Pro 数据库管理系统 (DBMS)。有关受支持的 DBMS 的完整列表，请参阅“硬件和软件要求”。考虑配置 DBMS 服务器参数，以优化 DBMS 与管理服务器的协同工作。DBMS 服务器参数符合建议值是安装 Kaspersky Next XDR Expert 的先决条件之一。参数是否符合要求将使用 KDT 进行验证。

查找DBMS配置文件：

- PostgreSQL 配置文件的默认路径为： `/etc/postgresql/<VERSION>/main/postgresql.conf`
- Postgres Pro 配置文件的默认路径为： `/var/lib/pgpro/std-<VERSION>/data/postgresql.conf`

如果默认路径下没有配置文件，请运行以下命令查找正确路径：

```
sudo su - postgres
psql -c 'SHOW config_file'
```

命令响应将包含配置文件路径。

然后运行以下命令登出`postgres`用户：

```
exit
```

PostgreSQL 和 Postgres Pro DBMS 与管理服务器协同工作的推荐参数：

- `listen_addresses = '*'`

  指定管理服务器将监听的IP接口。出于安全原因，请配置防火墙，仅允许访问受信任的IP地址访问端口5432。

- `max_connections = 512`

  这是推荐的最小值，您可以指定更大的值。如果您使用集群式 Postgres DBMS，请在所有 DBMS 服务器以及集群配置中指定 `max_connections` 参数。

- `shared_buffers = N`

  N = 安装了 DBMS 的设备的 RAM 值的 25%-40%，但不得小于 3 GB。

- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `maintenance_work_mem = 128MB`
- `max_stack_depth = N`

如果 DBMS 安装程序在 Linux 设备上，则 N = 最大堆栈大小减去 1 MB 安全余量。要获取最大堆栈大小值（以 KB 为单位），请执行“`ulimit -s`”命令。

如果 DBMS 安装在 Windows 设备上，则保留默认值 2 MB。

- `max_parallel_workers_per_gather = 0`
- `standard_conforming_strings = on`

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

```
enable_compound_index_stats = off
```

更新配置文件后，重新加载配置或重新启动DBMS服务器。

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

在 pg_hba.conf配置文件中为节点身份验证条目。您可以在 postgresql.conf 所在的同一路径中找到它。

- 在 `"# "local" is for Unix domain socket connections only"` 部分中，对于 `local`，在 `METHOD` 列中，将值更改为 `trust`
- 在 `"IPv4 local connections"` 部分中，对于 `host`，在 `ADDRESS` 列中，将值更改为 `0.0.0.0/0`
- 运行以下命令以应用更改，而无需重新启动数据库服务器：

  ```
  sudo -u postgres psql -c "SELECT pg_reload_conf();"
  ```

指定 `postgres` 用户的密码：

1. 运行以下命令：

   ```
   sudo su - postgres
   psql
   ```

   命令输出应如下所示：

   ```
   psql (15.12)
   Type "help" for help.
   postgres=#
   ```

2. 在 `postgres=#` 后，输入 `\password`：

   ```
   postgres=# \password
   ```

3. 输入并重复密码：

   ```
   Enter new password for user "postgres"
   Enter it again:
   ```

4. 要注销用户 `postgres`：

   ```
   postgres=# exit
   ```

Kaspersky Next XDR Expert 组件要求在 `parameters.psql_dsn` 中以 `value` 的形式提供 PostgrSQL 超级用户凭据。请在部署配置文件中指定postgres凭证。有关更多信息，根据您的部署模式，请参阅单节点部署：指定安装参数或多节点部署：指定安装参数部分。

检查数据库连接

要检查数据库连接：

1. 确保Postgres服务正在运行：

   ```
   systemctl list-unit-files | grep postgres
   ```

   示例输出：

   ```
   postgrespro-std-17.service                                              enabled         enabled
   ```

2. 重新启动 Postgres 服务：

   ```
   systemctl restart <Postgres_service>
   ```

   其中 <`Postgres_service`> 是在此过程的步骤 1 中获得的 Postgres 服务名称。

3. 运行 `psql` 检查连接：

   ```
   psql -h <fqdn> -U postgres -d postgres
   ```

   输入之前指定的密码：

   ```
   Password for user postgres:
   ```

   示例输出：

   ```
   psql (17.4)
   Type "help" for help.
   ```

4. 输入 `exit`：

   ```
   postgres=# exit
   ```

支持高可用性集群

高可用性 PostgreSQL 集群支持以下设置：

- 复制类型：同步。
- 最少节点数：3。
- 最大节点数：15。

按如下方式设置 psql_dsn 参数：postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>

当使用 Postgres 高可用性集群（版本 14 或更高版本）作为数据库时，数据库用户必须具有 pg_read_all_stats 权限。您可以通过运行以下命令授予此权限：

```
GRANT pg_read_all_stats TO "dbms_username";
```

其中 dbms_username 是拥有权限的内部 DBMS 账户的名称。

在配置文件（/etc/postgresql/< VERSION >/main/postgresql.conf)）中指定以下参数：

```
log_hostname = 1
```

Corosync/Pacemaker 支持

若要使用 Corosync/Pacemaker，请使用 DBMS 集群的虚拟 IP 地址设置 psql_dsn 参数，如下所示：

```
psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>
```

准备 KUMA 清查文件，以便在 Kubernetes 集群外部安装 KUMA 服务

KUMA 清查文件是一个 YAML 格式的文件，包含用于部署 Kubernetes 集群中未包含的 KUMA 服务的安装参数。KUMA 清查文件的路径包含在配置文件中，该配置文件供卡巴斯基部署工具包用于部署 Kaspersky Next XDR Expert。

KUMA 清查文件的模板位于分发包中。如果要在一台主机上安装KUMA服务（存储、收集器和关联器），请使用single.inventory.yaml文件。要在网络基础设施中的多台主机上安装服务，请使用distributed.inventory.yaml文件。

建议您备份用于安装 KUMA 服务的 KUMA 清查文件。您可以使用它来删除 KUMA。

要准备 KUMA 清查文件：

请打开分发包中的 KUMA 清查文件模板，然后编辑清查文件中的变量。

KUMA 清查文件包含以下区块：

- all 区块

  all 区块包含的变量应用于清查文件中指定的所有主机。变量位于 vars 部分。

- kuma 区块

  kuma 区块包含的变量应用于将安装 KUMA 服务的主机。这些主机列在 children 部分的 kuma 区块中。变量位于 vars 部分。

下表列出了可能的变量、它们的描述、可能值以及这些变量所在的 KUMA 清查文件区块。

vars 部分中可能的变量列表

变量	描述	可能值	阻止
位于 all 和 kuma 区块的 vars 部分中的变量			
ansible_connection	用于连接到 KUMA 服务主机的方法。	• ssh — 已通过 SSH 建立与目标主机的连接。 • local — 未与目标主机建立连接。 为确保 KUMA 服务正确安装，在 all 区块中，将 ansible_connection 变量设置为 local。 在 kuma 区块中，您必须指定 ansible_connection 变量并将 ansible_connection 设置为 ssh，以通过 SSH 与安装 KUMA 服务的主机建立连接。	• all • kuma
ansible_user	用于连接到 KUMA 服务主机以安装外部 KUMA 服务的用户名。	如果目标主机上的根用户被阻止，需指定一个有权建立 SSH 连接并可通过 su 或 sudo 提升权限的用户名。 为确保 KUMA 服务正确安装，在 all 区块中，将 ansible_user 变量设置为 nonroot。 在 kuma 区块中，您必须覆盖 ansible_user 变量并将 ansible_user 设置为可以通过 SSH 连接到远程主机的账户的用户名，为安装 KUMA 服务做好准备。	• all • kuma
ansible_become	用于指示需要增加用于安装 KUMA 组件的用户账户的权限的变量。	• false — 如果 ansible_user 的值为 root。 • true — 如果 ansible_user 的值不为 root。	kuma
ansible_become_method	用于提升安装 KUMA 组件所用的用户账户权限的方法。	su 或 sudo — 如果 ansible_user 的值不为 root。	kuma
位于 kuma 区块的 children 部分中的变量			
kuma_utils	用于存储 KUMA 服务文件和实用程序的主机组。 主机可以同时包含在 kuma_utils 组以及 kuma_collector、 kuma_correlator 或 kuma_storage 组中。 kuma_utils 组可以包含多个主机。 在 Kaspersky Next XDR Expert 部署期间，对于包含在 kuma_utils 中的主机，以下文件会被复制到 /opt/kaspersky/kuma/utils/ 目录中： • kuma 是用于安装 KUMA 服务的可执行文件。 • kuma.exe 是用于在基于 Windows 的主机上安装 KUMA 代理的可执行文件。 • LEGAL_NOTICES 是一个包含第三方代码信息的文件。 • kuma-ptvm.tar.gz 是用于与 MaxPatrol 集成的实用程序。 • ootb-content 是一个压缩文件，包含用于 KUMA 服务的开箱即用资源。	该主机组包含指定唯一主机 FQDN 和 IP 地址的 ansible_host 变量。	kuma
kuma_collector	KUMA 收集器主机组。该组可以包含多个主机。	KUMA 收集器主机组包含指定唯一主机 FQDN 和 IP 地址的 ansible_host 变量。	kuma
kuma_correlator	KUMA 关联器主机组。该组可以包含多个主机。	KUMA 关联器主机组包含指定唯一主机 FQDN 和 IP 地址的 ansible_host 变量。	kuma
kuma_storage	KUMA 存储主机组。该组可以包含多个主机。	KUMA 存储主机组包含指定唯一主机 FQDN 和 IP 地址的 ansible_host 变量。	kuma

用于在单个主机上安装KUMA服务的KUMA清查文件模板示例（single.inventory.yaml 文件）

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
```

```
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 1
```

用于在多个主机上安装KUMA服务的KUMA清查文件模板示例（distributed.inventory.yaml 文件）

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma-utils.example.com:
        ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
        ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
        ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-1.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 1
        kuma-storage-2.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 2
            keeper: 2
        kuma-storage-3.example.com:
```

```
        ansible_host: 0.0.0.0
        shard: 2
        replica: 1
        keeper: 3
    kuma-storage-4.example.com:
        ansible_host: 0.0.0.0
        shard: 2
        replica: 2
```

多节点部署：指定安装参数

配置文件是 YAML 格式的文件，包含 Kaspersky Next XDR Expert 组件的一组安装参数。

> 下表列出的安装参数是 Kaspersky Next XDR Expert 多节点部署的必要参数。要在单个节点上部署 Kaspersky Next XDR Expert，请使用包含特定于单节点部署的安装参数的配置文件。

配置文件的模板 (multinode.smp_param.yaml.template) 位于分发包中，压缩包内包含 KDT 实用程序。您可以手动填写配置文件模板；或者使用“部署向导”来指定 Kaspersky Next XDR Expert 部署所需的安装参数，然后生成配置文件。

配置文件模板中并未包含下面列出的所有参数。此模板仅包含在部署 Kaspersky Next XDR Expert 之前必须指定的参数。其余参数设置为默认值，不包含在模板中。您可以手动将这些参数添加到配置文件中以覆盖其原有值。参数值必须遵循下面描述的规则。在部署 Kaspersky Next XDR Expert 期间，KDT 会检查是否正确指定了所需的安装参数。如果配置文件中所需的参数缺失或无效，部署将会中断。

Kaspersky Next XDR Expert 多节点部署配置文件示例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Nodes on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
  # Control node settings.
    # 节点名称。 该值的长度必须在 1 到 63 个字符之间。
    # The node name can contain only ASCII characters: letters (a-z; A-Z), numbers (0-9),
    and hyphen (-).
  - desc: cdt-primary1
    # The node type.
    # Possible node types: control, worker.
    # The primary node is intended for managing the cluster, storing metadata, and
    distributing the workload.
    type: primary
    # The IP address of the node.
    # Primary and worker nodes must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.42
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
```

```
      # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
      9), and hyphen (-).
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
# Worker node settings.
  # 节点名称。 该值的长度必须在 1 到 63 个字符之间。
  # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
  and hyphen (-).
- desc: cdt-w1
  # The node type.
  # Possible node types: control, worker.
  # The workload of Kaspersky XDR components is distributed between worker nodes.
  type: worker
  # KUMA 服务安装在工作节点上。 可以指定一个、多个或不指定 KUMA 服务。
  kuma_roles: ["core","metrics","collector"]
  # The IP address of the node.
  # Primary and worker nodes must be included in the same subnet as the Kubernetes
  cluster gateway.
  host: 10.80.23.141
  access:
    ssh:
      # User account name.
      # A user account is created on the target device and is used by KDT for connection
      to the node.
      # The user name must be 1 to 31 characters long.
      # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
      9), and hyphen (-).
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
# Worker node settings.
  # 节点名称。 该值的长度必须在 1 到 63 个字符之间。
  # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
  and hyphen (-).
- desc: cdt-w2
  # The node type.
  # Possible node types: control, worker.
  # The workload of Kaspersky XDR components is distributed between worker nodes.
  type: worker
  # The IP address of the node.
  # Primary and worker nodes must be included in the same subnet as the Kubernetes
  cluster gateway.
  host: 10.80.23.45
  access:
    ssh:
      # User account name.
      # A user account is created on the target device and is used by KDT for connection
      to the node.
      # The user name must be 1 to 31 characters long.
      # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
      9), and hyphen (-).
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
# Worker node settings.
  # 节点名称。 该值的长度必须在 1 到 63 个字符之间。
```

```
    # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
    and hyphen (-).
  - desc: cdt-w3
    # The node type.
    # Possible node types: control, worker.
    # The workload of Kaspersky XDR components is distributed between worker nodes.
    type: worker
    # The IP address of the node.
    # Primary and worker nodes must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.30
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
        # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
        9), and hyphen (-).
        user: root
        # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
        # password: pass
# Parameters for the Kaspersky XDR deployment
parameters:
  # The connection string for access to the DBMS that is installed and configured on a
  separate server.
  # user_db – 具有权限的内部 DBMS 账户的用户名。 此账户被授予创建数据库和其他 DBMS 账户的权限。
  # password_db—The password of the privileged internal DBMS account.
  # fqdn_db:port_db is the fully qualified domain name and connection port of the
  separate server on which the DBMS is installed.
  # “psql_dsn” 参数值必须符合 URI 格式。 如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使
  用百分号编码进行编码。
  - name: psql_dsn
    source:
      value: "postgres://postgres:password@dbms.example.com:1234"
  # IP address of the Kubernetes cluster gateway
  # The Kubernetes cluster gateway is intended for connecting to the Kaspersky XDR
  components installed inside the Kubernetes cluster.
  # The gateway must be included in the same subnet as all cluster nodes.
  - name: ingress_ip
    source:
      value: 10.80.23.182
  # 使用 KDT 连接到主节点和工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
  # The parameter value must be a Linux file path or Base64-encoded file content.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky XDR user account that will be created during the
  installation.
  # The password must be 10 to 256 characters long.
  # It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
  numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \
  ` ~ " ( ) ;).
  # The password must not contain either whitespaces or ".@".
  - name: admin_password
    source:
      value: "password"
  # Disk space for the KUMA Core, in gigabytes.
```

```
# 指定为“<amount>Gi”。 默认值为 512Gi。
# If the 'low_resources' setting is set to true, the 'core_disk_request' setting is
ignored and 4Gi is allocated.
- name: core_disk_request
  source:
    value: 512Gi
# 包含 KUMA 服务部署安装设置的 KUMA 清单文件的路径。 此文件位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Kaspersky Endpoint Detection and Response 授权许可密钥的路径。 此文件位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: license
  source:
    value: "/home/user/license.key"
# 域名。 参数值必须满足四级及以下域名的命名要求。
# The service host name and domain name are parts of FQDNs of the Kaspersky XDR
services.
# Default values of service host names: nwc_host—"console", flow_host—"console",
hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host—"console",
api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom device names can be specified in the configuration file.
# 示例：console.smp.local 是提供对 OSMP 控制台的访问权限的服务的 FQDN。 此 FQDN 由
“console_host”和“smp_domain”设置的值组成。
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom
certificate must be generated.
# 参数值必须是主机名列表，以空格分隔。 如果未指定自定义主机名，则使用以下默认主机名：
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring"
- name: autodeploy_plan
  source:
    value: "edr"
# The user name of the account used to view OSMP metrics through the Grafana tool.
# The user name must be 1 to 30 characters long.
# A user name can contain lowercase letters ('a' to 'z'), numerals ('0' to '9') and
special characters (_ -.)&period;
# A user name must begin with a letter and may not contain spaces or the "@" character.
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# The password of the account used to view OSMP metrics through the Grafana tool.
# The password must be 8 to 256 characters long.
# It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' ,
&period; ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

为了使 KDT 与配置文件正确运行，请在文件末尾添加一个空行。

配置文件的“nodes”部分包含 Kubernetes 集群每个目标主机的安装参数。这些参数列于下表中。

参数名称	是否必需	Description
`desc`	是	节点名称。 值必须符合以下规则： • 节点名称的长度必须在 1 到 63 个字符之间。 • 节点名称可以包含以下字符： • 大写 ASCII 字母 (A-Z) • 小写 ASCII 字母 (a-z) • 数字 (0-9) • 连字符 (-) 所有集群节点必须具有唯一的名称。这一要求是安装Kaspersky Next XDR Expert的先决条件之一，并经KDT验证。
`type`	是	节点类型。 可能的参数值： • `primary` • `worker` • `loadbalancer`
`host`	是	节点的 IP 地址。 所有节点必须与 Kubernetes 集群网关位于同一子网中。 节点需要 IPv4 地址。KDT 会自动在集群节点上禁用 IPv6。 如果您有多个主节点，则需要负载均衡器来在主节点之间分配传入的请求，并确保工作负载均匀。如果您想使用外部负载均衡器，请在群集之外分配一个单独的主机，并在配置文件中指定其参数。如果您不想使用外部负载平衡器，工作线程节点将充当负载平衡器。
`kuma_role`	否	可以指定在工作节点上安装的 KUMA 服务。您可以指定一个、多个或不指定任何KUMA服务。 使用 OSMP 控制台在 Kubernetes 集群中安装 KUMA 服务时，会考虑 `kuma_roles` 参数。如果您计划安装 KUMA 服务的节点过载，集群将选择另一个负载较低的节点进行服务安装。 KUMA 服务（收集器、关联器和存储）可以完全安装在集群内的工作线程节点上，完全安装在 Kubernetes 集群外的单独主机上，或者部分安装在 Kubernetes 集群内，部分安装在 Kubernetes 集群外。如果所有 KUMA 服务都将安装在集群内部，请将 `inventory` 参数设置为 `/dev/null`。 不允许将由同一KUMA资源创建的存储放在同一工作线程节点上。此规则确保了所需的容错级别。 如果存储集群包含多个存储实例，则所有实例都必须部署在集群内部或集群外部。 可能的参数值： • `core`—KUMA Core • `metrics`—KUMA 指标 • `collector`—收集器 • `eventrouter`—事件路由器 • `correlator`—关联器 • `storage`—存储 参数值指定为包含 KUMA 角色的字符串列表。例如： `kuma_roles: ["core","metrics","collector"]`
`user`	是	在目标主机上创建、供 KDT 连接节点时使用的账户用户名。 值必须符合以下规则： • 用户名长度必须在 1 到 31 个字符之间。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 下划线 (_)、连字符 (-)
`password`	否	连接节点的密码。可以代替由 `ssh_pk` 参数指定的 SSH 密钥。

其他安装参数列在配置文件的“`parameters`”部分，并在下表中说明。

参数部分

参数名称	是否必需	Description

`psql_dsn`	是	用于访问在 Kubernetes 集群外部安装和配置的 DBMS 的连接字符串。
		此参数指定如下：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`
		其中：
		• `dbms_username` — 具有权限的内部 DBMS 账户的用户名。此账户被授予创建数据库和其他 DBMS 账户的权限。通过使用该具有权限的 DBMS 账户，您可以在部署期间创建 Kaspersky Next XDR Expert 组件所需的数据库和其他 DBMS 账户。
		• `password` — 具有权限的内部 DBMS 账户的密码。
		• `fqdn:port` — 安装 DBMS 的目标主机的 FQDN 和连接端口。
		要使用高可用性集群，请按如下方式指定此参数：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`
		要使用 Corosync/Pacemaker，请按如下方式使用虚拟 IP 指定此参数：
		`psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>`
		`psql_dsn` 参数值必须符合 URI 格式。如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使用百分号编码进行编码。
		“`psql_dsn`”参数值中必须替换的符号：
		• 空格 → `%20`
		• ! → `%21`
		• # → `%23`
		• % → `%25`
		• & → `%26`
		• / → `%2F`
		• : → `%3A`
		• = → `%3D`
		• ? → `%3F`
		• @ → `%40`
		• [→ `%5B`
		•] → `%5D`
		详情请参阅“PostgreSQL 连接字符串”一文。

`nwc-language`	是	OSMP 控制台界面的语言是默认指定的。安装完成后，您可以更改 OSMP 控制台语言。 可能的参数值： • `enUS`（默认值） • `ruRu` 如果未在配置文件中指定此参数，则使用默认值。
`ingress_ip`	是	Kubernetes 集群网关的预留静态 IPv4 地址。 Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。网关必须与主和工作节点位于同一子网中。
`ssh_pk`	是	位于管理员主机上的 SSH 密钥的私钥部分的路径，用于通过 KDT 连接到主工作线程节点和部署 KUMA 服务的节点（收集器、关联器和存储）。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。

参数名称	是否必需	Description
admin_password	是	"admin_password"参数指定 KDT 在安装期间创建的 Kaspersky Next XDR Expert 用户账户的密码。此账户的默认用户名是"admin"。 主管理员角色已分配给此用户账户。 密码必须符合以下规则： • 用户密码不能少于10个字符或超过256个字符。 • 密码必须包含以下组中三组的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密码不得包含任何空格或".@"组合。 当您手动指定"admin_password"参数值（而不是通过"部署向导"）时，请确保该值符合 YAML 标准对字符串中值的要求： • 包含特殊字符的参数值必须用单引号括起来。 • 参数值中的任何单引号（'）必须成对输入，才能实现该单引号的转义。 例如：用户账户密码"Any_pass%1234'5678"90"必须指定为"admin_password"参数的值"'Any_pass%1234''5678"90'"。
low_resources	否	用于指示在计算资源有限的目标主机上安装 Kaspersky Next XDR Expert 的参数。对于多节点部署，请将 low_resources 参数设置为 false。 可能的参数值： • true — 计算资源有限时的安装（适用于单节点部署） • false — 标准安装（默认值）
core_disk_request	是	指定运行 KUMA Core 所需的磁盘空间量的参数。 如果未指定 core_disk_request 参数，并且 low_resources 参数设置为 false 或未指定，则 KUMA Core 运行所需的默认磁盘空间量为 100 GB。 如果未指定 core_disk_request 参数，并且 low_resources 参数设置为 true，则 KUMA Core 运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 core_disk_request 参数。
metrics_disk_request	是	指定 Metrics 服务运行所需的磁盘空间量的参数。 如果未指定 metrics_disk_request 参数，并且 low_resources 参数设置为 false 或未指定，则 Metrics 服务运行所需的默认磁盘空间量为 80 GB。 如果未指定 metrics_disk_request 参数，并且 low_resources 参数设置为 true，则 Metrics 服务运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 metrics_disk_request 参数。
inventory	是	位于管理员主机上的 KUMA 清查文件的路径。清查文件包含用于部署 Kubernetes 集群中未包含的 KUMA 服务的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。如果所有 KUMA 服务都将安装在集群内，请将 inventory 参数设置为 /dev/null。
host_inventory	否	位于管理员主机上的附加 KUMA 清查文件的路径。此文件包含用于部分添加或删除搭载 KUMA 服务的主机的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果要执行 Kaspersky Next XDR Expert 的初始部署或运行需要配置文件的自定义操作，请保留默认参数值 (/dev/null)。
license	否	位于管理员主机上的KUMA授权许可密钥的路径。 参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 部署完成并登录OSMP后，您可以上传授权许可密钥或指定激活码。

参数名称	是否必需	Description
nwc_host flow_host hydra_host login_host ksc_host console_host api_host kuma_host monitoring_host xdr_edr_ingress_host	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的主机名。服务主机名和域名（smp_domain 参数值）是服务 FQDN 的一部分。 如果未指定自定义主机名，则使用以下默认主机名： • nwc_host—"console" • flow_host—"console" • hydra_host—"console" • login_host—"console" • ksc_host—"admsrv" • console_host—"console" • api_host—"api" • kuma_host—"kuma" • monitoring_host—"monitoring" • xdr_edr_ingress_host—"agentserver"
smp_domain	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的域名。参数值必须满足四级及以下域名的命名要求。 服务主机名和域名是服务 FQDN 的一部分。例如，如果 console_host 变量的值为 console，并且 smp_domain 变量的值为 smp.local，则提供对 OSMP 控制台的访问权限的服务的完整名称为 console.smp.local。
pki_host_list	是	需为其生成自签名证书或自定义证书的 Kaspersky Next XDR Expert 公共服务的主机名称列表。参数值必须是主机名列表，以空格分隔。
intermediate_enabled	否	该参数指示是否对公共 Kaspersky Next XDR Expert 服务使用自定义中间证书，而非自签名证书。 可能的参数值： • true — 使用自定义中间证书。 • false — 使用自签名证书（默认值）。
intermediate_bundle	否	用于访问公共 Kaspersky Next XDR Expert 服务的自定义中间证书的路径。如果"intermediate_enabled"参数设置为"true"，则指定此参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。自定义中间证书的有效期必须为 399 天或更长。
admsrv_bundle api_bundle console_bundle kuma_bundle monitoring_bundle	否	用于使用相应公共 Kaspersky Next XDR Expert 服务的自定义叶证书路径：<admsrv_host>.<smp_domain>、<api_host>.<smp_domain>、<kuma_host>.<smp_domain>、<monitoring_host>.<smp_domain> 和 <console_host>.<smp_domain>。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果要指定自定义叶证书，请将 intermediate_enabled 参数设置为 false，并且不要指定 intermediate_bundle 参数和 pki_host_list 参数。
ksc_state_size	是	分配用于存储管理服务器数据（更新、安装包和其他内部服务数据）的可用磁盘空间量。以千兆字节为单位，格式指定为"<数值>Gi"。所需的可用磁盘空间量取决于受管理设备的数量和其他参数，并且可以进行计算。 默认值是 30 GB。如果未在配置文件中指定此参数，则使用此值。
prometheus_size	是	分配用于存储指标的可用磁盘空间量。以千兆字节为单位，格式指定为"<数值>GB"。 推荐的最小值和默认值是 5 GB。如果未在配置文件中指定此参数，则使用默认值。
grafana_admin_user	否	用于通过 Grafana 工具查看 OSMP 指标的账户的用户名。 值必须符合以下规则： • 用户名长度必须为 1 到 30 个字符。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (_ - .) • 用户名必须以字母开头。 • 用户名不得包含空格或"@"符号。

参数名称	是否必需	Description
grafana_admin_password	否	用于通过 Grafana 工具查看 OSMP 指标的账户密码。 密码必须符合以下规则： • 用户密码不能少于 8 个字符或超过 256 个字符。 • 密码必须包含以下各组中的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
loki_size	是	分配用于存储 OSMP 日志的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。 推荐的最小值和默认值是 40 GB。如果未在配置文件中指定此参数，则使用默认值。
loki_retention_period	是	OSMP 日志的存储期限，超过此期限后，日志将自动删除。默认值为 72 小时（将配置文件中的参数值设置为“<时间（小时）>h”。例如，“72h”）。如果未在配置文件中指定此参数，则使用默认值。
file_storage_cp	否	分配给用于存储组件数据以处理响应操作的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。推荐的最小值为 20 GB。
psql_tls_off	否	该参数指示是否使用 TLS 协议对 Kaspersky Next XDR Expert 组件和 DBMS 之间的流量进行加密。如果 DBMS 安装在集群之外，则默认禁用 TLS 加密（默认值为 “true”）。 可能的参数值： • true — 不加密流量（默认值）。 • false — 加密流量。
psql_trusted_cas	否	可包含 DBMS 服务器 TLS 证书或可颁发该 TLS 服务器证书的根证书的 PEM 文件路径。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果将在单独的服务器上安装和配置 DBMS，并且已启用流量加密（“psql_tls_off”设置为“false”），请指定“psql_trusted_cas”参数。
proxy_enabled	否	该参数指示是否使用代理服务器将 Kaspersky Next XDR Expert 组件连接到互联网。如果安装了 Kaspersky Next XDR Expert 的主机可以访问互联网，您还可以为 Kaspersky Next XDR Expert 组件（例如，管理服务器）的运行以及卡巴斯基和第三方的特定集成提供互联网访问权限。要建立代理连接，您还必须在管理服务器属性中指定代理服务器参数。 可能的参数值： • true—使用代理服务器。 • false—不使用代理服务器（默认值）。
proxy_addresses	否	代理服务器的 IP 地址。如果代理服务器使用多个 IP 地址，请指定这些地址并用空格分隔（例如“0.0.0.0 0.0.0.1 0.0.0.2”）。如果“proxy_enabled”参数设置为“true”，请指定此参数。
proxy_port	否	将建立代理服务器连接的端口号。如果“proxy_enabled”参数设置为“true”，请指定此参数。
console_port	否	用于指定连接到 OSMP 控制台服务器所用的自定义端口号的参数。默认值是 443。
as_smp_port	否	用于指定 Endpoint Agent 连接到 agentserver 组件所用的自定义端口号的参数。默认值是 443。
kuma_gateway_telemetry_listener_port	否	用于指定发送遥测数据所用的自定义端口号的参数。默认值是 443。
trace_level	否	管理服务器跟踪文件的详细程度。在管理服务器运行期间会写入跟踪信息。 默认值为 0，不写入任何跟踪信息。 可能的参数值：0 – 5。 参数值越高，跟踪详情越详细。

参数名称	是否必需	Description
`ansible_extra_flags`	否	KDT 执行的 KUMA Core 和 KUMA 服务部署日志的详细程度。 可能的参数值： • `-v` • `-vv` • `-vvv` • `-vvvv` 标志中"v"字母的数量越多，日志的详细程度就越高。如果配置文件中未指定此参数，则保存标准组件安装日志。
`incident_attachments_max_count_limit`	否	您可以附加到事故的文件数。默认值为 `100`。
`incident_attachments_max_size_limit`	否	附加到该事故的文件的总大小。该值以字节为单位。在指定时不带计量单位。默认值为 `26214400`。
`ignore_precheck`	否	该参数用于指示部署前是否检查 Kubernetes 集群节点的硬件、软件和网络配置是否符合安装该解决方案的先决条件。 可能的参数值： • `true`—跳过预检查。 • `false`—执行预检查（默认值）。
`airgap_mode`	否	指示是否执行APT软件包管理器预检查和更新软件包缓存的参数。这可让您在物理隔离环境中部署Kaspersky Next XDR Expert。 可能的参数值： • `true`—跳过预检查和软件包缓存更新。 • `false`—执行预检查并更新软件包缓存（默认值）。
`grafana_smtp_host`	否	Grafana的SMTP服务器地址，用于发送有关Kubernetes集群运行状况事件的电子邮件通知。请以 `<host>:<port>` 格式指定此参数，例如 `localhost:25`。
`grafana_smtp_user`	否	用于SMTP服务器身份验证的用户名。
`grafana_smtp_password`	否	用于SMTP服务器身份验证的密码。
`grafana_smtp_bundle`	否	包含X.509证书链的文件，用于验证与SMTP服务器的TLS连接。
`grafana_smtp_skip_verify`	否	指示是否跳过SMTP服务器的TLS证书验证的参数。 可能的参数值： • `true`—跳过TLS证书验证。 • `false`—执行TLS证书验证（默认值）。
`grafana_smtp_from_address`	否	发件人的电子邮件地址，该地址将显示在发送电子邮件通知的"发件人"字段中。
`grafana_smtp_from_name`	否	在电子邮件通知中显示发件人的姓名。
`grafana_smtp_ehlo_identity`	否	连接到SMTP服务器时，EHLO命令中使用的标识符。
`grafana_starttls_policy`	否	连接到SMTP服务器时，使用STARTTLS的策略。 可能的参数值： • `OpportunisticStartTLS`—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器。 • `MandatoryStartTLS`—要求使用STARTTLS；如果SMTP服务器不支持STARTTLS，则连接失败。 • `NoStartTLS`—不使用STARTTLS；请在不加密的情况下连接到SMTP服务器。 • `empty`—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器（默认值）。
`grafana_smtp_enable_tracing`	否	指示是否启用SMTP连接跟踪以调试电子邮件发送的参数。 可能的参数值： • `true`—启用SMTP连接跟踪。 • `false`—禁用SMTP连接跟踪（默认值）。

参数名称	是否必需	Description
autodeploy_plan	否	该参数标明是为Kaspersky EDR还是为KASPERSKY NGFW部署KUMA服务。 可能的参数值： • edr—在 Kubernetes 集群内部署用于 OSMP 和 Kaspersky EDR 的 KUMA 服务（默认值）。 • ngfw—在 Kubernetes 集群内部署用于 OSMP 和 Kaspersky NGFW 的 KUMA 服务。此外，预定义的收集器 **[OOTB] Kaspersky NGFW** 将安装在 KUMA 清单文件的 kuma_collector 参数指定的主机列表中的第一个主机上。 • none—不部署用于 Kaspersky EDR 或 Kaspersky NGFW 的 KUMA 服务。在部署不含用于 Kaspersky EDR 和 Kaspersky NGFW 的 KUMA 服务的 Kaspersky Next XDR Expert 时，或从备份恢复 Kaspersky Next XDR Expert 时，请指定此值。恢复 Kaspersky Next XDR Expert 时指定 edr 或 ngfw，可能会导致已部署的服务与备份副本中的服务发生冲突。
tokenhub_access_token	否	访问令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可能值为 5m，最大值为 2h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 应用程序部署后，您可以更改 tokenhub_access_token 参数。
tokenhub_refresh_token	否	用于获取新访问令牌的刷新令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可能值为 12h，最大值为 4320h。 默认值为 24h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署后更改 tokenhub_refresh_token 参数。
credentials_session_ttl	否	单点登录会话的最大空闲时间。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可能值为 5m，最大值为 96h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署后更改 credentials_session_ttl 参数。

单节点部署：指定安装程序参数

用于在单个节点上部署Kaspersky Next XDR Expert的配置文件包含多节点和单节点部署所需的安装参数。此外，此配置文件还包含仅适用于单节点部署的参数（openbao_ha_mode、openbao_standalone 和 default_class_replica_count）。

配置文件模板 (singlenode.smp_param.yaml.template) 位于压缩文件（包含 KDT 实用程序）的分发包中。您可以手动填写配置文件模板；或者使用"部署向导"来指定 Kaspersky Next XDR Expert 部署所需的安装参数，然后生成配置文件。

配置文件模板中并未包含下面列出的所有参数。此模板仅包含在部署 Kaspersky Next XDR Expert 之前必须指定的参数。其余参数设置为默认值，不包含在模板中。您可以手动将这些参数添加到配置文件中以覆盖其原有值。参数值必须遵循下面描述的规则。在部署 Kaspersky Next XDR Expert 期间，KDT 会检查是否正确指定了所需的安装参数。如果配置文件中所需的参数缺失或无效，部署将会中断。

Kaspersky Next XDR Expert 单节点部署配置文件示例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
```

```
project: xdr
# Node on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
  # Primary/worker node settings.
    # 节点名称。 该值的长度必须在 1 到 63 个字符之间。
    # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
    and hyphen (-).
  - desc: cdt-1
    # The node type.
    # 对于单节点部署，请将“type”设置为“primary-worker”。 在这种情况下，目标主机将充当主节点和工
    作节点。
    type: primary-worker
    # The IP address of the node.
    # The primary worker node must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.42
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
        # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
        9), and hyphen (-).
        user: root
        # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
        # password: pass
# Parameters for the Kaspersky XDR deployment
parameters:
  # The connection string for access to the DBMS that is installed and configured on a
  separate server.
  # user_db – 具有权限的内部 DBMS 账户的用户名。 此账户被授予创建数据库和其他 DBMS 账户的权限。
  # password_db–The password of the privileged internal DBMS account.
  # fqdn_db:port_db is the fully qualified domain name and connection port of the
  separate server on which the DBMS is installed.
  # “psql_dsn” 参数值必须符合 URI 格式。 如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使
  用百分号编码进行编码。
  - name: psql_dsn
    source:
      value: "postgres://postgres:password@dbms.example.com:1234"
  # IP address of the Kubernetes cluster gateway
  # The Kubernetes cluster gateway is intended for connecting to the Kaspersky XDR
  components installed inside the Kubernetes cluster.
  # The gateway must be included in the same subnet as the primary worker node.
  - name: ingress_ip
    source:
      value: 10.80.23.182
  # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
  # The parameter value must be a Linux file path or Base64-encoded file content.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky XDR user account that will be created during the
  installation.
  # The password must be 10 to 256 characters long.
  # It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
  numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \
  ` ~ " ( ) ;).
```

```
# The password must not contain either whitespaces or ".@".
- name: admin_password
  source:
    value: ""
# The parameter indicating that Kaspersky XDR is installed on the target host with
limited computing resources.
# For the single-node deployment, set the 'low_resources' parameter to "true" so that
Kaspersky Next XDR Expert components will require less memory and CPU resources.
# Also, if you enable this parameter, 4 GB of free disk space will be allocated to
install KUMA Core on the target host.
- name: low_resources
  source:
    value: "true"
# The number of disk volumes that are used to store the service data of Kaspersky XDR
components and KDT.
# For the single-node deployment, set the parameter value to "1".
- name: default_class_replica_count
  source:
    value: "1"
# The parameter that indicates whether to run the secret storage in the High
Availability (HA) mode.
# For the single-node deployment, set the parameter value to "false".
- name: openbao_ha_mode
  source:
    value: "false"
# The parameter that indicates whether to run the secret storage in the standalone
mode.
# For the single-node deployment, set the parameter value to "true"&period;
- name: openbao_standalone
  source:
    value: "true"
# KUMA 清单文件的路径，该文件包含部署 KUMA 服务所需的安装设置。 此文件位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Kaspersky Endpoint Detection and Response 授权许可密钥的路径。 此文件位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: license
  source:
    value: "/home/user/license.key"
# 域名。 参数值必须满足二级域名的命名要求。
# The service host name and domain name are parts of FQDNs of the Kaspersky XDR
services.
# Default values of service host names: nwc_host—"console", flow_host—"console",
hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host—"console",
api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom device names can be specified in the configuration file.
# 示例：console.smp.local 是提供对 OSMP 控制台的访问权限的服务的 FQDN。 此 FQDN 由
“console_host”和“smp_domain”设置的值组成。
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom
certificate must be generated.
# 参数值必须是主机名列表，以空格分隔。 如果未指定自定义主机名，则使用以下默认主机名：
- name: pki_host_list
  source:
```

```
    value: "admsrv api console kuma monitoring"
- name: autodeploy_plan
  source:
    value: "edr"
# The user name of the account used to view OSMP metrics through the Grafana tool.
# The user name must be 1 to 30 characters long.
# A user name can contain lowercase letters ('a' to 'z'), numerals ('0' to '9') and
special characters (_ -.)&period;
# A user name must begin with a letter and may not contain spaces or the "@" character.
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# The password of the account used to view OSMP metrics through the Grafana tool.
# The password must be 8 to 256 characters long.
# It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' ,
&period; ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

为了使 KDT 与配置文件正确运行，请在文件末尾添加一个空行。

配置文件的nodes部分包含下表列出的目标主机参数。

节点部分

参数名称	是否必需	Description
desc	是	节点名称。 值必须符合以下规则： • 节点名称的长度必须在1到63个字符之间。 • 节点名称可以包含以下字符： • 大写 ASCII 字母 (A-Z) • 小写 ASCII 字母 (a-z) • 数字 (0-9) • 连字符 (-) 所有集群节点必须具有唯一的名称。这一要求是安装Kaspersky Next XDR Expert的先决条件之一，并经KDT验证。
type	是	节点类型。 对于目标主机，将type参数设置为primary-worker，以启用**单节点部署**。在这种情况下，目标主机将充当主节点和工作线程节点。
host	是	节点的 IP 地址。 主工作线程节点必须与 Kubernetes 集群网关位于同一子网中。 节点需要 IPv4 地址。KDT 会自动禁用集群节点上的 IPv6。
kuma_role	否	可以指定在工作节点上安装的 KUMA 服务。 KUMA服务（收集器、关联器和存储）可以完全安装在集群内的工作线程节点上，完全安装在Kubernetes集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。如果所有 KUMA 服务都将安装在集群内，请将 inventory 参数设置为 /dev/null。 对于**单节点部署**，请将此参数留空，因为所有服务都将安装在单个节点上。

参数名称	是否必需	Description
`user`	是	在目标主机上创建、供 KDT 连接节点时使用的账户用户名。 值必须符合以下规则： • 用户名长度必须在 1 到 31 个字符之间。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 下划线 (_)、连字符 (-)
`password`	否	连接节点的密码。可以代替由 `ssh_pk` 参数指定的 SSH 密钥。

其他安装参数列在配置文件的“`parameters`”部分，并在下表中说明。

参数部分

参数名称	是否必需	Description

`psql_dsn`	是	用于访问在 Kubernetes 集群外部安装和配置的 DBMS 的连接字符串。
		此参数指定如下：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`
		其中：
		• `dbms_username` — 具有权限的内部 DBMS 账户的用户名。此账户被授予创建数据库和其他 DBMS 账户的权限。通过使用该具有权限的 DBMS 账户，您可以在部署期间创建 Kaspersky Next XDR Expert 组件所需的数据库和其他 DBMS 账户。
		• `password` — 具有权限的内部 DBMS 账户的密码。
		• `fqdn:port` — 安装 DBMS 的目标主机的 FQDN 和连接端口。
		如果您的 DBMS 与 Kubernetes 集群节点安装在同一主机上，请勿在 `psql_dsn` 参数中将 `localhost` 或 `127.0.0.1` 用作 DBMS 地址。请使用可通过集群网络访问的主机IP地址（而非环回地址）。
		要使用高可用性集群，请按如下方式指定此参数：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`
		要使用 Corosync/Pacemaker，请按如下方式使用虚拟 IP 指定此参数：
		`psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>`
		`psql_dsn` 参数值必须符合 URI 格式。如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使用百分号编码进行编码。
		“`psql_dsn`”参数值中必须替换的符号：
		• 空格 → `%20`
		• ! → `%21`
		• # → `%23`
		• % → `%25`
		• & → `%26`
		• / → `%2F`
		• : → `%3A`
		• = → `%3D`
		• ? → `%3F`
		• @ → `%40`
		• [→ `%5B`
		•] → `%5D`
		详情请参阅“PostgreSQL 连接字符串”一文。

`nwc-language`	是	OSMP 控制台界面的语言是默认指定的。安装完成后，您可以更改 OSMP 控制台语言。 可能的参数值： • `enUS`（默认值） • `ruRu` 如果未在配置文件中指定此参数，则使用默认值。

参数名称	是否必需	Description
`ingress_ip`	是	Kubernetes 集群网关的预留静态 IPv4 地址。 Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。网关必须与主工作线程节点位于同一子网中。 Kubernetes 集群网关需要 IPv4 地址。KDT 会自动在集群节点上禁用 IPv6。 此参数的值不能是执行部署的同一主机的IP地址。
`ssh_pk`	是	位于管理员主机上的 SSH 密钥的私钥部分的路径，用于通过 KDT 连接到主工作线程节点和部署 KUMA 服务的节点（收集器、关联器和存储）。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。
`admin_password`	是	"`admin_password`"参数指定 KDT 在安装期间创建的 Kaspersky Next XDR Expert 用户账户的密码。此账户的默认用户名是"admin"。 主管理员角色已分配给此用户账户。 密码必须符合以下规则： • 用户密码不能少于10个字符或超过256个字符。 • 密码必须包含以下组中三组的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密码不得包含任何空格或".@"组合。 当您手动指定"`admin_password`"参数值（而不是通过"部署向导"）时，请确保该值符合 YAML 标准对字符串中值的要求： • 包含特殊字符的参数值必须用单引号括起来。 • 参数值中的任何单引号（'）必须成对输入，才能实现该单引号的转义。 例如：用户账户密码"`Any_pass%1234'5678"90`"必须指定为"`admin_password`"参数的值"`'Any_pass%1234''5678"90'`"。
`low_resources`	是	该参数用于指示在计算资源受限的环境中将 Kaspersky Next XDR Expert 安装到目标主机上。 可能的参数值： • `true` — 计算资源有限时的安装（适用于单节点部署） • `false` — 标准安装 对于**单节点部署**，将 `low_resources` 参数设置为 `true`，这样 Kaspersky Next XDR Expert 组件将需要更少的内存和 CPU 资源。此外，如果启用了此参数，将分配 4 GB 的可用磁盘空间以在目标主机上安装 KUMA Core。
`openbao_ha_mode`	是	该参数用于指示是否以高可用 (HA) 模式运行密钥存储。 可能的参数值： • `true` • `false` 对于**单节点部署**，将 `openbao_ha_mode` 参数设置为 `false`。
`openbao_standalone`	是	该参数用于指示是否以独立模式运行密钥存储。 可能的参数值： • `true` • `false` 对于**单节点部署**，将 `openbao_standalone` 参数值设置为 `true`。
`default_class_replica_count`	是	存储 Kaspersky Next XDR Expert 组件和 KDT 的服务数据所使用的磁盘卷数量。 默认值为 `3`。 对于**单节点部署**，将 `default_class_replica_count` 参数值设置为 `1`。
`core_disk_request`	是	指定运行 KUMA Core 所需的磁盘空间量的参数。 如果未指定 `core_disk_request` 参数，并且 `low_resources` 参数设置为 `false` 或未指定，则 KUMA Core 运行所需的默认磁盘空间量为 100 GB。 如果未指定 `core_disk_request` 参数，并且 `low_resources` 参数设置为 `true`，则 KUMA Core 运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 `core_disk_request` 参数。

参数名称	是否必需	Description
metrics_disk_request	是	指定 Metrics 服务运行所需的磁盘空间量的参数。 如果未指定 metrics_disk_request 参数，并且 low_resources 参数设置为 false 或未指定，则 Metrics 服务运行所需的默认磁盘空间量为 80 GB。 如果未指定 metrics_disk_request 参数，并且 low_resources 参数设置为 true，则 Metrics 服务运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 metrics_disk_request 参数。
inventory	是	位于管理员主机上的 KUMA 清查文件的路径。清查文件包含用于部署 Kubernetes 集群中未包含的 KUMA 服务的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。如果所有 KUMA 服务都将安装在集群内，请将 inventory 参数设置为 /dev/null。
host_inventory	否	位于管理员主机上的附加 KUMA 清查文件的路径。此文件包含用于部分添加或删除搭载 KUMA 服务的主机的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果要执行 Kaspersky Next XDR Expert 的初始部署或运行需要配置文件的自定义操作，请保留默认参数值(/dev/null)。
license	否	位于管理员主机上的KUMA授权许可密钥的路径。 参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 部署完成并登录OSMP后，您可以上传授权许可密钥或指定激活码。
nwc_host flow_host hydra_host login_host ksc_host console_host api_host kuma_host monitoring_host xdr_edr_ingress_host	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的主机名。服务主机名和域名（smp_domain 参数值）是服务 FQDN 的一部分。 如果未指定自定义主机名，则使用以下默认主机名： • nwc_host—"console" • flow_host—"console" • hydra_host—"console" • login_host—"console" • ksc_host—"admsrv" • console_host—"console" • api_host—"api" • kuma_host—"kuma" • monitoring_host—"monitoring" • xdr_edr_ingress_host—"agentserver"
smp_domain	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的域名。参数值必须满足四级及以下域名的命名要求。 服务主机名和域名是服务 FQDN 的一部分。例如，如果 console_host 变量的值为 console，并且 smp_domain 变量的值为 smp.local，则提供对 OSMP 控制台的访问权限的服务的完整名称为 console.smp.local。
pki_host_list	是	需为其生成自签名证书或自定义证书的 Kaspersky Next XDR Expert 公共服务的主机名称列表。参数值必须是主机名列表，以空格分隔。
intermediate_enabled	否	该参数指示是否对公共 Kaspersky Next XDR Expert 服务使用自定义中间证书，而非自签名证书。 可能的参数值： • true — 使用自定义中间证书。 • false — 使用自签名证书（默认值）。
intermediate_bundle	否	用于访问公共 Kaspersky Next XDR Expert 服务的自定义中间证书的路径。如果"intermediate_enabled"参数设置为"true"，则指定此参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。自定义中间证书的有效期必须为 399 天或更长。
admsrv_bundle api_bundle console_bundle kuma_bundle monitoring_bundle	否	用于使用相应公共 Kaspersky Next XDR Expert 服务的自定义叶证书路径：<admsrv_host>.<smp_domain>、<api_host>.<smp_domain>、<kuma_host>.<smp_domain>、<monitoring_host>.<smp_domain> 和 <console_host>.<smp_domain>。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果要指定自定义叶证书，请将 intermediate_enabled 参数设置为 false，并且不要指定 intermediate_bundle 参数和 pki_host_list 参数。

参数名称	是否必需	Description
`ksc_state_size`	是	分配用于存储管理服务器数据（更新、安装包和其他内部服务数据）的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。所需的可用磁盘空间量取决于受管理设备的数量和其他参数，并且可以进行计算。 默认值是 30 GB。如果未在配置文件中指定此参数，则使用此值。
`prometheus_size`	是	分配用于存储指标的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>GB”。 推荐的最小值和默认值是 5 GB。如果未在配置文件中指定此参数，则使用默认值。
`grafana_admin_user`	否	用于通过 Grafana 工具查看 OSMP 指标的账户的用户名。 值必须符合以下规则： • 用户名长度必须为 1 到 30 个字符。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (_ - .) • 用户名必须以字母开头。 • 用户名不得包含空格或“@”符号。
`grafana_admin_password`	否	用于通过 Grafana 工具查看 OSMP 指标的账户密码。 密码必须符合以下规则： • 用户密码不能少于 8 个字符或超过 256 个字符。 • 密码必须包含以下各组中的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配用于存储 OSMP 日志的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。 推荐的最小值和默认值是 40 GB。如果未在配置文件中指定此参数，则使用默认值。
`loki_retention_period`	是	OSMP 日志的存储期限，超过此期限后，日志将自动删除。默认值为 72 小时（将配置文件中的参数值设置为“<时间（小时）>h”。例如，“72h”）。如果未在配置文件中指定此参数，则使用默认值。
`file_storage_cp`	否	分配给用于存储组件数据以处理响应操作的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。推荐的最小值为 20 GB。
`psql_tls_off`	否	该参数指示是否使用 TLS 协议对 Kaspersky Next XDR Expert 组件和 DBMS 之间的流量进行加密。如果 DBMS 安装在集群之外，则默认禁用 TLS 加密（默认值为 “`true`”）。 可能的参数值： • `true` — 不加密流量（默认值）。 • `false` — 加密流量。
`psql_trusted_cas`	否	可包含 DBMS 服务器 TLS 证书或可颁发该 TLS 服务器证书的根证书的 PEM 文件路径。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果将在单独的服务器上安装和配置 DBMS，并且已启用流量加密（“`psql_tls_off`”设置为“`false`”），请指定“`psql_trusted_cas`”参数。
`proxy_enabled`	否	该参数指示是否使用代理服务器将 Kaspersky Next XDR Expert 组件连接到互联网。如果安装了 Kaspersky Next XDR Expert 的主机可以访问互联网，您还可以为 Kaspersky Next XDR Expert 组件（例如，管理服务器）的运行以及卡巴斯基和第三方的特定集成提供互联网访问权限。要建立代理连接，您还必须在管理服务器属性中指定代理服务器参数。 可能的参数值： • `true`—使用代理服务器。 • `false`—不使用代理服务器（默认值）。

参数名称	是否必需	Description
`proxy_addresses`	否	代理服务器的 IP 地址。如果代理服务器使用多个 IP 地址，请指定这些地址并用空格分隔（例如"`0.0.0.0 0.0.0.1 0.0.0.2`"）。如果"`proxy_enabled`"参数设置为"`true`"，请指定此参数。
`proxy_port`	否	将建立代理服务器连接的端口号。如果"`proxy_enabled`"参数设置为"`true`"，请指定此参数。
`console_port`	否	用于指定连接到 OSMP 控制台服务器所用的自定义端口号的参数。默认值是 443。
`as_smp_port`	否	用于指定 Endpoint Agent 连接到 agentserver 组件所用的自定义端口号的参数。默认值是 443。
`kuma_gateway_telemetry_listener_port`	否	用于指定发送遥测数据所用的自定义端口号的参数。默认值是 443。
`trace_level`	否	管理服务器跟踪文件的详细程度。在管理服务器运行期间会写入跟踪信息。 默认值为 0，不写入任何跟踪信息。 可能的参数值：0 – 5。 参数值越高，跟踪详情越详细。
`ansible_extra_flags`	否	KDT 执行的 KUMA Core 和 KUMA 服务部署日志的详细程度。 可能的参数值： • `-v` • `-vv` • `-vvv` • `-vvvv` 标志中"v"字母的数量越多，日志的详细程度就越高。如果配置文件中未指定此参数，则保存标准组件安装日志。
`incident_attachments_max_count_limit`	否	您可以附加到事故的文件数。默认值为 `100`。
`incident_attachments_max_size_limit`	否	附加到该事故的文件的总大小。该值以字节为单位。在指定时不带计量单位。默认值为 `26214400`。
`ignore_precheck`	否	该参数用于指示部署前是否检查 Kubernetes 集群节点的硬件、软件和网络配置是否符合安装该解决方案的先决条件。 可能的参数值： • `true`—跳过预检查。 • `false`—执行预检查（默认值）。
`airgap_mode`	否	指示是否执行APT软件包管理器预检查和更新软件包缓存的参数。这可让您在物理隔离环境中部署Kaspersky Next XDR Expert。 可能的参数值： • `true`—跳过预检查和软件包缓存更新。 • `false`—执行预检查并更新软件包缓存（默认值）。
`grafana_smtp_host`	否	Grafana的SMTP服务器地址，用于发送有关Kubernetes集群运行状况事件的电子邮件通知。请以 `<host>:<port>` 格式指定此参数，例如 `localhost:25`。
`grafana_smtp_user`	否	用于SMTP服务器身份验证的用户名。
`grafana_smtp_password`	否	用于SMTP服务器身份验证的密码。
`grafana_smtp_bundle`	否	包含X.509证书链的文件，用于验证与SMTP服务器的TLS连接。
`grafana_smtp_skip_verify`	否	指示是否跳过SMTP服务器的TLS证书验证的参数。 可能的参数值： • `true`—跳过TLS证书验证。 • `false`—执行TLS证书验证（默认值）。
`grafana_smtp_from_address`	否	发件人的电子邮件地址，该地址将显示在发送电子邮件通知的"发件人"字段中。
`grafana_smtp_from_name`	否	在电子邮件通知中显示发件人的姓名。
`grafana_smtp_ehlo_identity`	否	连接到SMTP服务器时，EHLO命令中使用的标识符。

参数名称	是否必需	Description
grafana_starttls_policy	否	连接到SMTP服务器时，使用STARTTLS的策略。 可能的参数值： • OpportunisticStartTLS—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器。 • MandatoryStartTLS—要求使用STARTTLS；如果SMTP服务器不支持STARTTLS，则连接失败。 • NoStartTLS—不使用STARTTLS；请在不加密的情况下连接到SMTP服务器。 • empty—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器（默认值）。
grafana_smtp_enable_tracing	否	指示是否启用SMTP连接跟踪以调试电子邮件发送的参数。 可能的参数值： • true—启用SMTP连接跟踪。 • false—禁用SMTP连接跟踪（默认值）。
autodeploy_plan	否	该参数标明是为Kaspersky EDR还是为KASPERSKY NGFW部署KUMA服务。 可能的参数值： • edr—在 Kubernetes 集群内部署用于 OSMP 和 Kaspersky EDR 的 KUMA 服务（默认值）。 • ngfw—在 Kubernetes 集群内部署用于 OSMP 和 Kaspersky NGFW 的 KUMA 服务。此外，预定义的收集器 **[OOTB] Kaspersky NGFW** 将安装在 KUMA 清单文件的 kuma_collector 参数指定的主机列表中的第一个主机上。 • none—不部署用于 Kaspersky EDR 或 Kaspersky NGFW 的 KUMA 服务。将此值用于Kaspersky Next XDR Expert部署，但不包含用于Kaspersky EDR和Kaspersky NGFW的KUMA服务，或用于Kaspersky Next XDR Expert从备份恢复。如果将 edr 或 ngfw 值用于恢复 Kaspersky Next XDR Expert，可能会导致已部署的服务与存储在备份中的服务之间发生冲突。
tokenhub_access_token	否	访问令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可能值为 5m，最大值为 2h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 应用程序部署后，您可以更改 tokenhub_access_token 参数。
tokenhub_refresh_token	否	用于获取新访问令牌的刷新令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可能值为 12h，最大值为 4320h。 默认值为 24h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署后更改 tokenhub_refresh_token 参数。
credentials_session_ttl	否	单点登录会话的最大空闲时间。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可能值为 5m，最大值为 96h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署后更改 credentials_session_ttl 参数。

通过代理节点连接 Endpoint Agent

本节介绍Kaspersky Next XDR Expert端点代理程序及其数据传输目标服务器在不同网络中的部署应用场景。此方法简化了网络配置，同时确保端点代理程序和服务器之间可靠的连接。

在此方案中，来自端点代理程序的数据通过中间代理节点路由。这样，代理节点和解决方案之间只需建立一条网络连接，而无需从每个端点代理程序建立多条连接。此方法适用于 Kaspersky Next XDR Expert 的单节点和多节点部署。

本节介绍如何在Linux设备上设置Nginx代理服务器。如有需要，您可以使用其他支持 mTLS 直通的代理服务器以及其他操作系统。

此场景使用在解决方案部署期间指定的示例公共 Kaspersky Next XDR Expert 服务的 FQDN（`<agentserver>.<smp_domain>`、`<ksc_host>.<smp_domain>` 和 `<kuma_host>.<smp_domain>`）、文件路径和目录路径。您应该将这些值替换为与您的基础设施对应的值。

如果您更改了 Endpoint Agent 用于连接到 agentserver 组件的端口，还应在 Nginx 配置文件中指定新的端口号。

部署步骤

通过中间代理节点配置来自端点代理程序数据的部署分几个步骤：

1. **安装和配置 Nginx**

   在位于端点代理程序所在的同一网络（子网）的服务器上安装Nginx代理服务器。

   1. 运行以下命令：

      ```
      sudo apt update
      sudo apt install nginx-full
      ```

   2. 确保 Nginx 中包含并加载了 `stream`、`stream_ssl` 和 `stream_ssl_preread` 模块：

      ```
      nginx -V 2>&1 | grep -E 'stream|stream_ssl|stream_ssl_preread
      ```

      命令输出必须包含 `stream`、`stream_ssl` 和 `stream_ssl_preread` 模块。

      服务器上安装了包含 `stream`、`stream_ssl` 和 `stream_ssl_preread` 模块的 Nginx 代理服务器。

   3. 确保 Nginx 配置文件（默认为 /etc/nginx/nginx.conf）包含 `stream {}` 块，并且在此块中配置了 `stream.d` 目录的连接。如果缺少 `stream` 块，请在与 `http {}` 块相同的级别添加此块：

      ```
      /etc/nginx/nginx.conf
      ...
      http {
          ...
      }
      stream {
          include /etc/nginx/stream.d/*.conf;
      }
      ```

   4. 根据以下模板，在 /etc/nginx/stream.d/ 目录中创建或编辑 CONF 格式的 Nginx 配置文件。

      如果 /etc/nginx/stream.d/ 目录不存在，请创建该目录。

      Nginx 配置文件的路径和名称：/etc/nginx/stream.d/asproxy.conf。

      模板变量（使用与您的基础架构相对应的值）：

      Endpoint Agent 与之通信的 Kaspersky Next XDR Expert 公共服务的 FQDN 主机名：

      - `<agentserver>.<smp_domain>` – 允许通过代理集成对资产执行响应操作的组件的 FQDN。
      - `in.<some_symbols>.<kuma_host>.<smp_domain>` – 用于遥测的目标后端服务器的 FQDN。

如何获取服务器地址

1. 在主菜单中，前往“**监控 → 资源和服务 → 服务管理操作 → 活动服务**”。
2. 在服务列表中找到**[OOTB] Kaspersky EDR**服务，选中它，然后点击菜单中的**部署**。
3. 在打开的窗口中，复制**API网关URL**字段中的服务器地址。
   服务器名称应采用以下格式：`in.blh4zjhm4edckdt8qyprkpm2b.kuma_host.smp_domain`。

- `<ksc_host>.<smp_domain>` – 用于代理管理的目标后端服务器的 FQDN。它可以是用于 Endpoint Agent 管理的 OSMP 组件的 FQDN，也可以是辅助 KSC 服务器的 FQDN。

IP 地址：

- `<ingress_ip>` – OSMP 集群 Ingress 的 IP 地址。
- `<ksc_ip>` – 辅助 OSMP 或 KSC 服务器的 IP 地址（如果使用）。

连接 Endpoint Agent 有三种方式：

- 通过策略。在这种情况下，请在 Nginx 代理服务器上配置 Endpoint Agent 与服务器之间通信的代理转发：指定 `<ksc_host>.<smp_domain>` 以及 TCP 13000、TCP 14000 和 TCP 13292 端口。

  示例

```
# ----- SNI → upstream -------------------------------------------------
map_hash_bucket_size 256;
map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    <ksc_host>.<smp_domain>          ksc_ingress;
    default                           deny-backend;
}
# ----- Backends-------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream ksc-ingress {
    server <ingress_ip>:13000;
    server <ingress_ip>:14000;
    server <ingress_ip>:13292;
}
upstream deny-backend {
    server 127.0.0.1:1;
}
# ----- Logging--------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;
# ----- Timeouts-------------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;
# ----- Server (port 443) ---------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    listen 13000;
    listen 14000;
    listen 13292;
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

- 通过辅助 OSMP 或 KSC 服务器上的策略。在这种情况下，请在 Nginx 代理服务器上配置 Endpoint Agent 与服务器之间通信的代理转发：指定 `<ksc_host>.<smp_domain>` 以及 TCP 13000、TCP 14000 和 TCP 13292 端口。

  示例

```
# ----- SNI → upstream ------------------------------------------------
map_hash_bucket_size 256;
map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    <ksc_host>.<smp_domain>          ksc_ingress;
    default                           deny-backend;
}
# ----- Backends------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream ksc-ingress {
    server <ksc_ip>:13000;
    server <ksc_ip>:14000;
    server <ksc_ip>:13292;
}
upstream deny-backend {
    server 127.0.0.1:1;
}
# ----- Logging-------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;
# ----- Timeouts------------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;
# ----- Server (port 443) --------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    listen 13000;
    listen 14000;
    listen 13292;
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

- 在本地。在这种情况下，无需在 Nginx 代理服务器上配置 `<ksc_host>.<smp_domain>` 和 TCP 端口。有关更多信息，请参见此场景的步骤 3。

  示例

```
# ----- SNI → upstream ------------------------------------------------
map_hash_bucket_size 256;
map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    default                           deny-backend;
}
# ----- Backends------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream deny-backend {
    server 127.0.0.1:1;
}
# ----- Logging-------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
```

```
error_log  /var/log/nginx/passthrough_error.log notice;
# ----- Timeouts -------------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;
# ----- Server (port 443) ----------------------------------------------
server {
    listen 443;                 # regular TCP-port, no  TLS termination
    ssl_preread on;             # reads only ClientHello
    proxy_pass $upstream_osmp;  # var from map
}
```

5. 检查 Nginx 配置：

```
nginx -t
```

测试成功时的命令输出：

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

6. 重启 Nginx 以应用配置文件中的更改：

```
nginx -s reload
```

已安装的 Nginx 代理服务器已配置为 Endpoint Agent 的数据代理。

2 配置 Nginx 代理节点与 Kaspersky Next XDR Expert 之间的网络连接

1. 配置网络连接。确保网络设置（防火墙、路由）允许从代理节点通过 TCP 13000、TCP 14000、TCP 13292 和 TCP 443 端口与 OSMP 平台以及辅助 OSMP 或 KSC 服务器建立出站连接。
2. 配置网络，以便将从 Endpoint Agent 节点发送到 `<smp_domain>` 的请求路由到代理节点。

3 配置Kaspersky Endpoint Security for Windows端点代理程序以使用代理节点

1. 配置网络连接。确保网络设置（防火墙、路由）允许 Endpoint Agent 通过 TCP 13000、TCP 14000、TCP 13292 和 TCP 443 端口与代理节点建立出站连接。
2. 下载以下 OSMP 证书：
   - certificate.pem – 响应服务器证书
   - certificate.pfx – 端点代理证书
   - [OOTB] Kaspersky EDR – 遥测服务器证书
3. 将证书文件复制到安装了端点代理的服务器（在本节示例中为 C:\Users\TestUser\）。
4. 以管理员权限打开命令提示符 `cmd.exe`。

5. 转到包含端点代理可执行文件的目录，然后运行以下命令：

```
./avp.com EDREXPERTONPREM `
/SET /mode=EDRExpertOnPrem `
/servers=<agentserver>.<smp_domain>:443 `
/server-certificate=C:\Users\TestUser\certificate.pem `
/client-certificate=C:\Users\TestUser\certificate.pfx `
/client-certificate-password=client certificate password`
/telemetry-servers=in.blh4zjhm4edckdt8qyprkpm2b.<kuma_host>.<smp_domain>:443 `
/telemetry-server-certificate='C:\Users\TestUser\[OOTB] Kaspersky EDR' `
/telemetry-client-certificate=C:\Users\TestUser\certificate.pfx `
/telemetry-client-certificate-password=client certificate password
```

6. 如果 Kaspersky Next XDR Expert 尚未启动，请将其启动：

```
./avp.com start EDREXPERTONPREM
```

有关使用命令行配置 Endpoint Agent 的更多信息，请参阅Kaspersky Endpoint Security文档。

Kaspersky Next XDR Expert 部署向导

为部署 Kaspersky Next XDR Expert 准备环境涉及多个手动步骤，例如：配置安装参数、准备目标主机以及验证系统要求。部署向导允许您指定部署 Kaspersky Next XDR Expert 所需的安装参数，然后生成配置文件。可选安装参数使用默认值，并且在部署向导中不可用。您可以手动将这些参数添加到配置文件以覆盖其默认值。

部署向导会自动检查目标主机是否已准备好进行部署，包括 SSH 连接、所需端口的可用性、IP 地址唯一性、集群节点上的 DNS 名称解析以及时间同步。如果检测到任何问题，该向导会显示描述该问题的错误消息。所有检查都成功完成后，您可以保存生成的配置文件，或直接继续部署 Kaspersky Next XDR Expert。

> 部署向导目前仅支持单节点部署。

先决条件

- 安装数据库管理系统

  在以单节点配置部署 Kaspersky Next XDR Expert 之前，您必须在目标主机上手动安装 DBMS。DBMS 和 Kaspersky Next XDR Expert 组件安装在同一主机上，但 DBMS 部署在 Kubernetes 集群之外。

- 执行管理员、目标主机和KUMA 主机所需的所有准备步骤（如果 KUMA 服务将安装在集群外部的独立服务器上）。

过程

要使用部署向导指定安装参数：

1. 在 KDT 实用程序所在的管理员主机上，使用以下命令运行部署向导：

```
./kdt wizard -k <path_to_transport_archive> -o <path_to_configuration_file>
```

其中：

- `<path_to_transport_archive>` 是 传输压缩文件的路径。这是一个可选参数，您可以稍后指定。
- `<path_to_configuration_file>` 是您要保存配置文件的路径和配置文件名。这是一个可选参数，您可以稍后指定。

部署向导会提示您指定安装参数。

如果您没有指定目录的写入权限，或者此目录中存在同名文件，则会发生错误并且向导会终止。

2. 输入传输压缩文件的路径。

   如果您在启动部署向导时指定了此参数，则会自动填充。

3. 输入配置文件路径。

   参数值必须是 Linux 文件路径或 Base64 编码的文件内容。如果您在启动部署向导时指定了此参数，则会自动填充。

4. 输入主工作节点的 IPv4 地址（配置文件的 `host` 参数）。

   该节点必须与集群网关 IP 地址位于同一子网中。

5. 输入 KDT 用于连接主工作节点的账户用户名（即配置文件中的 `user` 参数）。

   值必须符合以下规则：

   - 用户名长度必须在 1 到 31 个字符之间。
   - 用户名可以包含以下字符：
     - 小写字母 (a-z)
     - 数字 (0-9)
     - 下划线 (_)、连字符 (-)

6. 输入用于连接节点的密码（即配置文件中的 `password` 参数）。

   可以使用密码代替 SSH 密钥。

7. 输入 SSH 私钥的路径（即配置文件中的 `key` 参数）。

   SSH 私钥位于管理员主机上，KDT 使用该私钥连接主工作节点。默认值为 `/root/.ssh/id_rsa`。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。

   可以使用 SSH 密钥代替密码来连接节点。建议使用 SSH 密钥与节点建立连接。

8. 输入用于访问 DBMS 的连接字符串（即配置文件中的 `psql_dsn` 参数）。

   按如下方式指定此参数：`postgres://<dbms_username>:<password>@<fqdn>:<port>`

   其中：

   - `dbms_username` — 具有权限的内部 DBMS 账户的用户名。此账户被授予创建数据库和其他 DBMS 账户的权限。通过使用该具有权限的 DBMS 账户，您可以在部署期间创建 Kaspersky Next XDR Expert 组件所需的数据库和其他 DBMS 账户。
   - `password` — 具有权限的内部 DBMS 账户的密码。

- `fqdn:port` — 安装 DBMS 的目标主机的 FQDN 和连接端口。

  对于单节点部署，如果 DBMS 与 Kubernetes 集群节点安装在同一主机上，请勿在连接字符串中使用 `localhost` 或 `127.0.0.1` 作为 DBMS 地址。应使用主机的FQDN或IP地址。

> 部署向导仅为 DBMS 安装在 Kubernetes 集群外部的部署选项指定安装参数。

9. 输入位于管理员主机上的 KUMA 清查文件的路径（配置文件的 `inventory` 参数）。

   KUMA 清查文件包含用于部署未包含在 Kubernetes 集群中的 KUMA 服务的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。

   如果KUMA 服务安装在 Kubernetes 集群中，请指定路径 `/dev/null`。

10. 选择 OSMP Console 的界面语言。安装后，您可以更改 OSMP Console 语言（配置文件的 `nwc-language` 参数）。

    可能值：

    - enUS
    - ruRu

11. 输入 KDT 在安装过程中创建的 Kaspersky Next XDR Expert 用户账户的密码（配置文件的 `admin_password` 参数）。

    此账户的默认用户名是“admin”。主管理员角色已分配给此用户账户。

    密码必须符合以下规则：

    - 用户密码不能少于10个字符或超过256个字符。
    - 密码必须包含以下组中三组的字符：
      - 大写字母 (A-Z)
      - 小写字母 (a-z)
      - 数字 (0-9)
      - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
    - 密码不得包含任何空格或“.@”组合。

12. 输入Kubernetes集群网关的IPv4地址（配置文件的`ingress_ip`参数）。

    网关必须与主工作线程节点位于同一子网中。

13. 输入用于通过 Grafana 工具查看 OSMP 指标的账户的用户名（配置文件的 `grafana_admin_user` 参数）。

值必须符合以下规则：

- 用户名长度必须为 1 到 30 个字符。
- 用户名可以包含以下字符：
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (_ - .)
- 用户名必须以字母开头。
- 用户名不得包含空格或“@”符号。

14. 输入用于通过 Grafana 工具查看 OSMP 指标的账户的密码（配置文件的 `grafana_admin_password` 参数）。
    密码必须符合以下规则：
    - 用户密码不能少于10个字符或超过256个字符。
    - 密码必须包含以下组中三组的字符：
      - 大写字母 (A-Z)
      - 小写字母 (a-z)
      - 数字 (0-9)
      - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
    - 密码不得包含空格或“.@”。
15. 跳过指定 `extended_incident_lifecycle` 参数的步骤。这是一个服务参数。默认情况下，`extended_incident_lifecycle` 参数已禁用，请勿更改。
16. 输入公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的域名（配置文件的 `smp_domain` 参数）。
    参数值必须满足二级域名的命名要求。
17. 输入公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的主机名（配置文件的 `nwc_host`、`flow_host`、`hydra_host`、`login_host`、`ksc_host`、`console_host`、`api_host`、`kuma_host`、`monitoring_host`、`xdr_edr_ingress_host` 参数）。
    如果未指定自定义主机名，则使用以下默认主机名：
    - `nwc_host—"console"`
    - `flow_host—"console"`
    - `hydra_host—"console"`
    - `login_host—"console"`
    - `ksc_host—"admsrv"`

- `console_host–"console"`
- `api_host–"api"`
- `kuma_host–"kuma"`
- `monitoring_host–"monitoring"`
- `xdr_edr_ingress_host–"agentserver"`

服务主机名和域名（`smp_domain` 参数值）是服务 FQDN 的一部分。

18. 选择 `Validate` 以验证生成的配置文件，或选择 `Skip` 以在不验证的情况下继续。
19. 选择 `Save and exit` 以使用指定参数将生成的配置文件保存为 YAML 格式。其他安装参数包含在配置文件中，均采用默认值。您可以在部署 Kaspersky Next XDR Expert 之前手动编辑配置文件。选择 `Install` 以使用此配置文件开始部署 Kaspersky Next XDR Expert。

部署向导会使用指定参数将配置文件保存为 YAML 格式，并开始部署 Kaspersky Next XDR Expert。

Kaspersky Next XDR Expert 安装

Kaspersky Next XDR Expert 是使用 KDT 部署的。KDT 会自动部署 Kubernetes 集群，Kaspersky Next XDR Expert 组件和其他基础架构组件均安装于该集群中。Kaspersky Next XDR Expert 安装过程的步骤不取决于所选的部署选项。

如果需要使用 Kaspersky Next XDR Expert 实例安装多个 Kubernetes 集群，可以使用所需数量的上下文。

要安装 Kaspersky Next XDR Expert：

1. 在管理员主机上使用 KDT 解压下载的分发包。
2. 阅读包含 Kaspersky Next XDR Expert 组件的分发包中的 KDT 最终用户授权许可协议 (EULA)。

   当您开始使用 KDT 时，即表示您接受 KDT 的 EULA 条款。

   您可以在部署 Kaspersky Next XDR Expert 后阅读 KDT 的 EULA。`license_kdt.txt` 文件位于运行 Kaspersky Next XDR Expert 部署的用户的 `~/kaspersky_eula` 目录中。
3. 在安装过程中，KDT 会从操作系统存储库下载缺失的软件包。在安装 Kaspersky Next XDR Expert 之前，请在目标主机上运行以下命令，以确保 apt/yum 缓存是最新的。

   ```
   apt update
   ```
4. 重启目标主机。
5. 在管理员主机上，运行以下命令，使用 KDT 开始部署 Kaspersky Next XDR Expert。指定包含 Kaspersky Next XDR Expert 组件的传输压缩包路径以及您之前填写的配置文件路径（多节点和单节点部署的安装参数集不同）。

   ```
   chmod +x kdt
   ./kdt apply -k <full_path_to_transport_archive> -i <full_path_to_configuration_file>
   ```

如果您使用 `--accept-eula` 标志，则在安装 Kaspersky Next XDR Expert 时，系统不会提示您阅读 EULA 的条款和 OSMP 的隐私策略。在这种情况下，您必须在部署 Kaspersky Next XDR Expert 之前阅读 EULA 和 OSMP 的隐私策略。这些文件位于包含 Kaspersky Next XDR Expert 组件的分发包中。

如果您想在部署过程中阅读并接受 EULA 和隐私策略的条款，请不要使用“`--accept-eula`”标志。

如果使用 KDT 部署 Kaspersky Next XDR Expert 时发生错误，请通过指定不带 `-i` 标志的配置文件路径来重新启动部署。

6. 如果您在上一步中没有使用 `--accept-eula` 标志，请阅读 EULA 和 OSMP 的隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   a. 如果您理解并接受 EULA 的条款，请输入“`y`”。

      如果您不接受 EULA 的条款，请输入“`n`”。

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

      如果您不接受隐私策略的条款，请输入“`n`”。

      > 要使用 Kaspersky Next XDR Expert，您必须接受 EULA 和隐私策略的条款。

   在您开始部署后，KDT 会检查 Kubernetes 集群节点的硬件、软件和网络配置是否满足安装解决方案的先决条件。如果所有严格的预检查都成功完成，KDT 会在目标主机上的 Kubernetes 集群内部署 Kaspersky Next XDR Expert 组件。否则，部署将会中断。如果需要，您可以跳过部署前的预检查（将 `ignore_precheck` 安装参数设置为 `true`）。

   此外，KDT 还会检查所需的安装参数是否正确指定。如果配置文件中所需的参数缺失或无效，部署将会中断。安装参数值应遵循的规则在配置文件模板（multinode.smp_param.yaml.template 和 singlenode.smp_param.yaml.template）中指定。

   > 在 Kaspersky Next XDR Expert 部署期间，将在主管理服务器上创建一个新用户。为了开始配置 OSMP Console，该用户被分配了以下角色：根租户中主管理员的 XDR 角色和 Kaspersky Security Center 主管理员的角色。

7. 使用 KDT 实用程序查看目录中 Bootstrap 组件的安装日志，并获取有关 Kaspersky Next XDR Expert 组件的诊断信息（如需要）。

8. 登录OSMP控制台。

   OSMP Console 地址为 `https://<console_host>.<smp_domain>:443`。

   地址由配置文件中指定的 `console_host` 和 `smp_domain` 参数值组成。

Kaspersky Next XDR Expert 部署在目标主机上。安装 KUMA 服务以开始使用该解决方案。

为目标主机配置互联网访问

如果您组织的基础设施使用代理服务器访问互联网，并且您需要将目标主机连接到互联网，则必须在部署 Kaspersky Next XDR Expert 之前，将每个目标主机的 IP 地址添加到 /etc/environment 文件中的 `no_proxy` 变量中。这使您可以将目标主机直接连接到互联网，并正确部署 Kaspersky Next XDR Expert。

要配置目标主机的互联网访问：

1. 在目标主机上，使用文本编辑器打开 /etc/environment 文件。例如，以下命令使用 GNU nano 文本编辑器打开该文件：

   ```
   sudo nano /etc/environment
   ```

2. 在 /etc/environment 文件中，将目标主机的 IP 地址添加到 `no_proxy` 变量中，用逗号分隔且不加空格。

   例如， `no_proxy` 变量初始可指定如下：

   ```
   no_proxy=localhost,127.0.0.1
   ```

   您可以将目标主机的 IP 地址 (192.168.0.1) 添加到 `no_proxy` 变量中：

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.1
   ```

   或者，您可以指定包含目标主机的子网（采用 CIDR 表示法）：

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.0/24
   ```

3. 保存 /etc/environment 文件。

4. 重启目标主机：

   ```
   reboot
   ```

将/etc/environment文件中的IP地址添加到每个目标主机并重新启动它们后，您可以继续准备目标主机和进一步部署Kaspersky Next XDR Expert。

在计算机上同步时间

要在计算机上配置时间同步：

1. 运行以下命令以安装 chrony：

   ```
   sudo apt install chrony
   ```

2. 将系统时间配置为与 NTP 服务器同步：

   a. 确保虚拟机可以访问互联网。

   如果可以访问，请转到步骤 b。

   如果无法访问互联网，请将 `/etc/chrony.conf` 文件中的当前公共源（以 `pool` 开头）替换为您组织的内部 NTP 服务器的名称或 IP 地址。

   b. 通过执行以下命令启动系统时间同步服务：

   ```
   sudo systemctl enable --now chrony
   ```

   c. 等待几秒钟，然后运行以下命令：

   ```
   sudo timedatectl | grep 'System clock synchronized'
   ```

   如果系统时间同步正确，输出将包含 `System clock synchronized: yes` 行。

同步已配置。

在Kubernetes集群内安装KUMA服务

*服务*是KUMA SIEM系统的主要组成部分，可帮助系统管理事件。服务允许您从事件源接收事件，然后将它们转换为通用格式，以便于查找关联、存储和人工分析。

服务类型：

- 存储用于保存事件。
- 收集器用于接收事件并将其转换为 KUMA 格式。

  如果您计划在基础设施中使用多个租户，请为每个租户创建一个单独的收集器。

- 关联器用于分析事件并搜索定义的模式。
- 代理用于接收远程设备上的事件并将其转发到 KUMA 收集器。

您必须先部署 Kaspersky Next XDR Expert，然后才能安装 KUMA 服务。在 Kaspersky Next XDR Expert 部署期间，将准备所需的基础架构：在准备好的主机上创建服务目录，并将服务安装所需的文件添加到这些目录中。建议按以下顺序安装服务：存储、收集器、关联器和代理。

限制

在Kubernetes集群中安装KUMA服务时，请考虑以下限制：

- 每个安装程序只能部署一个KUMA Core实例。
- 被动式收集器只能在使用启用了TLS的HTTP或TCP连接器时部署。
- 对于被动式HTTP和TCP连接器，配置的服务器地址和端口将自动替换为`0.0.0.0:7310`。
- 存储集群必须完全部署在Kubernetes内部或完全部署在Kubernetes外部。不支持混合部署。
- 如果部署在Kubernetes外部的收集器或关联器向部署在Kubernetes内部的存储服务发送事件，则事件传递将通过单个入口URL进行。Kubernetes在TCP层执行存储节点之间的负载均衡。
- 如果流量必须路由到不同的存储节点组，则需要部署单独的eventRouter服务并通过它们路由流量。
- 当您更改部署在Kubernetes集群内部的收集器的设置时，KUMA不会验证修改后的设置。不正确的设置可能会导致收集器无法接收事件。
- 不能使用相同的**存储节点FQDN值**在单个Kubernetes集群中部署由同一存储资源创建的多个存储服务。

若要在Kubernetes集群中安装和配置KUMA服务：

1. 请按照以下说明之一，确保根据所选部署方案准备好Kaspersky Next XDR Expert的管理员主机和目标主机：
   - 多节点部署：准备管理员和目标主机
   - 单节点部署：准备管理员和目标主机
2. 在OSMP控制台中，为每个KUMA服务（存储、收集器和关联器）创建资源集。
3. 为存储、收集器和关联器创建服务。
4. **将每个服务部署到Kubernetes集群中**。
   1. 在主应用程序窗口中，前往**监控→资源和服务→活动服务**部分。
   2. 选择要部署的服务，然后点击**部署**按钮。
   3. 在**将服务添加到Kubernetes**窗口中，填写以下字段：
      - **存储节点FQDN**：指定存储资源中定义的存储集群节点的名称。此参数仅适用于存储服务，并且在服务部署后无法更改。
      - **存储类别**：选择用于存储服务状态的存储子系统。此参数的值在部署后无法更改。可用值：
        - **Longhorn**— 此存储类别提供支持复制的网络存储。默认情况下，服务状态会复制到三个网络驱动器。推荐将此存储类用于收集器、事件路由器、关联器、指标和Core服务，因为它允许Kubernetes在当前节点发生故障时将服务Pod迁移到另一个工作节点。它还可以用于为部署为单实例的存储服务提供高可用性。
        - **local-path**—此存储类使用挂载在/opt/lvp/hot目录下的Kubernetes工作节点的本地磁盘阵列，并提供最高性能。推荐将此存储类用于存储服务，因为存储支持原生集群，并且不依赖Kubernetes机制来实现高可用性。它还可以用于使用HTTP或TCP连接器的收集器服务，以及从单个KUMA资源创建的多个实例中部署的事件路由器服务。在单节点部署中，推荐所有KUMA服务类型都使用**Local-Path**。
      - **冷存储类别**：选择用于长期数据存储的存储子系统。此参数仅适用于存储服务，部署后无法更改。**local-path-cold**存储类别与**local-path**类似，但专用于在挂载于/opt/lvp/cold目录下的低速磁盘阵列上进行长期存储。
      - **最小CPU**：指定为该服务保留的CPU核心数（线程数）。该值必须是正整数。默认值为 `0`。
      - **最大CPU**：指定服务可用的最大CPU核心数（线程数）。该值必须为正整数，且不能小于**最小CPU**值。默认值为 `0`。
      - **最小RAM**：指定为该服务保留的RAM量（以GB为单位）。该值必须是正整数。默认值为 `0`。
      - **最大RAM**：指定服务可用的最大RAM量（以GB为单位）。该值必须为正整数，且不能小于**最小RAM**值。默认值为 `0`。

- **存储请求**：指定分配给服务的磁盘空间大小（以GB为单位）。只有在使用**longhorn**存储类别时，此参数才可用。
- **冷存储请求**：指定分配给长期数据存储的磁盘空间大小（以GB为单位）。此参数仅适用于使用**longhorn**存储类别的存储服务。

4. 点击**创建服务**按钮。

5. 如有必要，请验证收集器和关联器是否已准备好接收事件。

6. 如有必要，在 KUMA 网络基础设施中安装代理。

   代理安装所需的文件位于`/opt/kaspersky/kuma/utils`目录中。

Kaspersky Next XDR Expert功能所需的KUMA服务安装在Kubernetes集群中。

在 Kubernetes 集群外部安装 KUMA 服务

*服务*是 KUMA 组件的主要组成部分，可帮助系统管理事件。服务允许您从事件源接收事件，然后将它们转换为通用格式，以便于查找关联、存储和人工分析。

KUMA 服务（收集器、关联器和存储）可以完全安装在集群内的工作线程节点上，完全安装在 Kubernetes 集群外的单独主机上，或者部分安装在 Kubernetes 集群内，部分安装在 Kubernetes 集群外。

服务类型：

- 存储用于保存事件。
- 收集器用于接收事件并将其转换为 KUMA 格式。

  > 如果您计划在基础设施中使用多个租户，请为每个租户创建一个单独的收集器。

- 关联器用于分析事件并搜索定义的模式。
- 代理用于接收远程设备上的事件并将其转发到 KUMA 收集器。

您必须先部署 Kaspersky Next XDR Expert，然后才能安装 KUMA 服务。在 Kaspersky Next XDR Expert 部署期间，将准备所需的基础架构：在准备好的主机上创建服务目录，并将服务安装所需的文件添加到这些目录中。建议按以下顺序安装服务：存储、收集器、关联器和代理。

要在 Kubernetes 集群外部安装和配置 KUMA 服务：

1. 在 OSMP 控制台的主菜单中，转到“**设置**” → “**KUMA**”。
2. 在OSMP控制台的KUMA部分，为要在网络基础设施中准备好的主机上安装的每个 KUMA 服务（存储、收集器和关联器）创建一个资源集。
3. 为存储、收集器和关联器创建服务。

4. 获取服务标识符以绑定创建的资源集和 KUMA 服务：

   a. 在 OSMP 解决方案中，转到 **资源** → **活动服务**。

   b. 选择所需的 KUMA 服务，然后单击“**复制 ID**”按钮。

5. 在网络基础设施中准备好的主机上，运行相应的命令来安装 KUMA 服务。使用之前获取的服务标识符：

   - 存储的安装命令：

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the
     KUMA Core CA certificate> --id <service ID> --install
     ```

   - 收集器的安装命令：

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
     the KUMA Core CA certificate> --id <service ID> --api.port <API port>
     ```

   - 关联器的安装命令：

     ```
     sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
     the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
     ```

     其中：

     - <FQDN> 是 KUMA Core 服务器的完全限定域名。
     - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

       `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

       安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

       为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
     - <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
     - <API port> 是用于与已安装组件通信的端口。

   默认情况下，KUMA Core 的 FQDN 为 `<kuma_host>.<smp_domain>`。

   用于连接 KUMA Core 的端口无法更改。默认端口号是 7210。

   开放与服务器上已安装的收集器和关联器对应的端口（TCP 7221，以及作为 `--api.port <port>` 参数值用于安装服务的其他端口）。

6. 在安装 KUMA 服务期间，请阅读 KUMA 的最终用户授权许可协议 (EULA)。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   - 如果您理解并接受 EULA 的条款，请输入“`y`”。
   - 如果您不接受 EULA 的条款，请输入“`n`”。要使用 KUMA 服务，您必须接受 EULA 的条款。

您可以在安装 KUMA 服务后，通过以下方式之一阅读 KUMA 的 EULA：

- 在主机上，它包含在 KUMA 清查文件的 `kuma_utils` 组中：打开位于 `/opt/kaspersky/kuma/utils` 目录中的 LICENSE 文件。
- 在主机上，它包含在 KUMA 清查文件中的其他组（`kuma_storage`, `kuma_collector` 或 `kuma_correlator`）中：打开位于 `/opt/kaspersky/kuma` 目录中的 LICENSE 文件。
- 执行以下命令：

```
/opt/kaspersky/kuma/kuma license --show
```

接受 EULA 后，KUMA 服务将安装在网络基础设施中准备好的主机上。

7. 如有必要，请验证收集器和关联器是否已准备好接收事件。
8. 如有必要，在 KUMA 网络基础设施中安装代理。
   代理安装所需的文件位于 `/opt/kaspersky/kuma/utils` 目录中。

Kaspersky Next XDR Expert 功能所需的 KUMA 服务已安装。

部署多个 Kubernetes 集群和 Kaspersky Next XDR Expert 实例

KDT 允许您部署多个包含 Kaspersky Next XDR Expert 实例的 Kubernetes 集群，并使用上下文在这些集群之间切换。*上下文*是一组访问参数，用于定义用户可以选择与之交互的 Kubernetes 集群。上下文还包括使用 KDT 连接到集群的数据。

先决条件

在创建上下文和安装包含 Kaspersky Next XDR Expert 实例的 Kubernetes 集群之前，您必须执行以下操作：

1. 准备管理员主机和目标主机。
   若要安装多个集群和 Kaspersky Next XDR Expert 实例，您需要为所有集群准备一个管理主机，并为每个集群准备单独的目标主机集。不应在目标主机上安装 Kubernetes 组件。
2. 准备用于安装 KUMA 服务的主机。
   要安装 KUMA 服务，您需要为每个 Kaspersky Next XDR Expert 实例准备单独的主机组。
3. 准备 KUMA 清查文件。
   要安装 KUMA 服务，您需要为每个 Kaspersky Next XDR Expert 实例准备单独的清查文件。
4. 准备配置文件。
   要安装多个集群和 Kaspersky Next XDR Expert 实例，您需要为每个 Kaspersky Next XDR Expert 实例准备配置文件。在这些配置文件中，指定相应的管理和目标主机，以及特定集群和 Kaspersky Next XDR Expert 实例专属的其他参数。

Process

要创建包含 Kubernetes 集群和 Kaspersky Next XDR Expert 实例的上下文：

1. 在 KDT 实用程序所在的管理员主机上，运行以下命令并指定上下文名称：

   ```
   ./kdt ctx --create <context_name>
   ```

   将创建具有指定名称的上下文。

2. 安装 Kubernetes 集群和 Kaspersky Next XDR Expert。

   包含 Kaspersky Next XDR Expert 实例的集群将部署在上下文中。上下文创建完成。当您获取 Kaspersky Next XDR Expert 组件的日志文件时，日志文件包含您当前的上下文名称。

您可以重复此过程以创建所需数量的包含已安装集群和 Kaspersky Next XDR Expert 实例的上下文。

创建上下文后，必须部署 Kubernetes 集群和 Kaspersky Next XDR Expert 实例才能完成上下文创建。如果您不在上下文中执行部署，然后创建了另一个上下文，则第一个上下文将被删除。

要查看已创建的上下文列表和活动上下文名称：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt ctx
```

要切换到所需的上下文：

在 KDT 实用程序所在的管理员主机上，运行以下命令并指定上下文名称：

```
./kdt ctx <context_name>
```

选择上下文后，KDT 将连接到相应的 Kubernetes 集群。现在，您可以使用此集群和 Kaspersky Next XDR Expert 实例。KDT 命令应用于选定的集群。

当您使用 KDT 卸载安装在 Kubernetes 集群中的 Kaspersky Next XDR Expert 组件以及集群本身时，相应的上下文也会被删除。其他包含 Kaspersky Next XDR Expert 实例的上下文及其集群不会被删除。

在物理隔离环境中安装和更新 Kaspersky Next XDR Expert

Kaspersky Next XDR Expert 可以在物理隔离环境中安装或升级。使用kdt-airgap-preparation实用程序在物理隔离环境中进行安装和更新，包括以下阶段：

1. 准备管理员和目标主机，以及配置文件。
2. 获取位于物理隔离环境中的目标主机上安装的软件包的信息

   此信息与所需软件包列表进行比较，并将有关目标主机上缺少的内容的信息保存到YAML库存文件中。

3. 从开放环境中的公共互联网存储库或企业镜像存储库下载库存文件中指定的所需软件包及其依赖项。

   下载的包会被保存到本地的TAR软件包存档中。

4. 从本地TAR存档中安装或更新软件包及其对物理隔离环境中目标主机的依赖项。

5. 在物理隔离环境中安装或升级 Kaspersky Next XDR Expert

准备管理员主机和目标主机

您需要根据所选的部署方案，确定要部署 Kubernetes 集群以及该集群中所含 Kaspersky Next XDR Expert 组件的目标设备数量。按照以下指南之一准备管理员主机和目标主机，以便部署 Kaspersky Next XDR Expert（忽略涉及下载和安装软件包的步骤）：

- 多节点部署：准备管理员和目标主机
- 单节点部署：准备管理员和目标主机

以 YAML 格式准备配置文件。该配置文件包含要部署的目标主机列表以及 Kaspersky Next XDR Expert 组件的一组安装参数。

使用包含特定于所选部署方案的安装参数的配置文件：

- 多节点部署：指定安装参数
- 单节点部署：指定安装程序参数

> 在物理隔离环境中部署 Kaspersky Next XDR Expert 时，请将 `airgap_mode` 安装参数设置为 `true`。

获取位于物理隔离环境中的目标主机上安装的软件包的信息

若要获取有关目标主机的操作系统和已安装软件包的信息：

1. 在管理员主机上，运行以下命令。指定位于管理员主机上的用于连接到目标主机的SSH私钥的路径、您之前填写的配置文件的路径以及将保存信息的库存文件的路径：

   `kdt-airgap-preparation scan -k <ssh密钥的完整路径> -c <配置文件的完整路径> --airgap -i <清查文件的完整路径>`

   kdt-airgap-preparation实用程序将信息与所需软件包列表进行比较，并将有关目标主机上缺少的内容的信息保存到YAML清查文件中。YAML清查文件保存到指定目录中，并指定名称。

如果您需要检查目标主机上的其他软件包，例如Docker，请运行以下命令：

`kdt-airgap-preparation scan -k <ssh密钥的完整路径> -c <配置文件的完整路径> --airgap -i <清查文件的完整路径> --add-pkgs <软件包名称>`

有关未在目标主机上安装的其他软件包的信息已添加到YAML清查文件中。

创建的清查文件将用于从公共互联网存储库或开放环境中的公司镜像存储库下载目标主机的缺失软件包。如果发生错误，kdt-airgap-prepare实用程序将退出，并将相应的错误消息发送到日志文件和stdout。

在开放环境中下载所需的软件包

若要下载库存文件中指定的所需软件包：

1. 将YAML清查文件复制到可移动驱动器，然后将文件移动到开放环境中的管理员主机。
2. 在管理员主机上，运行以下命令。指定库存文件的路径和应保存所需缺失软件包的软件包存档的路径：

   `kdt-airgap-preparation pull -n <库存文件的完整路径> -a <软件包存档的完整路径>`

   kdt-airgap-preparation实用程序下载库存文件中列出的软件包及其依赖项，并将软件包保存到TAR软件包存档中。软件包存档以指定的名称保存到指定的目录中。
3. 将清查文件添加到软件包存档中。

创建的软件包存档将用于在物理隔离环境中的目标主机上安装缺失的所需软件包。如果出现错误，kdt-airgap-preparation实用程序将终止并将相应的错误消息输出到日志文件和stdout。

在物理隔离环境中的目标主机上安装或更新软件包

若要安装或更新软件包及其对目标主机的依赖项：

1. 将TAR软件包存档复制到可移动驱动器，然后将存档移动到物理隔离环境中的管理员主机。
2. 在管理员主机上，运行以下命令。指定TAR软件包存档的路径和位于管理员主机上的SSH私钥的路径，用于连接到目标主机：

   `kdt-airgap-preparation install -a <软件包存档的完整路径> -k <SSH密钥的完整路径>`

Kdt-airgap-preparation实用程序使用库存文件和软件包存档在目标主机上安装或更新所需的软件包。

准备好目标主机后，安装或升级Kaspersky Next XDR Expert。

部署前的基础架构就绪度预检查

在您开始部署 Kaspersky Next XDR Expert 后，KDT 会检查 Kubernetes 集群节点的硬件、软件和网络配置是否满足安装该解决方案的先决条件。对集群的每个节点执行预检查。

所有检查分为两组：

- 严格检查

  检查对 Kaspersky Next XDR Expert 的运行至关重要的参数。如果此检查失败，部署将中断。
- 非严格检查

  检查不影响 Kaspersky Next XDR Expert 运行的参数。如果此检查失败，部署将继续。

执行以下预检查：

- 硬件：
  - 磁盘上的可用空间足以进行部署。
  - CPU 配置符合要求。
  - 可用 RAM 空间足以进行部署。
  - CPU 支持 AVX、SSE 4.2 和 BMI 指令。
  - `/tmp` 目录中的可用磁盘空间量必须至少等于传输压缩文件的大小（对于管理员主机，严格检查）。
- 软件：
  - 操作系统及其版本符合要求。
  - 内核版本符合要求。
  - Systemctl 已安装并可用（严格检查）。
  - 软件包管理器缓存更新可用（严格检查）。
  - 节点上已安装正确版本的必需软件包（严格检查）。
  - 节点上未安装禁用软件包（docker 和 podman）（严格检查）。
  - 缺少过时的 k0s 二进制文件（严格检查）。
  - 缺少过时的 k0s 配置文件（严格检查）。
  - PostgreSQL或Postgres Pro DBMS服务器参数符合要求（严格检查）。
- 网络：
  - 所有集群节点都位于同一个广播域中。
  - 所有集群节点都有唯一的名称（配置文件的 `desc` 参数）（严格检查）。
  - 自定义证书文件对指定域有效，并包含加密私钥（严格检查）。
  - 自定义中间证书的有效期为399天或以上（严格检查）。
  - 自定义叶证书的有效期为399天或以上（严格检查）。
  - 节点上的 DNS 名称解析可用（严格检查）。
  - 集群节点上的时间同步已配置（严格检查）。
  - 所有节点上的本地时间相差不超过 5 秒（严格检查）。
  - 所需端口可用。

如果所有严格的预检查都成功完成，KDT 会在目标主机上的 Kubernetes 集群内部署 Kaspersky Next XDR Expert 组件。所有通过和失败的检查结果都保存在每个节点的 /tmp/k0s_report.txt 文件中。如果需要，您可以跳过部署前的预检查（将 `ignore_precheck` 安装参数设置为 `true`）。

Kaspersky Next XDR Expert组件的安装前完整性检查

收到包含Kaspersky Next XDR Expert组件的传输归档后，您可以验证其真实性和完整性。传输归档中的每个组件（CNAB）都包含一个XML格式的清单文件。该清单文件包含组件校验和，并使用GOST R 34.11-2012的256位算法进行数字签名。此数字签名既确保组件文件校验和的有效性，也确保清单中的校验和未被更改。

您可以验证组件的校验和是否与清单中指定的校验和匹配。这确认组件未被修改，并且来自可信来源。

要检查Kaspersky Next XDR Expert组件的完整性：

1. 解压传输归档。
2. 从包含提取的组件及其清单的目录中运行以下命令之一：

   - 验证单个组件

     指定清单文件名称以验证相应的组件。`integrity_checker`实用程序验证指定清单文件的数字签名：

     ```
     ./integrity_checker --signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
     <CNAB_manifest_file.xml>
     ```

   - 验证所有组件

     `integrity_checker`实用程序验证所有清单文件的数字签名：

     ```
     find . -type f -iname "*.xml" -print0 | xargs -0 -I {} echo --manifest {} | xargs ./integrity_checker --
     signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
     ```

成功进行完整性检查后的命令输出示例

已成功通过验证的清单文件数量显示在`Manifests`行的`succeeded`列中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 0 / 0 / 38
        Files: 0 / 0 / 38
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
SUCCEEDED
```

完整性检查失败后的命令输出示例

在此示例中，清单文件在签名后被修改，或者签名存在问题。跳过的清单文件或验证失败的清单文件的数量显示在`Manifests`行的`failed`列中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 2 / 0 / 36
        Files: 0 / 0 / 0
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
```

```
        Registry values: 0 / 0 / 0
================================================>
FAILED
ERR无法验证文件“/home/xdr_user/integrity_check.xml”的数字签名。 标志：无：0x80000106（对象不受信任）
清单文件/home/xdr_user/integrity_check.xml验证失败。原因：无法验证文件“/home/xdr_user/integrity_check.xml”的数字签名。 标志：无：0x80000106（对象不受信任）
```

Kaspersky Next XDR Expert组件的真实性和完整性已验证。

登录 Kaspersky Next XDR Expert

要登录 Kaspersky Next XDR Expert，您必须知道 OSMP 控制台的 Web 地址。在您的浏览器中，JavaScript 必须被启用。

登录 OSMP 控制台：

1. 在您的浏览器中，转到 `https://<console_host>.<smp_domain>:443`。

   OSMP 控制台地址由配置文件中指定的 `console_host` 和 `smp_domain` 参数值组成。

   登录页面显示。

2. 执行以下操作之一：

   - 要使用域用户账户登录 OSMP，请输入域用户的用户名和密码。

     您可以采用以下格式之一输入域用户的用户名：

     - 用户名`@dns.domain`
     - NTDOMAIN\用户名

   - 输入内部用户的用户名和密码。

3. 单击**登录**按钮。

4. 指定移动设备上的身份验证应用程序生成的一次性安全码。

   首次登录时，请为您的帐户配置双重身份验证。如果您无法配置双重身份验证，请联系在**常规功能： 用户权限**功能区域中拥有修改对象ACL权限且已配置双重身份验证的用户，将您的账户添加到双步骤身份验证允许列表中。

5. 如果为您的账户启用了强制更改密码或密码已过期，则会显示密码更改窗口。设置用于登录 OSMP 控制台的新密码。

登录后，将显示仪表板，其中包含您上次登录时使用的语言和主题。

登录尝试次数超出允许范围

OSMP发行包包含一条关联规则*[OOTB]：使用同一帐户多次尝试登录OSMP控制台*。此规则已添加到关联器中，该关联器在OSMP部署期间安装。该规则会在用户三次登录OSMP控制台失败后创建一个关联事件。

生成的关联事件将作为超出允许登录尝试次数警报的依据。

您可以修改允许的密码输入尝试次数。有关详细信息，请参阅以下文章：更改允许的密码输入尝试次数。

域认证

Kaspersky Next XDR Expert 允许您通过 Kerberos 协议使用域身份验证。有关详细信息，请参阅以下文章：配置Kerberos域身份验证。

要退出 OSMP 控制台，请执行以下操作：

在上方窗格中，单击您的帐户名称以打开帐户菜单，然后选择 **登出**。

OSMP 控制台被关闭，且登录页面被显示。

与端点代理的集成

若要集成端点代理，您需要上传OSMP证书，以便在OSMP和端点代理之间建立*受信任连接*。

要获得从端点代理程序接收遥测数据的证书：

1. 在主菜单中，前往**监控→资源和服务→活动服务**。
2. 在服务列表中，右键单击要用于收集端点代理程序发送的遥测数据的收集器，然后从上下文菜单中选择**下载证书**。
   浏览器会将服务器 TLS 证书下载到下载文件夹。

要获取向端点代理程序发送响应的证书：

1. 在主菜单中，前往**设置** → **租户** → 单击租户名称 → **设置** 选项卡 → **证书**。
2. 在**服务器证书**部分，单击**导出**。
   浏览器会将服务器 TLS 证书下载到下载文件夹。

若要获取端点代理TLS证书：

1. 在主菜单中，前往**设置** → **租户** → 单击租户名称 → **设置** 选项卡 → **证书**。
2. 在**端点代理程序**部分，选择当前的TLS证书，然后单击**导出**。
3. 为包含 Endpoint Agent TLS 证书的受密码保护的 PFX 存档指定密码，然后单击“**导出**”。
   浏览器会将 PFX 存档（加密容器）下载到下载文件夹。
   在向Endpoint Agent发送响应和从Endpoint Agent接收遥测数据时，需要使用获得的证书进行双向TLS身份验证。

下载所有必需的证书后，即可创建用于集成端点代理程序的政策。有关如何创建政策和添加证书的详细说明，请参阅端点代理文档：

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

Sandbox 的准备和安装

安装 Sandbox 前的准备工作及安装步骤：

1. 为安装 Sandbox 准备好您的 IT 基础设施。
2. 准备一台虚拟机。
3. 准备安装磁盘映像。
4. 安装 Sandbox。

准备用于 Sandbox 安装的 IT 基础架构

要准备用于 Sandbox 安装的 IT 基础架构：

1. 拒绝管理网络接口和用于对已处理对象进行互联网访问的网络接口访问 Sandbox 服务器的本地网络。
2. 请按如下方式指定与其他组件交互的端口：
   - 入站方向（管理界面）：
     - TCP 22
       通过 SSH 连接到服务器
     - TCP 443
       与OSMP的通信
     - TCP 8443
       访问应用程序的 Web 界面
   - 出站方向（管理界面）：
     - TCP 80 或 TCP 443
       与卡巴斯基更新服务器通信。
   - 出站和相应的入站方向（用于访问已处理对象的接口）：
     任意端口。
     访问互联网以分析已处理对象的网络行为。

     > 拒绝访问企业局域网以保护网络免受被分析对象的攻击。

准备用于安装 Sandbox 的虚拟机

要准备虚拟机以安装 Sandbox 组件：

1. 运行 VMware ESXi hypervisor。
2. 打开虚拟机管理控制台。
3. 在要安装 Sandbox 组件的虚拟机的上下文菜单中，选择“**编辑设置**”。
   虚拟机属性窗口打开。
4. 在**“虚拟硬件”**选项卡上，展开“CPU 设置”组，然后选中**“向来宾操作系统公开硬件辅助虚拟化”**复选框。
5. 在**虚拟机选项**选项卡上的**延迟敏感度**下拉列表中，选择**高**。
6. 单击**确定**。

虚拟机已准备好安装 Sandbox 组件。

准备安装磁盘镜像

在安装 Sandbox 之前，您必须准备一个基于 Astra Linux 操作系统的安装磁盘 ISO 镜像。

可用于创建 iso 镜像的设备的最低硬件要求：

- CPU：4 核，时钟频率 2500 MHz 或更高。
- RAM：8 GB
- 可用磁盘空间：100 GB。

软件要求：

- 基于最新 Linux 内核的操作系统。
- Docker 20 或更高版本。
- Astra Linux特别版1.8.2.8的ISO镜像（以下将该镜像称为astra-installation.iso）。

Kaspersky Next XDR Expert 不支持其他版本的 Astra Linux 操作系统。

要挂载基于 Astra Linux 操作系统的 Sandbox 组件的 iso 镜像，请执行以下操作：

1. 从分发工具包下载以下文件：
   - Sandbox 分发包中的 tar.gz 压缩包
   - 用于创建 ISO 镜像的工具

2. 创建 iso_builder.sh 文件，内容如下：

```
#!/bin/bash
usage="Builds the KEDR install ISO.
Usage:
$(basename "$0") [-h] source_iso distribution iso_builder_image build target_iso_name
where:
    -h, --help        - show this text and exit
    source_iso        - absolute path to the source OS ISO file
    distribution      - absolute path to the KEDR distribution archive
    iso_builder_image - absolute path to the iso_builder docker image
    build             - absolute path to a temporary build directory
    target_iso_name   - absolute path to the resulting ISO file
"
if [ "$#" -eq 0 ] || [ "$1" == "-h" ] || [ "$1" == "--help" ]
then
    echo "$usage"; exit 10;
fi
if [ "$#" -lt 5 ]
then
    echo "错误：参数不足。 请参考帮助文本。"; exit 11;
fi
docker load -i $3
docker run -v $1:$1 -v $2:$2 -v $4:/build kaspersky/kata/deployment/iso_builder:6.0 --source-iso-uri file://$1
--kata-distribution-uri file://$2 --target-iso-name $5
```

3. 执行以下命令：

```
mkdir /var/kedr_builder
```

4. 将步骤 1 中列出的文件和 astra-installation.iso 镜像放入新创建的 /var/kedr_builder 目录中。

5. 执行以下命令：

```
sudo ./iso_builder.sh \
 /var/kedr_builder/astra-installation.iso \
 /var/kedr_builder/kata-sb-distribution-<version>-x86_64_en-ru-zh.tar.gz \
 /var/kedr_builder/iso-builder-<version>-x86_64_en-ru-zh.tar \
 /var/kedr_builder buildSandboxAstra.iso
```

其中<版本>是沙盒的发行版。

安装磁盘映像 buildSandboxAstra.iso 已在 /var/kedr_builder 目录中创建。

如果您将文件保存在不同的目录中，可以运行以下命令：

```
sudo ./iso_builder.sh <source_iso_host_path> <distribution_host_path> <iso_builder_image_host_path>
<build_host_path> <target_iso_name>
```

在上述命令中：

- source_iso_host_path是Astra Linux特别版1.8.2.8的分发工具包的路径。
- distribution_host_path是沙盒分发包的路径。
- iso_builder_image_host_path 是 ISO 构建工具的路径。
- build_host_path 是挂载的 ISO 镜像必须所在的路径，无需指定分配给 ISO 镜像的名称。
- target_iso_name 是分配给 iso 镜像的名称。

安装 Sandbox

要开始 Sandbox 组件的安装：

1. 运行包含 Sandbox 组件的磁盘镜像。
   安装向导启动。
2. 选择“**继续**”，然后按 **Enter** 键。

步骤 1：查看最终用户授权许可协议和隐私策略

要继续安装，您必须阅读并接受 AO Kaspersky Lab 的最终用户授权许可协议和隐私政策的条款和条件（以下分别称为“EULA”和“隐私政策”）。仅当您接受EULA和隐私政策的条款后，安装才能继续进行。

在 Astra Linux 操作系统上，您还需要接受 Astra Linux 操作系统的最终用户授权许可协议。

要接受EULA和隐私政策的条款和条件：

1. 在列表中选择要阅读EULA和隐私政策文本的语言，然后按 **回车键**。
2. 在 Astra Linux 操作系统上，您必须首先接受 Astra Linux 操作系统的最终用户授权许可协议。阅读 EULA。如果您接受其条款和条件，请选择**“我接受”**并按 **Enter** 键。
3. 阅读卡巴斯基的 EULA。如果您接受其条款和条件，请选择**“我接受”**并按 **Enter** 键。
4. 阅读隐私政策。如果您接受其条款和条件，请选择**“我接受”**并按 **Enter** 键。

安装向导将继续执行下一步。

步骤 2：选择用于安装 Sandbox 的磁盘

要选择用于安装组件的磁盘：

1. 选择用于安装组件的建议驱动器之一，然后按 **Enter**。
2. 在确认窗口中，选择“**是**”并按 **Enter**。

安装向导将继续执行下一步。

步骤 3：配置 Sandbox 管理员密码的最小密码长度

要设置 Sandbox 组件的管理员密码的最小长度：

1. 在“**最小密码长度**”中，输入长度（以字符为单位）。
   建议密码长度为 12 个或更多字符。
2. 选择“**确定**”，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 4：创建 Sandbox 管理员账户

要创建 Sandbox 管理员账户：

1. 在“**新用户名**”字段中，输入管理员账户名称。默认使用'admin'账户。
2. 在“**新密码**”字段中，输入管理员账户的密码。
   密码必须符合以下规则：
   - 密码必须至少包含 8 个字符。
   - 密码必须包含至少三种字符：
     - 大写字母 (A-Z)。
     - 小写字母 (a-z)。
     - 数字。
     - 特殊字符。
   - 密码不能与用户名完全或基本相同。
   - 密码不能包含连续三个或更多相同的字符。
3. 在“**确认密码**”字段中，再次输入密码。
4. 选择“**确定**”，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 5.配置管理网络接口

为保证 Sandbox 组件正常运行，必须连接至少两个网卡，并配置以下网络接口：

- 管理网络接口。此接口旨在提供对 Sandbox 服务器的 SSH 访问；Sandbox 服务器也使用此接口接收要扫描的对象。
- 用于对已处理对象进行互联网访问的网络接口。由 Sandbox 处理的对象可以使用此接口尝试在互联网上活动，并且 Sandbox 可以分析其行为。如果阻止互联网访问，则 Sandbox 无法分析互联网上对象的行为，因此将只分析无互联网访问的对象的行为。

  > 用于对已处理对象进行互联网访问的网络接口必须与组织的本地网络隔离。

选择您想要用作管理接口的网络接口并进行配置。

要选择管理网络接口并进行配置：

1. 在网络接口列表中，选择您想要用作管理接口的网络接口。
2. 按下“**Enter**”。
3. 在“**地址**”字段中，输入想要分配给此网络接口的 IP 地址。
4. 在“**网络掩码**”字段中，输入想使用此网络接口的网络掩码。
5. 选择“**确定**”，然后按 **Enter** 键。
6. 选择“**继续**”，然后按 **Enter** 键。

安装向导将继续执行下一步。

步骤 6：分配主机名并添加 DNS 服务器地址

分配 DNS 服务器要使用的服务器主机名并添加 DNS 服务器地址。

要分配服务器主机名并添加 DNS 服务器地址：

1. 在“**DNS 设置**”窗口中，选择“**主机名**”。
2. 在“**主机名**”字段中，输入服务器的完整域名。
   以 FQDN 格式指定服务器名称（例如：host.domain.com 或 host.domain.subdomain.com）。
3. 选择“**确定**”，然后按 **Enter** 键。
4. 在“**DNS 设置**”窗口中，选择“**DNS 服务器**”。
5. 选择“**新建**”，然后按 **Enter** 键。
   DNS 服务器地址条目窗口打开。
6. 在“**DNS 服务器**”文本框中，以 IPv4 格式输入主 DNS 服务器的 IP 地址。
7. 选择“**确定**”，然后按 **Enter** 键。
   DNS 服务器地址条目窗口关闭。
8. 如果要添加其他 DNS 服务器的 IP 地址，请对要添加的每台服务器重复这些说明中的步骤 5 到 7。
9. 添加所有 DNS 服务器后，选择“**返回**”并按 **Enter**。
10. 在“DNS 服务器”窗口中，选择“**继续**”并按 **Enter**。

安装向导将继续执行下一步。

步骤 7：配置静态网络路由

要配置静态网络路由：

1. 在“**IPv4 路由**”窗口中，选择“**新建**”并按 **Enter**。
   “**IPv4 静态路由**”窗口打开。
2. 在**地址/掩码**字段中，输入要为其配置网络路由的子网的 IP 地址和掩码。
3. 如果要使用默认网络路由，请输入**0.0.0.0/0**。
4. 在**网关**字段中，输入网关的 IP 地址。
5. 选择“**确定**”，然后按 **Enter** 键。
6. 如果要添加其他网络路由，请对要添加的每个网络路由重复这些说明中的步骤 1 到 5。
7. 如果您已完成添加网络路由，请单击“**继续**”。

配置可能需要一些时间。然后安装完成。

与 Sandbox 集成

与 Sandbox 集成涉及两个步骤：

1. 在OSMP界面中创建连接到沙盒服务器的请求。
2. 在沙盒网页界面中接受请求。

要通过 OSMP 界面创建到 Sandbox 服务器的连接请求：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   这将打开“租户属性”窗口。
3. 在**设置**选项卡中，转到**“Sandbox 服务器”**部分。
   请注意*OSMP证书指纹*。稍后您需要使用此指纹与沙盒网页界面中显示的指纹进行匹配。
4. 然后单击“**添加**”按钮。
   添加 Sandbox 服务器面板出现在 Web 界面窗口的右侧。
5. 在 **IP** 字段中，输入 Sandbox 服务器的 IP 地址。
6. 点击“**获取证书指纹**”。Kaspersky Next XDR Expert显示*沙盒证书指纹*。稍后您需要使用此指纹与沙盒网页界面中显示的指纹进行匹配。

7. 在**"Sandbox 名称"**字段中，指定要在 OSMP 界面中显示的 Sandbox 组件名称。

8. 单击"**保存**"按钮。

OSMP 向 Sandbox 发送连接请求。现在您需要接受这个请求。

要接受来自 OSMP 的连接请求：

1. 在 Sandbox Web 界面中，转到**"授权"**部分。

2. 比较证书指纹：

   - 在沙盒IP下显示的沙盒证书指纹应与您之前在OSMP界面中获取的沙盒证书指纹相匹配。
   - 在OSMP发出的连接请求列表中，找到OSMP发出的此连接请求。**证书指纹**列包含发送连接请求的OSMP服务器的证书指纹。该证书指纹应与您之前在OSMP界面中获得的OSMP证书指纹相匹配。

3. 要接受连接请求，请单击**接受**。之后，您可以点击**撤销**按钮撤销之前接受的连接请求。

4. 单击"**应用**"。

与 Sandbox 的集成已准备就绪。

Kaspersky Next XDR Expert的高可用性部署

即使部署解决方案的任何Kubernetes集群节点出现故障或失去网络连接，Kaspersky Next XDR Expert的高可用性配置确保了其可以不间断运行。

按照此应用场景，您可以准备您的基础设施，以部署Open Single Management Platform和Kaspersky Next XDR Expert的高可用性配置（包括Kaspersky Endpoint Detection and Response功能）的所有必要组件，准备包含安装参数的配置文件，并使用Kaspersky Deployment Toolkit实用程序（以下简称KDT）部署解决方案。

在部署 Open Single Management Platform 和 Kaspersky Next XDR Expert 组件之前，建议先阅读强化指南。

部署方案分阶段进行：

1. **下载包含 Kaspersky Next XDR Expert 组件的分发包**

   分发包中包含以下组件：

   - 带有Kaspersky Next XDR Expert组件的传输档案、Kaspersky Next XDR Expert的最终用户许可协议和KDT的最终用户许可协议。

     组件使用RSA密钥和GOST R 34.11-2012密钥签名。

   - 包含KDT实用程序、配置文件和KUMA清查文件模板的存档文件

2. **安装数据库管理系统（DBMS）**

   手动将DBMS安装在不包含在Kubernetes集群中的单独服务器上。

   使用受支持的高可用性数据库配置之一：Kaspersky Next XDR Expert的高可用性配置。

3. **准备管理员主机和目标主机**

定义将部署Kubernetes集群和Kaspersky Next XDR Expert组件的目标主机数量。Kaspersky Next XDR Expert的高可用性配置必须至少有7个目标主机。

为部署Kaspersky Next XDR Expert准备管理员主机和目标主机。

操作说明：多节点部署：准备管理员主机和目标主机

4. **准备配置文件**

   以 YAML 格式准备配置文件。该配置文件包含要部署的目标主机列表以及 Kaspersky Next XDR Expert 组件的一组安装参数。

   操作说明：多节点部署：指定安装参数

   您可以手动填写配置文件模板；或者使用"部署向导"来指定 Kaspersky Next XDR Expert 部署所需的安装参数，然后生成配置文件。

   操作指南：使用"配置向导"指定安装参数

5. **部署 Kaspersky Next XDR Expert**

   使用 KDT 部署 Kaspersky Next XDR Expert。KDT 会自动部署 Kubernetes 集群，Kaspersky Next XDR Expert 组件和其他基础架构组件均安装于该集群中。

   操作说明：安装 Kaspersky Next XDR Expert

6. **在Kubernetes集群内安装KUMA服务**

   安装 KUMA 服务（收集器、关联器和存储）。

   操作说明：在Kubernetes集群内安装KUMA服务

7. **添加从属管理服务器（可选）**

   如需进一步集成端点代理程序，必须部署从属管理服务器。

   操作说明：添加从属管理服务器

8. **安装和集成端点代理**

   按照端点代理程序文档中的说明来安装端点代理程序：

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

   配置与端点代理的集成。

9. **安装和集成 Sandbox**

   安装沙盒，进行配置，然后在其中安装虚拟机。之后，配置与沙盒的集成。

   说明：

   - 安装 Sandbox 组件
   - 初始 Sandbox 设置
   - 准备虚拟机以供使用
   - 与 Sandbox 集成

Kaspersky Next XDR Expert 的高可用性配置

即使部署解决方案的任何Kubernetes集群节点出现故障或失去网络连接。，Kaspersky Next XDR Expert的高可用性配置确保了其可以不间断运行和访问数据。

在高可用性配置中，您至少需要7个Kubernetes集群节点：

- 3个主节点（控制平面节点）
- 4个工作线程节点

如果您计划在虚拟化环境中部署Kaspersky Next XDR Expert，其中集群节点作为虚拟机运行，我们建议将虚拟机分布在不同的物理目标主机上。这种方法确保单个物理主机的故障不会影响解决方案中的多个虚拟节点。虚拟机在物理主机上的放置和分布由Hypervisor程序管理。

支持以下高可用性数据库配置：

- Postgres Pro Enterprise BiHA集群
  - 版本： Postgres Pro Enterprise 16或更高版本
  - 集群类型：BiHA
  - 节点数量：3-15
  - 复制类型：同步。
  - 访问DBMS的连接字符串包括集群节点列表（由`psql_dsn`参数指定）：

    ```
    psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>
    ```

- 带有虚拟IP的PostgreSQL集群（Corosync/Pacemaker）
  - 集群类型：带有虚拟IP的PostgreSQL集群（Corosync/Pacemaker）
  - 节点数量：3个或更多
  - 访问DBMS的连接字符串包括DBMS集群的虚拟IP地址（由`psql_dsn`参数指定）：

    ```
    psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>
    ```

支持以下KUMA服务的高可用性配置，这些配置将安装在Kubernetes集群中：

- KUMA存储
  - 工作线程节点数量：3个或更多
  - KUMA存储绑定到这些节点，不得迁移到其他节点。

- KUMA存储直接使用这些节点的磁盘，不使用Longhorn。
- 不允许将由同一KUMA资源创建的KUMA存储放在同一工作线程节点上。此规则确保了所需的容错级别。

- KUMA Core
  - 工作线程节点数量：1个
    Kubernetes机制确保了高可用性；在节点故障的情况下，停机时间约为6分钟。
- KUMA收集器
  有两种高可用性配置：
  - 工作线程节点数量：2个
    节点故障时的停机时间最短。
  - 工作线程节点数量：1个
    Kubernetes机制确保了高可用性；停机时间约为6分钟。
- KUMA关联器
  - 工作线程节点数量：1个
    Kubernetes机制确保了高可用性。节点故障时的停机时间约为6分钟。
- KUMA事件路由器
  有两种高可用性配置：
  - 工作线程节点数量：2个
    节点故障时的停机时间最短。
  - 工作线程节点数量：1个
    Kubernetes机制确保了高可用性。节点故障时的停机时间约为6分钟。
- KUMA指标
  - 工作线程节点数量：1个
    Kubernetes机制确保了高可用性。节点故障时的停机时间约为6分钟。

恢复Kubernetes集群中的故障节点

如果Kubernetes集群节点发生电源或网络故障，但其磁盘数据完好无损且网络名称未更改，则管理员应恢复电源和网络连接。节点恢复运行后，大约会在5-6分钟内自动重新加入集群。

如果节点的磁盘数据损坏或丢失，或者由于故障导致其主机名发生更改，则必须重新配置节点并再次准备将其作为Kubernetes集群的一部分运行，然后再将其重新添加到集群中。

准备并将节点添加到Kubernetes集群中：

1. 准备将作为主节点和工作节点的目标主机。
2. 在管理员主机上，使用以下命令导出当前配置文件：

   ```
   ./kdt ec -e '<configuration_file_name_with_path>'
   ```

   配置文件的当前版本将以指定的名称保存到指定的目录中。
3. 在导出的配置文件的 nodes 部分中，删除故障节点参数并添加已恢复节点参数（`desc`、`type`、`host`、`kind`、`user` 和 `key`）。保存更新的配置文件。
4. 使用 ssh-copy-id 实用程序将公钥复制到每个新节点（例如，复制到 `~/.ssh` 目录）。
5. 在管理员主机上，运行以下命令将修改后的配置文件应用到Kubernetes集群，并指定配置文件的完整路径：

   ```
   ./kdt apply -i '<配置文件完整路径>'
   ```

   执行完毕后，KDT会验证配置文件。然后，它会检查Kubernetes集群节点的硬件、软件和网络配置是否符合安装先决条件。如果所有严格的预检查都成功完成，KDT会向stdout和KDT日志输出成功验证通知。否则，将保存包含验证失败信息的日志，并中断添加新主机的进程。如果需要，可以通过将`ignore_precheck`安装参数设置为`true`来跳过运行命令前的预检查。

恢复的节点随即添加到Kubernetes集群中。KDT将有关恢复节点的信息输出到stdout和KDT日志。

Kaspersky Next XDR Expert的高可用性多站点部署

Kaspersky Next XDR Expert 的高可用性多站点部署通过将 Kubernetes 集群节点分布在多个数据中心来提供容错能力。如果某个数据中心不可用，工作负载会自动转移到另一个数据中心的集群节点，使 Kaspersky Next XDR Expert 能够在中断最小的情况下继续运行。

多站点配置至少需要三个数据中心。在至少三个数据中心部署 Kaspersky Next XDR Expert 可确保在某个数据中心不可用时 Kubernetes 仲裁得以维持。在每个数据中心，必须部署至少四个集群节点：一个主节点和三个工作节点。每个数据中心都使用自己的 Kubernetes 集群网关，并具有专用 IP 地址。目标主机和 Kubernetes 集群网关必须位于数据中心内的同一子网中。

每个数据中心至少需要一台 Sandbox 主机。必须使用客户管理的高可用性负载均衡器，在不同数据中心的集群节点之间分配流量。您还必须将 DBMS 安装在受支持的高可用性配置中。

例如，在包含三个数据中心的多站点配置中，必须至少有 15 台主机：

- Kubernetes 集群中包含 12 台目标主机：
  - 一个主节点，3 个主节点（每个数据中心至少 1 个节点）
  - 9 个工作节点（每个数据中心至少 3 个节点）
- 3 台 Sandbox 主机（每个数据中心至少 1 个节点）

此外，部署还需要一个客户管理的高可用性负载均衡器，以及一个以受支持的高可用性配置部署的 DBMS。

多站点部署限制

- 位于不同数据中心的节点之间的带宽必须至少为 10 Gbps，延迟不得超过 20 毫秒。
- 任意两个数据中心之间的最大距离为 1200 公里（基于同步复制的 20 毫秒延迟要求）。
- 位于不同数据中心的 Kubernetes 集群节点必须能够通过 Kaspersky Next XDR Expert 使用的所有端口进行网络连接。
- 同一数据中心内的所有 Kubernetes 集群节点必须位于同一广播域中。
- 数据库必须以具有同步复制的高可用性配置进行部署，并且仲裁节点必须位于与数据库节点不同的可用区中。

数据中心故障期间的已知问题

- 如果数据中心发生故障，反恶意软件引擎发送到数据中心 Sandbox 进行扫描的文件可能会丢失。此外，Sandbox 中的自动扫描也可能会出现延迟。
- 停机时在数据中心运行的 IRP 任务（包括扫描任务）可能会丢失。将不会收到这些任务的检测结果。
- 当数据中心停机时，由于外部系统中的队列堆积，剩余数据中心的 Sandbox 可能会过载。因此，随着 Sandbox 负载的增加，任务可能会下降。
- 如果发送到数据中心进行扫描的文件因数据中心停机而未得到处理，则这些文件的扫描结果（检测）将丢失，并且这些文件默认情况下可能会被标记为“干净”。如果 Sandbox 满足大小要求，文件丢失和检测可能会持续 15 分钟，否则可能会持续 1 小时。
- 恢复数据中心或添加数据中心以创建多站点部署后，在同步集群数据期间，解决方案可能需要 30–60 分钟才能实现容错。在此期间，解决方案会正常运行，但如果其中一个数据中心离线，则可能会变得不可用。如果数据量大于默认大小，同步可能需要更长时间。数据中心之间的带宽较低或延迟较高也可能延长同步时间。

阶段

根据此场景，您可以准备基础架构，以便在多个数据中心部署 Open Single Management Platform 和 Kaspersky Next XDR Expert 所需的所有组件，准备包含安装参数的配置文件，并使用 Kaspersky Deployment Toolkit 实用程序（以下简称 KDT）部署解决方案。

> 在部署 Open Single Management Platform 和 Kaspersky Next XDR Expert 组件之前，建议先阅读强化指南。

部署方案分阶段进行：

1. **下载包含 Kaspersky Next XDR Expert 组件的分发包**

分发包中包含以下组件：

- 包含Kaspersky Next XDR Expert 组件以及Kaspersky Next XDR Expert和KDT最终用户授权许可协议的传输存档文件

  组件使用RSA密钥和GOST R 34.11-2012密钥签名。您可以验证Kaspersky Next XDR Expert组件的真实性和完整性。

- 包含KDT实用程序、配置文件和KUMA清查文件模板的存档文件

2 安装数据库管理系统（DBMS）

手动在单独的服务器上安装 DBMS，使用以下受支持的高可用性数据库配置之一：Kaspersky Next XDR Expert 的高可用性配置。

DBMS 由客户提供和配置。

3 配置高可用负载均衡器

配置高可用负载均衡器，以在位于多个数据中心的集群节点之间分配传入流量。

负载均衡器由客户提供和配置。

配置文件示例

例如，您可以使用开源 HAProxy 作为负载均衡器。在负载均衡器配置中，为每个数据中心指定 Kubernetes 集群网关 IP 地址（配置文件中的 `ingress_ip` 参数）。

```
global
  log /dev/log  local0
  log /dev/log  local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin
  stats timeout 30s
  user haproxy
  group haproxy
  daemon
defaults
  log  global
  mode  http
  option  httplog
  option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
  errorfile 400 /etc/haproxy/errors/400.http
  errorfile 403 /etc/haproxy/errors/403.http
  errorfile 408 /etc/haproxy/errors/408.http
  errorfile 500 /etc/haproxy/errors/500.http
  errorfile 502 /etc/haproxy/errors/502.http
  errorfile 503 /etc/haproxy/errors/503.http
  errorfile 504 /etc/haproxy/errors/504.http
listen stats
    mode http
    bind *:8080
    stats enable
    stats uri /stats
    stats refresh 10s
#    stats admin if LOCALHOST
frontend http
  mode tcp
  bind :80
  default_backend http_servers
backend http_servers
  mode tcp
  balance first
  option tcp-check
```

```
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:80 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:80 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:80 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend https
  mode tcp
  bind :443
  default_backend https_servers
backend https_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend https9
  mode tcp
  bind :9443
  default_backend https9_servers
backend https9_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:9443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:9443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:9443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend https4
  mode tcp
  bind :4443
  default_backend https4_servers
backend https4_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:4443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:4443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:4443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend ksc13000
  mode tcp
  bind :13000
  default_backend ksc13000
backend ksc13000
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:13000 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:13000 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:13000 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
```

4 准备管理员主机和目标主机

确定每个数据中心中要部署 Kubernetes 集群和 Kaspersky Next XDR Expert 组件的目标主机数量，然后准备管理员主机和目标主机，以部署 Kaspersky Next XDR Expert。

如果您要执行多站点部署，还必须配置 DNS 记录，以便服务 FQDN 解析为客户管理的负载均衡器的 IP 地址。

操作说明：多站点部署：准备管理员主机和目标主机

5. **准备 KUMA 主机以在 Kubernetes 集群外部安装 KUMA 服务（可选）**

KUMA服务（收集器、关联器和存储）可以完全安装在Kubernetes集群内，完全安装在集群外的单独主机上，或者部分安装在集群内，部分安装在集群外。

如果您希望将 KUMA 服务完全安装在 Kubernetes 集群外部的独立主机上，或者部分安装在集群内部，部分安装在集群外部，请准备 KUMA 目标主机以安装 KUMA 服务。

操作指南：准备 KUMA 主机以在 Kubernetes 集群外部通过安装程序安装 KUMA 服务

6. **准备 KUMA 清查文件以在 Kubernetes 集群外部安装 KUMA 服务（可选）**

如果您希望将 KUMA 服务完全安装在 Kubernetes 集群外部的独立主机上，或者部分安装在集群内部，部分安装在集群外部，请准备 YAML 格式的 KUMA 清查文件。KUMA 清查文件包含用于在 Kubernetes 集群外部安装 KUMA 服务的参数。

操作指南：准备 KUMA 清查文件以在 Kubernetes 集群外部安装 KUMA 服务

7. **准备配置文件**

以 YAML 格式准备配置文件。该配置文件包含要部署的目标主机列表以及 Kaspersky Next XDR Expert 组件的一组安装参数。

如果您正在执行多站点部署，还必须指定基础架构区域和数据中心的参数。

操作指南：多站点部署：指定安装参数

8. **部署 Kaspersky Next XDR Expert**

使用 KDT 部署 Kaspersky Next XDR Expert。KDT 会自动部署 Kubernetes 集群，Kaspersky Next XDR Expert 组件和其他基础架构组件均安装于该集群中。

操作说明：安装 Kaspersky Next XDR Expert

9. **安装 KUMA 服务**

安装 KUMA 服务（收集器、关联器和存储）。

KUMA服务可以完全安装在Kubernetes集群内，完全安装在集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。

操作指南：在Kubernetes集群外部安装KUMA服务

操作说明：在Kubernetes集群内安装KUMA服务

10. **添加从属管理服务器**

如需进一步集成端点代理程序，必须部署从属管理服务器。

操作说明：添加从属管理服务器

11. **安装和集成端点代理**

按照端点代理文档中的说明来安装端点代理：

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

配置与端点代理的集成。

12. **安装和集成 Sandbox**

    安装 Sandbox，进行配置，然后在其中安装虚拟机。

    配置与 Sandbox 的集成。

多站点部署：准备管理员主机和目标主机

准备多站点部署包括配置管理员主机和目标主机。准备好主机并指定配置文件后，您将能够使用 KDT 在目标主机上部署 Kaspersky Next XDR Expert。

准备管理员主机

首先需要准备一个设备作为管理员主机，KDT 将从该设备启动。该主机既可以纳入部署期间由 KDT 创建的 Kubernetes 集群，也可以不纳入。如果管理员主机不包含在集群中，它将仅用于部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert。如果管理员主机包含在集群中，它还将充当用于运行 Kaspersky Next XDR Expert 组件的目标主机。

要准备管理员主机：

1. 确保管理员主机上的硬件和软件满足要求。

   如果管理员主机未包含在 Kubernetes集群中，请使用KDT要求。

   如果管理员主机包含在集群中，请使用多节点部署的硬件要求和OSMP的软件要求。

2. 在临时文件目录（默认情况下，`/tmp`）中为 KDT 分配至少 15 GB 的可用空间。如果此目录中没有足够的可用空间，请运行以下命令指定另一个目录的路径：

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. 配置容器运行时。使用以下容器运行时之一：

   - KDT 内置容器运行时（基于 runc）。

     运行以下命令安装内置容器运行时：

     ```
     sudo ./kdt init
     ```

     如果内置容器运行时无法满足您的需求，您可以改用 Docker 容器运行时。

   - Docker 容器运行时。

     安装 Docker 版本 25 的安装包或更高版本，然后执行安装后步骤，以配置管理主机，确保其能与 Docker 正常协同工作。

     用于 Docker 数据存储的磁盘分区（默认情况下为 `/var/lib/docker`）必须至少有 60 GB 的可用空间。

     请勿从操作系统维护者的存储库中安装非官方的 Docker 软件包分发版。

4. 对于将被纳入该集群的管理员主机，请执行额外的准备操作：

   a. 由于该设备将充当管理员主机和目标主机，请确保其满足多节点部署的要求。

   b. 确保管理员主机支持 cgroup v2 技术。

准备目标主机

目标主机是用于部署 Kaspersky Next XDR Expert 的物理机或虚拟机，并包含在 Kubernetes 集群中。Kaspersky Next XDR Expert 组件在这些主机上运行。

> 其中一个目标主机可用作管理员主机。在这种情况下，您必须按照前面的步骤将此主机配置为管理员主机，然后执行目标主机的准备工作。

对于包含三个数据中心的多站点配置，必须至少有 12 个集群节点：

- 一个主节点，3 个主节点（每个数据中心至少 1 个节点）

  主节点用于管理集群、存储元数据和分配工作负载。

- 9 个工作节点（每个数据中心至少 3 个节点）

  工作节点用于执行 Kaspersky Next XDR Expert 组件的工作负载。

集群中的主节点和工作线程节点的数量可能会有所不同。为了在节点之间实现最佳工作负载分配，推荐使用性能大致相同的节点。

KUMA服务（收集器、关联器和存储）可以完全安装在集群内的工作节点上，完全安装在Kubernetes集群外的单独主机上，或者部分安装在Kubernetes集群内，部分安装在Kubernetes集群外。

要准备目标主机：

1. 确保目标主机上的硬件和软件满足多节点部署的要求，并且目标主机位于同一个广播域中。

   如果 KUMA 服务安装在集群内，目标主机必须满足安装 KUMA 服务所需的硬件、软件和安装要求。

   > 为了使 Kaspersky Next XDR Expert 正常运行，目标主机上 Ubuntu 系列操作系统的 Linux 内核版本必须为 5.15.0.107 或更高版本。

   > 目标主机上不得安装 Docker，除非目标主机将用作管理员主机。KDT 将在部署期间安装所有必要的软件和依赖项。

2. 确保挂载在 `/var` 的文件系统在每个目标主机上至少有 700 GB 的可用空间。

3. 在每个目标主机上，安装 sudo 包（如果尚未安装）。对于 Debian 系列操作系统，请在目标主机上安装 UFW 包。

4. 在每个目标主机上，配置 /etc/environment 文件。如果您组织的基础设施使用代理服务器来访问互联网，请使用目标主机上的代理服务器来配置互联网访问。

5. 在具有UFW配置的主节点上，允许IP转发。在 `/etc/default/ufw` 文件中，将 `DEFAULT_FORWARD_POLICY` 设置为 `ACCEPT`。

6. 提供对软件包存储库的访问权限，该存储库中存储了 Kaspersky Next XDR Expert 所需的以下软件包：

   - nfs-common
   - containerd
   - cron
   - cryptsetup
   - cryptsetup-bin
   - netcat-traditional
   - nfs-common
   - open-iscsi
   - python3-cffi-backend
   - python3-cryptography
   - python3-netaddr
   - python-apt-common
   - systemd
   - tar

   KDT 将在部署期间尝试从软件包存储库安装这些包。您也可以手动安装这些软件包。

7. 确保安装了以下软件包：

   - 在每个目标主机上：python3-apt
   - 在主节点上：curl

   在使用KDT从软件包存储库部署期间，这些软件包不会安装。如果尚未安装这些软件包，则必须手动安装。

8. 对于目标主机，请在虚拟机监控程序、虚拟交换机或网络基础设施级别禁用ARP/MAC欺骗保护机制。

   对于 VMware，请启用**伪造传输**和**MAC 地址更改**。对于 Hyper-V，请启用**MAC 地址欺骗**。对于网络设备，请禁用**动态 ARP 检测 (DAI)**，或将端口配置为受信任端口。

   有关检查 ARP 请求是否到达节点的示例，请参阅MetalLB 故障排除指南。

9. 为目标主机和 Kubernetes 集群网关预留静态 IP 地址。

   Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。网关 IP 地址是 IPv4 地址（例如，10.80.23.182）。

   在多站点配置中，每个数据中心使用自己的 Kubernetes 集群网关，并分配专用 IP 地址。它在每个数据中心的配置文件中指定（`zones` 部分中的 `ingress_ip` 参数）。

   目标主机和 Kubernetes 集群网关必须位于数据中心内的同一子网中。

Kubernetes 集群网关和目标主机需要 IPv4 地址。如果您的环境需要 IPv6 连接，请配置目标主机和 Kubernetes 集群网关上的操作系统，以将 IPv6 流量路由到 IPv6 网关 (NAT64) 或 IPv6 隧道。此配置可使集群在 IPv4 上运行，同时提供与 IPv6 网络的互操作性。

10. 在您的 DNS 服务器上，注册服务 FQDN 以连接到 Kaspersky Next XDR Expert 服务。

    默认情况下，Kaspersky Next XDR Expert 服务可通过以下地址访问：

    - <console_host>.<smp_domain>
    - <ksc_host>.<smp_domain>
    - <kuma_host>.<smp_domain>
    - <api_host>.<smp_domain>
    - <monitoring_host>.<smp_domain>
    - <xdr_edr_ingress_host>.<smp_domain>
    - <updater>.<smp_domain>

      其中<console_host>、<ksc_host>、<kuma_host>、<api_host>、<monitoring_host>、<xdr_edr_ingress_host>和<updater>是服务主机名，<smp_domain>是服务域名。这些参数是服务 FQDN 的一部分，您可以在配置文件中指定。如果您未指定服务主机名的自定义值，则使用默认值：`console_host`—“`console`”，`ksc_host`—“`admsrv`”，`kuma_host`—“`kuma`”，`api_host`—“`api`”，`monitoring_host`—“`monitoring`”，`xdr_edr_ingress_host`—“`agentserver`”，`updater`—“`updater`”。

    列出的服务 FQDN 必须解析为客户管理的负载均衡器的 IP 地址。

    例如：

    - <load_balancer_host_ip>—admsrv.<smp_domain>
    - <load_balancer_host_ip>—api.<smp_domain>
    - <load_balancer_host_ip>—console.<smp_domain>
    - <load_balancer_host_ip>—kuma.<smp_domain>
    - <load_balancer_host_ip>—*.kuma.<smp_domain>
    - <load_balancer_host_ip>—monitoring.<smp_domain>
    - <load_balancer_host_ip>—agentserver.<smp_domain>
    - <load_balancer_host_ip>—updater.<smp_domain>

11. 在目标主机上，创建将用于 Kaspersky Next XDR Expert 部署的账户。

    这些账户用于 SSH 连接，并且必须能够在不输入密码的情况下提升权限 (sudo)。为此，将创建的用户账户添加到 `/etc/sudoers` 文件。

    查看详情

要将创建的用户账户添加到 /etc/sudoers 文件：

1. 运行以下命令：

```
sudo useradd -m -s /bin/bash <user_name>
sudo usermod -aG sudo <user_name>
```

2. 使用以下命令打开 /etc/sudoers 文件：

```
sudo visudo
```

3. 在 # Allow members of group sudo to execute any command 部分的末尾添加以下行：

```
<user_name> ALL=(ALL) NOPASSWD: ALL
```

其中，<user_name> 是所创建用户的名称。

4. 保存并关闭 /etc/sudoers 文件。

12. 配置管理员和目标主机之间的 SSH 连接：

a. 在管理员主机上，使用 ssh-keygen 实用程序生成 SSH 密钥，不设置密码短语。

b. 使用 ssh-copy-id 实用程序将公钥复制到每个目标主机；如果使用负载均衡器，还要复制到负载均衡器主机（例如，复制到 /home/<user_name>/.ssh 目录）。

如果使用目标主机作为管理员主机，则还必须将公钥复制到该主机。

13. 为了确保 Kaspersky Next XDR Expert 组件正常运行，请在目标主机之间提供网络访问，并在必要时在管理员主机和目标主机的防火墙上打开所需端口。

14. 在管理员主机和目标主机上通过网络时间协议 (NTP) 配置时间同步。

15. 如有必要，请准备自定义证书以便使用 Kaspersky Next XDR Expert 公共服务。

您可以为每项服务使用一个基于组织根证书或叶证书颁发的中间证书。准备好的自定义证书将代替自签名证书。

多站点部署：指定安装参数

配置文件是 YAML 格式的文件，包含 Kaspersky Next XDR Expert 组件的一组安装参数。

配置文件模板中并未包含下面列出的所有参数。此模板仅包含在部署 Kaspersky Next XDR Expert 之前必须指定的参数。其余参数设置为默认值，不包含在模板中。您可以手动将这些参数添加到配置文件中以覆盖其原有值。参数值必须遵循下面描述的规则。在部署 Kaspersky Next XDR Expert 期间，KDT 会检查是否正确指定了所需的安装参数。如果配置文件中所需的参数缺失或无效，部署将会中断。

Kaspersky Next XDR Expert 多站点部署配置文件示例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
```

```
#Infrastructure regions that contain data centers
regions:
  # Infrastrusture region 1
  prox1:
    # Name of the infrastructure region.
    description: Proxmox1
  # Infrastructure region 2
  prox2:
    # Name of the infrastructure region.
    description: Proxmox2
  # Infrastructure region 3
  prox3:
    # Name of the infrastructure region.
    description: Proxmox3
# Data centers where the Kubernetes cluster nodes are distributed
zones:
  # Data center 1
  proxmox1:
    # Name of the infrastructure region that the data center belongs to.
    region: prox1
    # Kubernetes cluster gateway IP address of the data center 1.
    ingress_ip: 10.0.0.200
  # Data center 2
  proxmox2:
    # Name of the infrastructure region that the data center belongs to.
    region: prox2
    # Kubernetes cluster gateway IP address of the data center 2.
    ingress_ip: 10.10.20.100
  # Data center 3
  proxmox3:
    # Name of the infrastructure region that the data center belongs to.
    region: prox3
    # Kubernetes cluster gateway IP address of the data center 3.
    ingress_ip: 10.65.20.100
# Nodes on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
  # Data center 1 - primary node
  - desc: cdt-primary1
    # Node type.
    type: primary
    # Name of the data center that the node belongs to.
    zone: proxmox1
    # IP address of the node.
    host: 10.0.0.100
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
        # password: pass
        # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
        key: /root/.ssh/id_rsa
  # Data center 2 - primary node
  - desc: cdt-primary2
    # Node type.
    type: primary
    # Name of the data center that the node belongs to.
    zone: proxmox2
```

```
  # IP address of the node.
  host: 10.10.20.18
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
# Data center 3 - primary node
- desc: cdt-primary3
  # Node type.
  type: primary
  # Name of the data center that the node belongs to.
  zone: proxmox3
  # IP address of the node.
  host: 10.65.20.100
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 1
- desc: cdt-w1
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.101
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 2
- desc: cdt-w2
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.102
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
```

```
# Data center 1 - worker node 3
- desc: cdt-w3
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.103
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 1
- desc: cdt-w4
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.20
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 2
- desc: cdt-w5
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.21
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 3
- desc: cdt-w6
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.22
  access:
    ssh:
```

```
      # User name of the account&period;
      user: root
      # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
      # password: pass
      # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
      key: /root/.ssh/id_rsa
  # Data center 3 - worker node 1
  - desc: cdt-w7
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.11
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
        # password: pass
        # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
        key: /root/.ssh/id_rsa
  # Data center 3 - worker node 2
  - desc: cdt-w8
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.12
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
        # password: pass
        # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
        key: /root/.ssh/id_rsa
  # Data center 3 - worker node 3
  - desc: cdt-w9
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.13
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用于连接到节点的密码。 可以代替 ssh_pk 参数指定的 SSH 密钥使用。
        # password: pass
        # KDT 用于连接主工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
        key: /root/.ssh/id_rsa
# Parameters for the Kaspersky XDR deployment
parameters:
  # Connection string for accessing the DBMS installed and configured on a separate
  server.
```

```
# user_db — 具有权限的内部 DBMS 账户的用户名。 此账户被授予创建数据库和其他 DBMS 账户的权限。
# password_db—The password of the privileged internal DBMS account.
# fqdn_db:port_db—The FQDN and connection port of a separate server on which the DBMS
is installed.
# “psql_dsn” 参数值必须符合 URI 格式。 如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使
用百分号编码进行编码。
- name: psql_dsn
  source:
    value: "postgres://postgres:password@dbms.example.com:1234"
# 通过 KDT 连接到主节点和工作节点的 SSH 私钥路径。 SSH 私钥位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: ssh_pk
  source:
    path: /root/.ssh/id_rsa
# Password of the Kaspersky XDR user account that will be created during the
installation.
# Password must be 8 to 256 characters long.
# It can contain lowercase or uppercase letters ('a' to 'z'), digits ('0' to '9'), and
special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- name: admin_password
  source:
    value: "password"
# 包含 KUMA 服务部署安装设置的 KUMA 清单文件的路径。 此文件位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Kaspersky Endpoint Detection and Response 授权许可密钥的路径。 此文件位于管理员主机上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: license
  source:
    value: "/home/user/license.key"
# 域名。 参数值必须满足四级及以下域名的命名要求。
# The service host name and domain name are parts of FQDNs of the Kaspersky XDR
services.
# Default values of service host names: nwc_host—"console", flow_host—"console",
hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host—"console",
api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom host names can be specified in the configuration file.
# 示例：console.smp.local 是提供对 OSMP 控制台的访问权限的服务的 FQDN。 此 FQDN 由
“console_host”和“smp_domain”设置的值组成。
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom
certificate must be generated.
# 参数值必须是主机名列表，以空格分隔。 如果未指定自定义主机名，则使用以下默认主机名：
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring agentserver updater"
# The parameter that indicates whether to deploy the KUMA services for Kaspersky EDR or
for Kaspersky NGFW.
- name: autodeploy_plan
  source:
    value: "edr"
# User name for authentication on the SMTP server.
- name: grafana_admin_user
  source:
```

```
    value: xdr
# Password for authentication on the SMTP server.
- name: grafana_admin_password
  source:
    value: "password"
```

为了使 KDT 与配置文件正确运行，请在文件末尾添加一个空行。

`regions` 部分包含每个逻辑基础架构区域的安装参数。区域表示地理区域或部署位置，并将一个或多个数据中心（可用区）分组在一起。

Regions 部分

参数名称	是否必需	Description
`description`	是	基础架构区域的名称。 值必须符合以下规则： • 节点名称的长度必须在 1 到 63 个字符之间。 • 节点名称可以包含以下字符： • 大写 ASCII 字母 (A-Z) • 小写 ASCII 字母 (a-z) • 数字 (0-9) • 连字符 (-) 所有基础设施区域都必须具有唯一的名称。

`zones` 部分包含每个数据中心的安装参数。每个可用区都属于特定基础设施区域。

可用区部分

参数名称	是否必需	Description
`region`	是	该可用区所属的基础设施区域的名称。 值必须符合以下规则： • 节点名称的长度必须在 1 到 63 个字符之间。 • 节点名称可以包含以下字符： • 大写 ASCII 字母 (A-Z) • 小写 ASCII 字母 (a-z) • 数字 (0-9) • 连字符 (-) `region` 参数的值必须与 `regions` 部分中定义的区域标识符匹配。
`ingress_ip`	是	Kubernetes 集群网关的预留静态 IPv4 地址。 Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。 每个数据中心都必须拥有自己唯一的集群网关 IP 地址。网关必须与位于同一数据中心的主节点和工作节点位于同一子网中。

配置文件的 `nodes` 部分包含 Kubernetes 集群每个目标主机的安装参数。这些参数列于下表中。

参数名称	是否必需	Description
`desc`	是	节点名称。 值必须符合以下规则： • 节点名称的长度必须在 1 到 63 个字符之间。 • 节点名称可以包含以下字符： • 大写 ASCII 字母 (A-Z) • 小写 ASCII 字母 (a-z) • 数字 (0-9) • 连字符 (-) 所有集群节点必须具有唯一的名称。这一要求是安装Kaspersky Next XDR Expert的先决条件之一，并经KDT验证。
`type`	是	节点类型。 可能的参数值： • `primary` • `worker`
`host`	是	节点的 IP 地址。 属于同一数据中心的所有节点必须与该数据中心的 Kubernetes 集群网关位于同一子网中。 节点需要 IPv4 地址。KDT 会自动在集群节点上禁用 IPv6。
`zone`	是	节点所属数据中心的名称。 `zone` 参数的值必须与 `zones` 部分中定义的数据中心标识符匹配。
`kuma_role`	否	可以指定在工作节点上安装的 KUMA 服务。您可以指定一个、多个或不指定任何KUMA服务。 使用 OSMP 控制台在 Kubernetes 集群中安装 KUMA 服务时，会考虑 `kuma_roles` 参数。如果您计划安装 KUMA 服务的节点过载，集群将选择另一个负载较低的节点进行服务安装。 KUMA 服务（收集器、关联器和存储）可以完全安装在集群内的工作线程节点上，完全安装在 Kubernetes 集群外的单独主机上，或者部分安装在 Kubernetes 集群内，部分安装在 Kubernetes 集群外。如果所有 KUMA 服务都将安装在集群内部，请将 `inventory` 参数设置为 `/dev/null`。 不允许将由同一KUMA资源创建的存储放在同一工作线程节点上。此规则确保了所需的容错级别。 如果存储集群包含多个存储实例，则所有实例都必须部署在集群内部或集群外部。 可能的参数值： • `core`—KUMA Core • `metrics`—KUMA 指标 • `collector`—收集器 • `eventrouter`—事件路由器 • `correlator`—关联器 • `storage`—存储 参数值指定为包含 KUMA 角色的字符串列表。例如： `kuma_roles: ["core","metrics","collector"]`
`user`	是	在目标主机上创建、供 KDT 连接节点时使用的账户用户名。 值必须符合以下规则： • 用户名长度必须在 1 到 31 个字符之间。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 下划线 (_)、连字符 (-)
`password`	否	连接节点的密码。可以代替由 `ssh_pk` 参数指定的 SSH 密钥。

其他安装参数列在配置文件的“`parameters`”部分，并在下表中说明。

参数名称	是否必需	Description

`psql_dsn`	是	用于访问在 Kubernetes 集群外部安装和配置的 DBMS 的连接字符串。
		此参数指定如下：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`
		其中：
		• `dbms_username` — 具有权限的内部 DBMS 账户的用户名。此账户被授予创建数据库和其他 DBMS 账户的权限。通过使用该具有权限的 DBMS 账户，您可以在部署期间创建 Kaspersky Next XDR Expert 组件所需的数据库和其他 DBMS 账户。
		• `password` — 具有权限的内部 DBMS 账户的密码。
		• `fqdn:port` — 安装 DBMS 的目标主机的 FQDN 和连接端口。
		要使用高可用性集群，请按如下方式指定此参数：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`
		要使用 Corosync/Pacemaker，请按如下方式使用虚拟 IP 指定此参数：
		`psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>`
		`psql_dsn` 参数值必须符合 URI 格式。如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使用百分号编码进行编码。
		“`psql_dsn`”参数值中必须替换的符号：
		• 空格 → `%20`
		• ! → `%21`
		• # → `%23`
		• % → `%25`
		• & → `%26`
		• / → `%2F`
		• : → `%3A`
		• = → `%3D`
		• ? → `%3F`
		• @ → `%40`
		• [→ `%5B`
		•] → `%5D`
		详情请参阅“PostgreSQL 连接字符串”一文。

`nwc-language`	是	OSMP 控制台界面的语言是默认指定的。安装完成后，您可以更改 OSMP 控制台语言。 可能的参数值： • `enUS`（默认值） • `ruRu` 如果未在配置文件中指定此参数，则使用默认值。
`ssh_pk`	是	位于管理员主机上的 SSH 密钥的私钥部分的路径，用于通过 KDT 连接到主工作线程节点和部署 KUMA 服务的节点（收集器、关联器和存储）。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。
`admin_password`	是	“`admin_password`”参数指定 KDT 在安装期间创建的 Kaspersky Next XDR Expert 用户账户的密码。此账户的默认用户名是“admin”。 主管理员角色已分配给此用户账户。 密码必须符合以下规则： • 用户密码不能少于10个字符或超过256个字符。 • 密码必须包含以下组中三组的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密码不得包含任何空格或“.@”组合。 当您手动指定“`admin_password`”参数值（而不是通过“部署向导”）时，请确保该值符合 YAML 标准对字符串中值的要求： • 包含特殊字符的参数值必须用单引号括起来。 • 参数值中的任何单引号（'）必须成对输入，才能实现该单引号的转义。 例如：用户账户密码“`Any_pass%1234'5678"90`”必须指定为“`admin_password`”参数的值“`'Any_pass%1234''5678"90'`”。

参数名称	是否必需	Description
low_resources	否	用于指示在计算资源有限的目标主机上安装 Kaspersky Next XDR Expert 的参数。对于多节点部署，请将 low_resources 参数设置为 false。 可能的参数值： • true — 计算资源有限时的安装（适用于单节点部署） • false — 标准安装（默认值）
core_disk_request	是	指定运行 KUMA Core 所需的磁盘空间量的参数。 如果未指定 core_disk_request 参数，并且 low_resources 参数设置为 false 或未指定，则 KUMA Core 运行所需的默认磁盘空间量为 100 GB。 如果未指定 core_disk_request 参数，并且 low_resources 参数设置为 true，则 KUMA Core 运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 core_disk_request 参数。
metrics_disk_request	是	指定 Metrics 服务运行所需的磁盘空间量的参数。 如果未指定 metrics_disk_request 参数，并且 low_resources 参数设置为 false 或未指定，则 Metrics 服务运行所需的默认磁盘空间量为 80 GB。 如果未指定 metrics_disk_request 参数，并且 low_resources 参数设置为 true，则 Metrics 服务运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 metrics_disk_request 参数。
inventory	是	位于管理员主机上的 KUMA 清查文件的路径。清查文件包含用于部署 Kubernetes 集群中未包含的 KUMA 服务的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。如果所有 KUMA 服务都将安装在集群内，请将 inventory 参数设置为 /dev/null。
host_inventory	否	位于管理员主机上的附加 KUMA 清查文件的路径。此文件包含用于部分添加或删除搭载 KUMA 服务的主机的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果要执行 Kaspersky Next XDR Expert 的初始部署或运行需要配置文件的自定义操作，请保留默认参数值 (/dev/null)。
license	否	位于管理员主机上的KUMA授权许可密钥的路径。 参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 部署完成并登录OSMP后，您可以上传授权许可密钥或指定激活码。
nwc_host flow_host hydra_host login_host ksc_host console_host api_host kuma_host monitoring_host xdr_edr_ingress_host	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的主机名。服务主机名和域名（smp_domain 参数值）是服务 FQDN 的一部分。 如果未指定自定义主机名，则使用以下默认主机名： • nwc_host—"console" • flow_host—"console" • hydra_host—"console" • login_host—"console" • ksc_host—"admsrv" • console_host—"console" • api_host—"api" • kuma_host—"kuma" • monitoring_host—"monitoring" • xdr_edr_ingress_host—"agentserver"
smp_domain	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的域名。参数值必须满足四级及以下域名的命名要求。 服务主机名和域名是服务 FQDN 的一部分。例如，如果 console_host 变量的值为 console，并且 smp_domain 变量的值为 smp.local，则提供对 OSMP 控制台的访问权限的服务的完整名称为 console.smp.local。
pki_host_list	是	需为其生成自签名证书或自定义证书的 Kaspersky Next XDR Expert 公共服务的主机名称列表。参数值必须是主机名列表，以空格分隔。

参数名称	是否必需	Description
`intermediate_enabled`	否	该参数指示是否对公共 Kaspersky Next XDR Expert 服务使用自定义中间证书，而非自签名证书。 可能的参数值： • `true` — 使用自定义中间证书。 • `false` — 使用自签名证书（默认值）。
`intermediate_bundle`	否	用于访问公共 Kaspersky Next XDR Expert 服务的自定义中间证书的路径。如果“`intermediate_enabled`”参数设置为“`true`”，则指定此参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。自定义中间证书的有效期必须为 399 天或更长。

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	否	用于使用相应公共 Kaspersky Next XDR Expert 服务的自定义叶证书路径：`<admsrv_host>.<smp_domain>`、`<api_host>.<smp_domain>`、`<kuma_host>.<smp_domain>`、`<monitoring_host>.<smp_domain>` 和 `<console_host>.<smp_domain>`。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。
		如果要指定自定义叶证书，请将 `intermediate_enabled` 参数设置为 `false`，并且不要指定 `intermediate_bundle` 参数和 `pki_host_list` 参数。

`ksc_state_size`	是	分配用于存储管理服务器数据（更新、安装包和其他内部服务数据）的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。所需的可用磁盘空间量取决于受管理设备的数量和其他参数，并且可以进行计算。 默认值是 30 GB。如果未在配置文件中指定此参数，则使用此值。
`prometheus_size`	是	分配用于存储指标的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>GB”。 推荐的最小值和默认值是 5 GB。如果未在配置文件中指定此参数，则使用默认值。
`grafana_admin_user`	否	用于通过 Grafana 工具查看 OSMP 指标的账户的用户名。 值必须符合以下规则： • 用户名长度必须为 1 到 30 个字符。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (_ - .) • 用户名必须以字母开头。 • 用户名不得包含空格或“@”符号。
`grafana_admin_password`	否	用于通过 Grafana 工具查看 OSMP 指标的账户密码。 密码必须符合以下规则： • 用户密码不能少于 8 个字符或超过 256 个字符。 • 密码必须包含以下各组中的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配用于存储 OSMP 日志的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。 推荐的最小值和默认值是 40 GB。如果未在配置文件中指定此参数，则使用默认值。
`loki_retention_period`	是	OSMP 日志的存储期限，超过此期限后，日志将自动删除。默认值为 72 小时（将配置文件中的参数值设置为“<时间（小时）>h”。例如，“72h”）。如果未在配置文件中指定此参数，则使用默认值。
`file_storage_cp`	否	分配给用于存储组件数据以处理响应操作的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。推荐的最小值为 20 GB。

参数名称	是否必需	Description
psql_tls_off	否	该参数指示是否使用 TLS 协议对 Kaspersky Next XDR Expert 组件和 DBMS 之间的流量进行加密。如果 DBMS 安装在集群之外，则默认禁用 TLS 加密（默认值为 "true"）。 可能的参数值： • true — 不加密流量（默认值）。 • false — 加密流量。
psql_trusted_cas	否	可包含 DBMS 服务器 TLS 证书或可颁发该 TLS 服务器证书的根证书的 PEM 文件路径。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果将在单独的服务器上安装和配置 DBMS，并且已启用流量加密（"psql_tls_off"设置为"false"），请指定"psql_trusted_cas"参数。
proxy_enabled	否	该参数指示是否使用代理服务器将 Kaspersky Next XDR Expert 组件连接到互联网。如果安装了 Kaspersky Next XDR Expert 的主机可以访问互联网，您还可以为 Kaspersky Next XDR Expert 组件（例如，管理服务器）的运行以及卡巴斯基和第三方的特定集成提供互联网访问权限。要建立代理连接，您还必须在管理服务器属性中指定代理服务器参数。 可能的参数值： • true—使用代理服务器。 • false—不使用代理服务器（默认值）。
proxy_addresses	否	代理服务器的 IP 地址。如果代理服务器使用多个 IP 地址，请指定这些地址并用空格分隔（例如"0.0.0.0 0.0.0.1 0.0.0.2"）。如果"proxy_enabled"参数设置为"true"，请指定此参数。
proxy_port	否	将建立代理服务器连接的端口号。如果"proxy_enabled"参数设置为"true"，请指定此参数。
trace_level	否	管理服务器跟踪文件的详细程度。在管理服务器运行期间会写入跟踪信息。 默认值为 0，不写入任何跟踪信息。 可能的参数值：0 – 5。 参数值越高，跟踪详情越详细。
ansible_extra_flags	否	KDT 执行的 KUMA Core 和 KUMA 服务部署日志的详细程度。 可能的参数值： • -v • -vv • -vvv • -vvvv 标志中"v"字母的数量越多，日志的详细程度就越高。如果配置文件中未指定此参数，则保存标准组件安装日志。
incident_attachments_max_count_limit	否	您可以附加到事故的文件数。默认值为 100。
incident_attachments_max_size_limit	否	附加到该事故的文件的总大小。该值以字节为单位。在指定时不带计量单位。默认值为 26214400。
ignore_precheck	否	该参数用于指示部署前是否检查 Kubernetes 集群节点的硬件、软件和网络配置是否符合安装该解决方案的先决条件。 可能的参数值： • true—跳过预检查。 • false—执行预检查（默认值）。
airgap_mode	否	指示是否执行APT软件包管理器预检查和更新软件包缓存的参数。这可让您在物理隔离环境中部署Kaspersky Next XDR Expert。 可能的参数值： • true—跳过预检查和软件包缓存更新。 • false—执行预检查并更新软件包缓存（默认值）。
grafana_smtp_host	否	Grafana的SMTP服务器地址，用于发送有关Kubernetes集群运行状况事件的电子邮件通知。请以 <host>:<port> 格式指定此参数，例如 localhost:25。
grafana_smtp_user	否	用于SMTP服务器身份验证的用户名。
grafana_smtp_password	否	用于SMTP服务器身份验证的密码。

参数名称	是否必需	Description
grafana_smtp_bundle	否	包含X.509证书链的文件，用于验证与SMTP服务器的TLS连接。
grafana_smtp_skip_verify	否	指示是否跳过SMTP服务器的TLS证书验证的参数。 可能的参数值： • true—跳过TLS证书验证。 • false—执行TLS证书验证（默认值）。
grafana_smtp_from_address	否	发件人的电子邮件地址，该地址将显示在发送电子邮件通知的"发件人"字段中。
grafana_smtp_from_name	否	在电子邮件通知中显示发件人的姓名。
grafana_smtp_ehlo_identity	否	连接到SMTP服务器时，EHLO命令中使用的标识符。
grafana_starttls_policy	否	连接到SMTP服务器时，使用STARTTLS的策略。 可能的参数值： • OpportunisticStartTLS—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器。 • MandatoryStartTLS—要求使用STARTTLS；如果SMTP服务器不支持STARTTLS，则连接失败。 • NoStartTLS—不使用STARTTLS；请在不加密的情况下连接到SMTP服务器。 • empty—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器（默认值）。
grafana_smtp_enable_tracing	否	指示是否启用SMTP连接跟踪以调试电子邮件发送的参数。 可能的参数值： • true—启用SMTP连接跟踪。 • false—禁用SMTP连接跟踪（默认值）。
autodeploy_plan	否	该参数标明是为Kaspersky EDR还是为KASPERSKY NGFW部署KUMA服务。 可能的参数值： • edr—在 Kubernetes 集群内部署用于 OSMP 和 Kaspersky EDR 的 KUMA 服务（默认值）。 • ngfw—在 Kubernetes 集群内部署用于 OSMP 和 Kaspersky NGFW 的 KUMA 服务。此外，预定义的收集器 **[OOTB] Kaspersky NGFW** 将安装在 KUMA 清单文件的 kuma_collector 参数指定的主机列表中的第一个主机上。 • none—不部署用于 Kaspersky EDR 或 Kaspersky NGFW 的 KUMA 服务。在部署不含用于 Kaspersky EDR 和 Kaspersky NGFW 的 KUMA 服务的 Kaspersky Next XDR Expert 时，或从备份恢复 Kaspersky Next XDR Expert 时，请指定此值。恢复 Kaspersky Next XDR Expert 时指定 edr 或 ngfw，可能会导致已部署的服务与备份副本中的服务发生冲突。
tokenhub_access_token	否	访问令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可能值为 5m，最大值为 2h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 应用程序部署后，您可以更改 tokenhub_access_token 参数。
tokenhub_refresh_token	否	用于获取新访问令牌的刷新令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可能值为 12h，最大值为 4320h。 默认值为 24h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署后更改 tokenhub_refresh_token 参数。
credentials_session_ttl	否	单点登录会话的最大空闲时间。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可能值为 5m，最大值为 96h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署后更改 credentials_session_ttl 参数。

标准 Ubuntu Server 24.04 LTS 虚拟机上的跨数据中心多站点部署

本节包含有关在标准 Ubuntu Server 24.04 LTS 虚拟机上进行 Kaspersky Next XDR Expert 跨数据中心多站点部署的说明。

1 三个主节点、九个工作节点和 HAProxy 的典型配置

在此部署中，使用三个数据中心，每个数据中心包含一个主节点和三个工作节点。此部署总共需要三个主节点、九个工作节点和一个 HAProxy 节点。节点要求如下：

- 主节点：4 个虚拟 CPU，8 GB RAM，500 GB 固态硬盘*
- 工作节点：10 个虚拟 CPU，20 GB RAM，1 TB 固态硬盘*
- HAProxy 节点：4 个虚拟 CPU，8 GB RAM，100 GB 固态硬盘*

* 或任何随机访问模式下具有 8000 IOPS（每秒输入/输出操作数）的设备

> 硬件需求必须按照筛分向导进行计算。

2 配置 HAProxy、主节点和工作节点

2.1 配置 HAProxy 主机

要实现跨数据中心解决方案，必须将主机分布在不同子网中，使用相应子网中的三个 Kubernetes 集群网关，并在其中一个子网中部署一台 HAProxy 主机。

1. 安装 HAProxy：

```
sudo apt update
sudo apt install haproxy
```

2. 编辑 HAProxy 配置文件：

```
sudo nano /etc/haproxy/haproxy.cfg
```

配置文件示例：

```
global
  log /dev/log  local0
  log /dev/log  local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin
  stats timeout 30s
  user haproxy
  group haproxy
  daemon
defaults
  log  global
  mode  http
  option  httplog
  option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
  errorfile 400 /etc/haproxy/errors/400.http
  errorfile 403 /etc/haproxy/errors/403.http
  errorfile 408 /etc/haproxy/errors/408.http
  errorfile 500 /etc/haproxy/errors/500.http
  errorfile 502 /etc/haproxy/errors/502.http
  errorfile 503 /etc/haproxy/errors/503.http
  errorfile 504 /etc/haproxy/errors/504.http
listen stats
    mode http
    bind *:8080
    stats enable
    stats uri /stats
    stats refresh 10s
#    stats admin if LOCALHOST
frontend http
  mode tcp
  bind :80
  default_backend http_servers
backend http_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一个网关 IP>:80 check inter 5s # ingress_ip number 1
  server proxmox2 <第二个网关 IP>:80 check inter 5s # ingress_ip number 2
  server proxmox3 <第三个网关 IP>:80 check inter 5s # ingress_ip number 3
frontend https
  mode tcp
  bind :443
  default_backend https_servers
backend https_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一个网关 IP>:443 check inter 5s # ingress_ip number 1
  server proxmox2 <第二个网关 IP>:443 check inter 5s # ingress_ip number 2
  server proxmox3 <第三个网关 IP>:443 check inter 5s # ingress_ip number 3
frontend https9
  mode tcp
  bind :9443
  default_backend https9_servers
backend https9_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一个网关 IP>:9443 check inter 5s  # ingress_ip number 1
  server proxmox2 <第二个网关 IP>:9443 check inter 5s  # ingress_ip number 2
```

```
  server proxmox3 <第三个网关 IP>:9443 check inter 5s # ingress_ip number 3
frontend https4
  mode tcp
  bind :4443
  default_backend https4_servers
backend https4_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一个网关 IP>:4443 check inter 5s # ingress_ip number 1
  server proxmox2 <第二个网关 IP>:4443 check inter 5s # ingress_ip number 2
  server proxmox3 <第三个网关 IP>:4443 check inter 5s # ingress_ip number 3
frontend ksc13000
  mode tcp
  bind :13000
  default_backend ksc13000
backend ksc13000
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一个网关 IP>:13000 check inter 5s # ingress_ip number 1
  server proxmox2 <第二个网关 IP>:13000 check inter 5s # ingress_ip number 2
  server proxmox3 <第三个网关 IP>:13000 check inter 5s # ingress_ip number 3
```

3. 保存（**Ctrl+S**），然后关闭文件（**Ctrl+X**）。

4. 重新启动 HAProxy 服务：

```
sudo systemctl restart haproxy
```

2.2 配置主节点和工作节点

2.2.1 配置用于部署 Kaspersky Next XDR Expert 的用户账户

1. 打开 /etc/sudoers：

```
sudo visudo
```

2. 在文件末尾添加以下行：

```
{user} ALL=(ALL) NOPASSWD: ALL
```

其中 `{user}` 是用于部署的用户账户。

3. 保存（**Ctrl+S**），然后关闭文件（**Ctrl+X**）。

2.2.2 检查 /var、/opt 和 /tmp 目录中的可用空间

1. 在主节点上，运行以下命令：

```
df -h /var
```

必须至少有 200 GB 的可用空间。

```
df -h /opt
```

必须至少有 200 GB 的可用空间。

```
df -h /tmp
```

至少需要 50 GB 的可用空间。

2. 在 worker1 到 worker3 节点上，运行以下命令：

```
df -h /var
```

必须至少有 200 GB 的可用空间。

```
df -h /opt
```

必须至少有 700 GB 的可用空间。

```
df -h /tmp
```

至少需要 50 GB 的可用空间。

2.2.3 确保同步存储库时没有错误

执行以下命令：

```
sudo apt update
```

该命令不应返回任何错误。

2.2.3 安装 python3-apt 和 curl

执行以下命令：

```
sudo apt install python3-apt curl -y
```

2.2.4 将系统时间配置为与 NTP 服务器同步

1. 运行以下命令：

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

输出将包含以下行：

```
System clock synchronized: yes
```

2. 要检查同步情况，请运行：

```
date
```

输出必须包含当前日期和时间。

❸ 配置 DBMS 主机

DBMS 主机是安装了 DBMS 实例的主机。

安装 DBMS 实例的目标主机要求：

- 10 个虚拟 CPU
- 20 GB RAM
- 1.6 TB SSD 或任何随机访问 IOPS（每秒输入/输出操作数）达到 8000 的设备

有关受支持的 PostgreSQL 版本，请参阅硬件和软件要求一文。

3.1 安装和配置 PostgreSQL

1. 安装 PostgreSQL：

```
sudo apt install -y postgresql-<版本>
```

其中<版本>为 PostgreSQL 版本。

如果已连接的存储库中没有所需的 PostgreSQL 版本，则必须添加 `postgresql` 存储库。有关说明，请参阅 PostgreSQL 网站。

2. 创建单独的 PostgreSQL 超级用户：

```
sudo -u postgres createuser --superuser xdr
```

3. 设置用户密码：

```
sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD '您的密码';"
```

4. 创建一个与用户名相同的数据库：

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. 允许从任何 IP 地址访问 PostgreSQL：

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<版本>/main/pg_hba.conf
```

其中<版本>为 PostgreSQL 版本。

6. 在 PostgreSQL 配置文件（/etc/postgresql/<版本>/main/postgresql.conf）中编辑以下参数，其中 <版本> 是 PostgreSQL 版本。例如，对于 PostgreSQL 16：/etc/postgresql/16/main/postgresql.conf。

需要取消注释带注释 (#) 的行。

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. 重启 PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 将系统时间配置为与 NTP 服务器同步

1. 运行以下命令：

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

输出将包含以下行：

```
System clock synchronized: yes
```

2. 要检查同步情况，请运行：

```
date
```

输出必须包含当前日期和时间。

❹ 配置管理员主机

管理员主机是运行 KDT 工具的主机。分发包中的文件（包括包含 KDT 工具的压缩文件）必须位于管理员主机上。此主机可能是 KDT 工具在部署期间创建的 Kubernetes 集群的一部分，也可能位于集群之外。如果管理员主机不包含在集群中，它将仅用于部署和管理 Kubernetes 集群和 OSMP。如果管理员主机包含在集群中，它还用作运行 OSMP 组件的目标主机。

4.1 解压 KDT 工具

运行以下命令以创建目录并解压 KDT 工具：

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 Docker 安装

支持 Docker 25 及更高版本。

4.2.1 在 Ubuntu 24 上安装：

```
sudo apt update && sudo apt install docker.io
```

4.2.2 ***或*** *按照官方说明进行安装：*

1. 安装所需软件包：

   ```
   sudo apt update && sudo apt install ca-certificates curl
   ```

2. 下载 Docker 密钥环：

   ```
   sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod 0755
   /etc/apt/keyrings/docker.asc
   ```

3. 添加 Docker apt 存储库：

   ```
   sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
   Types: deb
   URIs: https://download.docker.com/linux/ubuntu
   Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
   Components: stable
   Architectures: $(dpkg --print-architecture)
   Signed-By: /etc/apt/keyrings/docker.asc
   EOF
   ```

4. 更新存储库缓存并安装 Docker 软件包：

   ```
   sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
   plugin
   ```

4.3 Docker 配置

1. 将当前用户添加到 docker 组：

```
sudo usermod -aG docker $USER
```

2. 在当前会话中激活用户在 docker 组中的成员身份：

```
newgrp docker
```

4.4 将系统时间配置为与 NTP 服务器同步

1. 运行以下命令：

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

输出将包含以下行：

```
System clock synchronized: yes
```

2. 要检查同步情况，请运行：

```
date
```

输出必须包含当前日期和时间。

4.5 检查 /tmp 目录的可用空间

执行以下命令：

```
df -h /tmp
```

至少需要 50 GB 的可用空间。

如果 /tmp 目录中没有足够的可用空间，请指定另一个目录的路径：

```
export TMPDIR=<new_directory>/tmp
```

或者分配所需的可用空间：

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

分配所需空间后，重启主机或重新挂载分区。

4.6 配置管理员主机与主节点和工作节点之间的 SSH 连接

1. 创建 SSH 密钥：

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. 将密钥逐个复制到每个目标主机：

```
ssh-copy-id {user}@{primary_ip}
ssh-copy-id {user}@{worker_ip}  # copy the key to each worker node in a subnet
```

其中 `{user}` 是在目标主机配置期间创建的 Kaspersky Next XDR Expert 部署用户账户。

4.7 DNS 配置

在您的 DNS 服务器上，注册要连接到 OSMP 服务的服务的 FQDN（`<smp_domain>`）。

要快速开始，请在 DNS 服务器中添加一条指向 HAProxy IP 地址的通配符 A 记录。HAProxy 在三个 Kubernetes 集群网关（`<ingress_ip>`）之间均衡流量，然后这些网关将流量路由到相应服务。

默认情况下，OSMP 服务可通过以下地址访问：

```
<haproxy_host_ip> - admsrv.<smp_domain>
<haproxy_host_ip> - api.<smp_domain>
<haproxy_host_ip> - console.<smp_domain>
<haproxy_host_ip> - kuma.<smp_domain>
<haproxy_host_ip> - *.kuma.<smp_domain>
<haproxy_host_ip> - monitoring.<smp_domain>
<haproxy_host_ip> - agentserver.<smp_domain>
<haproxy_host_ip> - updater.<smp_domain>
```

4.8 创建一个配置以运行安装

显示图例

- `10.0.0.100` — 第一个子网中第一个主节点的 IP 地址（`<primary1_ip>`）
- `10.10.20.18` — 第二个子网中第二个主节点的 IP 地址（`<primary2_ip>`）
- `10.65.20.10` — 第三个子网中第三个主节点的 IP 地址（`<primary3_ip>`）
- `10.0.0.101` — 第一个子网中第一个工作节点的 IP 地址（`<worker1_ip>`）
- `10.0.0.102` — 第一个子网中第二个工作节点的 IP 地址（`<worker2_ip>`）
- `10.0.0.103` — 第一个子网中第三个工作节点的 IP 地址（`<worker3_ip>`）
- `10.10.20.20` — 第二个子网中第一个工作节点的 IP 地址（`<worker4_ip>`）
- `10.10.20.21` — 第二个子网中第二个工作节点的 IP 地址（`<worker5_ip>`）
- `10.10.20.22` — 第二个子网中第三个工作节点的 IP 地址（`<worker6ip>`）
- `10.65.20.11` — 第三个子网中第一个工作节点的 IP 地址（`<worker7_ip>`）

- `10.65.20.12` — 第三个子网中第二个工作节点的 IP 地址（`<worker8_ip>`）
- `10.65.20.13` — 第三个子网中第三个工作节点的 IP 地址（`<worker9_ip>`）
- `10.0.0.150` — DBMS 主机的 IP 地址（`<DB_ip>`）
- `10.0.0.200` — 第一个 Kubernetes 集群网关的 IP 地址
- `10.10.20.100` — 第二个 Kubernetes 集群网关的 IP 地址
- `10.65.20.100` — 第三个 Kubernetes 集群网关的 IP 地址
- `10.0.0.111` — HAProxy 主机的 IP 地址
- `user` — 用于部署的用户帐户（`<user_name>`）
- `/home/user/.ssh/id_rsa` — 管理员主机上配置 SSH 连接期间创建的 SSH 密钥的路径（`<ssh_key_path>`）
- `xdr.mydomain.com` — Ingress 的域（`<smp_domain>`）

4.8.1 使用配置文件指定安装参数

配置文件的模板 (multinode.smp_param.yaml.template) 位于分发包中，压缩包内包含 KDT 实用程序。

`psql_dsn` 参数值必须符合 URI 格式。如果连接 URI 的任何部分包含具有特殊含义的符号，则必须使用百分号编码进行编码。

“`psql_dsn`”参数值中必须替换的符号：

- 空格 → `%20`
- `!` → `%21`
- `#` → `%23`
- `%` → `%25`
- `&` → `%26`
- `/` → `%2F`
- `:` → `%3A`
- `=` → `%3D`
- `?` → `%3F`
- `@` → `%40`
- `[` → `%5B`
- `]` → `%5D`

详情请参阅“PostgreSQL 连接字符串”一文。

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
regions:
    prox1:
        description: Proxmox1
    prox2:
        description: Proxmox2
    prox3:
        description: Proxmox3
zones:
    proxmox1:
        region: prox1
        ingress_ip: 10.0.0.200
    proxmox2:
        region: prox2
```

```
        ingress_ip: 10.10.20.100
    proxmox3:
        region: prox3
        ingress_ip: 10.65.20.100
nodes:
  - desc: cdt-primary1
    type: primary
    zone: proxmox1
    host: 10.0.0.100
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary2
    type: primary
    zone: proxmox2
    host: 10.10.20.18
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary3
    type: primary
    zone: proxmox3
    host: 10.65.20.100
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    zone: proxmox1
    host: 10.0.0.101
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    zone: proxmox1
    host: 10.0.0.102
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w3
    type: worker
    zone: proxmox1
    host: 10.0.0.103
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w4
    type: worker
    zone: proxmox2
    host: 10.10.20.20
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w5
    type: worker
    zone: proxmox2
    host: 10.10.20.21
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w6
    type: worker
    zone: proxmox2
    host: 10.10.20.22
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w7
    type: worker
    zone: proxmox3
    host: 10.65.20.11
    access:
```

```
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w8
    type: worker
    zone: proxmox3
    host: 10.65.20.12
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w9
    type: worker
    zone: proxmox3
    host: 10.65.20.13
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<your_password>@<DB_ip>:5432
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "your_password"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<domain_smp>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "your_password"
```

5 Kaspersky Next XDR Expert 安装

执行以下命令：

```
./kdt/bin/kdt apply --accept-eula -k xdr-<program_version>.tar -i params.yaml
```

如果安装成功，终端将显示以下信息：

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<ver>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

要检查安装情况，您需要前往授权页面。为此，请在浏览器的搜索栏中输入以下内容：

```
console.<smp_domain>
```

其中 `<smp_domain>` 是此过程第 4.7 步中的 FQDN。

Kaspersky Next XDR Expert 维护

本部分介绍如何使用 KDT 更新、删除和重新安装 Kaspersky Next XDR Expert 组件。此外，本部分还提供有关如何停止 Kubernetes 集群节点、更新公共 Kaspersky Next XDR Expert 服务的自定义证书以及如何获取配置文件的当前版本以及使用 KDT 对 Kaspersky Next XDR Expert 组件执行其他操作的说明。

更新 Kaspersky Next XDR Expert 组件

通过 KDT，您可以更新 Kaspersky Next XDR Expert 组件（包括管理 Web 插件）和 Bootstrap 组件。Kaspersky Next XDR Expert 组件的新版本已包含在分发包中。

不支持安装早期版本的组件。

要更新 Kaspersky Next XDR Expert 组件：

1. 下载包含 Kaspersky Next XDR Expert 组件新版本的分发包。
2. 如有必要，在管理员主机上导出当前版本的配置文件。

   如果没有添加或修改安装参数，则无需导出配置文件。
3. 更新 Kaspersky Next XDR Expert 组件和 Bootstrap。

   指定包含 Kaspersky Next XDR Expert 组件的传输压缩文件路径和配置文件路径。如果在 Bootstrap 更新命令中指定了配置文件路径或者未添加或修改安装参数，则配置文件路径是可选的：

   - 运行以下命令对 Kaspersky Next XDR Expert 组件进行标准更新：

     `./kdt apply -k <XDR 更新压缩文件的完整路径> -i <配置文件的完整路径>`

   - 如果安装的 Kaspersky Next XDR Expert 组件版本与分发包中的组件版本匹配，则跳过该组件的更新。使用 `force` 标志运行以下命令以强制更新此组件：

     `./kdt apply --force -k <XDR 更新压缩文件的完整路径> -i <配置文件的完整路径>`
4. 如果出现新版本的 EULA 和隐私策略，请阅读 Kaspersky Next XDR Expert 组件的最终用户授权许可协议 (EULA) 和隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   a. 如果您理解并接受 EULA 的条款，请输入“`y`”。

   如果您不接受 EULA 的条款，请输入“`n`”。要使用 Kaspersky Next XDR Expert 组件，您必须接受 EULA 的条款。

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

如果您不接受隐私策略的条款，请输入“n”。

> 要更新 Kaspersky Next XDR Expert 组件，您必须接受 EULA 和隐私策略的条款。

在您接受 EULA 和隐私策略后，KDT 将更新 Kaspersky Next XDR Expert 组件。

更新后，您可以阅读 Kaspersky Next XDR Expert 组件的 EULA 和隐私策略。这些文件位于运行 Kaspersky Next XDR Expert 部署的用户的 `~/kaspersky_eula` 目录中。

检查已安装的Kaspersky Next XDR Expert组件的完整性

部署Kaspersky Next XDR Expert后，您可以检查解决方案组件的真实性和完整性。传输归档中的每个组件（CNAB）都包含一个XML格式的清单文件。该清单文件包含组件校验和，并使用GOST R 34.11-2012的256位算法进行数字签名。此数字签名既确保组件文件校验和的有效性，也确保清单中的校验和未被更改。

您可以验证组件的校验和是否与清单中指定的校验和匹配。这确认组件未被修改，并且来自可信来源。

检查安装在Kubernetes集群内的Kaspersky Next XDR Expert组件的完整性

要检查Kaspersky Next XDR Expert组件的完整性：

1. 运行以下命令，将Kaspersky Next XDR Expert组件及其清单文件从已部署的解决方案提取到指定目录。仅从解决方案中提取位于传输存档中的组件：

```
./kdt extract --reference <path to transport archive> -d <path to extracted cnabs>
```

其中：

- `<path to transport archive>` — 传输压缩文件的路径
- `<path to extracted cnabs>` — 解决方案组件及其清单文件将被提取到的目录路径

2. 从包含已提取组件及其清单文件的目录运行以下命令。`integrity_checker`实用程序会将从已部署的解决方案中提取的组件的校验和与从传输压缩文件中提取的清单文件中的校验和进行比较：

```
find . -type f -iname "*.xml" -print0 | xargs -0 -I {} echo --manifest {} | xargs ./integrity_checker --
signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
```

成功进行完整性检查后的命令输出示例

已成功通过验证的清单文件数量显示在`Manifests`行的`succeeded`列中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 0 / 0 / 38
        Files: 0 / 0 / 38
        Directories: 0 / 0 / 0
```

```
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
SUCCEEDED
```

完整性检查失败后的命令输出示例

在此示例中，清单文件在签名后被修改，或者签名存在问题。跳过的清单文件或验证失败的清单文件的数量显示在`Manifests`行的`failed`列中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 2 / 0 / 36
        Files: 0 / 0 / 0
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
FAILED
ERR无法验证文件“/home/xdr_user/integrity_check.xml”的数字签名。 标志：无：0x80000106（对象不受信任）
清单文件/home/xdr_user/integrity_check.xml验证失败。原因：无法验证文件“/home/xdr_user/integrity_check.xml”的数字签名。 标志：无：0x80000106（对象不受信任）
```

验证了安装在Kubernetes集群内的Kaspersky Next XDR Expert组件的完整性。如果集群中也安装了KUMA服务，则还会验证其完整性。

您还可以检查安装在Kubernetes集群之外的KUMA服务的完整性。

无需重新安装即可更改 Kaspersky Next XDR Expert 参数

如果组织的基础设施发生了变化，那么 Kaspersky Next XDR Expert 可能需要快速更改主要参数值，而无需重新安装解决方案。Kaspersky Next XDR Expert 支持通过 KDT 来更改 Kubernetes 集群 IP 地址（`ingress_ip` 参数）和服务的 FQDN（特别是更改服务域名、`smp_domain` 参数）。

要更改参数值且无需重新安装 Kaspersky Next XDR Expert：

1. 在管理员主机上，导出当前配置文件。
2. 在导出的配置文件中，更改 `smp_domain` 或 `ingress_ip` 参数值。您可以同时更改这两个参数，也可以单独更改其中一个参数。

   如果您跨多个数据中心部署 Kaspersky Next XDR Expert，请更改配置文件的 `zones` 部分中的 `ingress_ip` 参数值。
3. 使用以下命令应用参数更改：

```
./kdt apply -i '<full_path_to_updated_configuration_file>'
```

`smp_domain` 和 `ingress_ip` 设置的值已更改。Kaspersky Next XDR Expert 使用新设置。

当 `smp_domain` 参数值更改时，FQDN 服务名称也会更改。因此，KDT 重新颁发了访问公共 Kaspersky Next XDR Expert 服务所需的所有证书。

添加和删除Kubernetes集群的主节点和工作线程节点

如果您需要扩展Kubernetes集群以满足当前工作负载、提高其容错性或优化计算资源，您可以使用KDT添加或删除集群中包含的主节点和工作线程节点。

只有在Kaspersky Next XDR Expert部署在多个节点上时，您才能添加或删除主节点和工作线程节点。

向Kubernetes集群添加新的主节点和工作线程节点

若要添加新的主节点和工作线程节点：

1. 准备将作为主节点和工作节点的目标主机。
2. 在管理员主机上，使用以下命令导出当前配置文件：

   ```
   ./kdt ec -e '<configuration_file_name_with_path>'
   ```

   配置文件的当前版本将以指定的名称保存到指定的目录中。
3. 在导出的配置文件的 `nodes` 部分中，添加一个或多个新节点的参数（`desc`、`type`、`host`、`kind`、`user` 和 `key`），然后保存配置文件。
4. 使用 ssh-copy-id 实用程序将公钥复制到每个新节点（例如，复制到 `~/.ssh` 目录）。
5. 在管理员主机上，运行以下命令将修改后的配置文件应用到 Kubernetes 集群。在命令中，指定此配置文件的完整路径：

   ```
   ./kdt apply -i '< 配置文件完整路径 >'
   ```

   启动命令后，KDT 会检查配置文件是否填写正确。然后，KDT检查Kubernetes集群节点的硬件、软件和网络配置是否符合安装解决方案的先决条件。如果所有严格的预检查都成功完成，KDT 会将验证成功通知输出到 stdout 和 KDT 日志。否则，将保存包含验证失败信息的日志，并中断添加新主机的进程。如果需要，您可以在运行命令之前跳过预检查（将 `ignore_precheck` 安装参数设置为 `true`）。

新的主节点和工作线程节点被添加到Kubernetes集群中。KDT将有关添加的主节点和工作线程节点的信息输出到stdout和KDT日志中。

从Kubernetes集群中删除主节点和工作线程节点

删除节点时，请注意集群中允许的主节点的最小数量为1个，工作线程节点数量为3个。如果删除时少于一个主节点和三个工作线程节点，操作将中断。您可以在导出后获得的配置文件中查看主节点和工作线程节点的数量。

若要删除主节点和工作线程节点：

1. 在管理员主机上，使用以下命令导出当前配置文件：

   ```
   ./kdt ec -e '<configuration_file_name_with_path>'
   ```

   配置文件的当前版本将以指定的名称保存到指定的目录中。

2. 在导出的配置文件的 `nodes` 部分，删除一个或多个主节点和工作线程节点的参数（`desc`、`type`、`host`、`kind`、`user`和`key`），然后保存配置文件。

确保删除节点后，集群中至少还剩下一个主节点和三个工作线程节点。多节点部署的最小集群配置包含四个节点（一个主节点和三个工作节点）。如果不满足此条件，删除过程将中断。

您也可以删除带有`kind=admsrv`的节点，前提是它并非集群中仅存的带有`kind=admsrv`的节点。如果尝试从集群中删除此节点，则删除过程中将跳过该节点。

3. 在管理员主机上，运行以下命令将修改后的配置文件应用到 Kubernetes 集群。在命令中，指定此配置文件的完整路径：

```
./kdt apply -i '<配置文件完整路径>'
```

指定的节点将被删除。KDT将有关已删除的主节点和工作线程节点的信息输出到stdout和KDT日志。

配置文件的版本控制

使用 Kaspersky Next XDR Expert 时，您可能需要更改在部署 Kaspersky Next XDR Expert 之前在配置文件中指定的参数。例如，当更改用于存储管理服务器数据的磁盘空间时，`ksc_state_size`参数会被修改。包含修改后的`ksc_state_size`参数的配置文件当前版本会在 Kubernetes 集群中更新。

如果您尝试在需要配置文件的 KDT 自定义操作中使用配置文件的先前版本，则会发生冲突。为避免冲突，您只能使用从 Kubernetes 集群导出的配置文件的当前版本。

要导出配置文件的当前版本：

请在 KDT 实用程序所在的管理员主机上，运行以下自定义操作，然后指定配置文件的路径及其名称：

```
./kdt ec -e <configuration_file_name_with_path>
```

配置文件的当前版本将以指定的名称保存到指定的目录中。

例如，您可以在更新 Kaspersky Next XDR Expert 组件或为卡巴斯基应用程序添加管理插件时使用导出的配置文件。

如果没有添加或修改安装参数，则无需导出配置文件。

卸载 Kaspersky Next XDR Expert

KDT 允许您卸载安装在 Kubernetes 集群中的所有 Kaspersky Next XDR Expert 组件、集群本身、集群外安装的 KUMA 服务以及在解决方案部署或运行期间创建的其他工件。

要卸载 Kaspersky Next XDR Expert 组件及其相关数据：

1. 请在管理员主机上运行以下命令：

```
./kdt remove --all
```

此命令将删除以下对象和工件：

- Kubernetes 集群中安装的所有 Kaspersky Next XDR Expert 组件以及集群本身。
- KDT 在部署期间创建的 Kaspersky Next XDR Expert 用户账户。
- 位于单独服务器或集群内的数据库、DBMS 架构，以及 KDT 在部署期间创建的 DBMS 账户。
- 安装在集群外的 KUMA 服务，部署于清查文件中指定的主机上。
- 目标主机上以下目录的内容：
  - `/var/spool/ksc/logs`
  - `/var/spool/ksc/backup`
  - `/var/spool/ksc/`
  - `/var/lib/k0s`
  - `/run/k0s`
  - `/etc/k0s/`
  - `/etc/containerd/`
  - `/var/lib/containerd/`
  - `/run/containerd/`
- 在安装和运行 Kaspersky Next XDR Expert 组件期间获取的日志。
- 与管理员主机上 Kaspersky Next XDR Expert 组件相关的数据。

如果管理员主机无法访问目标主机的网络，则组件的卸载将被中断。您可以恢复网络访问并重新开始卸载 Kaspersky Next XDR Expert。或者，您也可以从目标主机卸载 Kaspersky Next XDR Expert 组件。

> 如果您使用通过上下文管理的多个 Kubernetes 集群，则此命令仅删除当前 Kubernetes 上下文、相应的集群以及集群中安装的 Kaspersky Next XDR Expert 组件。其他包含 Kaspersky Next XDR Expert 实例的上下文及其集群不会被删除。

2. 如有必要，请关闭 Kaspersky Next XDR Expert 在部署期间打开的端口。这些端口不会自动关闭。
3. 如有必要，请删除在部署期间自动安装的操作系统软件包。这些软件包不会自动删除。
4. 删除 KDT 以及 `~/kaspersky_eula` 和 `~/.kdt` 目录的内容。

Kaspersky Next XDR Expert 组件、数据库和相关数据均被删除，Kaspersky Next XDR Expert 使用的端口也将关闭。

使用 `./kdt remove` 命令不会移除安装在受管理设备上的卡巴斯基应用程序。有关如何移除卡巴斯基应用程序的信息，请参阅相应的文档。

卸载 Kaspersky Next XDR Expert 后，目标主机不会自动重新启动。如有必要，您可以手动重新启动这些主机。

手动卸载 Kaspersky Next XDR Expert 组件

如果管理员主机无法与目标主机建立网络连接，通过 KDT 卸载 Kaspersky Next XDR Expert 组件的操作将会中断。您可以先恢复网络访问，然后重新开始卸载解决方案。或者，您也可以从目标主机手动卸载 Kaspersky Next XDR Expert 组件。

要从目标主机手动卸载 Kaspersky Next XDR Expert 组件：

1. 在目标主机上，运行以下命令停止 k0s 服务：

   ```
   /usr/local/bin/k0s stop
   ```

2. 运行以下命令将集群节点重置为初始状态：

   ```
   /usr/local/bin/k0s reset
   ```

3. 删除以下目录的内容：

   - 必需目录：
     - `/etc/k0s/`
     - `/var/lib/k0s/`
     - `/usr/libexec/k0s/`
     - `/usr/local/bin/`（仅删除 `k0s` 文件）
   - 可选目录：
     - `/var/lib/containerd/`
     - `/var/cache/k0s/`
     - `/var/cache/kubelet/`
     - `/var/cache/containerd/`

     如果 containerd 服务仅用于 Kaspersky Next XDR Expert 的功能，则可以删除 `/var/lib/containerd/` 和 `/var/cache/containerd/` 目录。否则，`/var/lib/containerd/` 和 `/var/cache/containerd/` 目录中包含的数据可能会丢失。

     重新启动目标主机后，`/var/cache/k0s/`、`/var/cache/kubelet/` 和 `/var/cache/containerd/` 目录的内容会自动删除。您不必手动清除这些文件夹。

4. 重新启动所有目标主机。

Kaspersky Next XDR Expert 组件将从目标主机中删除。

安装失败后重新安装 Kaspersky Next XDR Expert

如果 Kaspersky Next XDR Expert 安装失败，您可以重新开始安装。安装失败可能发生在 Bootstrap 或 Kaspersky Next XDR Expert 组件的安装过程中。重新安装 Kaspersky Next XDR Expert 所需的步骤取决于安装错误发生时 Kubernetes 集群是否已部署。

要确定安装失败发生在哪个阶段：

请运行以下命令查看所有已安装的 Kaspersky Next XDR Expert 组件的列表：

```
./kdt state
```

如果发生 Bootstrap 安装错误，KDT 会显示一条消息，提示 Bootstrap 未安装。在这种情况下，您必须手动卸载部署期间创建的目录。

如果 Bootstrap 安装成功，命令输出中会显示 `Success` 状态。这意味着 Kaspersky Next XDR Expert 组件安装发生错误。在这种情况下，您必须重新安装未正确安装的组件或重新安装整个解决方案。在命令输出中，此类组件会显示 `Failed` 状态。

如果未安装 Bootstrap，则需要重新安装 Kaspersky Next XDR Expert

要重新开始安装 Kaspersky Next XDR Expert：

1. 转到包含 KDT 实用程序的目录，然后查看 Bootstrap 组件的安装日志。

   如果在 Bootstrap 安装阶段发生故障，这将体现在日志中。在这种情况下，Bootstrap 未安装，Kubernetes 集群也未创建。

   运行 `/.kdt/kdt-{date}.log | grep -iE "connect|auth|ident|password"` 命令，查找与最常见安装问题相关的日志条目：

   - 数据库连接设置
   - 管理员密码格式
   - 硬件资源不足
   - 连接节点时出现授权问题

2. 手动卸载部署期间创建的目录。

   a. 在管理员主机上，转到 `.kdt` 目录，然后删除 `cluster.config` 文件。

   b. 删除以下目录的内容：

- 必需目录：
  - `/etc/k0s/`
  - `/var/lib/k0s/`
  - `/usr/libexec/k0s/`
  - `/usr/local/bin/`（仅删除 `k0s` 文件）
- 可选目录：
  - `/var/lib/containerd/`
  - `/var/cache/k0s/`
  - `/var/cache/kubelet/`
  - `/var/cache/containerd/`

  如果 containerd 服务仅用于 Kaspersky Next XDR Expert 的功能，则可以删除 `/var/lib/containerd/` 和 `/var/cache/containerd/` 目录。否则，`/var/lib/containerd/` 和 `/var/cache/containerd/` 目录中包含的数据可能会丢失。

  重新启动目标主机后，`/var/cache/k0s/`、`/var/cache/kubelet/` 和 `/var/cache/containerd/` 目录的内容会自动删除。您不必手动清除这些文件夹。

c. 重新启动所有目标主机。

3. 重新开始安装 Kaspersky Next XDR Expert。

如果已安装 Bootstrap，则重新安装 Kaspersky Next XDR Expert

要重新安装错误安装的 Kaspersky Next XDR Expert 组件：

1. 使用以下命令查看错误安装的 Kaspersky Next XDR Expert 组件的完整安装日志：

   `./kdt state -l <component_name>`

   您还可以使用以下命令输出有关 Kaspersky Next XDR Expert 组件的所有诊断信息：

   `./kdt logs get --to-archive`

2. 自行或在卡巴斯基技术支持的帮助下排查并解决安装错误。
3. 重新安装错误安装的 Kaspersky Next XDR Expert 组件。
   - 如果您没有修改配置文件，请运行以下命令，然后指定用于 Kaspersky Next XDR Expert 安装的相同传输存档文件：

     `./kdt apply -k <full_path_to_transport_archive>`

- 如果需要更改安装参数，请导出配置文件，进行修改，然后使用传输存档文件和更新的配置文件运行以下命令：

  ```
  ./kdt apply -k <full_path_to_transport_archive> -i
  <full_path_to_configuration_file>
  ```

KDT 仅重新安装未正确安装的 Kaspersky Next XDR Expert 组件。

4. 使用以下命令重新开始安装 Kaspersky Next XDR Expert：

   ```
   ./kdt apply --force -k <XDR 更新压缩文件的完整路径> -i <配置文件的完整路径>
   ```

如果重新安装组件未能修复安装错误，则可以卸载整个解决方案。

要重新开始安装 Kaspersky Next XDR Expert：

1. 使用以下命令输出有关 Kaspersky Next XDR Expert 组件的所有诊断信息：

   ```
   ./kdt logs get --to-archive
   ```

2. 自行或在卡巴斯基技术支持的帮助下排查并解决安装错误。

3. 卸载 Kaspersky Next XDR Expert。在管理员主机上，运行以下命令：

   ```
   ./kdt remove --all
   ```

4. 使用以下命令重新开始安装 Kaspersky Next XDR Expert：

   ```
   ./kdt apply --force -k <XDR 更新压缩文件的完整路径> -i <配置文件的完整路径>
   ```

重新安装 Kaspersky Next XDR Expert 组件

在安装 Kaspersky Next XDR Expert 期间，在管理员主机上，KDT 会显示安装日志，此日志表明 Kaspersky Next XDR Expert 组件是否已正确安装。

安装 Kaspersky Next XDR Expert 后，您可以运行以下命令查看所有已安装组件的列表：

```
./kdt state
```

显示已安装组件的列表。正确安装的组件的状态为`Success`。如果组件安装失败，则该组件的状态为`Failed`。

要查看错误安装的 Kaspersky Next XDR Expert 组件的完整安装日志，请运行以下命令：

```
./kdt state -l <component_name>
```

您还可以使用以下命令输出有关 Kaspersky Next XDR Expert 组件的所有诊断信息：

```
./kdt logs get --to-archive
```

您可以使用获取的日志自行或在卡巴斯基技术支持的帮助下排查并解决问题。

要重新安装错误安装的 Kaspersky Next XDR Expert 组件：

- 如果您没有修改配置文件，请运行以下命令，然后指定用于 Kaspersky Next XDR Expert 安装的相同传输存档文件：

  ```
  ./kdt apply -k <full_path_to_transport_archive>
  ```

- 如果需要更改安装参数，请导出配置文件，进行修改，然后使用传输存档文件和更新的配置文件运行以下命令：

  ```
  ./kdt apply -k <full_path_to_transport_archive> -i <full_path_to_configuration_file>
  ```

KDT 仅重新安装未正确安装的 Kaspersky Next XDR Expert 组件。

备份 Kaspersky Next XDR Expert 数据的副本和数据恢复

数据备份可用于保存 Kaspersky Next XDR Expert 数据的完整副本。在备份过程中，Kaspersky Next XDR Expert 组件的运行将暂时停止，以确保数据一致性。备份创建后，将保存在单独服务器上的网络文件夹中，然后解决方案将恢复运行。您可以手动或根据指定的计划创建备份。

按照此方案，您可以配置备份存储、设置计划备份或手动创建备份、管理备份以及从备份中恢复 Kaspersky Next XDR Expert 数据。

限制：

- 在备份过程中，Kaspersky Next XDR Expert 组件的运行将暂时停止，以确保数据一致性。
- 备份包括所有 Kaspersky Next XDR Expert 数据。不支持对单个组件单独创建备份或恢复数据。
- 从备份中恢复 Kaspersky Next XDR Expert 的数据时，必须使用创建该备份时所用的同版本 Kaspersky Next XDR Expert。
- 仅当 DBMS 未包含在 Kubernetes 集群中时，才支持备份和恢复 Kaspersky Next XDR Expert 数据。将 DBMS 安装到 Kubernetes 集群的配置仅用于熟悉该解决方案，不用于处理标准工作任务。
- 系统不会自动检查备份的可用空间。您必须确保网络文件夹中有足够的可用空间。

阶段

Kaspersky Next XDR Expert 数据的备份副本和恢复分阶段进行：

1. **配置备份存储**

   指定用于存储备份的网络文件夹的路径。此网络文件夹必须位于单独的服务器上，且必须可通过 CIFS 或 NFS 协议从 Kubernetes 集群访问。

   为了防止网络文件夹过载，网络文件夹中可存储备份的最大数量是有限的。默认情况下，您最多可以创建 10 个备份。您可以在手动创建备份或配置备份计划时，通过 `backup_retain` 参数设置备份的最大数量。如果网络文件夹已包含最大数量的备份，则下一个备份将覆盖最早的备份。

   由于系统不会自动检查网络文件夹中的可用空间，建议定期监控此文件夹中的可用空间以防止备份失败。

2. **创建 Kaspersky Next XDR Expert 数据的备份副本**

使用以下方式之一来创建备份：

- 计划备份

  如果要根据计划创建备份，则必须使用 KDT 配置计划。您只能指定一个备份计划。创建新计划将替换现有计划。此外，您可以查看当前计划，以及暂停或恢复自动备份。

  在使用自动计划备份之前，建议手动创建备份，以确保用于存储备份的网络文件夹配置正确且可以访问。

- 手动备份

  如果您需要保存备份而不等待下一次自动备份，您可以创建手动备份。

备份将保存到指定的网络文件夹。您可以查看可用备份列表以及每个备份的详细信息。

KDT 日志提供有关备份操作结果的详细信息，包括操作的成功或失败、执行的日期和时间以及备份副本的名称和位置。

3. **从备份副本恢复 Kaspersky Next XDR Expert 数据**

   恢复备份副本以将 Kaspersky Next XDR Expert 回滚到保存的状态。

配置 Kaspersky Next XDR Expert 备份副本的存储

所有创建的备份都存储在单独服务器上的网络文件夹中。此文件夹必须可通过 CIFS 或 NFS 协议从 Kubernetes 集群访问。

> 系统不会自动检查备份的可用空间。您必须确保网络资源上有足够的可用空间。

为了防止网络文件夹过载，网络文件夹中可存储备份的最大数量是有限的。默认情况下，您最多可以创建 10 个备份。您可以在手动创建备份或配置备份计划时，通过 `backup_retain` 参数设置备份的最大数量。如果网络文件夹已包含最大数量的备份，则下一个备份将覆盖最早的备份。

指定备份存储的网络文件夹路径

要指定可通过 CIFS/SMB 协议访问的备份存储路径：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a setBackupStore \
  --param backup_target_url="cifs://<host>/<path>" \
  --param cifs_username="<用户名>" \
  --param cifs_password="<密码>"
```

其中：

- < host > 是网络存储服务器的地址。
- < path > 是备份网络文件夹的路径。
- < 用户名 > 是访问网络文件夹的用户名。

- < 密码 > 是访问网络文件夹的密码。
  如果密码包含双引号，请使用反斜杠 (\") 将其转义。

要指定可通过 NFS 协议访问的备份存储路径：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a setBackupStore --param backup_target_url="nfs://<host>:/<path>"
```

其中：

- < host > 是网络存储服务器的地址。
- < path > 是备份网络文件夹的路径。

指定备份存储的网络文件夹路径。

查看备份存储网络文件夹的路径

要查看当前备份存储路径：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a getBackupStore
```

显示当前备份存储路径。

配置和管理备份计划

Kaspersky Next XDR Expert 允许您根据计划创建备份、查看当前计划、暂停或恢复计划备份以及删除计划。

> 您只能配置一个备份计划。创建新计划将替换现有计划。

> 在使用计划备份之前，建议手动创建备份，以确保用于存储备份的网络文件夹配置正确且可以访问。

配置备份计划

要配置备份计划：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a updateSchedule \
  --param schedule='<schedule>' \
```

```
    --param schedule_paused=<schedule_is_paused> \
    --param backup_retain=<max_number_of_backups>
```

其中：

- `<schedule>` 是一个采用 UNIX™ cron 格式的字符串，用于指定备份频率。例如，如果您想在每月 1 日和 15 日上午 9:30 以及每个周一创建备份，请使用以下命令：

  ```
  ./kdt invoke backup-operator -a updateSchedule --param schedule='30 9 1,15 * 1' --param schedule_paused=false --param backup_retain=5
  ```

  > 系统会验证格式的正确性：如果您输入了错误的参数，系统将显示错误消息。

- `<schedule_is_paused>` 参数用于指定创建计划后计划备份的状态：
  - `<schedule_is_paused>=false`—计划备份处于活动状态，并将按配置运行。
  - `<schedule_is_paused>=true`—计划备份已暂停，不会运行。
- `<max_number_of_backups>` 是网络文件夹中可存储的最大备份数。默认值是 10。如果网络文件夹已包含最大数量的备份，则下一个备份将覆盖最早的备份。如果减少参数值（例如，在手动创建备份或配置备份计划时，将 `<max_number_of_backups>` 设置为 3），KDT 将删除除最近三个备份之外的所有备份。

备份计划已配置。

查看备份计划的详细信息

要查看备份计划的详细信息：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a getBackupSchedule
```

显示已配置的备份计划详情，包括 NAME 列中显示的计划名称。

暂停计划备份

要暂停计划备份：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a updateSchedule --param schedule_paused=true
```

计划备份已暂停。

恢复计划备份

要恢复计划备份：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a updateSchedule --param schedule_paused=false
```

计划备份已恢复。

手动创建 Kaspersky Next XDR Expert 数据备份副本

如果您需要保存备份而不等待下一次自动备份，或者确保用于存储备份的网络文件夹配置正确且可以访问，则可以创建手动备份。在备份过程中，Kaspersky Next XDR Expert 组件的运行将暂时停止，以确保数据一致性。

要手动创建备份：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a createBackup --param backup_retain=
<max_number_of_backups>
```

其中，`<max_number_of_backups>` 是网络文件夹中可存储的最大备份数量。默认值是 10。如果网络文件夹已包含最大数量的备份，则下一个备份将覆盖最早的备份。如果减少参数值（例如，在手动创建备份或配置备份计划时，将 `<max_number_of_backups>` 设置为 3），KDT 将删除除最近三个备份之外的所有备份。

创建的备份副本将保存到配置的网络文件夹中。KDT 日志提供有关备份操作结果的详细信息，包括操作的成功或失败、执行的日期和时间以及备份副本的名称和位置。

查看 Kaspersky Next XDR Expert 数据的备份

查看备份列表

要查看备份列表：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a listBackups
```

备份列表随即显示。该列表显示备份大小、状态、备份执行日期和时间，以及 `NAME` 列中显示的备份名称和 `BACKUPID` 列中显示的唯一备份标识符。

查看备份的详细信息

要查看备份的详细信息：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a describeBackup --param backup_id='<backup_name>'
```

其中，`<backup_name>` 是显示在备份列表的 `NAME` 列中的备份名称。

将显示备份的详细信息。

如有必要，您可以使用自定义操作删除备份。为此，在KDT实用程序所在的管理员主机上运行以下命令：

```
./kdt invoke backup-operator -a deleteBackup --param
backup_id='01kp2qkprmwaajpd8cgy3zeqbt'
```

从备份副本恢复 Kaspersky Next XDR Expert 数据

恢复数据之前，请确保使用与创建备份所用的同版本 Kaspersky Next XDR Expert。

仅当 DBMS 未包含在 Kubernetes 集群中时，才支持备份和恢复 Kaspersky Next XDR Expert 数据。将 DBMS 安装到 Kubernetes 集群的配置仅用于熟悉该解决方案，不用于处理标准工作任务。

要从备份副本恢复 Kaspersky Next XDR Expert 数据：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a restoreFromBackup --param backup_id='<backup_id>'
```

其中，`<backup_id>` 是显示在已创建备份列表的 `BACKUPID` 列中的唯一备份标识符。

将从备份中恢复 Kaspersky Next XDR Expert 数据。KDT会在日志文件中输出有关恢复操作成功或失败以及总耗时的信息。

要查看从备份副本恢复 Kaspersky Next XDR Expert 数据的状态：

在管理员主机上，运行以下命令：

```
./kdt invoke backup-operator -a restoreStatus
```

停止 Kubernetes 集群节点

您可能需要停止整个 Kubernetes 集群或暂时分离集群的某个节点以进行维护。

在虚拟环境中，请勿关闭托管活动 Kubernetes 集群节点的虚拟机。

如果您没有超级用户权限，则需要获取该权限，或者在以下每个命令前加上 `sudo` 来提升权限，例如： `sudo k0s status`、 `sudo k0s stop`。

周三建议您参阅操作系统的官方文档，以获取有关要执行的命令的详细信息。

停止多节点 Kubernetes 集群

要停止多节点 Kubernetes 集群（多节点部署方案）：

1. 登录到工作节点并执行正常关机：

   a. 运行以下命令停止节点：

   ```
   k0s stop
   ```

   b. 运行以下命令检查节点是否已停止：

   ```
   k0s status
   ```

   c. 运行以下命令关闭节点：

   ```
   shutdown -now
   ```

   出于安全原因，我们不建议您使用 `--force` 密钥。

2. 对所有工作节点重复此过程。

3. 登录到主节点并按照步骤 a-c 所述执行正常关机。

如果 Kubernetes 集群中的活动节点数少于三个，则可能会出现部分功能丢失，直到恢复初始节点数。
关闭主节点时，将无法管理集群（包括通过 kdt 实用工具进行管理），直到主节点重新启动。

停止单节点 Kubernetes 集群

要停止单节点 Kubernetes 集群（单节点部署方案）：

登录到主节点并按照步骤 a-c 所述执行正常关机。

启动 Kubernetes 集群

要启动 Kubernetes 集群：

1. 操作系统加载后，运行以下命令：

   ```
   k0s start
   ```

2. 运行以下命令检查节点是否已启动：

   ```
   k0s status
   ```

3. 对于多节点部署方案，对所有节点重复此过程。

使用证书访问公共 Kaspersky Next XDR Expert 服务

要使用公共 Kaspersky Next XDR Expert 服务，您可以使用自签名证书或自定义证书。默认情况下，Kaspersky Next XDR Expert 使用自签名证书。

以下 Kaspersky Next XDR Expert 公共服务需要证书：

- `<console_host>.<smp_domain>`—访问 OSMP 控制台界面。
- `<ksc_host>.<smp_domain>`—与管理服务器交互。
- `<api_host>.<smp_domain>`—访问 Kaspersky Next XDR Expert API。
- `<monitoring_host>.<smp_domain>`—访问 OSMP 指标。
- `<kuma_host>.<smp_domain>`—访问 SIEM 组件。

公共 Kaspersky Next XDR Expert 服务的 FQDN 由配置文件中指定的主机名和域名组成。对于在部署期间定义了自签名或自定义证书的公共 Kaspersky Next XDR Expert 服务，在 `pki_host_list` 安装参数中指定其地址列表。

自定义证书必须指定为 PEM 格式的文件，并且包含完整的证书链（或仅一个证书）和未加密的私钥。

您可以从组织的私钥基础设施 (PKI) 中指定中间证书。公共 Kaspersky Next XDR Expert 服务的自定义证书由此自定义中间证书颁发。或者，您可以为每个公共服务指定叶证书。如果仅为部分公共服务指定叶证书，则会为其他公共服务颁发自签名证书。

对于 `<console_host>.<smp_domain>`、`<kuma_host>.<smp_domain>`、`<monitoring_host>.<smp_domain>` 和 `<api_host>.<smp_domain>` 公共服务，您只能在部署之前在配置文件中指定自定义证书。指定 `intermediate_bundle` 和 `intermediate_enabled` 安装参数以使用自定义中间证书。自定义中间证书的有效期必须为 399 天或更长。

如果要使用自定义叶证书来访问公共 Kaspersky Next XDR Expert 服务，请指定相应的 `console_bundle`、`admsrv_bundle`、`kuma_bundle`、`monitoring_bundle` 和 `api_bundle` 安装参数。将 `intermediate_enabled` 参数设置为 `false`，并且不要指定 `intermediate_bundle` 参数和 `pki_host_list` 参数。自定义叶子证书的有效期必须为399天或以上。

对于 <ksc_host>.<smp_domain> 服务，您可以使用 klsetsrvcert 实用程序将颁发的管理服务器自签名证书替换为自定义证书。

不支持证书自动轮换。请留意证书的有效期，并在证书到期时更新证书。

要更新自定义证书：

1. 在管理员主机上，导出当前配置文件。
2. 在导出的配置文件中，在 `intermediate_bundle` 安装参数中指定新的自定义中间证书的路径。如果为每个公共服务使用自定义叶子证书，请指定 `console_bundle`、`admsrv_bundle`、`kuma_bundle`、`monitoring_bundle` 和 `api_bundle` 安装参数。
3. 运行以下命令并指定修改后的配置文件的完整路径：

   ```
   ./kdt apply -i <配置文件完整路径>
   ```

   自定义证书将进行更新。

计算和更改用于存储管理服务器数据的磁盘空间

管理服务器数据包括以下对象：

- 有关资产（设备）的信息。
- 有关在管理服务器上针对所选客户端设备记录的信息事件。
- 有关包含资产的域的信息。
- 应用程序控制组件的数据。
- 更新。共享文件夹额外需要至少 4 GB 来存储更新。
- 安装包。如果某些安装包存储在管理服务器上，共享文件夹还需要额外的可用磁盘空间，其大小等于所有可供安装的安装包的总大小。
- “远程安装”任务。如果管理服务器上存在任何远程安装任务，需要与要安装的所有安装包大小相当的额外的可用磁盘空间量。

计算用于存储管理服务器数据的最小磁盘空间

可以使用以下公式粗略估算用于存储管理服务器数据所需的最小磁盘空间：

```
(724 * C + 0.15 * E + 0.17 * A + U), KB
```

其中：

- C 是资产（设备）数量。
- E 要存储的事件的数量。
- A 是域对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 组织单元
- U 是更新的大小（至少 4 GB）。

如果禁用域轮询，则 A 被视为等于零。

该公式用于计算存储来自受管理设备的典型数据和更新的典型大小所需的磁盘空间。该公式不包含与应用程序控制组件、安装包和远程安装任务的受管理设备数量无关的数据占用的磁盘空间量。

更改用于存储管理服务器数据的磁盘空间

在部署 Kaspersky Next XDR Expert 之前，在配置文件中指定分配用于存储管理服务器数据的可用磁盘空间量（`ksc_state_size` 参数）。考虑使用公式计算的最小磁盘空间。

要检查 Kaspersky Next XDR Expert 部署后用于存储管理服务器数据的磁盘空间占用情况：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke ksc --action getPvSize
```

将显示所需的可用磁盘空间量（以 GB 为单位）。

要在部署 Kaspersky Next XDR Expert 后更改用于存储管理服务器数据的磁盘空间量：

在 KDT 实用程序所在的管理员主机上，运行以下命令并指定所需的可用磁盘空间量（以 GB 为单位）（例如，“50Gi”）：

```
./kdt invoke ksc --action setPvSize --param ksc_state_size='<new_disk_space_amount>Gi'
```

将更改分配用于存储管理服务器数据的可用磁盘空间量。

查看和更改 KUMA Core 和 Metrics 服务的磁盘空间

您可以查看当前分配给 KUMA Core 和 Metrics 服务运行的磁盘空间。如有需要，您可以更改已分配的磁盘空间。

查看当前已分配的磁盘空间

查看磁盘空间的命令不会影响正在运行的服务。

要查看分配给 KUMA Core 的磁盘空间：

在管理员主机上，运行以下命令：

```
./kdt invoke kuma --action getCorePvcSize
```

要查看分配给 Metrics 服务的磁盘空间：

在管理员主机上，运行以下命令：

```
./kdt invoke kuma --action getMetricsPvcSize
```

更改当前已分配的磁盘空间

这些命令会更改`core_disk_request`和`metrics_disk_request`参数。运行命令时，相应的服务会停止，磁盘空间会更改，然后服务会重新启动。仅当命令成功完成时，应用程序才会更新`core_disk_request`和`metrics_disk_request`参数。

您只能增加当前磁盘空间。如果您尝试设置小于当前值的磁盘空间，命令将返回错误。在这种情况下，服务不会停止。

如果服务停止后发生错误，应用程序会尝试重启服务并保留之前的磁盘空间值。

要更改为 KUMA Core 分配的磁盘空间，请执行以下命令：

在管理员主机上，运行以下命令：

```
./kdt invoke kuma --action setCorePvcSize --param core_disk_request=<值>
```

其中，`<值>`是新的磁盘空间大小，例如`50Gi`。

要更改为 Metrics 服务分配的磁盘空间，请执行以下命令：

在管理员主机上，运行以下命令：

```
./kdt invoke kuma --action setMetricsPvcSize --param metrics_disk_request=<值>
```

其中，`<值>`是新的磁盘空间大小，例如`50Gi`。

查看和更改对象存储大小

对象存储是存储临时行动手册数据、警报和事故文件以及支持外部集成的S3 API的组件。如果对象存储卷空间即将用尽，您可以查看当前为其分配的大小。您可以使用 KDT 实用程序更改存储大小。这样可以防止存储溢出和相关的服务中断。

要查看对象存储容量：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke objectstorage --action getDataPvSize
```

命令输出中会显示对象存储PV的当前分配容量（以GB为单位）（例如，10GB）。

要增加对象存储容量：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke objectstorage --action setDataPvSize --param volumeDataSize=<new_size>
```

其中，`<new_size>` 是所需的对象存储容量，以 GB 为单位（例如，11GB）。该值必须大于当前容量。

对象存储的容量随即调整。新的对象存储容量无需重启服务即可生效。

增加可观测性存储大小

可观测性组件是一个用于集中查看事件、威胁和资产的组件。KDT 允许您增加可观测性组件 (VictoriaMetrics) 的存储大小。

要手动增加可观测性组件的存储大小，

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke observability --action increaseVMPvSize --param prometheus_size=<new_size>
```

其中，`<new_size>` 是所需的存储大小，以 GB 为单位（例如，11Gi）。该值必须大于当前容量。

可观测性组件的存储大小会调整为指定值。

Kubernetes集群证书轮换

KDT 允许您轮换Kubernetes集群证书，这些证书用于访问Kubernetes集群以及Kaspersky Next XDR Expert的基础设施组件。Kubernetes集群证书位于Kubernetes集群内的目标主机上。

若要手动轮换Kubernetes集群证书，

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke foreach --action RotateK0sConfig
```

新的Kubernetes集群证书随即生成。默认保留期是10年。

更新Bootstrap时，Kubernetes集群证书会自动更新。

注册表访问凭证轮换

KDT允许您根据组织的信息安全要求轮换注册表访问凭据。

若要手动轮换注册表访问凭据，

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke bootstrap --action RotateRegistryCreds
```

注册表访问凭据随即更新。

更新Bootstrap时，注册表访问凭据会自动更新。

DBMS 凭证和证书轮换

KDT 允许您轮换用于连接到 DBMS 的 DBMS 凭证和证书。您可以根据组织的信息安全要求轮换 DBMS 机密信息。

要手动轮换 DBMS 凭证和证书，

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke foreach --action rotatedbcreds
```

DBMS 凭证和证书已更新。

添加用于安装附加 KUMA 服务的主机

如果需要扩展存储，或者因为事件流增加而添加新的收集器和关联器，则可以添加其他主机来安装 KUMA 服务。

必须在 expand.inventory.yml 文件中指定其他主机的参数。此文件位于分发包中，其中包含传输存档文件、KDT、配置文件和其他文件。在 expand.inventory.yml 文件中，您可以一次性为收集器、关联器和存储同时指定多个其他主机。确保满足所选主机的硬件、软件和安装要求。

要在 expand.inventory.yml 文件中指定的主机上准备所需的基础架构，需要创建服务目录，并将安装服务所需的文件添加到这些目录。要准备基础架构，请运行以下命令并指定 expand.inventory.yml 文件：

```
./kdt invoke kuma --action addHosts --param host_inventory='<path_to_inventory_file>'
```

在 expand.inventory.yml 文件中指定的主机上，会创建服务目录，安装服务所需的文件将被添加到这些目录中。

用于安装 KUMA 服务的附加 KUMA 清查文件示例（expand.inventory.yml 文件）

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
    kuma_collector:
      hosts:
        kuma1.example.com:
            ansible_host: 0.0.0.0
        kuma2.example.com:
            ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma3.example.com:
            ansible_host: 0.0.0.0
        kuma4.example.com:
            ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma5.example.com:
            ansible_host: 0.0.0.0
        kuma6.example.com:
            ansible_host: 0.0.0.0
```

添加附加存储、收集器或关联器

您可以向现有基础架构添加额外的存储集群、收集器或关联器。如果要添加多个服务，建议按以下顺序安装：存储、收集器和关联器。

要添加额外的存储集群、收集器或关联器：

1. 在 OSMP 控制台的主菜单中，转到“**设置**” → “**KUMA**”。
2. 在OSMP控制台的KUMA部分，为要在准备好的主机上安装的每个KUMA服务（存储、收集器和关联器）创建一个资源集。

3. 为存储、收集器和关联器创建服务。

4. 获取服务标识符以绑定创建的资源集和 KUMA 服务：

   a. 在 OSMP 解决方案中，转到 **资源** → **活动服务**。

   b. 选择所需的 KUMA 服务，然后单击“**复制 ID**”按钮。

5. 在 expand.inventory.yml 清查文件的 KUMA_storage、KUMA_collector 和 KUMA_correlator 部分列出的每台准备好的主机上安装 KUMA 服务。在每台机器上，在安装命令中，指定与主机对应的服务 ID。运行相应的命令来安装 KUMA 服务：

   - 存储的安装命令：

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
     ```

   - 收集器的安装命令：

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port>
     ```

   - 关联器的安装命令：

     ```
     sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
     ```

     收集器和关联器的安装命令会在安装向导的 **扫描** 选项卡上自动生成。用于通信的端口会自动添加到命令中。使用生成的命令在主机上安装收集器和关联器。这能确保命令中指定的、用于与服务通讯的端口处于可用状态。

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。KUMA Core 的 FQDN 是 <kuma_host>.<smp_domain>。用于连接 KUMA Core 的端口无法更改。默认情况下使用端口 7210。

   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

     为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。

   - <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。

   - <API port> 是用于与已安装组件通信的端口。

   将安装附加的 KUMA 服务。

将主机添加到现有存储

您可以通过将主机添加为新的存储集群节点来扩展现有存储（存储集群）。

要将主机添加到现有存储：

1. 在 OSMP 控制台的主菜单中，转到“**设置**” → “**KUMA**”。
2. 将新节点添加到存储集群。为此，请编辑现有存储集群的设置：
   a. 在“**资源**”→“**存储**”部分，选择一个现有存储并打开该存储进行编辑。
   b. 在“**ClickHouse 集群节点**”部分，单击“**添加节点**”，然后在新节点的字段中指定角色。从 expand.inventory.yml 文件的 kuma_storage 部分指定相应的主机域名，然后指定新节点的角色。
   c. 保存更改。

   您无需创建单独的存储，因为您正在将服务器添加到现有存储集群。
3. 在OSMP控制台的KUMA部分为每个添加的存储集群节点创建存储服务，然后将服务绑定到存储集群。
4. 获取每个准备好的主机的存储服务标识符以安装 KUMA 服务：
   a. 在OSMP控制台的KUMA部分，前往**资源→活动服务**。
   b. 选择所需的 KUMA 服务，然后单击“**复制 ID**”按钮。
5. 在 expand.inventory.yml 清查文件的 kuma_storage 部分列出的每个准备好的主机上安装存储服务。在每台机器上，在安装命令中，指定与主机对应的服务 ID。运行以下命令来安装存储服务：

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。KUMA Core 的 FQDN 是 <kuma_host>.<smp_domain>。用于连接 KUMA Core 的端口无法更改。默认情况下使用端口 7210。
   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。

- <service ID> 是从 Web 界面复制的 KUMA 服务 ID。

其他主机将添加至存储集群。

在 distributed.inventory.yml 清查文件中指定添加的主机，以确保在 KUMA 组件更新时该文件包含最新信息。

更换使用 KUMA 存储的主机

要将使用 KUMA 存储的主机替换为另一个主机：

1. 填写 expand.inventory.yml 文件，指定要替换的主机的参数。
2. 运行以下命令，指定 expand.inventory.yml 文件以删除主机：

   ```
   ./kdt invoke kuma --action removeHosts --param
   host_inventory='<path_to_inventory_file>'
   ```

3. 填写 expand.inventory.yml 文件，指定要替换先前主机的新主机的参数，然后运行以下命令：

   ```
   ./kdt invoke kuma --action addHosts --param host_inventory='<path_to_inventory_file>'
   ```

4. 按照添加 KUMA 服务新主机说明中的步骤 2–6，添加一台搭载了 KUMA 存储的新主机。

搭载了 KUMA 存储的主机被另一个主机替换。

如果您的存储配置包括一个包含两个副本的分片，并且您按照上述步骤将第二个副本主机替换为新的主机，那么在安装新副本时可能会发生错误。在这种情况下，新副本将无法运行。

要在添加分片的新副本时修复错误：

1. 在另一台主机（该主机拥有与错误添加的副本同属一个分片的副本）上，使用以下命令启动 ClickHouse 客户端：

   ```
   /opt/kaspersky/kuma/clickhouse/bin/client.sh
   ```

   如果此主机不可用，请在同一存储集群中包含副本的任何其他主机上运行客户端。

2. 运行命令以删除有关要替换的主机的数据。

   - 如果拥有与错误添加的副本同属一个分片的副本的主机处于可用状态，请运行以下命令：

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM TABLE
     kuma.events_local_v2
     ```

   - 如果您正在使用另一个带副本的存储集群主机，则运行以下命令：

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM ZKPATH
     '/clickhouse/tables/kuma/<shard number of read-only node>/kuma/events_local_v2
     ```

3. 运行以下命令来恢复添加的带副本主机的运行：

```
SYSTEM RESTORE REPLICA kuma.events_local_v2
```

添加的带副本主机将恢复可运行状态。

使用部署在虚拟机上的 Kaspersky Next XDR Expert

如果您已在虚拟机上部署了 Kaspersky Next XDR Expert，则不建议在解决方案运行时使用虚拟机管理程序来拍摄快照或迁移这些虚拟机。在这种情况下，Kaspersky Next XDR Expert 将无法正常运行。为确保 Kaspersky Next XDR Expert 正常运行，请在创建快照或执行迁移之前停止 Kubernetes 集群内的所有虚拟机。

Kaspersky Next XDR Expert 的演示部署

如果您想了解 Kaspersky Next XDR Expert，则可以执行该解决方案的演示部署。

使用 Kaspersky Next XDR Expert 的演示部署（其中 DBMS 安装在 Kubernetes 集群中）仅用于了解该解决方案。不建议使用此方法来解决标准工作任务。对于标准用法，请执行多节点或单节点部署。

在演示部署中，所有 Kaspersky Next XDR Expert 组件都安装在 Kubernetes 集群的一个或多个节点上。

下列方案描述了单个节点上的演示部署。单节点部署需要的资源较少，因此更常用于演示部署。在单个节点上的演示部署中，Kubernetes 集群、Kaspersky Next XDR Expert 组件和 DBMS 安装在一个目标主机上。此外，您需要管理员主机来部署和管理 Kubernetes 集群与 Kaspersky Next XDR Expert，以及用于安装 KUMA 服务的目标主机。

在单节点配置中，您至少需要三台主机：

- 1台管理员主机
- 1台目标主机，用于安装 Kubernetes 集群、Kaspersky Next XDR Expert 组件和 DBMS
- 1台 KUMA 目标主机，用于安装 KUMA 服务

演示部署和标准部署之间的主要区别在于 DBMS 的位置。在标准部署（多节点或单节点）中，DBMS 安装在集群外的主机上。在演示部署中，DBMS 安装在集群内的目标主机上。

在部署 Open Single Management Platform 和 Kaspersky Next XDR Expert 组件之前，建议先阅读“强化指南”。

按照此方案，您可以准备演示部署的基础架构、准备配置文件，并使用卡巴斯基部署工具包实用程序（以下简称 KDT）部署解决方案。

演示部署方案分阶段进行：

1. **下载包含 Kaspersky Next XDR Expert 组件的分发包**

分发包中包含以下组件：

- 包含Kaspersky Next XDR Expert 组件以及Kaspersky Next XDR Expert和KDT最终用户授权许可协议的传输存档文件

  组件使用RSA密钥和GOST R 34.11-2012密钥签名。

- 包含KDT实用程序、配置文件和KUMA清查文件模板的存档文件

2. **准备管理员主机和目标主机**

   为 Kaspersky Next XDR Expert 的演示部署准备所选的管理员主机和目标主机。

   操作说明：准备管理员主机和目标主机

3. **准备 KUMA 主机**

   准备 KUMA 目标主机以安装 KUMA 服务（收集器、关联器和存储）。

   操作说明：准备主机以安装 KUMA 服务

4. **准备用于安装 KUMA 服务的 KUMA 清查文件**

   以 YAML 格式准备 KUMA 清查文件。KUMA 清查文件包含用于安装 KUMA 服务的参数。

   操作说明：准备 KUMA 清查文件

5. **准备配置文件**

   以 YAML 格式准备配置文件。配置文件包含目标主机参数和一组 Kaspersky Next XDR Expert 组件安装参数。

   操作说明：指定安装参数

6. **部署 Kaspersky Next XDR Expert**

   使用 KDT 部署 Kaspersky Next XDR Expert。KDT 会自动部署 Kubernetes 集群，Kaspersky Next XDR Expert 组件和其他基础架构组件均安装于该集群中。

   操作说明：安装 Kaspersky Next XDR Expert

7. **安装 KUMA 服务**

   在准备好的 KUMA 目标主机（位于 Kubernetes 集群外）上安装 KUMA 服务（收集器、关联器和存储）。

   操作说明：安装 KUMA 服务

8. **配置与 Kaspersky Anti Targeted Attack Platform 的集成**

   安装中央节点以接收来自 Kaspersky Anti Targeted Attack Platform 的遥测数据，随后配置 Kaspersky Next XDR Expert 与 KATA/KEDR 的集成，从而对接入 Kaspersky Endpoint Detection and Response 服务器的资产执行威胁响应操作管理。

   如有必要，您可以安装多个“中央节点”组件，既可以将它们彼此独立使用，也可以将其组合在一起，在分布式解决方案模式下进行集中管理。要组合多个中央节点组件，您必须将安装了这些组件的服务器组织成一个层次结构。

   > 配置中央节点服务器时，您必须在“**存储**”字段中指定尽可能小的值，以避免 Kaspersky Next XDR Expert 和 KEDR 数据库之间的数据重复。

准备管理员主机和目标主机

演示部署的准备工作包括配置管理员主机和目标主机。在单个节点上的演示部署中，Kubernetes 集群、Kaspersky Next XDR Expert 组件和 DBMS 安装在一个目标主机上。准备好目标主机并指定配置文件后，您将能够使用 KDT 在目标主机上部署 Kaspersky Next XDR Expert。

使用 Kaspersky Next XDR Expert 的演示部署（其中 DBMS 安装在 Kubernetes 集群中）仅用于了解该解决方案。不建议使用此方法来解决标准工作任务。对于标准用法，请执行多节点或单节点部署。

准备管理员主机

首先需要准备一个设备作为管理员主机，KDT 将从该设备启动。该主机既可以纳入部署期间由 KDT 创建的 Kubernetes 集群，也可以不纳入。如果管理员主机不包含在集群中，它将仅用于部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert。如果管理员主机包含在集群中，它还将充当用于运行 Kaspersky Next XDR Expert 组件的目标主机。在这种情况下，只有一台主机用于部署和运行该解决方案。

要准备管理员主机：

1. 确保管理员主机上的硬件和软件满足 KDT 的要求。
2. 在临时文件目录（默认情况下为 `/tmp`）中为 KDT 分配至少 10 GB 的可用空间。如果此目录中没有足够的可用空间，请运行以下命令指定另一个目录的路径：

   ```
   export TMPDIR=<new_directory>/tmp
   ```

3. 配置容器运行时。使用以下容器运行时之一：

   - KDT 内置容器运行时（基于 runc）。

     要安装该运行时，请运行以下命令：

     ```
     sudo ./kdt init
     ```

     如果内置容器运行时不适合您的环境，您可以改用 Docker 容器运行时。

   - Docker 容器运行时。

     安装适用于Docker 25 或更高版本的套件。请勿从操作系统维护者的存储库中安装非官方的 Docker 软件包分发版。

     如果 Docker 密钥环无法自动下载，请手动下载：

     a. 在浏览器中开放 https://download.docker.com/linux/ubuntu/gpg 链接，将密钥保存为 docker.asc。

     b. 执行以下命令：

     ```
     sudo mv docker.asc /etc/apt/keyrings/docker.asc
     ```

     用于 Docker 数据存储的磁盘分区（默认情况下为 `/var/lib/docker`）必须至少有 60 GB 的可用空间。

执行安装后步骤，配置管理主机以确保Docker正常运行：

```
sudo groupadd docker
sudo usermod -aG docker $USER
newgrp docker
sudo systemctl enable docker.service
sudo systemctl enable containerd.service
sudo systemctl status docker.service
```

4. 对于将被纳入该集群的管理员主机，请执行额外的准备操作：

   a. 由于该设备将充当管理员主机和目标主机，请确保其满足单节点部署的要求。

   b. 确保管理员主机支持 cgroup v2 技术。

准备目标主机

目标主机是用于部署 Kaspersky Next XDR Expert 并包含在 Kubernetes 集群中的物理机或虚拟机。目标主机管理 Kubernetes 集群、存储元数据，Kaspersky Next XDR Expert 组件也在此主机上运行。演示部署的最低集群配置包括一个充当主节点和工作节点的目标主机。此主工作节点上安装了 Kubernetes 集群、DBMS 和 Kaspersky Next XDR Expert 组件。

KUMA 服务（收集器、关联器和存储）可以完全安装在集群内部的主要工作节点上，也可以完全安装在 Kubernetes 集群外部的独立主机上，或者部分安装在 Kubernetes 集群内部，部分安装在 Kubernetes 集群外部。

如果要从目标主机运行 Kaspersky Next XDR Expert 部署程序，则必须按照前面的步骤将此主机配置为管理员主机，然后执行目标主机的准备工作。

要准备目标主机：

1. 确保目标主机上的硬件和软件满足单节点部署的要求（因为演示部署和单节点部署的方案类似）。

   如果KUMA服务安装在集群内部，则目标主机必须满足安装KUMA服务所需的硬件、软件和安装要求。

   为确保 Kaspersky Next XDR Expert 正常运行，搭载 Ubuntu 系列操作系统的目标主机，其 Linux 内核版本必须为 5.15.0.107 或更高版本。

   为确保 Kubernetes 集群及其组件正常运行，必须在所有集群节点上禁用交换分区。如果节点上启用了交换分区，KDT 将在部署期间自动将其禁用。

   除非目标主机将用作管理员主机，否则请勿在目标主机上安装 Docker。KDT 将在部署期间安装所有必要的软件和依赖项。

2. 确保挂载在 `/var` 的文件系统在目标主机上至少有 360 GB 的可用空间。

   我们建议将 `/opt/lvp/hot` 目录放置在专用的高性能磁盘子系统上，并将 `/opt/lvp/cold` 目录放置在单独的高容量磁盘子系统上。

3. 如果尚未安装 sudo 软件包，请安装此包。对于 Debian 系列操作系统，请安装 UFW 软件包。

4. 配置 /etc/environment 文件。如果您组织的基础设施使用代理服务器访问互联网，您还需要将目标主机连接到互联网。

5. 如果主工作节点具有 UFW 配置，则允许 IP 转发。在 `/etc/default/ufw` 文件中，将 `DEFAULT_FORWARD_POLICY` 设置为 `ACCEPT`。

6. 提供对软件包存储库的访问权限，该存储库中存储了 Kaspersky Next XDR Expert 所需的以下软件包：

   - nfs-common
   - containerd
   - cron
   - cryptsetup
   - cryptsetup-bin
   - netcat-traditional
   - nfs-common
   - open-iscsi
   - python3-cffi-backend
   - python3-cryptography
   - python3-netaddr
   - python-apt-common
   - systemd
   - tar

   KDT 将在部署期间尝试从软件包存储库安装这些包。您也可以手动安装这些软件包。

7. 确保以下软件包安装在主工作线程节点上：

   - python3-apt
   - curl

   在使用KDT从软件包存储库部署期间，这些软件包不会安装。如果尚未安装这些软件包，则必须手动安装。

8. 为目标主机和 Kubernetes 集群网关预留静态 IP 地址。

   Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。

   由于您将 DBMS 安装在 Kubernetes 集群内部，因此网关 IP 地址是一个 IP 范围（例如，192.168.0.1 — 192.168.0.2）。该范围内的第一个 IP 地址是 Kaspersky Next XDR Expert 服务的地址（不包括 DBMS 的 IP 地址）。该范围内的第二个 IP 地址是 DBMS 的 IP 地址。

   确保目标主机和 Kubernetes 集群网关位于同一广播域中。

9. 在您的 DNS 服务器上，注册服务 FQDN 以连接到 Kaspersky Next XDR Expert 服务。

默认情况下，Kaspersky Next XDR Expert 服务可通过以下地址访问：

- <console_host>.<smp_domain> — 访问 OSMP 控制台界面。
- <ksc_host>.<smp_domain> — 与管理服务器交互。
- <kuma_host>.<smp_domain>—访问SIEM组件。
- <api_host>.<smp_domain> — 访问 Kaspersky Next XDR Expert API。
- <monitoring_host>.<smp_domain> — 访问 OSMP 指标。
- <xdr_edr_ingress_host>.<smp_domain>—与代理服务器交互。

  其中<console_host>、<ksc_host>、<kuma_host>、<api_host>、<monitoring_host>和<xdr_edr_ingress_host>是服务主机名，<smp_domain>是服务域名。这些参数是服务 FQDN 的一部分，您可以在配置文件中指定。如果您未指定服务主机名的自定义值，则使用默认值：`console_host` — “`console`”、`ksc_host` — “`admsrv`”、`kuma_host` — “`kuma`”、`api_host` — “`api`”、`monitoring_host` — “`monitoring`”、`"xdr_edr_ingress_host"`—`"agentserver"`。

列出的服务 FQDN 必须解析为 Kubernetes 集群的 IP 地址。例如，如果 Kubernetes 集群地址为 10.80.23.182，则服务 FQDN 将按如下方式解析为 IP 地址：

- <console_host>.<smp_domain>—10.80.23.182
- <ksc_host>.<smp_domain>—10.80.23.182
- <kuma_host>.<smp_domain>—10.80.23.182
- <api_host>.<smp_domain>—10.80.23.182
- <xdr_edr_ingress_host>.<smp_domain>—10.80.23.182

10. 创建将用于部署 Kaspersky Next XDR Expert 的用户账户。

    这些账户用于 SSH 连接，并且必须能够在不输入密码的情况下提升权限 (sudo)。为此，将创建的用户账户添加到 `/etc/sudoers` 文件。

    查看详情

    要将创建的用户账户添加到 `/etc/sudoers` 文件：

    1. 运行以下命令：

       ```
       sudo useradd -m -s /bin/bash <user_name>
       sudo usermod -aG sudo <user_name>
       ```

    2. 使用以下命令打开 `/etc/sudoers` 文件：

       ```
       sudo visudo
       ```

3. 在 `# Allow members of group sudo to execute any command` 部分的末尾添加以下行：

   ```
   <user_name> ALL=(ALL) NOPASSWD: ALL
   ```

   其中，`<user_name>` 是所创建用户的名称。

4. 保存并关闭 `/etc/sudoers` 文件。

11. 配置管理员和目标主机之间的 SSH 连接：

    a. 在管理员主机上，使用 ssh-keygen 实用程序生成 SSH 密钥，不设置密码短语。

    b. 使用 ssh-copy-id 实用程序将公钥复制到目标主机（例如，复制到 `/home/<user_name>/.ssh` 目录）。

    如果使用目标主机作为管理员主机，则还必须将公钥复制到该主机。

12. 为确保 Kaspersky Next XDR Expert 组件正常运行，请在管理员主机和目标主机的防火墙上打开所需的端口（如有必要）。

13. 在管理员主机和目标主机上通过网络时间协议 (NTP) 配置时间同步。

14. 如有必要，请准备自定义证书以便使用 Kaspersky Next XDR Expert 公共服务。

    您可以为每项服务使用一个基于组织根证书或叶证书颁发的中间证书。准备好的自定义证书将代替自签名证书。

指定安装参数

在单个节点上部署 Kaspersky Next XDR Expert 所使用的配置文件包含多节点和单节点部署所需的安装参数。此外，此配置文件还包含仅适用于单节点部署的参数（`openbao_ha_mode`、`openbao_standalone` 和 `default_class_replica_count`）。配置文件模板 (singlenode.smp_param.yaml.template) 位于压缩文件（包含 KDT 实用程序）的分发包中。此配置文件可用于演示安装。

使用 Kaspersky Next XDR Expert 的演示部署（其中 DBMS 安装在 Kubernetes 集群中）仅用于了解该解决方案。我们不建议将此方法用于常规生产用途。对于标准用法，请执行多节点或单节点部署。

配置文件模板中并未包含下面列出的所有参数。此模板仅包含在部署 Kaspersky Next XDR Expert 之前必须指定的参数。其余参数设置为默认值，不包含在模板中。您可以手动将这些参数添加到配置文件中以覆盖其原有值。参数值必须遵循下面描述的规则。在部署 Kaspersky Next XDR Expert 期间，KDT 会检查是否正确指定了所需的安装参数。如果配置文件中所需的参数缺失或无效，部署将会中断。

为了使 KDT 与配置文件正确运行，请在文件末尾添加一个空行。

配置文件的`nodes`部分包含下表列出的目标主机参数。

节点部分

参数名称	是否必需	Description
`desc`	是	节点名称。 值必须符合以下规则： • 节点名称的长度必须在 1 到 63 个字符之间。 • 节点名称可以包含以下字符： • 大写 ASCII 字母 (A-Z) • 小写 ASCII 字母 (a-z) • 数字 (0-9) • 连字符 (-) 所有集群节点必须具有唯一的名称。这一要求是安装Kaspersky Next XDR Expert的先决条件之一，并经KDT验证。
`type`	是	节点类型。 对于目标主机，将 `type` 参数设置为 `primary-worker`，以启用**单节点演示部署**。在这种情况下，目标主机将充当主节点和工作线程节点。
`host`	是	节点的 IP 地址。 主工作线程节点必须与 Kubernetes 集群网关位于同一子网中。 节点需要 IPv4 地址。KDT 会自动禁用集群节点上的 IPv6。
`kind`	否	指定将在此节点上安装的 Kaspersky Next XDR Expert 组件的节点类型。 对于**单节点演示部署**，请将此参数留空，因为所有组件都将安装在单个节点上。
`user`	是	在目标主机上创建、供 KDT 连接节点时使用的账户用户名。 值必须符合以下规则： • 用户名长度必须在 1 到 31 个字符之间。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 下划线 (_)、连字符 (-)
`password`	否	连接节点的密码。可以代替由 `ssh_pk` 参数指定的 SSH 密钥。

其他安装参数列在配置文件的“`parameters`”部分，并在下表中说明。

参数部分

参数名称	是否必需	Description
`nwc-language`	是	OSMP 控制台界面的语言是默认指定的。安装完成后，您可以更改 OSMP 控制台语言。 可能的参数值： • `enUS`（默认值） • `ruRu` 如果未在配置文件中指定此参数，则使用默认值。
`ingress_ip`	是	Kubernetes 集群网关的预留静态 IPv4 地址。 Kubernetes 集群网关用于连接安装在 Kubernetes 集群内的 Kaspersky Next XDR Expert 组件。网关必须与主工作线程节点位于同一子网中。 Kubernetes 集群网关需要 IPv4 地址。KDT 会自动在集群节点上禁用 IPv6。 此参数的值不能是执行部署的同一主机的IP地址。 对于**演示部署**，当您在集群内部安装 DBMS 时，DBMS IP 地址与集群网关 IP 地址相同。
`ssh_pk`	是	位于管理员主机上的 SSH 密钥的私钥部分的路径，用于通过 KDT 连接到主工作线程节点和部署 KUMA 服务的节点（收集器、关联器和存储）。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。

参数名称	是否必需	Description
admin_password	是	"admin_password"参数指定 KDT 在安装期间创建的 Kaspersky Next XDR Expert 用户账户的密码。此账户的默认用户名是"admin"。 主管理员角色已分配给此用户账户。 密码必须符合以下规则： • 用户密码不能少于10个字符或超过256个字符。 • 密码必须包含以下组中三组的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密码不得包含任何空格或".@"组合。 当您手动指定"admin_password"参数值（而不是通过"部署向导"）时，请确保该值符合 YAML 标准对字符串中值的要求： • 包含特殊字符的参数值必须用单引号括起来。 • 参数值中的任何单引号（'）必须成对输入，才能实现该单引号的转义。 例如：用户账户密码"Any_pass%1234'5678"90"必须指定为"admin_password"参数的值"'Any_pass%1234''5678"90'"。
low_resources	是	指示 Kaspersky Next XDR Expert 以有限的计算资源安装在目标主机上的参数。 对于**单个节点上的演示部署**，将 low_resources 参数设置为 true，这样 Kaspersky Next XDR Expert 组件将需要更少的内存和 CPU 资源。此外，如果启用了此参数，将分配 4 GB 的可用磁盘空间以在目标主机上安装 KUMA Core。
openbao_ha_mode	是	该参数用于指示是否以高可用 (HA) 模式运行密钥存储。 对于**单个节点上的演示部署**，将 openbao_ha_mode 参数设置为 false。
openbao_standalone	是	该参数用于指示是否以独立模式运行密钥存储。 对于**单个节点上的演示部署**，将 openbao_standalone 参数值设置为 true。
default_class_replica_count	是	存储 Kaspersky Next XDR Expert 组件和 KDT 的服务数据所使用的磁盘卷数量。默认值为 3。 对于**单个节点上的演示部署**，将 default_class_replica_count 参数值设置为 1。
core_disk_request	是	指定运行 KUMA Core 所需的磁盘空间量的参数。 如果未指定 core_disk_request 参数，并且 low_resources 参数设置为 false 或未指定，则 KUMA Core 运行所需的默认磁盘空间量为 100 GB。 如果未指定 core_disk_request 参数，并且 low_resources 参数设置为 true，则 KUMA Core 运行所需的默认磁盘空间量为 4 GB。 您可以在应用程序部署后更改 core_disk_request 参数。
inventory	是	位于管理员主机上的 KUMA 清查文件的路径。清查文件包含用于部署 Kubernetes 集群中未包含的 KUMA 服务的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。如果所有 KUMA 服务都将安装在集群内，请将 inventory 参数设置为 /dev/null。
host_inventory	否	位于管理员主机上的附加 KUMA 清查文件的路径。此文件包含用于部分添加或删除搭载 KUMA 服务的主机的安装参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 如果要执行 Kaspersky Next XDR Expert 的初始部署或运行需要配置文件的自定义操作，请保留默认参数值 (/dev/null)。
license	否	位于管理员主机上的KUMA授权许可密钥的路径。 参数值必须是 Linux 文件路径或 Base64 编码的文件内容。 部署完成并登录OSMP后，您可以上传授权许可密钥或指定激活码。

参数名称	是否必需	Description

`nwc_host`
`flow_host`
`hydra_host`
`login_host`
`ksc_host`
`console_host`
`api_host`
`kuma_host`
`monitoring_host`
	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的主机名。服务主机名和域名（`smp_domain` 参数值）是服务 FQDN 的一部分。
		参数的默认值：
		• `nwc_host—"console"`
		• `flow_host—"console"`
		• `hydra_host—"console"`
		• `login_host—"console"`
		• `ksc_host—"admsrv"`
		• `console_host—"console"`
		• `api_host—"api"`
		• `kuma_host—"kuma"`
		• `monitoring_host—"monitoring"`

`smp_domain`	是	公共 Kaspersky Next XDR Expert 服务的 FQDN 中使用的域名。参数值必须满足四级及以下域名的命名要求。 服务主机名和域名是服务 FQDN 的一部分。例如，如果 `console_host` 变量的值为 `console`，并且 `smp_domain` 变量的值为 `smp.local`，则提供对 OSMP 控制台的访问权限的服务的完整名称为 `console.smp.local`。
`pki_host_list`	否	需为其生成自签名证书或自定义证书的 Kaspersky Next XDR Expert 公共服务的主机名称列表。参数值必须是主机名列表，以空格分隔。
`intermediate_enabled`	否	该参数指示是否对公共 Kaspersky Next XDR Expert 服务使用自定义中间证书，而非自签名证书。 可能的参数值： • `true` — 使用自定义中间证书。 • `false` — 使用自签名证书（默认值）。
`intermediate_bundle`	否	用于访问公共 Kaspersky Next XDR Expert 服务的自定义中间证书的路径。如果“`intermediate_enabled`”参数设置为“`true`”，则指定此参数。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。自定义中间证书的有效期必须为 399 天或更长。

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	否	用于访问以下相应公共 Kaspersky Next XDR Expert 服务的自定义叶证书的路径：`<ksc_host>.<smp_domain>`、`<api_host>.<smp_domain>`、`<console_host>.<smp_domain>`、`<kuma_host>.<smp_domain>` 和 `<monitoring_host>.<smp_domain>`。参数值必须是 Linux 文件路径或 Base64 编码的文件内容。
		如果要指定自定义叶证书，请将“`intermediate_enabled`”参数设置为“`false`”，且不要指定“`intermediate_bundle`”参数。

`ksc_state_size`	是	分配用于存储管理服务器数据（更新、安装包和其他内部服务数据）的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。所需的可用磁盘空间量取决于受管理设备的数量和其他参数，并且可以进行计算。 默认值是 30 GB。如果未在配置文件中指定此参数，则使用此值。
`prometheus_size`	是	分配用于存储指标的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>GB”。 推荐的最小值和默认值是 5 GB。如果未在配置文件中指定此参数，则使用默认值。
`grafana_admin_user`	否	用于通过 Grafana 工具查看 OSMP 指标的账户的用户名。 值必须符合以下规则： • 用户名长度必须为 1 到 30 个字符。 • 用户名可以包含以下字符： • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (_ - .) • 用户名必须以字母开头。 • 用户名不得包含空格或“@”符号。

参数名称	是否必需	Description
`grafana_admin_password`	否	用于通过 Grafana 工具查看 OSMP 指标的账户密码。 密码必须符合以下规则： • 用户密码不能少于 8 个字符或超过 256 个字符。 • 密码必须包含以下各组中的字符： • 大写字母 (A-Z) • 小写字母 (a-z) • 数字 (0-9) • 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配用于存储 OSMP 日志的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。 推荐的最小值和默认值是 40 GB。如果未在配置文件中指定此参数，则使用默认值。
`loki_retention_period`	是	OSMP 日志的存储期限，超过此期限后，日志将自动删除。默认值为 72 小时（将配置文件中的参数值设置为“<时间（小时）>h”。例如，“72h”）。如果未在配置文件中指定此参数，则使用默认值。
`file_storage_cp`	否	分配给用于存储组件数据以处理响应操作的可用磁盘空间量。以千兆字节为单位，格式指定为“<数值>Gi”。推荐的最小值为 20 GB。
`psql_tls_off`	否	该参数指示是否使用 TLS 协议对 Kaspersky Next XDR Expert 组件和 DBMS 之间的流量进行加密。 如果 DBMS 安装在集群之外，则默认禁用 TLS 加密。对于**演示部署**，如果 DBMS 安装在集群内部，则必须禁用 TLS 加密（`psql_tls_off` 设置为 `true`）。 可能的参数值： • `true` — 不加密流量（默认值）。 • `false` — 加密流量。
`proxy_enabled`	否	该参数指示是否使用代理服务器将 Kaspersky Next XDR Expert 组件连接到互联网。如果安装了 Kaspersky Next XDR Expert 的主机可以访问互联网，您还可以为 Kaspersky Next XDR Expert 组件（例如，管理服务器）的运行以及卡巴斯基和第三方的特定集成提供互联网访问权限。要建立代理连接，您还必须在管理服务器属性中指定代理服务器参数。 可能的参数值： • `true` —使用代理服务器。 • `false` —不使用代理服务器（默认值）。
`proxy_addresses`	否	代理服务器的 IP 地址。如果代理服务器使用多个 IP 地址，请指定这些地址并用空格分隔（例如“`0.0.0.0 0.0.0.1 0.0.0.2`”）。如果“`proxy_enabled`”参数设置为“`true`”，请指定此参数。
`proxy_port`	否	将建立代理服务器连接的端口号。如果“`proxy_enabled`”参数设置为“`true`”，请指定此参数。
`trace_level`	否	管理服务器跟踪文件的详细程度。在管理服务器运行期间会写入跟踪信息。 默认值为 0，不写入任何跟踪信息。 可能的参数值：0 – 5。 参数值越高，跟踪详情越详细。
`ansible_extra_flags`	否	KDT 执行的 KUMA Core 和 KUMA 服务部署日志的详细程度。 可能的参数值： • `-v` • `-vv` • `-vvv` • `-vvvv` 标志中“v”字母的数量越多，日志的详细程度就越高。如果配置文件中未指定此参数，则保存标准组件安装日志。
`incident_attachments_max_count_limit`	否	您可以附加到事故的文件数。默认值为 `100`。
`incident_attachments_max_size_limit`	否	附加到该事故的文件的总大小。该值以字节为单位。在指定时不带计量单位。默认值为 `26214400`。

参数名称	是否必需	Description
ignore_precheck	否	该参数用于指示部署前是否检查 Kubernetes 集群节点的硬件、软件和网络配置是否符合安装该解决方案的先决条件。 可能的参数值： • true—跳过预检查。 • false—执行预检查（默认值）。
airgap_mode	否	指示是否执行APT软件包管理器预检查和更新软件包缓存的参数。这可让您在物理隔离环境中部署Kaspersky Next XDR Expert。 可能的参数值： • true—跳过预检查和软件包缓存更新。 • false—执行预检查并更新软件包缓存（默认值）。
grafana_smtp_host	否	Grafana的SMTP服务器地址，用于发送有关Kubernetes集群运行状况事件的电子邮件通知。请以 <host>:<port> 格式指定此参数，例如 localhost:25。
grafana_smtp_user	否	用于SMTP服务器身份验证的用户名。
grafana_smtp_password	否	用于SMTP服务器身份验证的密码。
grafana_smtp_bundle	否	包含X.509证书链的文件，用于验证与SMTP服务器的TLS连接。
grafana_smtp_skip_verify	否	指示是否跳过SMTP服务器的TLS证书验证的参数。 可能的参数值： • true—跳过TLS证书验证。 • false—执行TLS证书验证（默认值）。
grafana_smtp_from_address	否	发件人的电子邮件地址，该地址将显示在发送电子邮件通知的"发件人"字段中。
grafana_smtp_from_name	否	在电子邮件通知中显示发件人的姓名。
grafana_smtp_ehlo_identity	否	连接到SMTP服务器时，EHLO命令中使用的标识符。
grafana_starttls_policy	否	连接到SMTP服务器时，使用STARTTLS的策略。 可能的参数值： • OpportunisticStartTLS—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器。 • MandatoryStartTLS—要求使用STARTTLS；如果SMTP服务器不支持STARTTLS，则连接失败。 • NoStartTLS—不使用STARTTLS；请在不加密的情况下连接到SMTP服务器。 • empty—如果SMTP服务器支持STARTTLS，请使用STARTTLS；否则，请在不加密的情况下连接到SMTP服务器（默认值）。
grafana_smtp_enable_tracing	否	指示是否启用SMTP连接跟踪以调试电子邮件发送的参数。 可能的参数值： • true—启用SMTP连接跟踪。 • false—禁用SMTP连接跟踪（默认值）。
tokenhub_access_token	否	访问令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可能值为 5m，最大值为 2h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署之后更改 tokenhub_access_token 参数。
tokenhub_refresh_token	否	用于获取新访问令牌的刷新令牌的有效期。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可能值为 12h，最大值为 4320h。 默认值为 24h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署之后更改 tokenhub_refresh_token 参数。
credentials_session_ttl	否	单点登录会话的最大空闲时间。 在配置文件中将参数值设置为"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可能值为 5m，最大值为 96h。 默认值为 1h。如果未在配置文件中指定此参数，则使用此值。 您可以在应用程序部署之后更改 credentials_session_ttl 参数。

单节点演示部署的配置文件示例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Node on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
    # Node name.
  - desc: cdt-1
    # Node type.
    type: primary-worker
   # IP address of the node.
    host: 10.80.23.42
    access:
      ssh:
        # User name of the account.
        user: root
# Parameters for the Kaspersky XDR deployment
parameters:
  # IP address of the Kubernetes cluster gateway.
  - name: ingress_ip
    source:
      value: 10.80.23.182
  # Path to the SSH private key for connection to the primary worker node by KDT.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky XDR user account that will be created during the
  installation.
  - name: admin_password
    source:
      value: ""
  # The parameter indicating that Kaspersky XDR is installed on the target host with
  limited computing resources.
  - name: low_resources
    source:
      value: "true"
  # The number of disk volumes that are used to store the service data of Kaspersky XDR
  components and KDT&period; For the single-node deployment, set the parameter value to
  "1".
  - name: default_class_replica_count
    source:
      value: "1"
  # The parameter that indicates whether to run the secret storage in the High
  Availability (HA) mode&period; For the single-node deployment, set the parameter value
  to "false".
  - name: openbao_ha_mode
    source:
      value: "false"
  # The parameter that indicates whether to run the secret storage in the standalone
  mode&period; For the single-node deployment, set the parameter value to "true".
  - name: openbao_standalone
    source:
      value: "true"
  # Path to the KUMA inventory file that contains the installation parameters for
  deployment of the KUMA services.
```

```
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# The path to the license key of KUMA Core&period; This file is located on the
administrator host.
- name: license
  source:
    value: "/home/user/license.key"
# Domain name&period; The service host name and domain name are parts of FQDNs of the
Kaspersky XDR services.
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom
certificate must be generated.
- name: pki_host_list
  source:
    value: "admsrv api console kumamonitoring"
```

将 Kaspersky Next XDR Expert 从版本 2.2 升级到 2.3

您可以使用 KDT 将 Kaspersky Next XDR Expert 从版本 2.2 升级到 2.3。KDT更新Kubernetes集群组件、Kaspersky Next XDR Expert组件以及安装在集群外KUMA目标主机上的KUMA服务。Kaspersky Next XDR Expert 升级过程的步骤与所选的部署选项无关。

> 您只能按顺序将解决方案升级到下一个主要版本。不支持跨多个主要版本升级。
> 热修复程序不受此限制。您可以安装当前主版本中的任何热修复程序，而无需安装所有先前的热修复程序。

要升级 Kaspersky Next XDR Expert：

1. 下载并解压包含 Kaspersky Next XDR Expert 版本 2.3 的分发包。
2. 阅读包含 Kaspersky Next XDR Expert 组件的分发包中的 KDT 最终用户授权许可协议 (EULA)。

   当您开始使用KDT时，即表示您确认已完整阅读、理解并接受KDT的EULA的条款。

   升级 Kaspersky Next XDR Expert 后，您可以阅读 KDT 的 EULA。`license_kdt.txt` 文件位于运行 Kaspersky Next XDR Expert 升级的用户的 `~/kaspersky_eula` 目录中。
3. 运行以下命令来升级 Kaspersky Next XDR Expert：

   ```
   ./kdt apply -k <full_path_to_XDR_updates_archive>
   ```

   要开始升级 Kaspersky Next XDR Expert，请接受 EULA 和隐私策略的条款。

   如果您使用 `--accept-eula` 标志，则在安装 Kaspersky Next XDR Expert 时，系统不会提示您阅读 EULA 的条款和 OSMP 的隐私策略。在这种情况下，您必须在升级 Kaspersky Next XDR Expert 之前阅读 EULA 和 OSMP 的隐私策略。这些文件位于包含 Kaspersky Next XDR Expert 组件的分发包中。使用 `--accept-eula` 标志，即表示您确认已完整阅读、理解并接受 EULA 和隐私策略的条款。

   如果您想在升级期间阅读并接受 EULA 和隐私策略的条款，请不要使用 `--accept-eula` 标志。
4. 如果您在上一步中没有使用 `--accept-eula` 标志，请阅读 EULA 和 OSMP 的隐私策略。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   a. 如果您理解并接受 EULA 的条款，请输入“`y`”。

      如果您不接受 EULA 的条款，请输入“`n`”。

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

      如果您不接受隐私策略的条款，请输入“`n`”。

   如果您不接受 EULA 和隐私策略的条款，Kaspersky Next XDR Expert 将无法升级。

   KDT执行更新，并在控制台中显示其进度。请等待更新完成。Kaspersky Next XDR Expert 已从版本 2.2 升级到 2.3。
5. 从文件导入 OSMP 资源。

   该文件位于以下路径：opt/kaspersky/kuma/utils/

   文件密码为：`w.zS81'ZdTgicHq;`

在 **选择要导入的资源** 字段中，您必须选择所有资源，然后清除 **目标位置** 复选框，以防止替换现有目标位置。

已知问题和故障排除：

如果您要升级到版本 2.3，并且配置了多个 OSMP 实例的层次结构，则子实例继承的资源以及在子实例中创建的资源可能不会显示在父实例中。如果出现这种情况，请在升级后重新保存子实例上的资源。或者，您可以导出这些资源（机密类型的资源除外），然后将其导入同一租户。

迁移到 Kaspersky Next XDR Expert

本部分介绍如何将数据从Kaspersky Security Center for Windows、KUMA和Kaspersky KEDR 7.1迁移到Kaspersky Next XDR Expert。

关于从 Kaspersky Security Center Windows 迁移

按照此方案，您可以将管理组结构、包含的受管理设备和其他组对象（策略、任务、全局任务、标签和设备分类）从 Kaspersky Security Center Windows 转移到 Kaspersky Next XDR Expert 的管理之下。

限制：

- 从版本 1.0 开始，只能从 Kaspersky Security Center 14.2 Windows 迁移到 Kaspersky Next XDR Expert。
- 您只能使用 Kaspersky Security Center Web Console 来执行此方案。

阶段

迁移方案分阶段进行：

1. **选择迁移方法**

   您可以通过迁移向导迁移到 Kaspersky Next XDR Expert。迁移向导的具体步骤取决于 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 的管理服务器是否排列为层次结构：

   - 使用管理服务器层级进行迁移

     如果 Kaspersky Security Center Windows 的管理服务器充当 Kaspersky Next XDR Expert 管理服务器的从属管理服务器，请选择此选项。您可以在 OSMP 控制台中管理迁移过程并在服务器之间切换。如果您更喜欢此选项，可以将管理服务器排列成层次结构以简化迁移过程。为此，请在开始迁移之前创建层次结构。

     如果您将从属管理服务器连接到 Kaspersky Next XDR Expert，请禁用管理这些服务器的 Web Console 的后台集成。

     要禁用后台集成，请执行以下操作：

     1. 登录管理服务器 Web Console。
     2. 在主菜单中，转到“**设置 → 整合**”。
     3. 在**后台连接**部分，禁用“**用于整合的后台连接 已启用**”切换开关。

   - 使用导出文件（ZIP 存档）进行迁移

     如果 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 的管理服务器未排列为层次结构，请选择此选项。您可以使用两个控制台管理迁移过程：一个是Kaspersky Security Center Windows 实例，另一个是 OSMP 控制台。在这种情况下，您可以使用在从 Kaspersky Security Center Windows 导出期间创建和下载的导出文件并将此文件导入 Kaspersky Next XDR Expert。

2. **从 Kaspersky Security Center Windows 导出数据**

   打开 Kaspersky Security Center Windows，然后运行迁移向导。

3. **将数据导入 Kaspersky Next XDR Expert**

   继续运行迁移向导，将导出的数据导入 Kaspersky Next XDR Expert。

   如果服务器按层次结构排列，则在同一向导中成功导出后，导入会自动开始。如果服务器未排列为层次结构，您可以在切换到 Kaspersky Next XDR Expert 后继续运行迁移向导。

4. **执行其他操作以手动将对象和设置从 Kaspersky Security Center Windows 转移到 Kaspersky Next XDR Expert（可选步骤）**

   您可能还想传输无法通过迁移向导传输的对象和设置。例如，您还可以执行以下操作：

   - 配置管理服务器的全局任务
   - 配置网络代理策略设置
   - 创建应用程序安装包
   - 创建虚拟服务器
   - 分配和配置分发点
   - 配置设备移动规则。
   - 配置自动标记设备规则
   - 创建应用程序类别

5. **将导入的受管理设备转移到 Kaspersky Next XDR Expert 的管理之下**

   要完成迁移，请将导入的受管理设备转移到 Kaspersky Next XDR Expert 的管理之下。您可以通过以下方式之一进行操作：

   - 通过 Kaspersky Security Center 组任务

     使用更改管理服务器任务将管理服务器更改为特定客户端设备的另一台管理服务器。

   - 通过klmover 实用程序

     使用 klmover 实用程序并指定新管理服务器的连接设置。

   - 通过在受管理设备上安装或重新安装网络代理

     创建新的网络代理安装包，并在安装包属性中指定新管理服务器的连接设置。使用安装包通过远程安装任务在导入的受管理设备上安装网络代理。

     您还可以创建并使用独立的安装包在本地安装网络代理。

6. **将网络代理更新到最新版本**

   我们建议您将网络代理升级到与 OSMP 控制台相同的版本。

7. **确保受管理设备在新管理服务器上可见**

   在 Kaspersky Next XDR Expert 管理服务器上，打开受管理设备列表（**资产管理** → **资产(设备)**），然后检查“**可见**”、“**网络代理已安装**”和“**上一次连接到管理服务器**”列中的值。

其他数据迁移方法

除了迁移向导之外，您还可以传输特定任务和策略：

- 从 Kaspersky Security Center Windows 导出任务，然后将任务导入 Kaspersky Next XDR Expert。
- 从 Kaspersky Security Center Windows 导出策略，然后导入策略到 Kaspersky Next XDR Expert。相关的策略配置文件与选定的策略一起导出和导入。

从 Kaspersky Security Center Windows 导出组对象

从 Kaspersky Security Center Windows 到 Kaspersky Next XDR Expert 的迁移管理组结构（包括受管理设备和其他组对象），需要您首先选择要导出的数据并创建导出文件。导出文件包含有关要迁移的所有组对象的信息。导出文件将用于后续导入到 Kaspersky Next XDR Expert 中。

您可以导出以下对象：

- 受管理应用程序的任务和策略
- 全局任务
- 自定义设备分类
- 管理组结构和包含的设备
- 已分配给迁移设备的标签

开始导出之前，请阅读有关迁移到 Kaspersky Next XDR Expert 的一般信息。选择迁移方法 — 使用或不使用 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 管理服务器的层次结构。

通过迁移向导导出受管理设备和相关组对象：

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 的管理服务器是否被排列成层次结构，执行以下操作之一：
   - 如果服务器被排列成层次结构，打开 OSMP Console，然后切换到 Kaspersky Security Center Windows 的服务器。
   - 如果服务器未排列成层次结构，请打开连接到 Kaspersky Security Center Windows 的 Kaspersky Security Center Web Console。
2. 在主菜单中，转到“**操作 → 迁移**”。
3. 选择**迁移到 Kaspersky Security Center Linux 或 Open Single Management Platform**启动向导并按照其步骤操作。
4. 选择要导出的管理组或子组。请确保所选的管理组或子组包含的设备不得超过 10,000 台。

5. 选择将导出其任务和策略的受管理应用程序。仅选择 Kaspersky Next XDR Expert 支持的应用程序。不受支持的应用程序的对象仍将被导出，但将不可操作。

6. 使用左侧的链接，以选择全局任务、设备分类和要导出的报告。您可通过“**组对象**”链接在导出中排除自定义角色、内部用户和安全组以及自定义应用程序类别。

导出文件（ZIP 存档）已创建。根据您是否使用管理服务器层次结构支持执行迁移，导出文件将保存如下：

- 如果服务器排列成层次结构，导出文件将保存到 OSMP Console 服务器上的临时文件夹中。
- 如果服务器未排列成层次结构，则导出文件将被下载到您的设备。

对于具有管理服务器层次结构支持的迁移，导入会在成功导出后自动开始。对于没有管理服务器层次结构支持的迁移，您可以手动将保存的导出文件导入到 Kaspersky Next XDR Expert。

将导出文件导入 Kaspersky Next XDR Expert

要传输有关从 Kaspersky Security Center Windows 导出的受管理设备、对象及其设置的信息，则必须将其导入到 Kaspersky Next XDR Expert。

通过迁移向导导入受管理设备和相关组对象：

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 的管理服务器是否被排列成层次结构，执行以下操作之一：

   - 如果服务器按层次结构排列，则在导出完成后继续执行迁移向导的下一步。在此向导中成功导出后，导入会自动开始（请参阅本说明的步骤 2）。
   - 如果服务器未按层次结构排列：

     a. 打开 OSMP Console。

     b. 在主菜单中，转到“**操作 → 迁移**”。

     c. 选择您在从 Kaspersky Security Center Windows 导出过程中创建并下载的导出文件（ZIP 存档）。开始上传导出文件。

2. 导出文件上传成功后，即可继续导入。如果服务器未排列成层次结构，则可以通过单击“**更改**”链接并选择所需文件来指定另一个导出文件。

3. Kaspersky Next XDR Expert 管理组的整个层级结构将得以显示。

   选中目标管理组旁边的复选框，导出的管理组的对象（受管理设备、策略、任务和其他组对象）必须还原到该目标管理组。

4. 开始导入组对象。导入期间将无法最小化迁移向导和执行任何并行操作。等待至对象列表中所有项目旁边的刷新图标 (🔄) 均替换为绿色复选标记 (✓)，导入完成。

5. 导入完成后，导出的管理组结构（包括设备详情）将显示在所选目标管理组下。如果还原的对象的名称与现有对象的名称相同，则将为还原的对象添加一个增量后缀。

如果在迁移的任务中指定了运行该任务的账户的详细信息，则导入完成后您必须打开该任务并再次输入密码。

如果导入已完成但出现错误，您可以执行以下操作之一：

- 对于具有管理服务器层次结构支持的迁移，您可以再次开始导入导出文件。在这种情况下，您必须按照步骤 3 中的说明选择管理组。
- 对于没有管理服务器层次结构支持的迁移，您可以启动迁移向导选择另一个导出文件，然后再次导入。

您可以检查导出范围中包含的组对象是否已成功导入到 Kaspersky Next XDR Expert。为此，请转到“**资产管理**”部分并确保导入的对象出现在相应的子部分中。

请注意，导入的受管理设备显示在 **受管理设备** 子部分中，但它们在网络中不可见，而且这些设备上未安装或运行网络代理（**可见**、**网络代理已安装**和 **上一次连接到管理服务器**列中均显示 *否*）。

要完成迁移，您需要如“迁移到 Kaspersky Next XDR Expert”中的阶段 5 所述，将受管理设备切换至 Kaspersky Next XDR Expert 的管理之下。

将受管理设备纳入 Kaspersky Next XDR Expert 管理

将受管理设备、对象及其设置的信息成功导入 Kaspersky Next XDR Expert 后，您需要将受管理设备切换到 Kaspersky Next XDR Expert 的管理下才能完成迁移。

您可以通过以下方法之一将受管理设备移至 Kaspersky Next XDR Expert 的管理下：

- 使用klmover 实用程序。
- 使用*更改管理服务器*任务。
- 通过远程安装任务在受管理设备上安装网络代理。

要通过安装网络代理将受管理设备切换为由 Kaspersky Next XDR Expert 管理：

1. 在将已导入的受管理设备切换至由 Kaspersky Next XDR Expert 管理时，删除网络代理。
2. 切换到 Kaspersky Security Center Windows 的管理服务器。
3. 进入**软件管理** → **安装包**，然后打开网络代理现有安装包的属性。

   如果软件包列表中没有网络代理安装包，请下载新的安装包。

   您还可以创建并使用独立的安装包在本地安装网络代理。
4. 在**设置**选项卡上，选择**连接**区域。指定 Kaspersky Next XDR Expert 管理服务器的连接设置。
5. 为导入的受管理设备创建远程安装任务，然后指定重新配置的网络代理安装包。

   您可以通过 Kaspersky Security Center Windows 的管理服务器或通过充当分发点的基于 Windows 的设备安装网络代理。如果您使用管理服务器，请启用**通过管理服务器使用操作系统资源**选项。如果您使用分发点，请启用“**通过分发点使用操作系统资源**”选项。
6. 运行远程安装任务。

远程安装任务成功完成后，请转至 Kaspersky Next XDR Expert 的管理服务器，确保受管理设备在网络中可见，并且网络代理已安装并在其上运行（“**可见**”、“**网络代理已安装**”和“**网络代理正在运行**”列中的值为“*是*”）。

关于从KEDR 7.1迁移

不支持将数据从 KEDR 7.1 直接迁移到 Kaspersky Next XDR Expert 2.3，因为与 2.1 版本相比，2.3 版本仅存在细微的功能差异。

要将数据从 KEDR 7.1 传输到 Kaspersky Next XDR Expert 2.3：

1. 安装 Kaspersky Next XDR Expert 2.1。
2. 按照 Kaspersky Next XDR Expert 2.1 帮助中的说明，执行从 KEDR 7.1 到 Kaspersky Next XDR Expert 2.1 的数据迁移。
3. 将 Kaspersky Next XDR Expert 从 2.1 版本升级到 2.3 版本。

设置和使用SIEM组件

本节提供有关安装和配置 KUMA SIEM 系统的信息。

KUMA 服务

*服务*是 KUMA 的主要组件，用于协助系统管理事件：服务允许您从事件源接收事件，然后将它们转换为通用格式，以便于查找关联、存储和人工分析。每个服务由协同工作的两部分组成：

- 服务的一部分是在 KUMA 控制台内基于服务资源集创建的。
- 服务的另一部分作为 KUMA 组件之一，安装在部署 KUMA 的网络基础设施中。服务的服务器部分可以由多个实例组成：例如，同一代理或存储的服务可同时安装在多个设备上。

  > 在服务器端，KUMA 服务位于 `/opt/kaspersky/kuma` 目录中。

  在高可用性模式下安装 KUMA 时，集群中仅安装 KUMA Core。收集器、关联器和存储托管在 Kubernetes 集群之外的主机上。

服务的各个部分通过服务 ID 相互连接。

服务类型：

- 收集器用于接收事件并将其转换为 KUMA 格式。
- 关联器用于分析事件并搜索定义的模式。
- 存储用于保存事件。
- 代理用于接收远程设备上的事件并将其转发到 KUMA 收集器。
- 事件路由器从收集器和关联器接收事件流，然后根据配置的过滤器将事件分发到目标位置。

在 KUMA 控制台中，服务以表格形式显示在“**资源**” → “**活动服务**”部分。单击“**刷新**”按钮即可更新服务表格，单击活动标题即可实现按列排序。

表格最大尺寸不受限制。若要选择所有服务，滚动到表格末尾并选中“**全选**”复选框，即可选中表格中所有可用服务。

表格列：

- **状态** – 服务状态：
  - 绿色表示服务正在运行。
  - 红色表示服务未运行。
  - 黄色是适用于所有服务（代理除外）的状态。黄色状态表示服务正在运行，但存在来自 Victoria Metrics 的错误或警报。您可以通过将鼠标指针悬停在状态上来查看错误消息。

- 紫色是适用于正在运行服务的状态，这些服务在数据库中的配置文件已被更改，但不存在其他错误。如果某个服务的配置文件不正确并且存在错误（例如来自 VictoriaMetrics 的错误），则该服务的状态为黄色。

- 灰色 – 若已删除的租户中存在仍在运行的服务，则该服务在“**活动服务**”页面上将显示为灰色状态。灰色状态的服务将保留，以便您复制其 ID 并从服务器上移除该服务。只有主管理员可以删除灰色状态的服务。删除租户后，该租户的服务将分配给主租户。

- **类型 – 服务类型**：**代理**、**收集器**、**关联器**或**存储**。
- **名称** – 服务名称。单击服务名称即可打开其设置。
- **版本** – 服务版本。
- **租户** – 拥有该服务的租户的名称。
- FQDN – 服务所在服务器的完全限定域名。
- IP **地址** – 安装服务的服务器的 IP 地址。
- API **端口** – 远程过程调用端口号。
- **正常运行时间** – 显示服务运行的时间。
- **创建时间** – 服务创建的日期和时间。

可以将该表格设置为按升序和降序排序，也可以按“**状态**”参数排序。要对活动服务进行排序，请右键单击上下文菜单并选择一个或多个状态。

单击“**服务**”窗口上部的按钮，以执行以下组操作：

- 添加服务

  您可以基于现有服务资源集创建新服务。在未事先仔细规划各服务与用户之间的租户间交互的情况下，我们不建议在主租户之外创建服务。

- 刷新

  您可以刷新活动服务列表。

- 更新配置
- 重新启动

要对单个服务执行操作，请右键单击该服务以显示其上下文菜单。可用的操作如下：

- 重置证书
- 删除
- 下载日志

  若要接收详细信息，请在服务设置中启用“调试”模式。

- 复制服务 ID

  您需要使用该 ID 来执行安装、重启、停止或删除服务操作。

- 转到事件

- 前往活动列表
- 前往上下文表
- 转到分区

要更改服务，请在“**资源**” → “**活动服务**”下选择一项服务。这将打开一个窗口，其中包含创建该服务所依据的资源集。您可以编辑资源集的设置并保存更改。要应用保存的更改，请重启服务。

如果在更改收集器资源集的设置时，更改或删除与其连接的规范化器中的转换，则编辑不会被保存，且规范化器本身可能被损坏。若需修改已属于某个服务的标准化器中的转换规则，则必须在 Web 界面的“**资源**” → “**规范化器**”下直接对该规范化器进行更改。

服务工具

本节介绍 OSMP 的“**资源和服务**” → “**活动服务**”部分中用于处理服务的工具。

获取服务标识符

服务标识符用于将驻留在 OSMP 内的服务部分与安装在网络基础设施中的服务部分绑定成一个单一整体。在 OSMP 中创建服务时会为服务分配一个标识符，随后在将服务安装到服务器时会使用该标识符。

要获取服务标识符：

1. 登录 OSMP 并打开 **资源和服务 → 活动服务**。
2. 选中要获取其 ID 的服务旁边的复选框，然后单击“**复制 ID**”。

   服务标识符将被复制到剪贴板。例如，可以使用此 ID 在服务器上安装服务。

停止、启动、检查服务状态

在管理 OSMP 时，您可能需要执行以下操作。

- 暂时停止服务。例如，从备份恢复 Core 时，或编辑与操作系统相关的服务设置时。
- 启动该服务。
- 检查服务状态。

下表列出了管理 OSMP 时可能有用的命令。

用于停止、启动和检查服务状态的命令

服务	停止服务	启动服务	检查服务状态
Core	`sudo systemctl stop kuma-core.service`	`sudo systemctl start kuma-core.service`	`sudo systemctl status kuma-core.service`
带 ID 的服务： • 收集器 • 关联器 • 存储	`sudo systemctl stop kuma-<collector/correlator/storage>-<服务 ID>.service`	`sudo systemctl start kuma-<collector/correlator/storage>-<服务 ID>.service`	`sudo systemctl status kuma-<collector/correlator/storage><服务 ID>.service`
不带 ID 的服务： • kuma-grafana.service • kuma-mongodb.service • kuma-victoria-metrics.service • kuma-vmalert.service	`sudo systemctl stop kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl start kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl status kuma-<grafana/victoria-metrics/vmalert>.service`
Windows 代理	要停止代理服务： 1. 在 KUMA 控制台中复制代理 ID。 2. 连接到要启动 KUMA 代理服务的主机。 3. 以具有管理员权限的用户身份运行 PowerShell™。 4. 在 PowerShell 中运行以下命令： `Stop-Service -Name "WindowsAgent-<代理 ID>"`	要启动代理服务： 1. 在 KUMA 控制台中复制代理 ID。 2. 连接到要启动 KUMA 代理服务的主机。 3. 以具有管理权限的用户身份运行 PowerShell。 4. 在 PowerShell 中运行以下命令： `Start-Service -Name "WindowsAgent-<代理 ID>"`	要查看代理服务的状态： 1. 在 Windows 中，转到“开始” → “服务”菜单，然后在服务列表中双击相关的 KUMA 代理。 2. 这将打开一个窗口；在该窗口中，可在服务状态字段中查看代理的状态。

重启服务

要重启该服务：

1. 登录 OSMP 并打开 **资源和服务** → **活动服务**。

2. 选中服务旁边的复选框并选择必要的选项：

   - “**更新配置**” – 对正在运行的服务配置执行热更新。例如，您可以通过这种方式更改字段映射设置或目标点设置。

   - **重新启动** – 停止服务并重启。此选项用于修改端口号或连接器类型。

     重启 OSMP 代理：

     - 只有当 OSMP Windows 代理在远程计算机上运行时，才能按上述方式重启。如果远程计算机上的服务处于非活动状态，则在尝试从 OSMP 重启时将收到错误消息。在这种情况下，您必须在远程 Windows 计算机上重启 OSMP Windows 代理服务。有关重启 Windows 服务的信息，请参阅针对远程 Windows 计算机操作系统版本的相关文档。

     - 使用此选项时，OSMP Linux 代理将停止运行。要再次启动，必须执行用于启动该代理服务的命令。

   - **重置证书** – 删除服务用于内部通信的证书。此选项不可用于续订 Core 证书。要续订 KUMA Core 证书，必须重新颁发证书。

删除 Windows 代理证书的特殊注意事项：

- 如果代理处于绿色状态并且您选择了“**重置证书**”，OSMP 会删除当前证书并创建新证书，代理会继续使用新证书。
- 如果代理处于红色状态并且您选择了“**重置证书**”，则 OSMP 会生成“代理未运行”的错误消息。在 %PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<agent ID>\certificates 文件夹中，手动删除 internal.cert 和 internal.key 文件，然后手动启动代理。代理启动时，会自动创建新证书。

删除 Linux 代理证书的特殊注意事项：

1. 无论代理状态如何，都应用 Web 界面中的“**重置证书**”选项以删除数据库中的证书。
2. 在代理安装文件夹 (/opt/kaspersky/agent/<Agent ID>/certificates) 中，手动删除 internal.cert 和 internal.key 文件。
3. 由于使用“**重置证书**”选项会导致代理停止运行，要让代理继续运行，请手动启动代理。代理启动时，会自动创建新证书。

删除设备.....

删除服务之前，请获取其 ID。从服务器中删除服务时需要使用该 ID。

要在 OSMP 中删除服务：

1. 登录 OSMP 并打开 **资源和服务** → **活动服务**。
2. 选中要删除的服务旁边的复选框，然后单击“**删除**”。
   确认窗口打开。
3. 单击“**确定**”。

服务已从 OSMP 中删除。

要从服务器中删除服务，请运行以下命令：

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage> --id <服务 ID> --uninstall
```

该服务已从服务器中删除。

查看活动查询表

主管理员可以查看其他用户当前正在执行的查询及其使用的 OSMP 资源。

若要查看活动查询表：

1. 在主应用程序窗口中，前往**监控中**→**资源和服务**→**活动服务**部分。
2. 选中相关存储旁边的复选框。

3. 在工具栏或菜单中（⋮），点击**有效查询**。
   这将打开一个窗口，其中包含**ClickHouse 有效查询**。选择多个存储时，表格会显示来自每个选定存储的活动查询。

资源表包含以下各列：

- **启动时间**显示查询启动的日期和时间。
- **创建者**显示查询的发起者。对于用户查询，显示用户名。对于**资源**类型的查询，显示资源名称。
- **查询**是ClickHouse中执行的SQL查询文本。
- **类型**是查询的类型。以下查询类型可供使用：
  - **后台运行**表示用户使用**在后台运行**按钮在后台启动了查询。
  - **资源**表示由OSMP资源发起的内部SQL查询，例如在数据处理或分析期间。
  - **用户**表示用户使用**运行查询**按钮启动并正常执行的SQL查询。
- **存储**是执行查询的ClickHouse存储的名称。

单击 ⚙ 用于配置查询表显示列的按钮。如有必要，您可以通过点击↻强制更新数据。

如果您想按特定列对查询进行排序，请点击其标题，然后从下拉列表中选择可用选项之一：**升序**或**降序**。

如有必要，您可以取消查询。

若要取消查询：

1. 打开**ClickHouse 有效查询**。
2. 选中查询旁边的复选框，然后点击**取消查询**。
   确认窗口打开。您还可以在**指定原因**字段中指定取消查询的原因。
3. 单击“**确定**”。

查询随即被取消并从表中删除。审计事件将自动生成。

分区窗口

如果存储服务已创建并安装，您可以在**分区**表格中查看其分区。

*要打开“**分区**”表格：*

1. 登录 OSMP 并打开 **资源和服务** → **活动服务**。
2. 选中相关存储旁边的复选框，然后单击**转至分区**。

“**分区**”表格将打开。

该表格包含以下列：

- **租户** – 拥有存储数据的租户的名称。
- **创建时间** – 分区的创建日期。
- **空间** – 空间名称。
- **大小** – 空间大小。
- **事件** – 存储的事件数量。
- **传输到冷存储** – 数据从 ClickHouse 集群迁移到冷存储磁盘的日期。
- **到期** – 分区到期的日期。在此日期之后，分区及其包含的事件将不再可用。

您可以删除分区。

要删除分区：

1. 打开“**分区**”表格（参见上文）。
2. 选中所需分区左侧的复选框。
3. 选择“**删除**”。
   确认窗口打开。
4. 单击“**确定**”。

分区已被删除。无法删除审计事件分区。

搜索相关事件

您可以搜索由关联器或收集器服务处理的事件。

要搜索与关联器或收集器服务相关的事件：

1. 登录 OSMP 并打开 **资源和服务** → **活动服务**。
2. 选中所需的关联器或收集器旁边的复选框，然后单击“**转到事件**”。
   将打开一个新的浏览器标签页，其中显示 OSMP 的“**事件**”部分。
3. 要查找事件，请单击 🔍 图标。
   将显示一个表格，其中包含由搜索表达式 `ServiceID = <所选服务的 ID>` 选择的事件。

服务资源集

*服务资源集*是一种资源类型，是 OSMP 的组件，也是用于创建和运行 OSMP 服务的一组设置。服务资源集是资源的集合。

添加到资源集中的任何资源都必须归创建该资源集的同一租户所有。共享租户是例外情况，其拥有的资源可用于其他租户的资源集。

服务资源集显示在 OSMP 的"**资源和服务**" → "**<服务的资源集类型>**"部分。可用类型：

- 收集器。
- 关联器。
- 存储
- 代理。

选择所需类型后，将打开一个表格，其中包含此类型服务的可用资源集。资源表包含以下各列：

- **名称** – 资源集的名称。可用于搜索和排序。
- **更新时间** – 资源集上次更新的日期和时间。可用于排序。
- **创建者** – 创建资源集的用户名称。
- **描述** – 资源集的描述。

创建存储

存储由两部分组成：一部分在 OSMP 内创建，另一部分安装在用于存储事件的网络基础设施服务器上。OSMP 存储的服务器部分由汇集成集群的 ClickHouse 节点组成。ClickHouse 集群可补充冷存储磁盘。

每个 ClickHouse 集群都必须安装单独的存储。

> 在创建存储之前，请仔细规划集群结构并部署必要的网络基础设施。选择 ClickHouse 集群配置时，需考虑组织对事件存储的特定需求。

> 我们建议使用 ext4 文件系统。

存储的创建分为几个步骤：

1. **在 OSMP 中为存储创建资源集**
2. **在 OSMP 中创建存储服务**
3. **在网络基础设施中安装存储节点**

> 创建存储集群节点时，请验证系统的网络连接并打开组件使用的端口。

如果更改了存储设置，则必须重启服务。

ClickHouse 集群结构

ClickHouse *集群*是拥有所有累积的规范化 KUMA 事件的逻辑设备组。它由一个或多个逻辑*分片*组成。

*分片*是拥有集群中累积的所有规范化事件的特定**部分**的逻辑设备组。它由一个或多个*副本*组成。增加分片数量可实现以下效果：

- 通过增加服务器总数和磁盘空间来积累更多事件。
- 通过分配与新增事件流入相关的负载，以承载更大的事件**流**。
- 将搜索范围分配到多个设备，以缩短事件查询时间。

*副本*是逻辑分片的成员设备，持有该分片数据的单个副本。如果存在多个副本，则意味着存在多个备份（即数据被复制）。增加副本数量可以实现以下效果：

- 提高容错能力。
- 将与数据搜索相关的总负载分配到多台设备上（不过，为此最好增加分片数量）。

*协调器*是一个参与**整个**集群层面数据副本**协调**的设备。每个集群至少需要一台设备担任此角色。建议分配 3 台设备担任该角色。参与副本协调的设备数量必须是**奇数**。*协调器*和*副本*角色可以组合在同一台设备上。

ClickHouse 集群节点设置

在创建存储之前，请仔细规划集群结构并部署必要的网络基础设施。选择 ClickHouse 集群配置时，需考虑组织对事件存储的特定需求。

创建 ClickHouse 集群节点时，请验证系统的网络连接并打开组件使用的端口。

对于 ClickHouse 集群的每个节点，您需要指定以下设置：

- 完全限定域名 (FQDN) — 访问节点的唯一地址。请指定完整的 FQDN，例如 `kuma-storage.example.com`。
- 分片、副本和协调器 ID — 这些设置的组合决定了节点在 ClickHouse 集群结构中的位置和节点角色。

节点角色

节点的角色取决于指定的设置：

- 分片、副本、协调器 — 节点参与规范化 KUMA 事件的累积和搜索，并帮助协调集群范围内的数据复制。
- 分片、副本 — 节点参与规范化 KUMA 事件的累积和搜索。
- 协调器 — 节点**不**累积规范化事件，但帮助协调集群范围的数据复制。专用协调器必须在**资源**→**存储**→<存储>→**基本设置**→**ClickHouse 集群节点**部分的列表开头进行指定。

ID 要求：

- 如果在同一个集群中创建了多个分片，则分片 ID 在该集群内必须是唯一的。
- 如果在同一个分片中创建了多个副本，则副本 ID 在该分片内必须是唯一的。
- 协调器 ID 在集群内必须是唯一的。

ClickHouse 集群节点 ID 的示例：

- 分片 1，副本 1，协调器 1；
- 分片 1，副本 2；
- 分片 2，副本 1；
- 分片 2，副本 2，协调器 3；
- 分片 2，副本 3；
- 协调器 2。

事件冷存储

在 OSMP 中，您可以配置将旧数据从 ClickHouse 集群迁移到冷存储。冷存储可以使用操作系统中挂载的本地磁盘、Hadoop 分布式文件系统 (HDFS) 或 S3 云存储（简单存储服务）来实现。

从 OSMP 2.1 版本开始，存储在 HDFS 磁盘上的数据将逐步迁移到 S3 云存储。对 HDFS 文件系统的支持将在解决方案的未来版本中停止。

当至少指定了一个冷存储磁盘时，即可启用冷存储。如果使用多个存储，则必须在每个包含数据的节点上按照存储配置中指定的路径挂载冷存储磁盘或 HDFS 或 S3 磁盘。如果未配置冷存储磁盘，并且服务器在热存储中的磁盘空间不足，则存储服务将停止。如果同时配置了热存储和冷存储，并且冷存储磁盘空间不足，则 OSMP 存储服务将停止。建议通过在热存储中添加自定义事件存储条件来避免这种情况。

可以添加或删除冷存储磁盘。如果您添加了多个冷存储磁盘，数据将以循环方式进行写入。如果要写入磁盘的数据占用的空间超过该磁盘上的可用空间，则这些数据和所有后续数据将循环写入下一个冷存储磁盘。如果您只添加了两个冷存储磁盘，数据将写入剩余可用空间的驱动器。

更改冷存储设置后，必须重启存储服务。如果服务无法启动，原因会显示在存储日志中。
如果 S3 存储路径指定不正确，也需要重启服务。请注意，创建的 *storage.xml* 文件不会自动删除。您需要手动清空 `/opt/kaspersky/kuma/clickhouse/cfg/config.d/` 文件夹并重新配置冷存储。

如果存储设置中指定的冷存储磁盘不可用（例如，故障），则可能导致存储服务运行错误。In this case, recreate a disk with the same path (for local disks) or the same address (for HDFS and S3 disks) and then remove it from the storage settings.

将数据移动到冷存储磁盘的规则

您可以通过设置基于保留时间或最大存储大小的限制来配置 ClickHouse 集群热存储中事件的存储条件。使用冷存储时，OSMP 每隔 15 分钟以及每次 Core 重启后都会检查是否满足指定的存储条件：

1. OSMP 获取正在检查的存储所对应的分区，并按冷存储磁盘和空间对这些分区进行分组。
2. 对于每个空间，OSMP 都会检查是否满足指定的存储条件。
3. 如果满足条件（例如，空间中包含已超过保留时间的数据，或者存储大小已达到或超过条件中指定的限制），OSMP 会将日期最早的所有分区转移到冷存储磁盘；如果未配置冷存储磁盘或配置不正确，则会删除这些分区。只要空间中配置的存储条件仍然满足，就会重复此操作；例如，如果在删除某个日期的分区后，存储大小仍然超过条件中指定的最大大小。

   数据传输开始和结束时或删除数据时，OSMP 会生成审计事件（审计事件、审计事件）。
4. 如果在 OSMP 中配置了保留时间，则每当分区转移到冷存储磁盘时，都会检查磁盘上是否满足配置的条件。如果在磁盘上发现存储时间超过**事件保留时间**的事件（该时间从 OSMP 收到事件时开始计算），解决方案会删除这些事件或日期最早的所有分区。

   删除数据时，OSMP 会创建审计事件（审计事件、审计事件）。

如果ClickHouse集群的磁盘已使用97%，则最大的分区要么自动转移到冷存储磁盘，要么在没有冷存储磁盘的情况下被删除。

数据传输期间，存储服务会保持运行，其状态在 OSMP Web 界面的 **资源 → 活动服务**部分中保持为绿色。将鼠标悬停在状态图标上时，会显示有关数据传输的消息。当冷存储磁盘被移除时，存储服务状态显示为黄色。

存储和访问事件的特殊注意事项

- 使用 HDFS 磁盘进行冷存储时，请使用以下方式之一保护您的数据：
  - 在 VLAN 中配置单独的物理接口，该接口仅包含 HDFS 磁盘和 ClickHouse 集群。
  - 配置网络分段和流量过滤规则，以排除对 HDFS 磁盘的直接访问或拦截来自 ClickHouse 的磁盘流量。
- 位于 ClickHouse 集群和冷存储磁盘上的事件均可在 OSMP Web 界面中查看。例如，在搜索事件或查看与警报相关的事件时。
- 您可以禁用冷存储磁盘上事件或审计事件的存储。为此，请在存储设置中指定以下内容：
  - 如果您不想将事件存储在冷存储磁盘上，请执行以下操作之一：
    - 如果在“**保留策略选项**”字段中，您选择了基于 GB 或百分比的存储条件，则在“**事件存储时间**”字段中指定 `0`。
    - 如果在“**保留策略选项**”字段中，您选择了以天为单位的存储条件，请在“**事件存储时间**”字段中指定与“**保留策略选项**”中相同的天数。
  - 如果您不想将审计事件存储在冷存储磁盘上，则在“**审核冷保留期**”字段中指定 `0`（天）。

使用 HDFS 磁盘的特殊注意事项

- 在连接 HDFS 磁盘之前，请先在这些磁盘上为 ClickHouse 集群的每个节点创建目录，格式如下：`<HDFS disk host>/<shard ID>/<replica ID>`。例如，如果集群由两个节点组成，且这些节点包含同一分片的两个副本，则必须创建以下目录：

  - hdfs://hdfs-example-1:9000/clickhouse/1/1/
  - hdfs://hdfs-example-1:9000/clickhouse/1/2/

  ClickHouse 集群节点中的事件将迁移到名称包含其分片和副本 ID 的目录中。如果您更改这些节点设置而没有在 HDFS 磁盘上创建相应的目录，则迁移过程中可能会丢失事件。

- 添加到存储的 HDFS 磁盘以 JBOD 模式运行。这意味着如果其中一个磁盘发生故障，您将无法访问存储。使用 HDFS 时，请考虑高可用性并配置 RAID，同时将来自不同副本的数据存储在不同的设备上。

- 将事件记录到 HDFS 的速度通常低于将事件记录到本地磁盘的速度。通常，在 HDFS 中访问事件的速度明显低于在本地磁盘上访问事件的速度。在同时使用本地磁盘和 HDFS 磁盘时，数据会依次进行写入。

- HDFS 仅用作 ClickHouse 的分布式文件数据存储。使用 ClickHouse 的压缩机制（而非 HDFS）来压缩数据。

- ClickHouse 服务器必须对相应的 HDFS 存储具有写入权限。

移除冷存储磁盘

在物理断开冷存储磁盘之前，需先从存储设置中移除这些磁盘。

要从存储设置中移除磁盘：

- 在 OSMP 中的 **资源和服务** → **存储** 下，选择相关存储。

  这将打开该存储。

- 在窗口的**冷存储磁盘**部分，在所需磁盘的设置组中，单击**删除磁盘**。

  已删除磁盘中的数据将自动迁移到其他冷存储磁盘，如果没有其他冷存储磁盘，则迁移到 ClickHouse 集群。在数据迁移期间，存储状态图标以黄色突出显示。数据传输开始和结束时会生成审计事件（审计事件、审计事件）。

- 事件迁移完成后，磁盘将自动从存储设置中移除。现在可以安全地断开连接。

已移除的磁盘仍可能包含事件。如果要删除这些事件，可以使用 DROP PARTITION 命令手动删除数据分区。

如果存储设置中指定的冷存储磁盘不可用（例如，故障），则可能导致存储服务运行错误。在这种情况下，请创建一个具有相同路径（针对本地磁盘）或相同地址（针对 HDFS 磁盘）的磁盘，然后将其从存储设置中删除。

断开、归档和连接分区

如果您要优化磁盘空间并加快 OSMP 中的查询速度，可以在 ClickHouse 中分离数据分区、将分区打包成压缩文件或将分区移动到驱动器。如有必要，您可以稍后重新附加所需的分区并执行数据处理。

分离分区

要分离分区：

1. 确定要分离分区的所有副本上的分片。
2. 使用以下命令获取分区 ID：

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "SELECT partition, name FROM system.parts;" |grep 20231130
   ```

   在此示例中，该命令返回 2023 年 11 月 30 日的分区 ID。
3. 对于每个副本的分片，使用以下命令并指定分区 ID 来分离分区：

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 DETACH PARTITION ID '<partition ID>'"
   ```

最终，该分区会在分片的所有副本上完成分离。现在，您可以将数据目录移动到驱动器或将分区打包成压缩文件。

存档分区

要将已分离的分区打包成压缩文件：

1. 在服务器的磁盘子系统中找到已分离的分区：

   ```
   sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <ID of the detached partition>\*
   ```
2. Change to the 'detached' directory that contains the detached partition, and while in the 'detached' directory, perform the archival:

   ```
   sudo cd <path to the 'detached' directory containing the detached partition>
   ```

   ```
   sudo zip -9 -r detached.zip *
   ```

   例如：

   ```
   sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   ```

   ```
   sudo zip -9 -r detached.zip *
   ```

该分区已打包成压缩文件。

附加分区

要将已打包成压缩文件的分区附加到 OSMP：

1. 增加“**保留期**”的值。

   OSMP 会根据“时间戳”字段中指定的日期（该字段记录事件的接收时间）以及为存储设置的“**保留期**”值来删除数据。

在恢复压缩数据之前，请确保“**保留期**”值与“时间戳”字段中的日期存在重叠。否则，压缩数据将在 1 小时内删除。

2. 将压缩文件分区放入存储的“detached”部分，然后解压缩该压缩文件：

   ```
   sudo unzip detached.zip -d <path to the 'detached' directory>
   ```

   例如：

   ```
   sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   ```

3. 运行命令以附加分区：

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<partition ID>'"
   ```

   ```
   Repeat the steps of extracting the archive and attaching the partition on each replica of the shard.
   ```

最终，压缩分区被附加并且其事件再次可供搜索。

为存储创建资源集

在 OSMP Web 界面中，存储服务是基于存储资源集创建的。

要在 OSMP Web 界面中为存储创建资源集：

1. 在 OSMP 的 **资源** → **存储** 部分，单击 **新建**。

   这将打开“**创建存储**”窗口。

2. 在“**基本设置**”选项卡上的“**存储名称**”字段中，输入要创建的服务的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。

3. 在“**租户**”下拉列表中，选择该存储所属租户。

4. 在“**标签**”下拉列表中，选择要创建的资源集的标签。

   该列表包含在资源租户和共享租户中创建的所有可用标签。您可以通过在字段中输入标签名称来在列表中找到标签。如果您输入的标签不存在，可以按 **Enter** 键或单击“**添加**”以创建该标签。

5. 您可以选择在“**描述**”字段中添加最多 256 个 Unicode 字符来描述服务。

6. 在“**保留策略选项**”字段中，为存储选择 ClickHouse 集群中的事件存储条件。当满足该条件时，事件将被传输到冷存储磁盘；如果未配置冷存储或冷存储配置不正确，则事件将被删除。该条件适用于默认空间以及已删除空间中的事件。

   默认情况下，如果存储使用率超过 97%，ClickHouse 会将事件移动到冷存储磁盘或删除这些事件。创建存储时，OSMP 还会应用额外的 **365 天**存储条件。您可以配置自定义存储条件，以提升存储的稳定性能。

   要设置存储条件，请执行以下操作之一：

   - 如果要限制事件的存储期限，请从下拉列表中选择“**天数**”，然后在字段中指定 ClickHouse 热存储集群中的最大事件存储期限（以天为单位）。

     在指定的时间段之后，事件将被自动传输到冷存储磁盘或从 ClickHouse 集群中删除，从日期最早的分区开始。最小值是 1。默认值是 365。

     对于 [OOTB] 存储，默认事件存储期限为两天。如果您想使用此存储，则可以根据需要更改其事件存储条件。

- 如果要限制最大存储大小，请从下拉列表中选择“**GB**”，然后在字段中指定最大存储大小（以千兆字节为单位）。

  当存储达到指定大小时，事件将被自动传输到冷存储磁盘或从 ClickHouse 集群中删除，从日期最早的分区开始。最小值和默认值均为 1。

- 如果希望将存储大小限制为存储磁盘空间的特定百分比，请从下拉列表中选择“**百分比**”，并指定最大存储大小占可用磁盘空间的百分比。

  > 您可以通过向 ClickHouse 发送 `'SELECT hostname(), name, total_space FROM system.disks'` 查询来获取有关可用磁盘空间的信息。

  当存储达到可用的磁盘空间的指定百分比时，事件将被自动传输到冷存储磁盘或从 ClickHouse 集群中删除，从日期最早的分区开始。可能值：1到 95。默认值是 80。如果要对所有存储空间使用百分比，则所有空间条件中的百分比总和不得超过 95，但我们建议为整个存储或单个空间指定最多 90% 的限制。

  我们不建议指定小于 5% 的值，因为这会增加存储中数据丢失的可能性。

  > 如果存储是集群式的，则每个服务器的已占用磁盘空间量都是单独确定的。服务器上各磁盘上存储的数据分布可能不均匀。当*集群中的任何一台服务器*达到最大存储大小时，OSMP 会将事件推送到冷存储磁盘或删除事件。

确定已占用存储空间大小的算法

已占用存储空间的大小确定如下：

1. 有关 KUMA 磁盘和分区状态的信息从所有可用的副本中获取。
2. 如果占用空间超过配置值，KUMA 将根据数据存储类型（热存储或冷存储）采取相应措施。

   对于热存储，将对每个可用节点和空间执行以下操作：

   a. 将计算副本上该空间各分区的总大小。

   b. 将计算副本上的最大空间大小：

   - 如果为存储大小设置了以 GB 为单位的绝对值，则副本上的最大空间大小计算如下：

     `<最大空间大小> = <配置阈值>/<集群中的副本数>`

     例如，考虑一个包含三个分片的集群，每个分片包含两个副本；设置了6GB的阈值，且每个副本上的最大数据大小为1GB。

   - 如果将存储大小设置为百分比的相对值，则副本上的最大空间计算如下：

     `<最大空间大小> = <副本上的空间大小> / <副本磁盘大小> * 100%`

     > 副本磁盘的大小不包括为 `ext4` 预留的空间。

   如果超过指定的阈值，主机上的分区将被删除或移至冷存储。所有分片上的分区都将被删除。

   对于冷存储，根据 KUMA 中配置的事件保留期 (TTL)，删除每个可用空间的分区。

7. 如果要使用附加存储条件，请单击“**添加策略选项**”并按照步骤 6 中的说明指定附加存储条件。

条件的最大数量为两个，并且您只能组合以下类型的条件：

- 天数和存储大小（以 GB 为单位）
- 天数和存储大小（以百分比为单位）

If you want to remove a storage condition, click the X icon next to this condition.

8. 在“**审计保留期**”字段中，指定存储审计事件的期限（以天为单位）。最小值和默认值均为 365。
9. 如需要使用冷存储，请指定事件存储期限：
   - **事件保留时间**指定 OSMP 事件的总存储期限（以天为单位），从收到事件时开始计算。当指定的期限到期时，会自动将事件从冷存储磁盘中删除。默认值是 0。

     事件保留时间计算为触发“**保留策略选项**”设置中指定的条件之前 ClickHouse 热存储集群中的事件保留时间与冷存储磁盘上的事件保留时间之和。触发其中一个存储条件后，日期最早的数据分区将移动到冷存储磁盘，并保留在该磁盘上，直到 OSMP 中的事件保留时间到期。

     根据指定的存储条件，最终的保留时间如下：

     - 如果以天为单位指定存储条件，则**事件保留时间**必须严格大于存储条件中指定的天数。您可以将事件的冷保留期计算为“**事件存储时间**”减去“**保留策略选项**”设置中指定的天数。

       如果您不想将事件存储在冷存储磁盘上，则可以在“**事件保留时间**”字段中指定与存储条件相同的天数。

     - 如果您以磁盘大小（绝对值或百分比）指定存储条件，则“**事件保留时间**”的最小值为 1。事件的冷存储持续时间计算为“**事件保留时间**”减去从收到事件到触发条件和磁盘分区填满的天数，但在触发条件之前，无法计算准确的持续时间。在这种情况下，建议为“**事件保留时间**”指定一个相对较大的值，以避免事件被删除。

       如果您不想将事件存储在冷存储磁盘上，则可以将“**事件保留时间**”设置为 0。

   - **审计冷保留期** — 存储审计事件的天数。最小值为 0。

   只有在添加至少一个冷存储磁盘后，“**事件存储时间**”和“**审核冷保留期**”设置才可用。
10. 如果要更改 ClickHouse 设置，请在“**ClickHouse 配置覆盖**”字段中，粘贴来自 ClickHouse 配置 XML 文件 (/opt/kaspersky/kuma/clickhouse/cfg/config.xml) 的设置行。无需指定根元素 <yandex>、</yandex>。此字段中传递的设置将代替默认设置。

    例如：

    <merge_tree>

    <parts_to_delay_insert>600</parts_to_delay_insert>

    <parts_to_throw_insert>1100</parts_to_throw_insert>

    </merge_tree>

    如果要加快图表绘制和威胁搜寻速度，您可以更改 ClickHouse 压缩算法。默认情况下使用 ZSTD 算法。您可以将默认设置替换为LZ4。为此，请在**ClickHouse 配置覆盖**字段中，按如下方式指定压缩算法：

    ```
    <compression>
      <case>
        <method>lz4</method>
      </case>
    <compression>
    ```

    解决方案将在存储服务重启后开始应用LZ4算法。更改算法之前存储在存储中的所有事件仍将使用ZSTD算法进行压缩。

11. 使用“**调试**”切换开关指定是否必须启用资源日志记录。如果希望仅记录所有 KUMA 组件的错误，请禁用调试。如果要在日志中获取详细信息，请启用调试。

12. 如有必要，在“**ClickHouse 集群节点**”部分中，将 ClickHouse 集群节点添加到存储。

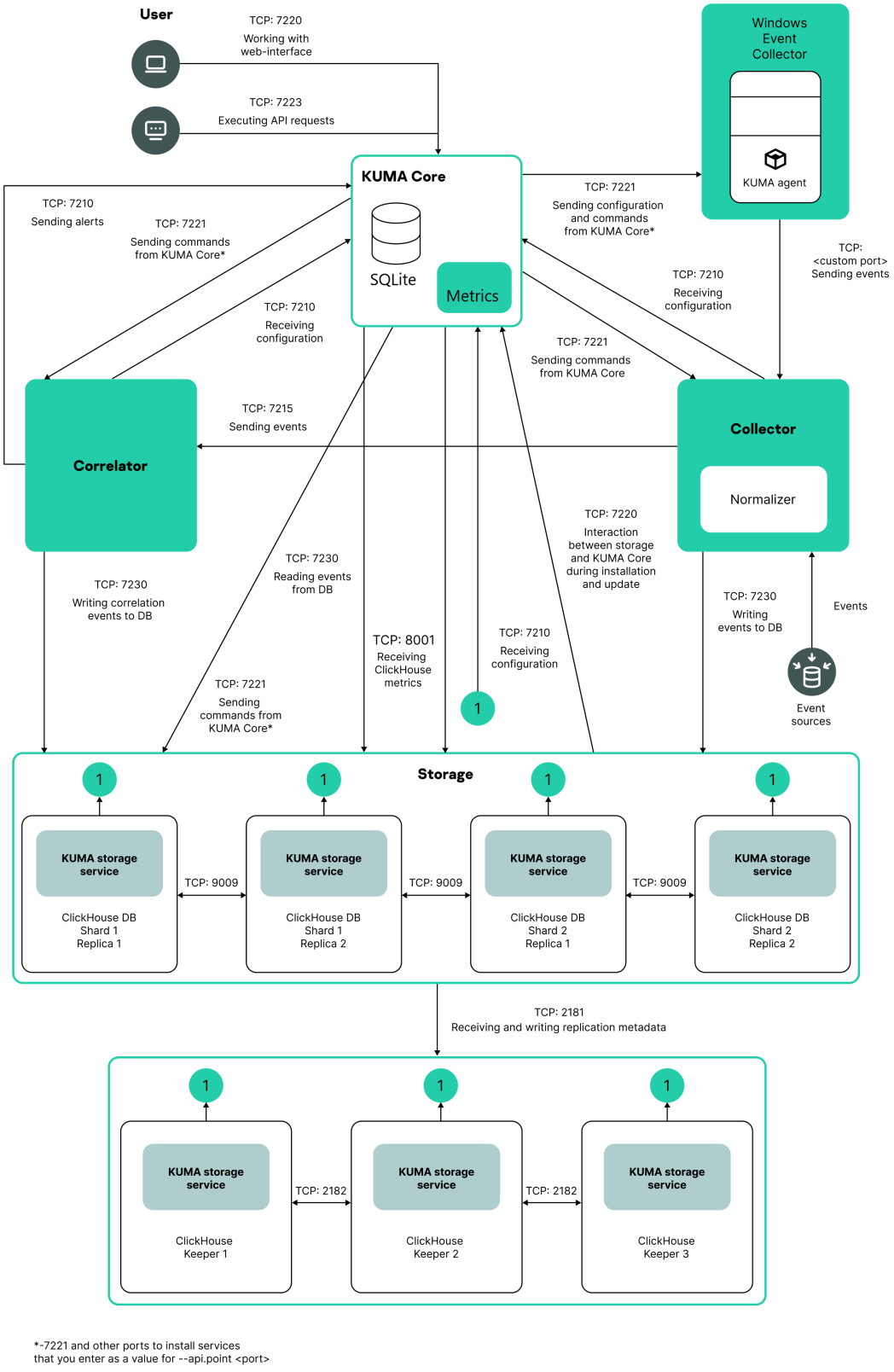
    可以设置多个节点。您可以通过单击“**添加节点**”按钮添加节点，或通过单击相关节点的 X 图标删除节点。

    可用设置：

    - 在“**FQDN**”字段中，输入要添加的节点的完全限定域名。例如，`kuma-storage-cluster1-server1.example.com`。

    - 在“**分片 ID**”、“**副本 ID**”和“**Keeper ID**”字段中，指定节点在 ClickHouse 集群中的角色。分片和 Keeper ID 在集群内必须是唯一的，副本 ID 在分片内必须是唯一的。以下示例展示了如何在分布式安装中为带有专用 keeper的存储填充**ClickHouse 集群节点**部分。您可以根据需要调整此示例。

分布式安装示意图



分布式安装示意图

例如：

ClickHouse 集群节点

FQDN：kuma-storage-cluster1-server1.example.com

Shard ID: 0

Replica ID: 0
Keeper ID: 1
FQDN: kuma-storage-cluster1server2.example.com
Shard ID: 0
Replica ID: 0
Keeper ID: 2
FQDN: kuma-storage-cluster1server3.example.com
Shard ID: 0
Replica ID: 0
Keeper ID: 3
FQDN: kuma-storage-cluster1server4.example.com
Shard ID: 1
Replica ID: 1
Keeper ID: 0
FQDN: kuma-storage-cluster1server5.example.com
Shard ID: 1
Replica ID: 2
Keeper ID: 0
FQDN: kuma-storage-cluster1server6.example.com
Shard ID: 2
Replica ID: 1
Keeper ID: 0
FQDN: kuma-storage-cluster1server7.example.com
Shard ID: 2
Replica ID: 2
Keeper ID: 0

13. 如有必要，在“**空间**”部分中，向存储中添加空间以分配所存储的事件。

    可以存在多个空间。您可以通过单击“**添加空间**”按钮来添加空间，或通过单击相关空间的 X 图标删除空间。

    可用设置：

    - 在“**名称**”字段中，为空间指定一个包含 1 到 128 个 Unicode 字符的名称。

    - 在“**保留策略选项**”字段中，为控件选择 ClickHouse 集群中的事件存储条件。当满足该条件时，事件将被传输到冷存储磁盘；如果未配置冷存储或冷存储配置不正确，则事件将被删除。添加空间时，OSMP 会应用 **365 天**存储条件。

      要设置空间的存储条件，请执行以下操作之一：

      - 如果要限制事件的存储期限，请从下拉列表中选择“**天数**”，然后在字段中指定 ClickHouse 热存储集群中的最大事件存储期限（以天为单位）。

        在指定的时间段之后，事件将被自动传输到冷存储磁盘或从 ClickHouse 集群中删除，从日期最早的分区开始。最小值是 1。默认值是 365。

      - 如果要限制最大存储空间大小，请从下拉列表中选择“**GB**”，然后在字段中指定最大空间大小（以 GB 为单位）。

        当空间达到指定大小时，事件将被自动传输到冷存储磁盘或从 ClickHouse 集群中删除，从日期最早的分区开始。最小值和默认值均为 1。

      - 如果要将空间大小限制为可用于存储的磁盘空间的百分比，请从下拉列表中选择“**百分比**”，然后在字段中将最大空间大小指定为可用于存储的磁盘大小的百分比。在这种情况下，当可用磁盘存储空间减少时，也会触发此条件。

        当空间达到指定的可用于存储的磁盘空间百分比时，事件将被自动传输到冷存储磁盘或从 ClickHouse 集群中删除，从日期最早的分区开始。可能值：1 到 95。默认值是 80。如果要对所有存储空间使用百分比，则所有空间条件中的百分比总和不得超过 95，但我们建议为整个存储或单个空间指定最多 90% 的限制。

不建议指定较小的百分比值，因为这会增加存储中数据丢失的可能性。

当使用大小作为存储条件时，必须保证存储条件中指定的所有空间的总大小不超过存储的物理大小，否则启动服务时会报错。

在具有大小限制的存储条件中，请对所有存储空间使用相同的度量单位（仅千兆字节或仅百分比值）。否则，如果一个空间的条件指定为百分比，而另一个空间指定为千兆字节，则存储可能会因值不匹配而溢出，从而导致数据丢失。

- 如果要在空间过期且不再相关时将其设为非活动状态，请选中“**只读**”复选框。

  这可以防止事件进入该空间。要使空间再次活动，请清除“**只读**”复选框。默认情况下，此复选框未被选中。

- 如有必要，请在“**事件保留时间**”字段中，指定 KUMA 事件的总存储时长（以天为单位），从收到事件的那一刻起计算。当指定的期限到期时，会自动将事件从冷存储磁盘中删除。默认值是 0。

  事件保留时间计算为触发“**保留策略选项**”设置中指定的条件之前 ClickHouse 热存储集群中的事件保留时间与冷存储磁盘上的事件保留时间之和。触发其中一个存储条件后，日期最早的数据分区将移动到冷存储磁盘，并保留在该磁盘上，直到 OSMP 中的事件保留时间到期。

  根据指定的存储条件，最终的保留时间如下：

  - 如果以天为单位指定存储条件，则**事件保留时间**必须严格大于存储条件中指定的天数。事件的冷存储时长计算为“**事件存储时间**”减去“**保留策略选项**”设置中指定的天数。

    如果您不想将此空间中的事件存储在冷存储磁盘上，则可以在“**事件保留时间**”字段中指定与存储条件中相同的天数。

  - 如果您以磁盘大小（绝对值或百分比）指定存储条件，则“**事件保留时间**”的最小值为 1。事件的冷存储持续时间计算为“**事件保留时间**”减去从收到事件到触发条件和磁盘分区填满的天数，但在触发条件之前，无法计算准确的持续时间。在这种情况下，建议为“**事件保留时间**”指定一个相对较大的值，以避免事件被删除。

    如果您不想将此空间中的事件存储在冷存储磁盘上，可以将“**事件保留时间**”设置为 0。

  只有添加至少一个冷存储磁盘后，“**事件保留时间**”设置才可用。

- 在“**过滤器设置**”部分，您可以指定条件来识别将放入此空间的事件。要创建新的过滤器，请在“**过滤器**”下拉列表中选择现有过滤器或**创建新的过滤器**。

  在资源中创建过滤器

  KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

  要创建过滤器：

  1. 在“**过滤器**”下拉列表中，选择“**新建**”。

  2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。

  3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。

4. 在**"条件"**下，指定事件必须满足的条件：

   a. 单击"**添加条件**"按钮。

   b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。

   c. 在"**运算符**"下拉列表中，选择一个运算符。

   过滤器运算符

   - **=** — 左操作数等于右操作数。
   - **<** — 左操作数小于右操作数。
   - **<=** — 左操作数小于或等于右操作数。
   - **>** — 左操作数大于右操作数。
   - **>=** — 左操作数大于或等于右操作数。
   - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
   - **contains** — 左操作数包含右操作数的值。
   - **startsWith** — 左操作数以右操作数的某个值开头。
   - **endsWith** — 左操作数以右操作数的某个值结尾。
   - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
   - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

     待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

     如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
   - **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

     如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
   - **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
   - **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
   - **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
   - **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
   - **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。

- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

创建服务后，您可以在存储资源设置中查看和删除空间。

> 您无需为审计事件（审计事件、审计事件）创建单独的空间。此类型 (Type=4) 的事件会自动放置在单独的审计空间中，存储期限至少为 365 天。无法从 OSMP Web 界面编辑或删除此空间。

14. 如有必要，在“**冷存储磁盘**”部分中，将要从 ClickHouse 集群传输事件以进行长期存储的磁盘添加到存储中。
可以存在多个磁盘。您可以通过单击“**添加磁盘**”按钮添加磁盘，或通过单击“**移除磁盘**”按钮删除磁盘。
可用设置：

- 在“**类型**”下拉列表中，选择正在连接的磁盘的域名类型：
  - **本地** — 用于作为目录挂载在操作系统中的磁盘。
  - **HDFS** — 用于 Hadoop 分布式文件系统的磁盘。
  - **S3** — 用于KUMA中使用的S3云存储。

    > 从4.2版本开始，存储在HDFS驱动器上的数据将逐步迁移到S3驱动器。对 HDFS 文件系统的支持将在解决方案的未来版本中停止。

- 在“**名称**”字段中指定磁盘名称。该名称必须包含 1 到 128 个 Unicode 字符。

  > 您不能在不更改驱动器路径的情况下更改 S3 驱动器的名称。

- 如果选择磁盘的**本地**域名类型，请在**路径**字段中输入以下值之一。
  - 如果存储服务部署在本地，请输入本地驱动器挂载目录的绝对路径。路径必须以“/”字符开头和结尾。

    > 挂载的本地磁盘目录必须归 KUMA 用户所有。

  - 如果存储服务部署在 Kubernetes 集群上，请输入路径： `/opt/cold/` 。将部署存储服务的 Kubernetes 集群节点的 `/opt/lvp/cold/` 目录挂载到 `/opt/cold` 目录。

- 如果为磁盘选择“**HDFS**”域名类型，请在“**主机**”字段中指定 HDFS 的路径（例如，`hdfs://hdfs1:9000/clickhouse/`）。
- 如果您选择**S3**作为驱动器的域名类型，请指定以下参数：
  - 在“**主机**”字段中，输入 S3 存储的地址（例如，`https://www.company.com/clickhouse/storagefolder/`）。

    指定 S3 存储地址的规则

    指定 S3 存储地址时，必须满足以下要求：
    - 地址必须以 URL 格式指定，例如：`https://<web address/IP address of the server>/<path to disk>/`
    - 地址必须以“/”字符结尾。
    - 最大长度为 2048 个字符。
    - 不允许使用非拉丁字母。

    > 您不能在不更改磁盘名称的情况下更改 S3 存储磁盘的地址。

  - 在**“密钥”**字段中，指定用于访问 S3 存储的密钥。您可以从下拉列表中选择一个密钥，也可以单击**“新建”**来创建一个密钥。

15. 在**“配置备份和恢复”**部分，管理以下设置：

    a. 在**“存储备份”**字段中，指定要保存备份文件的路径。例如，/mnt/data。
    路径要求：
    - 该路径必须存在，并且在存储集群的所有节点上都必须相同。
    - 用户必须对指定的目录具有读取、写入和执行权限。
    - 指定的目录必须属于第二层或更深层的嵌套目录。您不能使用第一级嵌套目录，例如/backup。
    - 目录名称不能包含句号。
    - **路径不得包含以下前缀。**

      指定文件路径时不能使用的前缀：
      - `/*`
      - `/bin`
      - `/boot`
      - `/dev`
      - `/etc`
      - `/home`

- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。

文件可通过以下路径获取：

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/metrics/log/

系统会在指定的路径下自动创建两个目录：**backup** 和 **restore**。

如果未指定路径，则计划备份、手动备份、从备份恢复和导入功能将不可用。

b. 要配置计划备份，请启用**“计划备份”**开关。

c. 在**“几天后备份”**字段中，指定分区创建后的天数（整数），在此之后将创建备份副本。例如，如果值为 **1**，则备份前天创建的分区。

d. 在**"副本"**下拉列表中，选择要备份的副本。选择同一分片的多个副本会导致数据重复。

e. 在**"分区"**下，单击**"添加分区"**并管理以下设置：

a. 在**"租户"**下拉列表中，选择包含要备份的分区的租户。

b. 在**"空间"**下拉列表中，选择属于要备份的分区的一个或多个存储空间。如果未指定值，则备份整个分区。

您可以管理多个分区的设置。如有必要，单击**"添加分区"**并在显示的字段中管理新分区的设置。例如，如果您要备份**审计**空间，并且您有10个租户，则必须为每个租户单独配置备份。

16. 转到"**高级设置**"选项卡并填写以下字段：

- 在"**缓冲区大小**"字段中，输入事件必须发送到数据库的缓冲区大小（以字节为单位）。默认值为128MB。未配置最大值。如果虚拟机的可用 RAM 少于指定的"**缓冲区大小**"，OSMP 会将限制设置为 128 MB。

  如果预计流向存储服务的流量大于 1 Gbps，我们建议将"**缓冲区大小**"设置的字节值更改为预期值，并将"**缓冲区刷新间隔**"设置为 2。

  缓冲区大小设置的值可以通过经验确定。如果存储的"**插入 QPS**"指标大于 1，并且发现请求队列不断增长，请遵循《查看 OSMP 指标》一文的"插入 QPS"部分中有关计算和调整"**缓冲区大小**"设置的建议。

- 在**"最大缓冲区大小"**字段中，以字节为单位指定最大缓冲区大小。默认值为256MB。

  默认情况下，事件每秒写入数据库一次。如果 EPS 上升且事件注册频率超过每秒一次，则缓冲区大小会自动增加。缓冲区大小最多增加到**"缓冲区大小"**值的三倍，但不能超过**"最大缓冲区大小"**值。当负载恢复正常时，缓冲区大小保持不变；不会自动减小缓冲区大小。

  如果**"最大缓冲区大小"**小于或等于**"缓冲区大小"**，则缓冲区大小不会改变。

  重新启动存储服务会将增加的缓冲区大小重置为**"缓冲区大小"**字段中的值。

- 在"**缓冲区刷新间隔**"字段中，输入 OSMP 等待缓冲区填满的时间（以秒为单位）。如果缓冲区未满，但指定的时间已过，OSMP 会将事件发送到数据库。默认值是 1 秒。

- 在**"所需内存大小"**字段中，以字节为单位指定最小可用 RAM 量。默认值为128MB。

  如果存储所在的节点的可用 RAM 小于此设置值，则数据库插入请求将返回错误，事件将被稍后记录。限制内存大小可以避免因任何原因导致数据库事件记录阻塞，数据开始在内存中累积，从而造成内存耗尽的情况。

- 在"**磁盘缓冲区大小限制**"字段中，输入一个以字节为单位的值。磁盘缓冲区用于临时存储无法发送以进行进一步处理或存储的事件。如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。默认值是 10 GB。

- 使用"**磁盘缓冲区**"切换开关可启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。

- 使用"**写入本地数据库表**"切换开关可启用或禁用写入本地数据库表。默认情况下，写入选项被禁用。

  如果启用，则数据仅写入存储所在的主机上。建议仅在已在收集器和/或关联器上配置均衡的情况下使用此功能 — 具体配置步骤参见**步骤6。在"高级设置"部分，路由**的"**URL 选择策略**"字段设置为"**循环**"。

  如果禁用写入，数据将分布在集群的各个分片上。

- 如有必要，可以使用"**调试**"切换开关来启用服务操作的日志记录功能。

- 您可以根据技术支持的要求，使用"**定期创建转储**"切换开关，以转储形式生成资源利用率报告（CPU 或 RAM）。

- 在"**转储设置**"字段中，您可以指定创建转储时要使用的设置。有关填写此字段的说明，请联系技术支持。

存储的资源集已创建并显示在“**资源**” → “**存储**”下。现在，您可以创建存储服务。

在 OSMP 中创建存储服务

为存储创建资源集后，您可以继续在 KUMA 中创建存储服务。

要在 OSMP 中创建存储服务：

1. 在 KUMA 控制台中，在“**资源**”→ “**活动服务**”下，单击“**添加服务**”。
2. 在打开的**选择服务**窗口中，选择刚为存储创建的资源集，然后单击**创建服务**。

存储服务已在 OSMP 中创建，并显示在“**资源**” →“**活动服务**”部分。现在必须使用服务 ID 将存储服务安装到 ClickHouse 集群的每个节点。

在 OSMP 网络基础设施中安装存储

要创建存储：

1. 登录到要安装该服务的服务器。
2. 创建 /opt/kaspersky/kuma/ 文件夹。
3. 将“kuma”文件复制到 /opt/kaspersky/kuma/ 文件夹。该文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/ 文件夹中。

   请确保 kuma 文件具有足够的运行权限。

4. 执行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。
   - <port> 是 KUMA Core 用于内部通讯的端口（默认使用端口 7210）。
   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书的指纹 ID。

     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

     为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。

   - <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。

例如：

```
sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --install
```

在同一主机上部署多个 KUMA 服务时，在安装过程中，您必须使用 `--api.port <端口>` 参数为每个组件指定唯一端口。默认使用以下设置值：`--api.port 7221`。

5. 对每个存储节点重复步骤 1 和 2。

存储已安装。

备份、恢复和导入分区

具有常规管理员角色的用户有权执行以下 OSMP 操作：

- 计划分区备份。
- 手动备份分区。
- 从备份恢复分区。
- 从外部 OSMP 实例导入分区。

您可以同时配置和使用事件冷存储和分区备份。

您可以在审计事件中查看分区备份、恢复和导入的状态。此外，在启动手动分区备份、从备份恢复分区或从外部 OSMP 实例导入分区后，**任务管理器**部分中会创建相应的任务。

计划分区备份

具有主管理员角色的用户可以配置分区计划备份。

要计划备份：

1. 在主菜单中，转到**监控→资源和服务→活动服务**部分，然后打开一个活动存储来管理其设置。
2. 在打开的**编辑存储**窗口中，在**基本设置**选项选项卡上的**设置备份和恢复**部分，管理以下设置：
   a. 在**"存储备份"**字段中，指定要保存备份文件的路径。例如，/mnt/data。如果没有指定路径，则无法执行备份。
   b. 启用**"计划备份"**切换开关。
   c. 在**在指定天数后备份**字段中，指定在创建分区后多少天创建其备份副本。例如，如果值为 **1**，则备份前天创建的分区。
   d. 在"**副本**"下拉列表中，选择要备份的副本。选择同一分片的多个副本会导致数据重复。
   如果集群中使用多个分片，**副本**列表仅包含所有碎片中指定ID的副本。

3. 在“**备份分区**”下，单击“**添加分区**”并管理以下设置：

   a. 在**“租户”**下拉列表中，选择包含要备份的分区的租户。

   b. 在**“空间”**下拉列表中，选择属于要备份的分区的一个或多个存储空间。如果未指定值，则备份整个分区。

   您可以管理多个分区的设置。如有必要，单击“**添加分区**”并在显示的字段中管理新分区的设置。例如，如果您要备份**审计**空间，并且您有10个租户，则必须为每个租户单独配置备份。

4. 单击“**保存**”。

保存设置后，**备份**和**恢复**目录将在指定路径自动创建。**备份**目录中会自动创建包含租户 ID 和空间 ID 的子目录。例如，如果您将 /mnt/data 指定为备份路径，则备份文件的完整路径为 /mnt/data/backup/<租户 ID>/<存储空间 ID>/<分区创建日期>.zip。如果您需要查找租户或空间的 ID，您可以转到**“事件”**部分，打开事件卡并查看您需要的信息。

要从备份恢复，您需要将备份文件移动到**恢复**目录。

计划分区备份被配置。如果备份失败，则会生成相应的审计事件，存储服务在**“活动服务”**部分中会显示黄色状态，并且当您将鼠标悬停在黄色状态指示器上时，会显示错误消息。下次启动计划备份时，会先尝试备份旧数据。

手动备份分区

具有主管理员角色的用户可以手动备份分区。

要手动创建分区备份副本：

1. 在主菜单中，转到**监控→资源和服务→活动服务**部分，然后打开一个活动存储来管理其设置。

2. 这将打开**编辑存储**窗口；在该窗口中，在**基本设置**选项卡的**备份设置**部分中的**存储备份**字段中，指定备份文件的路径。例如，/mnt/data。请确保“kuma”用户拥有对指定目录的访问权限。

   路径要求：

   - 该路径必须存在，并且在存储集群的所有节点上都必须相同。
   - 用户必须对指定的目录具有读取、写入和执行权限。
   - 指定的目录必须属于第二层或更深层的嵌套目录。您不能使用第一级嵌套目录，例如/backup。
   - 目录名称不能包含句号。
   - **路径不得包含以下前缀。**

     指定文件路径时不能使用的前缀：

     - `/*`
     - `/bin`
     - `/boot`
     - `/dev`

- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。

文件可通过以下路径获取：

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/metrics/log/

3. 在主菜单中，转到**监控→资源和服务→活动服务**部分，然后选中状态为绿色的存储服务旁边的复选框。

4. 在工具栏或菜单(⋮)中，选择“**备份**”，然后单击“**备份**”。

如果选择了一个存储服务且该服务处于绿色状态，则“**备份**”选项可用。

在以下情况下，此选项不可用：

- 如果在上一步中，您选中了多个服务旁边的复选框。
- 如果存储服务状态为红色。
- 如果未选中任何复选框。
- 如果您选中了其他类型服务旁边的复选框。

5. 则在打开的**“分区备份”**窗口中，管理以下设置：
   a. 在**“租户”**下拉列表中，选择包含要备份的分区的租户。
   b. 在**“空间”**下拉列表中，选择属于要备份的分区的一个或多个存储空间。如果未指定值，则备份整个分区。
   c. 在“**副本**”下拉列表中，选择要备份的一个副本或所有副本。选择同一分片的多个副本会导致数据重复。
   d. 在“**日期范围**”字段中，使用日历指定要包含在备份中的分区的日期范围。
6. 单击“**确定**”。
7. 在**“将执行备份”**确认窗口中，单击**“确定”**。
   确认**任务管理器**部分中的设置后，将创建分区备份任务和审计事件。

手动备份完成。

保存设置后，**备份**和**恢复**目录将在指定路径自动创建。**备份**目录中会自动创建包含租户 ID 和空间 ID 的子目录。例如，如果您将 /mnt/data 指定为备份路径，则备份文件的完整路径为 /mnt/data/backup/<租户 ID>/<存储空间 ID>/<分区创建日期>.zip。如果您需要查找租户或空间的 ID，您可以转到**“事件”**部分，打开事件卡并查看您需要的信息。

要从备份恢复，您需要将备份文件移动到**恢复**目录。

如果手动备份的文件名与计划备份文件的名称相同，则返回一个错误，指出无法保存备份文件。您必须重命名该文件或将其删除，然后再次执行手动备份。

通过查看存储服务的黄色状态和错误消息、**任务管理器**部分或审计事件，您可以在**活动服务**部分中找到有关备份错误的信息。

从外部 OSMP 实例导入分区

具有“常规管理员”角色的用户可以从外部 OSMP 实例导入分区。

要从外部 OSMP 实例导入分区：

1. 使用以下命令，授予“kuma”用户对您在管理备份设置时指定的备份目录的访问权限，以及对备份文件本身的访问权限：

```
sudo chown kuma <备份目录的完整路径>
sudo chown kuma *.zip
```

2. 将要从中导入分区的文件放入**恢复**目录。分区将从此目录导入。

3. 在主菜单中，转到**监控→资源和服务→活动服务**部分，然后选中状态为绿色的存储服务旁边的复选框。

4. 在工具栏或菜单（⋮）中，选择**备份→导入**。

5. 在显示的**从外部实例 OSMP 导入**窗口中，管理以下设置：

   a. 在**"租户"**下拉列表中，选择要导入分区的租户。

   b. 在**副本**下拉列表中，选择要将分区导入的副本。

   c. 在**排除项字段**下拉列表中，选中或清除复选框，即可指定要在导入过程中删除的字段。
   默认情况下，以下字段的复选框已选中：

   - AggregationRuleName
   - CorrelationRuleName
   - SourceAccountID
   - DestinationAccountID
   - SourceAssetID
   - DestinationAssetID
   - 设备资产 ID
   - KUMA 扩展事件模式字段：
     - 扩展事件模式字段
     - KSC 资产字段
     - KLCorrelationRulePriority = "KL_CorrelationRulePriority"
     - KLSourceAssetDisplayName = "KL_SourceAssetDisplayName"
     - KLDestinationAssetDisplayName = "KL_DestinationAssetDisplayName"
     - KLDeviceAssetDisplayName = "KL_DeviceAssetDisplayName"
     - KLSourceAccountDisplayName = "KL_SourceAccountDisplayName"
     - KLDestinationAccountDisplayName = "KL_DestinationAccountDisplayName"
     - KLDllHijackingResult = "KL_AI_DLLHijackingCheckResult"
       当您选择"**KUMA 扩展事件模式字段**"类别进行删除时，整个字段组将被删除。您无法删除单个字段。

默认情况下，以下字段将被移除，因此在 Web 界面中无法选择：

- ServiceID
- ServiceName
- CorrelationRuleID
- AggregationRuleID

6. 单击“**确定**”。
7. 在**“将要执行导入”**确认窗口中，单击**“确定”**。
   在**任务管理器**部分确认设置后，将创建分区导入任务和审计事件。

从外部 OSMP 实例导入分区。

从备份恢复分区

只有具有主管理员角色的用户才能从备份恢复分区。

要从备份恢复分区，请执行以下操作：

1. 使用以下命令，授予“kuma”用户对您在管理备份设置时指定的备份目录的访问权限，以及对备份文件本身的访问权限：

   ```
   sudo chown kuma <备份目录的完整路径>
   sudo chown kuma *.zip
   ```

2. 将备份文件从**备份**目录移动到**恢复**目录。
3. 在主菜单中，转到**监控→资源和服务→活动服务**部分，然后选中状态为绿色的存储服务旁边的复选框。
4. 在工具栏或菜单（⋮）中，选择**备份→恢复**。
5. 在打开的**从当前 KUMA 安装恢复**窗口中，从**副本**下拉列表中选择一个您要在其中执行从备份恢复操作的副本。
6. 单击“**确定**”。
7. 在**“将执行恢复”**确认窗口中，单击**“确定”**。
   在**任务管理器**部分中确认设置后，将创建分区恢复任务和审计事件。

分区从备份恢复完成。

创建关联器

关联器由两部分组成：一部分在 OSMP 内创建，另一部分安装在用于处理事件的网络基础设施服务器上。

OSMP 中的操作

使用安装向导在 OSMP 中创建关联器。此向导将必要的资源组合成关联器所需的资源集。完成向导后，系统将基于该资源集自动创建服务。

要在 OSMP 中创建关联器，

启动关联器安装向导：

- 在 OSMP 的主菜单中，在 **资源和服务** 下，单击 **添加关联器**。
- 在 OSMP 的主菜单中，在 **资源和服务** → **关联器** 下，单击 **添加关联器**。

完成向导的步骤后，将在 OSMP 中创建一个关联器服务。

关联器的资源集包括以下资源：

- 关联规则
- 富集规则（如需要）；
- 响应规则（如需要）
- 目标位置（通常用于将事件发送到存储）

这些资源可以提前准备，也可以在安装向导运行时进行创建。

OSMP 关联器服务器上的操作

如果要在计划用于事件处理的服务器上安装关联器，则需要在该服务器上运行安装向导最后一步显示的命令。安装时，必须指定 OSMP 中自动分配给服务的 ID，以及用于通信的端口。

测试安装

创建关联器后，建议确保其正常运行。

启动关联器安装向导

要启动关联器安装向导：

- 在 OSMP 的主菜单中，在 **资源和服务** 下，单击 **添加关联器**。
- 在 OSMP 的主菜单中，在 **资源和服务** → **关联器** 下，单击 **添加关联器**。

遵照向导的说明操作。

除了向导的第一步和最后一步之外，向导的步骤可以按任意顺序执行。您可以使用**下一步**和**上一步**按钮，或单击窗口左侧的步骤名称，在各步骤之间切换。

向导完成后，将在 OSMP 的 **资源和服务** → **关联器** 下创建关联器资源集，并在 **资源和服务** → **活动服务** 下添加关联器服务。

步骤 1：关联器常规设置

这是安装向导的必需步骤。在此步骤中，您可以指定关联器的主要设置：关联器名称和所属租户。

要定义关联器的主要设置：

- 在“**名称**”字段中，输入您正在创建的服务的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
- 在“**租户**”下拉列表中，选择必须拥有该关联器的租户。租户选择决定了创建收集器时可用的资源。

  > 如果您从安装向导的另一个后续步骤返回至此窗口并选择了另一个租户，则必须手动编辑已添加到服务的所有资源。只有选定租户和共享租户的资源能够添加到服务。

- 如需要，请在“**工作节点**”字段中指定服务可并发运行的进程数量。默认情况下，工作进程数量与安装服务的服务器上的 vCPU 数量相同。
- 如有必要，请使用“**调试**”下拉列表启用服务操作日志记录。
- 您可以选择在“**描述**”字段中添加最多 256 个 Unicode 字符来描述服务。

已定义关联器的主要设置。继续执行安装向导的下一步。

步骤 2：全局变量

如果跟踪事件字段、活动列表或字典中的值不足以涵盖某些特定的安全场景，则可以使用全局变量和局部变量。您可以使用这些变量对关联器收到的值执行各种操作，以实施复杂的威胁检测逻辑。可以为变量分配特定的函数，然后像查询普通事件字段一样从关联规则中进行查询，并在响应中收到触发的函数结果。

要在关联器中添加全局变量，

单击**添加变量**按钮并指定以下参数：

- 在“**变量**”窗口中，输入变量的名称。

  变量命名要求

  - 在关联器内必须是唯一的。
  - 必须包含 1 到 128 个 Unicode 字符。
  - 不能以 $ 字符开头。
  - 必须用 camelCase 或 CamelCase 形式书写。

- 在“**值**”窗口中，输入变量函数。

  变量函数描述。

已添加全局变量。可通过在变量名称前面添加 $ 字符，来从关联规则中查询。可以指定多个变量。可使用 × 图标编辑或删除已添加变量。

继续执行安装向导的下一步。

步骤 3：关联

这是安装向导中的可选步骤，但推荐执行。在安装向导的**关联**选项卡上，选择或创建关联规则。这些资源定义了指示安全相关事故的事件序列。当检测到这些序列时，关联器会创建关联事件和警报。

如果已将全局变量添加到关联器，则所有添加的关联规则都可查询这些变量。

添加到关联器资源集中的关联规则显示在具有以下列的表格中：

- **关联规则** – 关联规则资源的名称。
- **类型** – 关联规则的类型：**标准**、**简单**、**操作**。单击列标题并选择相关值，即可根据此列的值对表格内容进行筛选。
- **操作** – 当关联规则被触发时，关联器将执行的操作列表。这些操作在关联规则设置中指示。单击列标题并选择相关值，即可根据此列的值对表格内容进行筛选。

  可用值：

  - **输出** – 此关联规则创建的关联事件将传输到其他关联器资源，包括丰富规则、响应规则，然后再传输到其他 OSMP 服务。
  - **编辑活动列表** – 关联规则将更改活动列表。
  - **循环至关联器** – 关联事件将发送到相同的关联规则进行重新处理。
  - **分类** – 关联规则将更改资产类别。
  - **事件增强** – 关联规则配置为增强关联事件。
  - **不创建警报** – 当关联规则触发并创建关联事件时，不会为此创建警报。如果不想在触发关联规则时创建警报，但仍想将关联事件发送到存储，请选中**输出**和**不触发警报**复选框。如果仅选中“**不触发警报**”复选框，则关联事件不会保存在存储中。
  - **共享资源** – 关联规则或关联规则中使用的资源位于共享租户中。

您可以使用“**搜索**”字段来搜索关联规则。选择相关规则并单击“**删除**”，即可从资源集中移除已添加的关联规则。

选择关联规则后，将打开一个包含其设置的窗口，您可以编辑这些设置，然后单击“**保存**”进行保存。如果在此窗口中单击“**删除**”，关联规则将与资源集解除关联。

单击“**上移**”和“**下移**”按钮，即可更改所选关联规则在表格中的位置。这会影响处理事件时规则的执行顺序。使用“**将运行类规则移至顶部**”按钮，可以将**操作**类型的关联规则移至关联规则列表的开头。

要将现有的关联规则关联到关联器的资源集，请执行以下操作：

1. 单击“**链接**”。
   将打开资源选择窗口。
2. 选择相关的关联规则并单击“**确定**”。

关联规则将关联到关联器的资源集，并显示在规则表中。

要在关联器的资源集中创建新的关联规则，请执行以下操作：

1. 单击“**添加**”。
   关联规则创建窗口将打开。
2. 指定关联规则设置，然后单击“**保存**”。

将创建关联规则并将其关联到关联器的资源集。它显示在关联规则表中，以及“**资源**” → “**关联规则**”下的资源列表中。

继续执行安装向导的下一步。

步骤 4：增强

这是安装向导的可选步骤。在安装向导的“**增强**”选项卡中，您可以选择或创建增强规则，并指定要将哪些来源的哪些数据添加到关联器创建的关联事件中。可以指定多个增强规则。您可以通过单击“**添加**”按钮进行添加，也可以通过单击 ✕ 按钮进行删除。

要将现有的增强规则添加到资源集中：

1. 单击“**添加**”。
   这将打开增强规则设置块。
2. 在“**增强规则**”下拉列表中，选择相关资源。

增强规则将添加到关联器的资源集中。

要在资源集中创建新的增强规则：

1. 单击“**添加**”。
   这将打开增强规则设置块。
2. 在“**增强规则**”下拉列表中，选择“**新建**”。

3. 在“**源类型**”下拉列表中，选择要增强的数据源并定义其相应的设置：

- **常量**

  在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置：

  - 在“**常量**”字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。
  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

  如果对 `String`、 `Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。

  如果对 `Array of strings`、 `Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。

- **词典**

  如果需要从“字典”类型的**字典**中添加值，则使用此类型的增强规则。

  在“**字典名称**”下拉列表中选择此类型后，必须选择用于提供值的字典。在“**键字段**”设置块中，您必须点击“**添加字段**”按钮，然后选择相应的事件字段，其值将用于词典条目选择。

  如果您使用事件增强功能，并在“源类型”设置中选择了“字典”类型，且在“键增强字段”设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。

  示例：“键增强字段”设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”。以下值作为键传递给字典：['a','b','c']。

  如果“键增强字段”设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以“|”字符分隔。

  示例：“键增强字段”设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”；Code 字符串字段包含字符序列“myCode”。以下值作为键传递给词典：['a','b','c']myCode。

- **事件**

  若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置：

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
  - 在“**源字段**”下拉列表中，选择要将其值写入目标字段的事件字段。
  - 在“**转换**”下，您可以创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。可以从下拉列表中选择转换类型。您可以使用“**添加转换**”和“**删除转换**”按钮来添加或删除转换。转换的顺序很重要。

    可用转换

    转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

可用转换：

- **lower** — 用于将值的所有字符变为小写
- **upper** — 用于将值的所有字符变为大写
- **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
- **substring** — 用于提取"**开始**"和"**结束**"字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除"**字符**"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
- **append** 用于将"**常量**"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

- **模板**

在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

- 在“**模板**”字段中，输入 Go 模板。

  事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。

  例如：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。
- 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

如果您使用事件增强功能，并在“**源类型**”设置中选择了“**模板**”类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

例如：

{{.SA.StringArrayOne}}

例如：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

这种类型的增强功能用于向私有网络 DNS 服务器发送请求，以实现 IP 地址与域名之间的相互转换。仅对以下私有地址进行 IP 地址到 DNS 名称的转换：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、100.64.0.0/10、fd00::/8。

下表介绍了此类增强功能的设置。

“dns”类型的增强功能参数

设置	描述
网址	要向其发送请求的 DNS 服务器的 URL。 您可以使用 **添加 URL** 按钮指定多个 URL。 如果未指定 **URL** 设置，KUMA 将从本地主机的 `/etc/resolv.conf` 文件中获取 DNS 服务器列表。在这种情况下，您需要启用 **递归查询** 选项。否则，将不会执行增强操作。

设置	描述
每秒请求数	每秒向 DNS 服务器发送的最大查询数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
工作进程	服务可以同时运行以并行处理响应规则的处理程序数量。请指定一个介于 0 到 999 之间的正整数。如果指定为 0，则使用逻辑 CPU 核心数。默认值为 `1`。
数据增强队列中的最大事件数	重新提交队列中可容纳的最大事件数。默认值为 `1,000,000`。
超时时间	等待 DNS 服务器响应的时间（以秒为单位）。默认值为 `5`。
DNS 模式覆盖	使用的解析方法： • **仅正向** DNS将域名解析为 IP 地址。 • **仅反向** DNS将 IP 地址解析为域名。 • **正向和反向** DNS将域名解析为 IP 地址，或将 IP 地址解析为域名。
缓存 TTL	缓存中存储的值的生存时间（以秒为单位）。默认值为 `60` 秒。
缓存已停用	您可以使用此设置启用或禁用缓存。默认情况下启用缓存。
缓存刷新已停用	如果启用了缓存更新，当缓存的 TTL 到期时，收集器会多次向 DNS 服务器发送请求，以更新缓存中存储的数据。此设置仅在启用缓存时可用。默认情况下，缓存更新已启用。
递归查询	允许收集器向权威 DNS 服务器发送递归查询，以进行数据增强。默认值是“**已禁用**”。

- **cybertrace**

  此类增强功能用于将 CyberTrace 数据流中的信息添加到事件字段。

  可用设置：

  - **URL**（必填）— 在此字段中，您可以指定要向其发送请求的 CyberTrace 服务器的 URL。
  - **连接数** — KUMA 可与 CyberTrace 服务器建立的最大同时连接数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
  - **RPS** — 每秒向服务器发送的最大请求数。默认值为 `1000`。
  - **超时** — 等待 CyberTrace 服务器响应的时间（以秒为单位）。默认值为 `30`。
  - **映射**（必需）— 此设置块包含用于将 KUMA 事件字段映射到 CyberTrace 指标类型的映射表。**KUMA 字段**列显示 KUMA 事件字段的名称，**CyberTrace 指标**列显示 CyberTrace 指标的类型。

    可用的 CyberTrace 指标类型：

    - **ip**
    - **url**
    - **哈希**

    在映射表中，您必须提供至少一个字符串。您可以单击“**添加行**”按钮来添加字符串，也可以单击 ✕ 按钮来删除字符串。

- **时区**

  这种类型的增强功能在收集器和关联器中用于为事件分配特定的时区。在搜索发生在异常时间（例如夜间）的事件时，时区信息可能很有用。

选择这种类型的增强功能时，必须从“**时区**”下拉列表中选择所需的时区。

> 确保在增强功能服务的托管服务器上，已设置所需的时区。例如，您可以使用 `timedatectl list-timezones` 命令，该命令显示服务器上设置的所有时区。有关设置时区的更多详细信息，请参阅您的操作系统文档。

对事件进行增强后，所选时区相对于世界协调时 (UTC) 的时间偏移量会以 `+-hh:mm` 格式写入 DeviceTimeZone 事件字段。例如，如果您选择 **Asia/Yekaterinburg** 时区，则值 `+05:00` 将被写入 DeviceTimeZone 字段。如果经过增强的事件在 DeviceTimeZone 字段中已经存在值，则该值将被覆盖。

默认情况下，如果未在正在处理的事件中指定时区，并且未配置按时区增强规则，则将为事件分配处理事件的服务（收集器或关联器）所在服务器的时区。如果服务器时间被更改，则必须重启服务。

丰富 DeviceTimeZone 字段时允许的时间格式

在收集器中处理传入的原始事件时，以下时间格式可以自动转换为 +-hh:mm 格式：

已处理事件中的时间格式	示例
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

如果 `DeviceTimeZone` 字段中的日期格式与上述所列格式不同，那么在使用时区信息对事件进行增强时，收集器服务器的时区将会被写入该字段。您可以为非标准时间格式创建自定义规范化规则。

4. 使用 “**Debug**”下拉列表指示是否启用服务操作日志记录。日志记录默认被禁用。

5. 在“**过滤器**”部分，您可以指定条件来识别将通过增强规则来处理的事件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。

   在资源中创建过滤器

   KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

   要创建过滤器：

   1. 在“**过滤器**”下拉列表中，选择“**新建**”。
   2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
   3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
   4. 在**“条件”**下，指定事件必须满足的条件：
      a. 单击“**添加条件**”按钮。
      b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。

c. 在“**运算符**”下拉列表中，选择一个运算符。

过滤器运算符

- **=** — 左操作数等于右操作数。
- **<** — 左操作数小于右操作数。
- **<=** — 左操作数小于或等于右操作数。
- **>** — 左操作数大于右操作数。
- **>=** — 左操作数大于或等于右操作数。
- **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
- **contains** — 左操作数包含右操作数的值。
- **startsWith** — 左操作数以右操作数的某个值开头。
- **endsWith** — 左操作数以右操作数的某个值结尾。
- **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。

6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

新的扩充规则已添加到关联器的资源集中。

继续执行安装向导的下一步。

步骤 5：响应

这是安装向导的可选步骤。在安装向导的**响应**选项卡上，您可以选择或创建响应规则，并指示在触发关联规则时必须执行的操作。可以指定多个响应规则。您可以通过单击“**添加**”按钮进行添加，也可以通过单击 × 按钮进行删除。

要将现有响应规则添加到资源集：

1. 单击“**添加**”。

   响应规则设置窗口将打开。

2. 在“**响应规则**”下拉列表中，选择相关资源。

响应规则将添加到关联器的资源集中。

要在资源集中创建新的响应规则：

1. 单击“**添加**”。

   响应规则设置窗口将打开。

2. 在“**响应规则**”下拉列表中，选择“**新建**”。

3. 在“**类型**”下拉列表中，选择响应规则的类型并定义其相应的设置：

   - **KSC 响应** — 用于自动启动 Kaspersky Security Center 资产上的任务的响应规则。例如，您可以配置病毒扫描或数据库更新的自动启动。

     在 OSMP 与 Kaspersky Security Center 集成后，任务会自动启动。该任务仅针对从 Kaspersky Security Center 导入的资产运行。

     响应设置

     - **Kaspersky Security Center 任务**（必填）— 启动的 Open Single Management Platform 任务的名称。任务必须提前创建，并且其名称必须以“`KUMA `”开头。例如，“`KUMA antivirus check`”。

       可使用 KUMA 启动的 Open Single Management Platform 任务类型：

       - 更新
       - 病毒扫描

- **事件字段**（必填）— 定义必须为其启动 Open Single Management Platform 任务的资产的事件字段。可能值：
  - SourceAssetID
  - DestinationAssetID
  - 设备资产 ID

  要向 Open Single Management Platform 发送请求，必须确保能够通过 UDP 访问 Open Single Management Platform。

- **运行脚本** — 自动运行脚本的响应规则。例如，您可以创建一个脚本，其中包含在检测到选定事件时在 OSMP 服务器上执行的命令。

  脚本文件存储在安装了使用响应资源的关联器服务的服务器上：/opt/kaspersky/kuma/correlator/<关联器 ID>/scripts。

  此服务器的 `kuma` 用户需要运行该脚本的权限。

  响应设置

  - **超时** — 系统在运行脚本之前等待的秒数。
  - **脚本名称**（必填）— 脚本文件的名称。

    如果脚本响应资源已链接到关联器服务，但 /opt/kaspersky/kuma/correlator/<Correlator ID>/scripts 目录中没有脚本文件，则该服务将无法启动。
  - **脚本参数** — 必须传递给脚本的参数或事件字段值。

    如果脚本包含对文件采取的操作，则应指定这些文件的绝对路径。

    参数可以用引号 (") 括起书写。

    事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是其值必须传递给脚本的事件字段的名称。

    示例：`-n "\"usr\": {{.SourceUserName}}"`

- **KEDR 响应** — 用于自动创建防护规则、启动网络隔离或在 Kaspersky Endpoint Detection and Response 和 Kaspersky Security Center 资产上启动应用程序的响应规则。

  在 OSMP 与 Kaspersky Endpoint Detection and Response 集成后，将执行自动响应操作。

  响应设置

  - **事件字段**（必填）— 包含需要执行响应操作的资产的事件字段。可能值：
    - SourceAssetID
    - DestinationAssetID
    - 设备资产 ID
  - **任务类型** — 收到与过滤器匹配的数据时要执行的响应操作。可用的响应操作类型如下：
    - 启用网络隔离。

选择此类型的响应时，您需要定义以下设置的值：

- **隔离超时** — 资产的网络隔离处于活动状态的小时数。您可以设置 1 到 9,999 小时之间的数值。
  如有必要，您可以**添加网络隔离排除项**。

  要添加网络隔离排除项：

  a. 单击“**添加排除项**”按钮。

  b. 选择不得阻止的网络流量方向：

  - 入站。
  - 出站。
  - 入站/出站。

  c. 在“**资产 IP**”字段中，输入不得阻止其网络流量的资产的 IP 地址。

  d. 如果选择了“**入站**”或“**出站**”，请在“**远程端口**”和“**本地端口**”字段中指定连接端口。

  e. 如果要添加多个排除项，请单击“**添加排除项**”，然后重复相关步骤填写“**流量方向**”、“**资产 IP**”、“**远程端口**”和“**本地端口**”字段。

  f. 如果要删除某个排除项，请单击相关排除项下方的“**删除**”按钮。

  在向网络隔离规则添加排除项时，Kaspersky Endpoint Detection and Response 可能会错误显示规则详细信息中的端口值。这不会影响应用程序性能。有关查看网络隔离规则的更多详细信息，请参阅 *Kaspersky Anti Targeted Attack Platform 帮助指南*。

- 禁用网络隔离。
- 添加预防规则。
  选择此类型的响应时，您需要定义以下设置的值：

  - **要从中提取哈希值的事件字段** — KUMA 从中提取 SHA256 或 MD5 哈希值的事件字段，所对应的文件必须被阻止启动。

    所选事件字段和在**事件字段**中选定的值必须添加到关联规则的继承字段中。

  - **文件哈希 #1** — 要阻止的文件的 SHA256 或 MD5 哈希值。

  必须至少填写上述字段之一。

- 删除预防规则。
- 启动应用程序

选择此类型的响应时，您需要定义以下设置的值：

- **文件路径** — 要启动的进程的文件路径。
- **命令行参数** — 要用来启动文件的参数。
- **工作目录** — 启动时文件所在的目录。

具有主管理员角色的用户触发响应规则时，“**运行程序**”任务将显示在程序 Web 界面的“**任务管理器**”部分。此任务的**计划任务**显示在任务表的“**已创建**”列中。您可以查看任务完成结果。

> 所有列出的操作都可以在安装了 Kaspersky Endpoint Agent for Windows 的资产上执行。在安装了 Kaspersky Endpoint Agent for Linux 的资产上，该程序仅可执行启动操作。

> 在软件层面，针对已安装 Kaspersky Endpoint Agent for Linux 的资产，创建防护规则和网络隔离规则的能力不受限制。KUMA 和 Kaspersky Endpoint Detection and Response 不提供任何有关这些规则应用失败的通知。

- **通过 KICS for Networks 响应** — 用于在 KICS for Networks 资产上自动启动任务的响应规则。例如，您可以在 KICS for Networks 中更改资产状态。

  在 OSMP 与 KICS for Networks 集成后，任务会自动启动。

  响应设置

  - **事件字段**（必填）— 包含需要执行响应操作的资产的事件字段。可能值：
    - SourceAssetID
    - DestinationAssetID
    - 设备资产 ID
  - **KICS for Networks 任务** — 收到与过滤器匹配的数据时要执行的响应操作。可用的响应操作类型如下：
    - **将资产状态更改为已授权**。
    - **将资产状态更改为未授权**。

    当触发响应规则时，KUMA 将向 KICS for Networks 发送 API 请求，以将指定设备的状态更改为“**已授权**”或“**未授权**”。

- **通过 Active Directory 响应** — 用于更改 Active Directory 用户权限的响应规则。例如，阻止用户。

  如果配置了与 Active Directory 的集成，则会启动任务。

  响应设置

  - **账户 ID 源** — 事件字段，Active Directory 账户 ID 值的来源。可能值：
    - SourceAccountID
    - DestinationAccountID

- **AD 命令** — 触发响应规则时应用于账户的命令。可能值：
  - 将账户添加到组
  - 从组中删除账户
  - 重置账户密码
  - 阻止账户(B)

- 在“**Workers**”字段中，指定服务可以同时运行的进程数。

  默认情况下，工作进程数与安装程序服务的服务器上的虚拟处理器数相同。

  该字段是可选的。

1. 在“**过滤器**”部分，您可以指定条件来识别将使用响应规则处理的事件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。

   在资源中创建过滤器

   KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

   要创建过滤器：

   1. 在“**过滤器**”下拉列表中，选择“**新建**”。
   2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
   3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
   4. 在**“条件”**下，指定事件必须满足的条件：
      a. 单击“**添加条件**”按钮。
      b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。
      c. 在“**运算符**”下拉列表中，选择一个运算符。

      过滤器运算符

      - **=** — 左操作数等于右操作数。
      - **<** — 左操作数小于右操作数。
      - **<=** — 左操作数小于或等于右操作数。
      - **>** — 左操作数大于右操作数。
      - **>=** — 左操作数大于或等于右操作数。
      - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。

- **contains** — 左操作数包含右操作数的值。
- **startsWith** — 左操作数以右操作数的某个值开头。
- **endsWith** — 左操作数以右操作数的某个值结尾。
- **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

新的响应规则已添加到关联器的资源集中。

继续执行安装向导的下一步。

步骤 6：路由

这是安装向导的可选步骤。在安装向导的“**路由**”选项卡上，您可以选择或创建目标位置，并使用设置指定关联器创建的事件的转发目标位置。来自关联器的事件通常会重定向到存储，以便保存这些事件并在之后需要时查看。可以根据需要将事件发送到其他位置。可以设置多个目标位置。

要将现有目标位置添加到关联器的资源集：

1. 在“**添加目标位置**”下拉列表中，选择要添加的目标位置资源类型：

   - 如果要配置将已处理的事件转发到存储，请选择“**存储**”。
   - 如果要配置将已处理的事件转发到关联器，请选择“**关联器**”。
   - 如果要将事件发送到其他位置，请选择“**其他**”。

     此类资源包括在程序早期版本中创建的关联器和存储服务。

   “**添加目标位置**”窗口将打开，您可以在其中指定事件转发的参数。

2. 在“**目位置标**”下拉列表中，选择所需目标位置。

   窗口名称将更改为“**编辑目标位置**”，并显示所选资源的设置。可以使用 按钮在新的浏览器标签页中打开资源进行编辑。

3. 单击“**保存**”按钮。

选定的目标位置将显示在“安装向导”选项卡上。要删除目标位置资源，可以先选中该目标位置资源，然后在打开的窗口中单击“**删除**”。

要向关联器的资源集添加新目标位置：

1. 在“**添加目标位置**”下拉列表中，选择要添加的目标位置资源类型：

   - 如果要配置将已处理的事件转发到存储，请选择“**存储**”。
   - 如果要配置将已处理的事件转发到关联器，请选择“**关联器**”。
   - 如果要将事件发送到其他位置，请选择“**其他**”。

     此类资源包括在程序早期版本中创建的关联器和存储服务。

   “**添加目标位置**”窗口将打开，您可以在其中指定事件转发的参数。

2. 在“**基本设置**”选项卡上指定设置：

   - 在“**目标位置**”下拉列表中，选择“**新建**”。
   - 在“**名称**”字段中，输入目标位置资源的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
   - 使用“**禁用**”切换按钮指定是否将事件发送到此目标位置。默认情况下，发送事件处于启用状态。

- 选择目标位置资源的“**类型**”：
  - 如果要配置将已处理的事件转发到存储，请选择“**存储**”。
  - 如果要配置将已处理的事件转发到关联器，请选择“**关联器**”。
  - 如果要配置将事件发送到其他位置，请选择 **nats-jetstream**、**tcp**、**http**、**kafka** 或 **file**。
- 以 hostname:<API port> 格式指定接收事件的目标 **URL**。

  您可以通过单击除 **nats-jetstream** 和 **file** 之外的所有类型的 **URL** 按钮来指定多个目标地址。
- 对于 **nats-jetstream** 和 **kafka** 类型，使用“**Topic**”字段指定数据写入的目标主题。主题必须包含 Unicode 字符。Kafka 主题限制为 255 个字符。

3. 如有必要，请在“**高级设置**”选项卡上指定设置。可用的设置因所选目标位置资源类型而异：

- “**压缩**”是一个下拉列表，您可以在其中启用 Snappy 压缩。默认情况下，压缩处于**禁用**状态。
- “**代理**”是一个用于选择代理服务器的下拉列表。
- “**缓冲区大小**”字段用于设置目标位置的缓冲区大小（以字节为单位）。默认值为 1 MB，最大值为 64 MB。
- “**超时**”字段用于设置另一个服务或组件响应的超时时间（以秒为单位）。默认值为 `30`。
- “**磁盘缓冲区大小限制**”字段用于指定磁盘缓冲区的大小（以字节为单位）。默认大小为 10 GB。
- **集群 ID**是NATS集群的ID。
- “**TLS 模式**”是一个下拉列表，您可以在其中指定使用 TLS 加密的条件：
  - **禁用** （默认）—不使用 TLS 加密。
  - **启用** — 启用加密，但不进行验证。
  - **带验证** — 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。

  使用 TLS 时，无法将 IP 地址指定为 URL。
- “**URL 选择策略**”是一个下拉列表，您可以在其中选择一种方法来确定接收事件的目标 URL（如指定了多个 URL 的话）：
  - **任何**。只要此 URL 可以接收事件，就会将事件发送到其中一个可用的 URL。如果连接断开（例如，接收节点断开连接），将选择其他 URL 作为事件目标位置。
  - **第一个优先**。事件将发送到所添加地址列表中的第一个 URL。如果该 URL 不可用，则事件将按顺序发送到下一个可用节点。当第一个 URL 再次可用时，将再次开始向其发送事件。
  - **均衡**意味着包含事件的包会在列表中所有可用的 URL 之间进行平均分配。由于数据包是在目标位置缓冲区溢出或刷新计时器触发时发送的，因此该 URL 选择策略无法保证事件均匀分布到目标位置。
- **分隔符**用于指定分隔事件的字符。默认情况下，使用 `\n`。
- **Path** — 如果选择了**文件**目标位置类型，则该字段应填写文件路径。

- **缓冲区刷新间隔** — 此字段用于设置数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `100`。
- **Workers** — 此字段用于设置处理队列的服务数量。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
- 您可以使用“**健康检查路径**”和“**健康检查超时**”字段来设置健康检查。您也可以通过选中“**健康检查已禁用**”复选框来禁用健康检查。
- **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。
- “**磁盘缓冲区已禁用**”下拉列表用于启用或禁用磁盘缓冲区的使用。默认情况下，禁用磁盘缓冲区。
- 在“**过滤器**”部分，您可以指定条件来定义将由此资源处理的事件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。

  在资源中创建过滤器

  KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

  要创建过滤器：

  1. 在“**过滤器**”下拉列表中，选择“**新建**”。
  2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
  3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
  4. 在**“条件”**下，指定事件必须满足的条件：
     a. 单击“**添加条件**”按钮。
     b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。
     c. 在“**运算符**”下拉列表中，选择一个运算符。

     过滤器运算符

     - **=** — 左操作数等于右操作数。
     - **<** — 左操作数小于右操作数。
     - **<=** — 左操作数小于或等于右操作数。
     - **>** — 左操作数大于右操作数。
     - **>=** — 左操作数大于或等于右操作数。
     - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
     - **contains** — 左操作数包含右操作数的值。

- **startsWith** — 左操作数以右操作数的某个值开头。
- **endsWith** — 左操作数以右操作数的某个值结尾。
- **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

4. 单击“**保存**”按钮。

创建的目标位置显示在“安装向导”选项卡上。要删除目的地资源，可以先选中该目的地资源，然后在打开的窗口中单击“**删除**”。

继续执行安装向导的下一步。

步骤 7：设置验证

这是安装向导必须完成的最后一步。在此步骤中，OSMP 创建服务资源集，并根据此集合自动创建服务：

- 关联器的资源集显示在“**资源**” → “**关联器**”下。它可用于创建新的关联器服务。在此资源集发生变化时，基于此资源集运行的所有服务将在服务重启后开始使用新参数。为此，您可以单击“**保存并重启服务**”和“**保存并更新服务配置**”按钮。

  与其他资源一样，资源集可以修改、复制、从一个文件夹移动到另一个文件夹、删除、导入和导出。

- 服务显示在“**资源**” → “**活动服务**”中。使用安装向导创建的服务在 OSMP 内部执行功能。要与网络基础设施的外部部分通信，您需要在承载这些外部服务的服务器和资产上安装类似外部服务。例如，应在用于处理事件的服务器上安装外部关联器服务，在部署了 ClickHouse 服务的服务器上安装外部存储服务，以及在必须接收和转发 Windows 事件的 Windows 资产上安装外部代理服务。

要完成安装向导：

1. 单击“**创建并保存服务**”。

   安装向导的“**设置验证**”选项卡将显示一个基于安装向导中选定资源集创建的服务表格。窗口下方显示了在目标服务器和资产上安装这些服务的外部等效项时必须使用的命令示例。

   例如：

   ```
   /opt/kaspersky/kuma/kuma correlator --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。
   - <port> 是用于与 KUMA Core 通信的端口。
   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

     为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。

   - <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
   - <API port> 是用于与已安装组件通信的端口。

   “kuma”文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/ 目录中。

用于与 KUMA Core 通信的端口、服务 ID、KUMA Core CA 证书的指纹 ID 以及用于与服务通信的端口都会自动添加到命令中。还必须确保 OSMP 的网络连接正常，并在必要时打开其组件使用的端口。

2. 单击“**保存**”以关闭向导。

已在 OSMP 中创建关联器服务。现在，必须在用于处理事件的服务器上安装等效服务。

在 OSMP 网络基础设施中安装关联器

关联器由两部分组成：一部分在 OSMP 内创建，另一部分安装在用于处理事件的网络基础设施服务器上。关联器的第二部分安装在网络基础设施中。

要安装关联器：

1. 登录到要安装该服务的服务器。
2. 创建 /opt/kaspersky/kuma/ 文件夹。
3. 将“kuma”文件复制到 /opt/kaspersky/kuma/ 文件夹。该文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/ 文件夹中。

   请确保 kuma 文件具有足够的运行权限。

4. 执行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。
   - <port> 是 KUMA Core 用于内部通讯的端口（默认使用端口 7210）。
   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书的指纹 ID。

     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

     为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
   - <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
   - <API port> 是用于与已安装组件通信的端口。

   例如：

   ```
   sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX --api.port YYYY --install
   ```

您可以在安装向导的最后一步复制关联器安装命令。它会自动指定 KUMA Core 服务器的地址和端口、待安装关联器的标识符以及关联器用于通信的端口。安装程序前，请确保 KUMA 组件的网络连接。

在同一主机上部署多个 KUMA 服务时，安装过程中必须使用 `--api.port <port>` 参数为每个组件指定唯一端口。默认使用以下设置值：`--api.port 7221`。

关联器已安装。您可以使用它来分析事件中的威胁。

验证关联器安装

要验证关联器是否已准备好接收事件：

1. 在 OSMP 中，前往**资源和服务** → **活动服务**部分。
2. 确保您安装的关联器处于绿色状态。

如果传入关联器的事件中包含符合关联规则筛选条件的事件，则事件选项卡将显示这些事件，并带有 `DeviceVendor=Kaspersky` 和 `DeviceProduct=KUMA` 参数。所触发的关联规则的名称将显示为这些关联事件的名称。

如果没有找到关联事件

您可以创建一个更简单的关联规则版本来查找可能的错误。使用**简单的**关联规则并执行单个**输出**操作。建议创建一个过滤器来查找 OSMP 定期接收的事件。

在更新、添加或删除关联规则时，必须更新关联器的配置。

完成关联规则测试后，必须从 OSMP 中删除所有测试和临时关联规则，并更新关联器的配置。

创建 correlator-ng 关联器

correlator-ng 关联器是一个 OSMP 组件，用于关联和处理来自各种来源的事件。它允许使用关联规则、选择器和表达式来过滤、合并和分析事件。

当前版本的Kaspersky Next XDR Expert包含correlator-ng的测试版，仅供测试使用。在correlator API的正式版发布之前，其方法、算法、条件语法以及其他功能和特性可能会有所更改。

在当前版本中，关联器只能使用YAML配置进行管理。从 KUMA Core 获取初始配置后，您可以在文件中进一步更改设置；无法使用 OSMP Web 界面管理此关联器。

Correlator-ng并非标准模式的关联器的直接替代品。

其主要区别在于：

- 规则和选择器的新语法，与类似SQL的表达式和函数兼容。
- 支持连接选择器：来自不同选择器的事件将按接收顺序并行比较。
- 如果至少有一个选择器达到其阈值，则可以使用`anyMatch`属性触发关联规则。
- 扩展函数集，用于处理数据类型、数组、字符串、时间戳和CyberTrace字段。
- 更严格的表达式类型要求，以及将字段和变量值自动转换为所需类型，以确保正确处理操作。
- 正则表达式语法已更改：correlator-ng使用类似PCRE的语法，而标准关联器模型使用RE2。

correlator-ng的局限性

目前correlator-ng的使用存在一些局限性：

- 关联器无法根据传入事件自动对资产进行分类，也不支持触发响应规则时通常执行的操作。
- 关联器不能使用来自外部来源的额外数据自动增强事件，例如DNS查询、计算和检查脚本或CyberTrace系统。
- **存储**、**关联器**和**内部**类型的目标位置仅在没有磁盘缓冲区时才受支持。
- `S.KL_EventRoute`字段未添加到关联事件中。
- 关联器无法使用以下附加字段丰富关联事件：`SourceAssetKSCInstanceID`、`SourceAssetKSCHostID`、`DestinationAssetKSCInstanceID`、`DestinationAssetKSCHostID`、`DeviceAssetKSCInstanceID`、`DeviceAssetKSCHostIDKSC`、`S.KL_SourceAccountDisplayName`、`S.KL_DestinationAccountDisplayName`。
- 仅支持部分模板：某些模板可能无法处理，在某些情况下，`to_string`类型的函数可能无法运行。
- 可用的指标数量有限。
- `debug`参数不会更改日志记录级别。
- 存储桶内容只能以JSON格式导出。不支持导入和搜索存储桶内容。
- 不支持收集和分析关联统计信息以进行性能优化。
- 正则表达式不支持诸如`(?=...)`和`(?<=...)`之类的结构。
- 指向活动列表、上下文表、字典和资产类别的链接必须使用唯一的ID而不是名称。

配置关联器correlator-ng

当前版本的Kaspersky Next XDR Expert包含correlator-ng的测试版，仅供测试使用。在correlator API的正式版发布之前，其方法、算法、条件语法以及其他功能和特性可能会有所更改。

Correlator-ng作为独立的KUMA服务部署。其设置由YAML配置文件和进程的命令行选项定义。启动后，该服务与KUMA Core建立连接，接收规则和存储桶的配置，并开始处理事件。

可以使用一组YAML文件来管理correlator-ng。每个文件如下所述。

Correlator-ng配置文件

文件	描述
config.yaml	包含有关服务的基本信息，包括关联器的名称、描述和常规设置。
correlation-rules.yaml	包含关联规则的配置，包括规则类型：标准规则、简单规则、操作规则和定期规则。
selector-includes.yaml	包含链接到关联规则以实现重复使用的嵌套过滤器。
active-lists.yaml	包含活动列表的配置。
context-tables.yaml	包含上下文表的配置。
dictionaries.yaml	包含用于选择器和关联规则的静态字典。
global-variables.yaml	包含关联规则和选择器中可用的全局变量。
destinations.yaml	包含事件目标（`storage`、`correlator`、`internal`）及其 ID 和发送设置。

文件在关联器启动时按以下顺序加载：首先是config.yaml，然后是带有规则和选择器的文件，然后是带有活动列表、上下文表、字典和全局变量的文件。目标文件最后加载，以确保事件路由正确。

systemd-unit和关联器的启动

systemd-unit文件用于将关联器作为系统服务启动；该文件定义了correlator-ng的启动、停止和重启设置。

配置文件示例：

```
[Unit]
Description=KUMA Correlator NG
StartLimitIntervalSec=1
After=network.target
[Service]
Type=simple
Restart=always
RestartPreventExitStatus=99
TimeoutSec=0
RestartSec=5
Environment="RUST_BACKTRACE=full"
User=kuma
Group=kuma
ExecStart=/opt/kuma correlator --id <correlator_service_ID> --core https://<FQDN_of_KUMA_Core>:7210 --wd
/opt/correlator-ng --api.port <correlator 的 API 端口>
LimitFSIZE=infinity
LimitCPU=infinity
LimitAS=infinity
LimitNOFILE=500000
LimitNPROC=64000
LimitMEMLOCK=infinity
TasksMax=infinity
TasksAccounting=false
[Install]
WantedBy=multi-user.target
```

correlator-ng日志记录

`--logger.filter`选项设置correlator-ng的日志记录级别。在此选项中，您可以指定与标准`RUST_LOG`变量相同的日志记录级别：`trace`、`debug`、`info`、`warn`、`error`。

例如：

```
--logger.filter debug
```

您还可以使用`RUST_BACKTRACE`环境变量。将其设置为`full`可启用扩展错误信息的输出。

correlator-ng 支持的数据类型

当前版本的Kaspersky Next XDR Expert包含correlator-ng的测试版，仅供测试使用。在correlator API的正式版发布之前，其方法、算法、条件语法以及其他功能和特性可能会有所更改。

与标准版本的关联器相比，correlator-ng具有更严格的数据模型。这会影响关联规则、选择器和事件处理函数。事件、变量或选择器的每个字段现在都有定义的类型。自动类型转换仅用于兼容的类型；在其他情况下，必须使用`to_string`、`to_integer`和`to_float`转换函数。

支持以下数据类型：

支持的数据类型

数据类型	描述
字符串	字符串
VecString	字符串数组
I64	64位整数
VecI64	64位整数数组
F64	浮点数
VecF64	浮点数数组
时间戳	UNIX时间戳（以毫秒为单位）
VecTimestamp	UNIX时间戳数组（以毫秒为单位）
Uuid	UUIDv4格式的唯一ID
VecUuid	UUIDv4值数组
Ip	IPv4 或 IPv6 地址
VecIp	IP地址数组
IpNet	带有 CIDR 前缀的子网，例如 `192.168.1.0/24`。
VecIpNet	子网数组
布尔值	布尔值（`true` 或 `false`）
VecBool	布尔值数组。

更强的类型控制提高了关联器的效率，并减少了编译关联规则时的错误。但是，现在所有对数组、字符串和时间戳的操作都必须考虑数据类型，否则可能会发生运行时错误。

关联规则选择器和表达式

当前版本的Kaspersky Next XDR Expert包含correlator-ng的测试版，仅供测试使用。在correlator API的正式版发布之前，其方法、算法、条件语法以及其他功能和特性可能会有所更改。

在 correlator-ng 中，选择器可以执行变量可以执行的所有操作，并且可以使用用于处理字符串、数组和数字的函数（例如，`substring`、`tr`、`to_lower`）。使用函数无需创建单独的变量；选择器本身就可以使用这些函数。

选择器使用适用于 `WHERE` 子句的 SQL 语法进行描述。

使用表达式配置选择器和变量，以过滤和合并事件。它们支持与变量相同的操作，并能够构建复杂的条件。以下表达式类型可供使用。

> 编写涉及常量的值比较表达式时，常量必须放在右边。这可让关联器应用各种优化。如果常数位于左侧，则不进行优化。

常量

常量

常量	类型
`1`	I64（整数）
`3.14`	F64（浮点数）
`'myString'`	字符串

参考值

参考值

参考	Description
`DeviceVendor`	`DeviceVendor` 事件字段的值
`S.MyCustomField`	`S.MyCustomField` 复合字段的值
`$myVariable`	`myVariable` 变量的值

逻辑运算符和分组运算符

逻辑运算符和分组运算符

表达式	Description
`<expression> AND <expression>`	逻辑AND运算符
`<expression> OR <expression>`	逻辑OR运算符
`NOT <expression>`	表达式结果的否定
`IS [NOT] NULL`	检查是否缺少值（在correlator-ng中，未设置的值为`NULL`）
`()`	分组表达式

比较运算符

比较运算符

表达式	Description
`<expression> = <expression>`	检查值是否相等
`<expression> > <expression>`	使用`>`运算符比较值
`<expression> >= <expression>`	使用`>=`运算符比较值
`<expression> < <expression>`	使用`<`运算符比较值

表达式	Description
`<expression> <= <expression>`	使用<=运算符比较值
`Type BETWEEN 1 AND 3`	检查Type字段的值是否介于1到3之间（含1和3）

算术运算符

算术运算符

表达式	Description
`<expression> + <expression>`	附加
`<expression> - <expression>`	减法
`<expression> * <expression>`	乘法
`<expression> / <expression>`	除法
`<expression> % <expression>`	模除

功能

功能

函数	Description
`eq_fold (<left operand expression>, <right operand expression>)`	调用 `eq_fold` 函数。

有关可用函数的详细信息，请参阅correlator-ng中的"数据处理函数"部分。

标准关联规则的属性

当前版本的Kaspersky Next XDR Expert包含correlator-ng的测试版，仅供测试使用。在correlator API的正式版发布之前，其方法、算法、条件语法以及其他功能和特性可能会有所更改。

correlator-ng中的**标准**关联规则支持附加属性，允许修改完全匹配的条件并指定选择器之间事件的匹配。这些属性扩展了关联规则桶的标准操作模型，并应用于分析已经放置在存储桶中的事件的阶段。

目前correlator-ng的使用支持两个属性：

- `anyMatch`
- `joinSelector`

这两个属性仅适用于**标准**类型的关联规则，并且直接用于规则本身的配置中。

anyMatch属性

在关联器的标准模型中，当存储桶达到完全匹配状态时，即所有选择器累积的事件数都等于其阈值时，关联规则被认为已满足。

如果在关联规则的配置中指定了 `anyMatch: true`，当规则的任一选择器（**恢复**类型的选择器除外）达到其阈值时，存储桶将达到完全匹配状态。因此，规则由第一个满足的条件触发，无需等待其他选择器累积事件。每个选择器继续根据其配置独立累积事件，但是，一旦其中一个选择器达到其阈值，关联就会立即结束。

此类规则生成的关联事件还包含 `$KL_selectorName` 局部变量。该变量的值等于触发规则的阈值选择器的标签。这使得我们可以识别触发源，并对结果应用各种后续处理步骤。

> 包含 `anyMatch` 属性的规则不支持**超时时**类型的触发器。

JoinSelector属性

在关联器的标准模型中，当存储桶达到完全匹配状态时，即所有选择器累积的事件数都等于其阈值时，关联规则被认为已满足。

如果在关联规则的配置中指定了 `anyMatch: true`，当规则的任一选择器（**恢复**类型的选择器除外）达到其阈值时，存储桶将达到完全匹配状态。因此，规则由第一个满足的条件触发，无需等待其他选择器累积事件。每个选择器继续根据其配置独立累积事件，但是，一旦其中一个选择器达到其阈值，关联就会立即结束。

此类规则生成的关联事件还包含 `$KL_selectorName` 局部变量。该变量的值等于触发规则的阈值选择器的标签。这使得我们可以识别触发源，并对结果应用各种后续处理步骤。

> 包含 `anyMatch` 属性的规则不支持**超时时**类型的触发器。

JoinSelector属性

`joinSelector` 属性允许在达到完全匹配状态之前，额外检查同一存储桶中不同选择器累积的事件的关联性。

属性值是一个类似 SQL 的表达式，`joinSelector: <表达式>`

该表达式指定了比较不同选择器事件的条件。它必须是一个二元运算或函数，其操作数仅接受常量和 `with_selector('<选择器标签>', <表达式>)` 形式的表达式。

`with_selector` 函数表示该表达式是根据特定选择器的事件进行评估的。

解析配置时，关联器会自动确定参与表达式的所有选择器中该选择器的最小阈值。仅对等于此最小值的事件数量进行比较。

例如：

选择器A的选择器阈值（事件数量）为5，而选择器B为9。在表达式 `with_selector('A', DeviceHostName) = with_selector('B', DeviceHostName)` 中，仅比较每个选择器的前五个事件。

事件按到达顺序并行比较：选择器A的第一个事件与选择器B的第一个事件进行比较；第二个事件与第二个事件进行比较，依此类推。

`joinSelector` 属性也可以使用函数。例如：`joinSelector: contains_fold(with_selector('A', $var_A), with_selector('B', DeviceCustomString1))`

本示例使用 `contains_fold` 函数，该函数用于检查为选择器 A 计算的 `$var_A` 关联器变量的值是否存在于选择器 B 事件的 `DeviceCustomString1` 字段中，不区分大小写。

以下函数在 `joinSelector` 属性的表达式中不受支持：

- `has_ti_detect`
- `has_ti_detect_with_category`
- `has_ti_detect_with_indicator`
- `has_ti_detect_with_category_and_indicator`

correlator-ng中的数据函数

当前版本的Kaspersky Next XDR Expert包含correlator-ng的测试版，仅供测试使用。在correlator API的正式版发布之前，其方法、算法、条件语法以及其他功能和特性可能会有所更改。

correlator-ng中的函数用于选择器和变量中，以处理事件数据、类型转换和过滤。

通用语法：

- 必需参数包含在`< >`中，可选参数包含在`[ ]`中。
- 三个点`...`表示不确定数量的参数。
- 返回类型由`-> <data type>`表示。字母`T`表示类型取决于参数的类型。
- 参数的类型可以是具体类型（例如，`String`、`I64`），也可以是`T`，后者代表任何可用的数据类型。

类型转换函数

这些函数将值转换为特定类型。

类型转换函数

函数	Description
`to_string(< 表达式 >)`	将值转换为字符串。
`to_integer(< 表达式 >)`	将值转换为整数（I64）。
`to_float(< 表达式 >)`	将值转换为浮点数（F64）。
`to_uuid(< 表达式 >)`	将值转换为UUIDv4。
`to_ip(< 表达式 >)`	将值转换为IPv4或IPv6地址。
`to_ip_net(< 表达式 >)`	将值转换为IPNet子网。
`to_bool(< 表达式 >)`	将值转换为布尔值。
`to_timestamp(< 表达式 >, '[ 时区 ]')`	将值转换为时间戳，并可选择是否包含时区。

用于比较值的函数

用于比较值的函数

函数	Description
eq_fold(< 左操作数 >, < 右操作数 >) -> Bool	检查左侧值是否与右侧值相同，忽略大小写。
eq_any(< 左操作数 >, < 右操作数 1>, [...]) -> Bool	检查右侧的值是否与左侧的值相同。
eq_any_fold(< 左操作数 >, < 右操作数 >, [...]) -> Bool	将左侧值与多个右侧值进行比较，忽略大小写。
contains(< 左操作数 >, < 右操作数 >) -> Bool	检查左侧值是否包含右侧值。
contains_fold(< 左操作数 >, < 右操作数 >) -> Bool	检查左侧值是否包含右侧值，忽略大小写。
contains_any(< 左操作数 >, < 右操作数 1>, [...]) -> Bool	检查左侧值是否包含右侧的任何值。
contains_any_fold(< 左操作数 >, < 右操作数 >, [...]) -> Bool	检查左侧值是否包含右侧值中的任何值，忽略大小写。
starts_with(< 左操作数 >, < 右操作数 >) -> Bool	检查右侧值是否为左侧值的前缀。
starts_with_fold(< 左操作数 >, < 右操作数 >) -> Bool	检查前缀，不区分大小写。
starts_with_any(< 左操作数 >, < 右操作数 1>, [...]) -> Bool	检查右侧值之一是否是左侧值的前缀。
starts_with_any_fold(< 左操作数 >, < 右操作数 1>, [...]) -> Bool	检查右侧值之一的前缀，不区分大小写。
ends_with(< 左操作数 >, < 右操作数 >) -> Bool	检查右侧值是否是左侧值的后缀。
ends_with_fold(< 左操作数 >, < 右操作数 >) -> Bool	检查后缀，不区分大小写。
ends_with_any(< 左操作数 >, < 右操作数 1>, [...]) -> Bool	检查右侧值之一是否是左侧值的后缀。
ends_with_any_fold(< 左操作数 >, < 右操作数 1>, [...]) -> Bool	检查后缀，不区分大小写。
match(< 左操作数 >, < 右操作数 >) -> Bool	检查左侧值是否与右侧的正则表达式匹配。
match_any(< 左操作数 >, '< 右操作数 1>', '[右操作数 2]', [...]) -> Bool	检查左侧值是否与右侧的某个正则表达式匹配。

用于处理活动列表、字典和上下文表的函数

用于处理活动列表、字典和上下文表的函数

函数	Description
in_active_list('< 活动列表 ID >', < 密钥元素 1>, [...]) -> Bool	按键检查活动列表中是否存在某个值。
in_context_table('< 上下文表 ID >', '< 密钥字段名称 1>', < 密钥字段值 1>, '[密钥字段名称 2]', [密钥字段值 2], [...]) -> Bool	按键检查上下文表中是否存在某个值。
in_dictionary('< 字典 ID >', < 密钥元素 1>, [密钥元素 2], ...) -> Bool	按键检查字典中是否存在某个值。
dict('< 字典 ID >', < 密钥 1>, [...]) -> String	按密钥从字典中传回一个值。
table_dict('< 字典 ID >', < 列名称 >, < 密钥 1>, [...]) -> String	从表格字典中传回一个值。
active_list('< 活动列表 ID >', < 字段名称 >, < 密钥 1>, [...]) -> String	从活动列表中传回一个值。
context_table('< 上下文表 ID >', '< 字段名称 >', '< 密钥字段 >', < 值 >) -> T	从上下文表中传回一个字段的值。
context_table_list_item('< 上下文表 ID >', '< 字段名称 >', < 索引 >, ...) -> T	从上下文表中传回数组元素。
match_active_list(...)	如果密钥与正则表达式匹配，则从活动列表中传回一个值。
match_context_table(...)	如果正则表达式匹配成功，则从上下文表中传回一个值。
match_dictionary(...)	如果正则表达式匹配成功，则传回字典中的一个值。

子网功能

子网功能

函数	Description
in_subnet(< left_operand >, < subnet >) -> Bool	检查IP地址是否属于某个子网。
in_subnet_any(< left_operand >, < subnet 1>, [...]) -> Bool	检查IP地址是否属于某个子网。
in_subnet_active_list(...)	检查IP地址是否属于活动列表中的子网。
in_subnet_context_table(...)	检查IP地址是否属于上下文表中的子网。
in_subnet_dictionary(...)	检查IP地址是否属于字典中的子网。

字符串函数

字符串函数

函数	Description
to_lower(< 操作数 >) -> String	将字符串转换为小写。
to_upper(< 操作数 >) -> String	将字符串转换为大写。
substring(< 字符串 >, < 子字符串开头 >, [子字符串结尾]) -> String	传回一个子字符串。
index_of(< 查找内容 >, < 查找位置 >) -> I64	传回首次出现的位置。
last_index_of(< 查找内容 >, < 查找位置 >) -> I64	传回最后一次出现的位置。
tr(< 操作数 >) -> String	删除字符串开头和结尾的空白字符。
replace(< 字符串 >, < 子字符串 >, < 替换内容 >) -> String	替换子字符串。
regexp_replace(< 字符串 >, '< 正则表达式 >', '< 替换内容 >') -> String	使用正则表达式替换子字符串。
regexp_capture(< 字符串 >, '< 正则表达式 >') -> String	获取与正则表达式匹配的子字符串。
str_join('< 分隔符 >', < 字符串 1>, [...]) -> String	连接多个字符串。

数组函数

数组函数

函数	Description
append(< 左操作数 >, < 右操作数 >, '[分隔符]') -> T	在数组或字符串末尾添加一个值。
prepend(< 左操作数 >, < 右操作数 >, '[分隔符]') -> T	在数组或字符串的开头添加一个值。
len(< 操作数 >) -> I64	返回字符串或数组的长度。
item(< 数组 >, < 索引 >) -> T	通过索引传回数组中的一个元素。
distinct_items(< 数组 >) -> T	从数组中删除重复的元素。
sort_items(< 数组 >, '< 排序顺序 >') -> T	对数组进行排序。

时间戳函数

时间戳函数

函数	Description
now() -> Timestamp	传回当前时间戳。
year(<timestamp>) -> I64	传回年份。
month(<timestamp>) -> I64	传回月份。
month_str(<timestamp>) -> String	以字符串形式传回月份。

函数	Description
`weekday(<timestamp>) -> I64`	传回星期几。
`weekday_str(<timestamp>) -> String`	以字符串形式传回星期几。
`day(<timestamp>) -> I64`	传回月份中的日期。
`hour(<timestamp>) -> I64`	传回小时数。
`minute(<timestamp>) -> I64`	传回分钟数。
`second(<timestamp>) -> I64`	传回秒数。
`millisecond(<timestamp>) -> I64`	传回毫秒数。
`format_timestamp(<timestamp>, '< 格式 >') -> String`	将时间戳转换为字符串。
`truncate_timestamp(<timestamp>, '< 持续时间 >') -> Timestamp`	将时间戳四舍五入为整数值。

时间函数

时间函数

函数	Description
`duration_days(<t1>, <t2>) -> I64`	传回天数差值。
`duration_hours(<t1>, <t2>) -> I64`	传回小时差值。
`duration_minutes(<t1>, <t2>) -> I64`	传回分钟差值。
`duration_seconds(<t1>, <t2>) -> I64`	传回秒数差值。
`duration_milliseconds(<t1>, <t2>) -> I64`	传回毫秒差值。

数学函数

数学函数

函数	Description
`round(< 操作数 >) -> I64`	将数值四舍五入到最接近的整数。
`ceil(< 操作数 >) -> I64`	向上取整。
`floor(< 操作数 >) -> I64`	向下取整。
`abs(< 操作数 >) -> T`	传回一个数的绝对值。
`pow(< 操作数 >, '< 幂 >') -> T`	将一个数提升到幂。
`math_min(< 数组 >) -> T`	传回数组的最小元素。
`math_max(< 数组 >) -> T`	传回数组的最大元素。
`math_avg(< 数组 >) -> F64`	计算数组的平均值。

数据解码和分析功能

数据解码和分析功能

函数	Description
`decode_hex_integer(< 字符串 >) -> I64`	将十六进制字符串转换为数字。
`decode_hex(< 字符串 >) -> String`	解码十六进制字符串。
`decode_base64(< 字符串 >) -> String`	解码Base64字符串。
`decode_url(< 字符串 >) -> String`	解码URL编码字符串。
`entropy(< 字符串 >) -> F64`	计算字符串的Shannon熵。

函数	Description
`has_bit(< 左操作数 >, < 位置 >) -> Bool`	检查比特是否设置在指定位置。
`has_vulnerability(< 资产 ID >, (<CVE>), [ 严重级别 ]) -> Bool`	检查资产是否存在漏洞。

其他函数

其他函数

函数	Description
`include('< 谓词 ID >', '[ 谓词名称 ]')`	使用selector-includes.yaml文件中的预定义谓词。
`ti('< 类别 >', < 指标 >, '< 字段 >')`	从专门的TI字段（CyberTrace）中检索值。
`with_selector(' 关联规则选择器标记 ', < 表达式 >)`	只能在关联规则的 `joinSelector` 属性中使用，以区分事件集。
`template('< 模板 >', [ 参数 1], [ 参数 2], ...) -> String`	根据模板生成字符串，方法是将事件字段或变量的值插入到模板中。
`conditional('< 谓词 >', <then>, <else>)`	根据谓词的结果，返回两个值中的一个
`has_ti_detect*()`	检查按类别或指标触发的CyberTrace。
`has_ti_detect_with_category('< 类别 >')`	检查按类别触发的CyberTrace。
`has_ti_detect_with_indicator(< 指标 >)`	检查按指标触发CyberTrace。
`has_ti_detect_with_category_and_indicator('< 类别 >', < 指标 >)`	检查按类别或指标触发的CyberTrace。

创建事件路由器

事件路由器是一种服务，可用于从收集器和关联器接收事件流，然后根据配置的过滤器将事件分发到指定的目的位置。

要将事件从收集器发送到事件路由器，您必须使用事件路由器的地址创建一个`eventRouter`目标资源，并将该资源链接到要将事件发送到事件路由器的收集器。

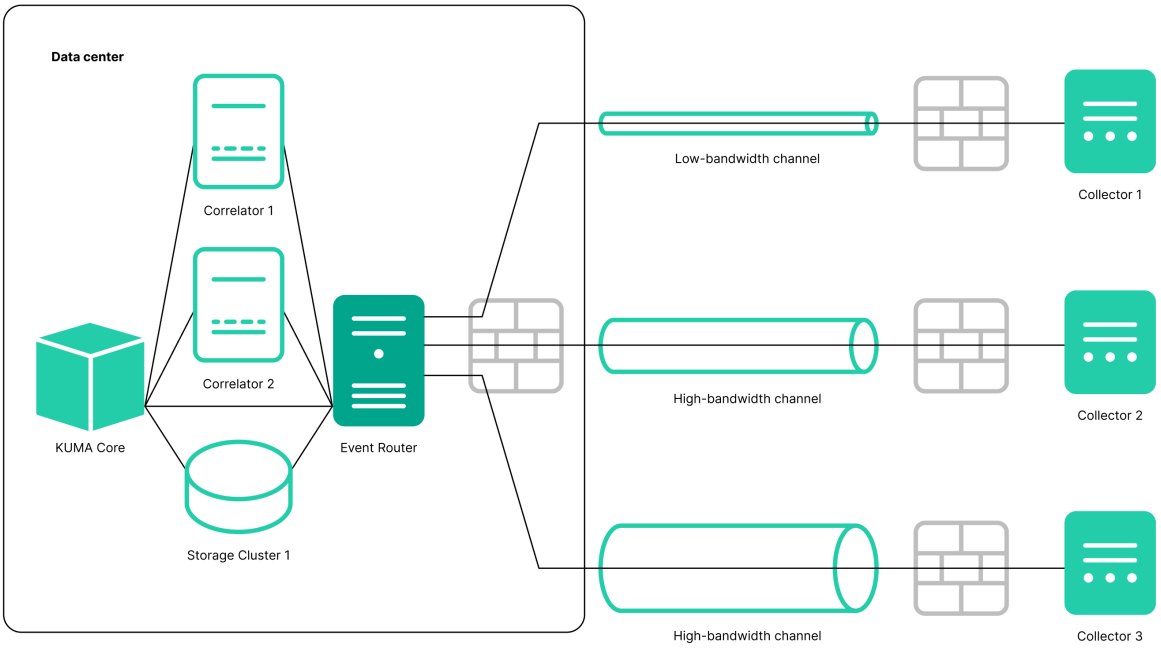
事件路由器在 API 端口上接收事件，与`storage`和`correlator`目标位置一样。

您可以在“**资源**”部分创建路由器。

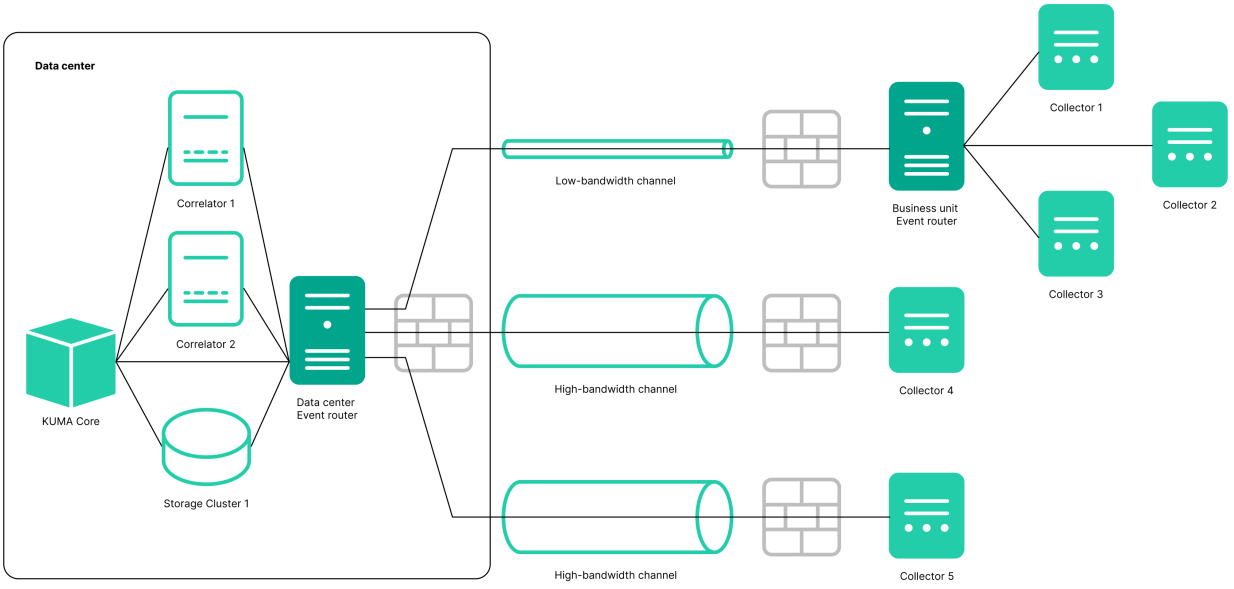
使用事件路由器可以减少链路的利用率，这对于低带宽和繁忙的链路尤为重要。

可能的用例：

收集器 – 数据中心的事件路由器



级联连接：多个收集器 – 分支机构的事件路由器；分支机构的事件路由器 – 数据中心的事件路由器



事件路由器必须安装在 Linux 设备上。只有具有主管理员角色的用户才能创建该服务。您可以在任何租户中创建服务；租户关系不施加任何限制。

您可以使用以下指标来获取有关服务性能的信息：

- IO
- 过程
- 操作系统

与其他资源一样，OSMP 中会为事件路由器生成以下审计事件：

- 资源已成功添加
- 资源已成功更新
- 资源已成功删除

安装事件路由器分为两个步骤：

1. 使用安装向导在 OSMP 中创建事件路由器服务。
2. 在服务器上安装事件路由器服务。

启动事件路由器安装向导

要启动事件路由器安装向导：

1. 在 OSMP 的主菜单中，在**资源和服务**区域，点击**事件路由器**。
2. 在打开的**事件路由器**窗口中，单击**添加**。

遵照向导的说明操作。

步骤 1：事件路由器的常规设置

这是安装向导的必需步骤。在此步骤中，您可以指定事件路由器的主要设置：其名称和将拥有它的租户。

要指定事件路由器的基本设置：

1. 在“**名称**”字段中，输入您正在创建的服务的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
2. 在“**租户**”下拉列表中，选择将拥有事件路由器的租户。归属于某一租户的事件路由器具有组织属性，且不施加任何限制。
3. 如有必要，请在“**处理程序**”字段中指定服务可以同时运行的进程数。默认情况下，处理程序的数量与安装服务的服务器上的 vCPU 数量相同。
4. 如有必要，请使用“**调试**”切换开关启用服务操作日志记录。
5. 您可以选择在“**描述**”字段中添加最多 4,000 个 Unicode 字符来描述服务。

事件路由器的基本设置已配置。继续执行安装向导的下一步。

步骤 2：路由

这是安装向导的必需步骤。建议将事件至少发送到两个目标位置：一个是发送到关联器进行分析，另一个是发送到存储进行存储。您还可以选择其他事件路由器作为目标位置。

要指定事件路由器将从收集器收到的事件发送到的目标位置的设置：

1. 在安装向导的“**路由**”步骤中，单击“**添加**”。
2. 这将打开**创建目标位置**窗口；在该窗口中，指定以下设置：
   a. 在**基本设置**选项卡上，在**名称**字段中，输入目标位置的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
   b. 您可以根据需要，使用“**状态**”切换开关来启用或禁用服务。
   c. 在“**类型**”下拉列表中，选择目标位置的类型。可用值如下：
      - nats-jetstream
      - TCP
      - http
      - kafka
      - 文件
      - 存储
      - 关联器
      - 事件路由器
   d. 在**高级设置**选项卡上，指定参数的值。可以配置的参数集取决于在**基本设置**选项卡上选择的目标位置类型。有关参数及其值的详细信息，请单击本说明“c”段中每种目标位置类型的链接。

创建的目标位置显示在“安装向导”选项卡上。要删除目标位置资源，可以先选中该目标位置资源，然后在打开的窗口中单击“**删除**”。

路由已配置完成。继续执行安装向导的下一步。

步骤 3：设置验证

这是安装向导必须完成的最后一步。

要在安装向导中创建事件路由器：

1. 单击**创建**并保存服务。
   窗口下部显示在服务器上安装事件路由器必须使用的命令。

命令示例：

```
/opt/kaspersky/kuma/kuma eventrouter --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core
CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 服务器的完全限定域名。
- <port> 是用于与 KUMA Core 通信的端口。
- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

  `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

  安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

  为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
- <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
- <API port> 是用于与已安装组件通信的端口。

与 KUMA Core 通信的端口、CA 证书指纹 ID、服务 ID 以及与服务通信的端口会自动添加到命令中。还必须确保 OSMP 的网络连接正常，并在必要时打开其组件使用的端口。

2. 单击“**保存**”以关闭向导。

该服务已安装在 OSMP 中。现在您可以继续在 OSMP 网络基础设施中安装该服务。

在服务器上安装事件路由器

要在服务器上安装事件路由器：

1. 登录要安装事件路由器服务的服务器。
2. 创建 /opt/kaspersky/kuma/ 文件夹。
3. 将“kuma”文件复制到 /opt/kaspersky/kuma/ 目录。该文件位于安装程序的 /kuma-ansible-installer/roles/kuma/files/ 目录中。
4. 请确保 kuma 文件具有足够的运行权限。如果该文件不可执行，请将其设置为可执行：

```
sudo chmod +x /opt/kaspersky/kuma/kuma
```

5. 将 /kuma-ansible-installer/roles/kuma/files/ 目录中的 LICENSE 文件放入 /opt/kaspersky/kuma/ 目录，然后运行以下命令接受最终用户授权许可协议的条款和条件：

```
sudo /opt/kaspersky/kuma/kuma license
```

6. 创建“kuma”用户：

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

7. 将“kuma”用户设置为 /opt/kaspersky/kuma 目录及其中所有文件的所有者：

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/
```

8. 将 OSMP 事件路由器端口添加到防火墙排除项。

> 为保证程序正常运行，请确保 OSMP 组件能够通过在安装 OSMP 组件期间指定的协议和端口与网络上的其他组件和程序交互。

9. 执行以下命令：

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 服务器的完全限定域名。
- <port> 是 KUMA Core 用于内部通讯的端口（默认使用端口 7210）。
- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书的指纹 ID。

  `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

  安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

  为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
- <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
- <API port> 是用于与已安装组件通信的端口。

例如：

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX --api.port YYYY --install
```

事件路由器将安装在服务器上。您可以使用它从收集器接收事件并将事件转发到指定的目标位置。

创建收集器

收集器由两部分组成：一部分在 OSMP 内创建，另一部分安装在用于接收事件的网络基础设施中的服务器上。

KUMA 控制台中的操作

使用安装向导在 OSMP 中创建收集器。此向导将必要的资源组合成收集器的资源集。完成向导后，系统将基于该资源集自动创建服务。

要在 OSMP 中创建收集器，

启动收集器安装向导：

- 在 OSMP 的主菜单中，在 **资源和服务** 区域，点击 **添加事件源**。
- 在 OSMP 的主菜单中，在“**资源和服务**” → “**收集器**”部分，单击“**添加收集器**”。

完成向导的步骤后，将在 OSMP 中创建一个收集器服务。

收集器的资源集包括以下资源：

- 连接器
- 规范化器（至少一个）
- 过滤器（如需要）
- 聚合规则（如需要）
- 富集规则（如需要）；
- 目标位置（通常定义两个，用于将事件发送到关联器和存储）

这些资源可以提前准备，也可以在安装向导运行时进行创建。

OSMP 收集器服务器上的操作

在计划用于接收事件的服务器上安装收集器时，请运行安装向导最后一步显示的命令。安装时，必须指定 OSMP 中自动分配给服务的 ID，以及用于通信的端口。

测试安装

创建收集器后，建议您确保其正常工作。

启动收集器安装向导

收集器由两部分组成：一部分在 OSMP 内创建，另一部分安装在用于接收事件的网络基础设施服务器上。安装向导将创建收集器的第一部分。

要启动收集器安装向导：

- 在 OSMP 的主菜单中，在 **资源和服务** 区域，点击 **添加事件源**。
- 在 OSMP 的主菜单中，在“**资源和服务**” → “**收集器**”部分，单击“**添加收集器**”。

遵照向导的说明操作。

除了向导的第一步和最后一步之外，向导的步骤可以按任意顺序执行。您可以使用**下一步**和**上一步**按钮，或单击窗口左侧的步骤名称，在各步骤之间切换。

向导完成后，将在 OSMP 的“**资源和服务**” → “**收集器**”下创建收集器资源集，并在“**资源和服务**” → “**活动服务**”下添加收集器服务。

步骤 1：连接事件源

这是安装向导的必需步骤。在此步骤中，您需要指定收集器的主要设置：名称及其所属的租户。

要指定收集器的基本设置：

1. 在“**收集器名称**”字段中，为您正在创建的服务输入一个唯一的名称。该名称必须包含 1 到 128 个 Unicode 字符。

   创建特定类型的收集器时，名为“代理：<收集器名称>，自动创建”的代理也会与这些收集器一起自动创建。如果此类代理之前已创建且尚未删除，则无法创建名为 <收集器名称> 的收集器。在这种情况下，您必须为收集器指定其他名称或删除之前创建的代理。

2. 在“**租户**”下拉列表中，选择您希望该收集器所属的租户。租户选择决定了创建收集器时可用的资源。

   如果您从安装向导的另一个后续步骤返回至此窗口并选择了另一个租户，则必须手动编辑已添加到服务的所有资源。只有选定租户和共享租户的资源能够添加到服务。

3. 如需要，请在“**工作节点**”字段中指定服务可并发运行的进程数量。默认情况下，工作进程数量与安装服务的服务器上的 vCPU 数量相同。

4. 如有必要，请使用“**调试**”下拉列表启用服务操作日志记录。

   即使禁用调试模式，收集器服务的错误消息也会被记录。可在安装收集器的计算机上的 /opt/kaspersky/kuma/collector/<collector ID>/log/collector 目录中查看日志。

5. 您可以选择在“**描述**”字段中添加最多 256 个 Unicode 字符来描述服务。

已指定收集器的主要设置。继续执行安装向导的下一步。

步骤 2：传输

这是安装向导的必需步骤。在安装向导的**传输方式**选项卡上，选择或创建一个连接器，并在其设置中指定收集器服务的事件来源。

要将现有连接器添加到资源集，

请从“**连接器**”下拉列表中选择所需连接器的名称。

安装向导的“**传输方式**”选项卡中显示了所选连接器的设置。您可以使用 按钮在新的浏览器选项卡中打开所选连接器进行编辑。

要创建新连接器：

1. 从“**连接器**”下拉列表中选择“**新建**”。
2. 在**类型**下拉列表中，选择连接器类型，然后在**基本设置**和**高级设置**选项卡上指定其设置。可用的设置取决于所选的连接器类型：

   - TCP
   - UDP
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - ftp
   - nfs
   - wmi
   - wec
   - SNMP

   在规范化阶段使用 tcp 或 udp 连接器类型时，如果 DeviceAddress 事件字段为空，则将从中接收事件的资产的 IP 地址将被写入该字段中。

   使用 **wmi** 或 **wec** 连接器时，将自动创建用于接收 Windows 事件的代理。

   建议使用默认编码（UTF-8），并且仅在事件字段中接收到位字符时才应用其他设置。

要使 OSMP 收集器监听 1,000 及以下的端口，需要以 root 权限运行相关收集器的服务。为此，请在安装收集器后，将行 `AmbientCapabilities = CAP_NET_BIND_SERVICE` 添加到其 systemd 配置文件的 [Service] 部分。
systemd 文件位于 /usr/lib/systemd/system/kuma-collector-<收集器 `ID`>.service 目录中。

连接器已添加到收集器的资源集中。创建的连接器仅在此资源集中可用，不会显示在 Web 界面的“**资源和服务**” → “**连接器** ”部分中。

继续执行安装向导的下一步。

步骤 3.事件解析

这是安装向导的必需步骤。在安装向导的**事件解析**选项卡上，选择或创建一个规范化器，其设置将定义将原始事件转换为规范化事件的规则。您可以向规范化器添加多个事件解析规则以实现复杂的事件处理逻辑。您可以使用测试事件来测试规范化器。

在“安装向导”中创建新的规范化器时，默认情况下它会保存在收集器的资源集中，且不能在其他收集器中使用。选中**保存规范化器**复选框，即可将规范化器创建为独立资源，这样该规范化器可以在其他租户的收集器中选择。

如果在更改收集器资源集的设置时，更改或删除与其连接的规范化器中的转换，则编辑不会被保存，且规范化器本身可能被损坏。若需修改已属于某个服务的标准化器中的转换规则，则必须在 Web 界面的“**资源**” → “**规范化器**”下直接对该规范化器进行更改。

添加规范化器

要将现有规范化器添加到资源集：

1. 单击“**添加事件解析**”按钮。

   将打开**事件基础解析**窗口，其中规范化器设置和**规范化方案**选项卡处于激活状态。

2. 在“**规范化器**”下拉列表中，选择所需的规范化器。下拉列表包括属于收集器租户和共享租户的规范化器。

   “**事件基础解析**”窗口显示了所选规范化器的设置。

   如果要编辑规范化器设置，请在“**规范化器**”下拉列表中，单击相关规范化器名称旁边的铅笔图标。这将打开带有深色圆圈的“**编辑规范化器**”窗口。单击深色圆圈将打开“**事件基础解析**”窗口，您可以在其中编辑规范化器设置。

   如果要编辑高级解析设置，请将光标移到深色圆圈上，以显示加号图标；单击加号图标即可打开“**高级事件解析**”窗口。有关配置高级事件解析的详细信息，请参阅以下说明。

3. 单击“**确定**”。

规范化器在安装向导的“**事件基础解析**”选项卡上显示为深色圆圈。单击圆圈将打开规范化器选项以供查看。

要在收集器中创建新的规范化器：

1. 在“事件解析”步骤的“**解析方案**”选项卡上，单击“**添加事件解析**”。

   将打开**事件基础解析**窗口，其中规范化器设置和**规范化方案**选项卡处于激活状态。

2. 如果要将规范化器保存为独立资源，请选中“**保存规范化器**”复选框；这样保存的规范化器可供租户的其他收集器使用。默认情况下，此复选框未被选中。

3. 在“**名称**”字段中，输入规范化器的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。

4. 在“**解析方法**”下拉列表中，选择要接收的事件类型。根据您的选择，您可以使用预配置的规则来匹配事件字段或设置您自己的规则。在选择某些解析方法时，可能需要填写额外的设置字段。

   可用的解析方法：

   - JSON

     此解析方法用于处理 JSON 数据，其中每个对象（包括其嵌套对象）均在文件中占用一行。

     在处理具有层次结构的数据文件时，可以通过指定参数名称并以句点分隔这些名称来访问嵌套对象的字段。例如，可以使用 `user.username` 查询来访问字符串 `"user": {"username": "system: node: example-01"}` 中的 `username` 参数。

     将逐行处理文件。具有嵌套结构的多行对象可能会被错误规范化。

     在使用附加规范化器的复杂规范化方案中，所有嵌套对象都在第一个规范化级别进行处理，但未指定额外规范化条件的情况除外。因此，正在处理的事件将被完整地传递给附加规范化器。

     换行符可以是 `\n` 和 `\r\n`。字符串必须采用 UTF-8 编码。

     如果要发送原始事件以进行高级规范化，请在“**高级事件解析**”窗口的每个嵌套级别上，在“**保留原始事件**”下拉列表中选择“**是**”。

   - CEF

     此解析方法用于处理 CEF 数据。

     选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。

   - regexp

     此解析方法用于创建自定义规则，以使用正则表达式的格式处理数据。

     在“**规范化**”参数块的字段中，添加一个包含命名捕获组的正则表达式（RE2 语法）。组名及其值将分别被视为原始事件的字段及其值，该字段可转换为 KUMA 格式的事件字段。

     要添加事件处理规则：

     1. 将要处理的数据示例复制到“**事件示例**”字段。该步骤为可选步骤，但建议执行。

        您还可以单击“**通过 KIRA 生成正则表达式**”，根据已添加的示例生成正则表达式。在这种情况下，生成的正则表达式将自动添加到“**规范化**”参数块。

     2. 在“**规范化**”参数块的字段中，添加一个采用 RE2 语法、包含命名捕获组的正则表达式，例如“(?P<name>regexp)”。添加到“**规范化**”参数中的正则表达式必须与事件完全匹配。此外，编写正则表达式时，建议使用匹配文本起始和结束位置的特殊字符：^、$。

        您可以使用“**添加正则表达式**”按钮添加多个正则表达式。如果需要删除正则表达式，请单击 ✕ 按钮。

     3. 单击“**将字段名称复制到映射表**”按钮。

        捕获组名称显示在**映射**表的“**KUMA 字段**”列中。现在，您可以在每个捕获组旁边的列中选择对应的 KUMA 字段。否则，如果您按照 CEF 格式命名了捕获组，可以选中“**使用 CEF 语法进行规范化**”复选框，以使用自动 CEF 映射。

     已添加事件处理规则。

- **Syslog**

  此解析方法用于处理 syslog 格式的数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。

- **csv**

  此解析方法用于创建处理 CSV 数据的自定义规则。

  选择此方法时，必须在“**分隔符**”字段中指定字符串中各值的分隔符。任何单字节 ASCII 字符都可以用作分隔符。

- **kv**

  此解析方法用于处理键值对格式的数据。

  如果选择此方法，必须在以下必填字段中提供值：

  - “**配对分隔符**”——指定用作键值对分隔符的字符。您可以指定任意单字符（1字节）值，但该字符不能与值分隔符相同。
  - “**值分隔符**”——指定用作键和值之间分隔符的字符。您可以指定任意单字符（1字节）值，但该字符不能与键值对分隔符相同。

- **xml**

  此解析方法用于处理 XML 数据。在文件中，每个对象（包括其嵌套对象）各占一行。将逐行处理文件。

  如果要发送原始事件以进行高级规范化，请在“**高级事件解析**”窗口的每个嵌套级别上，在“**保留原始事件**”下拉列表中选择“**是**”。

  选择此方法后，您可以在“**XML 属性**”参数块中指定要从标签中提取的关键属性。如果 XML 结构的同一标签中有多个值不同的属性，您可以在“**映射**”表的“**源**”列中指定所需值对应的键。

  要添加关键 XML 属性，

  单击“**添加字段**”按钮，然后在显示的窗口中指定所需属性的路径。

  您可以添加多个属性。可以使用叉号图标逐个移除属性，也可以使用“**重置**”按钮一次性移除所有属性。

  如果未指定 XML 键属性，则在字段映射过程中，XML 值的唯一路径将由一系列标签表示。

  标签编号

  标签编号功能自 KUMA 2.1.3 起可用。此功能可自动为 XML 事件中的标签编号，以便解析包含相同标签或未命名标签（例如 <Data>）的事件。

  下面以 **Microsoft Windows PowerShell 事件 ID 800** 的 EventData 属性为例，使用**标签编号**功能为其中的标签编号。

要解析此类事件，您必须：

- 配置标签编号。
- 配置编号后的标签与 KUMA 事件字段之间的数据映射。

KUMA 3.0.x 支持在同一个额外规范化器中同时使用**XML 属性**和**标签编号**功能。如果属性包含未命名标签或相同标签，建议使用**标签编号**功能。如果属性仅包含命名标签，请使用**XML 属性**功能。要在额外规范化器中使用此功能，您必须依次在事件到达目标额外规范化器所经过的每个额外规范化器中，以及目标额外规范化器本身，启用“保留原始事件”设置。

有关此功能的使用示例，请参阅 MicrosoftProducts 规范化器 — 其中在“AD FS”和“424”额外规范化器中依次启用了“保留原始事件”设置。

要配置对包含同名标签或未命名标签的事件的解析：

1. 创建新的规范化器，或打开现有规范化器进行编辑。
2. 在规范化器的**基本事件解析**窗口中，从**解析方法**下拉列表中选择“xml”，然后在**标签编号**字段中点击**添加字段**。

   在显示的字段中，输入要为其元素编号的标签的完整路径。例如，Event.EventData.Data。为标签分配的第一个编号为 0。如果标签为空，例如 <Data />，也会为其分配编号。
3. 要配置数据映射，请在**映射**下点击**添加行**，然后执行以下操作：

   a. 在新行的**来源**字段中，输入标签的完整路径及其索引。对于上述示例中的 Microsoft Windows 事件，带索引的完整路径如下：

   - Event.EventData.Data.0,
   - Event.EventData.Data.1
   - Event.EventData.Data.2，依此类推

   b. 在“**KUMA 字段**”下拉列表中，选择 KUMA 事件中用于接收解析后带编号标签对应值的字段。
4. 要保存更改：

   - 如果您创建了新的规范化器，请单击“**保存**”。
   - 如果您编辑了现有的规范化器，请在该规范化器关联的收集器中单击“**更新配置**”。

已配置解析。

- **netflow5**

  此解析方法用于处理 NetFlow v5 格式的数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 netflow5 类型进行主解析，则无法进行额外的规范化。

  > 在映射规则中，默认情况下不会在 KUMA 事件的字段中指明 **netflow5** 的协议类型。在解析 NetFlow 格式的数据时，在**增强**规范化器选项卡上，您必须创建一条**常量**数据增强规则，该规则会将 `netflow` 值添加到 `DeviceProduct` 目标字段。

- **netflow9**

  此解析方法用于处理 NetFlow v9 格式的数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 netflow9 类型进行主解析，则无法进行额外的规范化。

  > 在映射规则中，默认情况下不会在 KUMA 事件的字段中指明 **netflow9** 的协议类型。在解析 NetFlow 格式的数据时，在**增强**规范化器选项卡上，您必须创建一条**常量**数据增强规则，该规则会将 `netflow` 值添加到 `DeviceProduct` 目标字段。

- **sflow5**

  此解析方法用于处理 sflow5 格式的数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 sflow5 类型进行主解析，则无法进行额外的规范化。

- **ipfix**

  此解析方法用于处理 IPFIX 数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 ipfix 类型进行主解析，则无法进行额外的规范化。

  > 在映射规则中，默认情况下不会在 KUMA 事件的字段中指明 **ipfix** 的协议类型。在解析 NetFlow 格式的数据时，在**增强**规范化器选项卡上，您必须创建一条**常量**数据增强规则，该规则会将 `netflow` 值添加到 `DeviceProduct` 目标字段。

- sql — 仅在使用 sql 类型的连接器时，此方法才可用。

  规范化器使用此方法处理从数据库中查询得到的数据。

5. 在“**保留原始事件**”下拉列表中，指定是否将原始事件存储在新创建的规范化事件中。可用值：

   - **不保存** — 不保存原始事件。这是默认设置。
   - **仅出错时** — 如果解析原始事件时发生错误，将原始事件保存到规范化事件的 `Raw` 字段中。该值在调试服务时使用起来十分方便。在这种情况下，每当事件的 `Raw` 字段不为空时，您就知道出现了问题。

     > 如果包含名称 `*Address` 或 `*Date*` 的字段不符合规范化规则，这些字段会被忽略。在这种情况下，不会发生规范化错误，即使已选择“**保留原始事件**” → “**仅出错时**”选项，字段值也不会显示在规范化事件的 `Raw` 字段中。

   - **始终** — 始终将原始事件保存到规范化事件的 `Raw` 字段中。

6. 在“**保留额外字段**”下拉列表中，选择当原始事件字段未配置映射规则时，是否要将其存储在规范化事件中（详见下文）。数据存储在 `Extra` 事件字段中。您可以根据 `Extra` 字段中存储的数据对规范化事件进行搜索和筛选。

   基于“Extra”事件字段数据的筛选

基于 **Extra** 事件字段数据的筛选条件如下：

- 条件 — **如果**。
- 左操作数 — **事件字段**。
- 在此事件字段中，您可以指定以下值之一：
  - **Extra** 字段。
  - Extra 字段中的值格式如下：
    `Extra.<field name>`
    例如，`Extra.app`。
    此类型的值需手动指定。
  - 写入 **Extra** 字段的数组值格式如下：
    `Extra.<field name>.<array element>`
    例如，`Extra.array.0`。
    数组中的值从 0 开始编号。
    此类型的值需手动指定。
    要使用 Extra 字段中第 3 层及更深层级的值，请使用反引号 ``。例如，`Extra.lev1.lev2.lev3`。
- 运算符 — =。
- 右操作数 — **常量**。
- 值 — 用于过滤事件的值。

默认情况下，不保存字段。

7. 将要处理的数据示例复制到“**事件示例**”字段。该步骤为可选步骤，但建议执行。
8. 在“**映射**”表中，配置原始事件字段到 KUMA 格式事件字段的映射：
   a. 在“**源**”列中，提供要转换为 KUMA 事件字段的原始事件字段的名称。
   有关字段格式的详细信息，请参阅“规范化事件数据模型”文章。有关映射的说明，请参阅“预定义规范化器的字段映射”文章。
   单击“**源**”列中字段名称旁边的“🔧”按钮，将打开“**转换**”窗口。在该窗口中，您可以单击“**添加转换**”按钮，以创建在将原始数据写入 KUMA 事件字段之前进行修改的规则。
   可用转换
   转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。
   可用转换：
   - **lower** — 用于将值的所有字符变为小写
   - **upper** — 用于将值的所有字符变为大写
   - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。

- **substring** — 用于提取"**开始**"和"**结束**"字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除"**字符**"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
- **append** 用于将"**常量**"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

在“**转换**”窗口中，可以通过拖动 ⣿ 图标来交换添加的规则；您也可以使用 ✕ 图标来删除规则。

b. 在 **KUMA 字段**列中，从下拉列表中选择所需的 KUMA 事件字段。您可以通过在字段中输入名称来搜索字段。

有关 KUMA 字段列的建议

建议您配置以下 KUMA 字段的映射。否则，您将无法在警报详情和事故详情中查看可观察对象。

推荐的 KUMA 字段取决于可观察对象类型：

- 对于 MD5 哈希和 SHA256 类型的可观察对象：
  - FileHash
- 对于 URL 类型的可观察对象：
  - RequestUrl
- 对于 IP 地址类型的可观察对象：
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress
  - SourceTranslatedAddress
  - SourceAddress
- 对于域名类型的可观察对象：
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain
  - SourceDnsDomain
  - SourceNtDomain

- 对于 UserName 类型的可观察对象：
  - DestinationUserName
  - SourceUserName
- 对于 HostName 类型的可观察对象：
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. 如果上一步中选择的 KUMA 事件字段的名称以 `DeviceCustom*` 或 `Flex*` 开头，您可以在“**标签**”字段中添加唯一的自定义标签。

可以使用“**添加行**”按钮添加新的表格行。可以使用 ✕ 按钮逐行删除，也可以使用“**全部清除**”按钮一次性删除所有行。

如果希望 KUMA 使用资产信息增强事件数据，并在触发关联规则时在警报卡中显示资产信息，请在“**映射**”表中根据资产的用途配置主机地址和主机名字段的映射。例如，映射可以应用于 SourceAddress 和 SourceHostName，或 DestinationAddress 和 DestinationHostName 字段。进行事件增强后，事件卡将包含 SourceAssetID 或 DestinationAssetID 字段，以及指向资产卡的链接。此外，进行事件增强后，资产信息也将显示在警报卡中。

如果您已将数据加载到“**事件示例**”字段中，则该表将包含一个“**示例**”列，其中包含从原始事件字段转移到 KUMA 事件字段的值示例。

如果 KUMA 事件字段的大小小于其中放置值的长度，则该值将被截断为事件字段的大小。

9. 单击“**确定**”。

规范化器在“安装向导”**事件解析**”选项卡上显示为深色圆圈。如果要打开规范化器设置进行查看，请单击深色圆圈。将鼠标悬停在圆圈上时，会显示一个加号。单击加号，即可添加事件解析规则（请参阅下方说明）。

使用附加数据丰富规范化事件

您可以通过在规范化器中创建增强规则，向新创建的规范化事件添加额外数据。这些增强规则存储在创建它们的规范化器中。可以指定多个增强规则。

要向规范化器添加增强规则：

1. 选择主规范化规则或附加规范化规则以打开一个窗口，然后在该窗口中单击“**增强**”选项卡。
2. 单击“**添加增强规则**”按钮。

   增强规则参数块将会出现。您可以通过单击 ✕ 按钮来删除设置组。
3. 从“**源类型**”下拉列表中选择增强类型。根据所选类型，可能还需要完成高级设置。

可用的增强规则源类型：

- **常量**

  在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置：

  - 在“**常量**”字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。
  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

  如果对 `String`、 `Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。

  如果对 `Array of strings`、`Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。

- **词典**

  如果需要从“字典”类型的**字典**中添加值，则使用此类型的增强规则。

  在“**字典名称**”下拉列表中选择此类型后，必须选择用于提供值的字典。在“**键字段**”设置块中，您必须点击“**添加字段**”按钮，然后选择相应的事件字段，其值将用于词典条目选择。

  如果您使用事件增强功能，并在“源类型”设置中选择了“字典”类型，且在“键增强字段”设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。

  示例：“键增强字段”设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”。以下值作为键传递给字典：['a','b','c']。

  如果“键增强字段”设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以“|”字符分隔。

  示例：“键增强字段”设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”；Code 字符串字段包含字符序列“myCode”。以下值作为键传递给词典：['a','b','c']myCode。

- **表格**

  如果您需要从“表格”类型的**字典**中添加值，则需使用此类型的增强功能。

  在“**字典名称**”下拉列表中选择此增强类型后，选择用于提供值的字典。在“**键字段**”设置组中，单击“**添加字段**”按钮以选择其值用于字典条目选择的事件字段。

  在“**映射**”表格中，配置用于提供数据的字典字段和用于接收数据的事件字段：

  - 在“**字典字段**”列中，选择字典字段。可用字段取决于所选的字典资源。
  - 在“KUMA **字段**”列中，选择要写入值的事件字段。对于某些所选字段（`*custom*` 和 `*flex*`），在“**标签**”列中，可以为写入其中的数据指定一个名称。

  可通过单击“**添加新元素**”按钮添加新的表行。可通过单击 ✕ 按钮删除列。

- **事件**

  若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置：

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
  - 在“**源字段**”下拉列表中，选择要将其值写入目标字段的事件字段。
  - 单击 按钮将打开“**转换**”窗口。您可以在该窗口中使用“**添加转换**”按钮创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。

    可用转换

    转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

    可用转换：

    - **lower** — 用于将值的所有字符变为小写
    - **upper** — 用于将值的所有字符变为大写
    - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
    - **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
    - **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
      - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
      - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
    - **trim** — 用于同时从值的开始和结束位置删除“**字符**”字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
    - **append** 用于将“**常量**”字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
    - **prepend** — 用于将“**常量**”字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
    - **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
      - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
      - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
    - 将编码字符串转换为文本：
      - **decodeHexString** — 用于将 HEX 字符串转换为文本。
      - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
      - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。

- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

使用事件增强功能时，如果在“**源类型**”设置中选择了“**事件**”，并将扩展事件模式字段用作参数，则需要特别注意以下事项：

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `String` 类型的字段，则值会以 TSV 格式写入目标字段。

  例如：SA.StringArray 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 DeviceCustomString1 事件模式字段。操作后，DeviceCustomString1 字段包含 ["string1", "string2", "string3"]。

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `Array of strings` 类型的字段，则将源字段的值附加到目标字段的值之后，并将结果写入目标字段，使用逗号（","）作为分隔符。

  例如：SA.StringArrayOne 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 SA.StringArrayTwo 事件模式字段。操作后，SA.StringArrayTwo 字段包含 "string1"、"string2" 和 "string3"。

- **模板**

在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

- 在“**模板**”字段中，输入 Go 模板。

  事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。

  例如：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

- 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

如果您使用事件增强功能，并在“**源类型**”设置中选择了“**模板**”类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

例如：

{{.SA.StringArrayOne}}

例如：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

4. 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
   此设置不适用于“**表格**”类型的增强源。
5. 如果要在规范化器日志中启用详细信息，请将“**调试**”切换开关设置为启用。默认情况下禁用详细信息。
6. 单击“**确定**”。

带有附加数据的事件增强规则将被添加到规范化器中，适用于选定的解析规则。

配置链接到 IP 地址的解析

您可以将来自多个 IP 地址、不同类型的源的事件定向到同一个收集器，且收集器将应用所配置的相应规范化器。

您可以将此方法用于带有 UDP、TCP 或 HTTP 类型连接器的收集器。如果在**传输方式**步骤中，在收集器中指定了 UDP、TCP 或 HTTP 连接器，则在**事件解析**步骤中，您可以在**解析设置**选项卡上指定多个IP地址，并选择要对来自指定地址的事件使用的规范化器。可以使用以下类型的规范化器：json、cef、regexp、syslog、csv、kv、xml。

在配置了链接到IP地址的规范化器的收集器中，如果将连接器类型更改为UDP、TCP、HTTP以外的任何类型，则**解析设置**选项卡将消失，并且在**解析**步骤中仅保留先前指定的第一个规范化器。该选项卡将立即从 Web 界面中消失，但更改将在保存资源后应用。如果要恢复之前的设置，请退出收集器安装向导且不保存更改。

对于 Syslog 和 regexp 类型的规范化器，您可以根据 DeviceProcessName 字段的值指定额外的规范化条件。与额外规范化的区别在于您可以指定共享规范化器。

要配置链接到 IP 地址的解析：

1. 在**事件解析**步骤中，转到**解析设置**选项卡。
2. 在“**IP 地址**”字段中，指定一个或多个将从中接收事件的 IP 地址。您可以指定多个用逗号分隔的 IP 地址。可用格式：IPv4。地址列表的长度不受限制，但是，我们建议指定合理数量的地址，以保持收集器的负载平衡。如果要在一个收集器中应用多个规范化器，则此字段为必填字段。
   限制：对于每个“IP+规范化器”组合，IP 地址必须是唯一的。OSMP 会检查地址的唯一性。如果为不同的规范化器指定相同的 IP 地址，则会显示**该字段必须唯一**消息。
   如果要将所有事件发送到同一个规范化器而不指定 IP 地址，则建议创建单独的收集器。如果要将同一个规范化器应用于来自大量 IP 地址的事件，我们也建议创建一个带有单个规范化器的独立收集器，这有助于提高性能。
3. 在“**规范化器**”字段中，创建一个规范化器或从下拉列表中选择一个现有的规范化器。单击下拉列表旁边的箭头，即可转到“**解析方案**”选项卡。
   如果配置了连接器类型（UDP、TCP、HTTP），则会触发规范化。在配置 HTTP 的情况下，必须指定事件源标头。

考虑到可用的连接器，以下规范化器类型可用于自动源识别：json、cef、regexp、syslog、csv、kv、xml。

4. 如果选择了Syslog或regexp规范化器类型，则可以配置**附加条件**。如果在主规范化器中配置了DeviceProcessName 的**字段映射**，则可以进行条件规范化。在“**条件**”下，在“DeviceProcessName”字段中指定进程名称并创建一个规范化器，或从下拉列表中选择一个现有的规范化器。您可以指定多个“设备进程名称”与“规范化器”的组合，规范化过程将持续进行，直到找到第一个匹配项。

已配置与 IP 地址关联的解析。

创建事件规范化规则的结构

要实现复杂的事件处理逻辑，可以向规范化器添加多个事件解析规则。事件将在解析规则之间根据指定条件进行传输。创建解析规则的顺序至关重要。事件将按顺序处理，并使用箭头显示其路径。

要创建附加解析规则：

1. 创建规范化器（请参阅上述说明）。

   创建的规范化器在窗口中显示为深色圆圈。

2. 将鼠标悬停在圆圈上，然后单击出现的加号按钮。

3. 在打开的“**附加事件解析**”窗口中，指定附加事件解析规则的参数：

   - “**额外规范化条件**”选项卡：

     如果要发送原始事件进行额外规范化，请在“**保留原始事件**”下拉列表中选择“**是**”。默认值为“**否**”。建议将原始事件传递给 json 和 xml 类型的规范化器。如果要将原始事件发送到第二、第三等嵌套级别进行额外规范化，请在每个嵌套级别的“**保留原始事件**”下拉列表中选择“**是**”。

     要仅将具有特定字段的事件发送到附加规范化器，请在**要传入规范化器的字段**字段中指定此字段。

     在此选项卡上，您还可以定义其他条件。在满足这些条件时，发送事件进行附加解析。

   - “**规范化方案**”选项卡：

     在此选项卡上，您可以配置事件处理规则，类似于主规范化器设置（请参阅上述说明）。“**保留原始事件**”设置不可用。“**事件示例**”字段显示了创建初始规范化器时指定的值。

   - “**增强**”选项卡：

     在此选项卡上，您可以配置事件增强规则（请参阅上述说明）。

4. 单击“**确定**”。

附加解析规则已添加到规范化器。它显示为一个深色块，其中包含触发此规则的条件。单击附加解析规则，即可更改其设置。将鼠标悬停在附加解析规则上，则会出现一个加号按钮。单击此按钮，即可创建新的附加解析规则。要删除规范化器，请使用带有垃圾桶图标的按钮。

窗口右上角包含一个搜索框，您可以在其中按名称搜索解析规则。

继续执行安装向导的下一步。

步骤 4：筛选事件

这是安装向导的可选步骤。安装向导的**事件筛选**选项卡允许您选择或创建一个筛选器，其设置指定选择事件的条件。您可以向收集器添加多个过滤器。您可以通过拖动 ⣿ 图标来交换和删除过滤器。过滤器通过“AND”运算符组合。

要将现有过滤器添加到收集器资源集，

请单击“**添加过滤器**”按钮，然后从“**过滤器**”下拉菜单中选择所需的过滤器。

要向收集器资源集添加新过滤器：

1. 单击“**添加过滤器**”按钮，然后从“**过滤器**”下拉菜单中选择“**新建**”。
2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。如果决定在不同服务中重复使用相同的过滤器，这将非常有用。默认情况下，此复选框未被选中。
3. 如果选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器的名称。该名称必须包含 1 到 128 个 Unicode 字符。
4. 在“**条件**”部分，指定过滤事件必须满足的条件：
   - 单击“**添加条件**”按钮可添加过滤条件。您可以选择两个值（两个操作数，即左操作数和右操作数），并分配要使用选定值执行的操作。操作的结果为 True 或 False。
     - 在“**运算符**”下拉列表中，选择过滤器要执行的函数。

       在此下拉列表中，如果运算符应忽略值的大小写，则可以选中“**大小写不匹配**”复选框。如果选择了 **InSubnet**、**InActiveList**、**InCategory**、**InActiveDirectoryGroup** 操作员，则忽略此复选框。默认情况下，此复选框未被选中。

       过滤器运算符

       - **=** — 左操作数等于右操作数。
       - **<** — 左操作数小于右操作数。
       - **<=** — 左操作数小于或等于右操作数。
       - **>** — 左操作数大于右操作数。
       - **>=** — 左操作数大于或等于右操作数。
       - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
       - **contains** — 左操作数包含右操作数的值。
       - **startsWith** — 左操作数以右操作数的某个值开头。
       - **endsWith** — 左操作数以右操作数的某个值结尾。
       - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
       - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

         待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

         如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
       - **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

         如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。

- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 右操作数中指定的列表项是否存在于左操作数中。

- 在“**左操作数**”和“**右操作数**”下拉列表中，选择待筛选的数据来源。选择后，将显示“高级设置”。使用这些高级设置来确定将传递给过滤器的确切值。例如，选择“**活动列表**”时，您需要指定活动列表的名称、条目键和条目键字段。
- 可使用“**如果**”下拉列表来选择是否需要创建否定过滤条件。

单击 ✕ 按钮，即可删除条件。

- “**添加组**”按钮用于添加条件组。“**与**”可在“**与**”、“**或**”和“**非**”之间切换。

  单击 ✕ 按钮，即可删除条件组。
- 单击“**添加过滤器**”，即可将在“**选择过滤器**”下拉列表中选定的现有过滤器添加到条件中。您可以单击 以导航至嵌套过滤器。

  单击 ✕ 按钮，即可删除嵌套过滤器。

已添加过滤器。

继续执行安装向导的下一步。

步骤 5.事件聚合

这是安装向导的可选步骤。通过安装向导的“**事件聚合**”选项卡，您可以选择或创建聚合规则，其设置指定了聚合相同类型事件的条件。您可以向收集器添加多个聚合规则。

要将现有聚合规则添加到一组收集器资源，

请单击“**添加聚合规则**”，然后在下拉列表中选择“**聚合规则**”。

要将新的聚合规则添加到一组收集器资源：

1. 单击“**添加聚合规则**”按钮，然后从“**聚合规则**”下拉菜单中选择“**新建**”。
2. 在“**名称**”字段中输入新创建的聚合规则的名称。该名称必须包含 1 到 128 个 Unicode 字符。
3. 在“**阈值**”字段中，指定在聚合规则触发且事件被聚合之前必须累积多少个事件。默认值为 `100`。

4. 在“**触发后规则有效期**”字段中，指定收集器必须累积要聚合的事件的时长（以秒为单位）。当此时间到期时，聚合规则被触发并创建一个新的聚合事件。默认值为 `60`。

5. 在“**相同字段**”部分，单击“**添加字段**”按钮，以选择将用于标识相同类型事件的字段。可以通过单击带有叉号图标的按钮来删除选定的事件。

6. 在“**唯一字段**”部分，单击“**添加字段**”来选择某些字段。这些字段将使事件无法参与聚合，即使事件包含“**相同字段**”部分中列出的字段。可以通过单击带有叉号图标的按钮来删除选定的事件。

7. 在**求和字段**部分中，可以单击**添加字段**按钮以选择在聚合过程中将对其值进行求和的字段。可以通过单击带有叉号图标的按钮来删除选定的事件。

8. 在**筛选器**部分，您可以指定条件来定义将由此资源处理的事件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。

   在资源中创建过滤器

   KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

   要创建过滤器：

   1. 在“**过滤器**”下拉列表中，选择“**新建**”。

   2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。

   3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。

   4. 在**“条件”**下，指定事件必须满足的条件：

      a. 单击“**添加条件**”按钮。

      b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。

      c. 在“**运算符**”下拉列表中，选择一个运算符。

      过滤器运算符

      - **=** — 左操作数等于右操作数。
      - **<** — 左操作数小于右操作数。
      - **<=** — 左操作数小于或等于右操作数。
      - **>** — 左操作数大于右操作数。
      - **>=** — 左操作数大于或等于右操作数。
      - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
      - **contains** — 左操作数包含右操作数的值。

- **startsWith** — 左操作数以右操作数的某个值开头。
- **endsWith** — 左操作数以右操作数的某个值结尾。
- **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。
  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。
  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。
  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“ ”按钮查看嵌套过滤器设置。

添加聚合规则。可通过单击 ✕ 按钮进行删除。

继续执行安装向导的下一步。

步骤 6.事件增强

这是安装向导的可选步骤。在安装向导的“**事件增强**”选项卡上，您可以指定应将哪些数据从哪些来源添加到收集器处理的事件中。可以使用增强规则或 LDAP 获取的数据来增强事件。

基于规则的增强

可以指定多个增强规则。您可以单击“**添加增强规则**”按钮来添加增强规则，也可以单击 ✕ 按钮来删除增强规则。您可以使用现有的增强规则，也可以直接在安装向导中创建规则。

要将现有的增强规则添加到资源集中：

1. 单击“**添加增强规则**”。

   这将打开增强规则设置块。

2. 在“**增强规则**”下拉列表中，选择相关资源。

增强规则将添加到收集器的资源集中。

要在资源集中创建新的增强规则：

1. 单击“**添加增强规则**”。

   这将打开增强规则设置块。

2. 在“**增强规则**”下拉列表中，选择“**新建**”。

3. 在“**源类型**”下拉列表中，选择要增强的数据源并定义其相应的设置：

   - **常量**

     在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置：

     - 在“**常量**”字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。

     - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

     如果对 `String`、 `Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。

     如果对 `Array of strings`、`Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。

   - **词典**

     如果需要从“字典”类型的**字典**中添加值，则使用此类型的增强规则。

     在“**字典名称**”下拉列表中选择此类型后，必须选择用于提供值的字典。在“**键字段**”设置块中，您必须点击“**添加字段**”按钮，然后选择相应的事件字段，其值将用于词典条目选择。

     如果您使用事件增强功能，并在“源类型”设置中选择了“字典”类型，且在“键增强字段”设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。

     示例：“键增强字段”设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”。以下值作为键传递给字典：['a','b','c']。

     如果“键增强字段”设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以“|”字符分隔。

示例：“键增强字段”设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”；Code 字符串字段包含字符序列“myCode”。以下值作为键传递给词典：['a','b','c']myCode。

- **事件**

  若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置：

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
  - 在“**源字段**”下拉列表中，选择要将其值写入目标字段的事件字段。
  - 在“**转换**”下，您可以创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。可以从下拉列表中选择转换类型。您可以使用“**添加转换**”和“**删除转换**”按钮来添加或删除转换。转换的顺序很重要。

    可用转换

    转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

    可用转换：

    - **lower** — 用于将值的所有字符变为小写
    - **upper** — 用于将值的所有字符变为大写
    - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
    - **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
    - **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
      - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
      - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
    - **trim** — 用于同时从值的开始和结束位置删除“**字符**”字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
    - **append** 用于将“**常量**”字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
    - **prepend** — 用于将“**常量**”字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
    - **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
      - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
      - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。

- 将编码字符串转换为文本：

  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。

- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

- **模板**

在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

- 在“**模板**”字段中，输入 Go 模板。

  事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。

  例如：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

- 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

如果您使用事件增强功能，并在“**源类型**”设置中选择了“**模板**”类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

例如：

{{.SA.StringArrayOne}}

例如：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

  这种类型的增强功能用于向私有网络 DNS 服务器发送请求，以实现 IP 地址与域名之间的相互转换。仅对以下私有地址进行 IP 地址到 DNS 名称的转换：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、100.64.0.0/10、fd00::/8。

  下表介绍了此类增强功能的设置。

  "dns"类型的增强功能参数

设置	描述
网址	要向其发送请求的 DNS 服务器的 URL。 您可以使用 **添加 URL** 按钮指定多个 URL。 如果未指定 **URL** 设置，KUMA 将从本地主机的 `/etc/resolv.conf` 文件中获取 DNS 服务器列表。在这种情况下，您需要启用 **递归查询** 选项。否则，将不会执行增强操作。
每秒请求数	每秒向 DNS 服务器发送的最大查询数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
工作进程	服务可以同时运行以并行处理响应规则的处理程序数量。请指定一个介于 0 到 999 之间的正整数。如果指定为 0，则使用逻辑 CPU 核心数。默认值为 `1`。
数据增强队列中的最大事件数	重新提交队列中可容纳的最大事件数。默认值为 `1,000,000`。
超时时间	等待 DNS 服务器响应的时间（以秒为单位）。默认值为 `5`。
DNS 模式覆盖	使用的解析方法： • **仅正向** DNS将域名解析为 IP 地址。 • **仅反向** DNS将 IP 地址解析为域名。 • **正向和反向** DNS将域名解析为 IP 地址，或将 IP 地址解析为域名。
缓存 TTL	缓存中存储的值的生存时间（以秒为单位）。默认值为 `60` 秒。
缓存已停用	您可以使用此设置启用或禁用缓存。默认情况下启用缓存。
缓存刷新已停用	如果启用了缓存更新，当缓存的 TTL 到期时，收集器会多次向 DNS 服务器发送请求，以更新缓存中存储的数据。此设置仅在启用缓存时可用。默认情况下，缓存更新已启用。
递归查询	允许收集器向权威 DNS 服务器发送递归查询，以进行数据增强。默认值是"**已禁用**"。

- **cybertrace**

  此类增强功能用于将 CyberTrace 数据流中的信息添加到事件字段。

  可用设置：

  - **URL**（必填）— 在此字段中，您可以指定要向其发送请求的 CyberTrace 服务器的 URL。
  - **连接数** — KUMA 可与 CyberTrace 服务器建立的最大同时连接数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
  - **RPS** — 每秒向服务器发送的最大请求数。默认值为 `1000`。
  - **超时** — 等待 CyberTrace 服务器响应的时间（以秒为单位）。默认值为 `30`。
  - **映射**（必需）— 此设置块包含用于将 KUMA 事件字段映射到 CyberTrace 指标类型的映射表。**KUMA 字段**列显示 KUMA 事件字段的名称，**CyberTrace 指标**列显示 CyberTrace 指标的类型。

可用的 CyberTrace 指标类型：

- **ip**
- **url**
- **哈希**

在映射表中，您必须提供至少一个字符串。您可以单击“**添加行**”按钮来添加字符串，也可以单击 ✕ 按钮来删除字符串。

- **时区**

这种类型的增强功能在收集器和关联器中用于为事件分配特定的时区。在搜索发生在异常时间（例如夜间）的事件时，时区信息可能很有用。

选择这种类型的增强功能时，必须从“**时区**”下拉列表中选择所需的时区。

> 确保在增强功能服务的托管服务器上，已设置所需的时区。例如，您可以使用 `timedatectl list-timezones` 命令，该命令显示服务器上设置的所有时区。有关设置时区的更多详细信息，请参阅您的操作系统文档。

对事件进行增强后，所选时区相对于世界协调时 (UTC) 的时间偏移量会以 `+-hh:mm` 格式写入 DeviceTimeZone 事件字段。例如，如果您选择 **Asia/Yekaterinburg** 时区，则值 `+05:00` 将被写入 DeviceTimeZone 字段。如果经过增强的事件在 DeviceTimeZone 字段中已经存在值，则该值将被覆盖。

默认情况下，如果未在正在处理的事件中指定时区，并且未配置按时区增强规则，则将为事件分配处理事件的服务（收集器或关联器）所在服务器的时区。如果服务器时间被更改，则必须重启服务。

丰富 DeviceTimeZone 字段时允许的时间格式

在收集器中处理传入的原始事件时，以下时间格式可以自动转换为 +-hh:mm 格式：

已处理事件中的时间格式	示例
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

如果 `DeviceTimeZone` 字段中的日期格式与上述所列格式不同，那么在使用时区信息对事件进行增强时，收集器服务器的时区将会被写入该字段。您可以为非标准时间格式创建自定义规范化规则。

- **geographic data**

这种类型的增强功能用于将 IP 地址的地理数据添加到事件字段。了解有关将 IP 地址关联到地理数据的更多信息。

选择此类型后，在**将地理数据映射到事件字段**下，您必须指定从哪个事件字段读取 IP 地址，选择所需的地理数据属性，并定义要将地理数据写入的事件字段：

1. 在**带有 IP 地址的事件字段**下拉列表中，选择从中读取 IP 地址的事件字段。上传到 KUMA 的地理数据与此 IP 地址匹配。

   您可以使用“**添加带有 IP 地址的事件字段**”按钮来指定需要增强地理数据的多个带有 IP 地址的事件字段。单击“**删除带有 IP 地址的事件字段**”按钮，即可删除以这种方式添加的事件字段。

选择 SourceAddress、DestinationAddress 和 DeviceAddress 事件字段后，“**应用默认映射**”按钮将变为可用。您可以点击此按钮来添加地理数据属性和事件字段的预配置映射对。

2. 对于需要从中读取 IP 地址的每个事件字段，选择地理数据的类型以及要将地理数据写入其中的事件字段。

   您可以使用“**添加地理数据属性**”按钮来添加“**地理数据属性 - 目标事件字段**”的字段对。您还可以为一个 IP 地址配置不同类型的地理数据，以将其写入不同的事件字段。要删除字段对，请单击 ×。

   - 在“**地理数据属性**”字段中，选择与所读取的 IP 地址对应且应该被写入事件的地理数据。可用的地理数据属性：**国家/地区**、**地区**、**城市**、**经度**、**纬度**。
   - 在**目标“事件”字段**中，选择必须写入所选地理数据属性的事件字段。

   您可以将相同的地理数据属性写入不同的事件字段。如果配置了多个地理数据属性写入同一事件字段，则事件将以序列中最后一个映射的结果为准。

4. 使用“**Debug**”下拉列表指示是否启用服务操作日志记录。日志记录默认被禁用。

5. 在“**过滤器**”部分，您可以指定条件以识别将由增强规则资源处理的事件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。

   在资源中创建过滤器

   KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

   要创建过滤器：

   1. 在“**过滤器**”下拉列表中，选择“**新建**”。
   2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
   3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
   4. 在**“条件”**下，指定事件必须满足的条件：
      a. 单击“**添加条件**”按钮。
      b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。
      c. 在“**运算符**”下拉列表中，选择一个运算符。

      过滤器运算符

      - **=** — 左操作数等于右操作数。
      - **<** — 左操作数小于右操作数。
      - **<=** — 左操作数小于或等于右操作数。

- **>** — 左操作数大于右操作数。
- **>=** — 左操作数大于或等于右操作数。
- **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
- **contains** — 左操作数包含右操作数的值。
- **startsWith** — 左操作数以右操作数的某个值开头。
- **endsWith** — 左操作数以右操作数的某个值结尾。
- **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。
  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。
  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。
  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

新的扩充规则已添加到收集器的资源集中。

要使用 LDAP 启用增强功能：

1. 单击“**通过 LDAP 数据来添加数据增强**”。
   这将打开 LDAP 扩充设置组。

2. 在**LDAP 账户映射**设置区块中，单击**新建域**按钮以指定用户账户的域。您可以指定多个域。

3. 在**LDAP 映射**表中，定义将KUMA字段映射到LDAP属性的规则：

   - 在**KUMA 字段**列中，指定要将其数据与 LDAP 属性进行比较的 KUMA 事件字段。
   - 在 **LDAP 属性**列中，指定必须与 KUMA 事件字段进行比较的属性。下拉列表包含标准属性，并且可以通过**自定义属性**进行扩展。

     在使用自定义属性配置事件增强之前，请确保在 AD 中配置了自定义属性。

     要使用自定义属性通过账户丰富事件：

     1. 在 **LDAP 连接设置**中添加自定义 AD 账户属性。
        标准的**从 AD 导入的属性**不能添加为自定义属性。例如，如果添加标准 `accountExpires` 属性作为自定义属性，KUMA 在保存连接设置时返回错误。

        可以从 Active Directory 请求以下账户属性：

        - `accountExpires`
        - `badPasswordTime`
        - `cn`
        - `co`
        - `company`
        - `department`
        - `description`
        - `displayName`
        - `distinguishedName`
        - `division`
        - `employeeID`
        - `givenName`
        - `l`
        - `lastLogon`
        - `lastLogonTimestamp`

- Mail
- mailNickname
- managedObjects
- manager
- memberOf（此属性可用于关联时搜索）
- mobile
- name
- objectCategory
- objectGUID（即使用户未明确指定，也始终会从 Active Directory 请求此属性）
- objectSID
- physicalDeliveryOfficeName
- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

在 LDAP 连接设置中添加自定义属性后，收集器中待接收的 **LDAP 属性**下拉列表将自动包含这些新属性。自定义属性由属性名称旁边的问号标识。如果为多个域添加了相同的属性，则该属性在下拉列表中仅列出一次。您可以通过将光标移到问号上来查看域。域名显示为链接。如果单击链接，且该域之前未添加，则会自动将其添加到 **LDAP 账户映射**中。

如果在 LDAP 连接设置中删除了自定义属性，请从收集器的映射表手动删除包含该属性的行。每次导入账户时，KUMA 中的账户属性信息都会被更新。

2. 导入账户。

3. 在收集器的 **LDAP 映射**表中，定义将 KUMA 字段映射到 LDAP 属性的规则。

4. 重启收集器。

   重启收集器后，KUMA 开始使用账户丰富事件。

- 在**待写入列的 KUMA 事件字段**中，指定如果映射成功，应将从 LDAP 导入的用户账户 ID 放置在 KUMA 事件的哪个字段中。

可以单击“**添加行**”按钮向表中添加字符串，或单击 ✕ 按钮删除字符串。您可以使用**应用默认映射**按钮，用标准值填充映射表。

已将针对从 LDAP 接收的数据的事件增强规则添加到收集器的资源组中。

如果使用 LDAP 向现有收集器添加增强功能或更改增强功能设置，则必须停止并重启服务。

继续执行安装向导的下一步。

步骤 7：路由

这是安装向导的可选步骤。在安装向导的“**路由**”选项卡上，您可以选择或创建目标位置，并使用设置指示收集器处理的事件的转发目标位置。通常，收集器的事件会路由到两个位置：一个是关联器，用于分析和搜索威胁；另一个是存储，用于存储已处理的事件，以便之后查看。可以根据需要将事件发送到其他位置。可以设置多个目标位置。

要将现有目标位置添加到收集器资源集：

1. 在“**添加目的地**”下拉列表中，选择要添加的目的地资源类型：

   - 如果要配置将已处理的事件转发到存储，请选择“**存储**”。
   - 如果要配置将已处理的事件转发到关联器，请选择“**关联器**”。
   - 如果要将事件发送到其他位置，请选择“**其他**”。

     此类资源包括在程序早期版本中创建的关联器和存储服务。

   “**添加目标位置**”窗口将打开，您可以在其中指定事件转发的参数。

2. 在“**目位置标**”下拉列表中，选择所需目标位置。

   窗口名称将更改为“**编辑目的地**”，并显示所选资源的设置。要在新浏览器标签页中打开目标位置设置进行编辑，请单击 ↗。

3. 单击“**保存**”按钮。

选定的目标位置将显示在“安装向导”选项卡上。要删除目的地资源，可以先选中该目的地资源，然后在打开的窗口中单击“**删除**”。

要将新的目标资源添加到收集器资源集：

1. 在“**添加目标位置**”下拉列表中，选择要添加的目标位置资源类型：

   - 如果要配置将已处理的事件转发到存储，请选择“**存储**”。
   - 如果要配置将已处理的事件转发到关联器，请选择“**关联器**”。
   - 如果要将事件发送到其他位置，请选择“**其他**”。

     此类资源包括在程序早期版本中创建的关联器和存储服务。

   “**添加目标位置**”窗口将打开，您可以在其中指定事件转发的参数。

2. 在“**基本设置**”选项卡上指定设置：

   - 在“**目标位置**”下拉列表中，选择“**新建**”。
   - 在“**名称**”字段中，输入目标位置资源的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
   - 使用“**禁用**”切换按钮指定是否将事件发送到此目标位置。默认情况下，发送事件处于启用状态。
   - 选择目标位置资源的“**类型**”：
     - 如果要配置将已处理的事件转发到存储，请选择“**存储**”。
     - 如果要配置将已处理的事件转发到关联器，请选择“**关联器**”。
     - 如果要配置将事件发送到其他位置，请选择 **nats-jetstream**、**tcp**、**http**、**kafka** 或 **file**。
   - 以 hostname:<API port> 格式指定接收事件的目标 **URL**。
     对于除 **nats-jetstream**、**file** 和 **diode** 之外的所有类型，您都可以使用“**URL**”按钮指定多个目标地址。
   - 对于 **nats-jetstream** 和 **kafka** 类型，使用“**Topic**”字段指定数据写入的目标主题。主题必须包含 Unicode 字符。Kafka 主题限制为 255 个字符。

3. 如有必要，请在“**高级设置**”选项卡上指定设置。可用的设置因所选目标位置资源类型而异：

   - “**压缩**”是一个下拉列表，您可以在其中启用 Snappy 压缩。默认情况下，压缩处于**禁用**状态。
   - “**代理**”是一个用于选择代理服务器的下拉列表。
   - “**缓冲区大小**”字段用于设置目标位置的缓冲区大小（以字节为单位）。默认值为 1 MB，最大值为 64 MB。
   - “**超时**”字段用于设置另一个服务或组件响应的超时时间（以秒为单位）。默认值为 `30`。
   - “**磁盘缓冲区大小限制**”字段用于指定磁盘缓冲区的大小（以字节为单位）。默认大小为 10 GB。
   - **集群 ID**是NATS集群的ID。

- “**TLS 模式**”是一个下拉列表，您可以在其中指定使用 TLS 加密的条件：

  - **禁用** （默认）—不使用 TLS 加密。
  - **启用** — 启用加密，但不进行验证。
  - **带验证** — 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。

  使用 TLS 时，无法将 IP 地址指定为 URL。

- “**URL 选择策略**”是一个下拉列表，您可以在其中选择一种方法来确定接收事件的目标 URL（如指定了多个 URL 的话）：

  - **任何**。只要此 URL 可以接收事件，就会将事件发送到其中一个可用的 URL。如果连接断开（例如，接收节点断开连接），将选择其他 URL 作为事件目标位置。
  - **第一个优先**。事件将发送到所添加地址列表中的第一个 URL。如果该 URL 不可用，则事件将按顺序发送到下一个可用节点。当第一个 URL 再次可用时，将再次开始向其发送事件。
  - **均衡**意味着包含事件的包会在列表中所有可用的 URL 之间进行平均分配。由于数据包是在目标位置缓冲区溢出或刷新计时器触发时发送的，因此该 URL 选择策略无法保证事件均匀分布到目标位置。

- **分隔符**用于指定分隔事件的字符。默认情况下，使用 `\n`。

- **Path** — 如果选择了**文件**目标位置类型，则该字段应填写文件路径。

- **缓冲区刷新间隔** — 此字段用于设置数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `100`。

- **Workers** — 此字段用于设置处理队列的服务数量。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。

- 您可以使用“**健康检查路径**”和“**健康检查超时**”字段来设置健康检查。您也可以通过选中“**健康检查已禁用**”复选框来禁用健康检查。

- **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

- “**磁盘缓冲区已禁用**”下拉列表用于启用或禁用磁盘缓冲区的使用。默认情况下，禁用该选项。

  如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受“**磁盘缓冲区大小限制**”设置的值的限制。

  如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式轮换：新事件替换写入缓冲区的最旧事件。

- 在“**过滤器**”部分，您可以指定条件来定义将由此资源处理的事件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。

  在资源中创建过滤器

  KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

要创建过滤器：

1. 在“**过滤器**”下拉列表中，选择“**新建**”。

2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。

3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。

4. 在**“条件”**下，指定事件必须满足的条件：

   a. 单击“**添加条件**”按钮。

   b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。

   c. 在“**运算符**”下拉列表中，选择一个运算符。

   过滤器运算符

   - **=** — 左操作数等于右操作数。
   - **<** — 左操作数小于右操作数。
   - **<=** — 左操作数小于或等于右操作数。
   - **>** — 左操作数大于右操作数。
   - **>=** — 左操作数大于或等于右操作数。
   - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
   - **contains** — 左操作数包含右操作数的值。
   - **startsWith** — 左操作数以右操作数的某个值开头。
   - **endsWith** — 左操作数以右操作数的某个值结尾。
   - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
   - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

     待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

     如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
   - **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

     如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
   - **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
   - **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。

- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

4. 单击“**保存**”按钮。

创建的目标位置显示在“安装向导”选项卡上。要删除目的地资源，可以先选中该目的地资源，然后在打开的窗口中单击“**删除**”。

继续执行安装向导的下一步。

步骤 8：设置验证

这是安装向导必须完成的最后一步。在此步骤中，OSMP 创建服务资源集，并根据此集合自动创建服务：

- 收集器的资源集显示在“**资源和服务**” → “**收集器**”下。它可用于创建新的收集器服务。在此资源集发生变化时，基于此资源集运行的所有服务将在服务重启后开始使用新参数。为此，您可以单击“**保存并重启服务**”和“**保存并更新服务配置**”按钮。

  与其他资源一样，资源集可以修改、复制、从一个文件夹移动到另一个文件夹、删除、导入和导出。

- 服务显示在“**资源和服务**” → “**活动服务**”中。使用安装向导创建的服务在 OSMP 内部执行功能。要与网络基础设施的外部部分通信，您需要在承载这些外部服务的服务器和资产上安装类似外部服务。例如，应在用作事件接收方的服务器上安装外部收集器服务，在已部署 ClickHouse 服务的服务器上安装外部存储服务，以及在可接收和转发 Windows 事件的 Windows 资产上安装外部代理服务。

要完成安装向导：

1. 单击“**创建并保存服务**”。

   安装向导的“**设置验证**”选项卡将显示一个基于安装向导中选定资源集创建的服务表格。窗口下方显示了在目标服务器和资产上安装这些服务的外部等效项时必须使用的命令示例。

例如：

```
/opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 服务器的完全限定域名。
- <port> 是用于与 KUMA Core 通信的端口。
- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

  `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

  安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

  为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
- <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
- <API port> 是用于与已安装组件通信的端口。

> “kuma”文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/ 目录中。

与 KUMA Core 通信的端口、KUMA Core CA 证书的指纹 ID、服务 ID 以及与服务通信的端口会自动添加到命令中。还必须确保 OSMP 的网络连接正常，并在必要时打开其组件使用的端口。

2. 单击“**保存收集器**”以关闭向导。

已在 OSMP 中创建收集器服务。现在，您将在用于接收事件的服务器上安装类似的服务。

> 如果为收集器选择了 wmi 或 wec 连接器，则还必须安装自动创建的 OSMP 代理。

在 KUMA 网络基础设施中安装收集器

收集器由两部分组成：一部分在 KUMA 控制台内创建，另一部分安装在用于接收事件的网络基础设施服务器上。收集器的第二部分安装在网络基础设施中。

要安装收集器：

1. 登录到要安装该服务的服务器。
2. 创建 /opt/kaspersky/kuma/ 文件夹。

3. 将“kuma”文件复制到 /opt/kaspersky/kuma/ 文件夹。该文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/ 文件夹中。

   请确保 kuma 文件具有足够的运行权限。如果该文件不可执行，请将其设置为可执行：

   ```
   sudo chmod +x /opt/kaspersky/kuma/kuma
   ```

4. 将 /kuma-ansible-installer/roles/kuma/files/ 目录中的 LICENSE 文件放入 /opt/kaspersky/kuma/ 目录，然后运行以下命令接受最终用户授权许可协议的条款和条件：

   ```
   sudo /opt/kaspersky/kuma/kuma license
   ```

5. 创建“kuma”用户：

   ```
   sudo useradd --system kuma && usermod -s /usr/bin/false kuma
   ```

6. 将“kuma”用户设置为 /opt/kaspersky/kuma 目录及其中所有文件的所有者：

   ```
   sudo chown -R kuma:kuma /opt/kaspersky/kuma/
   ```

7. 执行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA
   Core CA certificate> --id <service ID> --api.port <API port>
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。
   - <port> 是用于与 KUMA Core 通信的端口。
   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

     为确保验证 KUMA Core CA 证书，建议安装服务时保留包含指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
   - <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
   - <API port> 是用于与已安装组件通信的端口。

   例如：

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
   --api.port YYYY
   ```

   如果在执行命令时检测到错误，请确保设置正确。例如，所需访问级别的可用性、收集器服务和 Core 之间的网络可用性，以及所选 API 端口的唯一性。修复错误后，继续安装收集器。

如果没有发现错误，并且 KUMA 控制台中的收集器状态变为*绿色*，请停止命令执行并继续下一步。

可以在安装程序向导的最后一步复制该命令。该命令自动指定 KUMA Core 服务器的地址和端口、要安装的收集器的标识符以及收集器用于通讯的端口。

在同一主机上部署多个 KUMA 服务时，必须在安装过程中使用 `--api.port <port>` 参数为每个组件指定唯一的端口。默认使用以下设置值：`--api.port 7221`。

安装程序前，请确保 KUMA 组件的网络连接。

8. 再次运行该命令，添加 `--install` 密钥：

```
sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 服务器的完全限定域名。
- <port> 是用于与 KUMA Core 通信的端口（默认使用端口 7210）。
- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

  `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

  安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

  为确保验证 KUMA Core CA 证书，建议安装服务时保留包含指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
- <服务 ID> 是从 Web 接口复制的 KUMA 服务标识符。
- <API port> 是用于与已安装组件通信的端口。

例如：

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX --api.port YYYY --install
```

9. 将 KUMA 收集器端口添加到防火墙排除项。

为保证程序正常运行，请确保 KUMA 组件能够通过在安装 KUMA 组件期间指定的协议和端口与网络上的其他组件和程序交互。

已安装收集器。您可以使用它从事件源接收数据并将其发送以供处理。

验证收集器安装

要验证收集器是否已准备好接收事件：

1. 在 KUMA 控制台中，转到“**资源**” → “**活动服务**”部分。
2. 确保所安装的收集器的状态为绿色。

   如果收集器的状态不是绿色，请在安装它的计算机上查看此服务的日志，该日志位于 /opt/kaspersky/kuma/collector/<collector ID>/log/collector 目录中。无论启用还是禁用调试模式，都会记录错误。

如果收集器安装正确，并且您确定数据来自事件源，则在搜索与收集器关联的事件时，表格中应该会显示这些事件。

*要使用 KUMA 控制台的“**事件**”部分检查规范化错误：*

1. 确保收集器服务正在运行。
2. 确保事件源正在向 KUMA 提供事件。
3. 请确保在KUMA控制台的**资源**部分的**规范化器**资源中，在**保留原始事件**下拉列表中选择了**仅当出错时**。
4. 在 KUMA 的“**事件**”部分中，使用以下参数搜索事件：
   - `ServiceID = <待检查的收集器 ID>`
   - `Raw != ""`

   如果通过此搜索找到任何事件，则表示存在规范化错误，需要对此进行调查。

要使用 Grafana™ 仪表板检查规范化错误：

1. 确保收集器服务正在运行。
2. 确保事件源正在向 KUMA 提供事件。
3. 打开“指标”部分并单击“KUMA 收集器”链接。
4. 查看“规范化”小部件的“错误”部分是否显示任何错误。

   如有任何错误，则表明存在规范化错误，应进行调查。

对于 WEC 和 WMI 收集器，必须确保使用唯一的端口连接到其代理。此端口在收集器安装向导的**传输方式**部分中指定。

确保收集器运行不间断

从事件源到 KUMA 的不间断事件流对于保护网络基础设施至关重要。可以通过将事件流自动转发到更多收集器来确保连续性：

- 在 KUMA 端，必须安装两个或更多相同的收集器。
- 在事件源端，必须使用第三方服务器负载管理工具（例如 rsyslog 或 nginx）配置收集器之间的事件流控制。

使用此收集器配置，即使收集器服务器因任何原因不可用，也不会丢失任何传入事件。

请记住，当事件流在收集器之间切换时，每个收集器将分别聚合事件。

如果 KUMA 收集器启动失败，并且其日志中包含"panic: runtime error: slice bounds out of range [8:0]"错误：

1. 停止收集器。

   ```
   sudo systemctl stop kuma-collector-<收集器 ID>
   ```

2. 删除 DNS 增强缓存文件。

   ```
   sudo rm -rf /opt/kaspersky/kuma/collector/<收集器 ID>/cache/enrichment/DNS-*
   ```

3. 删除事件缓存文件（磁盘缓冲区）。只有在能够接受丢弃收集器磁盘缓冲区中的事件时，才能运行该命令。

   ```
   sudo rm -rf /opt/kaspersky/kuma/collector/<收集器 ID>/buffers/*
   ```

4. 启动收集器服务。

   ```
   sudo systemctl start kuma-collector-<收集器 ID>
   ```

使用 rsyslog 控制事件流

要在事件源服务器上启用 rsyslog 事件流控制：

1. 创建两个或更多相同的收集器，以确保事件接收不间断。
2. 在事件源服务器上安装 rsyslog（请参阅 rsyslog 文档）。
3. 在配置文件 /etc/rsyslog.conf 中添加用于在收集器之间转发事件流的规则：

   ```
   *&period; * @@ <main collector server FQDN>: <port for incoming events>
   $ActionExecOnlyWhenPreviousIsSuspended on
   *&period; * @@ <backup collector server FQDN>: <port for incoming events>
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

   配置文件示例

   指定一个主收集器和两个备份收集器的示例配置文件。收集器配置为在 TCP 端口 5140 上接收事件。

```
*.* @@kuma-collector-01.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended on
& @@kuma-collector-02.example.com:5140
& @@kuma-collector-03.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended off
```

4. 通过运行以下命令重启 rsyslog：

   `systemctl restart rsyslog`。

现已在事件源服务器上启用事件流控制。

使用 nginx 控制事件流

要使用 nginx 控制事件流，您需要创建并配置一个 nginx 服务器，以接收来自事件源的事件，然后将这些事件转发给收集器。

要在事件源服务器上启用 nginx 事件流控制：

1. 创建两个或更多相同的收集器，以确保事件接收不间断。

2. 在用于事件流控制的服务器上安装 Nginx。

   - Oracle Linux 8.6 中的安装命令：

     ```
     $sudo dnf install nginx
     ```

   - Ubuntu 20.4 中的安装命令：

     ```
     $sudo apt-get install nginx
     ```

   从源代码安装时，必须使用 `-with-stream` 选项进行编译：

   ```
   $ sudo ./configure -with-stream -without-http_rewrite_module -without-
   http_gzip_module
   ```

3. 在 Nginx 服务器上，将流模块添加到包含收集器之间转发事件流规则的 nginx.conf 配置文件。

   示例流模块

   示例模块中，事件流在收集器 kuma-collector-01.example.com 和 kuma-collector-02.example.com 之间分配，它们通过 TCP 端口 5140 和 UDP 端口 5141 接收事件。负载均衡使用 nginx.example.com nginx 服务器。

```
stream {
upstream syslog_tcp {
server kuma-collector-1.example.com:5140;
server kuma-collector-2.example.com:5140;
}
upstream syslog_udp {
server kuma-collector-1.example.com:5141;
server kuma-collector-2.example.com:5141;
}
server {
listen nginx.example.com:5140;
proxy_pass syslog_tcp;
}
server {
listen nginx.example.com:5141 udp;
proxy_pass syslog_udp;
proxy_responses 0;
}
}
worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile 是工作进程可同时打开的文件数量限制 (RLIMIT_NOFILE)。此参数用于在不重启主进程的情况下提高该限制数量。
# worker_connections 是每个工作进程可以同时打开的最大连接数。
```

4. 通过运行以下命令重启 Nginx：

   ```
   systemctl restart nginx
   ```

5. 在事件源服务器上，将事件转发到 Nginx 服务器。

现已在事件源服务器上启用事件流控制。

要实现精细化的负载均衡调优，可能需要使用 Nginx Plus，但某些基础的负载均衡算法（如"轮询"和"最少连接"）在 Nginx 基础版中也可用。

有关配置 Nginx 的更多详细信息，请参阅 Nginx 文档。

预定义收集器

下表列出的预定义收集器包含在 OSMP 分发包中。

如果需要使预定义的 OOTB 资源适应组织的基础架构，请使用复制操作。您还可以导出和导入资源。无法保证手动创建的预定义资源副本能够正常工作。

预定义收集器

名称	描述
[OOTB] CEF	收集通过 TCP 协议接收的 CEF 事件。
[OOTB] 卡巴斯基 EDR	以 JSON 格式收集来自 Kaspersky Endpoint Detection and Response 的事件。
[OOTB] KSC	通过 Syslog TCP 协议收集来自 Kaspersky Security Center 的事件。

名称	描述
[OOTB] KSC SQL	使用 MS SQL 数据库查询收集来自 Kaspersky Security Center 的事件。
[OOTB] Syslog	通过 Syslog 协议收集事件。
[OOTB] Syslog-CEF	收集通过 UDP 协议传输并带有 Syslog 标头的 CEF 事件。

创建代理

KUMA 代理由两部分组成：一部分在 OSMP 内创建，另一部分安装在服务器或网络基础设施中的资产上。

代理创建分为以下几个步骤：

1. **在 OSMP 中为代理创建资源集**
2. **在 OSMP 中创建代理服务**
3. **将代理的服务器部分安装到将转发消息的资产上**

在创建采用 wmi 或 wec 传输类型的收集器时，将自动创建用于 Windows 资产的 KUMA 代理。尽管这些代理的资源和服务集是在收集器安装向导中创建的，但仍必须将其安装到用于转发消息的资产中。

为代理创建资源集

在 OSMP 中，将基于整合了连接器和目标的代理资源集创建代理服务。

要在 OSMP 中为代理创建资源集：

1. 在 OSMP 中，依次转到 **资源和服务** → **代理程序**，然后点击 **添加代理程序**。
   这将打开一个用于创建代理的窗口，其中“**基础设置**”选项卡处于激活状态。
2. 在“**基础设置**”选项卡上指定设置：
   - 在“**代理名称**”字段中，为创建的服务输入一个唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
   - 在“**租户**”下拉列表中，选择该存储所属租户。
   - 如有必要，请将“**调试**”切换开关拨动至启用位置，以启用服务操作日志记录。
   - 您可以选择在“**描述**”字段中添加最多 256 个 Unicode 字符来描述服务。
3. 单击加号图标 (+) 为代理创建连接，并切换到新增“**连接 <编号>**”选项卡。
   单击加号图标 (×)，即可移除选项卡。

4. 在“**连接器**”下，添加连接器：

- 如果要选择现有的连接器，请从下拉列表中选择该连接器。
- 如果要创建新的连接器，请在下拉列表中选择“**新建**”，然后指定以下设置：
  - 在“**名称**”字段中指定连接器名称。该名称必须包含 1 到 128 个 Unicode 字符。
  - 在**类型**下拉列表中，选择连接器类型，然后在**基本设置**和**高级设置**选项卡上指定其设置。可用的设置取决于所选的连接器类型：
    - TCP
    - UDP
    - nats-jetstream
    - kafka
    - http
    - file
    - ftp
    - nfs
    - wmi
    - wec
    - SNMP

    代理类型由代理中使用的连接器决定。唯一的例外是目标位置为二极管类型的代理。这些代理被视为二极管代理。

    在规范化阶段使用 tcp 或 udp 连接器类型时，如果 DeviceAddress 事件字段为空，则将从中接收事件的资产的 IP 地址将被写入该字段中。

    在代理、收集器和连接器中编辑先前创建的 wec 或 wmi 连接的能力受到限制。您可以将连接类型从 **wec** 更改为 **wmi**，反之亦然，但不能将 **wec** 或 **wmi** 连接更改为任何其他连接类型。同时，在编辑其他连接类型时，您无法选择 **wec** 或 **wmi** 类型。您可以创建连接，而不受连接器类型的任何限制。
- 您可以选择在“**描述**”字段中添加最多 4,000 个 Unicode 字符来描述资源。

连接器将添加到代理资源集的选定连接中。创建的连接器仅在此资源集中可用，不会显示在 Web 界面的“**资源和服务**” → “**连接器**”部分中。

5. 在设置的“**目标位置**”分组中，添加目标位置。

   - 如果要选择现有目标位置，请从下拉列表中选择。
   - 如果要创建新目标位置，请在下拉列表中选择“**新建**”并指定以下设置：
     - 在“**名称**”字段中指定目标位置名称。该名称必须包含 1 到 128 个 Unicode 字符。
     - 在**类型**下拉列表中，选择目标位置类型，并在**基本设置**和**高级设置**选项卡中指定其设置。可用设置取决于所选的目标位置类型：
       - **nats-jetstream** — 用于 NATS 通信。
       - **tcp** — 用于 TCP 通信。
       - **http** — 用于 HTTP 通信。
       - **diode** — 用于使用数据二极管传输事件。
       - **kafka** — 用于 Kafka 通信。
       - **file** — 用于写入文件。
   - 您可以选择在“**描述**”字段中添加最多 4,000 个 Unicode 字符来描述资源。

     代理目标位置的高级设置（例如 TLS 模式和压缩）必须与要链接到代理的收集器的高级目标位置设置相匹配。

   可以设置多个目标位置。您可以通过单击“**添加目标位置**”按钮进行添加，也可以通过单击“✕”按钮进行删除。

6. 对要创建的每个代理连接重复步骤 3-5。
7. 单击“**保存**”按钮。

代理的资源集已创建并显示在“**资源和服务**” → “**代理程序**”下。现在，您可以在 KUMA 中创建代理服务。

在 OSMP 中创建代理服务

为代理创建资源集后，您可以继续在 OSMP 中创建代理服务。

要在 OSMP 中创建代理服务，请执行以下操作：

1. 在 OSMP 的主菜单中，依次转到“**资源和服务**”→“**活动服务**”，然后点击“**添加服务**”。
2. 在打开的**选择服务**窗口中，选择刚刚为代理程序创建的资源集，然后单击**创建服务**。

代理服务已在 OSMP 中创建，并显示在“**资源和服务**”→“**活动服务**”下。现在，必须将代理服务安装到要从中将数据转发到收集器的每个资产上。安装过程中会使用服务 ID。

在 OSMP 网络基础设施中安装代理

在 OSMP 中创建代理服务后，您可以继续将代理安装到用于将数据转发到收集器的网络基础设施资产上。

在安装之前，请验证系统的网络连接并打开其组件使用的端口。

在 Linux 资产上安装 KUMA 代理

关闭终端或重启服务器时，安装在 Linux 设备上的 KUMA 代理会停止运行。为避免手动启动代理，我们建议使用在服务器重启时自动启动应用程序的系统（例如 Supervisor）来安装代理。要自动启动代理，请在配置文件中定义自动启动和自动重启设置。有关配置设置的更多详细信息，请参阅应用程序自动启动系统的官方文档。在 Supervisor 中配置设置的示例，您可以根据需要进行调整：

```
[program:agent_<agent name>] command=sudo /opt/kaspersky/kuma/kuma agent --core
https://<KUMA Core server FQDN>:<port used by KUMA Core>

autostart=true

autorestart=true
```

要将 KUMA 代理安装到 Linux 资产上：

1. 登录到要安装该服务的服务器。
2. 创建以下目录：
   - /opt/kaspersky/kuma/
   - /opt/kaspersky/agent/
3. 将“agent”文件复制到 /opt/kaspersky/kuma/ 目录。“agent”文件位于 KUMA 清单文件中指定为 `kuma_utils` 变量值的主机上的 `/opt/kaspersky/kuma/utils` 目录中。

   请确保 kuma 文件具有足够的运行权限。

4. 执行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA
   certificate> --id <agent ID> --wd <path>
   ```

   其中：
   - <FQDN> 是 KUMA Core 服务器的完全限定域名。
   - <port> 是 KUMA Core 用于内部通讯的端口（默认使用端口 7210）。

- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书的指纹 ID。

  `--pair.fingerprint` 参数是可选的。安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，这意味着在建立连接时不会验证 KUMA Core 的证书颁发机构 (CA) 证书。如果使用 `insecure` 值，则在证书颁发机构 (CA) 证书重新颁发后，无需更新指纹。
  如果要指定用于验证 KUMA Core 的证书颁发机构 (CA) 证书的指纹 ID，请转到 **资源和服务 → 活动服务**，然后在菜单 (⋮) 中选择 **复制证书指纹**。然后，在代理安装命令中使用复制的 ID。如果证书颁发机构 (CA) 证书已重新颁发，请从 Web 界面复制新的证书指纹，并使用更新后的参数值重新启动服务。

- <agent ID> 是在 OSMP 中创建的代理服务的 ID。

- <path> 是安装的代理文件所在目录的路径。如果未指定此标志，文件将存储在 kuma 文件所在的目录中。

例如：

```
sudo /opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX
```

KUMA 代理被安装在 Linux 资产上。该代理将数据转发给 OSMP，您可以设置一个收集器来接收这些数据。

在 Windows 资产上安装 KUMA 代理

在将 Open Single Management Platform 代理安装到 Windows 资产之前，服务器管理员必须在 Windows 资产上创建一个具有 EventLogReaders 权限和作为服务登录权限的用户账户。必须使用此用户账户来启动代理。
如果要使用本地账户运行代理，则需要管理员权限和作为服务登录权限。如果要远程执行收集并仅读取域账户下的日志，则仅需要 EventLogReaders 权限。

要将 KUMA 代理安装到 Windows 资产上：

1. 将 kuma.exe 文件复制到 Windows 资产上的文件夹中。建议使用 `C:\Users\<User name>\Desktop\KUMA` 文件夹进行安装。

   kuma.exe 文件位于 KUMA 清单文件中以 `kuma_utils` 变量值形式指定的主机上的 `/opt/kaspersky/kuma/utils` 目录中。

2. 使用管理员权限在 Windows 资产上启动命令提示符，并找到包含 kuma.exe 文件的文件夹。

3. 执行以下命令：

   ```
   kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <agent
   ID> --user <user> --install [--accept-eula]
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。

   - <port> 是 KUMA Core 用于内部通讯的端口（默认使用端口 7210）。

- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书的指纹 ID。

  `--pair.fingerprint` 参数是可选的。安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，这意味着在建立连接时不会验证 KUMA Core 的证书颁发机构 (CA) 证书。如果使用 `insecure` 值，则在证书颁发机构 (CA) 证书重新颁发后，无需更新指纹。
  如果要指定用于验证 KUMA Core 的证书颁发机构 (CA) 证书的指纹 ID，请转到 **资源和服务** → **活动服务**，然后在菜单 (⋮) 中选择 **复制证书指纹**。然后，在代理安装命令中使用复制的 ID。如果证书颁发机构 (CA) 证书已重新颁发，请从 Web 界面复制新的证书指纹，并使用更新后的参数值重新启动服务。

- <agent ID> 是在 OSMP 中创建的代理服务的 ID。

- <user> 是用于运行代理的用户帐户名称，包括域。

要运行代理，您需要接受最终用户授权许可协议。您可以在命令中添加 `--accept-eula` 选项，以便在代理安装期间自动接受最终用户授权许可协议。这使您能够以非交互方式执行安装。如果您未指定此选项，则需要在安装 KUMA 代理期间手动接受或拒绝授权许可协议。

示例：

- 在未自动接受最终用户授权许可协议的情况下安装 KUMA 代理：

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install
```

- 在自动接受最终用户授权许可协议的情况下安装 KUMA 代理：

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install --accept-eula
```

在安装 KUMA 代理期间使用 `--accept-eula` 选项，即表示您确认同意并接受最终用户授权许可协议的条款和条件。

您可以通过执行 `kuma help agent` 命令来获取帮助信息。

4. 如果在安装代理过程中没有自动接受最终用户授权许可协议，则系统将提示您阅读最终用户授权许可协议的文本，您可以选择接受或拒绝该最终用户授权许可协议。

5. 如果您选择在安装时自动接受最终用户授权许可协议并希望阅读最终用户授权许可协议的文本，或者如果在安装过程中未自动向您提供最终用户授权许可协议的文本，请运行以下命令：

```
kuma.exe license --show
```

如果您想接受最终用户授权许可协议，请运行以下命令并按“`y`”：

```
kuma.exe license
```

6. 通过以下方式之一指定代理用户的密码：

- 手动。

- 在安装代理时从文件中指定。

为避免手动输入密码，您可以将密码添加到 .TXT 文件并将该文件放在与代理的可执行文件相同的目录中。

在命令中指定包含密码的文件。例如：

```
kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install < <name of the file with the password>.txt
```

密码文件中的所有数据（例如，password.txt）都将作为密码重定向到命令，不包括行尾字符（\n\r、\n）。

安装后存储代理文件夹的路径：C:\ProgramData\Kaspersky Lab\KUMA\agent\${agent_id}。

如果在安装带有"< <密码文件名>.txt"标志的代理之前，您没有接受最终用户授权许可协议 (EULA)，则会显示一条错误消息，指出该协议未被接受。

您可以通过以下方式接受 EULA：

a. 在密码文件中，您可以指定 EULA 接受标志。为此，包含密码的文件必须包含两行：第一行包含"y"，用于声明接受 EULA，第二行包含密码。例如：

y

<password>

代理安装命令如下所示：

```
kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install < <name of the file with the password>.txt
```

在这种情况下，您在安装代理时无需额外接受 EULA。

如果在使用密码文件运行命令之前已经接受了 EULA，则文件中的第一行将被解释为密码，并且安装将因"Access denied"错误而中止。

b. 您可以使用 --accept-eula 标志同时接受 EULA 和执行静默安装。

代理安装命令如下所示：

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --accept-eula --install < <name of the file with the password>.txt
```

确保文件中的第一行仅指定了密码，否则将出错。

将创建 C:\ProgramData\Kaspersky Lab\KUMA\agent\<代理 ID> 文件夹，并在其中安装 KUMA 代理服务。代理将 Windows 事件转发到 KUMA，您可以设置收集器来接收这些事件。

代理服务安装后会自动启动。此外，该服务还配置了在发生任何故障时进行重启。可以从 KUMA Web 界面重新启动代理，但前提是服务处于活动状态。否则，需要在 Windows 资产上手动重启服务。

从 Windows 资产中删除 Open Single Management Platform 代理

要从 Windows 资产中移除 KUMA 代理：

1. 在 Windows 计算机上以管理员权限启动命令提示符，并找到包含 kuma.exe 文件的文件夹。
2. 运行以下任意命令：
   - `kuma.exe agent --cfg <path to agent configuration file> --uninstall`
   - `kuma.exe agent --id <在 KUMA 中创建的代理服务的 ID> --uninstall`

   指定的 KUMA 代理已从 Windows 资产中移除。Windows 事件将不再发送到 KUMA。

配置服务时，您可以在安装前通过使用以下命令运行代理来检查配置是否存在错误：

```
kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service
ID> --user <user>
```

自动创建的代理

使用 wec 或 wmi 连接器创建收集器时，会自动创建用于接收 Windows 事件的代理。

自动创建的代理具有以下特殊条件：

- 自动创建的代理只能有一个连接。
- 自动创建的代理显示在 **资源和服务** → **代理程序** 下，其名称末尾会显示 `auto created`。可以审查或删除代理。
- 自动创建的代理的设置是根据**连接事件源**和**传输方式**部分的收集器设置自动定义的。您只能更改已创建代理的收集器的设置。
- 自动创建的代理的描述取自“**连接事件源**”部分的收集器描述。
- 自动创建的代理的调试功能可以在收集器的“**连接事件源**”部分中启用和禁用。
- 删除带有自动创建代理的收集器时，系统将提示您选择是将收集器与代理一起删除，还是仅删除收集器。仅删除收集器时，代理将变为可编辑状态。
- 删除自动创建的代理时，收集器的类型将更改为 **http**，并且连接地址将从收集器的 **URL** 字段中删除。
- 如果 wec 或 wmi 连接器中至少一个 Windows 日志名称指定不正确，代理将不会从连接器中列出的任何 Windows 日志接收事件。同时代理状态将呈现为绿色。每 60 秒重复尝试接收事件，并将错误消息添加到服务日志中。

在 KUMA 界面中，创建收集器时会同时出现自动创建的代理。但是，它们仍然必须安装在用于转发消息的资产上。

更新代理

更新 OSMP 版本时，还必须更新安装在远程计算机上的 WMI 和 WEC 代理。

要更新代理，请使用管理员账户按照以下步骤操作：

1. 在 OSMP 的主菜单中，转到 **资源和服务** → **活动服务** → **代理程序** 部分，选择要更新的代理并复制其 ID。
   删除旧代理后，需要使用该 ID 来安装具有相同 ID 的新代理。
2. 在 Windows 中的“**服务**”部分中，打开代理并单击“**停止**”。
3. 在命令行中，转到安装代理的文件夹，并运行命令以从服务器中删除代理。
   kuma.exe agent --id <在 KUMA 中创建的代理服务的 ID> --uninstall
4. 将新代理放在同一文件夹中。
5. 在命令行中，进入包含新代理的文件夹，然后从该文件夹使用步骤 1 中的代理 ID 运行安装程序命令。

   ```
   kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <agent ID> --user <user> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 服务器的完全限定域名。
   - <port> 是 KUMA Core 用于内部通讯的端口（默认使用端口 7210）。
   - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书的指纹 ID。
     `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。
     安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。
     为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。
   - <agent ID> 是在 OSMP 中创建的代理服务的 ID。
   - <user> 是用于运行代理的用户帐户名称，包括域。

代理已更新。

将事件从隔离网段传输到 KUMA

数据传输场景

数据二极管可用于将事件从隔离网段传输到 KUMA。数据传输流程如下：

1. 安装在独立服务器上的 KUMA 代理（带有**二极管**目标），接收事件并将其移动到数据二极管将从中获取事件的目标位置。
   代理将事件累积在缓冲区中，直至缓冲区溢出或达到用户定义的上一次写入磁盘后的时间间隔。然后，事件将被写入代理临时目录中的文件。该文件被移动到数据二极管处理的目录；其名称是文件内容哈希 (SHA256) 和文件创建时间的组合。

2. 数据二极管将文件从隔离服务器目录移动到外部服务器目录。

3. 安装在外部服务器上的带有**二极管**连接器的 KUMA 收集器，会从数据二极管放置文件的目录中的文件中读取并处理事件。

   从文件读取所有事件后，该文件将被自动删除。在读取事件之前，会根据文件名中的哈希值验证文件内容。如果内容验证失败，则删除该文件。

在所述场景中，KUMA 组件负责将事件移动到隔离网段内的特定目录，并接收来自外部网段中特定目录的事件。数据二极管将包含事件的文件从隔离网段的目录传输到外部网段的目录。

对于隔离网段内的每个数据源，您必须创建自己的 KUMA 收集器和代理，并配置数据二极管以与单独的目录协同工作。

配置 KUMA 组件

配置用于从隔离网段传输数据的 KUMA 组件包括以下步骤：

1. 在外部网段中创建收集器服务。

   在此步骤中，您必须创建并安装一个收集器，以接收和处理数据二极管将从隔离网段传输的文件。您可以使用收集器安装向导创建收集器及其所需的所有资源。

   在**传输方式**步骤中，您必须选择或创建**二极管**类型的连接器。在连接器中，您必须指定数据二极管从隔离网段移动文件所到达的目标目录。

   运行收集器的用户“kuma”必须对数据二极管从隔离网段移动数据所到达的目录具有读/写/删除权限。

2. 为 KUMA 代理创建资源集。

   在此步骤中，您必须为 KUMA 代理创建资源集，该代理将接收隔离网段中的事件，并准备将其传输到数据二极管。二极管代理资源集具有以下要求：

   - 代理中的目标位置必须具有**二极管**类型。在此资源中，您必须指定数据二极管将从哪个目录移动文件到外部网段。
   - 您不能为二极管代理选择 **sql** 或 **netflow** 类型的连接器。
   - 必须在二极管代理的连接器中禁用 TLS 模式。

3. 将代理配置文件下载为 JSON 文件。

   a. 必须将来自二极管类型目标位置的代理资源集下载为 JSON 文件。

   b. 如果代理资源集中使用了机密资源，则必须手动将机密数据添加到配置文件。

4. 在隔离网段中安装 KUMA 代理服务。

   在此步骤中，您必须根据上一步创建的代理配置文件将代理安装在隔离网段中。它可以安装到 Linux 和 Windows 设备上。

配置数据二极管

必须按如下方式配置数据二极管：

- 数据必须原子性地从隔离服务器目录（KUMA 代理存放数据的位置）传输到外部服务器目录（KUMA 收集器读取数据的位置）。
- 必须从隔离服务器中删除已传输的文件。

有关配置数据二极管的信息，请参阅组织中使用的数据二极管文档。

特殊注意事项

使用隔离网段时，不支持使用 SQL 和 NetFlow 进行操作。

使用上述场景时，由于代理位于隔离网段中，因此无法通过 KUMA 控制台进行管理。此类代理不会显示在活跃的 KUMA 服务列表中。

二极管代理配置文件

可以将创建的一组具有二极管类型目标位置的代理资源下载为配置文件。在隔离网段中安装代理时需要使用此文件。

要下载配置文件：

在 OSMP 的主菜单中，依次选择 **资源和服务** → **代理程序**，选择目标位置为“二极管”的相关代理资源集，然后点击 **下载配置**。

代理设置配置根据浏览器的设置，以 JSON 文件形式下载。代理资源集所使用的密钥会以空值形式下载。它们的 ID 在文件的 `secrets` 部分中指定。要使用配置文件在隔离网段中安装代理，您必须手动将密钥添加到配置文件（例如，指定代理连接器中用于接收事件的 URL 和密码）。

您必须使用访问控制列表 (ACL) 来配置在待安装代理的服务器上访问文件的权限。运行二极管代理的用户账户必须具有文件读取访问权限。

以下是带有 kafka 连接器的二极管代理配置文件的示例。

```
{
"config": {
"id": "<代理资源集的 ID>",
"name": "<代理资源集的名称>",
"proxyConfigs": [
{
"connector": {
"id": "<连接器的 ID。此示例展示的是 kafka 类型的连接器，但二极管代理中也可以使用其他类型的连接器。如果直接在代理资源集中创建连接器，则无需定义 ID>",
"name": "<连接器的名称>",
"kind": "kafka",
"connections": [
{
"kind": "kafka",
"urls": [
"localhost:9093"
],
"host": "",
"port": "",
"secretID": "<密钥的 ID>",
"clusterID": "",
"tlsMode": "",
"proxy": null,
"rps": 0,
"maxConns": 0,
"urlPolicy": "",
"version": "",
"identityColumn": "",
"identitySeed": "",
"pollInterval": 0,
"query": "",
"stateID": "",
"certificateSecretID": "",
"authMode": "pfx",
"secretTemplateKind": "",
"certSecretTemplateKind": ""
}
],
"topic": "<kafka 主题名称>",
"groupID": "<kafka 组 ID>",
"delimiter": "",
"bufferSize": 0,
"characterEncoding": "",
"query": "",
"pollInterval": 0,
"workers": 0,
"compression": "",
"debug": false,
"logs": [],
"defaultSecretID": "",
"snmpParameters": [
{
"name": "-",
"oid": "",
"key": ""
}
],
"remoteLogs": null,
"defaultSecretTemplateKind": ""
},
"destinations": [
{
"id": "<目标位置的 ID。如果直接在代理资源集中创建目标位置，则无需定义 ID。>,
"name": "<目标位置名称>",
"kind": "diode",
"connection": {
"kind": "file",
"urls": [
"<目标位置应放置数据二极管将从隔离网段传输的事件的目录路径>",
"<放置事件以准备二极管进行数据传输的临时目录的路径>"
],
"host": "",
"port": "",
"secretID": "",
"clusterID": "",
"tlsMode": "",
"proxy": null,
"rps": 0,
```

```
"maxConns": 0,
"urlPolicy": "",
"version": "",
"identityColumn": "",
"identitySeed": "",
"pollInterval": 0,
"query": "",
"stateID": "",
"certificateSecretID": "",
"authMode": "",
"secretTemplateKind": "",
"certSecretTemplateKind": ""
},
"topic": "",
"bufferSize": 0,
"flushInterval": 0,
"diskBufferDisabled": false,
"diskBufferSizeLimit": 0,
"healthCheckPath": "",
"healthCheckTimeout": 0,
"healthCheckDisabled": false,
"timeout": 0,
"workers": 0,
"delimiter": "",
"debug": false,
"disabled": false,
"compression": "",
"filter": null,
"path":""
}
]
}
],
"workers": 0,
"debug": false
},
"secrets": {
"<secret ID>": {
"pfx": "<加密的 pfx 密钥>",
"pfxPassword": "<pfx 加密密钥的密码。changeit 值是从 KUMA 导出的，而非实际密码。在配置文件中，您必须手动指定密钥的内容>"
}
},
"tenantID": "<租户的 ID>"
}
```


密钥字段描述

密钥字段

字段名称	类型	描述
`user`	字符串	用户名
`password`	字符串	密码
`token`	字符串	令牌
`urls`	字符串数组	URL 列表
`publicKey`	字符串	公钥（用于 PKI）
`privateKey`	字符串	私钥（用于 PKI）
`pfx`	包含 base64 编码的 pfx 文件的字符串	PFX 文件的 Base64 编码内容。在 Linux 中，您可以通过运行以下命令获取文件的 base64 编码： `base64 -w0 src > dst`
`pfxPassword`	字符串	PFX 字符串的密码
`securityLevel`	字符串	用于 snmp3 中。可能值： `NoAuthNoPriv`、 `AuthNoPriv`、 `AuthPriv`
`community`	字符串	用于 snmp1

`authProtocol`	字符串	用于 snmp3 中。可能值：`MD5`、`SHA`、`SHA224`、`SHA256`、`SHA384`、`SHA512`
`privacyProtocol`	字符串	用于 snmp3 中。可能值：`DES`、`AES`
`privacyPassword`	字符串	用于 snmp3
`certificate`	包含 base64 编码的 pem 文件的字符串	PEM 文件的 Base64 编码内容。在 Linux 中，您可以通过运行以下命令获取文件的 base64 编码： `base64 -w0 src > dst`

在隔离网段中安装 Linux 代理

要将 KUMA 代理安装到隔离网段中的 Linux 设备：

1. 将以下文件放置在隔离网段中的 Linux 服务器上，代理将使用该服务器接收事件，并且数据二极管会从该服务器将文件移动到外部网段：

   - 代理配置文件。

     您必须使用访问控制列表 (ACL) 对配置文件的访问权限进行配置，以便只有 KUMA 用户才具有文件读取权限。

   - 执行文件 /opt/kaspersky/kuma/kuma（“kuma”文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/folder 文件夹中）。

2. 执行以下命令：

   ```
   sudo ./kuma agent --cfg <path to the agent configuration file> --wd <path to the directory where the files of the agent being installed will reside&period; If this flag is not specified, the files will be stored in the directory where the kuma file is located>
   ```

代理服务已安装，并在隔离网段中的服务器上运行。该服务接收事件并将其中继到数据二极管，以便将其发送到外部网段。

在隔离网段中安装 Windows 代理

在将 Open Single Management Platform 代理安装到 Windows 资产之前，服务器管理员必须在 Windows 资产上创建一个具有 EventLogReaders 权限和作为服务登录权限的用户账户。必须使用此用户账户来启动代理。

要将 KUMA 代理安装到隔离网段中的 Windows 设备：

1. 将以下文件放置在隔离网段中的 Windows 服务器上，代理将使用该服务器接收事件，并且数据二极管会从该服务器将文件移动到外部网段：

   - 代理配置文件。

     您必须使用访问控制列表 (ACL) 来对配置文件的访问权限进行配置，以便只有运行代理的用户账户才能读取该文件。

   - Kuma.exe 可执行文件。此文件位于安装程序中的 /kuma-ansible-installer/roles/kuma/files/ 目录中。

周三建议使用 `C:\Users\<user name>\Desktop\KUMA` 文件夹。

2. 使用管理员权限在 Windows 资产上启动命令提示符，并找到包含 kuma.exe 文件的文件夹。

3. 执行以下命令：

```
kuma.exe agent --cfg <path to the agent configuration file> --user <user name that
will run the agent, including the domain> --install
```

> 您可以通过运行以下命令获取安装程序帮助信息：
>
> ```
> kuma.exe help agent
> ```

4. 输入用于运行代理的用户账户的密码。

将创建 `C:\Program Files\Kaspersky Lab\KUMA\agent\<Agent ID>` 文件夹，KUMA 代理服务安装在该文件夹中。代理将事件移动到文件夹，以便数据二极管对其进行处理。

> 安装代理时，代理配置文件将被移动到目录 C:\Program Files\Kaspersky Lab\KUMA\agent\ <配置文件中指定的代理 ID>。kuma.exe 文件将被移动到 C:\Program Files\Kaspersky Lab\KUMA 目录。

> 安装代理时，其配置文件不得位于代理的安装目录中。

代理服务安装完成后会自动启动。此外，该服务还配置了在发生任何故障时进行重启。

从 Windows 资产中删除 Open Single Management Platform 代理

要从 Windows 资产中移除 KUMA 代理：

1. 在 Windows 计算机上以管理员权限启动命令提示符，并找到包含 kuma.exe 文件的文件夹。

2. 运行以下任意命令：

   - `kuma.exe agent --cfg <path to agent configuration file> --uninstall`
   - `kuma.exe agent --id <在 KUMA 中创建的代理服务的 ID> --uninstall`

指定的 KUMA 代理已从 Windows 资产中移除。Windows 事件将不再发送到 KUMA。

> 配置服务时，您可以在安装前通过使用以下命令运行代理来检查配置是否存在错误：
>
> ```
> kuma.exe agent --cfg <path to agent configuration file>
> ```

将事件从 Windows 计算机传输到 OSMP

要将事件从 Windows 计算机传输到 OSMP，需结合使用 KUMA 代理和收集器。数据传输流程如下：

1. 安装在计算机上的 KUMA 代理接收 Windows 事件：
   - 使用 WEC 连接器：代理接收根据订阅到达主机的事件以及服务器日志。
   - 使用 WMI 连接器：代理连接到配置中指定的远程服务器并接收事件。
2. 代理将事件（不经预处理）发送到目标位置中指定的收集器。
   您可以配置代理，以便将不同的日志发送到不同的收集器。
3. 收集器从代理接收事件，执行完整的事件处理周期，然后将处理后的事件发送到目标位置。

使用 Windows 事件转发 (WEF) 从 Windows 主机集中收集事件时，建议从 WEC 代理接收事件。代理必须安装在收集事件的服务器上，它充当 Windows 事件收集器 (WEC)。不建议在每个需接收事件的端点主机上安装 KUMA 代理。

使用 WEC 代理配置接收事件的过程在附录中有详细描述：使用 KUMA 代理 (WEC) 配置从 Windows 设备接收事件。

有关 Windows 事件转发技术的详细信息，请参阅 Microsoft® 官方文档。

建议在以下情况下使用 WMI 代理接收事件：

- 如果无法使用 WEF 技术实现集中收集事件，并且同时禁止在事件源服务器上安装第三方软件（例如 KUMA 代理）。
- 如果您需要从少量主机获取事件，每个 KUMA 代理不超过 500 台主机。

要将 Windows 日志连接为事件源时，建议使用“**添加事件源**”向导。当使用向导创建带有 WEC 或 WMI 连接器的收集器时，会自动创建用于接收 Windows 事件的代理。您也可以手动创建收集 Windows 事件所需的资源。

用于接收 Windows 事件的代理和收集器的创建和安装分多个步骤进行：

1. **为代理创建资源集**

   代理连接器：

   创建代理时，在“**连接**”选项卡上，您必须创建或选择 WEC 或 WMI 类型的连接器。

   如果 WEC 或 WMI 连接器中至少一个 Windows 日志名称指定错误，代理将从连接器中列出的所有 Windows 日志接收事件，但不包括有问题的日志。同时代理状态将呈现为绿色。每 60 秒重复尝试接收事件，并将错误消息添加到服务日志中。

   代理目标位置：

   代理目标位置的类型取决于您使用的数据传输方法：nats、tcp、http、diode、kafka 和 file。

   您必须使用 `\0` 值作为目标分隔符。

   代理目标位置的高级设置（例如分隔符、压缩和 TLS 模式）必须与要链接到代理的收集器连接器的高级目标位置设置相匹配。

2. **在 OSMP 中创建代理服务**

3. **在 Windows 计算机上安装 KUMA 代理，以便从该计算机接收 Windows 事件。**

   安装前，请确保系统组件可以访问网络并打开必要的网络端口：

   - 端口 7210，TCP：从带有收集器的服务器到 Core。
   - 端口 7210，TCP：从代理服务器到 Core。
   - 创建连接器时在“**URL**”字段中配置的端口：从代理服务器到包含收集器的服务器。

4. **创建和安装收集器。**

   创建一组收集器时，在“**传输方式**”步骤中，必须创建或选择一个连接器，收集器将使用该连接器接收来自代理的事件。连接器类型必须与代理目标位置的类型匹配。

   连接器的高级设置（例如分隔符、压缩和 TLS 模式）必须与您要链接到代理的代理目标位置的高级设置相匹配。

为了确保某些行动手册正常工作，您可能需要配置收集器的额外增强功能。

要在收集器中编辑增强规则设置：

1. 要添加增强规则，请单击“添加增强规则”，并在相应字段中指定以下信息：
   - **名称**：为规则指定任意名称。
   - **源类型**：dns。
   - **URL**：域控制器的 IP 地址。
   - **每秒请求数**：5。
   - **工作线程数**：2。
   - **缓存 TTL**：3600。
2. 要添加增强规则，请单击添加增强规则并执行以下操作：
   a. 填充以下字段：
      - **名称**：为规则指定任意名称。
      - **源类型**：事件。
      - **源字段**：DestinationNTDomain。
      - **目标字段**：DestinationNTDomain。
   b. 单击“**添加转换**”并在相应字段中指定以下信息：
      - **类型**：附加。
      - **常量**：`.RU`。
      - **类型**：替换。

- **字符**：`RU.RU`。
- **带字符**：`RU`。

3. 重复步骤 2 中的子步骤，并将 SourceNTDomain 指定为**源字段**和**目标字段**。
4. 添加 LDAP 数据增强功能并执行以下操作：
   - 在**LDAP 账户映射**下，指定域控制器的名称。
   - 单击“**应用默认映射**”，以使用标准值填充映射表。

配置代理以接收来自隔离网段的 Netflow 事件

为了接收来自隔离网段的 NetFlow 事件，将使用安装在该网段内的专用代理。该代理充当中间节点：它在本地接收 NetFlow 事件，并将其转发到配置了 NetFlow 连接器的收集器。

事件从代理到收集器的传输通过 UDP 协议进行。

要配置接收 NetFlow 事件：

1. 创建或配置具有 NetFlow 连接器的收集器，并在**传输**步骤的**高级设置**选项卡上，将**缓冲区大小**设置为 **65467**。
2. 确保隔离网段允许发往收集器的出站 UDP 流量。
3. 创建用于接收事件的代理，并配置使用 **NetFlow** 连接器将事件发送到收集器：
   a. 在 OSMP 主菜单中，在“**资源和服务**”→“**代理程序**”下，单击“**创建**”。
   b. 在打开的“**创建代理程序**”窗口中，在“**基础设置**”选项卡上，指定“**名称**”和“**租户**”设置。
   c. 在“**配置资源 #{{index}}**”选项卡的“**连接器**”下，在“**基本设置**”选项卡上，指定以下设置：
      - 在“**名称**”字段中，指定连接器的名称。
      - **类型**—指定 **udp** 连接器类型。
      - **URL**—指定将安装用于接收 NetFlow 事件的代理的主机。
   d. 在“**配置资源 #{{index}}**”选项卡的“**连接器**”下，在“**高级设置**”选项卡上，指定以下设置：
      - 将“**缓冲区大小**”设置为 **65467**。这是缓冲区的最大大小，以字节为单位。
   e. 在“**配置资源 #{{index}}**”选项卡的“**目标位置**”下，在“**基本设置**”选项卡上，指定以下设置：
      - 在“**名称**”字段中，指定目标的名称。
      - **类型**—指定用于发送事件的 UDP 协议。
      - **URL**—指定安装了带有 **NetFlow** 连接器的收集器的主机。

f. 在“**配置资源 #{{index}}**”选项卡的“**目标位置**”下，在“**高级设置**”选项卡上，指定以下设置：

- 将“**缓冲区大小**”设置为 **65467**。这是缓冲区的最大大小，以字节为单位。

g. 单击“**创建**”。

h. 在隔离网段中安装代理。它可以安装到 Linux 和 Windows 设备上。

已配置从隔离网段接收 NetFlow 事件。

AI 服务

本部分提供有关 Kaspersky Next XDR Expert 使用的 AI 服务的信息。

使用 KIRA 分析警报和事故

您可以使用 Kaspersky Investigation & Response Assistant (KIRA) 来分析警报和事件。分析的结果是，您将收到自动生成的警报或事故的描述，包括简短摘要、可观察对象列表、事件时间线、警报或事故报告和缓解建议。

此功能可加速警报或安全事故的调查和初步分析，且无论警报或事故中包含何种事件类型，均可使用。

使用第三方LLM提供商（**自定义**模式）时，请求将直接发送到指定的API。用户选择提供商、模式和参数。数据处理在所选服务的一侧执行。

如果满足以下条件，则此功能可用：

- 拥有涵盖 AI 模块的当前授权许可。
  如果授权许可已过期，分析结果仍可通过任务在缓存有效期内（即自结果缓存之日起 14 天内）访问。
- 已配置与第三方 LLM 提供商 API 的连接。
- 用户拥有**“警报和事故”**功能区域的**写入**权限。

透过LLM提供商配置与KIRA的集成

KIRA 支持以下第三方 LLM 提供商：

- GPT-5.4
- Deepseek-V4-Pro
- Kimi K2.6
- GLM-5.1
- MiniMax M2.7

要使用第三方LLM提供商配置KIRA集成：

1. 获取包含 AI 模块的授权许可，并在 KUMA 中激活该功能。
2. 在应用程序主窗口中，转到**设置**→**KUMA**→**打开KUMA设置**部分。
   这将打开 KUMA 设置窗口。
3. 在**集成**部分，单击**AI服务**
4. 这会打开一个窗口；在该窗口中，前往**Kaspersky Investigation & Response Assistant**选项卡。
5. 启用**"状态"**切换开关，以启用与 KIRA 的集成。
   默认情况下，此切换开关处于关闭状态。
6. 在**模型**下，选择与KIRA交互的**自定义**模型。默认情况下，已选择**KSN**模式。
7. 在**基本URL**字段中，输入提供商的API地址（例如，https://api.openai.com/v1）。地址必须以http://或https://开头。
8. 在**API密钥**下拉列表中，选择或创建**令牌**类型的密钥。
   要创建新 Secret，请选择"**新建**"。如果您使用的API不需要密钥，请在**API密钥**字段中指定一个值为**api-key**的密钥。
9. 在**模型**字段中，指定您的提供商使用的模型的名称（例如，gpt-4-turbo、llama3-70b）。
10. 在**最大提示大小**字段中，指定请求中的最大令牌数。
11. 在**代理服务器**下拉列表中，选择先前创建的资源或新建资源。
12. 选择KIRA响应语言，俄语或英语。KUMA 以您选择的语言发送和存储 KIRA 响应。
    默认情况下已选中俄语。
13. 点击**添加JSON文件**按钮，上传包含模型参数和HTTP标头的文件。
    在此文件中，您可以指定向LLM提供商发出的请求的其他参数（例如，`temperature`、`max_tokens`）。您还可以指定其他HTTP标头。为此，您需要使用`"headers"`密钥。如果文件中指定了多个`"headers"`密钥，则仅使用其中的第一个。

    文件内容示例

    ```
    {
      "temperature": 0.5,
      "max_tokens": 20000,
      "headers": {
        "OpenAI-Organization": "ORG_ID"
      }
    }
    ```

    如果 JSON 文件中指定了以下任一参数，AI 服务将返回错误：`messages`、`model`、`audio`、`function_call`、`functions`、`modalities`、`n`、`parallel_tool_calls`、`prediction`、`response_format`、`stop`、`stream`、`stream_options`、`tool_choice`、`tools`、`web_search_options`。
14. 点击**测试连接**向指定的API发送测试请求。
15. 单击"**保存**"。

点击**"保存"**后，系统会提示您接受最终用户授权许可协议的条款和条件。如果您不接受最终用户授权许可协议，您将无法保存设置或继续使用该功能。

保存设置后，将显示可用令牌数量。令牌每天都会补充。

集成随即配置，您可以继续进行分析。分析适用于所有事件：新事件和以前收到的事件。

使用 KIRA 进行分析

配置集成后，您可以使用 KIRA 分析警报和事故。

要执行分析：

1. 打开警报或事故详细信息。
2. 在警报或事故详情上方的工具栏中，单击"**AI 分析→使用 KIRA 分析**"。

   如果您有足够的令牌，则会启动分析和"**在 KIRA 中查询**"任务。

   处理请求可能需要 30 秒或更长时间。

   即使请求返回错误，表明请求的主题在拒绝列表中，令牌也会被消耗；剩余令牌的信息也会被更新。

对警报或事故进行分析。

要查看分析结果，请在警报或事故详情上方的工具栏中，单击"**AI 分析→查看报告**"。在**"使用 KIRA 分析"**窗口中，分析结果将显示以下详细信息：

- 警报或事故的简要概述。
- 可观察对象列表。
- 警报或事故时间线及事件发生顺序。
- 案例报告。
- 上次请求的日期和时间。
- 已消耗令牌的数量。

您可以单击**重新分析**按钮以执行新的分析，而不使用缓存中存储的上一次分析的数据。此分析会消耗令牌。

"使用 KIRA 进行分析"任务可能出现的错误

使用 KIRA 进行警报和事故分析时可能会出现错误。

可能的错误

HTTP 代码	Description
400	服务请求无效或客户端证书无效。可能的原因：缺少必需参数或参数值无效；用于 KSN 的客户端证书已过期或由不受信任的证书颁发机构颁发。
401	身份验证失败。客户端证书有效，但限制数据库中没有相应的记录。可能的原因：记录被删除、未及时创建，或者由于技术错误发布了不正确的数据。
403	已超过每日令牌限制。

HTTP 代码	Description
404	未知或不支持的用户任务
413	超过了请求令牌限制。请求包含太多的输入令牌。每个请求允许的最大令牌数为 16,000 个，包括服务参数。如果超过此限制，则不进行分析。
500	内部服务错误。处理请求时发生未指明的错误。
502	AI 服务不可用。KIRA 无法连接。
503	服务连接错误。从 KIRA 获取访问令牌失败。
其他	连接错误。KSN 服务返回的任何其他未在上方列出的错误代码。
无代码	KUMA 端请求处理错误。可能的原因包括：读取 KSN 的响应失败、将数据保存到数据库失败，或者检索集成设置失败。

使用KIRA以自然语言创建搜索查询

在**威胁搜索**部分，您可以使用自然语言输入事件搜索查询，使用Kaspersky Investigation & Response Assistant（KIRA）自动将查询转换为数据库查询语法，检查查询的正确性并在必要时进行改进，然后运行系统生成的查询并获取事件搜索结果。每次发送请求时，都会生成一个审计事件。如果在生成请求时发生错误，则会显示错误代码。

令牌数量限制在以下选项中共享：

- 使用 KIRA 以自然语言进行搜索查询
- 使用 KIRA 进行分析

令牌总数取决于查询和响应。您可以预览查询和响应将花费的令牌数量，并编辑响应以减少令牌花费。

如果满足以下条件，则此功能在俄罗斯 (RU) 地区可用：

- 拥有涵盖 AI 模块的当前授权许可。
- 配置 KIRA 集成时已上传证书。您可以从技术支持处获取PFX格式的证书文件（打包在<企业名称>.ZIP压缩包中）以及证书密码。
- 用户拥有以下具有相应访问权限的角色之一：主管理员、管理员、二级分析师、一级分析师和初级分析师。只有具有主管理员角色的用户才能配置集成。

使用KIRA创建自然语言搜索查询并将其转换为SQL查询

配置好 KIRA 集成后，就可以开始生成搜索查询来查找事件了。

若要使用KIRA生成自然语言搜索查询并将其转换为SQL查询：

1. 在**“威胁搜索”**部分，SQL 查询字段下方，单击按钮（）。
2. 这将打开“**KIRA SQL 查询生成器**”窗口；在该窗口的查询字段中，输入您希望 KIRA 转换为 SQL 的查询文本。
   例如：“显示2024年1月15日至16日的所有事件，其中文件名为'file.txt'”。
   支持俄语和英语查询的转换。

3. 点击**生成**按钮。

   生成的 SQL 查询将显示在输出字段中。

   例如：

   ```
   SELECT *
   FROM events
   WHERE FileName = 'file.txt'
   ORDER BY Timestamp DESC
   ```

   生成的时间段显示在**“时间段”**字段中：

   例如：

   2024-01-15T00:00:00.000 - 2024-01-16T00:00:00.000

   如果您在输入内容中未指定事件搜索的时间范围，则使用**“事件”**选项卡中设置的时间段。例如，在**“事件”**中设置了“5 分钟”，查询于 1 月 15 日 15:30 发出，则时间段设置为 2026-01-15T15:25:00.000 - 2026-01-15T15:30:00.000

   在应用生成的查询之前，您可以编辑**SQL查询**和**时间间隔**字段中的值。

4. 如果您想知道发送查询将消耗多少令牌，请点击**计算令牌消耗数量**。

5. 如果要使用生成的 SQL 查询执行事件搜索，请单击**“应用”**按钮。

   “**KIRA SQL 查询生成器**”窗口自动关闭。

   生成的 SQL 查询会自动插入到**“威胁搜索”**选项卡的主查询字段中。

   绝对时间范围字段会自动填充生成的查询中的值。

   例如：2026-01-15T00:00:00.000 - 2026-01-15T00:00:00.000

6. 如果您想使用生成的 SQL 查询执行事件搜索，请单击**“运行查询”**。

自然语言搜索查询将转换为 SQL 查询，并获取事件搜索结果。

使用自然语言构建查询时可能出现的错误

可能的错误

HTTP 代码	Description
400	无效的客户端证书。
404	请求错误。
401	缺少证书信息。联系技术支持。
403	每日令牌数量已用尽。
413	请求的令牌数量已达上限。请减少请求数量。
422	自然语言查询无法转换为SQL语法。
500	服务出现未知错误。
502	KIRA 服务不可用。
503	获取服务访问令牌时出错。
其他	未知错误。
无代码	处理请求时出错。

配置 DLL 劫持检测

DLL 劫持是一种攻击技术，它会将存在漏洞的合法软件与恶意的动态链接库 (DLL) 一起传送到目标系统。当存在漏洞的软件启动时，它不会验证动态库的合法性，而是通过文件名进行加载。因此，恶意的代码会在合法软件的上下文中执行。由于启动的软件是合法的，因此 DLL 劫持攻击很难检测。为了检测此类攻击，需使用 AI 模块。AI 模块会分析应用程序的启动和运行时参数，并识别可疑的带有恶意库的合法软件启动。

为了获取状态，KUMA 会向 KSN 发送请求。该请求包含分析所需的事件字段信息。作为对请求的响应，KSN 会发送以下分析结果之一：

- `0` – **未分类**。为了获取状态，您需要重新发送请求。您可以使用“**执行重复请求设置**”来配置请求的重新发送。
- `1` – **未知**。收到该状态时，该库不会被视为恶意库。
- `2` – **可疑**。如果您配置了相应的关联规则，则收到此类结果时会创建警报。
- `3` – **恶意软件**。如果您配置了相应的关联规则，则收到此类结果时会创建警报。**恶意软件**判定表示检测到DLL劫持的可能性高于**可疑**判定。

结果将以数值和文本注释的形式写入事件的 KL_AI_DLLHijackingCheckResult 字段。

DLL 劫持攻击在事件数据增强阶段被检测出来。这是通过使用**检查 DLL 劫持**数据增强类型来实现的。您可以在收集器或关联器中嵌入此类型的数据增强功能。建议在关联器中嵌入此类型的数据增强功能。这样，KSN 服务的负载会比在收集器中检查事件时低得多。

> 要使用**检查 DLL 劫持**类型的数据增强功能，您的授权许可必须包含AI模块。主管理员还必须在**卡巴斯基安全网络**部分（**设置 → 集成 → AI 服务 → 卡巴斯基安全网络**）接受附加的 KSN 声明。如果您的 KUMA 实例有多个主管理员，则其中一位接受 KSN 声明即可。

通过在关联器中使用事件数据增强功能来检测 DLL 劫持攻击

要配置通过在关联器中使用事件数据增强功能来检测 DLL 劫持攻击：

1. 在应用程序 Web 界面中，选择**资源 → 关联器**。
2. 开始创建关联器或打开现有关联器的设置。
3. 添加“检查 DLL 劫持”类型的数据增强功能。

   配置数据增强功能时，您需要指定与创建 KSN 请求所需的参数相对应的字段列表。确保您指定的字段在收集器的规范化处理环节中已完成填充。
4. 进入数据增强功能设置，在“**过滤器参数**”下的列表中，选择以下过滤器：**[OOTB] DLL 劫持事件数据增强功能**。关联器的过滤器。如果列表中缺少此过滤器，请从存储库中将其导入。您也可以自行配置过滤器。
5. 如果要将应用程序配置为在收到**可疑**或**恶意软件**判定时生成警报，请创建执行此操作的关联规则。创建关联规则时，选择简单或标准类型，然后在“**选择器**”选项卡上，在过滤器参数中指定两个条件：

   `KL_AI_DLLHijackingCheckResult = 2` 或 `KL_AI_DLLHijackingCheckResult = 3`

此外，在关联规则中，指定添加数据增强功能时指定的字段（请参阅说明的步骤 3）。如果您创建的是简单类型的关联规则，则必须在“**传播字段**”设置中列出这些字段；如果您创建的是标准类型的关联规则，则必须在“**相同字段**”设置中列出这些字段。

通过在收集器中使用事件数据增强功能来检测 DLL 劫持攻击

不建议在收集器中使用 **DLL 劫持**数据增强功能。这会增加 KSN 服务的负载。请改为将此类型的数据增强功能添加至关联器。

要配置通过在收集器中使用事件增强功能来检测 DLL 劫持攻击：

1. 在应用程序 Web 界面中，选择 **资源 → 收集器**。
2. 开始创建收集器或打开现有收集器的设置。
3. 添加“检查 DLL 劫持”类型的数据增强功能。

   配置数据增强功能时，您需要指定与创建 KSN 请求所需的参数相对应的字段列表。确保您指定的字段在收集器的规范化处理环节中已完成填充。
4. 进入数据增强功能设置，在“**过滤器参数**”下的列表中，选择以下过滤器：**[OOTB] DLL 劫持事件数据增强功能**。收集器的过滤器。如果列表中缺少此过滤器，请从存储库中将其导入。您也可以自行配置过滤器。
5. 如果要将应用程序配置为在收到**可疑**或**恶意软件**判定时生成警报，请创建执行此操作的关联规则。创建关联规则时，选择简单或标准类型，然后在“**选择器**”选项卡上，在过滤器参数中指定两个条件：

   `KL_AI_DLLHijackingCheckResult = 2` 或 `KL_AI_DLLHijackingCheckResult = 3`

   此外，在关联规则中，指定在添加数据增强功能时指定的字段（请参阅说明的步骤 3）以及“KL_AI_DLLHijackingCheckResult”字段。如果您创建的是简单类型的关联规则，则必须在“**传播字段**”设置中列出这些字段；如果您创建的是标准类型的关联规则，则必须在“**相同字段**”设置中列出这些字段。

AI资产评分和状态。

如果您的授权许可包含AI模块，则可以安装**AI 资产评分和状态**服务。

AI服务有助于精确评估由触发的关联规则生成的关联事件的严重等级。

AI服务从可用的存储集群中获取**受影响资产**字段非空的关联事件，构建预期的事件序列，并训练AI模型。基于触发的关联规则链，AI服务计算此类事件序列是否是此基础设施的典型模式。非典型模式会增加资产的评分。

AI服务计算**AI评分**和**AI状态**，这些信息可在资产卡片中查看。如果移除授权许可密钥， **AI评分**和**AI状态**字段将从资产卡片中隐藏。重新添加授权许可密钥后， **AI评分**和**AI状态**字段的值将再次显示。

AI评分是一个数值，用于量化资产活动的非典型程度，以及是否值得关注。**AI状态**字段的可能值为：**低**、**中**、**高**、**严重**。AI评分的取值范围为0到1。

四个范围分别对应四个状态：

低：0 ≤ 评分 < 0.25

中：0.25 ≤ 评分 < 0.5

高：0.5 ≤ 评分 < 0.75

紧急：0.75 ≤ 评分 ≤ 1

在搜索资产时，您可以根据**AI评分**和**AI状态**字段进行筛选。您还可以根据**AI评分**和**AI状态**字段设置资产的主动分类，一旦AI服务为资产分配了评分，资产就会被自动移至与风险级别对应的类别。

您可以创建多类别结构，并根据计算出的风险值自动填充资产。

在**设置→资产审计**部分，您可以配置在资产添加到某个类别时生成的审计事件。审计事件可以纳入关联规则，并且您可以在控制板和报告中监控这些事件。

若要在控制板监控资产类别变更，请创建一个**事件**小部件，并使用类似于以下的查询：

```
SELECT count(ID) AS `metric`,
formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'),
'%d.%m.%Y %H:%m:%S') AS `value` FROM `events`

where DeviceVendor = 'Kaspersky' and DeviceProduct = 'KUMA' and

DeviceEventCategory = 'Audit assets' and DeviceAction= 'asset added to category'

and DeviceCustomString1 = 'Main/Categorized assets/ML/score>0.5'

GROUP BY Timestamp ORDER BY value LIMIT 250
```

若要监控控制板按状态分组的资产分布情况，请创建一个**按严重等级分组的资产小部件**。如果授权许可包含AI模块，则可以使用**按严重等级分组的资产**小部件。饼图显示了按状态分组的资产数量。

每次AI服务重启时，AI服务都会从头开始训练模型，并重新评估当天事件中提到的资产的评分。

配置文件中指定的目录存储AI服务从KUMA存储集群获取的指定天数内的事件。例如，如果配置文件指定为12天，则AI服务将获取过去12天的事件。目录中最早的事件将被删除。训练好的模型存储在同一目录下。

模型于UTC时午夜开始重新训练。对于当天（UTC）事件中提及的所有资产，资产评分每小时重新评估一次。

服务日志存储在/var/log/syslog中。

安装AI资产评分和状态服务

安装AI资产评分和状态服务

若要安装服务：

1. 解压分发工具包中包含的**mlservice-installer-XX.tgz**压缩包。

   mlservice-installer-XX.tgz压缩包包含用于安装和卸载服务的脚本，以及config.yaml配置文件。

2. 在config.yaml配置文件中，在`kuma_address`设置中，指定安装KUMA Core的主机的FQDN和KUMA Core监听AI服务连接的端口。

   在高可用性配置中，必须指定端口7226。您可以保留其余设置的默认值。安装完成后，服务将使用config.yaml文件中指定的设置启动。

3. 如果要将服务安装在远程主机上，请在inventory.yaml文件中指定远程主机的地址，并确保您拥有网络访问权限。默认情况下，服务安装在inventory.yaml文件中指定的本地主机上。

4. 在KUMA网页界面中获取Core证书。为此，请在KUMA网页界面的主窗口中，点击窗口底部的用户账户名称以打开菜单，然后选择**AI服务证书**。证书将下载到您的默认下载目录。

   如有必要，您可以重新签发AI服务证书。

5. 将下载的证书文件重命名为**core-external-ca.cert**。

6. 将KUMA Core证书文件保存在安装程序目录下的roles/mlservice/files目录中。

7. 切换到服务文件所在的目录，然后从该目录运行以下命令：

   ```
   ./install < inventory.yaml 的路径 >
   ```

8. 如果您接受最终用户授权许可协议的条款和条件，请按Y。如果您不接受最终用户授权许可协议的条款和条件，则无法继续安装此服务。您可以在mlservice-installer/eula目录中找到包含最终用户授权许可协议文本的文件。

9. 安装程序会在安装过程中生成证书和密钥，并将它们放置在 config.yaml配置文件中指定的目录中。您必须将证书上传到KUMA。

   在KUMA网页界面中，依次进入**设置→集成→AI服务**部分的**AI 资产评分和状态**窗口，填写以下字段：

   a. 在**URL**字段中，指定KUMA Core主机的FQDN以及KUMA Core用于监听AI服务的端口，例如：<KUMA Core主机的FQDN>:7226。端口号必须与配置文件中指定的端口号匹配。请确保该端口未被其他应用程序占用。

      对于高可用性配置的KUMA安装程序，**URL**字段不会显示在界面中，端口值取自KUMA_APPRAISER_AI_API_PORT环境变量，并且该端口将为KUMA Core主机的所有IP地址打开。

   b. 在**证书**下拉列表中，选择**新建**以打开**创建密钥**窗口；在该窗口中，将密钥类型指定为**证书**，并从config.yaml配置文件中指定的目录上传证书。

   c. 开启**状态**切换开关。默认情况下，此切换开关处于关闭状态。

   d. 单击“**保存**”。

   安装完成后，服务将立即尝试以1分钟的间隔连接KUMA，持续15分钟。如果未在KUMA网页界面中添加证书，连接将失败，服务将停止。在这种情况下，您可以添加证书并重启AI服务；服务将再次尝试连接。

   保存设置后，获取Core 服务器日志，并确保其中不包含“<port number>: bind: address already in use”错误

AI服务随即安装。

移除AI资产评分和状态服务

要移除AI服务，请切换到包含AI服务文件的目录，并在该目录中运行以下命令：

```
./uninstall <path to inventory.yaml>
```

重新签发AI服务证书

若要重新签发AI服务证书：

1. 在 OSMP 控制台中，转到**设置** → **其他** → **通用**部分。
2. 在**Core 设置**中，找到**AI服务证书**设置，点击**重新签发**按钮。
3. 单击**确定**以确认操作。
4. 将/opt/kaspersky/mlservice目录中的证书替换为新证书。
5. 运行`systemctl restart mlservice`命令重启AI评分和AI状态服务；同时重启KUMA Core。

新的AI服务证书随即应用。

AI资产评分和状态服务的设置

可用的AI服务设置

设置	描述
`cert_file_path`	安装程序生成的证书所在的目录路径。 默认路径： /opt/kaspersky/mlservice/service.crt 您可以指定不同的路径。在这种情况下，请确保启动服务的用户有访问指定目录的权限。
`key_file_path`	安装程序生成的密钥所在的目录路径。 默认路径： /opt/kaspersky/mlservice/service.key 您可以指定不同的路径。在这种情况下，请确保启动服务的用户有访问指定目录的权限。
`kuma_address`	安装KUMA Core主机的FQDN和KUMA Core用于监听AI服务的端口。要以高可用性配置进行安装，必须指定端口7226。 例如： <安装KUMA Core主机的FQDN>:7226
`kuma_cert_file_path`	KUMA Core证书所在的目录路径。 默认路径： /opt/kaspersky/mlservice/core-external-ca.cert
`event_storage_path`	服务放置接收相关事件的目录的路径。 默认路径： /var/mlservice/events
`model_storage_path`	服务放置训练模型的目录的路径。 默认路径： /var/mlservice/models
`period_for_train_days`	您想要从可用存储集群中获取涉及资产的相关事件以训练模型的天数。 默认设置是 12 天。 这意味着目录将包含过去<N>天的事件。最早的事件将被删除。
`events_overlap_in_seconds`	重叠时间。当按计划下载用于评估资产评分的事件时，其起始时间是从当天最后一次下载事件的时间减去`events_overlap_in_seconds`设置的值开始计算的。 默认值是 60 秒。 例如：上次接收事件的时间为8:58，则下一批要下载的事件的起始时间为8:57。

配置事件通知

本部分提供了有关配置从各种来源接收事件的信息。

配置 Auditd 事件的接收

KUMA 支持监控和审计 Linux 设备上的 Auditd 事件。

在配置事件接收之前，请确保为 Auditd 事件创建一个新的 KUMA 收集器。

配置 Auditd 事件的接收涉及以下步骤：

1. 在网络基础设施中安装 KUMA 收集器。
2. 配置事件源服务器。
3. 验证 KUMA 收集器是否收到 Auditd 事件。
   您可以通过在 KUMA 控制台中搜索相关事件来验证 Auditd 事件源服务器是否配置正确。

安装 KUMA 收集器以接收 Auditd 事件

创建收集器后，为了使用 rsyslog 配置事件接收，您必须在用于接收事件的网络基础设施服务器上安装收集器。

有关安装 KUMA 收集器的详细信息，请参阅“在网络基础设施中安装收集器”部分。

配置事件源服务器

rsyslog 服务用于将事件从服务器传输到 KUMA 收集器。

要配置从服务器到收集器的事件传输：

1. 请确保事件源服务器上已安装 rsyslog 服务。为此，请运行以下命令：
   ```
   systemctl status rsyslog.service
   ```
   如果服务器上尚未安装 rsyslog 服务，请执行以下命令进行安装：
   - 对于基于 RPM 的发行版：
     ```
     yum install rsyslog
     ```
   - 对于基于 Debian 或 Ubuntu 的发行版：
     ```
     apt-get install rsyslog
     ```

   通过执行以下命令启用该服务：

```
systemctl enable rsyslog.service
systemctl start rsyslog.service
```

2. 在 /etc/rsyslog.d 文件夹中，创建包含以下内容的 audit.conf 文件：

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
*.* @<KUMA collector IP address>:<KUMA collector port>
```

> 如果要通过 TCP 发送事件，请在文件中插入以下行来替代最后一行：
> `*.* @@<KUMA collector IP address>:<KUMA collector port>`。

3. 保存对 audit.conf 文件所做的更改。

4. 重新启动 rsyslog 服务：

```
systemctl restart rsyslog.service
```

事件源服务器已配置。有关事件的数据从服务器传输到 KUMA 收集器。

配置 KATA/EDR 事件的接收

您可以在 KUMA SIEM 系统中配置 Kaspersky Anti Targeted Attack Platform 事件的接收。

在配置事件接收之前，请确保为 KATA/EDR 事件创建 KUMA 收集器。

> 在 KUMA 控制台中创建收集器时，请确保端口号与配置将 Kaspersky Anti Targeted Attack Platform 事件导出到 KUMA 的步骤 4c 中指定的端口匹配，并且连接器类型与步骤 4d 中指定的类型相对应。

> 要使用Syslog接收Kaspersky Anti Targeted Attack Platform事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] KATA**规范化器。

配置 KATA/EDR 事件的接收涉及以下步骤：

1. 配置 KATA/EDR 事件的转发
2. 在网络基础设施中安装 KUMA 收集器
3. 在 KUMA 收集器中验证 KATA/EDR 事件的接收

   您可以通过在 KUMA 控制台中搜索相关事件来验证 KATA/EDR 事件源服务器是否配置正确。Kaspersky Anti Targeted Attack Platform 事件在搜索结果表中显示为 KATA。

配置将 KATA/EDR 事件导出到 KUMA

要配置将事件从 Kaspersky Anti Targeted Attack Platform 导出到 KUMA：

1. 在任何可以访问中央节点服务器的计算机上的浏览器中，输入托管中央节点组件的服务器的 IP 地址。
   将打开一个用于输入 Kaspersky Anti Targeted Attack Platform 用户凭证的窗口。
2. 在用户凭证输入窗口中，选中“**本地管理员**”复选框，然后输入管理员凭证。
3. 转到“**设置**” → “**SIEM 系统**”部分。
4. 指定下列设置：
   a. 选中“**活动日志**”和“**检测**”复选框。
   b. 在“**主机/IP**”字段中，输入 KUMA 收集器的 IP 地址或主机名。
   c. 在“**端口**”字段中，指定要连接到 KUMA 收集器的端口号。
   d. 在“**协议**”字段中，从列表中选择“**TCP**”或“**UDP**”。
   e. 在“**主机 ID**”字段中，指定要在 SIEM 系统日志中指定为检测源的服务器主机 ID。
   f. 在“**警报频率**”字段中，输入发送消息的间隔：1 至 59 分钟。
   g. 如有必要，请启用 TLS 加密。
   h. 单击“**应用**”。

已配置将 Kaspersky Anti Targeted Attack Platform 事件导出到 KUMA。

创建用于接收 KATA/EDR 事件的 KUMA 收集器

配置事件导出设置后，必须在 KUMA 控制台中创建用于 Kaspersky Anti Targeted Attack Platform 事件的收集器。

有关创建 KUMA 收集器的详细信息，请参阅“创建收集器”。

在 KUMA 控制台中创建收集器时，请确保端口号与配置将 Kaspersky Anti Targeted Attack Platform 事件导出到 KUMA 的步骤 4c 中指定的端口匹配，并且连接器类型与步骤 4d 中指定的类型相对应。

要使用Syslog接收Kaspersky Anti Targeted Attack Platform事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] KATA**规范化器。

安装用于接收 KATA/EDR 事件的 KUMA 收集器

创建收集器后，要配置接收 Kaspersky Anti Targeted Attack Platform 事件，请在用于接收事件的网络基础设施服务器上安装新的收集器。

有关安装 KUMA 收集器的详细信息，请参阅“在网络基础设施中安装收集器”部分。

配置 Open Single Management Platform 以将事件导出到 KUMA SIEM 系统

KUMA 支持从 Open Single Management Platform 管理服务器接收事件并将其导出到 KUMA SIEM 系统。

配置 Open Single Management Platform 事件的导出和接收分阶段进行：

1. 配置 Open Single Management Platform 事件的导出。
2. 配置 KUMA 收集器。
3. 在网络基础设施中安装 KUMA 收集器。
4. 验证 KUMA 收集器中 Open Single Management Platform 事件的接收情况

   您可以使用 KUMA 控制台搜索相关事件，以验证来自 Open Single Management Platform 管理服务器的事件是否已正确导出到 KUMA SIEM 系统。

   要在表格中以 CEF 格式显示 Open Single Management Platform 事件，请输入以下搜索表达式：

   ```
   SELECT * FROM `events` WHERE DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT
   250
   ```

配置 KUMA 收集器以收集 Open Single Management Platform 事件

配置从 Open Single Management Platform 管理服务器导出 CEF 格式的事件后，请在 KUMA 控制台中配置收集器。

要为 Open Single Management Platform 事件配置 KUMA 收集器：

1. 在 KUMA 控制台中，选择“**资源**” → “**收集器**”。
2. 在收集器列表中，找到包含 **[OOTB] KSC** 规范化器的收集器，并将其打开进行编辑。
3. 在“**传输方式**”步骤中，在“**URL**”字段中指定收集器用于接收 Open Single Management Platform 事件的端口。

   该端口必须与 KUMA SIEM 系统服务器的端口匹配。
4. 在**事件解析**步骤中，确保已选择**[OOTB] KSC**规范化器。

5. 在“**路由**”步骤中，确保已将以下目标位置添加到收集器资源集：

   - **存储**。将处理过的事件发送到存储。
   - **关联器**。将处理过的事件发送到关联器。

   如果未添加“**存储**”和“**关联器**”目标位置，请进行创建。

6. 在“**设置验证**”选项卡上，单击“**创建并保存服务**”。

7. 复制出现的安装 KUMA 收集器的命令。

安装 KUMA 收集器以收集 Open Single Management Platform 事件

在配置用于收集 CEF 格式的 Open Single Management Platform 事件的收集器后，请在用于接收事件的网络基础设施服务器上安装 KUMA 收集器。

有关安装 KUMA 收集器的详细信息，请参阅“在网络基础设施中安装收集器”部分。

配置从 MS SQL 接收 Open Single Management Platform 事件

KUMA 支持从 MS SQL 数据库接收有关 Open Single Management Platform 事件的信息。

在配置之前，请确保您已经为来自 MS SQL 的 Open Single Management Platform 事件创建了 KUMA 收集器。

在KUMA网页界面中创建收集器时，请在**传输方式**步骤中选择**[OOTB] KSC SQL**连接器。

要从MS SQL数据库接收Open Single Management Platform事件，请在**事件解析**步骤中选择**[OOTB] KSC from SQL**规范化器。

配置事件接收包括以下步骤：

1. 在 MS SQL 中创建账户。
2. 配置 SQL Server® 浏览器服务。
3. 创建密钥。
4. 配置连接器。
5. 在网络基础设施中安装收集器。
6. 在 KUMA 收集器中验证是否收到来自 MS SQL 的事件。
   您可以通过在 KUMA Web 界面中搜索相关事件来验证是否正确配置了来自 MS SQL 的事件接收。

在 MS SQL 数据库中创建账户

要从 MS SQL 接收 Kaspersky Security Center 事件，需要一个具有连接和使用数据库所需权限的用户账户。

要创建用于 MS SQL 的账户：

1. 登录安装了 Kaspersky Security Center 的 MS SQL 服务器。
2. 通过 **SQL Server Management Studio**，使用具有管理员权限的账户连接到 MS SQL。
3. 在“对象资源管理器”窗格中，展开**安全性**部分。
4. 右键单击“**登录**”文件夹，然后从上下文菜单中选择“**新建登录**”。
   打开“**登录 - 新建**”窗口。
5. 在“**常规**”选项卡上，单击“**登录名称**”字段旁边的“**搜索**”按钮。
   “**选择用户或组**”窗口将打开。
6. 在“**输入要选择的对象名称（示例）**”字段中，指定对象名称，然后单击“**确定**”。
   “**选择用户或组**”窗口将关闭。
7. 在“**登录 - 新建**”窗口的“**常规**”选项卡上，选择“**Windows 身份验证**”选项。
8. 在“**默认数据库**”字段中，选择 Kaspersky Security Center 数据库。
   默认的 Kaspersky Security Center 数据库名称是 KAV。
9. 在“**用户映射**”选项卡上，配置账户权限：
   a. 在“**映射到此登录的用户**”部分，选择 Kaspersky Security Center 数据库。
   b. 在“**数据库角色成员资格**”部分，选中“**db_datareader**”和“**public**”权限旁边的复选框。
10. 在“**状态**”选项卡上，配置将账户连接到数据库的权限：
    - 在“**连接到数据库引擎的权限**”部分，选择“**授予**”。
    - 在“**登录**”部分，选择“**启用**”。
11. 单击“**确定**”。
    “**登录 - 新建**”窗口将关闭。

要检查账户权限：

1. 使用创建的账户运行 **SQL Server Management Studio**。
2. 转到任意 MS SQL 数据库表，并根据该数据库表进行选择。

配置 SQL Server Browser 服务

在 MS SQL 中创建账户后，必须配置 SQL Server Browser 服务。

要配置 SQL Server Browser 服务：

1. 打开“**SQL Server 配置管理器**”。
2. 在左侧窗格中，选择“**SQL Server Services**”。
   服务列表将打开。
3. 通过以下方式之一打开 **SQL Server Browser** 服务属性：
   - 双击 **SQL Server Browser** 服务的名称。
   - 右键单击 **SQL Server Browser** 服务的名称，然后从上下文菜单中选择“**属性**”。
4. 在打开的**SQL Server Browser属性**窗口中，选择**服务**选项卡。
5. 在“**启动模式**”字段中，选择“**自动**”。
6. 选择“**登录**”选项卡，然后单击“**开始**”按钮。
   已启用 **SQL Server Browser** 服务的自动启动。
7. 通过执行以下操作启用并配置 **TCP/IP** 协议：
   a. 在左侧窗格中，展开“**SQL Server 网络配置**”部分，然后选择“**<SQL Server 名称> 协议**”的子部分。
   b. 右键单击“**TCP/IP**”协议，然后从上下文菜单中选择“**启用**”。
   c. 在打开的“**警告**”窗口中，单击“**确定**”。
   d. 通过以下方式之一打开“**TCP/IP**”协议属性：
      - 双击“**TCP/IP**”协议。
      - 右键单击“**TCP/IP**”协议，然后从上下文菜单中选择“**属性**”。
   e. 选择“**IP 地址**”选项卡，然后在“**IPALL**”部分的“**TCP 端口**”字段中指定端口 1433。
   f. 单击“**应用**”以保存更改。
   g. 单击“**确定**”以关闭窗口。
8. 通过执行以下操作重启“**SQL Server (<SQL Server 名称>)**”服务：
   a. 在左侧窗格中，选择“**SQL Servers Services**”。
   b. 在右侧的服务列表中，右键单击“**SQL Server (<SQL Server 名称>)**”服务，然后从上下文菜单中选择“**重启**”。
9. 在“**高级安全 Windows Defender 防火墙**”中，允许服务器通过 TCP 端口 1433 进行入站连接。

在 KUMA 中创建密钥

在 MS SQL 中创建和配置账户后，必须在 KUMA 控制台中添加密钥。此资源用于存储连接到 MS SQL 的凭证。

要创建 KUMA 密钥：

1. 在 KUMA 控制台中，打开“**资源**” → “**密钥**”部分。
   可用密钥的列表将显示。
2. 单击“**添加密钥**”按钮以创建新密钥。
   此时将显示密钥窗口。
3. 输入有关密钥的信息：
   a. 在“**名称**”字段中，选择添加的密钥的名称。
   b. 在“**租户**”下拉列表中，选择将拥有所创建资源的租户。
   c. 在“**类型**”下拉列表中，选择“**URL**”。
   d. 在“**URL**”字段中，指定以下形式的字符串：
   `sqlserver://[<域>%5C]<用户名>:<密码>@<服务器>:1433/<数据库名称>`
   其中：
   - “域”是域名。
   - `%5C` 是域/用户分隔符。代表 URL 格式的“\”字符。
   - “用户名”是创建的 MS SQL 账户的名称。
   - “密码”是创建的 MS SQL 账户的密码。
   - “服务器”是安装 Kaspersky Security Center 的 MS SQL 数据库的服务器的名称或 IP 地址。
   - “数据库名称”是 Kaspersky Security Center 数据库的名称。默认名称是 KAV。

   例如：
   `sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV`

   如果 MS SQL 数据库账户密码包含特殊字符（@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;），请将其转换为 URL 格式。
4. 单击“**保存**”按钮。

出于安全原因，保存密钥后，URL 字段中指定的字符串将被隐藏。

配置连接器

要将 KUMA 连接到 MS SQL 数据库，必须配置连接器。

要配置连接器：

1. 在 KUMA 控制台中，转到“**资源**” → “**连接器**”部分。
2. 在连接器列表中，找到“**[OOTB] KSC SQL**”连接器，并打开进行编辑。

   如果连接器不可编辑，请复制该连接器并打开其副本进行编辑。

   如果 **[OOTB] KSC SQL** 连接器不可用，请联系您的系统管理员。
3. 在**基本设置**选项卡的**URL**下拉列表中，选择为连接MS SQL数据库创建的密钥。
4. 单击“**保存**”按钮。

配置 KUMA 收集器以从 MS SQL 数据库接收 Kaspersky Security Center 事件

配置事件导出设置后，您必须在 KUMA 控制台中为从 MS SQL 接收的 Kaspersky Security Center 事件创建收集器。

有关创建 KUMA 收集器的详细信息，请参阅“创建收集器”。

在KUMA控制台中创建收集器时，请在**传输方式**步骤中选择**[OOTB] KSC SQL连接器**。

要从MS SQL接收Kaspersky Security Center事件，请在**事件解析**步骤中选择**[OOTB] KSC from SQL**规范化器。

安装 KUMA 收集器以从 MS SQL 数据库接收 Kaspersky Security Center 事件

配置收集器以从 MS SQL 接收 Kaspersky Security Center 事件后，在要接收事件的网络基础设施服务器上安装 KUMA 收集器。

有关安装 KUMA 收集器的详细信息，请参阅“在网络基础设施中安装收集器”部分。

使用 KUMA 代理 (WEC) 配置从 Windows 设备接收事件。

KUMA 允许您使用 WEC KUMA 代理接收来自 Windows 设备的事件信息。

配置事件接收包括以下步骤：

1. 配置从 Windows 设备接收事件的策略。
2. 使用 Windows 事件收集器服务配置事件的集中接收。
3. 授予查看事件的权限。
4. 授予作为服务登录的权限。
5. 配置 KUMA 收集器。
6. 安装 KUMA 收集器。
7. 将事件从 Windows 设备转发到 KUMA。

配置来自 Windows 设备的事件审计

您可以为单个设备或域中的所有设备配置 Windows 设备的事件审计。

本部分介绍了如何在单个设备上配置审计以及如何使用域组策略配置审计。

在 Windows 设备上配置审计策略

要在设备上配置审计策略：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `secpol.msc`，然后单击“**确定**”。
   将打开“**本地安全策略**”窗口。
3. 选择“**安全设置**” → “**本地策略**” → “**审计策略**”。
4. 在右侧窗格中，双击打开要启用成功和失败尝试审计的策略的属性窗口。
5. 在“**<策略名称> 属性**”窗口的“**本地安全设置**”选项卡上，选中“**成功**”和“**失败**”复选框以追踪成功和中断的尝试。
   建议为以下策略启用成功尝试和失败尝试的审计：
   - 审计登录
   - 审计策略更改
   - 审计系统事件

- 审计登录事件
- 审计账户管理

设备上的审计策略配置已完成。

使用组策略配置审计

除了在单个设备上配置审计策略外，您还可以使用域组策略来配置审计。

要使用组策略配置审计：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `gpedit.msc`，然后单击“**确定**”。
   将打开“**本地组策略编辑器**”窗口。
3. 选择“**计算机配置**” → “**Windows 配置**” → “**安全设置**” → “**本地策略**” → “**审计策略**”。
4. 在右侧窗格中，双击打开要启用成功和失败尝试审计的策略的属性窗口。
5. 在“**<策略名称> 属性**”窗口的“**本地安全设置**”选项卡上，选中“**成功**”和“**失败**”复选框以追踪成功和中断的尝试。
   建议为以下策略启用成功尝试和失败尝试的审计：
   - 审计登录
   - 审计策略更改
   - 审计系统事件
   - 审计登录事件
   - 审计账户管理

> 如果您要从大量服务器接收 Windows 日志，或者不允许在域控制器上安装 KUMA 代理，建议将 Windows 日志重定向配置到已配置 Windows 事件收集器服务的独立服务器。

现已在服务器或工作站上配置了审计策略。

使用 Windows 事件收集器服务配置从 Windows 设备集中接收事件

Windows 事件收集器服务支持集中接收有关运行 Windows 的服务器和工作站上的事件的数据。您可以使用 Windows 事件收集器服务订阅在远程设备上注册的事件。

您可以配置以下类型的事件订阅：

- **源发起的订阅**。远程设备将事件数据发送到组策略中指定地址的 Windows 事件收集器服务器。有关订阅配置过程的详细信息，请参阅“配置从事件源服务器传输数据”部分。
- **收集器发起的订阅**。Windows 事件收集器服务器连接到远程设备并独立地从本地日志收集事件。有关订阅配置过程的详细信息，请参阅“配置 Windows 事件收集器服务”部分。

配置从事件源服务器的数据传输

您可以通过配置从远程设备到 Windows 事件收集器服务器的数据传输，接收有关服务器和工作站的事件信息。

准备步骤

1. 通过在 PowerShell 控制台中运行以下命令验证是否在事件源服务器上配置了 Windows 远程管理服务：

   ```
   winrm get winrm/config
   ```

   如果未配置 Windows 远程管理服务，请运行以下命令对其进行初始化：

   ```
   winrm quickconfig
   ```

2. 如果事件源服务器是域控制器，请以管理员身份在 PowerShell 中运行以下命令，使 Windows 日志可通过网络访问：

   ```
   wevtutil set-log security /ca:’O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)
   ```

   通过运行以下命令验证访问权限：

   ```
   wevtutil get-log security
   ```

在事件源服务器上配置防火墙

要使 Windows 事件收集器服务器能够接收 Windows 日志条目，必须在事件源服务器上打开入站连接端口。

要为入站连接打开端口，请执行以下操作：

1. 在事件源服务器上，按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `wf.msc`，然后单击“**确定**”。
   将打开“**高级安全 Windows Defender 防火墙**”窗口。
3. 转到“**入站规则**”部分，然后单击“**操作**”窗格中的“**新建规则**”。
   将打开“**新建入站规则向导**”。
4. 在“**规则类型**”步骤中，选择“**端口**”。
5. 在“**协议和端口**”步骤中，选择“**TCP**”作为协议。在“**特定本地端口**”字段中，指示相关端口号：

   - `5985`（用于 HTTP 访问）
   - `5986`（用于 HTTPS 访问）

   您可以指定其中一个端口，或同时指定两个端口。
6. 在“**操作**”步骤中，选择“**允许连接**”（默认选择）。
7. 在“**配置文件**”步骤中，清除“**私有**”和“**公共**”复选框。
8. 在“**名称**”步骤中，指定新入站连接规则的名称，然后单击“**完成**”。

从事件源服务器传输数据的配置已完成。

Windows 事件收集器服务器必须具有读取事件源服务器上的 Windows 日志的权限。这些权限可以分配给 Windows 事件收集器服务器账户和特殊用户账户。有关授予权限的详细信息，请参阅“授予用户查看 Windows 事件日志的权限”。

配置 Windows 事件收集器服务

Windows 事件收集器服务器可以独立连接到设备并收集任何严重级别事件的数据。

要配置 Windows 事件收集器服务器接收事件数据：

1. 在事件源服务器上，按 **Win** + **R** 键以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `services.msc`，然后单击“**OK**”。
   “**服务**”窗口将打开。
3. 在服务列表中，找到并启动“**Windows 事件收集器**”服务。
4. 通过执行以下操作打开“**事件查看器**”管理单元：
   a. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
   b. 在打开的窗口中，输入 `eventvwr`，然后单击“**确定**”。
5. 转到“**订阅**”部分，然后单击“**操作**”窗格中的“**创建订阅**”。
6. 在打开的“**订阅属性**”窗口中，指定订阅的名称和描述，并定义以下设置：
   a. 在“**目标位置日志**”字段中，从列表中选择“**转发的事件**”。
   b. 在“**订阅类型和源计算机**”部分中，单击“**选择计算机**”按钮。
   c. 在打开的“**计算机**”窗口中，单击“**添加域计算机**”按钮。
   “**选择计算机**”窗口将打开。
   d. 在“**输入要选择的对象名称（示例）**”字段中，列出要从中接收事件信息的设备名称。单击“**确定**”。
   e. 在“**计算机**”窗口中，检查 Windows 事件收集器服务器将从中收集事件数据的设备列表，然后单击“**确定**”。
   f. 在“**订阅属性**”窗口的“**收集的事件**”字段中，单击“**选择事件**”按钮。
   g. 在打开的“**请求过滤器**”窗口中，指定要接收设备事件数据的频率和类型。
   h. 如有必要，在“**<所有事件代码>**”字段中，列出您希望接收或不希望接收其信息的事件代码。单击“**确定**”。

7. 如果想使用特殊账户查看事件数据，请执行以下操作：

   a. 在“**订阅属性**”窗口中，单击“**高级**”按钮。

   b. 在打开的“**高级订阅设置**”窗口，在“用户账户设置”中选择“**特定用户**”。

   c. 单击“**用户和密码**”按钮，输入所选用户的账户凭证。

事件收集器服务配置已完成。

要验证配置是否正确以及 Windows 事件收集器服务器是否正在接收事件数据：

在“**事件查看器**”管理单元中，转至“**事件查看器（本地）**” → “**Windows 日志**” → “**转发的事件**”。

授予查看 Windows 事件的权限

您可以授予查看特定设备或域中所有设备的 Windows 事件的权限。

要授予查看特定设备上的事件的权限：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `compmgmt.msc`，然后单击“**确定**”。
   将打开“**计算机管理**”窗口。
3. 转至“**计算机管理（本地）**” → “**本地用户和组**” → “**组**”。
4. 在右侧窗格中，选择“**事件日志读取者**”组，然后双击打开策略属性。
5. 单击“**属性：事件日志读取者**”窗口底部的“**添加**”按钮。
   “**选择用户、计算机或组**”窗口将打开。
6. 在“**输入对象名称来选择（示例）**”字段中，列出您要授予其查看事件数据权限的用户或设备的名称。单击“**确定**”。

要授予查看域中所有设备的事件的权限：

1. 使用管理员权限登录到域控制器。
2. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
3. 这将打开一个窗口；在该窗口中，输入 `dsa.msc`，然后单击“**确定**”。
   将打开“**Active Directory 用户和计算机**”窗口。
4. 前往“**Active Directory 用户和计算机**” → “**<域名>**” → “**内置**”。
5. 在右侧窗格中，选择“**事件日志读取者**”组，然后双击打开策略属性。
   在“**属性：事件日志读取者**”窗口中，打开“**成员**”选项卡并单击“**添加**”按钮。
   “**选择用户、计算机或组**”窗口将打开。
6. 在“**输入对象名称来选择（示例）**”字段中，列出您要授予其查看事件数据权限的用户或设备的名称。单击“**确定**”。

授予作为服务登录的权限

您可以向特定设备或域中的所有设备授予作为服务登录的权限。“**作为服务登录**”权限允许您使用已获得此权限的账户启动进程。

*要向设备授予“**作为服务登录**”权限：*

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `secpol.msc`，然后单击“**确定**”。
   将打开“**本地安全策略**”窗口。
3. 转到“**安全设置**” → “**本地策略**” → “**用户权限分配**”。
4. 在右侧窗格中，双击打开“**作为服务登录**”策略的属性窗口。
5. 在打开的“**属性：作为服务登录**”窗口中，单击“**添加用户或组**”按钮。
   “**选择用户或组**”窗口将打开。
6. 在“**输入要选择的对象名称（示例）**”字段中，列出要授予作为服务登录权限的账户或设备的名称。单击“**确定**”。

> 在授予权限之前，请确保要授予“**作为服务登录**”权限的账户或设备未在“**拒绝作为服务登录**”策略的属性中列出。

*要向域中的设备授予“**作为服务登录**”权限：*

1. 按组合键 “**Win**” + “**R**”以 打开“**运行**”窗口。
2. 在打开的窗口中，输入 `gpedit.msc`，然后单击“**确定**”。
   将打开“**本地组策略编辑器**”窗口。
3. 选择“**计算机配置**” → “**Windows 配置**” → “**安全设置**” → “**本地策略**” → “**用户权限分配**”。
4. 在右侧窗格中，双击打开“**作为服务登录**”策略的属性窗口。
5. 在打开的“**属性：作为服务登录**”窗口中，单击“**添加用户或组**”按钮。
   “**选择用户或用户组**”窗口将打开。
6. 在“**输入要选择的对象名称（示例）**”字段中，列出要授予其作为服务登录权限的用户或设备的名称。单击“**确定**”。

> 在授予权限之前，请确保要授予“**作为服务登录**”权限的账户或设备未在“**拒绝作为服务登录**”策略的属性中列出。

配置 KUMA 收集器以接收来自 Windows 设备的事件

完成配置设备审核策略、创建事件订阅和授予所有必要的权限后，您需要在 KUMA 控制台中为来自 Windows 设备的事件创建一个收集器。

有关创建 KUMA 收集器的详细信息，请参阅“创建收集器”。

要从 Windows 设备接收事件，请在“KUMA 收集器安装向导”中定义以下收集器设置：

1. 在“**传输方式**”步骤中，定义以下设置：
   a. 在**连接器**窗口中，选择**创建**。
   b. 在“**类型**”字段中，选择“**http**”。
   c. 在“**分隔符**”字段中，选择“**\0**”。
2. 在**高级设置**选项卡上，在**TLS模式**字段中，选择**带验证**。
3. 在**事件解析**步骤中，单击**添加事件解析**按钮。
4. 在打开的**事件基础解析**窗口的**规范化器**字段中，选择**[OOTB] Windows Extended v.1.0**并单击**确定**。
5. 在“**路由**”步骤中，添加以下目标位置：
   - **存储**。将处理过的事件发送到存储。
   - **关联器**。将处理过的事件发送到关联器。

   如果未添加“**存储**”和“**关联器**”目标位置，请进行创建。
6. 在“**设置验证**”选项卡上，单击“**创建并保存服务**”。
7. 复制出现的安装 KUMA 收集器的命令。

安装 KUMA 收集器以从 Windows 设备接收事件

配置收集器以接收 Windows 事件后，在用于接收事件的网络基础设施的服务器上安装 KUMA 收集器。

有关安装 KUMA 收集器的详细信息，请参阅“在网络基础设施中安装收集器”部分。

使用 KUMA 代理 (WEC) 配置从 Windows 设备到 KUMA 的事件转发

要完成数据转发配置，您必须创建 WEC KUMA 代理，然后将其安装在需要从中接收事件信息的设备上。

有关在 Windows 设备上创建和安装 WEC KUMA 代理的更多详细信息，请参阅“将事件从 Windows 设备转发到 KUMA”部分。

使用 KUMA 代理 (WMI) 配置从 Windows 设备接收事件

KUMA 支持使用 WMI KUMA 代理接收来自 Windows 设备的事件信息。

配置事件接收包括以下步骤：

1. 配置用于管理 KUMA 的审计设置。
2. 配置从事件源服务器的数据传输。
3. 授予查看事件的权限。
4. 授予作为服务登录的权限。
5. 创建 KUMA 收集器。

   要从Windows设备接收事件，请在KUMA收集器安装向导的**事件解析**步骤中，在**规范化器**字段中选择**[OOTB] Windows Extended v.1.0**。
6. 安装 KUMA 收集器。
7. 将事件从 Windows 设备转发到 KUMA。

   要完成数据转发配置，您必须创建一个 WMI KUMA 代理，然后将其安装在需要接收事件信息的设备上。

配置用于管理 KUMA 的审计设置

您可以在 Windows 设备上使用本地策略在特定设备上配置审计事件，也可以使用组策略在域中的所有设备上配置审计事件。

本节介绍了如何在单个设备上配置审计以及如何使用域组策略配置审计。

使用本地策略配置审计

要使用本地策略配置审计：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `secpol.msc`，然后单击“**确定**”。

   将打开“**本地安全策略**”窗口。
3. 选择“**安全设置**” → “**本地策略**” → “**审计策略**”。
4. 在右侧窗格中，双击打开要启用成功和失败尝试审计的策略的属性窗口。
5. 在“**<策略名称> 属性**”窗口的“**本地安全设置**”选项卡上，选中“**成功**”和“**失败**”复选框以追踪成功和中断的尝试。

建议为以下策略启用成功尝试和失败尝试的审计：

- 审计登录
- 审计策略更改
- 审计系统事件
- 审计登录事件
- 审计账户管理

设备上的审计策略配置已完成。

使用组策略配置审计

除了在单个设备上配置审计之外，您还可以使用域组策略配置审计。

要使用组策略配置审计：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `gpedit.msc`，然后单击“**确定**”。
   将打开“**本地组策略编辑器**”窗口。
3. 选择“**计算机配置**” → “**Windows 配置**” → “**安全设置**” → “**本地策略**” → “**审计策略**”。
4. 在右侧窗格中，双击打开要启用成功和失败尝试审计的策略的属性窗口。
5. 在“**<策略名称> 属性**”窗口的“**本地安全设置**”选项卡上，选中“**成功**”和“**失败**”复选框以追踪成功和中断的尝试。
   建议为以下策略启用成功尝试和失败尝试的审计：
   - 审计登录
   - 审计策略更改
   - 审计系统事件
   - 审计登录事件
   - 审计账户管理

现已在服务器或工作站上配置了审计策略。

配置从事件源服务器的数据传输

准备步骤

1. 在事件源服务器上，按组合键“**Win**” + “**R**”以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `services.msc`，然后单击“**OK**”。
   “**服务**”窗口将打开。
3. 在服务列表中，找到以下服务：
   - 远程过程调用
   - RPC 端点映射器
4. 检查“**状态**”列以确认这些服务具有“**正在运行**”状态。

在事件源服务器上配置防火墙

如果事件源服务器上的端口已开放用于入站连接，Windows Management Instrumentation 服务器便可以接收 Windows 日志条目。

要为入站连接打开端口，请执行以下操作：

1. 在事件源服务器上，按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `wf.msc`，然后单击“**确定**”。
   将打开“**高级安全 Windows Defender 防火墙**”窗口。
3. 在“**高级安全 Windows Defender 防火墙**”窗口中，转到“**入站规则**”部分，然后在“**操作**”窗格中单击“**新建规则**”。
   将打开“**新建入站规则向导**”。
4. 在“**新建入站规则向导**”的“**规则类型**”步骤中，选择“**端口**”。
5. 在“**协议和端口**”步骤中，选择“**TCP**”作为协议。在“**特定本地端口**”字段中，指示相关端口号：
   - `135`
   - `445`
   - `49152-65535`
6. 在“**操作**”步骤中，选择“**允许连接**”（默认选择）。

7. 在“**配置文件**”步骤中，清除“**私有**”和“**公共**”复选框。

8. 在“**名称**”步骤中，指定新入站连接规则的名称，然后单击“**完成**”。

从事件源服务器传输数据的配置已完成。

授予查看 Windows 事件的权限

您可以授予查看特定设备或域中所有设备的 Windows 事件的权限。

要授予查看特定设备上的事件的权限：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。

2. 在打开的窗口中，输入 `compmgmt.msc`，然后单击“**确定**”。
   将打开“**计算机管理**”窗口。

3. 转至“**计算机管理（本地）**” → “**本地用户和组**” → “**组**”。

4. 在右侧窗格中，选择“**事件日志读取者**”组，然后双击打开策略属性。

5. 单击“**属性：事件日志读取者**”窗口底部的“**添加”**按钮。
   “**选择用户、计算机或组**”窗口将打开。

6. 在“**输入对象名称来选择（示例）**”字段中，列出您要授予其查看事件数据权限的用户或设备的名称。单击“**确定**”。

要授予查看域中所有设备的事件的权限：

1. 使用管理员权限登录到域控制器。

2. 按组合键 **Win** + **R** 以打开“**运行**”窗口。

3. 这将打开一个窗口；在该窗口中，输入 `dsa.msc`，然后单击“**确定**”。
   将打开“Active Directory **用户和计算机**”窗口。

4. 在“Active Directory **用户和计算机**”窗口中，转到“Active Directory **用户和计算机**”部分 → “**<域名>**” → “**内置**”。

5. 在右侧窗格中，选择“**事件日志读取者**”组，然后双击打开策略属性。
   在“**属性：事件日志读取者**”窗口中，打开“**成员**”选项卡并单击“**添加**”按钮。
   “**选择用户、计算机或组**”窗口将打开。

6. 在“**选择用户、计算机或组**”窗口中，在“**输入对象名称来选择（示例）**”字段中，列出您要授予其查看事件数据权限的用户或设备的名称。单击“**确定**”。

授予作为服务登录的权限

您可以向特定设备或域中的所有设备授予作为服务登录的权限。“**作为服务登录**”权限允许您使用已获得此权限的账户启动进程。

在授予权限之前，请确保要授予“**作为服务登录**”权限的账户或设备未在“**拒绝作为服务登录**”策略的属性中列出。

要向设备授予“作为服务登录”权限：

1. 按组合键 **Win** + **R** 以打开“**运行**”窗口。
2. 在打开的窗口中，输入 `secpol.msc`，然后单击“**确定**”。
   将打开“**本地安全策略**”窗口。
3. 在“**本地安全策略**”窗口中，转到“**安全设置**” → “**本地策略**” → “**用户权限分配**”部分。
4. 在右侧窗格中，双击打开“**作为服务登录**”策略的属性窗口。
5. 将打开“**属性：作为服务登录**”窗口；在该窗口中，单击“**添加用户或组**”。
   将打开“**选择用户或组**”窗口。
6. 在“**输入要选择的对象名称（示例）**”字段中，列出要授予作为服务登录权限的账户或设备的名称。单击“**确定**”。

要向域中的设备授予“作为服务登录”权限：

1. 按组合键 “**Win**” + “**R**”以 打开“**运行**”窗口。
2. 在打开的窗口中，输入 `gpedit.msc`，然后单击“**确定**”。
   将打开“**本地组策略编辑器**”窗口。
3. 选择“**计算机配置**” → “**Windows 配置**” → “**安全设置**” → “**本地策略**” → “**用户权限分配**”。
4. 在右侧窗格中，双击打开“**作为服务登录**”策略的属性窗口。
5. 将打开“**属性：作为服务登录**”窗口；在该窗口中，单击“**添加用户或组**”。
   将打开“**选择用户或组**”窗口。
6. 在“**输入要选择的对象名称（示例）**”字段中，列出要授予其作为服务登录权限的用户或设备的名称。单击“**确定**”。

配置 PostgreSQL 事件接收

KUMA 允许您使用 rsyslog 监控和审计 Linux 设备上的 PostgreSQL 审计事件。

使用 pgAudit 插件审计事件。该插件支持 PostgreSQL 9.5 及更高版本。有关 pgAudit 插件的详细信息，请参阅 https://github.com/pgaudit/pgaudit。

配置事件接收包括以下步骤：

1. 安装 pdAudit 插件。
2. 为 PostgreSQL 事件创建 KUMA 收集器。
   要使用 rsyslog 接收 PostgreSQL 事件，请在收集器安装向导的“**事件解析**”步骤中，选择 **[OOTB] PostgreSQL pgAudit syslog** 标准化器。

3. 在 KUMA 网络基础设施中安装收集器。

4. 配置事件源服务器。

5. 验证 KUMA 收集器中 PostgreSQL 事件的接收
   您可以在 KUMA 控制台的"搜索相关事件"部分验证 PostgreSQL 事件源服务器是否已正确配置。

安装 pgAudit 插件

要安装 pgAudit 插件：

1. 在 OS 命令行上，以具有管理员权限的用户身份运行以下命令：

   ```
   sudo apt update
   sudo apt -y install postgresql-<PostgreSQL version>-pgaudit
   ```

   您必须选择与 PostgreSQL 版本匹配的插件版本。有关 PostgreSQL 版本及其匹配插件版本的信息，请参阅 https://github.com/pgaudit/pgaudit#postgresql-version-compatibility。

   例如：
   ```
   sudo apt -y install postgresql-12-pgaudit
   ```

2. 查找 postgres.conf 配置文件。为此，请在 PostgreSQL 命令行中运行以下命令：

   ```
   show data_directory
   ```

   响应将指示配置文件的位置。

3. 创建 postgres.conf 配置文件的备份副本。

4. 打开 postgres.conf 文件并将其中的值复制或替换为下面列出的值。

   ```
   ## pgAudit settings
   shared_preload_libraries = 'pgaudit'
   ## database logging settings
   log_destination = 'syslog'
   ## syslog facility
   syslog_facility = 'LOCAL0'
   ## event ident
   syslog_ident = 'Postgres'
   ## sequence numbers in syslog
   syslog_sequence_numbers = on
   ## split messages in syslog
   syslog_split_messages = off
   ## message encoding
   lc_messages = 'en_US.UTF-8'
   ## min message level for logging
   client_min_messages = log
   ## min error message level for logging
   ```

```
log_min_error_statement = info
## log checkpoints (buffers, restarts)
log_checkpoints = off
## log query duration
log_duration = off
## error description level
log_error_verbosity = default
## user connections logging
log_connections = on
## user disconnections logging
log_disconnections = on
## log prefix format
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
## log_statement
log_statement = 'none'
## hostname logging status&period; dns bane resolving affect
#performance!
log_hostname = off
## logging collector buffer status
#logging_collector = off
## pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```

5. 使用以下命令重启 PostgreSQL 服务：
   ```
   sudo systemctl restart postgresql
   ```
6. 要将 pgAudit 插件加载到 PostgreSQL，请在 PostgreSQL 命令行上运行以下命令：
   ```
   CREATE EXTENSION pgaudit
   ```

pgAudit 插件已安装。

配置 Syslog 服务器以发送事件

rsyslog 服务用于将事件从服务器传输到 KUMA。

要配置从安装了 PostgreSQL 的服务器向收集器发送事件：

1. 要验证事件源服务器上是否安装了 rsyslog 服务，请以管理员身份运行以下命令：
   ```
   sudo systemctl status rsyslog.service
   ```

如果服务器上尚未安装 rsyslog 服务，请执行以下命令进行安装：

- 对于基于 RPM 的发行版：

  ```
  yum install rsyslog
  ```

- 对于基于 Debian 或 Ubuntu 的发行版：

  ```
  apt-get install rsyslog
  ```

通过执行以下命令启用该服务：

```
sudo systemctl enable rsyslog.service
sudo systemctl start rsyslog.service
```

2. 在 /etc/rsyslog.d/ 目录中，创建一个 pgsql-to-siem.conf 文件，其中包含以下内容：

   ```
   If $programname contains 'Postgres' then @<收集器的 IP 地址>:<收集器的端口>
   For example:
   If $programname contains 'Postgres' then @192.168.1.5:1514
   ```

   如果要通过 TCP 发送事件，则文件的内容必须如下：

   ```
   If $programname contains 'Postgres' then @@192.168.1.5:2514
   ```

   将更改保存到 pgsql-to-siem.conf 配置文件。

3. 将以下行添加到 /etc/rsyslog.conf 配置文件：

   ```
   $IncludeConfig /etc/pgsql-to-siem.conf
   $RepeatedMsgReduction off
   ```

   将更改保存到 /etc/rsyslog.conf 配置文件。

4. 重新启动 rsyslog 服务：

   ```
   sudo systemctl restart rsyslog.service
   ```

配置接收 IVK Kolchuga-K 事件

您可以配置从 IVK Kolchuga-K 系统接收事件到 KUMA SIEM 系统。

配置事件接收包括以下步骤：

1. 配置将 IVK Kolchuga-K 事件发送到 KUMA。
2. 创建用于接收来自 IVK Kolchuga-K 系统的事件的 KUMA 收集器。

   要使用Syslog接收IVK Kolchuga-K事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] Kolchuga-K syslog**规范化器。

3. 安装 KUMA 收集器以接收 IVK Kolchuga-K 事件。
4. 验证 KUMA 中 IVK Kolchuga-K 事件的接收情况。

   您可以在 KUMA 控制台的“搜索相关事件”部分验证 IVK Kolchuga-K 事件源是否配置正确。

配置将 IVK Kolchuga-K 事件导出到 KUMA

要配置通过 syslog 将 IVK Kolchuga-K 防火墙事件导出到 KUMA 收集器：

1. 使用管理员权限通过 SSH 连接到防火墙。
2. 创建 /etc/services 和 /etc/syslog.conf 文件的备份副本。
3. 在 /etc/syslog.conf 配置文件中，指定 KUMA 收集器的 FQDN 或 IP 地址。例如：

   . @kuma.example.com

   或

   . @192.168.0.100

   保存对配置文件 /etc/syslog.conf 的更改。
4. 在 /etc/services 配置文件中，指定 KUMA 收集器使用的端口和协议。例如：

   syslog 10514/udp

   保存对 /etc/services 配置文件的更改。
5. 重启防火墙的 syslog 服务器：

   ```
   service syslogd restart
   ```

配置 CryptoPro NGate 事件的接收

您可以在 KUMA SIEM 系统中配置 CryptoPro NGate 事件的接收。

配置事件接收包括以下步骤：

1. 配置将 CryptoPro NGate 事件导出至 KUMA。
2. 创建用于接收 CryptoPro NGate 事件的 KUMA 收集器。

   要使用 Syslog 接收 CryptoPro NGate 事件，请在收集器安装向导的**事件解析**步骤中，选择**[OOTB] NGate syslog**标准化器。
3. 创建用于接收 CryptoPro NGate 事件的 KUMA 收集器。
4. 验证 KUMA 收集器中 CryptoPro NGate 事件的接收情况。

   您可以在 KUMA 控制台的“搜索相关事件”部分验证 CryptoPro NGate 事件源服务器是否配置正确。

配置将 CryptoPro NGate 事件导出至 KUMA

要配置将事件从 CryptoPro NGate 发送到 KUMA：

1. 连接 NGate 管理系统的 Web 界面。
2. 将远程 syslog 服务器连接到管理系统。为此请执行以下操作：
   a. 打开包含 syslog 服务器列表的页面：**外部服务** → **Syslog 服务器** → **添加 Syslog 服务器**。
   b. 输入 syslog 服务器的设置，然后单击 ✔。
3. 将 syslog 服务器分配到配置中以记录集群的日志。为此请执行以下操作：
   a. 在“**集群** → **摘要**”部分，选择要配置的集群。
   b. 在“**配置选项**”选项卡上，单击相关集群的“**配置**”控件，转到配置设置页面。
   c. 在当前配置的“**Syslog 服务器**”字段中，单击“**分配**”。
   d. 选中要分配的 Syslog 服务器的复选框，然后单击 ✔。
   您可以分配无限数量的服务器。
   要添加新的 syslog 服务器，请单击 ✚。
   e. 发布配置以激活新设置。
4. 将 syslog 服务器分配至管理系统，用于记录管理员活动日志。为此请执行以下操作：
   a. 选择“**管理中心设置**”菜单项，然后在所显示页面的“**Syslog 服务器**”下，单击“**分配**”。
   b. 在“**将 Syslog 服务器分配至管理中心**”窗口中，选中要分配的 syslog 服务器的复选框，然后单击 ☁。
   您可以分配无限数量的服务器。

这样一来，CryptoPro NGate 的事件将被发送到 KUMA。

配置 Ideco UTM 事件的接收

您可以通过 Syslog 协议，在 KUMA 中配置 Ideco UTM 应用程序事件的接收。

配置事件接收包括以下步骤：

1. 配置将 Ideco UTM 事件导出至 KUMA。
2. 创建用于接收 Ideco UTM 的 KUMA 收集器。
   要接收Ideco UTM事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] Ideco UTM syslog**规范化器。
3. 创建用于接收 Ideco UTM 事件的 KUMA 收集器。

4. 验证 KUMA 中 Ideco UTM 事件的接收情况。
   您可以在 KUMA 控制台的"搜索相关事件"部分验证 Ideco UTM 事件源服务器是否配置正确。

配置将 Ideco UTM 事件导出至 KUMA

要配置将事件从 Ideco UTM 发送到 KUMA：

1. 使用具有管理员权限的用户帐户连接到 Ideco UTM Web 界面。
2. 在"**系统消息转发**"菜单中，将"**Syslog**"切换开关移到"**已启用**"位置。
3. 对于"**IP 地址**"设置，指定 KUMA 收集器的 IP 地址。
4. 对于端口设置，输入 KUMA 收集器正在监听的端口。
5. 单击"**保存**"以应用更改。

已配置将 Ideco UTM 事件传输到 KUMA。

配置 KWTS 事件的接收

您可以在 KUMA 中配置从 Kaspersky Web Traffic Security (KWTS) Web 流量分析和过滤系统接收事件。

配置事件接收包括以下步骤：

1. 配置将 KWTS 事件导出至 KUMA。
2. 创建用于接收 KWTS 事件的 KUMA 收集器。
   要接收KWTS事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] KWTS**规范化器。
3. 安装用于接收 KWTS 事件的 KUMA 收集器。
4. 验证 KUMA 收集器中 KWTS 事件的接收情况。
   您可以在 KUMA 控制台的"搜索相关事件"部分中验证 KWTS 事件导出是否正确配置。

配置将 KWTS 事件导出至 KUMA

要配置将 KWTS 事件导出至 KUMA：

1. 以根用户身份通过 SSH 连接到 KWTS 服务器。
2. 在进行更改之前，请创建以下文件的备份副本：
   - /opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template
   - /etc/rsyslog.conf

3. 确保 /opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template 配置文件中的设置具有以下值，并在必要时进行更改：

```
"siemSettings":
{
"enabled": true,
"facility": "Local5",
"logLevel": "Info",
"formatting":
{
```

4. 保存更改。

5. 要通过 UDP 发送事件，请对 /etc/rsyslog.conf 配置文件进行以下更改：

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local5.* @<< KUMA 收集器的 IP 地址 >:< 收集器的端口 >>
```

如果要通过 TCP 发送事件，最后一行应如下所示：

```
local5.* @@<< KUMA 收集器的 IP 地址 >:< 收集器的端口 >>
```

6. 保存更改。

7. 使用以下命令重新启动 rsyslog 服务：

```
sudo systemctl restart rsyslog.service
```

8. 进入 KWTS Web 界面，转到“**设置**” - “**Syslog**”选项卡，然后启用“**有关流量配置文件的日志信息**”选项。

9. 单击“**保存**”按钮。

配置 KLMS 事件的接收

您可以配置从 Kaspersky Linux Mail Server (KLMS) 邮件流量分析和过滤系统接收事件并发送至 KUMA SIEM 系统 。

配置事件接收包括以下步骤：

1. 配置将 KLMS 事件导出至 KUMA

2. 创建用于接收 KLMS 事件的 KUMA 收集器

   要接收 KLMS 事件，请在收集器安装向导的**事件解析**步骤中，选择 **[OOTB] KLMS syslog CEF 规范化器**。

3. 安装用于接收 KLMS 事件的 KUMA 收集器

4. 验证 KUMA 收集器中 KLMS 事件的接收情况

   您可以在 KUMA 控制台的"搜索相关事件"部分验证 KLMS 事件源服务器是否配置正确。

配置将 KLMS 事件导出至 KUMA

要配置将 KLMS 事件导出至 KUMA：

1. 通过 SSH 连接 KLMS 服务器并转到"**技术支持模式**"菜单。

2. 使用 klms-control 实用程序将设置下载到 settings.xml 文件中：

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f
   /tmp/settings.xml
   ```

3. 确保 /tmp/settings.xml 文件中的设置具有以下值；如有必要，请进行更改：

   ```
   <siemSettings>
   <enabled>1</enabled>
   <facility>Local1</facility>
   ...
   </siemSettings>
   ```

4. 使用以下命令来应用设置：

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```

5. 要通过 UDP 发送事件，请对 /etc/rsyslog.conf 配置文件进行以下更改：

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local1.* @<< KUMA 收集器的 IP 地址 >:< 收集器的端口 >>
   ```

   如果要通过 TCP 发送事件，最后一行应如下所示：

   ```
   local1.* @@<< KUMA 收集器的 IP 地址 >:< 收集器的端口 >>
   ```

6. 保存更改。

7. 使用以下命令重新启动 rsyslog 服务：

   ```
   sudo systemctl restart rsyslog.service
   ```

配置 KSMG 事件的接收

您可以在 KUMA SIEM 系统中配置从 Kaspersky Secure Mail Gateway (KSMG) 1.1 邮件流量分析和过滤系统接收事件。

配置事件接收包括以下步骤：

1. 配置将 KSMG 事件导出至 KUMA
2. 创建用于接收 KSMG 事件的 KUMA 收集器

   要接收KSMG事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] KSMG**规范化器。
3. 安装用于接收 KSMG 事件的 KUMA 收集器
4. 验证 KUMA 收集器中 KSMG 事件的接收情况

   您可以在 KUMA 控制台的"搜索相关事件"部分验证 KSMG 事件源服务器是否已正确配置。

配置将 KSMG 事件导出至 KUMA

要配置将 KSMG 事件导出至 KUMA：

1. 使用具有管理员权限的账户，通过 SSH 连接 KSMG 服务器。
2. 使用 ksmg-control 实用程序将设置下载到 settings.xml 文件：

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-control --get-settings EventLogger -n -f
   /tmp/settings.xml
   ```
3. 确保 /tmp/settings.xml 文件中的设置具有以下值；如有必要，请进行更改：

   ```
   <siemSettings>
   <enabled>1</enabled>
   <facility>Local1</facility>
   ```
4. 使用以下命令来应用设置：

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```
5. 要通过 UDP 发送事件，请对 /etc/rsyslog.conf 配置文件进行以下更改：

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local1.* @<< KUMA 收集器的 IP 地址 >:< 收集器的端口 >>
   ```

   如果要通过 TCP 发送事件，最后一行应如下所示：

   ```
   local1.* @@<< KUMA 收集器的 IP 地址 >:< 收集器的端口 >>
   ```
6. 保存更改。
7. 使用以下命令重新启动 rsyslog 服务：

   ```
   sudo systemctl restart rsyslog.service
   ```

配置 PT NAD 事件的接收

您可以在 KUMA SIEM 系统中配置 PT NAD 事件的接收。

配置事件接收包括以下步骤：

1. 配置将 PT NAD 事件导出至 KUMA。
2. 创建用于接收 PT NAD 事件的 KUMA 收集器。
   要使用Syslog接收PT NAD事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] PT NAD json**规范化器。
3. 安装用于接收 PT NAD 事件的 KUMA 收集器。
4. 验证 KUMA 收集器中 PT NAD 事件的接收情况。
   您可以在 KUMA 控制台的“搜索相关事件”部分验证 PT NAD 事件源服务器是否已正确配置。

配置将 PT NAD 事件导出至 KUMA

配置通过 Syslog 将事件从 PT NAD 11 导出到 KUMA 涉及以下步骤：

1. 配置 ptdpi-worker@notifier 模块。
2. 配置发送包含活动、攻击和入侵指标信息的 syslog 消息。

配置 ptdpi-worker@notifier 模块。

要启用检测到的信息安全威胁相关信息的发送功能，您必须配置 ptdpi-worker@notifier 模块。

在多服务器配置中，必须在主服务器上遵循这些说明。

要配置 ptdpi-worker@notifier 模块：

1. 打开 /opt/ptsecurity/etc/ptdpi.settings.yaml 文件：
   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```
2. 在“**常规设置**”设置组中，取消对“workers”的注释，并将“notifier”添加到其值列表中。
   例如：
   ```
   workers: ad alert dns es hosts notifier
   ```
3. 在文件末尾添加一行代码，格式如下：notifier.yaml.nad_web_url: <PT NAD 控制台的 URL>
   例如：
   ```
   notifier.yaml.nad_web_url: https://ptnad.example.com
   ```
   ptdpi-worker@notifier 模块在发送消息时使用指定的 URL 生成会话和活动卡的链接。

4. 重新启动传感器：

```
sudo ptdpictl restart-all
```

ptdpi-worker@notifier 模块已配置。

配置发送包含活动、攻击和入侵指标信息的 syslog 消息

配置文件中可能不存在以下说明中列出的设置。如果缺少某个设置，则必须将其添加到文件中。

在多服务器 PT NAD 配置中，编辑主服务器上的设置。

要配置发送包含活动、攻击和入侵指标信息的 syslog 消息：

1. 打开 /opt/ptsecurity/etc/ptdpi.settings.yaml 文件：

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. 默认情况下，PT NAD 以俄语发送活动信息。要接收英文信息，请将 notifier.yaml.syslog_notifier.locale 设置的值更改为 `en`。

   例如：

   ```
   notifier.yaml.syslog_notifier.locale: en
   ```

3. 在 notifier.yaml.syslog_notifier.addresses 设置中，添加一个部分，其中包含向 KUMA 发送事件的设置。

   <连接名称> 设置只能包含拉丁字母、数字和下划线字符。

   对于“地址”设置，请指定 KUMA 收集器的 IP 地址。

   其他设置可以省略，在这种情况下将使用默认值。

   ```
   notifier.yaml.syslog_notifier.addresses:
   <Connection name>:
   address: <For sending to a remote server, specify protocol: UDP (default) or TCP, address and port; for local connection, specify Unix domain socket>
   doc_types: [<Comma-separated message types ('alert' for information about attacks, 'detection' for activities, and 'reputation' for information about indicators of compromise)&period; By default, all types of messages are sent>]
   facility: <Numeric value of the subject category>
   ident: <software tag>
   <Connection name>:
   ...
   ```

   以下是一个配置示例，用于通过 TCP 和 UDP 将包含活动、攻击和失陷指标信息的 syslog 消息发送到两台远程服务器，而不写入本地日志：

   ```
   notifier.yaml.syslog_notifier.addresses:
   remote1:
   address: tcp://198.51.100.1:1514
   remote2:
   address: udp://198.51.100.2:2514
   ```

4. 将更改保存在 /opt/ptsecurity/etc/ptdpi.settings.yaml 中。

5. 重新启动 ptdpi-worker@notifier 模块：

   ```
   sudo ptdpictl restart-worker notifier
   ```

已配置通过 Syslog 向 KUMA 发送事件。

使用 MariaDB 审计插件配置事件的接收

KUMA 允许使用 MariaDB 审计插件来审计事件。该插件支持 MySQL 5.7 和 MariaDB。该审计插件不支持 MySQL 8。有关该插件的详细信息可在 MariaDB 官方网站上找到。

建议使用 MariaDB Audit Plugin 版本 1.2 或更高版本。

配置事件接收包括以下步骤：

1. 配置 MariaDB 审计插件以发送 MySQL 事件并配置 Syslog 服务器以发送事件。
2. 配置 MariaDB 审计插件以发送 MariaDB 事件并配置 Syslog 服务器以发送事件。
3. 为 MySQL 5.7 和 MariaDB 事件创建 KUMA 收集器。

   要使用 MariaDB 审计插件接收 MySQL 5.7 和 MariaDB 事件，请在 KUMA 收集器安装向导的 **事件解析**步骤中，从 **规范化器**字段中选择 **[OOTB] MariaDB 审计插件 syslog**。
4. 在 KUMA 网络基础设施中安装收集器。
5. 验证 KUMA 收集器是否收到 MySQL 和 MariaDB 事件。

   要验证 MySQL 和 MariaDB 事件源服务器是否配置正确，您可以搜索相关事件。

配置 MariaDB 审计插件以发送 MySQL 事件

MariaDB 审计插件支持 MySQL 5.7 版本（最高 5.7.30），并与 MariaDB 捆绑提供。

要使用 MariaDB 审计插件配置 MySQL 5.7 事件报告：

1. 下载 MariaDB 分发包并解压。

   您可以从 MariaDB 官方网站下载 MariaDB 分发包。MariaDB 发行版的操作系统必须与运行 MySQL 5.7 的操作系统相同。
2. 通过运行以下命令，使用具有管理员权限的账户连接到 MySQL 5.7：

   ```
   mysql -u <用户名> -p
   ```
3. 要获取 MySQL 5.7 插件所在的目录，请在 MySQL 5.7 命令行上运行以下命令：

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```
4. 在步骤 3 获得的目录中，从<分发包解压到的目录>/mariadb-server-<版本>/lib/plugins/server_audit.so 复制 MariaDB 审计插件。
5. 在操作系统命令行中，运行以下命令：

   ```
   chmod 755 <分发包解压到的目录>server_audit.so
   ```

例如：

```
chmod 755 /usr/lib64/mysql/plugin/server_audit.so
```

6. 在 MySQL 5.7 命令行中，运行以下命令：

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

7. 创建 /etc/mysql/mysql.conf.d/mysqld.cnf 配置文件的备份副本。

8. 在配置文件 /etc/mysql/mysql.conf.d/mysqld.cnf 的 `[mysqld]` 部分中，添加以下行：

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   如果要禁用某些审计事件组的事件导出，请从 `server_audit_events` 设置中移除部分值。设置说明可在 MariaDB 审计插件供应商的网站上找到。

9. 保存对配置文件的更改。

10. 通过运行以下命令之一重新启动 MariaDB 服务：

    - `systemctl restart mysqld` 适用于使用 systemd 初始化的系统。
    - `service mysqld restart` 适用于使用 init 初始化的系统。

已配置适用于 MySQL 5.7 的 MariaDB 审计插件。如有必要，您可以在 MySQL 5.7 命令行上运行以下命令：

- 运行 `show plugins` 以查看当前插件列表。
- 运行 `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` 以查看当前审计设置。

配置 MariaDB 审计插件以发送 MariaDB 事件

从版本 5.5.37 和 10.0.10 开始，MariaDB 审计插件已纳入 MariaDB 分发包中。

要使用 MariaDB 审计插件配置 MariaDB 事件导出：

1. 通过运行以下命令，使用具有管理员权限的账户连接到 MariaDB：

   ```
   mysql -u <用户名> -p
   ```

2. 要检查插件是否存在于操作系统插件所在的目录中，请在 MariaDB 命令行中运行以下命令：

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

3. 在操作系统命令行中，运行以下命令：

   ```
   ll <通过上一命令获取的目录> | grep server_audit.so
   ```

   如果命令输出为空且插件不在目录中，则可以将 MariaDB 审计插件复制到该目录中或使用较新版本的 MariaDB。

4. 在 MariaDB 命令行中，运行以下命令：

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

5. 创建 /etc/mysql/my.cnf 配置文件的备份副本。

6. 在 /etc/mysql/my.cnf 配置文件的 `[mysqld]` 部分中，添加以下行：

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   如果要禁用某些审计事件组的事件导出，请从 `server_audit_events` 设置中移除部分值。设置说明可在 MariaDB 审计插件供应商的网站上找到。

7. 保存对配置文件的更改。

8. 通过运行以下命令之一重新启动 MariaDB 服务：

   - `systemctl restart mariadb`，适用于使用 systemd 初始化的系统。
   - `service mariadb restart`，适用于使用 init 初始化的系统。

MariaDB 的 MariaDB 审计插件已配置。如有必要，您可以在 MariaDB 命令行中运行以下命令：

- 运行 `show plugins` 以查看当前插件列表。
- 运行 `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` 以查看当前审计设置。

配置 Syslog 服务器以发送事件

rsyslog 服务用于将事件从服务器传输到收集器。

要配置从安装了 MySQL 或 MariaDB 的服务器向收集器发送事件：

1. 在进行任何更改之前，请创建 /etc/rsyslog.conf 配置文件的备份副本。

2. 要通过 UDP 发送事件，请在 /etc/rsyslog.conf 配置文件中添加以下行：

   ```
   *.* @<KUMA 收集器的 IP 地址>:<KUMA 收集器的端口>
   ```

   例如：

   ```
   *.* @192.168.1.5:1514
   ```

   如果要通过 TCP 发送事件，则该行应如下所示：

   ```
   *.* @@192.168.1.5:2514
   ```

   将更改保存到 /etc/rsyslog.conf 配置文件。

3. 重新启动 rsyslog 服务：

   ```
   sudo systemctl restart rsyslog.service
   ```

配置 Apache Cassandra 事件的接收

KUMA 允许接收有关 Apache Cassandra 事件的信息。

配置事件接收包括以下步骤：

1. 在 KUMA 中配置 Apache Cassandra 事件日志记录。
2. 为 Apache Cassandra 事件创建 KUMA 收集器。

   要接收Apache Cassandra事件，请在KUMA收集器安装向导的**传输方式**步骤中选择**文件**类型的连接器；在**事件解析**步骤中，在**规范化器**字段中选择**[OOTB] Apache Cassandra文件**。
3. 在 KUMA 网络基础设施中安装收集器。
4. 验证 KUMA 收集器中 Apache Cassandra 事件的接收情况。

   要验证 Apache Cassandra 事件源服务器是否配置正确，您可以搜索相关事件。

在 KUMA 中配置 Apache Cassandra 事件日志记录

要在 KUMA 中配置 Apache Cassandra 事件日志记录：

1. 确保安装了 Apache Cassandra 的服务器有 5 GB 的可用磁盘空间。
2. 使用具有管理员权限的账户连接到 Apache Cassandra 服务器。
3. 在进行更改之前，请创建以下配置文件的备份副本：
   - /etc/cassandra/cassandra.yaml
   - /etc/cassandra/logback.xml
4. 确保 /etc/cassandra/cassandra.yaml 配置文件中的设置具有以下值；如有必要，请进行更改：
   a. 在 `audit_logging_options` 部分中，将 `enabled` 设置为 `true`。
   b. 在 `logger` 部分中，将 `class_name` 设置为 `FileAuditLogger`。
5. 将以下行添加到 /etc/cassandra/logback.xml 配置文件：

```
<!-- Audit Logging (FileAuditLogger) rolling file appender to audit.log -->
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
<file>${cassandra.logdir}/audit/audit.log</file>
<rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
<!-- rollover daily -->
<fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-
dd}.%i.zip</fileNamePattern>
<!-- each file should be at most 50MB, keep 30 days worth of history, but at most 5GB
-->
<maxFileSize>50MB</maxFileSize>
<maxHistory>30</maxHistory>
<totalSizeCap>5GB</totalSizeCap>
</rollingPolicy>
<encoder>
```

```
<pattern>%-5level [%thread] %date{ISO8601} %F:%L - %replace(%msg){'\n', '
'}%n</pattern>
</encoder>
</appender>
<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log -->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
<appender-ref ref="AUDIT"/>
</logger>
```

6. 保存对配置文件的更改。
7. 使用以下命令重新启动 Apache Cassandra 服务：

   a. `sudo systemctl stop cassandra.service`

   b. `sudo systemctl start cassandra.service`

8. 重新启动后，使用以下命令检查 Apache Cassandra 的状态：

   ```
   sudo systemctl status cassandra.service
   ```

   确保命令输出包含以下字符序列：

   ```
   Active: active (running)
   ```

Apache Cassandra 事件导出已配置。事件位于 /var/log/cassandra/audit/ 目录的 audit.log 文件 (${cassandra.logdir}/audit/audit.log) 中。

配置 FreeIPA 事件的接收

您可以通过 Syslog 协议在 KUMA 中配置 FreeIPA 事件的接收。

配置事件接收包括以下步骤：

1. 配置将 FreeIPA 事件导出到 KUMA。
2. 创建用于接收 FreeIPA 事件的 KUMA 收集器。

   要接收FreeIPA事件，请在KUMA收集器安装向导的**事件解析**步骤中，在**规范化器**字段中选择**[OOTB] FreeIPA**。
3. 在网络基础设施中安装 KUMA 收集器。
4. 验证 KUMA 是否收到 FreeIPA 事件。

   要验证 FreeIPA 事件源服务器是否配置正确，您可以搜索相关事件。

配置将 FreeIPA 事件导出到 KUMA

要配置通过 Syslog 协议以 JSON 格式将 FreeIPA 事件导出到 KUMA：

1. 使用具有管理员权限的账户通过 SSH 连接到 FreeIPA 服务器。
2. 在 /etc/rsyslog.d/ 目录中，创建一个名为 freeipa-to-siem.conf 的文件。
3. 将以下行添加到 /etc/rsyslog.d/freeipa-to-siem.conf 配置文件：

```
$ModLoad imfile
$InputFileName /var/log/httpd/error_log
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log
$InputRunFileMonitor
$InputFileName /var/log/dirsrv/slapd-*/audit
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_audit
$InputRunFileMonitor
$InputFileName /var/log/dirsrv/slapd-*/errors
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_errors
$InputRunFileMonitor
$InputFileName /var/log/dirsrv/slapd-*/access
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_access
$InputRunFileMonitor
$InputFileName /var/log/krb5kdc.log
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_krb5kdc
$InputRunFileMonitor
template(name="ls_json" type="list" option.json="on") {
constant(value="{")
constant(value="\"@timestamp\":\"") property(name="timegenerated"
dateFormat="rfc3339")
constant(value="\",\"@version\":\"1")
constant(value="\",\"message\":\"") property(name="msg")
constant(value="\",\"host\":\"") property(name="fromhost")
constant(value="\",\"host_ip\":\"") property(name="fromhost-ip")
constant(value="\",\"logsource\":\"") property(name="fromhost")
constant(value="\",\"severity_label\":\"") property(name="syslogseverity-text")
constant(value="\",\"severity\":\"") property(name="syslogseverity")
```

```
constant(value="\",\"facility_label\":\"") property(name="syslogfacility-text")
constant(value="\",\"facility\":\"") property(name="syslogfacility")
constant(value="\",\"program\":\"") property(name="programname")
constant(value="\",\"pid\":\"") property(name="procid")
constant(value="\",\"syslogtag\":\"") property(name="syslogtag")
constant(value="\"}\n")
}
if $syslogtag contains 'tag_FreeIPA_log' then {
*.* action(type="omfwd" target="<KUMA 收集器的 IP 地址>" port="<KUMA 收集器的端口>"
protocol="<udp 或 tcp>" template="ls_json")
stop
}
```

4. 将以下行添加到 /etc/rsyslog.conf 配置文件：

   ```
   $IncludeConfig /etc/freeipa-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. 保存对配置文件的更改。

6. 重新启动 rsyslog 服务：

   ```
   sudo systemctl restart rsyslog.service
   ```

配置 VipNet TIAS 事件的接收

您可以通过 Syslog 协议在 KUMA 中配置 ViPNet TIAS 事件的接收。

配置事件接收包括以下步骤：

1. 配置将 ViPNet TIAS 事件导出到 KUMA。
2. 创建用于接收 ViPNet TIAS 事件的 KUMA 收集器。

   要使用Syslog接收ViPNet TIAS事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] Syslog-CEF**规范化器。

3. 安装用于接收 ViPNet TIAS 事件的 KUMA 收集器。
4. 验证 KUMA 中 ViPNet TIAS 事件的接收情况。

   您可以在 KUMA 控制台的“搜索相关事件”部分验证 ViPNet TIAS 事件源服务器是否配置正确。

配置将 ViPNet TIAS 事件导出到 KUMA

要配置通过 syslog 协议将 ViPNet TIAS 事件导出到 KUMA：

1. 使用具有管理员权限的用户账户连接到 ViPNet TIAS Web 界面。
2. 转到“**管理**” – “**集成**”部分。
3. 在“**集成**”页面上，转到 Syslog 选项卡。
4. 在接收服务器列表的工具栏中，单击“**新建服务器**”。
5. 这将打开新服务器卡；在该卡中：
    1. 在“**服务器地址**”字段中，输入 KUMA 收集器的 IP 地址或域名。
       例如，10.1.2.3 或 syslog.siem.ru
    2. 在“**端口**”字段中，指定 KUMA 收集器的入站端口。默认端口号是 514。
    3. 在“**协议**”列表中，选择 KUMA 收集器正在监听的传输层协议。默认情况下已选中 UDP。
    4. 在“**组织**”列表中，使用复选框选择 ViPNet TIAS 基础设施中的组织。
       仅针对从该基础设施选定组织的传感器接收的事件所检测到的事故发送消息。
    5. 在“**状态**”列表中，使用复选框选择事故状态。
       仅当向事故分配了选定状态时，才会发送消息。
    6. 在“**严重级别**”列表中，使用复选框选择事故的严重级别。
       仅发送有关具有所选严重级别的事故的消息。默认情况下，仅列表中的高严重级别被选中。
    7. 在“**UI 语言**”列表中，选择您希望在消息中接收事故相关信息的语言。默认情况下已选中俄语。
6. 单击“**添加**”。
7. 在列表的工具栏中，将“**不以 CEF 格式发送事故信息**”切换开关设置为启用状态。
   这样一来，当检测到新事故或先前检测到的事故的状态发生变化时，相应的信息将根据配置期间选择的状态，通过 syslog 协议以 CEF 格式发送到接收服务器的指定地址。
8. 单击“**保存更改**”。

已配置将事件导出至 KUMA 收集器。

配置 Nextcloud 事件的接收

您可以在 KUMA 中配置 Nextcloud 26.0.4 事件的接收。

配置事件接收包括以下步骤：

1. 配置 Nextcloud 事件审计。
2. 配置 Syslog 服务器以发送事件。

   rsyslog 服务用于将事件从服务器传输到收集器。
3. 创建用于接收 Nextcloud 事件的 KUMA 收集器。

   要接收Nextcloud事件，请在收集器安装向导的**事件解析**步骤中，选择**[OOTB] Nextcloud syslog**规范化器，并在**传输方式**步骤中选择**tcp**或**udp**连接器类型。
4. 安装 KUMA 收集器以接收 Nextcloud 事件
5. 验证 KUMA 收集器中是否收到 Nextcloud 事件

   您可以在 KUMA 控制台的"搜索相关事件"部分验证 Nextcloud 事件源服务器是否配置正确。

配置 Nextcloud 事件审计

要配置将 Nextcloud 事件导出到 KUMA：

1. 在安装了 Nextcloud 的服务器上，创建 /home/localuser/www/nextcloud/config/config.php 配置文件的备份副本。
2. 编辑 /home/localuser/www/nextcloud/config/config.php Nextcloud 配置文件。
3. 按如下方式编辑设置：

```
'log_type' => 'syslog',
'syslog_tag' => 'Nextcloud',
'logfile' => '',
'loglevel' => 0,
'log.condition' => [
'apps' => ['admin_audit'],
],
```

4. 重新启动 Nextcloud 服务。

```
sudo service restart nextcloud
```

已配置将事件导出至 KUMA 收集器。

配置 Syslog 服务器以发送 Nextcloud 事件

要配置从安装了 Nextcloud 的服务器向收集器发送事件：

1. 在 /etc/rsyslog.d/ 目录中，创建包含以下内容的 Nextcloud-to-siem.conf 文件：

```
If $programname contains 'Nextcloud' then @<收集器的 IP 地址>:<收集器的端口>
```

例如：

```
If $programname contains 'Nextcloud' then @192.168.1.5:1514
```

如果要通过 TCP 发送事件，则文件的内容必须如下：

```
If $programname contains 'Nextcloud' then @<收集器的 IP 地址>:<收集器的端口>
```

2. 将更改保存到 Nextcloud-to-siem.conf 配置文件。
3. 创建 /etc/rsyslog.conf 文件的备份副本。
4. 将以下行添加到 /etc/rsyslog.conf 配置文件：

```
$IncludeConfig /etc/Nextcloud-to-siem.conf
$RepeatedMsgReduction off
```

5. 保存更改。
6. 重新启动 rsyslog 服务：

```
sudo systemctl restart rsyslog.service
```

已配置将 Nextcloud 事件导出至收集器。

配置 Snort 事件的接收

您可以在 KUMA 中配置接收 Snort® 3 事件。

配置事件接收包括以下步骤：

1. 配置 Snort 事件的日志记录。
2. 创建用于接收 Snort 事件的 KUMA 收集器。

   要接收Snort事件，请在收集器安装向导的**事件解析**步骤中，选择**[OOTB] Snort 3 json file**规范化器，并在**传输方式**步骤中选择**文件**连接器类型。
3. 安装用于接收 Snort 事件的 KUMA 收集器
4. 验证 KUMA 收集器中是否收到 Snort 事件

   您可以在 KUMA 控制台的“搜索相关事件”部分中验证 Snort 事件源服务器是否配置正确。

配置 Snort 事件的日志记录

请确保运行 Snort 的服务器至少有 500 MB 的可用磁盘空间，用于存储单个 Snort 事件日志。
当日志达到 500 MB 时，Snort 会自动创建一个新文件，其名称包含 unixtime 格式的当前时间。
建议监控磁盘空间使用情况。

要配置 Snort 事件日志记录：

1. 使用具有管理员权限的帐户连接到安装了 Snort 的服务器。
2. 编辑 Snort 配置文件。为此，请在命令行中运行以下命令：

```
sudo vi /usr/local/etc/snort/snort.lua
```

3. 在配置文件中，编辑 alert_json 区块：

```
alert_json =
{
file = true,
limit = 500,
fields = 'seconds action class b64_data dir dst_addr dst_ap dst_port eth_dst eth_len \
eth_src eth_type gid icmp_code icmp_id icmp_seq icmp_type iface ip_id ip_len msg mpls
\
pkt_gen pkt_len pkt_num priority proto rev rule service sid src_addr src_ap src_port \
target tcp_ack tcp_flags tcp_len tcp_seq tcp_win tos ttl udp_len vlan timestamp',
}
```

4. 要完成配置，请运行以下命令：

```
sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l
/var/log/snort -i <Snort 侦听的接口名称> -m 0x1b
```

最终，Snort 事件会记录到 /var/log/snort/alert_json.txt 中。

配置 Suricata 事件的接收

您可以在 KUMA 中配置 Suricata 7.0.1 事件的接收。

配置事件接收包括以下步骤：

1. 配置将 Suricata 事件导出到 KUMA
2. 创建用于接收 Suricata 事件的 KUMA 收集器。

   要接收Suricata事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] Suricata json file**规范化器，并在**传输方式**步骤中选择**文件**连接器类型。
3. 安装用于接收 Suricata 事件的 KUMA 收集器
4. 验证 KUMA 收集器中是否收到 Suricata 事件

   您可以在 KUMA 控制台的"搜索相关事件"部分验证 Suricata 事件源服务器是否配置正确。

配置 Suricata 事件的日志记录。

要配置 Suricata 事件日志记录：

1. 通过 SSH 连接到具有管理用户账户的服务器。
2. 创建 /etc/suricata/suricata.yaml 文件的备份副本。
3. 在 /etc/suricata/suricata.yaml 配置文件的 eve-log 部分设置以下值：

```
- eve-log:
enabled: yes
```

```
filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
filename: eve.json
```

4. 将更改保存到 /etc/suricata/suricata.yaml 配置文件。

最终，Suricata 事件会记录到 /usr/local/var/log/suricata/eve.json 文件中。

Suricata 不支持限制 eve.json 事件文件的大小。如有必要，您可以使用轮转机制来管理日志大小。例如，要配置每小时日志轮转，请将以下行添加到配置文件：

```
outputs:

- eve-log:

filename: eve-%Y-%m-%d-%H:%M.json

rotate-interval: hour
```

配置 FreeRADIUS 事件的接收

您可以在 KUMA 中配置 FreeRADIUS 3.0.26 事件的接收。

配置事件接收包括以下步骤：

1. 配置 FreeRADIUS 事件审计。
2. 配置 Syslog 服务器以发送 FreeRADIUS 事件。
3. 创建用于接收 FreeRADIUS 事件的 KUMA 收集器。

   要接收FreeRADIUS事件，请在收集器安装向导的**事件解析**步骤中，选择**[OOTB] FreeRADIUS syslog**规范化器，并在**传输方式**步骤中选择**tcp**或**udp**连接器类型。
4. 安装用于接收 FreeRADIUS 事件的 KUMA 收集器。
5. 验证 KUMA 收集器中是否收到 FreeRADIUS 事件。

   您可以在 KUMA 控制台的"搜索相关事件"部分验证 FreeRADIUS 事件源服务器是否配置正确。

配置 FreeRADIUS 事件审计

要在 FreeRADIUS 系统中配置事件审计：

1. 使用具有管理权限的用户账户连接到安装了 FreeRADIUS 系统的服务器。
2. 创建 FreeRADIUS 配置文件的备份副本：

   ```
   sudo cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius /3.0/radiusd.conf.bak
   ```
3. 打开 FreeRADIUS 配置文件进行编辑：

   ```
   sudo nano /etc/freeradius/3.0/radiusd.conf
   ```

4. 在“日志”部分，按如下所示编辑设置：

```
destination = syslog
syslog_facility = daemon
stripped_names = no
auth = yes
auth_badpass = yes
auth_goodpass = yes
```

5. 保存配置文件。

FreeRADIUS 事件审计已配置。

配置 Syslog 服务器以发送 FreeRADIUS 事件

rsyslog 服务用于将事件从 FreeRADIUS 服务器传输到 KUMA 收集器。

要配置从安装了 FreeRADIUS 的服务器向收集器发送事件：

1. 在 /etc/rsyslog.d/ 目录中，创建 FreeRADIUS-to-siem.conf 文件并向其中添加以下行：

```
If $programname contains 'radiusd' then @<收集器的 IP 地址>:<收集器的端口>
```

如果要通过 TCP 发送事件，则文件的内容必须如下：

```
If $programname contains 'radiusd' then @<收集器的 IP 地址>:<收集器的端口>
```

2. 创建 /etc/rsyslog.conf 文件的备份副本。

3. 将以下行添加到 /etc/rsyslog.conf 配置文件：

```
$IncludeConfig /etc/FreeRADIUS-to-siem.conf
$RepeatedMsgReduction off
```

4. 保存更改。

5. 重新启动 rsyslog 服务：

```
sudo systemctl restart rsyslog.service
```

已配置将事件从 FreeRADIUS 服务器导出至 KUMA 收集器。

配置 VMware vCenter 事件接收

您可以在 KUMA SIEM 系统中配置 VMware vCenter 事件的接收。

配置事件接收包括以下步骤：

1. 配置与 VMware vCenter 的连接。

2. 创建用于接收 VMware vCenter 事件的 KUMA 收集器。

要接收 VMware vCenter 事件，请在收集器安装向导的“**传输方式**”步骤中选择 vmware 连接器类型。指定所需的设置：

- VMware API 可用的 URL，例如 https://vmware-server.com:6440。
- VMware 凭证 — 指定用于连接到 VMware API 的用户名和密码的密钥。

在**事件解析**步骤中，选择**[OOTB] VMware vCenter API**规范化器。

3. 安装用于接收 VMware vCenter 事件的 KUMA 收集器。
4. 在 KUMA 收集器中验证 VMware vCenter 事件的接收情况。
   您可以在 KUMA 控制台的“搜索相关事件”部分验证 VMware vCenter 事件源服务器是否配置正确。

配置与 VMware vCenter 的连接

要配置与 VMware vCenter 的连接以接收事件：

1. 使用具有管理权限的用户账户连接到 VMware vCenter Web 界面。
2. 转到“**安全和用户**”部分并选择“**用户**”。
3. 创建用户账户。
4. 转到“**角色**”部分，并为所创建的账户分配“**只读：查看对象角色的详细信息，但不能更改**”角色。
   您将在收集器的密钥中使用此用户账户的凭证。
   有关创建用户账户的详细信息，请参阅 VMware vCenter 文档。

已配置用于接收事件的 VMware vCenter 的连接。

配置 zVirt 事件的接收

您可以在 KUMA 中配置 zVirt 3.1 事件的接收。

配置事件接收包括以下步骤：

1. 配置将 zVirt 事件导出至 KUMA。
2. 创建用于接收 zVirt 事件的 KUMA 收集器。

   要接收zVirt事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] OrionSoft zVirt syslog**规范化器，并在**传输方式**步骤中选择**tcp**或**udp**连接器类型。
3. 安装用于接收 zVirt 事件的 KUMA 收集器
4. 验证 KUMA 收集器中是否收到 zVirt 事件
   您可以在 KUMA 控制台的“搜索相关事件”部分验证 zVirt 事件源服务器是否配置正确。

配置 zVirt 事件的导出

ZVirt 可以在 Hosted Engine 安装模式下将事件发送到外部系统。

要配置将 zVirt 事件导出到 KUMA：

1. 在 zVirt Web 界面中的“**资源**”下，选择“**虚拟机**”。
2. 选择运行 HostedEngine 虚拟机的计算机，然后单击“**编辑**”。
3. 在“**编辑虚拟机**”窗口中，转到“**日志记录**”部分。
4. 选中“**确定 Syslog 服务器地址**”复选框。
5. 在文本框中，按以下格式输入收集器信息：`<KUMA 收集器的 IP 地址或 FQDN>：<KUMA 收集器的端口>`。
6. 如果要使用 TCP 而不是 UDP 发送日志，请选中“**使用 TCP 连接**”复选框。

事件导出已配置。

配置 Zeek IDS 事件的接收

您可以在 KUMA 中配置 Zeek IDS 1.8 事件的接收。

配置事件接收包括以下步骤：

1. 转换 Zeek IDS 事件日志格式。

   KUMA 规范化器支持 JSON 格式的 Zeek IDS 日志。要将事件发送到 KUMA 规范化器，必须将日志文件转换为 JSON 格式。

2. 创建用于接收 Zeek IDS 事件的 KUMA 收集器。

   要接收Zeek IDS事件，请在收集器安装向导的**事件解析**步骤中选择**[OOTB] ZEEK IDS json file**规范化器，并在**传输方式**步骤中选择**文件**连接器类型。

3. 安装用于接收 Zeek IDS 事件的 KUMA 收集器

4. 验证 KUMA 收集器中是否收到 Zeek IDS 事件

   您可以在 KUMA 控制台的“搜索相关事件”部分验证 Zeek IDS 事件源服务器是否配置正确。

转换 Zeek IDS 事件日志格式

默认情况下，Zeek IDS 事件记录在 /opt/zeek/logs/current 目录中的文件中。

“[OOTB] ZEEK IDS json 文件”规范化器支持 JSON 格式的 Zeek IDS 日志。要将事件发送到 KUMA 规范化器，必须将日志文件转换为 JSON 格式。

每次接收 Zeek IDS 事件之前，都必须重复此过程。

要转换 Zeek IDS 事件日志格式：

1. 使用具有管理权限的用户账户连接到安装了 Zeek IDS 的服务器。
2. 创建必须存储 JSON 事件日志的目录：

   ```
   sudo mkdir /opt/zeek/logs/zeek-json
   ```

3. 更改到此目录：

   ```
   sudo cd /opt/zeek/logs/zeek-json
   ```

4. 运行使用 jq 实用程序的命令将原始事件日志格式转换为目标格式：

   ```
   jq &period; -c <要转换为不同格式的日志文件的路径> >> <新文件名>.log
   ```

   例如：

   ```
   jq &period; -c /opt/zeek/logs/current/conn.log >> conn.log
   ```

   运行该命令的结果是，如果此文件之前不存在，则会在 /opt/zeek/logs/zeek-json 目录中创建一个新文件。如果该文件已存在于当前目录中，则新信息将附加到文件末尾。

使用 ETW 连接器配置 DNS 服务器事件接收

Event Tracing for Windows 连接器（下称“ETW 连接器”）是一种用于记录 DNS 服务器上应用程序和驱动程序生成的事件的机制。您可以使用 ETW 连接器来排查开发过程中的错误或查找恶意的活动。

ETW 连接器对 DNS 服务器性能的影响微乎其微。例如，一台运行在现代硬件上、每秒查询次数 (QPS) 高达 100,000 的 DNS 服务器在使用 ETW 连接器时，性能可能会下降 5%。如果 DNS 服务器每秒请求次数不超过 50,000，则不会出现性能下降。使用 ETW 连接器时，无论每秒请求数量如何，建议对 DNS 服务器的性能进行监控。

默认情况下，您可以在 Windows Server 2016 或更高版本上使用 ETW 连接器。如果安装了事件日志记录和更改审计更新，Windows Server 2012 R2 也支持 ETW 连接器。此更新可在 Microsoft 支持网站 上获取。

ETW 连接器包含以下组件：

- *提供者*是生成事件并将事件发送到 ETW 连接器的软件。例如，Windows 内核或设备驱动程序可以充当提供者。开发人员在编写代码时，必须指定提供者必须将哪些事件发送至 ETW 连接器。一个事件可能代表开发人员认为重要的某个函数的执行，例如允许访问安全账号管理器 (SAM) 的函数。
- *消费者*是指从 ETW 连接器接收并使用由提供者生成的事件的软件。例如，KUMA 可以充当消费者。
- *控制器*是管理提供者和消费者之间交互的软件。例如，Logman 或 Wevtutil 实用程序可以充当控制器。提供者向控制器注册以将事件发送给消费者。控制器可以启用或禁用提供者。如果提供者被禁用，它将不会生成事件。

  控制器使用跟踪会话实现提供者和消费者之间的通讯。跟踪会话还用于根据指定参数过滤数据，因为消费者可能需要不同的事件。

使用 ETW 连接器配置 DNS 服务器事件接收涉及以下步骤：

1. Windows 端配置。
2. 创建 KUMA 收集器。

   创建 KUMA 收集器时，请按照以下步骤操作：

   a. 在收集器安装向导的步骤 2 中：

      1. 在“**类型**”下拉列表中，选择“**tcp**”连接器类型。您还可以指定“**http**”连接器类型以及其他带有安全传输验证的连接器类型。
      2. 在“**URL**”字段中，输入 KUMA 收集器将侦听来自 KUMA 代理的连接的 FQDN 和端口号。您可以指定任何未占用的端口号。
      3. 在“**分隔符**”字段中，输入“\n”。

   b. 在收集器安装向导的步骤 3 中，在“**规范化器**”下拉列表中选择一个规范化器。建议选择适用于Windows事件的预定义扩展规范化器 **[OOTB] Microsoft DNS ETW logs json**。

   c. 在收集器安装向导的步骤 7 中，添加用于存储事件的“**存储**”类型的目标位置。如果计划使用事件关联，则还需要添加“**关联器**”类型的目标位置。

   d. 在收集器安装向导的步骤 8 中，单击“**创建并保存服务**”，然后在窗口的下半部分，复制用于在服务器上安装 KUMA 收集器的命令。

3. 在服务器上安装 KUMA 收集器。

   执行以下操作：

   a. 使用具有根权限的用户账户连接到 KUMA 命令行界面。

   b. 通过运行在收集器安装向导的步骤 8 中复制的命令来安装 KUMA 收集器。

   c. 如果要将 KUMA 收集器端口添加到防火墙排除项并更新防火墙设置，请运行以下命令：

      1. `firewall-cmd --add-port=<collector port number>/tcp --permanent`
      2. `firewall-cmd --reload`

   KUMA 收集器已安装，且 KUMA 控制台中 KUMA 收集器服务的状态更改为绿色。

4. 创建 KUMA 代理。

   创建 KUMA 代理时，请按照以下步骤操作：

   a. 转到“**连接 1**”选项卡。

   b. 在**连接器**下的**连接器**下拉列表中，选择**创建**并指定以下设置：

      1. 在“**类型**”下拉列表中，选择“**etw**”连接器类型。
      2. 在**会话名称**字段中，输入在Windows端使用ETW连接器配置DNS服务器事件接收时指定的提供者名称。

c. 在**目标位置**下的**目标位置**下拉列表中，选择**创建**并指定以下设置：

1. 在“**类型**”下拉列表中，选择“tcp”目标位置类型。

2. 在“**URL**”字段中，输入 KUMA 收集器将侦听来自 KUMA 代理的连接的 FQDN 和端口号。该值必须与您在收集器安装向导的步骤 2 中指定的值匹配。

d. 转到**高级设置**选项卡，然后在**磁盘缓冲区大小限制**字段中输入1073741824。

5. 创建 KUMA 代理服务。

您需要复制创建的 KUMA 代理服务的 ID。为此，请单击 KUMA 代理服务，然后在上下文菜单中选择“**复制 ID**”。

6. 为 KUMA 代理创建账户。

创建一个域用户账户或本地 Windows 用户账户，用于运行 KUMA 代理并读取分析日志。您需要将创建的用户账户添加到“**性能日志用户**”用户组，并向该用户账户授予“**登录服务**”权限。

7. 在 Windows 服务器上安装 KUMA 代理。

您需要在将从提供者接收事件的 Windows 服务器上安装 KUMA 代理。为此请执行以下操作：

a. 将 KUMA Core 服务器的 FQDN 添加到 Windows 服务器上的 hosts 文件或 DNS 服务器。

b. 在 Windows 服务器上创建 C:\Users\<user name>\Desktop\KUMA 文件夹。

c. 将 KUMA 安装包压缩文件中的 kuma.exe 文件复制到 C:\Users\<user name>\Desktop\KUMA 文件夹。

d. 以管理员身份运行命令解释器。

e. 更改为 C:\Users\<user name>\Desktop\KUMA 文件夹并运行以下命令：

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core <FQDN>:7210 --id <agent ID>
```

其中：

- <FQDN> 是 KUMA Core 服务器的完全限定域名。
- <agent ID> 是在 OSMP 中创建的代理服务的 ID。

在 KUMA 控制台的“**资源 → 活动服务**”部分中，确保 KUMA 代理服务正在运行并且其状态现在为绿色，然后中止该命令。

f. 通过下列其中一种方式启动 KUMA 代理安装程序：

- 如果要使用域用户账户启动 KUMA 代理安装程序，请运行以下命令：

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core <FQDN>:7210 --pair.fingerprint <fingerprint ID
of the KUMA Core CA certificate> --id <agent ID> --user <user> --install
```

其中：

- <FQDN> 是 KUMA Core 服务器的完全限定域名。
- <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

`--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。

- <agent ID> 是在 OSMP 中创建的代理服务的 ID。
- <user> 是用于运行代理的用户账户名称，包括域。

- 如果要使用本地用户账户启动 KUMA 代理安装程序，请运行以下命令：

  ```
  C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core <FQDN>:7210 --pair.fingerprint <KUMA Core CA 证书的指纹 ID> --id <agent ID> --user <user> --install
  ```

  其中：

  - <FQDN> 是 KUMA Core 服务器的完全限定域名。
  - <fingerprint ID of the KUMA Core CA certificate> 是连接服务时用于身份验证的 CA 证书指纹 ID。

    `--pair.fingerprint` 参数是可选的。创建服务时，OSMP 会自动将此选项添加到安装命令中，并指定指纹 ID。

    安装服务时，可以不指定 `--pair.fingerprint` 选项。在这种情况下，OSMP 默认使用 `insecure` 值，从而在建立连接时跳过对 KUMA Core CA 证书的验证。如果值为 `insecure`，则重新颁发 CA 证书后无需更新指纹。

    为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带指纹 ID 的 `--pair.fingerprint` 选项。重新颁发 CA 证书时，需要从 Web 界面复制新证书的指纹，并使用更新后的指纹 ID 重启服务。

  - <agent ID> 是在 OSMP 中创建的代理服务的 ID。
  - <user> 是用于运行代理的用户帐户名称，包括域。

  您将需要输入 KUMA 代理用户账户的密码。

KUMA Windows 代理服务 <KUMA 代理服务 ID> 已安装在 Windows 服务器上。在 KUMA 控制台的"**资源 → 活动服务**"部分中，如果 KUMA 代理服务未运行且状态显示为红色，则需要确保端口 7210 可用，以及从 KUMA 代理到 KUMA 收集器方向的 Windows 收集器端口可用。

要删除 Windows 服务器上的 KUMA 代理服务，请运行以下命令：

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --id <agent ID> --uninstall
```

其中：

<agent ID> 是在 OSMP 中创建的代理服务的 ID。

8. 验证 KUMA 收集器中 DNS 服务器事件的接收情况。

   您可以在 KUMA 控制台的"**搜索相关事件**"部分中验证是否已正确配置使用 ETW 连接器来接收 DNS 服务器事件。

Windows 端配置

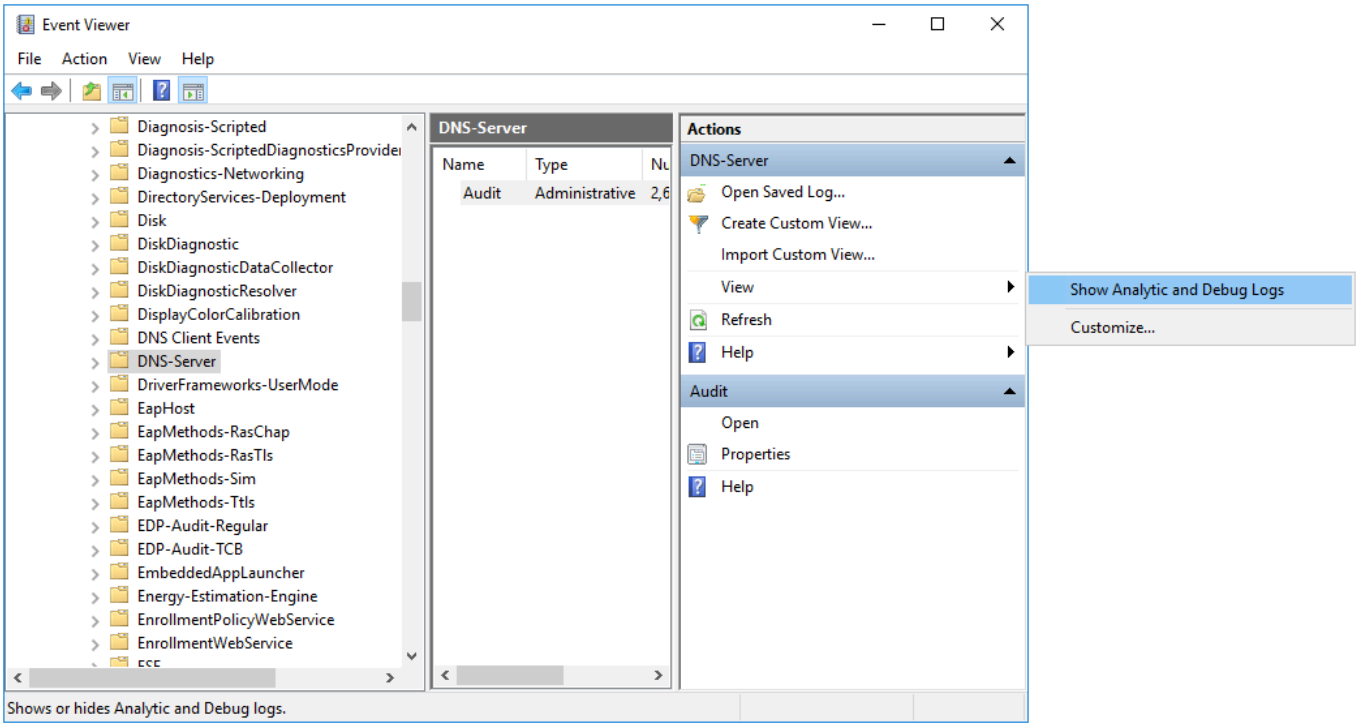
要在 Windows 端配置使用 ETW 连接器来接收 DNS 服务器事件：

1. 通过运行以下命令启动事件查看器：

   eventvwr.msc

2. 在打开的窗口中，转到“**应用程序和服务日志** → **Microsoft** → **Windows** → **DNS 服务器**”文件夹。

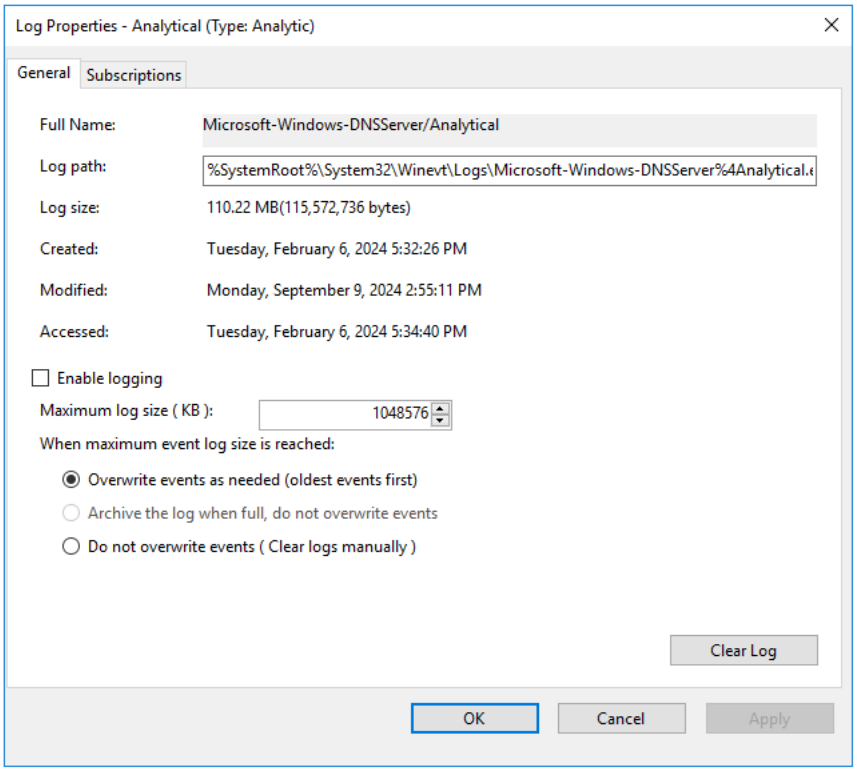
3. 打开“**DNS 服务器**”文件夹的上下文菜单，然后选择“**查看** → **显示分析和调试日志**”。



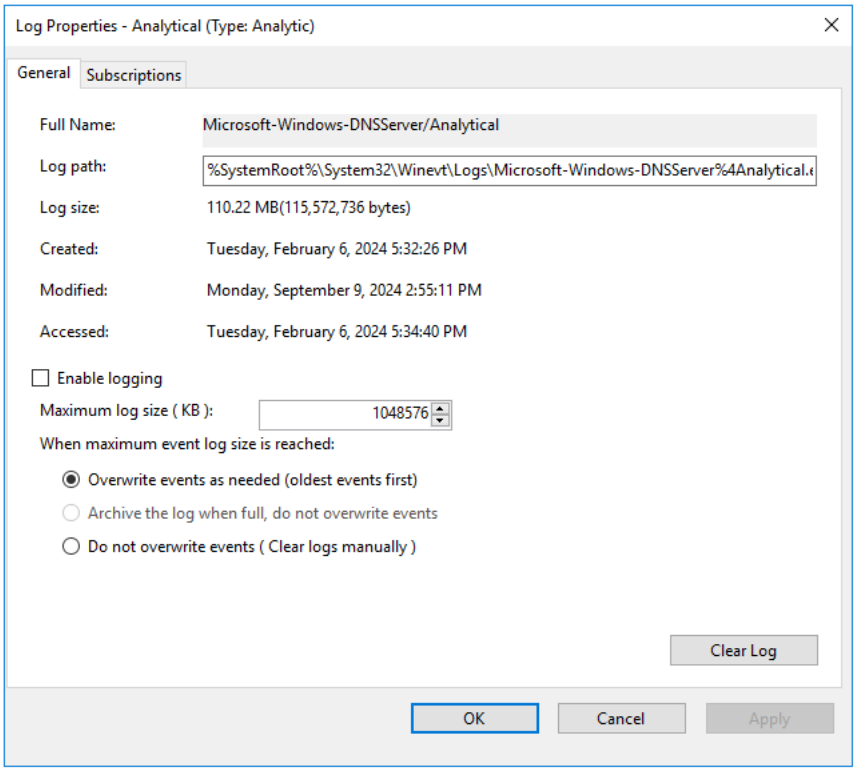
将显示“**审计**”调试日志和“**分析**”日志。

4. 配置分析日志：

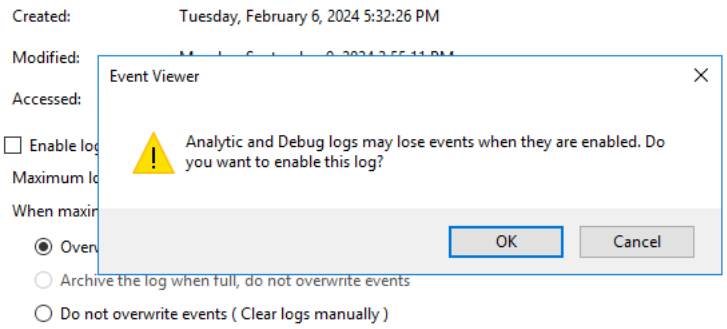
a. 打开“**分析**”日志的上下文菜单，然后选择“**属性**”。



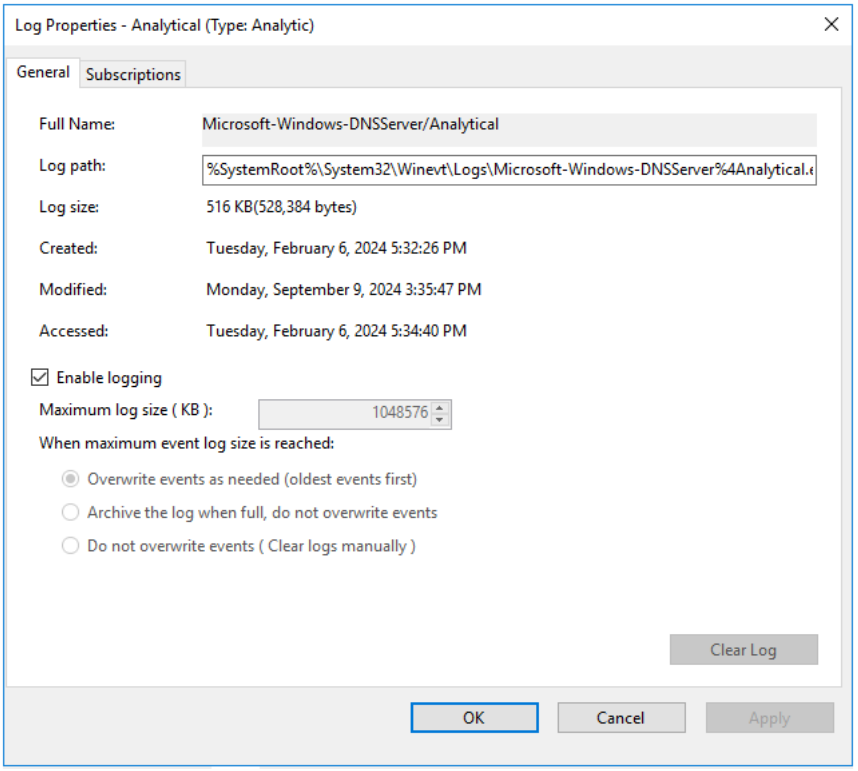
a. 在打开的窗口中，确保“**最大日志大小 (KB)**”字段中的值为 1048576。



a. 选中“**启用日志记录**”复选框，然后在确认窗口中单击“**确定**”。

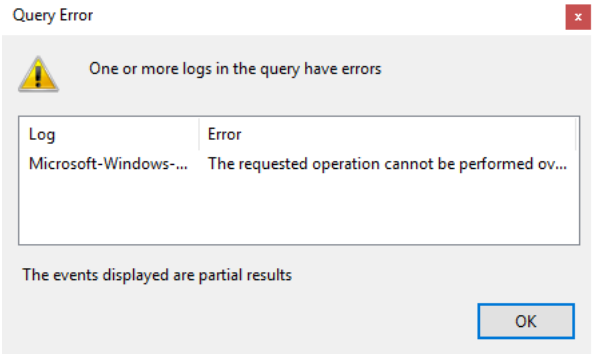


必须按如下方式配置分析日志：

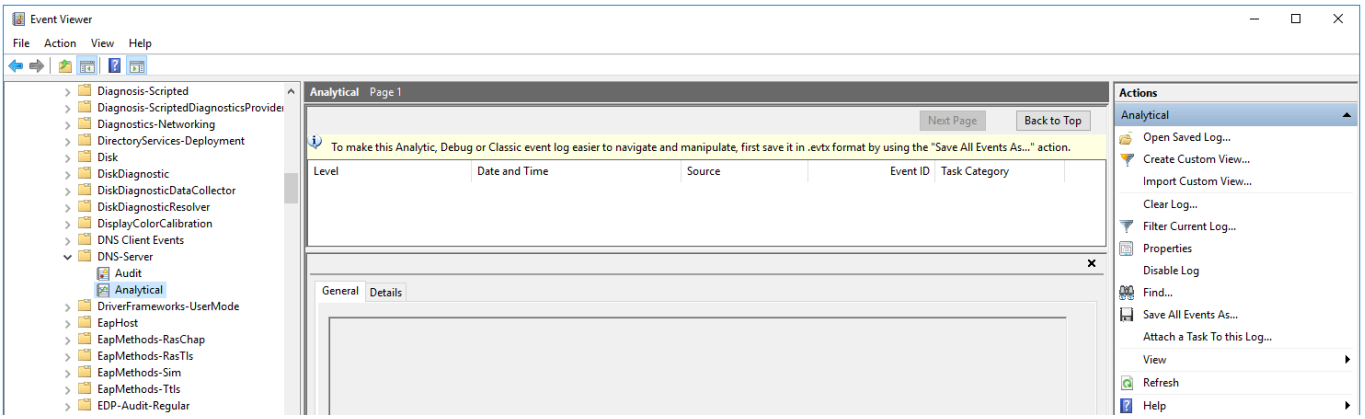


a. 单击“**应用**”，然后单击“**确定**”。

将显示一个错误窗口。

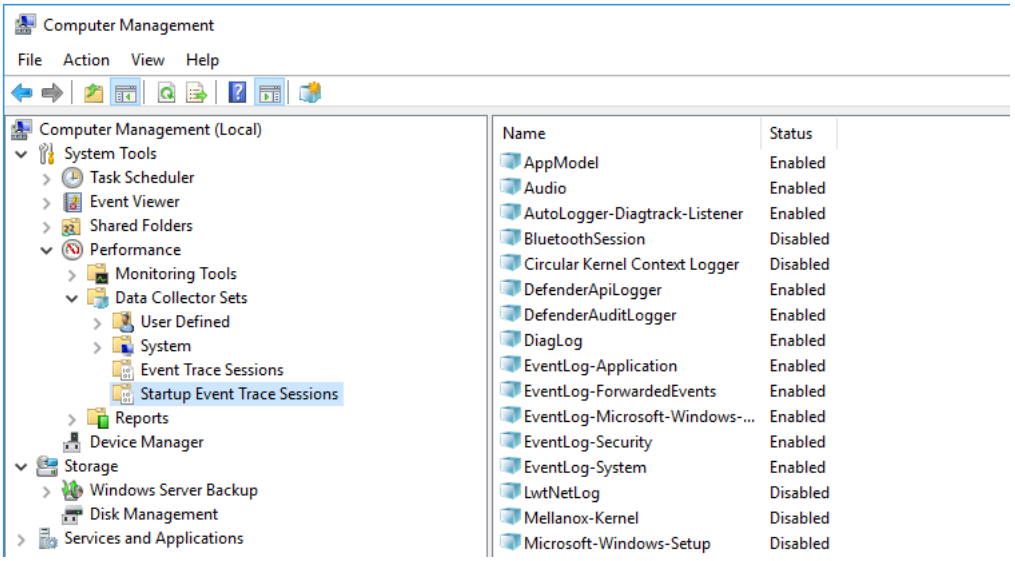


启用分析日志轮换后，事件不会显示。要查看事件，请在“**操作**”窗格中单击“**停止日志记录**”。



5. 以管理员身份启动"计算机管理"。

6. 在打开的窗口中，转到"**系统工具 → 性能 → 启动事件跟踪会话**"文件夹。

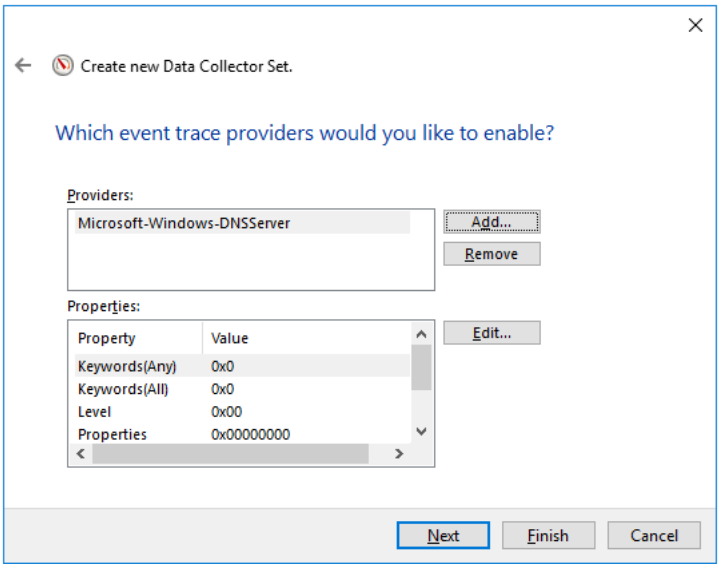


7. 创建提供者：

   a. 打开"**启动事件跟踪会话**"文件夹的上下文菜单，并选择"**创建 → 数据收集器集**"。

   b. 这将打开一个窗口；在该窗口中，输入提供者的名称，然后单击"**下一步**"。

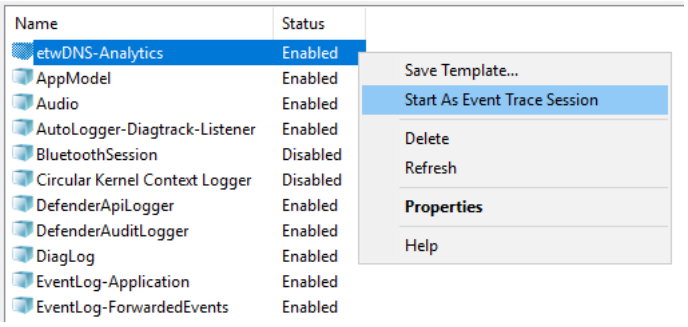
   c. 单击"**添加...**"，然后在显示的窗口中，选择"**Microsoft-Windows-DNSServer**"提供者。



带有 ETW 连接器的 KUMA 代理仅适用于 System.Provider.Guid: {EB79061A-A566-4698-9119-3ED2807060E7} - Microsoft-Windows-DNSServer。

a. 单击“**下一步**”两次，然后单击“**完成**”。

8. 打开所创建的提供者的上下文菜单，并选择“**作为事件跟踪会话启动**”。

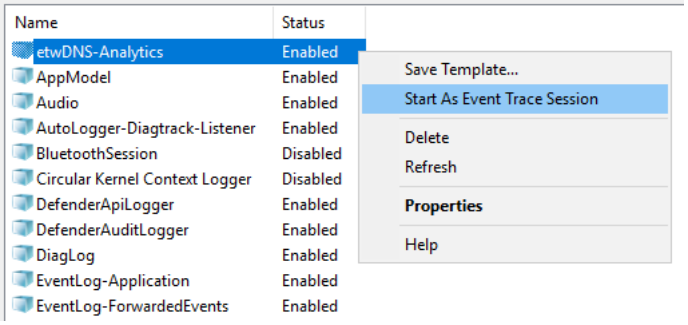


9. 转到“**事件跟踪会话**”文件夹。

显示事件跟踪会话。

10. 打开创建的事件跟踪会话的上下文菜单并选择“**属性**”。

11. 这将打开一个窗口；在该窗口中，选择“**跟踪会话**”选项卡，然后在“**流模式**”下拉列表中选择“**实时**”。



12. 单击“**应用**”，然后单击“**确定**”。

已配置使用 ETW 连接器接收 DNS 服务器事件。

使用 Kaspersky Endpoint Security for Windows 配置 Windows 事件接收

从 Kaspersky Endpoint Security for Windows 12.6 版本开始，可以将 Windows 日志中的事件发送到 KUMA 收集器。通过这种方式，KUMA 可以从所有安装了 KES for Windows 12.6 的主机的 Windows 日志中获取事件（支持微软产品的一组有限 EventID），而无需在这些主机上安装 KUMA 代理。在KES for Windows版本12.6–12.12中，筛选了具有相同参数的事件：只发送第一个事件，而后续的类似事件不会传输。如果系统生成大量类似事件，其中一些事件可能仍会被发送。通常需要生成数百或数千个此类事件才会出现这种情况。参数不同的事件（例如，当其他用户登录时）的传输不受限制。筛选逻辑由卡巴斯基专家定义，旨在减少传输的事件数量，同时避免丢失攻击检测所需的数据。

要激活该功能，您需要：

- 有效的 KUMA 授权许可
- KSC 14.2 或更高版本
- KES for Windows 版本 12.6 或更高版本

配置事件接收包括以下步骤：

1. 将规范化器导入 Kaspersky Next XDR Expert。

   在 Kaspersky Next XDR Expert 中，您必须配置通过卡巴斯基更新服务器进行更新。

   单击“导入资源”，然后在可供安装的规范化器列表中，选择“**[OOTB] Microsoft Products via KES WIN**”。

2. 创建用于接收 Windows 事件的 KUMA 收集器。

   要接收 Windows 事件，请在**传输方式**步骤中选择**TCP**或**UDP**，并指定收集器必须侦听的端口号。在**事件解析**步骤中，选择**[OOTB] Microsoft Products via KES WIN**规范化器。在**事件筛选**步骤中，选择**[OOTB] Microsoft Products via KES WIN - 收集器事件过滤器**。

3. 向卡巴斯基技术支持申请密钥。

   如果您的许可证不包含用于激活向 KUMA 收集器发送 Windows 日志功能的密钥，请向技术支持发送以下消息：我们已购买 KUMA 许可证，并且正在使用 KES for Windows 12.6 版本.我们希望激活向 KUMA 收集器发送 Windows 日志的功能。请提供密钥文件以激活该功能。Kaspersky Next XDR Expert 新用户无需向技术支持提交请求，因为新用户会获得 2 个密钥，分别用于 KUMA 许可和激活 KES for Windows 功能。

   回复您的消息后，您将获得一个密钥文件。

4. 在 KSC 和 KES for Windows 端进行配置。

   必须将用于激活向 KUMA 收集器发送 Windows 事件功能的密钥文件导入 KSC，并按照说明分发到 KES 端点。您还必须将 Kaspersky Next XDR Expert 服务器地址添加到 KES 策略中，并指定网络连接设置。

5. 验证 KUMA 收集器中是否收到 Windows 事件。

   您可以在 OSMP 控制台的搜索相关事件部分中验证 Windows 事件源服务器是否配置正确。

   下表列出了 KES for Windows 传输的 Microsoft 产品事件：

事件日志	事件 ID
DNS 服务器	150
DNS 服务器	770
MSExchange Management	1
安全性	4781
安全性	6416
安全性	1100
安全性	1102 / 517
安全性	1104
安全性	1108
安全性	4610 / 514
安全性	4611
安全性	4614 / 518
安全性	4616 / 520

事件日志	事件 ID
安全性	4622
安全性	4624 / 528 / 540
安全性	4625 / 529
安全性	4648 / 552
安全性	4649
安全性	4662
安全性	4663
安全性	4672 / 576
安全性	4696
安全性	4697 / 601
安全性	4698 / 602
安全性	4702
安全性	4704 / 608
安全性	4706
安全性	4713/617
安全性	4715
安全性	4717 / 621
安全性	4719 / 612
安全性	4720 / 624
安全性	4722 / 626
安全性	4723 / 627
安全性	4724 / 628
安全性	4725 / 629
安全性	4726 / 630
安全性	4727
安全性	4728 / 632
安全性	4729 / 633
安全性	4732 / 636
安全性	4733 / 637
安全性	4738 / 642
安全性	4739 / 643
安全性	4740 / 644
安全性	4741
安全性	4742 / 646
安全性	4756 / 660
安全性	4757 / 661
安全性	4765
安全性	4766
安全性	4767
安全性	4768 / 672
安全性	4769 / 673

事件日志	事件 ID
安全性	4770
安全性	4771 / 675
安全性	4775
安全性	4776 / 680
安全性	4778 / 682
安全性	4780 / 684
安全性	4794
安全性	4798
安全性	4817
安全性	4876 / 4877
安全性	4882
安全性	4885
安全性	4886
安全性	4887
安全性	4890
安全性	4891
安全性	4898
安全性	4899
安全性	4900
安全性	4902
安全性	4904
安全性	4905
安全性	4928
安全性	4946
安全性	4947
安全性	4948
安全性	4949
安全性	4950
安全性	4964
安全性	5025
安全性	5136
安全性	5137
安全性	5138
安全性	5139
安全性	5141
安全性	5142
安全性	5143
安全性	5144
安全性	5145
安全性	5148
安全性	5155

事件日志	事件 ID
安全性	5376
安全性	5377
安全性	5632
安全性	5888
安全性	5889
安全性	5890
安全性	676
操作系统	1
系统	104
系统	1056
系统	12
系统	13
系统	6011
系统	7040
系统	7045
系统，源 Netlogon	5723
系统，源 Netlogon	5805
终端服务远程连接管理器	1149
终端服务远程连接管理器	1152
终端服务远程连接管理器	20523
终端服务远程连接管理器	258
终端服务远程连接管理器	261
Windows PowerShell	400
Windows PowerShell	500
Windows PowerShell	501
Windows PowerShell	800
应用程序，源 ESENT	301
应用程序，源 ESENT	302
应用程序，源 ESENT	325
应用程序，源 ESENT	326
应用程序，源 ESENT	327
应用程序，源 ESENT	2001
应用程序，源 ESENT	2003
应用程序，源 ESENT	2005
应用程序，源 ESENT	2006
应用程序，源 ESENT	216
应用程序	1000
应用程序	1002
应用程序	1 / 2

Codemaster Mirada

您可以在卡巴斯基 SIEM (KUMA) 中配置接收 Codemaster Mirada 事件。

配置事件接收包括以下步骤：

1 配置 Codemaster Mirada 系统的审计

Codemaster Mirada 系统可以通过 Syslog 协议发送事件。

1. 使用具有管理员权限的用户账户连接到 Codemaster Mirada Web 界面。
2. 转到“**设置**” →“**Syslog**”部分。
3. 使用切换开关启用事件传输服务。
4. 单击圆圈中有个点的图标，选择协议的类型和格式。
5. 在“**主机**”字段中，指定 KUMA 收集器的 IP 地址。
6. 在“**协议**”字段中，指定“**UDP**”或“**TCP**”传输协议。
7. 在“**端口**”字段中，指定 KUMA 收集器正在监听的端口。
   默认端口号是 514。
8. 在“**格式**”字段中，指定“**RFC 3164**”标准。
9. 单击页面下方的“**保存**”以保存更改。

2 创建用于接收 Codemaster Mirada 事件的 KUMA 收集器

要接收 Codemaster Mirada 事件，请在创建收集器时，在**事件解析**步骤选择**[OOTB] Codemaster Mirada syslog**规范化器，并在**传输**步骤选择**tcp**或**udp**连接器类型。

3 在网络基础设施中安装收集器

配置用于接收 Codemaster Mirada 事件的收集器后，在网络基础设施中用于接收事件的服务器上安装 KUMA 收集器。

4 验证 KUMA 收集器是否收到 Codemaster Mirada 事件

要验证 Codemaster Mirada 事件源服务器是否配置正确，可以在卡巴斯基 SIEM (KUMA) Web 界面中搜索相关事件。

配置 Codemaster Mirada 事件的接收

Codemaster Mirada 系统可以通过 Syslog 协议发送事件。

要在 Codemaster Mirada 系统中配置事件审计：

1. 使用具有管理权限的用户账户连接到 Codemaster Mirada Web 界面。
2. 转到“**设置**” →“**Syslog**”部分。
3. 使用切换开关启用事件传输服务。
4. 单击圆圈中有个点的图标，选择协议的类型和格式。
5. 在“**主机**”字段中，指定 KUMA 收集器的 IP 地址。
6. 在“**协议**”字段中，指定“**UDP**”或“**TCP**”传输协议。
7. 在“**端口**”字段中，指定 KUMA 收集器正在监听的端口。
   默认端口号是 514。
8. 在“**格式**”字段中，指定“**RFC 3164**”标准。
9. 单击页面下方的“**保存**”以保存更改。

配置 Postfix 事件的接收

您可以在 KUMA 中配置接收 Postfix 事件。仅当使用 TCP 协议，通过 syslog 发送事件时才可集成。本文描述的资源适用于 KUMA 3.0 及更高版本。

配置事件接收包括以下步骤：

1. 配置 CommuniGate Pro 以发送事件
2. 创建用于接收 Postfix 事件的 KUMA 收集器。
3. 验证 KUMA 收集器中 Postfix 事件的接收情况
   您可以在 KUMA 控制台的“搜索相关事件”部分验证 Postfix 事件源服务器是否已配置正确。

Postfix 系统以两种格式生成事件：

- 包含消息相关信息的多行事件（附带唯一 ID）。这些事件具有以下形式：
  <syslog PRI> time host process_name: ID: information from base event 1

<syslog PRI> time host process_name: ID: information from base event 2

- 包含错误相关信息的单行事件（不附带 ID）。这些事件具有以下形式：

  <syslog PRI> time host process_name: severity: basic information for parsing

一组 KUMA 资源用于处理 Postfix 事件；创建收集器时必须应用此资源集：

- 规范化器
- 聚合规则
- 目标位置过滤器

收集器根据事件 ID 聚合多行基础事件，对其进行规范化处理，然后将聚合后的事件发送至存储和关联器。

聚合事件具有以下形式：

Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

聚合完成后，接收到的事件会发送至同一收集器，聚合事件将在该收集器中接受规范化处理。

Postfix 事件处理算法

已采用以下算法来处理 Postfix 事件：

1. 初始规范化

   在此阶段，对通过系统日志接收的以“<”字符开头的基础事件进行初始规范化。事件将被转换为适合后续聚合处理的格式：从事件中提取第一个字符并将其放入 FlexString1 字段，将标识符放入 ExternalID 字段，将主机名称放入 DeviceHostName 字段。基本规范化在主规范化器中执行。

2. 检查聚合情况

   检查事件是否已聚合。因此，非聚合事件（第一个字符不是“{”且 ID 不为空）将应用聚合规则，然后聚合事件将被发送以进行重新规范化处理。

3. 应用聚合规则

   在此阶段，聚合规则会应用于事件，系统整理基础事件并呈现为以下形式：

   Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

4. 聚合完成后，整理后的事件被发送回同一个收集器，以便聚合事件接受规范化处理。

   要关闭事件处理循环，必须指定与目标位置相同的收集器。图中，目标位置名为“Loop”，以突出事件处理循环这一核心机制。您可以为目标位置指定任意名称。

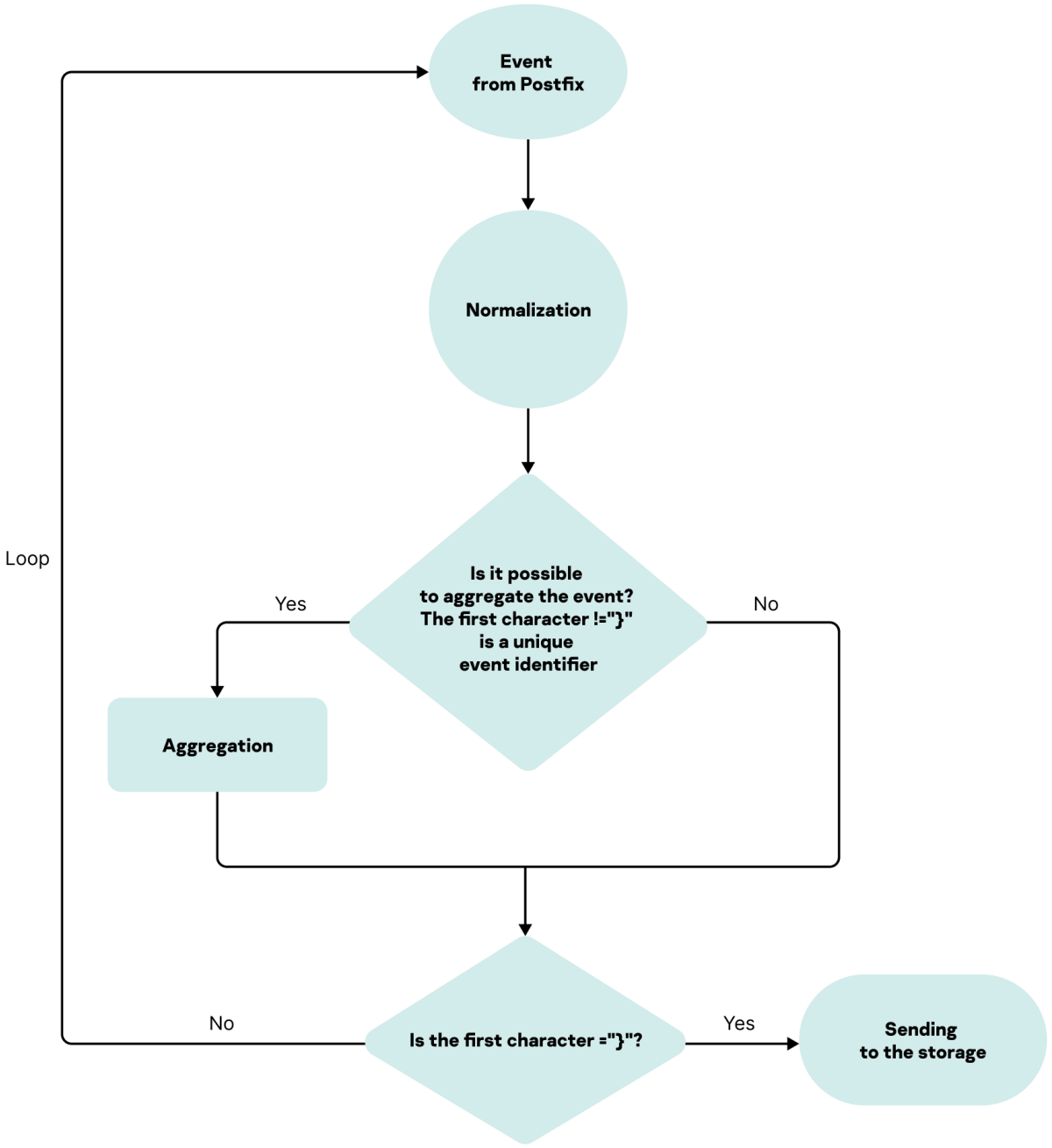
5. 聚合事件的规范化

   以“{”字符开头的聚合事件的规范化在下列额外规范化器中执行：聚合事件、聚合事件。消息 KV 解析器、聚合事件。消息正则表达式 1、聚合事件。消息正则表达式 2。

6. 发送到存储和关联器

   经过聚合和规范化处理的事件被发送到存储和关联器。

下图为 Postfix 事件处理流程图。



Postfix 系统事件处理流程图

配置 Postfix 以发送事件

默认情况下，Postfix 系统的审计事件会输出到 /var/log/maillog 或 /var/log/mail。

要将事件发送到 KUMA：

1. 创建 /etc/rsyslog.conf 文件的备份副本。
2. 打开 /etc/rsyslog.conf 文件进行编辑。

3. 在 /etc/rsyslog.conf 文件末尾添加以下行：

```
mail.* @@<IP address of the KUMA collector>:<port of the KUMA collector>
```

4. 保存 /etc/rsyslog.conf 文件。

5. 重新启动 rsyslog 服务：

```
sudo systemctl restart rsyslog
```

配置 KUMA 收集器以接收和处理 Postfix 事件

要配置 KUMA 收集器以接收 Postfix 事件：

1. 从 KUMA 存储库导入 [OOTB] Postfix 软件包。该软件包适用于 KUMA 3.0 及更高版本。

2. 创建一个新的收集器，并在收集器安装向导中配置以下内容：

    1. 在**传输方式**步骤中，在**类型**字段中，选择**tcp**类型，并在**URL**字段中指定收集器的FQDN或IP地址和端口。

    2. 在**事件解析**步骤中，单击**添加事件解析**，然后在显示的**事件基础解析**窗口的**规范化器**下拉列表中，选择**[OOTB] Postfix syslog**规范器。

    3. 在**事件聚合**步骤中，单击**添加聚合**规则，然后在显示的**事件聚合**窗口中，从**聚合规则**下拉列表中选择**[OOTB] Postfix。聚合规则**"。

    4. 在**路由**步骤中，单击**添加**，然后在显示的**创建目标位置**窗口中，逐个创建三个目标点 – 名称为Loop的同一个收集器、一个存储和一个关联器。

        a. 使用以下参数创建名为 Loop 的目标位置。

        - 在**基本设置基本设置类型**下拉列表中，选择**tcp**传输类型；在**URL**字段中，指定您之前在本说明的步骤2.1中指定的收集器的FQDN或IP地址和端口。
        - 在**高级设置**选项卡的**过滤器**下拉列表中，选择**后缀。"事件聚合过滤器**"过滤器。

          此配置对于将聚合事件发送到同一收集器进行后续规范化处理是不可缺少的。

        b. 创建关联器目标位置：

        c. 在**基本设置**选项卡上的**类型**下拉列表中，选择**关联器**并填写**URL**字段。

        d. 在**高级设置**选项卡的**过滤器**下拉列表中，选择**后缀。将聚合事件发送到存储和关联器**。

        e. 创建存储目标位置：

        - 在**基本设置**选项卡上的**类型**下拉列表中，选择**存储**并填写**URL**字段。
        - 在**高级设置**选项卡的**过滤器**下拉列表中，选择**后缀。将聚合事件发送到存储和关联器**。

          此配置的作用是将聚合后的规范化事件发送到存储和关联器。

3. 单击"**创建**"按钮。

   使用 KUMA 控制台中指定的设置创建收集器服务。将显示在服务器上安装该服务的命令。

4. 复制收集器安装命令并在相关服务器上运行该命令。

收集器配置为接收和处理 Postfix 事件。

配置 CommuniGate Pro 事件的接收

您可以在 KUMA 中配置接收 CommuniGate® Pro 6.1 事件。仅当使用 TCP 协议，通过 syslog 发送事件时才可集成。本文描述的资源适用于 KUMA 3.0 及更高版本。支持处理 SIP 模块事件（此类事件包含“SIPDATA”字符序列）。

配置事件接收包括以下步骤：

1. 配置 CommuniGate Pro 以发送事件
2. 配置 KUMA 收集器以接收 CommuniGate Pro 事件
3. 验证 KUMA 收集器中是否收到 CommuniGate Pro 事件
   您可以在 KUMA 控制台的“搜索相关事件”部分验证 CommuniGate Pro 事件源服务器是否已正确配置。

CommuniGate Pro 系统会将审计事件生成为几个单独的记录，如下所示：

```
<event code> timestamp ID direction: information from base event 1

<event code> timestamp ID direction: information from base event 2

<event code> timestamp ID direction: base information n
```

一组 KUMA 资源用于处理 CommuniGate Pro 事件；创建收集器时必须应用此资源集：

- 规范化器
- 聚合规则
- 目标位置过滤器

收集器根据事件 ID 聚合多行基础事件，对其进行规范化处理，然后将聚合后的事件发送至存储和关联器。

聚合事件具有以下形式：

```
Service information from the aggregation rule: ID: information from base event 1,
information from base event 2, information from base event n
```

聚合完成后，接收到的事件会发送至同一收集器，聚合事件将在该收集器中接受规范化处理。

CommuniGate Pro 事件的处理算法

已采用以下算法来处理 CommuniGate Pro 事件：

1. 初始规范化
   在此阶段，会执行基础事件的初始规范化。基础事件中的第一个字符是数字。事件将被转换为适合后续聚合处理的格式：从事件中提取第一个字符并将其放入 DeviceCustomString1 字段，将标识符放入 ExternalID 字段，将主机名称放入 DeviceHostName 字段。基本规范化在主规范化器中执行。

2. 检查聚合情况

   检查事件是否已聚合。因此，会对未聚合的事件（第一个字符是数字）应用聚合规则，然后将聚合事件发送至重新规范化处理。使用 **[OOTB] CommuniGate Pro 执行聚合操作。聚合规则**。

3. 应用聚合规则

   在此阶段，聚合规则会应用于事件，系统整理基础事件并呈现为以下形式：

   Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

   聚合完成后，整理后的事件被发送回同一个收集器，以便聚合事件接受规范化处理。

   要关闭事件处理循环，必须指定与目标位置相同的收集器。图中，目标位置名为“Loop”，以突出事件处理循环这一核心机制。您可以为目标位置指定任意名称。

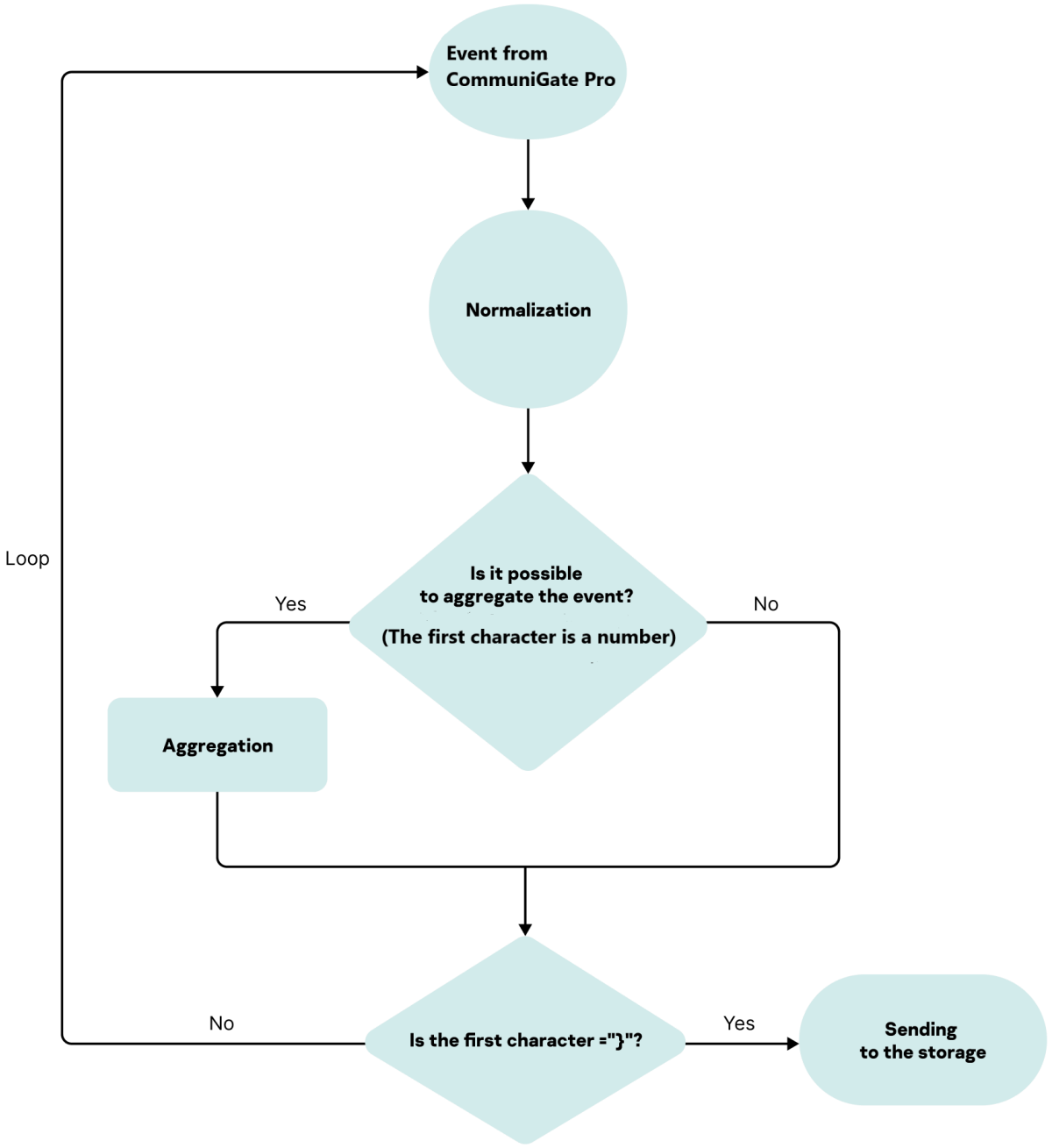
4. 聚合事件的规范化

   以“{”字符开头的聚合事件的规范化在下列额外规范化器中执行：聚合事件、聚合事件 - kv 部分。

5. 发送到存储和关联器

   经过聚合和规范化处理的事件被发送到存储和关联器。

下图为 CommuniGate Pro 事件处理流程图。



CommuniGate Pro 系统事件处理流程图

配置 CommuniGate Pro 以发送事件

默认情况下，CommuniGate Pro 审计事件会发送到 /var/CommuniGate/SystemLogs/ 目录中的 .log 文件。

要将事件发送到 KUMA，您需要在 CommuniGate Pro 服务器上安装 KUMA 代理，并将其配置为读取 /var/CommuniGate/SystemLogs/ 目录中的 .log 文件，并通过 TCP 将其发送到 KUMA 收集器。

要创建用于读取事件并将其发送到 KUMA 的代理：

1. 在 KUMA 控制台中，转到“**资源和服务**” → “**代理**”，然后单击“**添加**”。
2. 这将打开**创建代理程序**窗口；在该窗口中，在**基本设置**选项卡上的**名称**字段中，指定代理程序名称。

3. 在“**配置 #1**”选项卡上，填写以下字段：

   a. 在**基本设置**选项卡上的**连接器**设置组中，为连接器设置以下值：

      1. 在“**名称**”字段中，输入名称，例如 `CommuniGate file`。
      2. 在“**类型**”下拉列表中，选择“**文件**”。
      3. 在“**文件路径**”字段中，输入以下值：
         /var/CommuniGate/SystemLogs/.*.log

   b. 在**基本设置**选项卡上的**目标位置**设置组中，为目标位置设置以下值：

      1. 在“**名称**”字段中，输入名称，例如 `CommuniGate TCP collector`。
      2. 在“**类型**”下拉列表中，选择“**tcp**”。
      3. 在“**URL**”字段中，输入 KUMA 收集器的 FQDN 或 IP 地址和端口。

4. 单击“**创建**”按钮。

5. 在 KUMA 中创建代理服务后，请在要通过其向收集器发送数据的网络基础设施设备上安装代理。

配置 KUMA 收集器以接收和处理 CommuniGate Pro 事件

要配置 KUMA 收集器以接收 CommuniGate Pro 事件：

1. 从 KUMA 存储库导入 [OOTB] CommuniGate Pro 软件包。该软件包适用于 KUMA 3.0 及更高版本。

2. 创建一个新的收集器，并在收集器安装向导中配置以下内容：

   1. 在**传输方式**步骤中，在**类型**字段中，选择**tcp**类型，并在**URL**字段中指定收集器的FQDN或IP地址和端口。
   2. 在**事件解析**步骤中，单击**添加事件解析**，然后在显示的**事件基础解析**窗口的**规范化器**下拉列表中，选择**[OOTB] CommuniGate Pro**规范化器。
   3. 在**事件聚合**步骤中，单击**添加聚合规则**，然后在显示的**事件聚合**窗口的**聚合规则**下拉列表中，选择**[OOTB] CommuniGate Pro。聚合规则**。
   4. 在**路由**步骤中，单击**添加**，然后在显示的**创建目标位置**窗口中，逐个创建三个目标点 – 名称为`Loop`的同一个收集器、一个存储和一个关联器。

      a. 使用以下参数创建名为 `Loop` 的目标位置。

      - 在**基本设置**选项卡上的**类型**下拉列表中，选择**tcp**传输类型；在**URL**字段中，指定您之前在本说明的步骤2.1中指定的收集器的FQDN或IP地址和端口。
      - 在**高级设置**选项卡的**筛选器**下拉列表中，选择**[OOTB] CommuniGate Pro。“事件聚合过滤器**”过滤器。

      此配置对于将聚合事件发送到同一收集器进行后续规范化处理是不可缺少的。

b. 创建关联器目标位置：

- 在**基本设置**选项卡上的**类型**下拉列表中，选择**关联器**并填写**URL**字段。
- 在**高级设置**选项卡的**筛选器**下拉列表中，选择**[OOTB] CommuniGate Pro。将聚合事件发送到存储和关联器**。

c. 创建存储目标位置：

- 在**基本设置**选项卡上的**类型**下拉列表中，选择**存储**并填写**URL**字段。
- 在**高级设置**选项卡的**筛选器**下拉列表中，选择**[OOTB] CommuniGate Pro。将聚合事件发送到存储和关联器**。

此配置的作用是将聚合后的规范化事件发送到存储和关联器。

3. 单击"**创建**"按钮。
   使用 KUMA 控制台中指定的设置创建收集器服务。将显示在服务器上安装该服务的命令。
4. 复制收集器安装命令并在相关服务器上运行该命令。

收集器配置为接收和处理 CommuniGate Pro 事件。

配置 Yandex Cloud 事件的接收

您可以在 KUMA 中配置 Yandex Cloud 事件的接收。规范化器支持处理存储在 .json 文件中的配置级审计事件。

配置事件接收包括以下步骤：

1. 配置 Yandex Cloud 事件的审计。
2. 配置 Yandex Cloud 事件的导出。
3. 配置 KUMA 收集器以接收和处理 Yandex Cloud 事件。
   要在 KUMA 收集器安装向导中接收 Yandex Cloud 事件：
   1. 在KUMA收集器安装向导的**传输方式**步骤中，选择**文件**类型的连接器。
   2. 在 **URL** 字段中，输入 `/var/log/yandex-cloud/<audit_trail_id>/*/*/*/*.json`，其中 <audit_trail_id> 是审计 ID。
   3. 在**事件解析**步骤的**规范化器**字段中，选择**[OOTB] Yandex Cloud**。
4. 在 KUMA 网络基础设施中安装收集器。
5. 验证 KUMA 收集器中是否收到 Yandex Cloud 事件
   要验证 Yandex Cloud 事件源服务器是否配置正确，您可以搜索相关事件。

配置 Yandex Cloud 事件的审计

配置事件导出分阶段进行：

1. 准备使用 Yandex Cloud 的环境。
2. 创建审计日志存储桶。
3. 在密钥管理服务中创建加密密钥。
4. 启用存储桶加密。
5. 创建服务账户。
6. 创建静态密钥。
7. 将角色分配给服务账户。
8. 创建审计跟踪。

准备使用 Yandex Cloud 的环境。

要管理配置，您需要 Yandex Cloud CLI；安装并进行初始化。

注意：默认情况下，在 CLI 配置文件中指定的 Yandex Cloud 文件夹中执行审计。您可以使用 `--folder-name` 或 `--folder-id` 参数指定其他文件夹。

要配置审计，您需要一个有效的结算账户，因为使用 Yandex Cloud 基础架构需要付费。

要配置 Yandex Cloud 审计，您需要一个有效的结算账户：

1. 前往管理控制台，然后登录 Yandex Cloud 或注册。
2. 在“Yandex Cloud Billing”页面，确保您已绑定结算账户，并且其状态为“ACTIVE”或“TRIAL_ACTIVE”。如果您没有结算账户，请创建一个。

如果您有有效的结算账户，则可以在云页面中创建或选择一个 Yandex Cloud 文件夹，您的基础架构将在该文件夹中运行。

创建审计日志存储桶

要创建存储桶：

1. 在管理控制台中，转到要在其中创建存储桶的文件夹，例如 **example-folder**。
2. 选择“**对象存储**”服务。

3. 单击“**创建存储桶**”。
4. 在存储桶创建页面上：
    1. 按照命名规则输入存储桶名称，例如 **kumabucket**。
    2. 如有必要，可限制存储桶的最大容量。容量为“0”表示无限制，相当于启用“**无限制**”选项。
    3. 对于访问类型，选择“**受限**”。
    4. 选择默认存储类别。
    5. 单击“**创建存储桶**”。

存储桶创建完成。

在密钥管理服务中创建加密密钥

要创建加密密钥：

1. 在管理控制台中，转到 **example-folder** 文件夹。
2. 选择“**密钥管理服务**”。
3. 单击“**创建密钥**”按钮并指定以下设置：
    - 名称（例如，**kuma-kms**）。
    - 加密算法，**AES-256**。
    - 其余设置保留默认值。
4. 点击“**创建**”按钮。

加密密钥已创建。

启用存储桶加密

要启用存储桶加密：

1. 在管理控制台中，转到您之前创建的存储桶。
2. 在左侧窗格中，选择“**加密**”。
3. 在“**KMS 密钥**”字段中，选择“**kuma-kms**”密钥。
4. 单击“**保存**”按钮。

存储桶加密已启用。

创建服务账户

要创建服务账户（用于跟踪的单独账户和用于存储桶的单独账户）：

1. 创建 **sa-kuma** 服务账户：
    1. 在管理控制台中，转到 **example-folder** 文件夹。
    2. 在屏幕上方，进入“**服务账户**”选项卡。
    3. 单击“**创建服务账户**”并输入服务账户的名称（例如 **sa-kuma**），确保名称符合命名规则：
        - 长度：3 到 63 个字符
        - 可以包含拉丁字母的小写字母、数字和连字符
        - 第一个字符必须是字母，最后一个字符不能是连字符
    4. 点击“**创建**”按钮。
2. 创建 **sa-kuma-bucket** 服务账户：
    1. 在管理控制台中，转到 **example-folder** 文件夹。
    2. 在屏幕上方，进入“**服务账户**”选项卡。
    3. 单击“**创建服务账户**”，输入服务账户名称（例如 **sa-kuma-bucket**），注意名称必须符合命名规则：
        - 长度：3 到 63 个字符
        - 可以包含拉丁字母的小写字母、数字和连字符
        - 第一个字符必须是字母，最后一个字符不能是连字符
    4. 点击“**创建**”按钮。

服务账户创建完成。

创建静态密钥

挂载存储桶时，您需要密钥 ID 和私钥。您可以使用管理控制台或 CLI 来创建密钥。

要使用管理控制台创建密钥，请执行以下操作：

1. 在管理控制台中，转到 **example-folder** 文件夹。
2. 在屏幕上方，进入“**服务账户**”选项卡。
3. 选择 **sa-kuma-bucket** 服务账户，然后单击其名称所在的行。

4. 在上部的面板中，单击“**创建新密钥**”。
5. 选择“**创建静态访问密钥**”。
6. 输入密钥的描述，然后单击“**创建**”。
7. 保存 ID 和密钥。

静态访问密钥已创建。关闭对话框后，密钥值将不可用。

要使用 CLI 创建密钥：

1. 为 **sa-kuma-bucket** 服务账户创建访问密钥：

   ```
   yc iam access-key create --service-account-name sa-kuma-bucket
   ```

   结果：

   ```
   access_key:
   id: aje*******k2u
   service_account_id: aje*******usm
   created_at: "2022-09-22T14:37:51Z"
   key_id: 0n8*******0YQ
   secret: JyT*******zMP1
   ```

2. 保存“secret”值中的 key_id 和密钥。您将无法再次获取密钥值。

访问密钥已创建。

将角色分配给服务账户

要将 audit-trails.viewer、storage.uploader 和 kms.keys.encrypterDecrypter 角色分配给 sa-kuma 服务账户：

1. 在 CLI 中，将 audit-trails.viewer 角色分配给文件夹：

   ```
   yc resource-manager folder add-access-binding \
   --role audit-trails.viewer \
   --id <folder_id> \
   --service-account-id <service_account_id>
   ```

   其中：

   - `--role` 是分配的角色。
   - `--id` 是“example-folder”文件夹的 ID。
   - `--service-account-id` 是 sa-kuma 服务账户的 ID。

2. 将 storage.uploader 角色分配给包含存储桶的文件夹：

   ```
   yc resource-manager folder add-access-binding \
   --role storage.uploader \
   --id <folder_id> \
   ```

```
--service-account-id <service_account_id>
```

其中：

- `--role` 是分配的角色。
- `--id` 是“example-folder”文件夹的 ID。
- `--service-account-id` 是 sa-kuma 服务账户的 ID。

3. 将 kms.keys.encrypterDecrypter 角色分配给 kuma-kms 加密密钥：

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

其中：

- `--role` 是分配的角色。
- `--id` 是 kuma-kms KMS 密钥的 ID。
- `--service-account-id` 是 sa-kuma 服务账户的 ID。

要将 storage.viewer 和 kms.keys.encrypterDecrypter 角色分配给 sa-kuma-bucket 服务账户：

1. 在 CLI 中，将 storage.viewer 角色分配给文件夹：

```
yc resource-manager folder add-access-binding \
--id <folder_id> \
--role storage.viewer \
--service-account-id <service_account_id>
```

其中：

- `--id` 是“example-folder”文件夹的 ID。
- `--role` 是分配的角色。
- `--service-account-id` 是 sa-kuma-bucket 服务账户的 ID。

2. 将 kms.keys.encrypterDecrypter 角色分配给 kuma-kms 加密密钥：

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

其中：

- `--role` 是分配的角色。
- `--id` 是 kuma-kms KMS 密钥的 ID。
- `--service-account-id` 是 sa-kuma-bucket 服务账户的 ID。

创建审计跟踪

要创建审计跟踪：

1. 在管理控制台中，转到 **example-folder** 文件夹。
2. 选择“**审计跟踪**”服务。
3. 单击“**创建跟踪**”并为要创建的跟踪指定名称，例如 **kuma-trail**。
4. 在“**目标位置**”部分，指定目标位置对象的参数：
   - **目标位置**：**对象存储**。
   - **存储桶**：存储桶的名称，例如 **kumabucket**。
   - **对象前缀**：可选参数，用于构成审计日志文件的完整名称。
     如果您将审计日志和第三方数据存储在同一个存储桶中，请使用前缀。请勿对存储桶中的日志和其他对象使用相同的前缀，因为这可能会导致日志和第三方对象相互覆盖。
   - **加密密钥**：指定存储桶加密所使用的 kuma-kms 加密密钥。
5. 在“**服务账户**”部分，选择“**sa-kuma**”。
6. 在“**收集管理事件**”部分，指定收集管理事件审计日志的设置：
   - **收集事件**：选择“**已启用**”。
   - **资源**：选择“**文件夹**”。
   - **文件夹**：无需填写，其中包含当前文件夹的名称。
7. 在“**收集数据事件**”的“**收集事件**”字段中，选择“**已禁用**”。
8. 点击“**创建**”按钮。

配置 Yandex Cloud 事件的导出

存储桶必须挂载到将安装 KUMA 收集器的服务器上。

要挂载存储桶：

1. 在服务器上，为“kuma”用户创建一个目录：
   ```
   sudo mkdir /home/kuma
   ```
2. 在服务器上，为 sa-kuma-bucket 服务账户创建一个带有静态访问密钥的文件，并向“kuma”用户授予适当的访问权限：
   ```
   sudo bash -c 'echo <access_key_ID>:<secret_access_key> > /home/kuma/.passwd-s3fs'
   sudo chmod 600 /home/kuma/.passwd-s3fs
   sudo chown -R kuma:kuma /home/kuma
   ```

3. 安装 s3fs 软件包：

   ```
   sudo apt install s3fs
   ```

4. 创建必须挂载存储桶的目录并将权限授予 kuma 用户：

   ```
   sudo mkdir /var/log/yandex-cloud/
   sudo chown kuma:kuma /var/log/yandex-cloud/
   ```

5. 挂载存储桶：

   ```
   sudo s3fs kumabucket /var/log/yandex-cloud -o passwd_file=/home/kuma/.passwd-s3fs -o url=https://storage.yandexcloud.net -o use_path_request_style -o uid=$(id -u kuma) -o gid=$(id -g kuma)
   ```

   您可以通过在 /etc/fstab 中添加一行来将存储桶配置为在操作系统启动时挂载，例如：

   ```
   s3fs#kumabucket /var/log/yandex-cloud fuse _netdev,uid=<kuma_uid>,gid=<kuma_gid>,use_path_request_style,url=https://storage.yandexcloud.net,passwd_file=/home s3fs 0 0
   ```

   其中：

   <kuma_uid> 是操作系统中 kuma 用户的 ID。

   <kuma_gid> 是操作系统中 kuma 用户组的 ID。

   要查看 kuma_uid 和 kuma_gid，请在控制台中运行以下命令：

   ```
   id kuma
   ```

6. 验证存储桶是否已挂载：

   ```
   sudo ls /var/log/yandex-cloud/
   ```

   如果一切配置正确，该命令将返回 <audit_trail_id>，其中 <audit_trail_id> 是审计跟踪 ID。

Yandex Cloud 事件的导出已配置。事件将位于 .json 文件里的目录中：

/var/log/yandex-cloud/{audit_trail_id}/{year}/{month}/{day}/*.json

配置 Microsoft 365 事件的接收

您可以在 KUMA 中配置接收来自 Microsoft 365 (Office 365®) 云解决方案的事件。

配置事件接收包括以下步骤：

1. 使用标准 Microsoft 方法配置对 Office 365 管理 API https://learn.microsoft.com/en-us/office/office-365-management-api/get-started-with-office-365-management-apis 的访问

   要在 KUMA 中接收事件，请授予必要的 API 权限集：

   Microsoft.Graph

   Directory.Read.All

   Office 365 管理 API

   ActivityFeed.Read

   ActivityFeed.Read.Dlp

2. 创建 KUMA 收集器。

要接收 Microsoft 365 事件，请使用以下参数创建收集器：

- 在**传输方式**步骤中，指定**office365**连接器类型。
- 在"**解析事件**"步骤中，指定 **[OOTB] Microsoft Office 365 json** 规范化器。

3. 在 KUMA 网络基础设施中安装收集器
4. 在 KUMA 收集器中验证 Windows Microsoft 365 事件的接收情况

   要验证 Microsoft 365 事件源服务器是否配置正确，您可以搜索相关事件。

配置 Kontinent 加密系统事件的接收

Kaspersky Next XDR Expert 分发包中包含 kuma-kont 实用程序，该实用程序由一个可执行文件和一个配置文件组成。支持的操作系统包括 Astra Linux、Ubuntu 22.04 LTS 和 RED OS 7.3.4 和 8。该实用程序可用于连接 MSSQL 数据库、接收 Kontinent 加密系统事件，并将数据以 JSON 格式发送到 KUMA 收集器。Kontinent 3.9.2 支持数据导入。

配置从 MSSQL 数据库检索 Kontinent 事件并将其发送到 KUMA 收集器包括以下步骤：

1. 准备接收 Kontinent 事件。

   在此步骤中，您需要创建一个将接收事件的 KUMA 收集器，并在 MSSQL 数据库中创建一个用户。

2. 配置 KUMA-kont 实用程序。

   在此步骤中，您需要创建该实用程序的配置文件和该实用程序的服务。

3. 启动 kuma-kont 实用程序。

   激活后，该实用程序开始从 MS SQL 数据库导出事件，并将其发送到 KUMA 收集器。它会在 kuma-kont.log 文件中记录日志。

准备接收 Kontinent 事件

1. 创建 KUMA 收集器。

   1. 为 Kontinent 3.9 事件创建 KUMA 收集器。

      要使用收集器安装向导接收Kontinent 3.9系统的审计事件，请在**事件解析**步骤中选择**[OOTB] SecurityCode Continent 3.9 json**规范化器。此外，在**传输方式**选项卡上，您需要根据*配置Kontinent 3.9事件导出*说明的第2.1.4段来指定端口和协议。

   2. 在 Kaspersky Next XDR Expert 网络基础架构中安装收集器。

2. 在 MS SQL DBMS 中创建账户。

   在数据库中创建一个账户，并授予其连接并读取以下表格中数据的最低必要权限：ALERTLOG、SERVERACCESSLOG、SYSTEMLOG、PACKETLOG、FILTERS。

3. 确保网络连接正常。

   您必须确保运行该实用程序的服务器与 Kontinent 系统的数据库服务器之间以及运行该实用程序的服务器与 KUMA 收集器服务器之间的网络连接正常。

配置 kuma-kont 实用程序

配置 kuma-kont 实用程序包括以下步骤：

1. 创建 kuma-kont-config.yaml 配置文件。
2. 创建 KUMA-kont 服务。

创建 kuma-kont-config.yaml 配置文件

要创建 kuma-kont-config.yaml 配置文件：

1. 执行以下命令，转到 Kaspersky Next XDR Expert 安装程序目录：
   ```
   cd kuma-ansible-installer/roles/kuma/files
   ```
2. 将 KUMA-kont.tar 压缩文件解压：
   ```
   tar -xvf kuma-kont.tar
   ```
3. 转到实用程序目录：
   ```
   cd kuma-kont
   ```
4. 复制 kuma-kont-config-template.yaml 模板以创建名为 kuma-kont-config.yaml 的配置文件：
   ```
   cp kuma-kont-config-template.yaml kuma-kont-config.yaml
   ```
5. 更改配置文件的读取权限：
   ```
   sudo chown <用户名>:<组> kuma-kont-config.yaml
   sudo chmod 600 kuma-kont-config.yaml
   ```
   将 <user name> 替换为服务将使用的操作系统用户名。
6. 编辑 kuma-kont-config.yaml 配置文件中的设置。
   指定以下参数的值：
   - 常规设置：state_file、log_file_path。
   - Kontinent 数据库：名称、用户、密码、主机、端口。
   - KUMA 收集器：地址、端口、协议。
     kuma-kont-config-template.yaml 文件中给出了配置示例。
7. 将更改保存到文件。

配置文件被创建。

创建服务

要创建 kuma-kont 服务：

1. 更改可执行文件的执行权限：

   ```
   sudo chown <用户名>:<组> <可执行文件路径>
   sudo chmod 700 <可执行文件路径>
   ```

2. 创建 /etc/systemd/system/kuma-kont.service 文件，内容如下：

   ```
   [Unit]
   Description=Connector Kontinent 3.9
   After=network.target
   [Service]
   User=<用户名>
   ExecStart=<可执行文件路径> --config <配置文件路径>
   Restart=always
   RestartSec=10
   [Install]
   WantedBy=multi-user.target
   ```

   将 <user name> 替换为服务将使用的操作系统用户名。

3. 指定可执行文件的路径。

   在 ExecStart 字段中指定 kuma-kont 可执行文件的路径。

   例如，如果 kuma-kont 文件位于 /usr/bin/ 目录中，请保留默认值。

4. 指定配置文件的路径。

   在 ExecStart 字段中指定 kuma-kont-config.yaml 配置文件的路径。例如，如果 kuma-kont-config.yaml 文件位于 /path/to/ 目录中，请指定该路径。

   kuma-kont.service 文件示例

   ```
   [Unit]
   Description=Continent Service
   After=network.target
   [Service]
   User=user-example
   ExecStart=./usr/bin/kuma-kont --config /path/to/kuma-kont-config.yaml
   Restart=always
   RestartSec=10
   [Install]
   WantedBy=multi-user.target
   ```

5. 加载 systemd 配置：

   ```
   sudo systemctl daemon-reload
   ```

6. 将该服务设置为在开机时运行：

   ```
   sudo systemctl enable kuma-kont
   ```

kuma-kont 实用程序将在系统启动时作为服务启动。

启动和管理 kuma-kont 服务

要启动实用程序服务，请运行以下命令：

```
sudo systemctl start kuma-kont
```

开始从 MSSQL 数据库收集事件，并将事件发送到 KUMA 收集器。

可以使用以下命令控制实用程序服务：

1. 启动 KUMA-kont 服务：

   ```
   sudo systemctl start kuma-kont
   ```

2. 停止 KUMA-kont 服务：

   ```
   sudo systemctl stop kuma-kont
   ```

3. 重新启动 kuma-kont 服务：

   ```
   sudo systemctl restart kuma-kont
   ```

您还可以使用作为应用程序运行的 kuma-kont 实用程序来发送事件。要开始向 KUMA 收集器发送事件，您需要在可执行文件所在的目录中运行以下命令：

```
./kuma-kont --config < kuma-kont-config.yaml 文件的路径 >
```

连接丢失时的行为

与 MSSQL 数据库的连接。

如果与 MSSQL 数据库的连接丢失，该实用程序会每 n 秒尝试重新连接一次（其中 n 等于配置文件中 poll_interval 设置的值），直到连接恢复正常。

与 KUMA 收集器的连接

如果使用 TCP 协议发送事件，则当与 KUMA 收集器的连接丢失时，该实用程序也会尝试恢复连接。连接尝试的间隔会逐渐增加，直至达到一小时，之后的重新连接尝试将每小时进行一次。

已知限制

来自 `AlertLog` 表且 AL_CATEGORY=5 的事件未被完全解码。

kuma-kont-config.yaml 配置文件中的设置

该表列出了您可以在 KUMA-kont-config.yaml 文件中指定的设置。

kuma-kont-config.yaml 配置文件中的设置

设置	描述
`debug`	“**常规设置**”组中的可选设置。 用于需要输出调试级别日志时。 如果设置为“false”，则仅包含启动和停止消息，以及发送过程中发生的错误。 可用值： • **true** • **false** 默认设置：**false**。
`need_reconnect`	“**常规设置**”组中的可选设置。 此设置确定实用程序是否在每次请求时重新连接到数据库。 可用值： • **true** • **false** 默认设置：**false**。
`state_file`	“**常规设置**”组中的必需设置。 保存所处理日志状态的 JSON 文件的绝对路径。 该文件将在此路径下自动创建。 请确保用户具有足够的权限写入此目录。 示例：/home/user/kuma-kont/state.json
`log_file_path`	“**常规设置**”组中的必需设置。 用于记录连接器活动的日志文件的绝对路径。 该文件将在此路径下自动创建。 请确保用户具有足够的权限写入此目录。 示例：/home/user/kuma-kont/kuma-kont.log
`poll_interval`	“**常规设置**”组中的可选设置。 数据库轮询间隔。 默认设置是10秒。 对于高 EPS，建议将值设置为 15 秒以内。
`name`	“**Kontinent 数据库**”组中的必需设置。 接收 Kontinent 日志的数据库名称。
`user`	“**Kontinent 数据库**”组中的必需设置。 数据库用户的名称。
`password`	“**Kontinent 数据库**”组中的必需设置。 数据库用户的密码。
`host`	“**Kontinent 数据库**”组中的必需设置。 数据库服务器的 URL。
`port`	“**Kontinent 数据库**”组中的必需设置。 数据库服务器的端口。 确保可以从安装该实用程序的服务器进行访问。
`limit`	“**Kontinent 数据库**”组中的可选设置。 单次轮询可从数据库下载的事件数量上限。 默认情况下，每次数据库轮询的事件数量为 100,000 条。 如果 EPS 较高，建议设置为等于或大于此值。
`alert_log`	“**最后 ID**”组中的可选设置。 指定从哪个 AlertLog 类型的事件开始向 KUMA 收集器发送事件。 仅在首次运行或状态文件不存在时有效。 默认值是 0。
`packet_log`	“**最后 ID**”组中的可选设置。 指定从哪个 PacketLog 类型的事件开始向 KUMA 收集器发送事件。 仅在首次运行或状态文件不存在时有效。 默认值是 0。

设置	描述
`server_access_log`	“**最后 ID**”组中的可选设置。 指定从哪个 ServerAccessLog 类型的事件开始向 KUMA 收集器发送事件。 仅在首次运行或状态文件不存在时有效。 默认值是 0。
`system_log`	“**最后 ID**”组中的可选设置。 指定从哪个 SystemLog 类型的事件开始向 KUMA 收集器发送事件。 仅在首次运行或状态文件不存在时有效。 默认值是 0。
`address`	“**KUMA 收集器**”组中的必需设置。 KUMA 收集器所在服务器的完全限定域名 (FQDN) 或 IP 地址。
`port`	“**KUMA 收集器**”组中的必需设置。 KUMA 收集器的端口。
`protocol`	“**KUMA 收集器**”组中的必需设置。 KUMA 收集器使用的数据传输协议。 如果使用 UDP 协议，则在与 KUMA 收集器的连接中断时，不会重新发送事件。 可用值： • TCP • UDP

与其他解决方案集成

在本部分中，您将了解如何将 KUMA 与其他解决方案集成以增强其功能。

与 Kaspersky Security Center 集成

您可以在 OSMP 控制台中创建或编辑 Kaspersky Security Center 集成设置。

在 OSMP 控制台中，您可以查看一个、多个或所有 KUMA 租户与所选 Kaspersky Security Center 服务器的集成。如果启用了与卡巴斯基安全管理中心的集成，您可以手动导入资产、编辑自动计划导入间隔或暂时禁用计划导入。

配置 Kaspersky Security Center 资产的数据刷新间隔

KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

- 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
- 资产属性信息：漏洞；软件，包括操作系统；资产所有者

要配置来自 Kaspersky Security Center 的资产数据刷新间隔：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要导入KSC资产信息的租户。
   这将打开"租户属性"窗口。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产设置**。
4. 在**KSC导入**选项卡中，确保**状态**切换开关已打开。
5. 指定从卡巴斯基安全管理中心自动导入资产信息和资产漏洞信息的时间间隔：
   - 在**硬件信息**下的**导入间隔（小时）**字段中，输入自动导入资产基本属性信息的间隔时间（以小时为单位）。默认设置是1小时。
   - 在**资产属性**下的**导入间隔（小时）**字段中，输入自动导入资产其他属性信息的间隔时间（以小时为单位）。默认设置是12小时。
     导入有关资产属性（漏洞、软件、所有者）的信息可能涉及下载大量数据，这可能需要更长的时间才能完成，我们建议设置比硬件信息导入更长的间隔。
6. 单击"**保存**"按钮。

所选租户的 Kaspersky Security Center 资产数据更新设置已配置完成。

如果所需的租户不在租户列表中，请使用 OSMP 控制台将其添加到租户列表中。

按计划导入 Kaspersky Security Center 资产

要设置导入 Kaspersky Security Center 资产的计划：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在"**集成**"下，单击"**Kaspersky Security Center**"。
   Kaspersky Security Center 集成窗口将打开。
3. 选择要为其计划导入 Kaspersky Security Center 资产的租户。
   Kaspersky Security Center 集成窗口将打开。
4. 如有必要，请取消选中"**已禁用**"复选框以启用所选租户与 Kaspersky Security Center 的集成。默认情况下，此复选框未被选中。
   如果您要暂时禁用所选租户与 Kaspersky Security Center 的集成，请选中"**已禁用**"复选框。这将关闭按计划导入 Kaspersky Security Center 资产的功能。
5. 在"**数据刷新间隔**"字段中，指定 KUMA 更新 Kaspersky Security Center 设备数据的时间间隔。
   间隔以小时为单位，并且必须是整数。

默认时间间隔为 12 小时。

6. 单击“**保存**”按钮。

将应用为所选租户按计划导入 Kaspersky Security Center 资产指定的设置。

手动导入 Kaspersky Security Center 资产

KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

- 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
- 资产属性信息：漏洞；软件，包括操作系统；资产所有者

要手动导入 Kaspersky Security Center 资产：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要导入KSC资产信息的租户。
   该租户的属性窗口将打开。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产设置**。
4. 在KSC**导入**选项卡中，确保**状态**切换开关已打开。
5. 指定从卡巴斯基安全管理中心自动导入资产信息和资产漏洞信息的时间间隔：
   - 若要导入资产基本属性信息，请在**硬件信息**下，点击**导入**按钮。
   - 若要导入资产其他属性信息，请在**资产属性**下，点击**导入**按钮。

此时将创建*KSC资产导入*任务。无论配置的计划如何，都会为指定租户导入 Kaspersky Security Center 资产。

查看 Kaspersky Security Center 服务器的层次结构

要查看 Kaspersky Security Center 服务器的层次结构：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在“**集成**”下，单击“**Kaspersky Security Center**”。
   Kaspersky Security Center 集成窗口将打开。
3. 在“**租户**”下拉列表中，选择要查看其层次结构的租户。
   “**连接参数**”窗口将打开。
4. 在“**连接参数**”窗口中，单击“**加载层次结构**”。

指定租户的 Kaspersky Security Center 服务器的层次结构显示在“**连接参数**”窗口中。

从 Kaspersky Security Center 数据库导入事件

在 KUMA 中，您可以从 Kaspersky Security Center SQL 数据库接收事件。使用收集器接收事件，收集器使用以下资源：

- 预定义连接器：[OOTB] KSC MSSQL 或 [OOTB] KSC MySQL。
- 预定义 [OOTB] KSC from SQL 规范化器。

配置从 Kaspersky Security Center 导入事件的操作包含以下步骤：

1. 创建预定义连接器的副本。

   预定义连接器的设置不可编辑，因此，要配置与数据库服务器的连接，必须创建预定义连接器的副本。

2. 创建收集器：
   - 在 Web 界面中。
   - 在服务器上。

要配置从 Kaspersky Security Center 导入事件：

1. 创建与 Kaspersky Security Center 使用的数据库类型相对应的预定义连接器的副本：
   a. 在 OSMP 控制台的“**监控**” → “**资源**” → “**连接器**”部分中，在文件夹层次结构中找到相关的预定义连接器，选中该连接器旁边的复选框，然后单击“**复制**”。
   b. **创建连接器**窗口随即打开。在该窗口的**基本设置**选项卡的**默认查询**字段中，如有必要，请将KAV数据库名称替换为您所使用的Kaspersky Security Center数据库的名称。

      向 Kaspersky Security Center SQL 数据库查询示例如下

      SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

      ev.product_name AS product_name, ev.product_version AS product_version,

      ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As msg,

      CASE

      WHEN ev.rise_time is not NULL THEN
      DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time)

      ELSE ev.rise_time

      END

      AS endTime,

      CASE

      WHEN ev.registration_time is not NULL

```
THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )

ELSE ev.registration_time

END

AS kscRegistrationTime,

cast(ev.par7 as varchar(4000)) as sourceUserName,

hs.wstrWinName as dHost,

hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,

CAST(hs.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp % 256 AS VARCHAR) AS sourceAddress,

serv.wstrWinDomain as kscNtDomain,

CAST(serv.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp % 256 AS VARCHAR) AS kscIP,

CASE

WHEN virus.tmVirusFoundTime is not NULL

THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )

ELSE ev.registration_time

END

AS virusTime,

virus.wstrObject As filePath,

virus.wstrVirusName as virusName,

virus.result_ev as result

FROM KAV.dbo.ev_event as ev

LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId

INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1
```

Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus

where registration_time >= DATEADD(minute, -191, GetDate())

c. 将光标放在“**URL**”字段中，然后在显示的列表中，单击在您正在使用的密钥行中的 。

d. 这将打开“**密钥**”窗口；在该窗口的“**URL**”字段中，按以下格式指定服务器连接地址：

`sqlserver://user:password@kscdb.example.com:1433/database`

其中：

- `user` — 具有所需数据库的 public 权限和 db_datareader 权限的用户账户。
- `password` — 用户账户密码。
- `kscdb.example.com:1433` — 数据库服务器的地址和端口。
- `database` — Kaspersky Security Center 数据库的名称。默认为“KAV”。

单击“**保存**”按钮。

e. 在“**创建连接器**”窗口的“**连接**”部分的“**查询**”字段中，将“KAV”数据库名称替换为您正在使用的 Kaspersky Security Center 数据库的名称。

如果要使用查询所引用的 ID 列，则必须执行此操作。

单击“**保存**”按钮。

2. 在 Web 界面中安装收集器：

a. 通过下列其中一种方式启动收集器安装向导：

- 在OSMP控制台中的**监控→资源**部分中，单击**添加事件源**。
- 在 OSMP 控制台中的“**监控**” → “**资源**” → “**收集器**”部分中，单击“**添加收集器**”。

b. 在安装向导的步骤 1“**连接事件源**”中，指定收集器名称并选择租户。

c. 在安装向导的步骤2**传输方式**中，选择您在步骤1中创建的连接器的副本。

d. 在安装向导的步骤3**事件解析**中，在**解析方案**选项卡上，单击**添加事件解析**。

e. 此时将打开“**事件基础解析**”窗口；在该窗口的“**规范化方案**”选项卡上，从“**规范化器**”下拉列表中选择“**[OOTB] KSC from SQL**”，然后单击“**确定**”。

f. 如有必要，请根据收集器的要求指定其他设置。为了导入事件，可以在安装向导的其余步骤中编辑设置。

g. 在安装向导的步骤 8“**安装验证**”中，单击“**创建并保存服务**”。

窗口下部显示在服务器上安装收集器必须使用的命令。将此命令复制到剪贴板。

h. 单击**保存收集器**以关闭收集器安装向导。

3. 在服务器上安装收集器。

为此，在您想要接收 Kaspersky Security Center 事件的服务器上，运行在 Web 界面中创建收集器后复制到剪贴板的命令。

这样一来，收集器就将安装完成，并且可以从 Kaspersky Security Center 的 SQL 数据库接收事件。

您可以在 Web 界面的“**事件**”部分查看 Kaspersky Security Center 事件。

Kaspersky Endpoint Detection and Response 集成

Kaspersky Endpoint Detection and Response （以下简称“KEDR”）是 Kaspersky Anti Targeted Attack Platform 的一个功能单元，用于保护企业 LAN 中的资产。

您可以配置 KUMA 与 Kaspersky Endpoint Detection and Response 的集成，以管理对连接到 Kaspersky Endpoint Detection and Response 服务器的资产以及 Kaspersky Security Center 资产执行的威胁响应操作。执行操作的命令由 Kaspersky Endpoint Detection and Response 服务器接收，然后将这些命令转发到安装在资产上的 Kaspersky Endpoint Agent。

您还可以将事件导入 KUMA 并接收有关 Kaspersky Endpoint Detection and Response 警报的信息（有关警报的更多详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助中的“*配置与 SIEM 系统的集成*”部分）。

当 KUMA 与 Kaspersky Endpoint Detection and Response 集成时，您可以对搭载了 Kaspersky Endpoint Agent 的 Kaspersky Endpoint Detection and Response 资产执行以下操作：

- 管理资产的网络隔离。
- 管理防护规则。
- 启动应用程序。

要获取有关配置响应操作管理集成的说明，请联系您的客户经理或技术支持。

使用 kafka 连接器导入 Kaspersky Endpoint Detection and Response 事件

从 Kaspersky Endpoint Detection and Response 导入事件时，遥测数据以明文形式传输，可能会被入侵者截获。

可以使用 Kafka 连接器将 Kaspersky Endpoint Detection and Response 4.0、4.1、5.0 和 5.1 事件导入 KUMA。

从 Kaspersky Endpoint Detection and Response 4.0 和 4.1 导入事件有几个限制：

- 如果在 Kaspersky Endpoint Detection and Response 中使用 KATA 和 KEDR 授权许可密钥，则可以导入事件。
- 如果将安装在单独服务器上的传感器组件用作 Kaspersky Endpoint Detection and Response 的一部分，则**无法**导入事件。

要导入事件，请执行 Kaspersky Endpoint Detection and Response 和 KUMA 中的操作。

从 Kaspersky Endpoint Detection and Response 4.0 或 4.1 导入事件

要将 Kaspersky Endpoint Detection and Response 4.0 或 4.1 事件导入 KUMA：

在 Kaspersky Endpoint Detection and Response 中：

1. 使用 SSH 或终端登录到要从中导出事件的中央节点服务器的管理控制台。
2. 根据系统提示，输入在安装 Kaspersky Endpoint Detection and Response 期间设置的管理员账户名和密码。
   程序组件管理员菜单随即出现。
3. 在程序组件管理员菜单中，选择“**技术支持模式**”。
4. 按下“**Enter**”。
   “技术支持模式”确认窗口随即打开。
5. 确认您要在技术支持模式下操作应用程序。为此，请选择“**是**”并按下“**Enter**”。
6. 执行以下命令：
   ```
   sudo -i
   ```
7. 在 `/etc/sysconfig/apt-services` 配置文件的 `KAFKA_PORTS` 字段中，删除值 `10000`。

   如果从属中央节点服务器或安装在单独服务器上的传感器组件连接到中央节点服务器，则需要允许通过端口 10000 连接到您修改了配置文件的服务器。

   不建议将此端口用于除 KUMA 之外的任何外部连接。要仅允许 KUMA 通过端口 10000 建立连接，请运行以下命令：

   ```
   iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP
   ```
8. 在配置文件 `/usr/bin/apt-start-sedr-iptables` 中，在 `WEB_PORTS` 字段内添加值 `10000`，使用逗号分隔且逗号后不加空格。
9. 执行以下命令：
   ```
   sudo sh /usr/bin/apt-start-sedr-iptables
   ```

现在，在 Kaspersky Endpoint Detection and Response 端导出事件的准备工作已经完成。

在Kaspersky Next XDR Expert的SIEM组件中：

1. 在 KUMA Core 服务器上，将中央节点服务器的 IP 地址以 `<IP address> centralnode` 格式添加到以下文件之一：
   - `%WINDIR%\System32\drivers\etc\hosts` — 对于 Windows。
   - `/etc/hosts file` — 对于 Linux。

2. 在OSMP控制台中，创建一个Kafka类型的连接器。

   创建连接器时，指定以下参数：

   - 在 **URL** 字段中，指定 `<Central Node server IP address>:10000`。
   - 在 **主题** 字段中，指定 `EndpointEnrichedEventsTopic`。
   - 在“**消费者组**”字段中，指定任意唯一名称。

3. 在OSMP控制台中，创建收集器。

   使用上一步创建的连接器作为收集器的传输通道。使用“[OOTB] KEDR 遥测”作为收集器的规范化器。

如果已成功创建并安装收集器，Kaspersky Endpoint Detection and Response 事件将导入 KUMA。您可以在事件表中找到并查看这些事件。

从 Kaspersky Endpoint Detection and Response 5.0 和 5.1 导入事件

从 Kaspersky Endpoint Detection and Response 5.0 和 5.1 导入事件时有几个限制：

- 仅非高可用性版本的 Kaspersky Endpoint Detection and Response 支持事件导入功能。
- 如果在 Kaspersky Endpoint Detection and Response 中使用 KATA 和 KEDR 授权许可密钥，则可以导入事件。
- 如果将安装在单独服务器上的传感器组件用作 Kaspersky Endpoint Detection and Response 的一部分，则**无法**导入事件。

要将 Kaspersky Endpoint Detection and Response 5.0 或 5.1 事件导入 KUMA：

在 Kaspersky Endpoint Detection and Response 中：

1. 使用 SSH 或终端登录到要从中导出事件的中央节点服务器的管理控制台。
2. 根据系统提示，输入在安装 Kaspersky Endpoint Detection and Response 期间设置的管理员账户名和密码。

   程序组件管理员菜单随即出现。
3. 在程序组件管理员菜单中，选择“**技术支持模式**”。
4. 按下“**Enter**”。

   “技术支持模式”确认窗口随即打开。
5. 确认您要在技术支持模式下操作应用程序。为此，请选择“**是**”并按下“**Enter**”。
6. 在 `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.py` 配置文件中，为 `WEB_PORTS` 常量指定附加端口 `10000`：

   ```
   WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
   ```

   ```
   You do not need to perform this step for Kaspersky Endpoint Detection and Response 5.1
   because the port is specified by default.
   ```
7. 运行以下命令：

   ```
   kata-firewall stop
   ```

```
kata-firewall start --cluster-subnet <network mask for addressing cluster servers>
```

现在，在 Kaspersky Endpoint Detection and Response 端导出事件的准备工作已经完成。

在Kaspersky Next XDR Expert的SIEM组件中：

1. 在 KUMA Core 服务器上，将中央节点服务器的 IP 地址以 `<IP address> kafka.services.external.dyn.kata` 格式添加到下列文件之一：
   - `%WINDIR%\System32\drivers\etc\hosts` — 对于 Windows。
   - `/etc/hosts file` — 对于 Linux。
2. 在OSMP控制台中，创建一个Kafka类型的连接器。
   创建连接器时，指定以下参数：
   - 在 **URL** 字段中，指定 `<Central Node server IP address>:10000`。
   - 在 **主题** 字段中，指定 `EndpointEnrichedEventsTopic`。
   - 在“**消费者组**”字段中，指定任意唯一名称。
3. 在OSMP控制台中，创建收集器。
   使用上一步创建的连接器作为收集器的传输通道。建议使用 *[OOTB] KEDR 遥测*规范化器作为收集器的规范化器。

如果已成功创建并安装收集器，Kaspersky Endpoint Detection and Response 事件将导入 KUMA。您可以在事件表中找到并查看这些事件。

使用 kata/edr 连接器导入 Kaspersky Endpoint Detection and Response 事件

要使用 kata/edr 连接器从主机导入 Kaspersky Endpoint Detection and Response 5.1 或更早版本的事件：

1. 在SIEM组件中配置接收事件。为此，在OSMP控制台中，使用“kata/edr”连接器创建并安装收集器，或编辑现有收集器，然后保存修改后的设置并重新启动收集器。
2. 在KEDR端，接受来自SIEM组件的授权请求，以开始在Kaspersky Next XDR Expert中接收事件。

因此，集成随即配置，KEDR事件开始传输到Kaspersky Next XDR Expert。

创建收集器以接收来自 KEDR 的事件

要创建用于接收来自 KEDR 事件的收集器：

1. 在OSMP控制台中，前往**资源和服务→收集器**，选择**添加收集器**。
2. “**创建收集器**”窗口将打开。在该窗口的步骤 1“**连接事件源**”中，指定任意“**收集器名称**”，然后在下拉列表中选择相应的**租户**。

3. 在步骤 2 "**传输方式**"中，执行以下操作：

   1. 在"**基本设置**"选项卡上：

      a. 在**连接器**字段中，选择**创建**，如果要使用之前创建的连接器，则在该字段开始输入连接器的名称。

      b. 在**连接器类型**下拉列表中，选择**kata/edr**连接器。选择 kata/edr 连接器类型后，将显示更多需要填写的字段。

      c. 在"**URL**"字段中，按照 <主机的名称或 IP 地址>:<连接端口，默认使用端口 443> 的格式指定连接到 KEDR 服务器的地址。如果 KEDR 解决方案部署在集群中，您可以单击"**添加**"以添加所有节点。KUMA 将按顺序连接到每个指定节点。如果 KEDR 解决方案安装在分布式配置中，则在 KUMA 端，您必须为每个 KEDR 服务器配置单独的收集器。

      d. 在**密钥**字段中，选择**创建**以创建新的密钥。将打开"**创建密钥**"窗口；在该窗口中，指定"**名称**"，然后单击"**生成并下载证书和私有加密密钥**"。

      结果，certificate.zip 压缩文件将下载到浏览器的"下载"文件夹中；该压缩文件中包含"key.pem"密钥文件和"cert.pem"证书文件。对压缩文件进行解压。单击"**上传证书**"并选择 cert.pem 文件。单击"**上传私钥**"并选择 key.pem 文件。单击"**创建**"按钮。该密钥将添加到"**密钥**"下拉列表中，并被自动选中。

      您也可以从"**密钥**"列表中选择已创建的密钥。KUMA 使用选定的密钥连接到 KEDR。

      e. "**外部 ID**"字段包含外部系统的 ID。授权 KUMA 服务器时，此 ID 将显示在 KEDR Web 界面中。KUMA 会自动生成 ID，并且"**外部 ID**"字段会自动预填充。

   2. 在"**高级设置**"选项卡上：

      a. 要获取收集器日志中的详细信息，请将"**调试**"切换开关移至启用位置。

      b. 如有必要，在"**字符编码**"字段中，选择要转换为 UTF-8 的源数据编码。仅建议在规范化事件的字段中发现无效字符时配置转换。默认情况下，未选中任何值。

      c. 指定每次向KEDR发出请求的**事件数**。默认值为 0，表明 KUMA 将使用 KEDR 服务器上指定的值。有关详情，请参阅KATA 帮助。您可以指定任意值，但不得超过 KEDR 端的值。如果指定的值超过了KEDR服务器上指定的**最大事件数**设置，则KUMA收集器日志将显示错误信息：*请求错误：max_events参数的值N大于允许的最大值*。

      d. 填写"**事件获取超时时间**"字段，以便在指定的时间段后接收事件。默认值是 0。这意味着将应用 KEDR 服务器的默认值。有关详情，请参阅"KATA 帮助"。该字段指定了 KEDR 服务器必须在多长时间后向 KUMA 发送事件。KEDR 服务器使用两个参数：最大事件数和事件获取超时时间。当收集到指定数量的事件或配置的时间已到（以先发生者为准）时，将发送事件。如果已到达指定时间，但尚未收集到指定数量的事件，则 KEDR 服务器将发送已收集的事件，而无需等待更多事件。

      e. "**客户端超时时间**"字段指定了 KUMA 必须等待 KEDR 服务器响应的时间（以秒为单位）。默认值为 1,800 秒，显示为 0。"**客户端超时时间**"字段指定了客户端等待响应的时间限制。**客户端超时时间**时间必须大于服务器的**事件获取超时时间**，以确保客户端持续等待服务器响应，不会因发起新请求而中断当前事件收集任务。若最终未能收到 KEDR 服务器的响应，KUMA 会重复发起请求。

      f. 在"**KEDRQL 筛选器**"字段中，指定筛选请求的条件。如此，便能从 KEDR 接收经过预筛选的事件。有关可用筛选器字段的详细信息，请参阅"KATA 帮助"。

4. 在步骤 3"**解析**"中，单击"**添加事件解析**"，然后在"**事件基础解析**"窗口中选择"**[OOTB] KEDR 遥测**"。

5. 要在 Web 界面中完成收集器创建，请单击"**创建并保存服务**"。然后从 Web 界面复制收集器安装命令，并在要安装收集器的服务器的命令行上运行此安装命令。

   如果您正在编辑现有收集器，请单击"**保存并重启服务**"。

因此，收集器创建完成并可以发送请求。在 KEDR 接受来自 KUMA 的授权请求之前，收集器会显示在“**资源和服务 → 活动服务**”部分中，状态为黄色。

在 KEDR 端授权 KUMA

在 KUMA 中创建收集器后，要确保 KUMA 的请求开始到达 KEDR，必须在 KEDR 端接受 KUMA 授权请求。授权请求被接受后，KUMA 收集器会自动向 KEDR 发送预定的请求并等待响应。等待期间，收集器的状态为黄色；收到首个请求响应后，收集器的状态变为绿色。

集成随即配置，您可以在OSMP控制台的**事件**部分查看来自KEDR的事件。

初始请求获取在配置集成之前发生的部分历史事件。所有历史事件接收完毕后，当前事件开始传入。如果您更改 **URL** 设置的值或现有收集器的**外部 ID**，KEDR 会将下一个请求视为初始请求，并且在使用修改后的设置启动 KUMA 收集器后，您将再次收到部分历史事件。如果您不想接收历史事件，请转到相关收集器的设置，在规范化器中配置 KEDR 和 KUMA `timestamp` 字段的映射，并在收集器安装向导的“事件筛选”步骤中按 `timestamp` 指定筛选器 — 事件的 `timestamp` 必须大于收集器启动时的 `timestamp`。

可能出现的错误和解决方案

如果在收集器日志中看到“*冲突：已存在具有以下 IP 和证书摘要的外部系统”。删除该系统，或提供新证书*的错误提示，请在收集器的连接器中创建一个包含新证书的新密钥。

如果在收集器日志中看到事件请求响应中出现“*未找到延续令牌*”错误，请创建一个新连接器，将其附加到收集器并重启收集器；或者，在收集器的连接器中创建一个包含新证书的新密钥。如果您不想接收错误发生之前生成的事件，请在收集器中配置时间戳筛选器。

配置在 KUMA 警报中显示指向 Kaspersky Endpoint Detection and Response 检测的链接

当收到 Kaspersky Endpoint Detection and Response 检测时，KUMA 会为每个检测创建警报。您可以配置在 KUMA 警报信息中显示指向 Kaspersky Endpoint Detection and Response 检测的链接。

如果您在 Kaspersky Endpoint Detection and Response 中仅使用一个中央节点服务器，则可以配置显示检测链接。如果在分布式解决方案模式下使用Kaspersky Endpoint Detection and Response，则无法在KUMA中配置显示指向Kaspersky Endpoint Detection and Response检测的链接。

要配置在 KUMA 警报详情中显示指向检测的链接，您需要完成 Kaspersky Endpoint Detection and Response Web 界面和 KUMA 中的步骤。

在 Kaspersky Endpoint Detection and Response Web 界面中，您需要将该应用程序配置为与作为 SIEM 系统的 KUMA 集成。有关配置集成的详细信息，请参阅 *Kaspersky Anti Targeted Attack Platform* 文档中的“*配置与 SIEM 系统的集成*”部分。

在OSMP控制台中设置显示链接包括以下步骤：

1. 添加资产，其中包含要从中接收检测信息的 Kaspersky Endpoint Detection and Response 中央节点服务器的相关信息，并将某个类别分配给该资产。
2. 创建关联规则。
3. 创建关联器。

您可以使用预配置的关联规则。在这种情况下，在 OSMP 控制台中配置显示链接的操作包括以下步骤：

1. 创建关联器。

   选择 `[OOTB] KATA Alert` 关联规则。
2. 添加资产，其中包含要从中接收检测信息的 Kaspersky Endpoint Detection and Response 中央节点服务器的相关信息，并将 `KATA standAlone` 类别分配给该资产。

步骤 1：添加资产并为其分配类别

首先，您需要创建一个类别，该类别将分配给要添加的资产。然后添加资产。

要添加资产：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**” → “**检测和响应**”。
2. 然后单击“**添加**”按钮。

   “**添加资产**”详情区域在窗口右侧打开。
3. 定义以下资产参数：
   a. 在“**资产名称**”字段中，输入资产名称。
   b. 在“**租户**”下拉列表中，选择将拥有该资产的租户。
   c. 在“**IP 地址**”字段中，指定要从中接收检测的 Kaspersky Endpoint Detection and Response 中央节点服务器的 IP 地址。
   d. 在“**类别**”字段中，选择您在上一步中添加的类别。

   > 如果您使用预定义的关联规则，则需要选择 `KATA standAlone` 类别。

   e. 如有必要，定义下列字段的值：
   - 在“**FQDN**”字段中，指定 Kaspersky Endpoint Detection and Response 服务器的完全限定域名。
   - 在“**MAC 地址**”字段中，指定 Kaspersky Endpoint Detection and Response 中央节点服务器的 MAC 地址。
   - 在“**所有者**”字段中，定义资产所有者的姓名。
4. 单击“**保存**”按钮。

步骤 2：添加关联规则

要添加关联规则：

1. 在主菜单中，前往**监控→资源和服务**。
2. 选择**关联规则**，然后单击**创建关联规则**按钮。
3. 在“**常规**”选项卡上，指定以下设置：
   a. 在“**名称**”字段中，定义规则名称。
   b. 在“**类型**”下拉列表中，选择“**简单**”。
   c. 在“**传播字段**”字段中，添加以下字段：DeviceProduct、DeviceAddress、EventOutcome、SourceAssetID、DeviceAssetID。
   d. 如有必要，定义下列字段的值：
      - 在“**频率限制**”字段中，定义将触发规则的每秒最大次数。
      - 在“**严重级别**”字段中，定义由于触发规则而创建的警报和关联事件的严重级别。
      - 在“**描述**”字段中，提供任何附加信息。
4. 在“**选择器**” → “**设置**”选项卡中，指定以下设置：
   a. 在“**过滤器**”下拉列表中，选择“**新建**”。
   b. 在“**条件**”字段中，单击“**添加组**”按钮。
   c. 在您添加的组的运算符字段中，选择“**AND**”。
   d. 添加按 KATA 值过滤的条件：
      1. 在“**条件**”字段中，单击“**添加条件**”按钮。
      2. 在“条件”字段中，选择“**If**”。
      3. 在“**左操作数**”字段中，选择“**事件字段**”。
      4. 在“**事件**”字段中，选择“**DeviceProduct**”。
      5. 在“**运算符**”字段中，选择“=”。
      6. 在“**右操作数**”字段中，选择“**常量**”。
      7. 在**值**字段中，输入KATA。
   e. 添加类别过滤条件：
      1. 在“**条件**”字段中，单击“**添加条件**”按钮。
      2. 在“条件”字段中，选择“**If**”。
      3. 在“**左操作数**”字段中，选择“**事件字段**”。

4. 在**事件**字段中，选择**设备资产 ID**。

5. 在“**运算符**”字段中，选择“**inCategory**”。

6. 在“**右操作数**”字段中，选择“**常量**”。

7. 单击 按钮。

8. 选择您放置 Kaspersky Endpoint Detection and Response 中央节点服务器资产的类别。

9. 单击“**保存**”按钮。

f. 在“**条件**”字段中，单击“**添加组**”按钮。

g. 在您添加的组对应的运算符字段中，选择“**OR**”。

h. 添加按事件类标识符过滤的条件：

1. 在“**条件**”字段中，单击“**添加条件**”按钮。

2. 在“条件”字段中，选择“**If**”。

3. 在“**左操作数**”字段中，选择“**事件字段**”。

4. 在“**事件**”字段中，选择“**DeviceEventClassID**”。

5. 在“**运算符**”字段中，选择“=”。

6. 在“**右操作数**”字段中，选择“**常量**”。

7. 在**值**字段中，输入**taaScanning**。

i. 对以下每个事件类 ID 重复 F 中的步骤 1-7：

- file_web。
- file_mail。
- file_endpoint。
- file_external。
- ids。
- url_web。
- url_mail。
- dns。
- iocScanningEP。
- yaraScanningEP。

5. 在“**操作**”选项卡上，指定以下设置：

   a. 在“**操作**”部分中，打开“**每次事件发生时**”下拉列表。

   b. 选中“**输出**”复选框。

   c. 在“**增强**”部分中，单击“**添加增强**”按钮。

   d. 在**来源类型**下拉列表中，选择**模板**。

   e. 在“**模板**”字段中，输入“*https://{{.DeviceAddress}}:8443/katap/#/alerts?id={{.EventOutcome}}*”。

   f. 在“**目标字段**”下拉列表中，选择“**DeviceExternalID**”。

   g. 如有必要，请打开“**调试**”切换开关以记录与资源操作相关的信息。

6. 单击“**保存**”按钮。

步骤 3：创建关联器

您需要启动关联器安装向导。在向导的步骤 3中，您需要选择按照本指南添加的关联规则。

创建关联器后，从 Kaspersky Endpoint Detection and Response 接收检测结果时所创建警报的详细信息中会显示指向这些检测结果的链接。该链接显示在关联事件详情（“**威胁搜索**”部分）的“**DeviceExternalID**”字段中。

如果您希望 Kaspersky Endpoint Detection and Response Central Node 服务器的 FQDN 显示在检测详情的“DeviceHostName”字段中，则需要为该服务器创建 DNS 记录，并在向导的步骤 4中创建 DNS 增强规则。

与 Kaspersky CyberTrace 集成

Kaspersky CyberTrace（以下简称“CyberTrace”）是一种将威胁数据流与 SIEM 解决方案集成的工具。它为用户提供对分析数据的即时访问权限，从而提高他们对安全决策的认知水平。

您可以通过以下方式之一将 CyberTrace 与 KUMA 集成：

- 集成 CyberTrace 指标搜索功能，以使用来自 CyberTrace 数据流的信息来增强 KUMA 事件。
- 将整个 CyberTrace Web 界面集成到 KUMA 中以获得对 CyberTrace 的完全访问权限。

  仅当您的 CyberTrace 授权许可包含多用户功能时，才可以进行 CyberTrace 控制台集成。

集成 CyberTrace 指标搜索

要集成 CyberTrace 指标搜索：

1. 配置 CyberTrace 以接收和处理 KUMA 请求。

   您可以在快速启动向导中安装 CyberTrace 后立即配置与 KUMA 的集成，也可以稍后在 CyberTrace Web 界面中配置。

2. 创建事件扩展规则。

   在增强规则中，您可以指定要使用 CyberTrace 中的哪些数据来增强事件。

3. 创建一个收集器来接收您想要使用 CyberTrace 数据来增强的事件。

4. 将增强规则关联到收集器。

5. 保存并创建服务：

   - 如果将规则关联到新的收集器，请单击“**保存并创建**”，在打开的窗口中复制收集器 ID，然后使用复制的 ID，通过命令行界面在服务器上安装收集器。
   - 如果将规则关联到现有收集器，请单击“**保存并重新启动服务**”以应用这些设置。

   CyberTrace 指标搜索功能集成的配置已完成，KUMA 事件将使用 CyberTrace 数据进行增强。

CyberTrace 数据增强测试示例

默认情况下，KUMA 不会测试与 CyberTrace 的连接。

如果您想测试与 CyberTrace 的集成并确保事件增强操作正常运行，您可以按照以下示例的步骤操作或根据您的情况调整示例。该示例展示了一个集成测试，它执行增强操作并显示事件包含指定的测试 URL。

要运行测试：

1. 使用下表列出的参数创建一个测试增强规则。

设置	参数值
名称	测试 CT 增强
租户	共享
源类型	cybertrace
网址	<您要向其发送请求的 cybertrace 服务器的 URL>：9999
映射	KUMA 字段：RequestURL CyberTrace 指标：url
调试	已启用

1. 使用以下参数创建测试收集器：

   在步骤 2“**传输**”中，指定 http 连接器。

   在步骤 3“**解析**”中，指定规范化器并选择 json 解析方法，设置 RequestUrl – RequestUrl 字段的映射。

   在步骤 6“**增强**”中，指定“测试 CT 增强”规则。

   在步骤 7“**路由**”中，指定事件必须发送到的存储。

2. 单击“**创建并保存服务**”。

   窗口中显示安装收集器的完整命令。

3. 单击“**复制**”，将命令复制到剪贴板并在命令行中运行该命令。等待命令完成后，返回 KUMA 控制台，然后单击“**保存收集器**”。

   测试收集器已创建，测试增强规则将关联至该收集器。

4. 使用命令行界面向收集器发送请求，这将触发一个事件，然后该事件将使用测试 URL `http://fakess123bn.nu` 进行增强。例如：

```
curl --request POST \
  --url http://<安装收集器的主机 ID>:<收集器的端口>/input \
  --header 'Content-Type: application/json' \
  --data '{"RequestUrl":"http://fakess123bn.nu"}'
```

5. 转到 KUMA“**事件**”部分并运行以下查询以过滤事件输出并找到经过增强的事件：

```
SELECT * FROM `events` WHERE RequestUrl = 'http://fakess123bn.nu' ORDER BY Timestamp
DESC LIMIT 250
```

结果：

增强成功完成，该事件现在具有一个值为 `http://fakess123bn.nu` 的 **RequestURL** 字段，以及包含 CyberTrace 数据的 TI 指标和指标类别。

如果测试未实现增强，例如，如果威胁情报指标缺失，建议执行以下操作：

1. 检查收集器和增强规则的设置。
2. 使用以下命令下载收集器日志并查找日志中的错误：

```
tail -f /opt/kaspersky/kuma/collector/<collector ID>/log/collector
```

配置 CyberTrace 以接收和处理请求

安装 CyberTrace 后，您可立即在快速启动向导中配置该工具以接收并处理来自 KUMA 的请求，也可后续在程序 Web 界面中进行配置。

要在快速启动向导中配置 CyberTrace 以接收和处理请求：

1. 程序安装完成后，等待 CyberTrace 快速启动向导启动。

   “**欢迎使用 Kaspersky CyberTrace**”窗口随即打开。

2. 在 **选择 SIEM** 下拉列表中，选择要从中接收数据的 SIEM 系统类型，然后单击 **下一步** 按钮。

   “**连接参数**”窗口将打开。

3. 执行以下操作：

   a. 在“**服务监听**”设置区块中，选择“**IP 和端口**”选项。

   b. 在“**IP 地址**”字段中，输入 `0.0.0.0`。

   c. 在“**端口**”字段中，输入用于接收事件的端口，默认端口为 `9999`。

   d. 在“**服务发送事件至**”下，在“**IP 地址或主机名**”字段中指定 `127.0.0.1`，并在“**端口**”字段中指定 `9998`。

   保留其他所有选项的默认值。

   e. 单击“**下一步**”。

   “**代理设置**”窗口随即打开。

4. 如果您的组织正在使用代理服务器，请定义连接代理服务器的设置。如果没有，请将所有字段留空，然后单击“**下一步**”。

   “**授权许可设置**”窗口随即打开。

5. 在“**Kaspersky CyberTrace 授权许可密钥**”字段中，添加 CyberTrace 的授权许可密钥。

6. 在“**Kaspersky Threat Data Feeds 证书**”字段中，添加允许您从服务器下载更新数据馈送的证书，然后单击“**下一步**”。

CyberTrace 将配置完成。

要在程序 Web 界面中配置 CyberTrace 以接收和处理请求：

1. 在 CyberTrace Web 界面中，选择“**设置**” – “**服务**”。

2. 在“**连接设置**”区块中：

   a. 选择“**IP 和端口**”选项。

   b. 在“**IP 地址**”字段中，输入 `0.0.0.0`。

   c. 在“**端口**”字段中，指定接收事件的端口，默认端口为 `9999`。

3. 在“**Web 界面**”设置区块的“**IP 地址或主机名**”字段中，输入 `127.0.0.1`。

4. 在上方的工具栏中，单击“**重新启动 CyberTrace 服务**”。

5. 选择“**设置**” - “**事件格式**”。

6. 在“**警报事件格式**”字段中，输入 `%Date% alert=%Alert%%RecordContext%`。

7. 在“**检测事件格式**”字段中，输入 `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`。

8. 在“**记录上下文格式**”字段中，输入 `|%ParamName%=%ParamValue%`。

9. 在“**可操作字段上下文格式**”字段中，输入 `%ParamName%:%ParamValue%`。

CyberTrace 将配置完成。

更新 CyberTrace 配置后，您必须重新启动 CyberTrace 服务器。

创建事件增强规则

要创建事件增强规则：

1. 在主菜单中，前往**监控→资源和服务→扩展规则**。

2. 在窗口左侧，选择或创建一个文件夹用于存放新规则。

   可用增强规则的列表将显示。

3. 单击**创建**以创建新规则。

   将显示增强规则窗口。

4. 输入规则配置参数：

   a. 在“**名称**”字段中，输入规则的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。

   b. 在“**租户**”下拉列表中，选择将拥有此资源的租户。

   c. 在**来源类型**下拉列表中，选择**CyberTrace**。

   d. 指定要连接的 CyberTrace 服务器的 **URL**。例如，*example.domain.com:9999*。

   e. 如有必要，使用“**连接数**”字段指定 OSMP 可以同时建立的 CyberTrace 服务器最大连接数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。

   f. 在“**RPS**”字段中，输入 OSMP 每秒可以向 CyberTrace 服务器发送的请求数。默认值为 `1000`。

   g. 在“**增强队列中的最大事件数量**”中，指定存储在增强队列中用于重新发送的最大事件数量。默认值为 `1000000`。

   h. 在“**超时**”字段中，指定 OSMP 等待 CyberTrace 服务器响应的最大秒数。直到收到响应或指定时间到期时，事件才不会发送到关联器。如果在超时之前收到响应，则将其添加到事件的 `TI` 字段，并继续处理事件。默认值为 `30`。

   i. 使用 “**Debug**”下拉列表指示是否启用服务操作日志记录。日志记录默认被禁用。

   j. 在**“标签”**下拉列表中，选择事件增强规则的标签。

   k. 如有必要，在“**描述**”字段中添加最多 4,000 个 Unicode 字符来描述资源。

   l. 在“**映射**”下，您必须指定要通过 CyberTrace 检查的事件字段，并定义将 KUMA 事件字段映射到 CyberTrace 指标类型的规则：

      - 在“**KUMA 字段**”列中，选择必须发送其值到 CyberTrace 的字段。
      - 在“**CyberTrace 指标**”列中，为每个所选字段选择 CyberTrace 指标类型：
        - **ip**
        - **url**
        - **哈希**

      您必须向表格提供至少一个字符串。您可以单击**添加**按钮来添加字符串，也可以单击 × 按钮来删除字符串。

   m. 在“**过滤器**”部分，您可以指定条件来识别将通过增强规则来处理的事件。您可以从**筛选器**下拉列表中选择现有过滤器，也可以**创建**筛选器。

      在资源中创建过滤器

      KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

要创建过滤器：

1. 在“**过滤器**”下拉列表中，选择“**新建**”。

2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。

3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。

4. 在**“条件”**下，指定事件必须满足的条件：

   a. 单击“**添加条件**”按钮。

   b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。

   c. 在“**运算符**”下拉列表中，选择一个运算符。

   过滤器运算符

   - **=** — 左操作数等于右操作数。
   - **<** — 左操作数小于右操作数。
   - **<=** — 左操作数小于或等于右操作数。
   - **>** — 左操作数大于右操作数。
   - **>=** — 左操作数大于或等于右操作数。
   - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
   - **contains** — 左操作数包含右操作数的值。
   - **startsWith** — 左操作数以右操作数的某个值开头。
   - **endsWith** — 左操作数以右操作数的某个值结尾。
   - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
   - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

     待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

     如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
   - **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

     如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
   - **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
   - **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。

- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

5. 然后单击**创建**按钮。

将创建新的增强规则。

CyberTrace 指标搜索集成现已配置完成。您现在可以将创建的增强规则添加到收集器。您必须重新启动 KUMA 收集器才能应用新设置。

如果事件详情区域中的任何 CyberTrace 字段包含“ [{ ”或“ }] ”值，则表示 CyberTrace 数据源的信息处理不正确，部分数据可能无法显示。您可以通过从 KUMA 复制事件“**TI 指标**”字段值，并在 CyberTrace 的指标部分中搜索该值来获取所有数据源信息。所有相关信息将显示在 CyberTrace 的“**指标上下文**”部分。

集成 CyberTrace 界面

您可以将CyberTrace网页界面与OSMP控制台集成。启用此集成后，KUMA 控制台将包含一个**CyberTrace**部分，可用于访问CyberTrace网页界面。您可以在OSMP控制台的**设置→KUMA→打开 KUMA 设置→Kaspersky CyberTrace**部分配置集成。

若要在OSMP控制台中集成CyberTrace网页界面：

1. 在主菜单中，前往**监控→资源和服务→密钥**。
   可用密钥的列表将显示。
2. 单击“**创建**”按钮以创建新密钥。此资源用于存储 CyberTrace 服务器的凭证。
   此时将显示密钥窗口。

3. 输入有关密钥的信息：

   a. 在“**名称**”字段中，选择添加的密钥的名称。该名称必须包含 1 到 128 个 Unicode 字符。

   b. 在“**租户**”下拉列表中，选择将拥有此资源的租户。

   c. 在“**类型**”下拉列表中，选择“**凭证**”。

   d. 在“**用户**”和“**密码**”字段中，输入 CyberTrace 服务器的凭证。

   e. 如有必要，请从“**标签**”下拉列表中选择密钥的标签。

   f. 如有必要，在“**描述**”字段中添加最多 4,000 个 Unicode 字符来描述资源。

4. 然后单击**创建**按钮。

   CyberTrace 服务器凭证现已保存，可用于其他 KUMA 资源。

5. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。

   这将打开 KUMA 设置窗口。

6. 在**威胁情报**下，点击**Kaspersky CyberTrace**。

   这将打开**Kaspersky CyberTrace 集成**窗口。

7. 对以下参数进行必要的更改：

   - **状态** — 如果要将 CyberTrace Web 界面集成到 OSMP Console，请启用此切换开关。
   - **主机**（必填）— 输入 CyberTrace 服务器的地址。
   - **端口**（必填）— 输入 CyberTrace 服务器的端口；管理 Web 界面的默认端口为 443。
   - 在“**密钥**”下拉列表中，选择之前创建的密钥。
   - 在**允许主机**下拉列表中，选择支持CORS技术的主机。
   - 在**“CyberTrace 主版本”**字段中，选择 CyberTrace 版本。可选值：**<5**、**≥ 5.0**。如果选择版本**≥ 5.0**，则请求将在CyberTrace的“通用”租户中执行，并使用Kaspersky CyberTrace 5.0及更高版本提供的新版API。如果您选择 **<5**，则请求将使用 Kaspersky CyberTrace 4.x API。默认值是 **<5**。

8. 您可以通过以下方式配置对 CyberTrace Web 界面的访问：

   - 登录OSMP控制台时使用主机名或IP地址。

     为此，在**允许主机**部分中，单击**添加主机**，然后在显示的字段中输入设备的IP或主机名。

   - 登录OSMP控制台时使用FQDN。

     如果您使用 Mozilla Firefox 浏览器来管理控制台，“CyberTrace”部分可能无法显示数据。在这种情况下，请配置数据显示（见下文）。

9. 单击“**保存**”按钮。

CyberTrace现在与KUMA集成，**CyberTrace**部分显示在OSMP控制台中。

*要在Mozilla Firefox中使用FQDN登录OSMP时配置**CyberTrace**部分中的数据显示：*

1. 清除浏览器缓存。
2. 在浏览器的地址栏中，输入带有端口号的OSMP控制台的FQDN。
   一个窗口随即打开，警告您存在潜在的安全威胁。
3. 单击“**详情**”按钮。
4. 在窗口下方，单击“**接受风险并继续**”按钮。
   OSMP控制台的URL的排除项随即创建。
5. 在浏览器的地址栏中，输入带有端口号的OSMP控制台的URL。
6. 转到“**CyberTrace**”部分。

数据将显示在此部分中。

更新 CyberTrace 拒绝列表（内部 TI）

当CyberTrace网页界面集成到OSMP控制台中时，您可以使用KUMA事件的信息更新CyberTrace拒绝列表或**内部TI**。

要更新 CyberTrace 内部 TI：

1. 从事件表、警报窗口或关联事件窗口打开事件详情区域，然后单击域、网址、IP 地址或文件哈希上的链接。
   上下文菜单打开。
2. 选择“**添加到 CyberTrace 的内部 TI**”。

所选对象现已添加到 CyberTrace 拒绝列表中。

LDAP 连接

LDAP连接在OSMP控制台的**设置→KUMA→打开 KUMA 设置→LDAP服务器**下创建和管理。**LDAP 服务器按租户集成**部分显示了为其创建了LDAP连接的租户。可以创建或删除租户。

如果选择了某个租户，**LDAP 服务器集成**窗口将打开，显示包含现有LDAP连接的表格。您可以创建或编辑连接。在此窗口中，您可以更改发送到 LDAP 服务器的查询频率，并设置过时数据的保留期限。

启用集成后，有关 Active Directory 账户的信息将在“警报”窗口、“关联事故详情视图”窗口以及“事故”窗口中可用。如果单击窗口的“**相关用户**”部分中的账户名称，将打开“**账户详情**”窗口，其中包含从 Active Directory 导入的数据。

在扩展收集器和分析中的事件时，也可以使用来自LDAP的数据。

导入的 Active Directory 属性

可以从 Active Directory 请求以下账户属性：

- accountExpires
- badPasswordTime
- cn
- co
- company
- department
- description
- displayName
- distinguishedName
- division
- employeeID
- givenName
- l
- lastLogon
- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf（此属性可用于关联时搜索）
- mobile
- name
- objectCategory
- objectGUID（即使用户未明确指定，也始终会从 Active Directory 请求此属性）
- objectSID
- physicalDeliveryOfficeName

- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

有关 Active Directory 属性的详细信息，请参阅Microsoft 文档。

启用和禁用 LDAP 集成

您可以同时启用或禁用租户的所有 LDAP 连接，也可以单独启用和禁用 LDAP 连接。

要启用或禁用租户的所有 LDAP 连接：

1. 在应用程序主窗口中，转到**设置**→KUMA→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，点击**LDAP服务器**，然后选择要为其启用或禁用所有LDAP连接的租户。
   将打开“**LDAP 服务器集成**”窗口。
3. 启用或禁用**状态**切换开关。
4. 单击“**保存**”按钮。

要启用或禁用特定的 LDAP 连接：

1. 在应用程序主窗口中，转到**设置**→KUMA→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，点击**LDAP服务器**，然后选择要为其启用或禁用所有LDAP连接的租户。
   将打开“**LDAP 服务器集成**”窗口。
3. 在连接表中，启用或禁用相关连接的**状态**切换开关。
4. 单击“**保存**”按钮。

将租户添加到 LDAP 服务器集成列表

要将租户添加到与 LDAP 服务器集成的租户列表中：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 单击**为新租户添加设置**按钮。
   将显示“**LDAP 服务器集成**”窗口。
4. 在“**租户**”下拉列表中，选择需要添加的租户。
5. 单击“**保存**”按钮。

所选租户将添加到“LDAP 服务器集成”列表中。

要从与 LDAP 服务器集成的租户列表中删除租户：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 选中要删除的租户旁边的复选框，然后单击“**删除**”。
4. 确认删除租户。

所选租户将从“LDAP 服务器集成”列表中删除。

创建 LDAP 服务器连接

要创建与 Active Directory 的新 LDAP 连接：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 选择或创建要为其建立 LDAP 连接的租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 单击“**添加连接**”按钮。
   “**连接参数**”窗口将打开。

5. 添加一个密钥，其中包含用于连接到 Active Directory 服务器的账户凭证。为此请执行以下操作：

   a. 如果您之前添加了密钥，请在“**密钥**”下拉列表中选择现有密钥（类型为“**凭证**”）。
   可以通过单击铅笔图标 ( ) 来更改所选密钥。

   b. 如果要创建新密钥，请单击加号图标 (+)。
   “**密钥**”窗口随即打开。

   c. 在“**名称**”（必填）字段中，输入包含 1 到 128 个 Unicode 字符的密钥名称。

   d. 在“**用户**”和“**密码**”（必填）字段中，输入用于连接到 Active Directory 服务器的账户凭证。
   您可以采用以下格式之一输入用户名：<用户名>@<域> 或 <域><用户名>。

   e. 在“**描述**”字段中，输入最多 4,000 个 Unicode 字符的描述。

   f. 单击“**保存**”按钮。

6. 在“**名称**”（必填）字段中，输入 LDAP 连接的唯一名称。
   字符串长度必须为 1 到 128 个 Unicode 字符。

7. 在“**URL**”（必填）字段中，以 `<hostname or IP address of server>:<port>` 格式输入域控制器的地址。

   > 如果出现服务器可用性问题，您可以指定多个带有域控制器的服务器，并用逗号分隔。所有指定的服务器必须位于同一个域中。

8. 如果要对与域控制器的连接使用 TLS 加密，请从“**类型**”下拉列表中选择以下选项之一：

   - **startTLS**。
     使用“startTLS”方法时，它首先通过端口 389 建立未加密的连接，然后发送加密请求。如果 STARTTLS 命令以错误结束，则连接终止。

     > 确保端口 389 已打开。否则，将无法与域控制器建立连接。

   - **ssl**。
     使用 SSL 时，会立即通过端口 636 建立加密连接。

   - **不安全**。

   使用加密连接时，无法将 IP 地址指定为 URL。

9. 如果您在上一步启用了 TLS 加密，请添加 TLS 证书。为此请执行以下操作：

   a. 如果您之前已上传证书，请从“**证书**”下拉列表中选择该证书。
   如果之前未添加证书，下拉列表将显示“**无数据**”。

   b. 如果要上传新证书，请单击位于“**证书**”列表右侧的加号图标 (+)。
   “**密钥**”窗口随即打开。

   c. 在“**名称**”字段中，输入证书添加后将显示在证书列表中的名称。

d. 单击“**上传证书文件**”按钮以添加包含 Active Directory 证书的文件。支持 Base64 编码的 X.509 证书公钥。

e. 如有必要，请在“**描述**”字段中提供有关证书的任何信息。

f. 单击“**保存**”按钮。

证书将上传并显示在“**证书**”列表中。

10. 在“**超时（秒）**”字段中，指示等待域控制器服务器响应的时间。

    如果在“**URL**”字段中指定了多个地址，KUMA 会在指定的秒数内等待第一台服务器的响应。如果在此时间内未收到响应，则会尝试连接到下一台服务器。如果在指定的时间内所有指定的服务器均未响应，则连接将终止并出现错误。

11. 在“**基本 DN**”字段中，输入应执行搜索请求的目录的基本可分辨名称。

12. 在“**自定义 AD 账户属性**”字段中，指定**要用于增强事件的其他属性**。

    在使用自定义属性配置事件增强之前，请确保在 AD 中配置了自定义属性。

    要使用自定义属性通过账户丰富事件：

    1. 在 **LDAP 连接设置**中添加自定义 AD 账户属性。

       标准的**从 AD 导入的属性**不能添加为自定义属性。例如，如果添加标准 `accountExpires` 属性作为自定义属性，KUMA 在保存连接设置时返回错误。

       可以从 Active Directory 请求以下账户属性：

       - `accountExpires`
       - `badPasswordTime`
       - `cn`
       - `co`
       - `company`
       - `department`
       - `description`
       - `displayName`
       - `distinguishedName`
       - `division`
       - `employeeID`
       - `givenName`
       - `l`
       - `lastLogon`

- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf（此属性可用于关联时搜索）
- mobile
- name
- objectCategory
- objectGUID（即使用户未明确指定，也始终会从 Active Directory 请求此属性）
- objectSID
- physicalDeliveryOfficeName
- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

在 LDAP 连接设置中添加自定义属性后，收集器中待接收的 **LDAP 属性**下拉列表将自动包含这些新属性。自定义属性由属性名称旁边的问号标识。如果为多个域添加了相同的属性，则该属性在下拉列表中仅列出一次。您可以通过将光标移到问号上来查看域。域名显示为链接。如果单击链接，且该域之前未添加，则会自动将其添加到 **LDAP 账户映射**中。

如果在 LDAP 连接设置中删除了自定义属性，请从收集器的映射表手动删除包含该属性的行。每次导入账户时，KUMA 中的账户属性信息都会被更新。

2. 导入账户。

3. 在收集器的 **LDAP 映射**表中，定义将 KUMA 字段映射到 LDAP 属性的规则。

4. 重启收集器。
   重启收集器后，KUMA 开始使用账户丰富事件。

13. 如果不想使用此 LDAP 连接，请选中“**已禁用**”复选框。
    默认情况下，此复选框未被选中。

14. 单击“**保存**”按钮。

LDAP与Active Directory的连接随即创建并显示在**LDAP 服务器按租户集成**窗口中。

保存连接后，将立即请求来自 Active Directory 的账户信息，然后这些信息以指定的频率进行更新。

如果要为一个租户同时使用多个 LDAP 连接，则需要确保每个连接中指示的域控制器地址都是唯一的。否则，KUMA 只允许您启用其中一个连接。检查域控制器地址时，应用程序不会检查端口是否唯一。

创建 LDAP 服务器连接的副本

您可以通过复制现有连接来创建 LDAP 连接。在这种情况下，原始连接的所有设置都会复制到新创建的连接中。

要复制 LDAP 连接：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。

2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。

3. 选择要复制LDAP连接的租户。
   将打开“**LDAP 服务器集成**”窗口。

4. 选择相关连接。

5. 在打开的**连接参数**窗口中，单击**重复连接**按钮。
   “新建连接”窗口将打开。“copy”这个词将被添加到连接名称中。

6. 如有必要，更改相关设置。

7. 单击“**保存**”按钮。

新连接已创建。

如果要为一个租户同时使用多个 LDAP 连接，则需要确保每个连接中指示的域控制器地址都是唯一的。否则，KUMA 只允许您启用其中一个连接。检查域控制器地址时，应用程序不会检查端口是否唯一。

更改 LDAP 服务器连接

要更改 LDAP 服务器连接：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 选择要为其更改 LDAP 服务器连接的租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 单击要更改的 LDAP 服务器连接。
   包含所选 LDAP 服务器连接设置的窗口随即打开。
5. 对设置进行必要的更改。
6. 单击“**保存**”按钮。

LDAP 服务器连接已更改。重新启动使用 LDAP 服务器数据增强的 KUMA 服务，以使更改生效。

更改数据更新频率

KUMA 查询 LDAP 服务器以更新账户数据。发生的情况包括：

- 创建新连接后立即执行。
- 更改现有连接的设置后立即执行。
- 每隔几个小时按照定期计划执行。默认每 12 小时执行一次。
- 每当用户创建更新账户数据的任务时。

查询 LDAP 服务器时，会在 KUMA 控制台的“**任务管理器**”部分创建一个任务。

要更改 KUMA 查询 LDAP 服务器的计划：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。

3. 选择相关租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 在“**数据刷新间隔**”字段中，指定所需的频率（以小时为单位）。默认值是 12。

查询计划已更改。

更改数据存储期限

如果不再从 Active Directory 服务器接收有关这些账户的信息，则默认情况下，接收到的用户账户数据将在 KUMA 中存储 90 天。该期限结束后，数据将被删除。

删除 KUMA 账户数据后，新事件和现有事件将不再使用此信息进行增强。账户信息在警报中也将不可用。如果要查看整个警报存储期间的账户信息，则必须将账户数据存储期限设置为比警报存储期限更长。

要更改账户数据的存储期限：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 选择相关租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 在“**数据存储时间**”字段中，指定从 LDAP 服务器接收的数据的存储天数。

账户数据存储期限已更改。

启动账户数据更新任务

创建与 Active Directory 服务器的连接后，将自动创建获取账户数据的任务。发生的情况包括：

- 创建新连接后立即执行。
- 更改现有连接的设置后立即执行。
- 每隔几个小时按照定期计划执行。默认每 12 小时执行一次。可以更改计划。

可以手动创建账户数据更新任务。您可以下载所有连接的数据，也可以下载所需租户的一个连接的数据。

为租户的所有 LDAP 连接启动账户数据更新任务：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。

3. 选择相关租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 单击“**导入账户**”按钮。

KUMA 控制台的“任务管理器”部分添加了一个从所选租户接收账户数据的**任务**。

要为租户的一个 LDAP 连接启动账户数据更新任务：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 选择相关租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 选择相关的 LDAP 服务器连接。
   “**连接参数**”窗口将打开。
5. 单击“**导入账户**”按钮。

从租户所选连接接收账户数据的任务将添加到 KUMA 控制台的“**任务管理器**”部分。

删除 LDAP 服务器连接

要删除与 Active Directory 的 LDAP 连接：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**集成**下，单击**LDAP服务器**。
   将打开“**LDAP 服务器按租户集成**”窗口。
3. 选择拥有相关LDAP连接的租户。
   将打开“**LDAP 服务器集成**”窗口。
4. 选择要删除的 LDAP 连接并单击“**删除**”按钮。
5. 确认删除连接。

与 Active Directory 的 LDAP 连接将被删除。

Kaspersky Industrial CyberSecurity for Networks 集成

Kaspersky Industrial CyberSecurity for Networks（以下简称“KICS for Networks”）是一款旨在保护工业企业基础设施免受信息安全威胁并确保其不间断运行的应用程序。该应用程序通过分析工业网络流量来识别过程参数值的偏差，检测网络攻击的迹象，并监控网络设备的运行和当前状态。

KICS for Networks 4.0 或更高版本可以与 KUMA 集成。配置集成后，您可以在 KUMA 中执行以下任务：

- 将资产信息从 KICS for Networks 导入 KUMA。
- 将资产状态更改命令从 KUMA 发送到 KICS for Networks。

> 与 KUMA 不同，KICS for Networks 将资产称为设备。

必须在两个应用程序中配置 KICS for Networks 和 KUMA 的集成：

1. 在 KICS for Networks 中，您需要创建一个 KUMA 连接器并保存此连接器的通讯数据包。
2. 在 KUMA 中，连接器的通讯数据包用于创建与 KICS for Networks 的连接。

> 本部分中描述的集成适用于导入资产信息。KICS for Networks 也可以配置为向 KUMA 发送事件。为此，您需要在 KICS for Networks 中创建 SIEM/ Syslog 连接器，并在 KUMA 端配置收集器。

在 KICS for Networks 中配置集成

> 该应用程序支持与 KICS for Networks 4.0 或更高版本集成。

> 建议在结束"过程控制"规则学习模式后，配置 KICS for Networks 和 KUMA 的集成。有关更多详细信息，请参阅 KICS for Networks 文档。

在 KICS for Networks 端，集成配置包括创建 *KUMA 类型的连接器*。在 KICS for Networks 中，连接器是专用的应用程序模块，用于支持 KICS for Networks 与接收方系统（包括 KUMA）进行数据交换。有关创建连接器的更多详细信息，请参阅 KICS for Networks 文档。

将连接器添加到 KICS for Networks 时，会自动为该连接器创建*通讯数据包*。这是用于连接到 KICS for Networks 的加密配置文件，在 KUMA 端配置集成时使用。

在 KUMA 中配置集成

> 建议在结束"过程控制"规则学习模式后，配置 KICS for Networks 和 KUMA 的集成。有关更多详细信息，请参阅 KICS for Networks 文档。

要在 KUMA 中配置与 KICS for Networks 的集成：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要为其创建与KICS for Networks集成的租户。
   这将打开"租户属性"窗口。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产设置**。

4. 在**KICS/KATA导入**选项卡上，点击**添加**按钮。
5. 这将打开**创建连接**窗口。
6. 若要启用或禁用连接，请打开或关闭**状态**切换开关
7. 点击加号图标 （+），然后选择在KICS for Networks中创建的通信数据包。
8. 在"**通信数据包密码**"字段中，输入通讯数据包的密码。
9. 在**API 版本**字段中，输入将用于与KICS/KATA通讯的KICS/KATA API版本。默认情况下，使用版本4。
10. 然后单击"**添加**"按钮。
11. 如果您想使用KUMA响应规则更改网络资产的KICS状态，请打开**启用响应操作**切换开关。
12. 单击"**保存**"按钮。

在 KUMA 中配置了与 KICS for Networks 集成，窗口将显示 KICS for Networks 连接器将运行的节点的 IP 地址及其 ID。

启用和禁用与 KICS for Networks 的集成

要为租户启用或禁用 KICS for Networks 集成：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要导入KICS/KATA资产的租户。
   这将打开"租户属性"窗口。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产设置**。
4. 在**KICS/KATA导入**选项卡上，启用或禁用**状态**切换开关。
5. 单击"**保存**"按钮。

更改数据更新频率

KUMA 查询 KICS for Networks 以更新其资产信息。发生的情况包括：

- 创建新集成后立即执行。
- 更改现有集成的设置后立即执行。
- 每隔几个小时按照定期计划执行。默认情况下，每 3 小时执行一次。
- 每当用户创建更新资产数据的任务时。

查询 KICS for Networks 时，会在 OSMP 控制台的"**任务管理器**"部分中创建一个任务。

要编辑导入 KICS for Networks 资产信息的计划：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要导入KICS/KATA资产的租户。
   这将打开“租户属性”窗口。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产设置**。
4. 在**KICS/KATA导入**选项卡上的**导入间隔（小时）**字段中，指定OSMP更新KICS/KATA资产数据的时间间隔。

导入计划已更改。

从 KICS for Networks 导入资产信息时的特殊注意事项

导入资产

根据资产导入规则导入资产。仅导入具有“**已授权**”和“**未授权**”状态的资产。

KICS for Networks 资产由以下参数组合标识：

- 已配置集成的 KICS for Networks 实例的 IP 地址。
- 使用 KICS for Networks 连接器 ID 来配置集成。
- 分配给 KICS for Networks 实例中资产（或“设备”）的 ID。

导入漏洞信息

导入资产时，KUMA 还会接收有关 KICS for Networks 中活动漏洞的信息。如果漏洞在 KICS for Networks 中被标记为“已修复”或“可忽略”，则下次导入时将从 KUMA 中删除有关此漏洞的信息。

资产漏洞信息以 KICS for Networks 的本地化语言显示在**资产详细信息**窗口的**漏洞**下。

> 在 KICS for Networks 中，漏洞被称为风险，并分为几种类型。所有类型的风险都会导入 KUMA。

导入数据的存储期限

如果不再从 KICS for Networks 收到有关先前导入的资产的信息，则该资产将在 30 天后删除。

更改 KICS for Networks 资产的状态

配置集成后，您可以从 KUMA 更改 KICS for Networks 资产的状态。状态可以自动或手动更改。

仅当您在连接 KICS for Networks 的设置中启用了响应时，才能更改资产状态。

手动更改 KICS for Networks 资产的状态

在可用的租户中拥有主管理员、管理员和分析师角色的用户可以手动更改从 KICS for Networks 导入的资产的状态。

要手动更改 KICS for Networks 资产状态：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**” → “**检测和响应**”。
2. 点击要编辑的资产。
   “**资产详情**”区域在窗口右侧打开。
3. 在“**KICS for Networks 中的状态**”下拉列表中，选择需要分配给 KICS for Networks 资产的状态。支持“*已授权*”或“*未授权*”状态。

资产状态已更改。新状态显示在 KICS for Networks 和 KUMA 中。

自动更改 KICS for Networks 资产的状态

使用响应规则自动更改 KICS for Networks 资产的状态。必须将规则添加到关联器，关联器将确定触发这些规则的条件。

与 Neurodat SIEM IM 集成

Neurodat SIEM IM 是一个信息安全监控系统。

您可以配置将 KUMA 事件导出到 Neurodat SIEM IM。根据传入的事件和关联规则，Neurodat SIEM IM 会自动生成信息安全事故。

要配置与 Neurodat SIEM IM 的集成：

1. 使用具有管理权限的账户，通过 SSH 连接到 Neurodat SIEM IM 服务器。
2. 创建 /opt/apache-tomcat-<server version>/conf/neurodat/soz_settings.properties 配置文件的备份副本。

3. 在 /opt/apache-tomcat-<server version>/conf/neurodat/soz_settings.properties 配置文件中，按如下方式编辑以下设置：

   - `kuma.on=true`

     此设置是 Neurodat SIEM IM 与 KUMA 交互的属性。

   - `job_kuma=com.cbi.soz.server.utils.scheduler.KumaIncidentsJob`

   - `jobDelay_kuma=5000`

   - `jobPeriod_kuma=60000`

4. 保存配置文件的更改。

5. 运行以下命令来重新启动 tomcat 服务：

   ```
   sudo systemctl restart tomcat
   ```

6. 在 KUMA 中获取用户的令牌。为此请执行以下操作：

   a. 在主菜单中，前往**设置**→**API令牌**。

   这将打开**API令牌**窗口。

   b. 单击“**添加令牌**”按钮。

   添加令牌窗口将打开。

   c. 如有必要，请设置令牌到期日期：

   - 选中**无到期日期**复选框。
   - 在“**到期日期**”字段中，使用日历来指定创建的令牌到期的日期和时间。

   d. 点击**生成**按钮。

   带有自动生成令牌的“**令牌**”字段将显示在用户详情区域中。复制该令牌。

   关闭窗口后，令牌将不再显示。如果您在关闭窗口前未复制令牌，则必须生成新的令牌。

   e. 单击“**保存**”按钮。

7. 使用“管理员”账户或其他具有您正在配置的组织的管理员角色或所有组织的管理员角色的账户登录 Neurodat SIEM IM。

8. 在“**管理**” → “**组织结构**”菜单项中，选择或创建您希望从 KUMA 接收事故的组织。

9. 在组织表单中，执行以下操作：

   a. 选中“**配置与 KUMA 的集成**”复选框。

   b. 在“**KUMA IP 地址和端口**”字段中，指定 KUMA API 地址，例如 `https://192.168.58.27:7223/api/v1/`。

   c. 在“**KUMA API 密钥**”字段中，指定在步骤 6 中获取的用户令牌。

   d. 保存组织信息。

与 KUMA 的集成已配置完成。

Neurodat SIEM IM 测试对 KUMA 的访问，如果成功，则会显示一条消息，提示已准备好从 KUMA 接收数据。

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform（以下简称"KASAP"）是一个在线学习平台，让用户能够在日常工作中学习信息安全规则及其相关威胁，并通过实际案例进行练习。

KASAP 可以与 KUMA 集成。配置集成后，您可以在 KUMA 中执行以下任务：

- 更改用户的学习分组。
- 查看用户参加的课程及其获得的证书信息。

KASAP 与 KUMA 的集成包括配置 API 连接到 KASAP。该过程在两种解决方案中均会执行：

1. 在 KASAP 中，创建授权令牌并获取 API 请求的地址。
2. 在 KUMA 中，指定 KASAP 中 API 请求的地址，添加 API 请求的授权令牌，并指定 KASAP 管理员的电子邮件地址以接收通知。

在 KASAP 中创建令牌并获取 API 请求的链接

为了获得授权，从 KUMA 发送到 KASAP 的 API 请求必须通过在 KASAP 中创建的令牌进行签名。只有公司管理员可以创建令牌。

创建令牌

要创建令牌：

1. 登录 KASAP Web 界面。
2. 在 **控制面板** 部分，单击 **导入和同步**，然后打开 **Open API** 选项卡。
3. 单击"**新建令牌**"按钮并在打开的窗口中选择用于集成的 API 方法：
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
4. 单击"**生成令牌**"按钮。
5. 复制令牌并以任何方便的方式保存。此令牌是在 KUMA 中配置集成所必需的。

令牌无法以明文形式存储在 KASAP 系统中。关闭"**获取令牌**"窗口后，将无法查看该令牌。如果您关闭窗口而不复制令牌，则需要再次单击"**新建令牌**"按钮，以便系统生成新令牌。

签发的令牌有效期为 12 个月。该期限结束后，令牌将被撤销。如果 6 个月内未使用，签发的令牌也将被撤销。

获取 API 请求的链接

要获取 KASAP 中用于 API 请求的链接：

1. 登录 KASAP 平台控制台。
2. 在 **控制面板** 部分，单击 **导入和同步**，然后打开 **Open API** 选项卡。
3. 使用 Open API 访问 KASAP 的链接位于窗口底部。复制链接并以任何方便的方式进行保存。此链接是在 KUMA 中配置集成所必需的。

在 KUMA 中配置集成

要配置 KUMA 与 KASAP 的集成：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开“**KUMA 设置**”窗口。
2. 在“**集成**”下，单击“**Kaspersky Automated Security Awareness Platform**”。
   “**Kaspersky Automated Security Awareness Platform**”窗口随即打开。
3. 在“**密钥**”字段中，单击加号图标 (+)，通过输入从 KASAP 收到的令牌来创建**令牌**的密钥：
   a. 在“**名称**”字段中，输入密钥的名称。必须包含 1 到 128 个 Unicode 字符。
   b. 在“**令牌**”字段中，输入用于向 KASAP 发出 API 请求的授权令牌。
   c. 如有必要，在“**描述**”字段中添加密钥描述。
   d. 单击“**保存**”按钮。
4. 在“**KASAP Open API URL**”字段中，指定 KASAP 用于 API 请求的地址。
5. 在“**KASAP 管理员电子邮件**”字段中，指定 KASAP 管理员的电子邮件地址，当使用 KUMA 将用户添加到学习组时，该管理员将收到通知。
6. 如有必要，在“**代理**”下拉列表中选择用于连接到 KASAP 的代理服务器资源。
7. 要禁用或启用与 KASAP 的集成，请选中或取消选中“**已禁用**”复选框。
8. 单击“**保存**”按钮。

与 KASAP 的集成已在 KUMA 中配置完成。查看有关警报和事故的信息时，您可以选择关联用户来查看他们参加过的学习课程并更改他们的学习组。

查看有关 KASAP 用户的信息并更改学习组

配置 KASAP 和 KUMA 之间的集成后，当您查看关联用户的相关数据时，警报和事故中将显示来自 KASAP 的以下信息：

- 用户所属的学习组。
- 用户通过的培训。
- 计划的培训和当前进度。
- 收到的证书。

要从 KASAP 查看有关用户的数据：

1. 在 OSMP Console 的“**警报**”或“**事故**”部分中，选择相关警报或事故。
2. 在“**相关用户**”部分中，单击所需的账户。
   “**账户详情**”窗口将在屏幕右侧打开。
3. 选择“**KASAP 课程详情**”选项卡。

   该窗口显示来自 KASAP 的用户相关信息。

您可以在 KASAP 中更改用户的学习组。

要在 KASAP 中更改用户学习组：

1. 在 OSMP Console 的“**警报**”或“**事故**”部分中，选择相关警报或事故。
2. 在“**相关用户**”部分中，单击所需的账户。
   “**账户详情**”窗口将在屏幕右侧打开。
3. 在“**分配 KASAP 组**”下拉列表中，选择要为用户分配的 KASAP 学习组。
4. 单击“**应用**”。

   用户将被移至所选的 KASAP 组，KASAP 公司管理员将收到学习组变更的通知，并重新计算所选学习组的学习计划。

有关学习组以及如何开始的详细信息，请参阅 KASAP 文档。

向 Telegram 发送通知

此集成仅为示例，根据所使用的版本和基础设施的具体情况，可能需要额外配置。
高级技术支持的条款和条件不适用于此集成；处理支持请求时不保证响应时间。

您可以配置在触发 KUMA 关联规则时向 Telegram 发送通知。这可以减少对威胁的响应时间，并在必要时让更多人了解情况。

配置 Telegram 通知的操作包含以下步骤：

1. **创建和配置 Telegram 机器人**
   一个特殊的机器人会发送有关触发的关联规则的通知。它可以向 Telegram 私人聊天或群组聊天发送通知。
2. **创建用于发送通知的脚本**
   您必须创建一个脚本并将其保存在安装了关联器的服务器上。
3. **在 KUMA 中配置通知**
   配置一个启动脚本以发送通知的 KUMA 响应规则，并将此规则添加到关联器。

创建和配置 Telegram 机器人

要创建和配置 Telegram 机器人：

1. 在 Telegram 应用程序中，找到 BotFather 机器人并开始聊天。
2. 在聊天中，单击“**开始**”。
3. 使用以下命令创建一个新机器人：
   `/newbot`
4. 输入机器人的名称。
5. 输入机器人的登录名。
   机器人创建完成。您会收到一个类似于 t.me/<bot login> 的聊天链接和用于联系机器人的令牌。
6. 如果您想在群聊中，而不是在私人消息中使用机器人，请编辑隐私设置：
   a. 在 BotFather 聊天中，输入以下命令：
      `/mybots`
   b. 从列表中选择相关机器人。
   c. 单击“**机器人设置**” → “**群组隐私**”，然后选择“**关闭**”。
      机器人现在可以向群聊发送消息。
7. 要与您创建的机器人开始聊天，请使用您在步骤 5 中获得的 t.me/<botlogin> 链接，然后单击“**开始**”。
8. 如果您希望机器人向用户发送私人消息：
   a. 在与机器人的聊天中，发送任何消息。
   b. 访问 https://t.me/getmyid_bot 链接并单击“**开始**”。
   c. 响应包含 `Current chat ID`。您需要使用此值来配置消息的发送。

9. 如果您希望机器人向群聊发送消息：

   a. 请将 https://t.me/getmyid_bot 添加到群聊中，以便接收来自 KUMA 的通知。

   机器人向群聊发送一条消息，消息中包含 `Current chat ID` 值。您需要使用此值来配置消息的发送。

   b. 请从群中移除该机器人。

10. 通过机器人发送一条测试消息。为此，将以下链接粘贴到浏览器的地址栏中：

    `https://api.telegram.org/bot<token>/sendMessage?chat_id=<chat_id>&text=test`

    其中 `<token>` 是在步骤 5 中获得的值，`<chat_id>` 是在步骤 8 或 9 中获得的值。

因此，测试消息应该会出现在个人聊天或群聊中，并且浏览器响应中的 JSON 应该没有错误。

创建用于发送通知的脚本

要创建脚本：

1. 在安装关联器的服务器的控制台中，创建一个脚本文件并向其中添加以下几行：

```
#!/bin/bash
set -eu
CHAT_ID=<Current chat ID value obtained at step 8 or 9 of the Telegram bot setup instructions>
TG_TOKEN=<token value obtained at step 5 of the Telegram bot setup instructions>
RULE=$1
TEXT="<b>$RULE</b> rule triggered"
curl --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

   如果关联器服务器无法访问互联网，您可以使用代理服务器：

```
#!/bin/bash
set -eu
CHAT_ID=<Current chat ID value obtained at step 8 or 9 of the Telegram bot setup instructions>
TG_TOKEN=<token value obtained at step 5 of the Telegram bot setup instructions>
RULE=$1
TEXT="<b>$RULE</b> rule triggered."
PROXY=<代理服务器的地址和端口>
curl --proxy $PROXY --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
```

2. 将脚本保存到关联器目录 /opt/kaspersky/kuma/correlator/<必须响应事件的关联器 ID>/scripts/。

   有关获取关联器 ID 的信息，请参阅"获取服务标识符"部分。

3. 使 KUMA 用户成为文件的所有者并授予执行权限：

```
chown kuma:kuma /opt/kaspersky/kuma/correlator/<必须响应的关联器 ID>/scripts/<脚本名称>.sh
chmod +x /opt/kaspersky/kuma/correlator/<必须响应的关联器 ID>/scripts/<脚本名称>.sh
```

在 KUMA 中配置发送通知

要配置向 Telegram 发送 KUMA 通知：

1. 创建响应规则：

   a. 在主菜单中，转到“**监控**” → “**资源和服务**” → “**响应规则**”，然后点击“**添加响应规则**”。

   b. “**创建响应规则**”窗口随即打开；在该窗口中，在“**名称**”字段中输入规则的名称。

   c. 在“**租户**”下拉列表中，选择拥有该资源的租户。

   d. 在“**类型**”下拉列表中，选择“**运行脚本**”。

   e. 在“**脚本名称**”字段中，输入脚本的名称。

   f. 在“**脚本参数**”字段中，输入 `{{.Name}}`。
   这会将关联事件的名称作为脚本的参数传递。

   g. 单击“**保存**”按钮。

2. 将响应规则添加到关联器：

   a. 在主菜单中，转到**监控** → **资源和服务** → **“关联器”**，然后选择您存放已创建的通知发送脚本的关联器的文件夹。

   b. 在步骤树中，选择“**响应规则**”。

   c. 然后单击“**添加**”按钮。

   d. 在“**响应规则**”下拉列表中，选择在本说明的步骤 1 中添加的规则。

   e. 在步骤树中，选择“**设置验证**”。

   f. 单击“**保存并重新启动服务**”按钮。

   g. 单击“**保存**”按钮。

关于触发的 KUMA 规则的通知已配置为发送到 Telegram。

UserGate 集成

此集成是一个示例，可能需要根据所用版本和基础设施的具体情况进行额外配置。
高级技术支持的条款和条件不适用于此集成；处理支持请求时不保证响应时间。

UserGate 是一种网络基础设施安全解决方案，可保护个人信息免受外部入侵、未经授权的访问、病毒和恶意软件的风险。

与 UserGate 集成可以在触发 KUMA 响应规则时自动阻止来自 IP 地址、URL 或域名的威胁。

配置集成的操作包含以下步骤：

1. **在 UserGate 中配置集成**
2. **准备响应规则的脚本**
3. **配置 KUMA 响应规则**

在 UserGate 中配置集成

要在 UserGate 中配置集成：

1. 使用管理员账户连接到 UserGate Web 界面。
2. 转到“**UserGate**” → “**管理员**” → “**管理员配置文件**”，然后单击“**添加**”。
3. 在“**配置文件设置**”窗口中，指定配置文件名称，例如，`API`。
4. 在“**API 权限**”选项卡上，为以下对象添加读写权限：
   - 内容
   - Core
   - 防火墙
   - nlists
5. 单击“**保存**”按钮。
6. 在“**UserGate**” → “**管理员**”部分中，单击“**添加**” → “**添加本地管理员**”。
7. 在“**管理员属性**”窗口中，指定管理员的登录名和密码。
   在“**管理员配置文件**”字段中，选择在步骤 3 中创建的配置文件。
8. 单击“**保存**”按钮。
9. 在浏览器的地址栏中，在 UserGate 的地址和端口后添加 `?features=zone-xml-rpc`，然后按 **ENTER** 键。
10. 转到“**网络**” → “**区域**”部分，对于要用于 API 交互的接口区域，转到“**访问控制**”选项卡并选中 **XML-RPC 管理**服务旁边的复选框。
    如有必要，您可以将必须触发 UserGate 阻止功能的 KUMA 关联器的 IP 地址添加至允许地址列表。
11. 单击“**保存**”按钮。

准备用于与 UserGate 集成的脚本

要准备待使用的脚本：

1. 复制要触发 UserGate 中 URL、IP 地址或域名阻止功能的关联器的 ID：

   a. 在主菜单中，前往“**监控**” → “**资源和服务**” → “**活动服务**”。

   b. 选中要获取其 ID 的关联器旁边的复选框，然后单击“**复制 ID**”。

   关联器 ID 将被复制到剪贴板。

2. 下载脚本：

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. 打开脚本文件，在“**输入 UserGate 参数**”部分的“**登录名**”和“**密码**”参数中，指定在 UserGate 中配置集成的步骤 7 中创建的 UserGate 管理员账户的凭证。

4. 将下载的脚本放在 KUMA 关联器服务器上的以下路径中：/opt/kaspersky/kuma/correlator/<步骤 1 中的关联器 ID>/scripts/。

5. 通过 SSH 连接到关联器服务器，然后转到步骤 4 中的路径：

   ```
   cd /opt/kaspersky/kuma/correlator/<步骤 1 中的关联器 ID>/scripts/
   ```

6. 执行以下命令：

   ```
   chmod +x ug.py && chown kuma:kuma ug.py
   ```

脚本已准备就绪，可供使用。

配置用于与 UserGate 集成的响应规则

要配置响应规则：

1. 创建响应规则：

   a. 在主菜单中，转到“**监控**” → “**资源和服务**” → “**响应规则**”，然后点击“**添加响应规则**”。

   b. “**创建响应规则**”窗口随即打开；在该窗口中，在“**名称**”字段中输入规则的名称。

   c. 在“**租户**”下拉列表中，选择拥有该资源的租户。

   d. 在“**类型**”下拉列表中，选择“**运行脚本**”。

   e. 在“**脚本名称**”字段中，输入脚本的名称。`ug.py`.

f. 在“**脚本参数**”字段中，指定：

- 根据被阻止对象的类型执行以下某项操作：
  - `blockurl`，用于按 URL 阻止访问
  - `blockip`，用于按 IP 地址阻止访问
  - `blockdomain`，用于按域名阻止访问
- `-i {{< KUMA 字段，必须根据操作从中获取被阻止对象的值 >}}`

  例如：
  `blockurl -i {{.RequetstUrl}}`

g. 在“**条件**”部分，添加与触发时需要在 UserGate 中阻止的关联规则相对应的条件。

h. 单击“**保存**”按钮。

2. 将响应规则添加到关联器：

a. 在主菜单中，转到“**监控**” → “**资源和服务**” → “**关联器**”，选择必须响应的关联器，并将脚本放置在其目录中。

b. 在步骤树中，选择“**响应规则**”。

c. 然后单击“**添加**”按钮。

d. 在“**响应规则**”下拉列表中，选择在本说明的步骤 1 中添加的规则。

e. 在步骤树中，选择“**设置验证**”。

f. 单击“**保存并重新加载服务**”。

g. 单击“**保存**”按钮。

响应规则已关联到关联器并可供使用。

与 Kaspersky Web Traffic Security 集成

此集成是一个示例，可能需要根据所用版本和基础设施的具体情况进行额外配置。
高级技术支持的条款和条件不适用于此集成；处理支持请求时不保证响应时间。

您可以配置与 Kaspersky Web Traffic Security Web 流量分析和过滤系统（以下简称“KWTS”）的集成。

配置集成涉及创建允许运行 KWTS 任务的 KUMA 响应规则。必须提前在 KWTS Web 界面中创建任务。

配置集成的操作包含以下步骤：

1. **在 KWTS 中配置集成**
2. **准备响应规则的脚本**
3. **配置 KUMA 响应规则**

在 KWTS 中配置集成

要在 KWTS 中准备集成：

1. 使用管理员账户连接到 KWTS Web 界面，并创建具有查看和创建/编辑规则权限的角色。
   有关创建角色的更多详细信息，请参阅 *Kaspersky Web Traffic Security 帮助*。
2. 将创建的角色分配给采用 NTML 身份验证的用户。
   您可以改用本地管理员账户。
3. 在**规则**部分，转到**访问**选项卡，然后单击**添加规则**。
4. 在“**操作**”下拉列表中，选择“**阻止**”。
5. 在“**流量过滤**”下拉列表中，选择“**URL**”值，然后在右侧的字段中输入不存在或已知的恶意地址。
6. 在“**名称**”字段中，输入规则的名称。
7. 使用“**状态**”切换开关来启用规则。
8. 然后单击“**添加**”按钮。
9. 在 KWTS Web 界面中，打开刚刚创建的规则。
10. 记下浏览器地址栏中页面地址末尾显示的 ID 值。
    在 KUMA 中配置响应规则时必须使用此值。

集成在 KWTS 端准备就绪。

准备与 KWTS 集成的脚本

要准备待使用的脚本：

1. 复制要在 KWTS 中触发 URL、IP 地址或域名阻止功能的关联规则的关联器 ID：
   a. 在主菜单中，前往“**监控**” → “**资源和服务**” → “**活动服务**”。
   b. 选中要获取其 ID 的关联器旁边的复选框，然后单击“**复制 ID**”。
      关联器 ID 将被复制到剪贴板。
2. 下载脚本和库：
   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. 将下载的脚本放在 KUMA 关联器服务器上的以下路径中：/opt/kaspersky/kuma/correlator/<步骤 1 中的关联器 ID>/scripts/。

4. 通过 SSH 连接到关联器服务器，然后转到步骤 3 中的路径：

   ```
   cd /opt/kaspersky/kuma/correlator/<步骤 1 中的关联器 ID>/scripts/
   ```

5. 执行以下命令：

   ```
   chmod +x kwts.py kwtsWebApiV6.py && chown kuma:kuma kwts.py kwtsWebApiV6.py
   ```

脚本已准备就绪，可供使用。

配置与 KWTS 集成的响应规则

要配置响应规则：

1. 创建响应规则：

   a. 在主菜单中，转到“**监控**” → “**资源和服务**” → “**响应规则**”，然后点击“**添加响应规则**”。

   b. “**创建响应规则**”窗口随即打开；在该窗口中，在“**名称**”字段中输入规则的名称。

   c. 在“**租户**”下拉列表中，选择拥有该资源的租户。

   d. 在“**类型**”下拉列表中，选择“**运行脚本**”。

   e. 在“**脚本名称**”字段中，输入脚本名称 kwts.py。

   f. 在“**脚本参数**”字段中，指定：

   - `--host` — KWTS 服务器的地址。
   - `--username` — 在 KWTS 中创建的用户账户或本地管理员的名称。
   - `--password` — KWTS 用户账户密码。
   - `--rule_id` — 在 KWTS 中创建的规则的 ID。
   - 根据被阻止对象的类型指定以下选项之一：
     - `--url` — 指定要从中获取 URL 的 KUMA 事件字段，例如，`{{.RequestUrl}}`。
     - `--ip` — 指定要从中获取 IP 地址的 KUMA 事件字段，例如，`{{.DestinationAddress}}`。
     - `--domain` — 指定要从中获取域名的 KUMA 事件字段，例如，`{{.DestinationHostName}}`。
   - `--ntlm` — 如果 KWTS 用户是使用 NTLM 身份验证创建的，则指定此选项。

     例如：
     ```
     --host <address> --username <user> --password <pass> --rule_id <id> --url {{.RequestUrl}}
     ```

   g. 在“**条件**”部分，添加与需要在触发时阻止 KWTS 的关联规则相对应的条件。

   h. 单击“**保存**”按钮。

2. 将响应规则添加到关联器：

   a. 在主菜单中，转到“**监控**” → “**资源和服务**” → “**关联器**”，选择必须响应的关联器，并将脚本放置在其目录中。

   b. 在步骤树中，选择“**响应规则**”。

   c. 然后单击“**添加**”按钮。

   d. 在“**响应规则**”下拉列表中，选择在本说明的步骤 1 中添加的规则。

   e. 在步骤树中，选择“**设置验证**”。

   f. 单击“**保存并重新加载服务**”。

   g. 单击“**保存**”按钮。

响应规则已关联到关联器并可供使用。

与 Kaspersky Secure Mail Gateway 集成

此集成是一个示例，可能需要根据所用版本和基础设施的具体情况进行额外配置。
高级技术支持的条款和条件不适用于此集成；处理支持请求时不保证响应时间。

您可以配置与 Kaspersky Secure Mail Gateway 邮件流量分析和过滤系统（以下简称“KSMG”）的集成。

配置集成涉及创建允许运行 KSMG 任务的 KUMA 响应规则。任务必须提前在 KSMG Web 界面中创建。

配置集成的操作包含以下步骤：

1. **在 KSMG 中配置集成**
2. **准备响应规则的脚本**
3. **配置 KUMA 响应规则**

在 KSMG 中配置集成

要准备在 KSMG 中集成：

1. 使用管理员账户连接到 KSMG Web 界面并创建具有查看和创建/编辑规则权限的角色。
   有关创建角色的更多详细信息，请参阅 *Kaspersky Secure Mail Gateway 帮助*。

2. 将创建的角色分配给采用 NTML 身份验证的用户。
   您可以使用“管理员”本地管理员账户。

3. 在**规则**部分中，单击**创建**。

4. 在左侧窗格中，选择“**常规**”部分。

5. 使用“**状态**”切换开关来启用规则。
6. 在“**规则名称**”字段中，指定新规则的名称。
7. 在“**模式**”下，选择符合此规则条件的邮件处理选项之一。
8. 在“**电子邮件地址**”选项卡的“**发件人**”下，输入不存在或已知的恶意发件人地址。
9. 在“**电子邮件地址**”选项卡上的“**收件人**”下，指定相关收件人或使用“*”字符选择所有收件人。
10. 单击“**保存**”按钮。
11. 在 KSMG Web 界面中，打开您刚刚创建的规则。
12. 记下浏览器地址栏中页面地址末尾显示的 ID 值。
    在 KUMA 中配置响应规则时必须使用此值。

KSMG 端的集成已准备就绪。

准备与 KSMG 集成的脚本

要准备待使用的脚本：

1. 复制其关联规则必须触发 KSMG 中邮件发件人 IP 地址或电子邮件地址阻止功能的关联器的 ID：
   a. 在主菜单中，前往“**监控**” → “**资源和服务**” → “**活动服务**”。
   b. 选中要获取其 ID 的关联器旁边的复选框，然后单击“**复制 ID**”。
      关联器 ID 将被复制到剪贴板。
2. 下载脚本和库：
   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/
3. 将下载的脚本放在 KUMA 关联器服务器上的以下路径中：/opt/kaspersky/kuma/correlator/<步骤 1 中的关联器 ID>/scripts/。
4. 通过 SSH 连接到关联器服务器，然后转到步骤 3 中的路径：
   ```
   cd /opt/kaspersky/kuma/correlator/<步骤 1 中的关联器 ID>/scripts/
   ```
5. 执行以下命令：
   ```
   chmod +x ksmg.py ksmgWebApiV2.py && chown kuma:kuma ksmg.py ksmgWebApiV2.py
   ```

脚本已准备就绪，可供使用。

从 RedCheck 导入资产信息

此集成是一个示例，可能需要根据所用版本和基础设施的具体情况进行额外配置。
高级技术支持的条款和条件不适用于此集成；处理支持请求时不保证响应时间。

RedCheck 是一个用于监控和管理组织信息安全的系统。

您可以将 RedCheck 网络设备扫描报告中的资产信息导入 KUMA。

可以从按主机分组的 CSV 格式的简单“漏洞”报告和“清查”报告中导入数据。

导入的资产将显示在 OSMP Console 的**资产管理 → 资产(设备) → “Detection and Response”**部分。如有必要，您可以编辑资产的设置。

数据通过 API 使用 redcheck-tool.py 实用程序导入。该实用程序需要 Python 3.6 或更高版本以及以下库：

- csv
- re
- JSON
- requests
- argparse
- sys

要从 RedCheck 报告导入资产信息：

1. 以 CSV 格式在 RedCheck 中生成网络资产扫描报告，并将报告文件复制到脚本所在的服务器。
   有关扫描任务和输出文件格式的更多详细信息，请参阅 RedCheck 文档。
2. 创建一个包含用于访问 KUMA REST API 的令牌的文件。
   创建令牌的账户必须满足以下要求：
   - 管理员或分析师角色。
   - 访问将导入资产的租户。
   - 使用 API 请求的权限：GET /assets、GET /tenants、POST/assets/import。
3. 下载脚本：
   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/
4. 将 redcheck-tool.py 工具复制到托管 KUMA Core 的服务器并将该工具的文件设置为可执行：
   `chmod +x <redcheck-tool.py 文件的路径>`
5. 运行 redcheck-tool.py 实用程序：
   `python3 redcheck-tool.py --kuma-rest <KUMA REST API 服务器的地址和端口> --token <API 令牌> --tenant <必须放置资产的租户名称> --vuln-report <“Vulnerabilities”报告文件的完整路径> --inventory-report <“Inventory”报告文件的完整路径>`

   ```
   例如：
   python3 --kuma-rest kuma.example.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant Main --vuln-report
   /home/user/vuln.csv --inventory-report /home/user/inventory.csv
   ```

您可以使用附加标志和命令进行导入操作。例如，`-v` 命令显示有关接收到的资产的扩展报告。关于可用标志和命令的详细说明，请参阅“redcheck-tool.py 的标志与命令”表格。您还可以使用 `--help` 命令查看有关可用标志和命令的信息。

资产信息从 RedCheck 报告导入到 KUMA。控制台显示新增和已更新资产数量的信息。

例如：

```
inventory has been imported for 2 host(s)
software has been imported for 5 host(s)
vulnerabilities has been imported for 4 host(s)
```

扩展导入信息示例：

```
[inventory import] Host: localhost Code: 200 Response: {'insertedIDs': {'0': '52ca11c6-a0e6-4dfd-8ef9-
bf58189340f8'}, 'updatedCount': 0, 'errors': []}
[inventory import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {'0': '1583e552-5137-4164-92e0-
01e60fb6edb0'}, 'updatedCount': 0, 'errors': []}
[software import][error] Host: localhost Skipped asset with FQDN localhost or IP 127.0.0.1
[software import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.1 Code: 200 Response: {'insertedIDs': {'0': '0628f683-c20c-4107-abf3-
d837b3dbbf01'}, 'updatedCount': 0, 'errors': []}
[vulnerabilities import] Host: localhost Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.3 Code: 200 Response: {'insertedIDs': {'0': 'ed01e0a8-dcb0-4609-ab2b-
91e50092555d'}, 'updatedCount': 0, 'errors': []}
inventory has been imported for 2 host(s)
software has been imported for 1 host(s)
vulnerabilities has been imported for 4 host(s)
```

该工具在导入资产时的工作方式如下：

- KUMA 会覆盖通过 API 导入的资产数据，并删除其已解决漏洞的信息。
- KUMA 跳过包含无效数据的资产。

redcheck-tool.py 的标志和命令

标志和命令	必需项	Description
`--kuma-rest <KUMA 服务器的地址和端口>`	是	默认情况下，端口 7223 用于 API 请求。您可以根据需要更改端口。
`--token <token>`	是	选项的值必须仅包含令牌。 必须将管理员或分析师角色分配给生成 API 令牌的用户账户。
`--tenant <租户名称>`	是	要从 RedCheck 报告中导入资产的 KUMA 租户的名称。
`--vuln-report <“漏洞”报告的完整路径>`	是	CSV 格式的“漏洞”报告文件。
`--inventory-report <“清查”报告文件的完整路径>`	否	CSV 格式的“清查”报告文件。
`-v`	否	显示有关导入资产的扩展信息。

可能的错误

错误消息	描述
未找到租户 %w	未找到租户名称。
租户搜索错误：状态代码异常：%d	搜索租户时收到异常 HTTP 响应代码。
资产搜索错误：状态代码异常：%d	在搜索资产时收到异常 HTTP 响应代码。
[%w 导入][错误] 主机：%w 跳过了 FQDN 为 localhost 或 IP 为 127.0.0.1 的资产	导入清查/漏洞信息时，跳过了 cfqdn=localhost 或 ip=127.0.0.1 的主机。

配置 Sendmail 事件的接收

您可以在 KUMA SIEM 系统中配置 Sendmail 邮件代理事件的接收。

配置事件接收包括以下步骤：

1. 配置 Sendmail 日志记录。
2. 配置事件源服务器。
3. 创建 KUMA 收集器。
   要接收 Sendmail 事件，请在收集器安装向导中使用以下值：
   - 在**事件解析**步骤中，选择**[OOTB] Sendmail syslog**规范化器。
   - 在**传输方式**步骤中，选择**tcp**或**udp**连接器类型。
4. 安装 KUMA 收集器。
5. 验证 KUMA 收集器中 Sendmail 事件的接收情况
   您可以在 OSMP Console 的"搜索相关事件"部分验证 Sendmail 事件源服务器是否配置正确。

配置 Sendmail 日志记录

默认情况下，Sendmail 系统的事件会记录到 syslog 中。

要确保日志记录配置正确：

1. 通过 SSH 连接到安装了 Sendmail 系统的服务器。
2. 执行以下命令：
   `cat /etc/rsyslog.d/50-default.conf`
   该命令应返回以下字符串：
   `mail.* -/var/log/mail.log`

如果日志记录配置正确，您可以继续配置 Sendmail 事件的导出。

配置 Sendmail 事件的导出

事件通过 rsyslog 服务从 Sendmail 邮件代理服务器发送到 KUMA 收集器。

要配置 Sendmail 事件到收集器的传输：

1. 使用具有管理权限的账户连接到安装了 Sendmail 的服务器。
2. 在 /etc/rsyslog.d/ 目录中，创建 Sendmail-to-siem.conf 文件并向其中添加以下行：
   `If $programname contains 'sendmail' then @<收集器的 IP 地址>:<收集器的端口>`

   例如：
   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   如果要通过 TCP 发送事件，则文件的内容必须如下：
   `If $programname contains 'sendmail' then @@<收集器的 IP 地址>:<收集器的端口>`
3. 创建 /etc/rsyslog.conf 文件的备份副本。

4. 将以下行添加到 /etc/rsyslog.conf 配置文件：

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. 保存更改。

6. 重新启动 rsyslog 服务：

   ```
   sudo systemctl restart rsyslog.service
   ```

配置与外部SIEM系统的集成

OSMP可以使用Syslog协议将有关应用程序网页界面中的警报和用户操作的信息发送到您企业正在使用的外部SIEM系统。

外部SIEM系统可以是：

- Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- 第三方SIEM系统

要传输数据，您需要根据所选协议创建tcp或udp类型的目的地。通过TCP传输数据时，您可以使用TLS加密。为此，请在创建目的地时指定TLS证书。

要上传TLS证书，以加密与SIEM系统的连接：

1. 在创建tcp类型目的地的窗口中，选择**高级设置**选项卡。
2. 在**TLS模式**字段中，选择以下值之一：
   - **自定义CA**

     如果要上传证书文件，请选择此项。在**自定义CA**字段中，指定包含证书文件的密钥。您可以选择现有 Secret 或创建新 Secret。要创建密钥，请从列表中选择**新建**，然后在显示的窗口中上传 TLS 证书。
   - **自定义PFX**

     如果要上传PFX格式的证书文件，请选择此项。在**PFX密钥**字段中，指定包含证书文件的密钥。您可以选择现有 Secret 或创建新 Secret。要创建密钥，请从列表中选择**新建**，然后在显示的窗口中上传包含TLS证书的PFX文件。
3. 根据需要管理其他目标位置设置。然后单击**创建**按钮。

上传的TLS证书将用于加密与SIEM系统的连接。

管理 KUMA

本节介绍 KUMA 的常规设置。

配置 KUMA Core

要配置 KUMA Core 设置：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。

   这将打开 KUMA 设置窗口。

2. 在“**其他**”下，单击“**通用**”。

   “**通用**”窗口随即打开。

3. 在“**Core 设置**”部分，指定以下设置：

   - 使用“**调试**”切换开关启用或禁用系统操作日志记录（调试模式）。默认情况下，此切换开关处于关闭状态。
   - 如果启用调试模式，您可以使用“**转储 KSC HTTP 流量**”切换开关启用或禁用转储 Kaspersky Security Center 的 HTTP 流量的功能。
   - 如果启用了 Kaspersky Security Center 的 HTTP 流量转储，您可以使用“**定期转储**”切换开关启用或禁用将 Kaspersky Security Center 的 HTTP 请求和响应转储到事件日志的功能。

     选中“**启用定期转储**”复选框后，请在“**转储设置**”下指定转储设置。
   - 在“**每周起始日**”下拉列表中，选择要用于整个 KUMA 实例的一周的第一天。所选值将应用于在 KUMA 的所有部分中选择时间段和指定时间间隔的场景。默认值为“**周一**”。只有具有主管理员角色的用户才能修改此设置。所选值保存在 KUMA Core 设置中。
   - 在“**KUMA 资源本地化**”下拉列表中，选择从存储库导入的 KUMA 资源的本地化语言。默认语言为“英语”。如果更改此设置，则只有新的 KUMA 资源会以所选语言导入。如果您之前导入过其他语言的资源，此类资源将保持不变。要更改之前导入的资源的语言，您需要从存储库重新导入这些资源。

     “**KUMA 资源本地化**”设置独立于 Kaspersky Next XDR Expert 语言设置。您可以在这些设置中选择不同的本地化语言。在这种情况下，例如，资源表中的文本语言可能与界面的本地化语言不同。

     “**KUMA 资源本地化**”设置不会影响手动创建的资源。
   - 如有必要，请单击“**重新签发**”按钮以重新颁发 AI 服务证书和内部 CA 证书。

     > 重新颁发 AI 服务证书后，您必须手动重启所有服务。要应用新的 AI 服务证书，您必须重启 KUMA Core。

4. 如果您不想使用自签名 KUMA 证书，请在“**外部 TLS 证书对**”部分上传 TLS 对的证书和密钥。

   单击“**更新证书**”按钮，即可更新 TLS 对的证书。

5. 在“**Core 属性**”下，指定以下设置：

   - 选中“**SQLite 压缩**”复选框，并指定磁盘空间大小（以 GB 为单位）。这样可以减小数据库大小，从而更有效地利用磁盘空间。

     默认情况下，该复选框处于选中状态，磁盘空间设置为10,000GB。
   - 在“**激活标签**”字段中，指定一个适用的标签。

- 在“**警报保留期（天）**”字段中，以天为单位指定警报的保留期。您可以指定任何大于 0 的值。

  默认保留期是365天。

- 在“**资产批量合并大小**”大小字段中，指定在合并开始之前，所有资产被拆分后，一个组（批次）中包含的资产数量。程序会按顺序处理每个资产组：合并、验证并保存资产。如果指定值为 10，则 100 个资产将被拆分成 10 组，每组 10 个资产，然后逐组处理。指定较小的值会生成更小的组，从而加快合并速度，因为应用程序每一步处理的数据更少。

  您可以指定任何大于 0 的值。默认设置是 10。

- 在“**可同时启动的最大服务数量**”字段中，指定 KUMA 可以同时启动的服务数量。

  默认设置是 10。

  > 同时运行的服务过多会降低 KUMA 数据的处理速度。

- 在“**关联规则排除项 TTL（小时）**”字段中，指定关联规则排除项的有效期（以小时为单位）。您可以指定 1 到 8760 (24*365) 之间的值（包含 1 和 8760）。

  默认设置是 72。

- 在“**Core 服务目标位置（用于发送事件）的磁盘缓冲区大小 (MB)**”字段中，指定在 Core 上分配给每个服务的磁盘缓冲区大小。当内部事件无法发送到关联器时，将使用此缓冲区。您可以设置大于 0 的任何缓冲区大小。

  默认设置是1,024MB。

- 在“**通过 Core 服务目标位置发送事件的超时时间（秒）**”字段中，指定发送事件时建立与服务连接的超时时间。您可以指定大于 0 秒的任何超时时间。

  默认设置是15秒。

- 在**Core 服务获授权执行自助任务的时段（小时）**字段中，指定Core可以执行自助服务操作的时间（UTC 时间）。KUMA Core 每天执行此类操作。您可以指定 0 到 23 之间的值（包含 0 和 23）。

  > 周三建议在夜间执行 KUMA Core 维护，因为此时用户不会使用 KUMA Core 的功能。

  默认设置是 1（UTC 时间）。

- 在**最大存储文件大小 (MB)**字段中，指定已下载的 GeoIP 数据库和存储库软件包的压缩数据的最大大小。

  默认设置是300MB。

- 在“**资源历史保留期（天）**”字段中，指定资源更改历史记录的保留期（以天为单位）。您可以设置大于或等于 0 的任何值。

  默认设置是12天。

- 在“**从 UI 发起集群请求的超时时间（秒）**”字段中，指定 KUMA Web 客户端在请求存储列表后必须等待响应的时间。您可以设置大于 0 的任何值。

  默认设置是30秒。

- 在“**存储节点健康检查超时时间（秒）**”字段中，指定请求对特定存储节点进行可用性检查后等待响应的时间。您可以设置大于 0 的任何值。

  默认设置是30秒。

- 如有必要，请在“**KUMA UI 负载均衡器主机名和端口**”字段中，指定 KUMA 用户界面负载均衡器的主机名和端口。

  鉴于 KUMA Core 的分布式特性，可以将多个 Core 节点配置为一个集群。您可以通过负载均衡器配置与集群的连接。

  > 您只能指定一个负载均衡器 URL。

  负载均衡器 URL 必须以 `hostname:port` 格式指定，其中

  - `hostname` 是负载均衡器的主机名。
  - `port` 是负载均衡器的端口。

  > 不允许使用其他负载均衡器 URL 格式。

6. 单击**“保存”**。

代理

代理服务器用于存储代理服务器配置设置，例如存储在目标位置中。支持 http 类型。

可用设置：

- **名称**（必填）– 代理服务器的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） – 拥有该资源的租户的名称。
- **单独设置密钥** – 如果选中此复选框，窗口将显示必填的“**URL**”字段（您可以在其中指定连接 URL），以及一个包含“凭证”类型密钥的“**密钥**”下拉列表。这样一来，即便用于连接的用户账户密码发生更改，您也无需重新创建大量连接，即可查看连接信息。如果取消选中此复选框，则“**URL**”和“**密钥**”字段不可用。默认情况下，此复选框未被选中。
- “**URL**”字段（必填）用于指定连接 URL。它需与“凭证”类型的密钥配合使用。选中“**单独设置密钥**”复选框后可用。
- “**密钥**”下拉列表用于选择现有密钥或创建“凭证”类型的新密钥。选中“**单独设置密钥**”复选框后，该下拉列表可用。
- **使用密钥中的 URL**（必填） – 下拉列表，用于选择存储代理服务器URL的密钥资源。如有必要，可以在代理服务器创建窗口中通过单击加号图标 (+) 来创建密钥。可以通过单击铅笔图标 (✎) 来更改所选密钥。
- **不用于以下域** – 一个或多个需要直接访问的域。
- **描述** – 最多 4,000 个 Unicode 字符。

连接到 SMTP 服务器

KUMA 可以配置为使用 SMTP 服务器发送电子邮件通知。如果用户在其配置文件设置中选中**接收电子邮件通知**复选框，则用户将收到通知。

只能添加一个 SMTP 服务器来处理 KUMA 通知。SMTP服务器连接在OSMP控制台的**设置**→**KUMA**→**打开 KUMA 设置**→**通用**→**SMTP 服务器设置**。

要配置 SMTP 服务器连接：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
2. 这将打开 KUMA 设置窗口。
3. 在“**其他**”下，单击“**通用**”。
4. “**通用**”窗口随即打开。
5. 在“**SMTP 服务器设置**”区块中，更改相关设置：
   - **已禁用** — 如果要禁用与 SMTP 服务器的连接，请选中此复选框。
   - **主机**（必填）— SMTP 主机采用以下格式之一：主机名、IPv4、IPv6。
   - **端口**（必填）— SMTP 端口。该值必须是 1 到 65,535 之间的整数。
   - **发件人**（必填） — 邮件发件人的电子邮件地址。例如，`kuma@company.com`。
   - **KUMA Core 服务器别名** — 网络中使用的 KUMA Core 服务器的名称。必须与 FQDN 不同。
   - 如有必要，从“**密钥**”下拉列表中选择“**凭证**”类型的密钥，其中包含用于连接 SMTP 服务器的账户凭证。
     添加密钥

     要创建密钥：

     1. 在“**名称**”字段中，输入密钥的名称。
     2. 在“**用户**”和“**密码**”字段中，输入代理将用于连接到连接器的用户账户的凭证。
     3. 如有必要，请在“**描述**”字段中输入密钥的描述。
     4. 然后单击**创建**按钮。

        密钥将添加并显示在“**密钥**”下拉列表中。
   - 在“**监控通知间隔**”下拉列表中选择必要的通知频率。
     来自源的有关触发监控策略的通知将在选定时间段后重复发送，直到源的状态恢复为绿色。
     如果选择了“**通知一次**”设置，您将只收到一次有关监控策略激活的通知。
   - 如果您不想接收有关事件源状态的通知，请打开“**停用监控通知**”切换按钮。默认情况下，此切换开关处于关闭状态。

- 单击“**测试连接**”按钮。KUMA 会向当前用户个人资料中指定的电子邮件地址发送测试消息。即使未在用户个人资料中选中“**接收电子邮件通知**”复选框，也会发送测试消息。

  请检查您的电子邮件收件箱。如果测试消息已送达，则表示 SMTP 服务器配置正确。如果发送测试消息时发生错误，请检查 SMTP 服务器设置。错误会显示在界面中，并且还会记录在 KUMA Core 日志中。如果消息已发送但未送达邮箱，请检查 SMTP 服务器日志中的错误消息。

  建议您每次更改 SMTP 服务器设置或通知模板时都发送测试消息。

6. 单击“**保存**”按钮。

SMTP 服务器连接现已配置，用户可以接收来自 KUMA 的电子邮件。

操作 Kaspersky Security Center 任务

您可以将 Kaspersky Security Center 资产连接到 KUMA，并将数据库和应用程序模块更新下载到这些资产，或者使用 Kaspersky Security Center 任务对其运行反病毒扫描。任务在 KUMA 控制台中启动。

要对连接到 KUMA 的资产运行 Kaspersky Security Center 任务，建议使用以下脚本：

1. **在 Kaspersky Security Center 管理控制台中创建用户账户**

   此账户的凭证在创建密钥以与 Kaspersky Security Center 建立连接时使用，并可用于创建任务。

   有关创建用户账户和为用户分配权限的更多详细信息，请参阅 *Kaspersky Security Center 帮助指南*。

2. **在 Kaspersky Security Center 中创建 KUMA 任务**

3. **配置 KUMA 与 Kaspersky Security Center 的集成**

4. **将资产信息从 Kaspersky Security Center 导入 KUMA**

   受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

   KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

   - 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
   - 资产属性信息：漏洞；软件，包括操作系统；资产所有者

   若要导入卡巴斯基安全管理中心资产信息：

   1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
   2. 点击**导入**，然后选择以下操作之一：
      - 如要导入资产基本属性信息，请点击**导入KSC资产**。
        这将打开**导入KSC资产**窗口。
      - 若要导入资产其他属性信息，请点击**导入KSC资产属性**。
        这将打开**导入KSC资产属性**窗口。
   3. 在下拉列表中，选择要为其执行导入操作的租户。

在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。

如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。

4. 单击“**导入**”按钮。

将导入资产信息。

此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

5 为导入的资产分配类别

导入后，资产将自动放入“**未分类设备**”组中。您可以将现有类别之一分配给导入的资产，也可以创建一个类别并将其分配给资产。

6 在资产上运行任务

您可以在资产信息中手动运行任务，也可以配置任务以自动运行。

在 Kaspersky Security Center 中创建 KUMA 任务

您可以对连接到 KUMA 的 Kaspersky Security Center 资产运行反病毒数据库和应用程序模块更新任务以及病毒扫描任务。资产必须安装 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux。任务在 OSMP 控制台中创建。

有关在安装了 Kaspersky Endpoint Security for Windows 的资产上创建*更新*和*病毒扫描*任务的更多详细信息，请参阅 *Kaspersky Endpoint Security for Windows* 帮助指南。

有关在安装了 Kaspersky Endpoint Security for Linux 的资产上创建*更新*和*病毒扫描*任务的更多详细信息，请参阅 *Kaspersky Endpoint Security for Linux* 帮助指南。

任务名称必须以“kuma”开头（不区分大小写且不带引号）。例如，`KUMA antivirus check`。否则，该任务不会显示在 KUMA 控制台的可用任务列表中。

手动启动 Kaspersky Security Center 任务

您可以在连接到 KUMA 的 Kaspersky Security Center 资产上手动运行反病毒数据库、应用程序模块更新任务和病毒扫描任务。资产必须安装 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux。

首先，您需要配置 Kaspersky Security Center 与 KUMA 的集成，并在 Kaspersky Security Center 中创建任务。

要手动启动 Kaspersky Security Center 任务：

1. 在 KUMA 控制台中，转到“**资产**”部分，然后选择从 Kaspersky Security Center 导入的资产。

“**资产详情**”窗口打开。

2. 单击“**OSMP 响应**”。

如果启用了与所选资产所属的 Kaspersky Security Center 的连接，此按钮将显示。

3. 在打开的“**选择任务**”窗口中，选中要启动的任务旁边的复选框，然后单击“**启动**”按钮。

Kaspersky Security Center 将启动所选任务。

某些类型的任务仅适用于某些资产。

您只能获取运行 Windows 操作系统的资产的漏洞和软件信息。

自动启动 Kaspersky Security Center 任务

您可以为连接到 KUMA 的 Kaspersky Security Center 资产配置反病毒数据库和应用程序模块更新任务以及病毒扫描任务的自动启动。资产必须安装 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux。

首先，您需要配置 Kaspersky Security Center 与 KUMA 的集成，并在 Kaspersky Security Center 中创建任务。

配置 Kaspersky Security Center 任务的自动启动包括以下步骤：

步骤 1：添加关联规则

要添加关联规则：

1. 在 KUMA 控制台中，选择“**资源**”部分。
2. 选择“**关联规则**”，然后单击“**添加关联规则**”按钮。
3. 在“**常规**”选项卡上，指定以下设置：
   a. 在“**名称**”字段中，定义规则名称。
   b. 在“**租户**”下拉列表中，选择拥有该资源的租户。
   c. 在“**类型**”下拉列表中，选择“**简单**”。
   d. 在“**传播字段**”字段中，添加以下字段：DestinationAssetID。
   e. 如有必要，定义下列字段的值：
   - 在“**频率限制**”字段中，定义将触发规则的每秒最大次数。
   - 在“**严重级别**”字段中，定义由于触发规则而创建的警报和关联事件的严重级别。
   - 在“**描述**”字段中，提供任何附加信息。

4. 在“**选择器**”→“**设置**”选项卡上：

   a. 在“**过滤器**”下拉列表中，选择“**新建**”。

   b. 在“**条件**”字段中，单击“**添加组**”按钮。

   c. 在您添加的组的运算符字段中，选择“**AND**”。

   d. 添加按“DeviceProduct”字段值进行过滤的条件：

      1. 在“**条件**”字段中，单击“**添加条件**”按钮。
      2. 在“条件”字段中，选择“**If**”。
      3. 在“**左操作数**”字段中，选择“事件字段”。
      4. 在“**事件**”字段中，选择“DeviceProduct”。
      5. 在“**运算符**”字段中，选择“=”。
      6. 在“**右操作数**”字段中，选择“**常量**”。
      7. 在“**值**”字段中，输入 `OSMP`。

   e. 添加按“名称”字段值过滤的条件：

      1. 在“**条件**”字段中，单击“**添加条件**”按钮。
      2. 在“条件”字段中，选择“**If**”。
      3. 在“**左操作数**”字段中，选择“事件字段”。
      4. 在“事件”字段中，选择“名称”。
      5. 在“**运算符**”字段中，选择“=”。
      6. 在“**右操作数**”字段中，选择“**常量**”。
      7. 在“**值**”字段中，输入事件的名称。当检测到此事件时，任务将自动启动。

         例如，如果您希望在 Kaspersky Security Center 注册“*已检测到恶意的对象*”事件时，启动“*病毒扫描*”任务，请在“**值**”字段中指定此名称。

         您可以在事件详情的“**名称**”字段中查看事件名称。

5. 在“**操作**”选项卡上，指定以下设置：

   a. 在“**操作**”部分中，打开“**每次事件发生时**”下拉列表。

   b. 选中“**输出**”复选框。

      您不需要填写其他字段。

6. 单击“**保存**”按钮。

关联规则将被创建。

步骤 2：创建关联器

您需要启动关联器安装向导。在向导的步骤 3中，您需要选择按照本指南添加的关联规则。

> “DeviceHostName”字段必须显示资产的域名 (FQDN)。如果未显示，请为此资产创建 DNS 记录，并在向导的步骤 4中创建 DNS 增强规则。

步骤 3：添加过滤器

要添加过滤器：

1. 在 KUMA 控制台中，选择“**资源**”部分。
2. 选择“**过滤器**”，然后单击“**添加过滤器**”按钮。
3. 在“**名称**”字段中，指定过滤器名称。
4. 在“**租户**”下拉列表中，选择拥有该资源的租户。
5. 在“**条件**”字段中，单击“**添加组**”按钮。
6. 在您添加的组的运算符字段中，选择“**AND**”。
7. 添加按“DeviceProduct”字段值进行过滤的条件：
   a. 在“**条件**”字段中，单击“**添加条件**”按钮。
   b. 在“条件”字段中，选择“**If**”。
   c. 在“**左操作数**”字段中，选择“事件字段”。
   d. 在“**事件**”字段中，选择“类型”。
   e. 在“**运算符**”字段中，选择“=”。
   f. 在“**右操作数**”字段中，选择“**常量**”。
   g. 在“**值**”字段中，输入“3”。
8. 添加按“名称”字段值过滤的条件：
   a. 在“**条件**”字段中，单击“**添加条件**”按钮。
   b. 在“条件”字段中，选择“**If**”。
   c. 在“**左操作数**”字段中，选择“事件字段”。
   d. 在“事件”字段中，选择“名称”。
   e. 在“**运算符**”字段中，选择“=”。
   f. 在“**右操作数**”字段中，选择“**常量**”。
   g. 在“**值**”字段中，输入在步骤 1 中创建的关联规则的名称。

步骤 4：添加响应规则

要添加响应规则：

1. 在 KUMA 控制台中，选择“**资源**”部分。
2. 选择**响应规则**，然后单击**添加响应规则**按钮。
3. 在“**名称**”字段中，定义规则名称。
4. 在“**租户**”下拉列表中，选择拥有该资源的租户。
5. 在“**类型**”下拉列表中，选择“**通过 OSMP 响应**”。
6. 在“**Open Single Management Platform 任务**”下拉列表中，选择要启动的 Kaspersky Security Center 任务。
7. 在“**事件字段**”下拉列表中，选择“DestinationAssetID”。
8. 在“**Workers**”字段中，指定服务可以同时运行的进程数。
   默认情况下，工作进程数与安装关联器服务的服务器上的虚拟处理器的数量相同。

- 在“**描述**”字段中，您最多可以添加 4,000 个 Unicode 字符。
- 在“**过滤器**”下拉列表中，选择在本说明的步骤 3 中添加的过滤器。

要向 Kaspersky Security Center 发送请求，您必须确保 Kaspersky Security Center 可通过 UDP 协议使用。

如果响应规则属于共享租户，则主租户所连接的 Kaspersky Security Center 服务器上的任务将显示为可供选择的 Kaspersky Security Center 任务。

如果响应规则选择了租户连接到的 Kaspersky Security Center 服务器中不存在的任务，则不会针对此租户的资产执行该任务。例如，当两个租户使用同一个关联器时，可能会出现这种情况。

步骤 5：向关联器添加响应规则

要向关联器添加响应规则：

1. 在 KUMA 控制台中，选择“**资源**”部分。
2. 选择“**关联器**”。
3. 在关联器列表中，选择在本说明的步骤 2 中添加的关联器。
4. 在步骤树中，选择“**响应规则**”。
5. 然后单击“**添加**”按钮。
6. 在“**响应规则**”下拉列表中，选择在本说明的步骤 4 中添加的规则。
7. 在步骤树中，选择“**设置验证**”。

8. 单击“**保存并重新启动服务**”按钮。

9. 单击“**保存**”按钮。

响应规则将添加到关联器。

将为连接到 KUMA 的 Kaspersky Security Center 资产上的反病毒数据库和应用程序模块更新任务以及病毒扫描任务配置自动启动。当在资产上检测到威胁并且 KUMA 收到相应事件时，这些任务将会启动。

检查 Kaspersky Security Center 任务的状态

在 KUMA 控制台中，您可以检查 Kaspersky Security Center 任务是否已启动，或者监听 Kaspersky Security Center 事件的采集器所关联的事件搜索是否已完成。

要检查 Kaspersky Security Center 任务的状态：

1. 在 KUMA 中，选择“**资源**” → “**活动服务**”。

2. 选择配置为从 Kaspersky Security Center 服务器接收事件的收集器，然后单击“**转到事件**”按钮。

KUMA 的“**事件**”部分将打开一个新的浏览器标签页。该表显示来自 Kaspersky Security Center 服务器的事件。任务的状态显示在“**名称**”列中。

Kaspersky Security Center 事件字段：

- **名称** — 任务的状态或类型。
- **消息** — 有关任务或事件的消息。
- **FlexString<number>Label** — 从 Kaspersky Security Center 接收的属性的名称。例如，`FlexString1Label=TaskName`。
- **FlexString<number>** — FlexString<number>Label 属性的值。例如，`FlexString1=Download updates`。
- **DeviceCustomNumber<number>Label** — 与任务状态相关的属性的名称。例如，`DeviceCustomNumber1Label=TaskOldState`。
- **DeviceCustomNumber<number>** — 与任务状态相关的值。例如，`DeviceCustomNumber1=1` 表示任务正在执行。
- **DeviceCustomString<number>Label** — 与检测到的漏洞相关的属性名称：例如，病毒名称、受影响的应用程序。
- **DeviceCustomString<number>** — 与检测到的漏洞相关的值。例如，属性-值对 `DeviceCustomString1Label=VirusName` 和 `DeviceCustomString1=EICAR-Test-File` 表示检测到了 EICAR 测试病毒。

KUMA 日志

组件日志

默认情况下，仅记录所有 KUMA 组件的错误信息。要接收日志中的详细数据，请在组件设置中配置“**调试**”模式。

日志将不断追加，直至达到 5 GB。当日志达到 5 GB 时，会将其归档为压缩文件，并将新事件写入新日志。存档将在日志文件夹中保存 7 天，7 天后将删除存档。服务器上最多同时存储四个存档日志。每当创建新的日志存档时，如果存档总数大于四个，则删除最早的日志存档。

以下组件可使用“**调试**”模式：

服务：
• 存储库
• 关联器
• 收集器
• 代理
	要启用它，请使用服务设置中的“**调试**”切换开关。
	
	存储位置：服务安装目录。例如，/opt/kaspersky/kuma/<服务名称>/log/<服务名称>。您可以进入 KUMA 控制台的“**资源**” → “**活动服务**”部分，选择所需的服务并单击“**日志**”，即可下载服务日志。
	
	可以通过运行 journalctl 和 tail 命令来查看 Linux 计算机上的日志。例如：
	• 存储。要从安装在服务器上的存储返回最新日志，请运行以下命令：
	`journalctl -f -u kuma-storage-< 存储ID >`
	• 关联器。要从服务器上安装的关联器返回最新日志，请运行以下命令：
	`journalctl -f -u kuma-correlator-< 关联器 ID >`
	• 收集器。要从服务器上安装的特定收集器返回最新日志，请运行以下命令：
	`journalctl -f -u kuma-collector-< 收集器 ID >`
	• 代理。要从服务器上安装的代理返回最新日志，请运行以下命令：
	`tail -f /opt/kaspersky/agent/< 代理 ID >/log/agent`
	如果为 Windows 计算机上的代理分配了“作为服务登录”权限，则始终会记录代理的活动。选中“**调试**”复选框后，可以指定更详细的数据。Windows 计算机上的代理日志可在路径 %PROGRAMDATA%\Kaspersky Lab\KUMA\<代理 ID>\agent.log 对应的文件中查看。Linux 计算机上的代理日志存储在代理安装目录中。

资源： • 连接器 • 目标位置 • 增强规则	要启用它，请使用与资源关联的服务设置中的“**调试**”切换开关。 日志存储在托管使用相关资源的已安装服务的计算机上。可以在与资源关联的服务日志中查看资源的详细数据。

KUMA 通知

标准通知

KUMA 可以配置为使用 SMTP 服务器发送电子邮件通知。为此，请配置与SMTP服务器的连接，并为应接收通知的用户选中**接收电子邮件通知**复选框。

KUMA 会自动通知用户以下事件：

- 已创建报告（报告模板中列出的用户会收到通知）。
- 已执行任务（创建任务的用户会收到通知）。
- 有新的资源包可用。可以通过更新 KUMA 存储库获取这些资源包（在任务设置中指定电子邮件地址的用户会收到通知）。

编辑 KUMA 用户配置文件

要编辑 KUMA 用户配置文件：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。

   这将打开 KUMA 设置窗口。

2. 在**"访问"**下，单击**"配置文件"**。

   "**配置文件**"窗口随即打开。

3. 指定下列设置：

   - 在**"时区"**字段中，选择您希望在 KUMA 中显示时间戳的时区。该列表根据用户操作系统的设置生成，并考虑了夏令时。默认情况下使用用户浏览器的时区。
   - 选中**使用ISO 8601格式**复选框，即可用ISO 8601格式显示时间戳（例如，2026-02-08T17:35:27+03:00）。KUMA Web 界面中那些使用日期和时间缩写或完整显示的部分会采用这种格式，并且 KUMA 系统也采用这种格式。配置的格式保存在 KUMA Core 设置中。
   - 如果您希望用户接收来自 KUMA 的**SMTP 通知，接收电子邮件通知**接收电子邮件通知"复选框。
   - **显示不可打印字符**—如果您希望 KUMA Web 界面显示空格、制表符和换行符等不可打印字符，请选中此复选框。如果选中**"显示不可打印字符"**复选框，您可以按 **`Ctrl/Command+*`** 启用或禁用不可打印字符的显示。

     所有输入字段（**描述**除外）、规范化器、关联规则、过滤器和连接器，以及用于在**事件**部分中搜索事件的 SQL 查询都会显示空格和制表符。空格显示为点。制表符在规范化器、关联规则、过滤器和连接器中显示为短横线。在其他字段中，制表符显示为一个或两个点。

     换行符显示在支持多行输入的所有输入字段中，例如事件搜索字段。
   - 在**空间集合**下拉列表中，选中要授予访问权限的一个或多个空间集旁边的复选框。如果用户未选择任何空间集，则授予其对默认空间集的访问权限。

4. 单击"**保存**"按钮。

KUMA用户配置文件已修改。

处理租户

租户显示在"设置"→"KUMA"→"打开 KUMA 设置"→"租户"下的表格中。您可以通过单击列对表格进行排序。

可用列：

- “**名称**”是租户的名称。
- “**EPS 限制**”是指分配给租户的 EPS（每秒事件数）配额，该配额占授权许可确定的总 EPS 配额的比例。
- “**描述**”是租户的描述。
- “**创建日期**”是指租户的创建日期。
- “**更新时间**” 是租户信息的最近修改日期和时间。

您可以导出租户列表，例如，以便在“活动列表”或“上下文表”小部件中显示租户名称。在这种情况下，请先导出租户列表，然后再将其导入到字典中。为此，请单击**“导出”** → **“字典”**按钮。包含租户列表的文件将下载到您的计算机。

您还可以将租户表中的所有信息导出到文件中。为此，请点击**“导出→所有字段”**按钮。包含租户列表的文件将下载到您的计算机。

管理证书

本节介绍如何使用证书。

下载证书

您可以在 OSMP Web 界面中下载以下证书：

- REST API CA 证书。

  此证书用于对提供 KUMA 公共 API 的 API 服务器进行身份验证。从 MaxPatrol 报告导入数据时，也可以使用此证书。

  如果您希望使用公司的证书和密钥，而不是自签名 Web 界面证书，可以更改该证书。

  下载后，可以将证书导入操作系统或浏览器的信任存储区。之后，客户端将信任由 OSMP 颁发并由证书颁发机构签名的 TLS 证书。

  下载的 CA 证书不可编辑。如果您需要更改节点名称列表 (SAN)，或使用企业证书颁发机构颁发的证书，则应签发新的 TLS 证书，并在 OSMP 的 **设置** → **KUMA** → **打开 KUMA 设置** → **常规** → **外部 TLS 证书对**部分上传该证书。

  如果集群包含多个运行 KUMA Core 服务的节点，并且需要直接连接到每个节点，建议使用 SAN 中包含所有 KUMA Core 节点 FQDN 的 TLS 证书。否则，浏览器可能会显示警告，提示节点名称与证书不匹配。

  节点的 FQDN 是在颁发新 TLS 证书时于使用者可选名称 (SAN) 字段中指定的。您无需修改下载的 REST API CA 证书。

- 微服务 CA 证书。

  当使用 TLS 将日志源连接到被动收集器且未指定自有证书时，此证书用于身份验证。

- AI 服务证书。

  需要此证书才能安装**资产的 AI 评级和 AI 状态**服务。

要下载证书：

1. 在 OSMP Web 界面中，转到**资源和服务** → **活动服务**部分。
2. 在工具栏的 (⋮) 菜单中，选择一个命令：
   - **下载 REST API CA 证书**
   - **下载微服务 CA 证书**
   - **下载 AI 服务证书**

   证书将保存到浏览器设置中指定的文件夹中。

要复制证书指纹：

1. 在 OSMP Web 界面中，转到**资源和服务** → **活动服务**部分。
2. 在工具栏的菜单 (⋮) 中，选择**复制指纹**。

   证书指纹 ID 已复制到剪贴板。将 CA 证书的指纹 ID 用作服务安装命令中 `--pair.fingerprint` 选项的值，以便服务首次连接到 KUMA Core 时验证 KUMA Core 证书。

修改自签名 Web 界面证书

您可以使用公司证书和密钥来代替自签名 Web 界面证书。例如，如果要将自签名 CA Core 证书替换为企业 CA 颁发的证书，则必须提供 PEM 格式的 `external.cert` 和未加密的 `external.key`。

此说明介绍了如何将自签名 CA Core 证书替换为 PFX 格式的企业证书。您可以参考此说明，并根据需要调整相关步骤。

要将 OSMP Web 界面证书替换为 PFX 格式的企业证书，请执行以下操作：

1. 如果您使用 PFX 容器中的证书和密钥，请使用 OpenSSL 将 PFX 文件转换为 PEM 格式的证书和加密密钥：

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nokeys -out external.cert
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nocerts -nodes -out external.key
   ```

   执行命令时，需要指定 PFX 密钥密码（输入导入密码）。

   您将获得 PEM 格式的 `external.cert` 证书和 `external.key` 密钥。

2. 如果您的 `external.key` 未加密，请确保该密钥采用 PKCS#8 格式。如果密钥文件以 `BEGIN RSA PRIVATE KEY` 标记开头，Kaspersky SIEM 将无法处理该文件。在这种情况下，请使用以下命令转换文件：

   ```
   openssl rsa -in rsa_private.key -outform PEM -out private.key
   ```

   此命令生成的文件以 `BEGIN PRIVATE KEY` 标记开头，OSMP 接受此类密钥文件。

3. 在 OSMP Web 界面中，转到 **设置** → **KUMA** → **开放 KUMA 设置** → **常规** 部分。
4. 在 **外部 TLS 证书对**下，上传 PEM 格式的 `external.cert` 和未加密的 `external.key`。

5. 重新启动 KUMA Core：

```
systemctl restart kuma-core
```

6. 刷新网页或重新启动用于管理 OSMP Web 界面的浏览器。

您的公司证书和密钥已被替换。

重新颁发内部 CA 证书

只有具有主管理员角色的用户才能重新颁发内部 CA 证书。

要重新颁发并应用内部 CA 证书：

1. 在 Web 界面中，打开**设置** → **KUMA** → **开放 KUMA 设置** → **常规**部分。
2. 在“核心设置”下，单击**重新签发内部 CA 证书**按钮。
3. 在打开的窗口中确认重新颁发证书。

   KUMA 服务的 CA 证书和 ClickHouse 的 CA 证书将被重新颁发。必须应用重新颁发的证书。
4. 连接到部署了采集器、关联器和事件路由器服务的主机：
   a. 运行以下命令停止所有服务：

   ```
   sudo systemctl stop kuma-<collector/correlator/eventRouter/metrics>-<service_ID>.service
   ```

   其中：

   <service_ID> 是从 OSMP Web 界面复制的服务 ID。

   b. 使用以下命令从`/opt/kaspersky/kuma/<service type>/<service ID>/certificates`目录中删除`internal.cert`和`internal.key`文件：

   ```
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.cert
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.key
   ```
5. 连接到部署了存储服务的主机：
   a. 停止所有存储服务：

   ```
   sudo systemctl stop kuma-<storage>-<service_ID>.service
   ```

b. 使用以下命令从`/opt/kaspersky/kuma/storage/<service ID>/certificates`目录中删除`internal.cert`和`internal.key`文件：

```
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.cert
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.key
```

6. 使用以下命令从`/opt/kaspersky/kuma/clickhouse/certificates`目录中删除所有 ClickHouse 证书：

```
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.cert
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.key
```

7. 连接到部署了代理服务的主机：

   a. 停止 Windows 代理和 Linux 代理的服务。

   b. 从代理的工作目录中删除`internal.cert`和`internal.key`文件。

8. 重启 KUMA Core 以应用新的 CA 证书：

   - 要进行单服务器部署和分布式部署，请运行以下命令：

     ```
     sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
     ```

   - 要在 Kubernetes 集群中部署，请在任意控制器上运行以下命令：

     ```
     sudo k0s kubectl exec deployment/metrics -n kuma -- rm -rf /opt/kaspersky/kuma/metrics/certificates
     sudo k0s kubectl rollout restart deployment metrics -n kuma
     sudo k0s kubectl rollout restart deployment/core-deployment -n kuma
     ```

     建议使用命令重启 KUMA Core，因为通过 Web 界面重启只会重启 KUMA Core 存储桶，而不会重启整个 KUMA Core。

9. 重启所有已停止的服务：

```
sudo systemctl start kuma-<collector/correlator/eventRouter/storage/metrics>-<service_ID>.service --
pair.fingerprint <CA_cert_ID>
```

其中：

- <service_ID> 是从 KUMA Web 界面复制的服务 ID。
- <CA_cert_ID> 是连接服务时用于身份验证的 CA 证书的指纹 ID。

  `--pair.fingerprint`参数是可选的。创建服务时，KUMA 会自动将此选项添加到安装命令中，并指定指纹 ID。
  安装服务时可以不指定`--pair.fingerprint`选项。在这种情况下，KUMA 默认使用`insecure`值，该值会在建立连接时跳过对 KUMA Core CA 证书的验证。如果将其设置为`insecure`，则重新颁发 CA 证书后无需更新指纹。

  为确保 KUMA Core CA 证书得到验证，建议在安装服务时保留带有指纹 ID 的`--pair.fingerprint`选项。在这种情况下，重新颁发 CA 证书时，需要从**资源和服务** → **活动服务** → 菜单 (⋮) → **复制指纹**部分复制指纹 ID。

已应用内部 CA 证书。

重新颁发特定服务的证书

要重置特定服务的证书：

1. 在 Web 界面中，转到**资源和服务** → **活动服务**部分。
2. 选中要重新颁发证书的服务旁边的复选框。
3. 在工具栏或菜单 ⋮ 中，选择**重置证书**。

   此选项不能用于续订 KUMA Core 证书。要更新 KUMA Core 证书，必须重新颁发这些证书并应用内部 CA 证书。

4. 删除服务安装目录中的旧证书。

   解决方案将自动生成新证书。无需重启正在运行的服务，新证书会自动应用。必须重启已停止的服务，才能应用证书。

删除 Windows 代理证书的特殊注意事项：

- 如果代理处于绿色状态，OSMP 会删除当前证书并生成新证书。代理将使用新证书继续运行。
- 如果代理处于红色状态，则会显示一条错误消息，指示代理未运行。在 `%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<agent ID>\certificates` 代理安装文件夹中，删除 `internal.cert` 和 `internal.key` 文件，并手动启动代理。代理启动时，会自动创建新证书。

删除 Linux 代理证书的特殊注意事项：

- 无论代理处于何种状态，都会通过 Web 界面重置证书。
- 在 `/opt/kaspersky/agent/<agent ID>/certificates` 代理安装文件夹中，删除 `internal.cert` 和 `internal.key` 文件。
- 由于重置证书会停止代理，因此必须手动启动代理才能恢复其运行。代理启动时，会自动创建新证书。

处理地理数据

可以将 IP 地址或 IP 地址范围与地理数据的映射列表上传到 KUMA 以用于事件增强。

地理数据格式

地理数据可以按 UTF-8 编码的 CSV 文件形式上传到 KUMA。使用逗号作为分隔符。文件的第一行包含字段标头：`Network,Country,Region,City,Latitude,Longitude`。

CSV 中的字段标头名称	字段描述	示例
Network	IP 地址采用以下格式之一： • IP 地址 • IP 地址范围 • CIDR 格式的 IP 地址。 IPv4 和 IPv6 地址可以混合使用。 必填字段。	• 192.168.2.24 • 192.168.2.25-192.168.2.35 • 131.10.55.70/8 • 2001:DB8::0/120
Country	您的组织使用的国家/地区名称。例如，这可以是其名称或代码。 必填字段。	• Russia • RU
Region	您的组织使用的区域名称。例如，这可以是其名称或代码。	• Sverdlovsk Oblast • RU-SVE
City	您的组织使用的城市名称。例如，这可以是其名称或代码。	• Yekaterinburg • 65701000001
Latitude	所描述位置的纬度（十进制格式）。此字段可以为空，在这种情况下，将数据导入 KUMA 时将使用值 0。	56.835556
Longitude	所描述位置的经度（十进制格式）。此字段可以为空，在这种情况下，将数据导入 KUMA 时将使用值 0。	60.612778

将地理数据从 MaxMind 转换为 IP2Location

KUMA 可以使用来自 MaxMind、IP2Location 或其他兼容格式的地理数据。待转换文件的名称必须符合以下模板：(GeoIP2|GeoLite2)-(City|Country)-Blocks-IPv(4|6).csv。但是，您必须将要使用的文件转换为 KUMA 支持的格式。您可以使用以下脚本进行转换。请确保文件不包含重复记录。例如，如果文件只有几列，则不同的记录可能来自同一网络，并且具有相同的地理数据。此类文件无法转换。要成功执行转换，请确保没有重复的行，并且每行至少包含一个唯一字段。

下载脚本

运行脚本需要 Python 2.7 及更高版本。

脚本启动命令：

```
python converter.py --type <type of geographic data being processed: "maxmind" or "ip2location"> --out <directory where a CSV file containing geographic data in KUMA format will be placed> --input <path to the ZIP archive containing geographic data from MaxMind or IP2location>
```

使用 `--help` 标志运行脚本时，将显示可用脚本参数的帮助信息：`python converter.py --help`

从 MaxMind ZIP 压缩包中转换包含俄罗斯 IP 地址范围数据库的文件的命令：

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out geoip_maxmind_ru.csv
```

如果未指定“`--lang`”参数，则脚本默认从 ZIP 压缩文件中的 GeoLite2-City-Locations-en.csv 文件获取信息。

对于 MaxMind，缺少“--lang”参数相当于以下命令：

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

从 IP2Location ZIP 压缩包中转换文件的命令：

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out
geoip_ip2location.csv
```

从多个 IP2Location ZIP 压缩包中转换文件的命令：

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP
IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out geoip_ip2location_ipv4_ipv6.csv
```

> IP2Location 不使用“--lang”参数。

必需的字段集

MaxMind 源文件 GeoLite2-City-Blocks-IPv4.csv 和 GeoLite2-City-Blocks-IPv6.csv 必须包含以下字段集：

network、geoname_id、registered_country_geoname_id、represented_country_geoname_id、is_anonymous_proxy、is_satellite_provider、postal_code、latitude、longitude、accuracy_radius

源数据示例集：

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000

1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

其余带有区域设置代码的 CSV 文件必须包含以下字段集：

geoname_id、locale_code、continent_code、continent_name、country_iso_code、country_name、subdivision_1_iso_code、subdivision_1_name、subdivision_2_iso_code、subdivision_2_name、city_name、metro_code、time_zone、is_in_european_union

源数据示例集：

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0

7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

源 IP2Location 文件必须包含有关网络范围、国家、地区、城市、纬度和经度的数据

源数据示例集：

```
"0","16777215","-","-","-","-","0.000000","0.000000","-","-"

"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"

"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+
```

如果源文件包含的字段集与本部分所示不同，或者缺少某些字段，则转换后目标 CSV 文件中缺失的字段将为空。

导入和导出地理数据

如有必要，您可以手动导入和导出地理数据至 KUMA。地理数据将以 CSV 文件的形式导入和导出。如果地理数据导入成功，先前添加的数据将被覆盖，并在 KUMA 中生成审计事件（审计事件、审计事件）。

要将地理数据导入 KUMA：

1. 准备包含地理数据的 CSV 文件。

   从 MaxMind 和 IP2Location 接收的地理数据必须转换为 KUMA 支持的格式。

2. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。

   这将打开 KUMA 设置窗口。

3. 在“**其他**”下，单击“**通用**”。

   “**通用**”窗口随即打开。

4. 在**GeoIP 设置**区块中，点击**从文件导入**按钮，然后选择一个包含地理数据的CSV文件。

   等待地理数据导入完成。如果刷新页面，数据导入将会中断。

地理数据将上传到 KUMA。

要从 KUMA 导出地理数据：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。

   这将打开 KUMA 设置窗口。

2. 在“**其他**”下，单击“**通用**”。

   “**通用**”窗口随即打开。

3. 在**GeoIP 设置**区块中，点击**导出**按钮。

地理数据将根据浏览器设置下载为名为 geoip.csv（UTF-8 编码）的 CSV 文件。

数据的导出格式与上传格式相同，但 IP 地址范围除外。如果在导入到 KUMA 的文件中，地址范围是以 `1.0.0.0/24` 格式表示的，那么在导出的文件中，地址范围将以 `1.0.0.0-1.0.0.255` 格式显示。

地理数据的默认映射

如果在配置地理数据扩充规则时选择 `SourceAddress`、`DestinationAddress` 和 `DeviceAddress` 事件字段作为 IP 地址源，则 **应用默认映射**按钮将变为可用。您可以单击此按钮来添加预配置的地理数据属性和事件字段的映射对，具体如下所述。

SourceAddress 事件字段的默认映射

地理数据属性	事件字段
国家/地区	`SourceCountry`
地区	`SourceRegion`
城市	`SourceCity`
纬度	`SourceLatitude`
经度	`SourceLongitude`

DestinationAddress 事件字段的默认映射

地理数据属性	事件字段
国家/地区	`DestinationCountry`
地区	`DestinationRegion`
城市	`DestinationCity`
纬度	`DestinationLatitude`
经度	`DestinationLongitude`

DeviceAddress 事件字段的默认映射

地理数据属性	事件字段
国家/地区	`DeviceCountry`
地区	`DeviceRegion`
城市	`DeviceCity`
纬度	`DeviceLatitude`
经度	`DeviceLongitude`

使用知识库

在 OSMP 控制台中，您可以找到**知识库**部分，该部分可让您以更加直观的方式管理 Kaspersky 软件包和资源。在此部分中，您可以查看可用和已安装的软件包及资源，评估已安装资源对 MITRE ATT&CK 技术的覆盖范围，监控资源版本的最新状态，按指定参数进行搜索和筛选，以及安装单个资源或整个软件包。

软件包包含用于配置 OSMP 的资源集。软件包可从 Kaspersky 存储库下载。

> 如果到目前为止尚未从存储库下载任何软件包，则**知识库**部分中的软件包和资源列表为空。要获取可供安装的软件包和资源，您需要配置预定义资源的更新。
> 有关如何从存储库获取资源的更多信息，请参阅更新资源部分。

要打开**知识库**部分，请在 OSMP 控制台中转到**监控** → **资源和服务** → **知识库**部分。

此部分包含一些小部件，用于显示解决方案实例中软件包和资源的摘要信息。要显示或隐藏小部件，请点击 图标。可用的小部件如下：

- **包状态**显示处于以下状态的软件包数量：
  - **可用**表示软件包可供安装。
  - **已安装**表示整个软件包已安装。
  - **紧急**表示软件包包含需要尽快安装的高优先级资源。
  - **新增**表示软件包添加到存储库不到三个月，且用户尚未安装或查看该软件包。
- **资源状态**显示处于以下状态的各种类型的资源数量：
  - **可用**表示资源可供安装。
  - **已安装**表示资源已安装且不需要更新。
  - **需更新**表示存储库中有该资源的较新版本可用。
- **MITRE 技术覆盖范围，{{ filter }}**显示有关所选资源涵盖的 MITRE ATT&CK 技术数量或涵盖率百分比的信息。

小部件还可用作页面上表格的筛选器。当您在小部件中选择一个值时，表格会根据所选筛选器自动更新。例如，您可以仅显示具有**需更新**状态的资源。

此部分显示以下选项卡：

- 在**包**选项卡上，会显示包含资源的包列表（这是默认选项卡）。
- 在**资源**选项卡上，会显示各个资源的列表。

您可以使用“**搜索**”字段搜索包或资源。搜索仅在当前打开的选项卡上执行。在选项卡之间切换时，输入的搜索查询会保留并应用于所选选项卡。在“**搜索**”字段中，您可以输入资源名称、事件源、事件类型、包名称或任何子字符串。

要筛选**包**和**资源**选项卡的内容，请单击筛选器 图标。

您可以通过单击相关参数的列标题并选择“**升序**”或“**降序**”，对**包**和**资源**选项卡上的表格进行排序。您还可以通过单击相关列的标题并选择需要显示的值，按**资源类型**或**状态**列筛选表格。

查看包详细信息

要查看可用包，

在 OSMP 控制台中，打开 **监控** → **资源和服务** → **知识库** 部分，然后转到 **包** 选项卡（默认已选中）。

包选项卡显示可用包的表格，其中包含以下列：

- “**名称**”是包的名称。
- “**版本**”是包的版本。
- “**发布日期**”是包发布的日期。
- “**资源类型**”是包中包含的资源类型：
  - 活动列表。
  - 上下文表
  - 规范化器
  - 事件聚合规则
  - 关联规则
  - 增强规则
  - 词典
  - 过滤器
  - 通知模板
- “**资源数量**”是包中资源的数量。
- “**状态**”是包的状态。
  - **可用**表示软件包可供安装。
  - **已安装**表示整个软件包已安装。
  - **紧急**表示软件包包含需要尽快安装的高优先级资源。
  - “**新增**”表示包是新的并且可供安装。
- “**描述**”是包的描述。

要查看包的信息，请点击包的名称。这将打开一个包含包相关信息的窗口，其中包含“**常规**”和“**变更日志**”选项卡。

“**常规**”选项卡上显示以下信息：

- 包名称
- 描述
- 发布日期
- 版本

此选项卡还包含“**待导入资源**”部分，该部分显示包中包含的资源列表。您可以在此筛选资源，并仅选择需要安装的资源。

“**变更日志**”选项卡显示有关包变更的信息。

查看资源详细信息

要查看可用资源，

在 OSMP 控制台中，打开 **监控** → **资源和服务** → **知识库** 部分，然后转到 **资源** 选项卡。

资源 选项卡显示可用资源表，其中包含以下列：

- **名称** – 资源的名称。
- **资源类型** – 可用的资源类型：
  - 活动列表。
  - 上下文表
  - 规范化器
  - 事件聚合规则
  - 关联规则
  - 增强规则
  - 词典
  - 过滤器
  - 通知模板
- **安装日期** 是资源在 KUMA 中的安装日期。
- **租户** 是安装该资源的租户。

  如果同一资源安装在多个租户中，则会在表中作为一个组显示。要查看每个安装了该资源的租户中的资源详细信息，请展开该组。
- **版本** 是资源的版本。

- **状态** 是资源的状态。
  - **可用**表示资源可供安装。
  - **已安装** 表示资源已安装。
  - **需更新** 表示该资源有较新版本可用。
- **包名称** 列出包含此资源的包。
- **供应商标签** 是资源供应商分配的标签。
- MITRE **技术** 是与该资源关联的 MITRE ATT&CK 技术。

要查看资源的相关信息，请点击其名称。这将打开资源信息窗口，其中包含 **一般信息** 和 **关联的资源** 选项卡。

在 **关联的资源** 选项卡上，您可以查看链接到所选资源的资源。您还可以在 **资源** 选项卡上点击 **显示依赖关系** 按钮来查看依赖关系。

安装和更新包及资源

安装包

仅当包中包含的所有资源均已安装时，该包才会获得 **已安装** 状态。

要安装整个包：

1. 转到 **监控** → **资源和服务** → **知识库** → **包** 部分。
2. 执行以下操作之一：
   - 选中相关包旁边的复选框，然后单击 **安装** 按钮。
   - 单击包的名称以打开窗口，然后在该窗口中单击 **安装** 按钮。
3. 选择租户。
4. 单击“**安装**”按钮。
   之后，资源将导入 OSMP，并可用于进一步配置。

安装单个资源

要从包中安装单个资源：

1. 转到 **监控** → **资源和服务** → **知识库** → **资源** 部分。
2. 执行以下操作之一：
   - 选中相关资源旁边的复选框，然后单击 **安装** 按钮。
   - 单击资源的名称以打开窗口，然后在该窗口中单击 **安装** 按钮。
3. 选择租户。
4. 单击“**安装**”按钮。

更新资源

如果已安装的资源有新版本可用，该资源将获得 **需更新** 状态。

要更新资源：

1. 转到 **监控** → **资源和服务** → **知识库** → **资源** 部分。
2. 选中一个或多个处于 **需更新** 状态的资源旁边的复选框。
3. 单击**更新**按钮。

KUMA 资源

*资源*是 KUMA 组件，包含用于实现各种功能的参数：例如，与给定的网址建立连接或根据某些规则转换数据。这些组件可通过多种组合方式组装成服务的资源集，这些资源集将进一步用作创建 KUMA 服务的基础。

资源位于 KUMA 控制台的**资源**部分中。

在**资源**下的**规则**中，您可以找到以下类型的资源：

- **规范化器** – 此类资源包含用于将传入事件转换为 KUMA 所用格式的规则。在规范化器中处理后，原始事件将规范化，并可由其他 KUMA 资源和服务处理。
- **连接器**–此类资源包含用于建立网络连接的设置。
- **目标位置** – 此类资源包含将事件转发到目标位置以进一步处理或存储的设置。
- **过滤器** – 此类资源包含从事件流中拒绝或选择单个事件的条件。
- **活动列表** – 此类资源供关联器在根据关联规则分析事件时，用于动态数据处理。

- **字典** – 此类资源用于存储其他 KUMA 资源和服务可能需要的键及其值。
- **代理** – 此类资源包含使用代理服务器的设置。
- **密钥** – 此类资源用于安全存储 KUMA 与外部服务交互所需的机密信息（例如凭证）。
- **上下文表** – 此类资源供 KUMA 关联器用于根据关联规则分析事件。
- **通知模板** – 此类资源用于发送有关新告警的通知。
- **关联规则** – 此类资源包含用于识别指示威胁的事件模式的规则。如果满足这些资源中指定的条件，则会生成关联事件。
- **聚合规则** – 此类资源包含用于将多个相同类型的基本事件合并为一个聚合事件的规则。
- **富集规则** – 此类资源包含使用第三方来源的信息补充事件的规则。
- **响应规则** – 此类资源在关联器中用于在满足特定条件时执行脚本或启动 Kaspersky Security Center 任务等。
- **数据收集和分析规则** – 此类资源包含允许按计划对存储执行带聚合函数的 SQL 查询的规则。从 SQL 查询获取的数据随后将用于关联分析。

单击某个资源类型时，将打开一个窗口，其中显示包含此类型可用资源的表格。资源表包含以下各列：

- **名称** – 资源的名称。可用于搜索资源并对其进行排序。
- **更新时间** – 资源上次更新的日期和时间。可用于对资源进行排序。
- **创建者** – 创建资源的用户的名称。
- **描述** – 资源的描述。

表格最大尺寸不受限制。如果要选择所有资源，滚动到表格末尾并选中“**全选**”复选框，则可以选择表格中所有可用的资源。

资源可以整理成各个文件夹。文件夹结构显示在窗口左侧：根文件夹对应于租户，包含租户所有资源的列表。根文件夹中嵌套的所有其他文件夹显示单个文件夹的资源。选择一个文件夹后，它包含的资源将作为表格显示在窗口右侧窗格中。

可以创建、编辑、复制、移动（从一个文件夹移动到另一个文件夹）以及删除资源。还可以导出和导入资源。

KUMA 带有一组预定义资源，可以通过 `[OOTB]< 资源名称 >` 名称来识别。OOTB 资源受到保护，无法编辑。

如果您想将预定义的 OOTB 资源适配到您组织的基础架构：

1. 在“**资源**”-<资源类型> 部分中，选择要编辑的 OOTB 资源。
2. 在 KUMA 控制台的上部，单击“**复制**”，然后再单击“**保存**”。
   名为 `[OOTB]< 资源名称 > - copy` 的新资源显示在 Web 界面中。
3. 根据需要编辑预定义资源的副本并保存更改。

调整后的资源可供使用。

资源操作

要管理 KUMA 资源，您可以创建、移动、复制、编辑、删除、导入和导出这些资源。这些操作适用于各种类型的所有资源。

KUMA 资源存储在文件夹中。您可以添加、重命名、移动或删除资源文件夹。

创建、重命名、移动和删除资源文件夹

资源可以整理到文件夹中。文件夹结构显示在窗口左侧：根文件夹对应于租户，包含租户所有资源的列表。根文件夹中嵌套的所有其他文件夹显示单个文件夹的资源。选择一个文件夹后，它包含的资源将作为表格显示在窗口右侧窗格中。

您可以创建、重命名、移动和删除文件夹。

要创建文件夹：

1. 在树形结构中选择需要新文件夹的文件夹。
2. 单击**添加文件夹**按钮。

   该文件夹将创建完成。

要重命名文件夹：

1. 在文件夹结构中找到所需的文件夹。
2. 将鼠标悬停在该文件夹的名称上。

   ... 图标将出现在文件夹名称附近。
3. 打开 ... 下拉列表并选择“**重命名**”。

   文件夹名称将变为可编辑的活动状态。
4. 输入新文件夹名称，然后按下“**ENTER**”。

   > 文件夹名称不能为空。

   文件夹将被重命名。

要移动文件夹：

单击文件夹名称，将其拖放到文件夹结构中的所需位置。

> 文件夹无法从一个租户拖到另一个租户。

要删除文件夹：

1. 在文件夹结构中找到所需的文件夹。
2. 将鼠标悬停在该文件夹的名称上。
   ... 图标将出现在文件夹名称附近。
3. 打开 ... 下拉列表并选择“**删除**”。
   确认窗口随即出现。
4. 单击“**确定**”。

文件夹将被删除。

> 程序不会删除包含文件或子文件夹的文件夹。

创建、复制、移动、编辑和删除资源

您可以创建、移动、复制、编辑和删除资源。

要创建资源：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**<资源类型>**”。
2. 选择或创建一个用于添加新资源的文件夹。
   根文件夹与租户相对应。要使资源可供特定租户使用，必须在该租户的文件夹中创建该资源。
3. 单击“**添加<资源类型>**”按钮。
   用于配置所选资源类型的窗口随即打开。可用的配置参数取决于资源类型。
4. 在“**名称**”字段中输入唯一的资源名称。
5. 指定所需参数（标有红色星号）。
6. 如有必要，指定可选参数（非必填）。
7. 单击“**保存**”按钮。

资源将被创建并可用于服务和其他资源。

要将资源移动到新文件夹：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**<资源类型>**”。
2. 在文件夹结构中找到所需的资源，然后选中要移动的资源旁边的复选框。您可以选择多个资源。
   ⣿ 图标出现在所选资源附近。
3. 使用 ⣿ 图标，将资源拖放到所需文件夹。

资源将被移动到新文件夹。

> 您只能将资源移动到创建资源的租户的文件夹。资源无法移动到其他租户的文件夹。

要复制资源：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**<资源类型>**”。
2. 在文件夹结构中找到所需的资源，然后选中要复制的资源旁边的复选框，然后单击“**复制**”。
   一个窗口随即打开，其中包含您选择复制的资源的设置。可用的配置参数取决于资源类型。
   “`<selected resource name> - copy`”值显示在“**名称**”字段中。
3. 对参数进行必要的更改。
4. 在“**名称**”字段中输入唯一名称。
5. 单击“**保存**”按钮。

   将创建资源的副本。

要编辑资源：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**<资源类型>**”。
2. 在文件夹结构中找到所需的资源，然后选择该资源。
   一个窗口随即打开，其中包含所选资源的设置。可用的配置参数取决于资源类型。
3. 对参数进行必要的更改。
4. 单击“**保存**”按钮。

   资源将进行更新。如果此资源已在服务中使用，重新启动服务以应用新设置。

要删除资源：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**<资源类型>**”。
2. 在文件夹结构中找到所需的资源。
3. 选中要删除的资源旁边的复选框，然后单击“**删除**”。
   确认窗口打开。
4. 单击“**确定**”。

   资源将被删除。

将资源与服务链接起来

现在，您可以将资源（关联规则、丰富规则、响应规则、聚合规则和目标）关联到收集器、关联器和事件路由器等服务。可用服务取决于所选资源的类型。

要将资源关联到服务：

1. 在主菜单中，前往“**监控 → 资源和服务 → <资源名称>**”部分。
2. 选中要链接的每个资源旁边的复选框，然后在工具栏或菜单中（⋮），点击**关联至服务 → 关联到<服务名称>**。

   编辑资源设置时，也可以将资源关联到服务。为此，请单击资源名称，选择**服务**选项卡，然后单击**关联至服务 → 关联到<服务名称>**。

   > 管理关联规则的设置时，可以使用“**关联器**”选项卡将规则链接到关联器。

3. 在显示的**<服务名称>**窗口中，选中所需服务旁边的复选框，然后单击**“确定”**。

   该资源被关联到该服务。

要将资源与服务取消链接：

1. 在主菜单中，前往“**监控 → 资源和服务 → <资源名称>**”部分。
2. 点击资源并选择**“服务”**选项卡。

   > 对于关联规则，将显示**“关联器”**选项卡。

3. 选中要从中取消资源链接的每个服务旁边的复选框。
4. 单击**“删除”**并确认从服务取消链接。

   资源被从服务中取消链接。

更新资源

KUMA 更新子系统提供了接收、存储和应用事件处理和威胁检测所需资源的机制。该子系统包含两种独立的更新机制：

- **存储库更新** — 用于下载资源包，并可对其进行查看、分析和导入到租户中。
- **OSMP 更新** — 用于自动接收和应用资源，无需用户干预和手动导入。

两种机制都可以使用以下更新源：

- 卡巴斯基更新服务器。
- 自定义源（存储库或更新镜像）。

更新子系统扩展了 KUMA 的功能，以应对威胁形势和基础架构的变化。无需直接访问互联网即可使用它，有助于确保系统处理的数据的隐私。

更新资源工作流

要更新资源，请执行以下步骤：

1. 更新存储库以将资源包传输到存储库。存储库更新有两种模式：
   - 自动更新
   - 手动更新
2. 将资源包从更新后的存储库导入租户。
3. 确保在执行导入后映射已更新的资源。如有必要，请将资源关联到收集器、关联器或代理，并更新设置。

存储库更新

卡巴斯基定期发布包含可从存储库导入的资源的包。您可以在“**存储库更新**”任务的设置中指定电子邮件地址。首次执行任务后，KUMA 会开始向指定地址发送有关可用更新包的通知。

存储库更新机制允许检索软件包、查看其内容，并决定是否将其部署到操作系统基础架构中。存储库更新可以以自动或手动模式执行。

如果您的基础架构中还有其他卡巴斯基应用程序，则可以将 KUMA 连接到现有的更新镜像。

要启用自动更新：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
2. 在“**其他**”下，单击“**更新设置**” 。
3. 在“**存储库更新**”下，配置“**数据刷新间隔（小时）**”。默认值是 24 小时。
4. 指定**更新源**。下列选项可用：
   - Kaspersky 更新服务器。
     您可以在知识库中查看服务器列表。
   - 自定义源：
     - HTTP 服务器上共享文件夹的 URL。
     - 安装 KUMA Core 的主机上的本地文件夹的完整路径。
       如果使用本地文件夹，则 kuma 系统用户必须具有此文件夹及其内容的读取权限。

5. 单击**添加**按钮来指定**用于通知的电子邮件地址**。当存储库中出现已导入租户的新包或包的新版本时，相关通知将发送至指定电子邮件地址。

   如果指定KUMA用户的电子邮件地址，则必须在用户配置文件中选中**接收电子邮件通知**复选框。对于不属于任何 KUMA 用户的电子邮件，无需额外设置即可接收消息。在所有情况下都必须指定连接到 SMTP 服务器的设置。

6. 单击“**保存**”按钮。更新任务即将启动。然后，任务将根据计划重新启动。

要手动启动存储库更新：

1. 要禁用自动更新，请在“**设置** → KUMA → **打开** KUMA **设置** → **更新设置** → **存储库更新**”部分中，打开“**停用自动更新**”切换开关。默认情况下，此切换开关处于关闭状态。您还可以启动手动存储库更新，而无需禁用自动更新。手动启动更新不会影响自动更新计划。

2. 指定**更新源**。下列选项可用：

   - Kaspersky 更新服务器。
   - 自定义源：
     - HTTP 服务器上共享文件夹的 URL。
     - 安装 KUMA Core 的主机上的本地文件夹的完整路径。

       如果使用本地文件夹，则 kuma 用户必须能够访问此文件夹及其内容。

3. 单击**添加**按钮来指定**用于通知的电子邮件地址**。当存储库中出现已导入租户的新包或包的新版本时，相关通知将发送至指定电子邮件地址。

   如果指定KUMA用户的电子邮件地址，则必须在用户配置文件中选中**接收电子邮件通知**复选框。对于不属于任何 KUMA 用户的电子邮件，无需额外设置即可接收消息。在所有情况下都必须指定连接到 SMTP 服务器的设置。

4. 单击“**运行更新**”。这样，您就可以同时保存设置并手动启动“**存储库更新**”任务。

OSMP 更新

如果授权许可支持，OSMP 更新机制会自动接收和应用资源。OSMP 更新在后台自动执行，无需手动导入、分析或批准软件包。

更新完成后，新的事件字段和关联规则即可用于处理，无需额外配置。

要配置 OSMP 更新：

1. 在主菜单中，转到“**设置**” → “KUMA” → “**打开 KUMA 设置**” → “**更新设置**”。
2. 指定**更新源**。下列选项可用：
   - Kaspersky 更新服务器。
   - 自定义源：
     - HTTP 服务器上共享文件夹的 URL。
     - 安装 KUMA Core 的主机上的本地文件夹的完整路径。
       如果使用本地文件夹，则 kuma 用户必须能够访问此文件夹及其内容。如果使用自定义源，请根据需要配置代理设置。
3. 在“**OSMP 更新**”下，在“**数据刷新间隔（分钟）**”字段中，以分钟为单位指定自动更新检查和下载的频率。默认值是 30。
4. 单击“**保存**”按钮。

默认情况下，“**停用自动更新**”切换开关处于关闭状态，OSMP 更新会根据“**数据刷新间隔（分钟）**”字段中指定的间隔自动运行。

如果您想禁用 OSMP 自动更新，请打开“**停用自动更新**”切换开关并单击“**保存**”。在这种情况下，将不会执行自动更新检查和下载。要手动启动 OSMP 更新，请单击“**运行更新**”。

使用卡巴斯基更新实用程序配置自定义源

您可以通过卡巴斯基更新实用程序使用自定义更新源，在无法访问互联网的情况下更新资源。

配置包括以下步骤：

1. 使用卡巴斯基更新实用程序配置自定义源：
   a. 在公司 LAN 中的其中一台计算机上安装和配置卡巴斯基更新实用程序。
   b. 在卡巴斯基更新实用程序设置中配置将更新复制到共享文件夹。
2. 配置从自定义源更新 KUMA 存储库。

使用卡巴斯基更新实用程序配置自定义源：

您可以从卡巴斯基技术支持网站下载卡巴斯基更新实用程序分发包。

1. 在卡巴斯基更新实用程序中，启用 KUMA 更新下载：
   - 在“**应用程序-周边控制**”下，选中 KUMA 旁边的复选框以启用更新功能。
   - 如果您通过命令行使用卡巴斯基更新实用程序，请将以下行添加到 updater.ini 配置文件的 [ComponentSettings] 部分，或为现有行指定 `true` 值：

     ```
     KasperskyUnifiedMonitoringAndAnalysisPlatform_XDR_1_1=true
     ```

2. 在“**下载**”部分，指定更新源。默认情况下，使用卡巴斯基更新服务器作为更新源。

3. 在“**下载**”部分的“**更新文件夹**”设置组中，指定卡巴斯基更新实用程序下载更新所在的共享文件夹。下列选项可用：

   - 指定安装卡巴斯基更新实用程序的主机上的本地文件夹。部署用于分发更新的 HTTP 服务器，并在该服务器上发布本地文件夹。在OSMP控制台中，进入**设置**→KUMA→**打开 KUMA 设置**→**存储库更新**→**自定义来源**部分，指定在HTTP服务器上发布的本地文件夹的URL。

   - 指定安装卡巴斯基更新实用程序的主机上的本地文件夹。使此本地文件夹可通过网络访问。在安装 KUMA 的主机上挂载可通过网络访问的本地文件夹。在OSMP控制台中，进入**设置**→KUMA→**打开 KUMA 设置**→**存储库更新**→**自定义来源**部分，指定本地文件夹的完整路径。

有关使用卡巴斯基更新实用程序的详细信息，请参阅“卡巴斯基知识库”。

导出资源

如果共享资源对用户隐藏，则用户无法导出共享资源或使用共享资源的资源。

要导出资源：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**关联规则**”。

2. 单击“**导出资源**”。

   将打开“**导出资源**”窗口，其中显示所有可用资源的树形结构。

3. 在“**密码**”字段中输入必须用于保护导出数据的密码。

4. 在“**租户**”下拉列表中，选择要导出其资源的租户。

5. 选中要导出的资源旁边的复选框。

   如果所选资源已关联到其他资源，则关联的资源也将被导出。

6. 单击“**导出**”按钮。

受密码保护的文件中的资源将根据您的浏览器设置保存在您的计算机上。导出的“密钥”资源为空。

导入资源

要导入资源：

1. 在主菜单中，转到“**监控**” → “**资源**”。

2. 单击“**导入资源**”。

   “**资源导入**”窗口随即打开。

3. 在“**租户**”下拉列表中，选择将拥有所导入资源的租户。

4. 在“**导入源**”下拉列表中，选择下列选项之一：

- **文件**

  如果选择此选项，请输入密码并单击“**导入**”按钮。

- **存储库**

  如果选择此选项，将显示可导入的包列表。建议您确保存储库更新日期相对较新，并在必要时配置自动更新。

  您可以选择一个或多个要导入的包，然后单击“**导入**”按钮。共享租户的依赖资源将导入到共享租户中，其余资源将导入到所选的租户中。您不需要共享租户的特殊权限；您只需拥有在所选租户中导入的权限。

  导入的资源标记为“**此资源是软件包的一部分”。您可以删除它，但无法编辑**，只能删除。要重命名、编辑或移动导入的资源，请使用“**复制**”按钮制作资源的副本，并使用资源的副本执行所需的操作。导入包的未来版本时，副本不会更新，因为它是一个单独的对象。

  标记为“**此资源是软件包的一部分**”，位于“`Integration`”目录中的导入资源可以进行编辑。例如，您可以在“`Integration`”目录中编辑关联规则的排除项过滤器。排除项过滤器包含一系列条件，用于防止关联规则触发误报。根据您的网络环境，在使用关联规则之前或同时向排除项过滤器添加条件，以减少误报。默认情况下，卡巴斯基提供的排除项过滤器会添加到关联规则选择器中。

  导入软件包的后续版本时，已编辑的资源不会被软件包中的相应资源替换，从而可以保留您的更改。与临时排除项不同，对排除项过滤器所做的更改是永久生效的。

  从存储库导入资源时，会使用 KUMA Core 设置 部分的 KUMA 资源本地化设置中指定的语言。

5. 如果从文件导入的资源与现有资源之间发生冲突，请解决这些冲突。阅读下文了解有关资源冲突的更多信息。

   a. 如果导入资源的名称、类型和 GUID 与现有资源的名称、类型和 GUID 完全匹配，则“**冲突**”窗口将会打开，其中的表格显示了冲突资源的类型和名称。解决显示的冲突：

   - 要用新资源替换现有资源，请单击“**替换**”。

     要替换所有冲突资源，请单击“**全部替换**”。

   - 要保留现有资源，请单击“**跳过**”。

     对于依赖资源（即与其他资源关联的资源），**跳过**选项不可用；您只能**替换**依赖资源。

     要保留所有现有资源，请单击“**全部跳过**”。

   b. 单击“**解决**”按钮。

资源将导入到 KUMA。导入的“密钥”资源为空。

导入使用扩展事件模式的资源

如果导入使用扩展事件模式的一个或多个字段的规范化器，KUMA 会自动创建一个在规范化器中使用的扩展模式字段。

如果导入在其逻辑中使用扩展事件模式字段的其他类型的资源，则会成功导入资源。为确保导入的资源正常运行，必须在“规范化器”类型的资源中创建扩展事件模式的相应字段。

如果将使用扩展事件模式字段的规范化器导入 KUMA，并且 KUMA 中已存在相同的字段，则使用先前创建的字段。

关于冲突解决

当从文件将资源导入 KUMA 时，会将它们与现有资源进行比对；具体会比对以下参数：

- 名称和类型。如果导入资源的名称和类型参数与现有资源的名称和类型参数匹配，则导入资源的名称将自动更改。
- 如果两个资源的标识符匹配，则会出现冲突，必须由用户解决。当您将资源导入其导出来源的同一台 KUMA 服务器时，可能会出现此情况。

在解决冲突时，您可以选择用导入的资源*替换现有资源*，或者*保留现有资源*，跳过导入的资源。

某些资源是关联的：例如，在某些类型的连接器中，必须指定连接器的密钥。如果密钥与连接器关联，则这些密钥也会被导入。这类关联资源将一起导出和导入。

导入的特殊注意事项：

1. 资源将导入所选的租户。
2. 如果关联资源位于共享租户中，则导入后仍保留在共享租户中。
3. 在**冲突**窗口中，**父级**列始终显示导入期间所选资源中最顶层的父级资源。
4. 如果在导入过程中发生冲突，并且您选择用新资源替换现有资源，则意味着所有与被替换资源关联的其他资源将自动替换为导入的资源。

已知错误：

1. 在以下情况下，关联的资源会导入至导入期间指定的租户中，而不是"**冲突**"窗口中所示的共享租户中：
   a. 关联资源最初位于共享租户中。
   b. 在**冲突**窗口中，选择**跳过**来自共享租户的关联资源的所有父对象。
   c. 保留共享租户中的已关联资源以进行替换。
2. 导入后，在以下情况下，类别在过滤器中没有指定的租户：
   a. 过滤器包含来自不同租户的已关联资产类别。
   b. 资产类别名称相同。
   c. 您正在将带有已关联资产类别的过滤器导入新服务器。
3. 在租户 1 中，资产类别名称会在以下情况下出现重复：
   a. 在租户 1 中，有一个过滤器包含来自租户 1 和共享租户的已关联资产类别。
   b. 已关联资产类别的名称相同。
   c. 您正在将这样的过滤器从租户 1 导入到共享租户。
4. 您无法将存在冲突的资源导入同一租户。

*不允许将冲突资源导入同一租户*错误表示导入的包中包含来自不同租户的冲突资源，因此无法导入共享租户。

解决方案：选择非共享租户以导入包。在这种情况下，导入时原本位于共享租户中的资源将导入至共享租户，而来自其他租户的资源则导入至导入过程中所选的租户。

5. 只有主管理员才能将类别导入共享租户。

   错误"*仅主管理员才能将类别导入共享租户*"表示导入的包中含有已关联共享资产类别的资源。KUMA Core 日志中会显示类别或已关联共享资产类别的资源。Core 日志路径：

   /opt/kaspersky/kuma/core/log/core

   解决方案：选择以下选项之一：

   - 不得导入已关联共享类别的资源：取消选中相关资源旁边的复选框。
   - 使用主管理员账户执行导入。

6. 只有主管理员才能将资源导入共享租户。

   错误"*仅主管理员才能将资源导入共享租户*"表示导入的包中含有已关联共享资源的资源。已关联共享资源的资源会显示在 KUMA Core 日志中。Core 日志路径：

   /opt/kaspersky/kuma/core/log/core

   解决方案：选择以下选项之一：

   - 不得导入已关联共享租户中资源的资源及共享资源本身：取消选中相关资源旁边的复选框。
   - 使用主管理员账户执行导入。

标签管理

为了帮助管理资源，KUMA允许您为资源添加标签。您可以使用标签搜索组件，以及管理标签、关联或取消关联标签。

您不能向通过其他资源的接口创建的资源添加标签。标签只能从资源自身的卡片中添加。您也不能为不可编辑的资源添加标签。

标签管理

标签列表显示在**设置**→KUMA→**打开**KUMA**设置**→**标签**部分，并以表格形式显示，包含以下列：**名称**、**租户**、**用于资源**。

在**标签**表中，您可以：

- 按**名称**对标签进行排序，**用于资源**字段。
- 按**租户**字段的值进行筛选。
- 根据**名称**字段查找标签。
- 前往具有所选标签的资源列表。

添加标签

若要添加标签：

1. 在主菜单中，前往**监控→资源和服务**，然后选择一个资源。
2. 在表格上方的面板中，点击**添加**。
3. 在所选资源的**标签**字段中，添加新标签，或从列表中选择一个标签。
4. 点击“**创建**”按钮。

   新标签随即添加。

您还可以从现有标签中添加标签。

添加标签时，请注意以下特殊事项：

- 您可以添加多个标签。
- 标签可以包含各种字母（例如西里尔字母、拉丁字母或希腊字母）、数字、下划线和空格的字符。
- 除了下划线和空格外，标签不得包含任何特殊字符。
- 您可以输入大写或小写标签，但保存后，标签总是以小写显示。
- 标签会继承它所在资源的租户信息。
- 标签是资源的一部分，只要创建或使用该标签的资源存在，标签就一直存在。
- 标签在同一租户内是唯一的。
- 标签作为资源的一部分，与资源一起导入或导出。

按标签搜索

在**资源**部分，您可以搜索资源：

- 按标签
- 按资源名称

搜索将涵盖所有资源类型和服务。

搜索结果会显示资源和服务列表。

若要按标签查找资源：

1. 在主菜单中，前往**监控→资源和服务**，然后选择一个资源。
2. 在资源表中，选择**标签**列。
3. 在显示的**搜索**字段中，输入或选择标签名称。
   在资源本身和资源列表中按标签搜索，会返回输入的文本与标签名称的完整匹配项和部分匹配项。

   如果指定的标签出现在某些资源中，则显示这些资源的列表。

在资源列表中，您可以：

- 按名称和资源或服务类型对列表进行排序。
- 按资源或服务类型或标签筛选资源或服务。
- 关联或取消关联标签。

添加依赖资源时显示标签

添加依赖资源时，该资源的标签会显示在**筛选设置**的下拉列表中。

无法单行显示的资源标签将被隐藏。特殊指示器会显示隐藏的标签。

下拉列表可以按资源名称和资源标签进行筛选。

关联或取消关联标签

若要将标签关联到资源或从资源取消关联标签：

1. 在主菜单中，前往**监控→资源和服务**。
2. 选择**列表**选项卡。
3. 在**名称**列中，选中相关资源旁边的复选框。
4. 在列表上方的面板中，选择**标签**选项卡。
5. 点击**关联**或**取消关联**，选择所需的标签或创建新标签。

   选定的标签将关联到资源或从资源中取消关联。

   您也可以在资源卡片中关联或取消关联标签。

规范化器

规范化器用于将来自不同来源、不同格式的原始事件转换为 KUMA 事件数据模型。规范化事件可供其他 KUMA 资源和服务进行处理。

规范化器由*主*事件解析规则和可选的*附加事件解析规则*组成。通过创建主解析规则和一组附加解析规则，您可以实现复杂的事件处理逻辑。数据根据"**额外规范化条件**"设置中指定的条件沿着解析规则树传递。解析规则的创建顺序非常重要：事件按顺序处理，处理顺序用箭头表示。

现在可以使用以下事件规范化选项：

- 1个收集器 – 1个规范化器

  若存在大量同类型事件，或有多个 IP 地址可能产生同类型事件，建议使用此方法。一个收集器仅可配置一个规范化器，此配置在性能方面为最优方案。

- 1个收集器 – 关联到 IP 的多个规范化器

  此方法适用于使用 UDP、TCP 或 HTTP 类型连接器的收集器。如果在"传输"步骤中，在收集器中指定了 UDP、TCP 或 HTTP 连接器，则在"事件解析"步骤中，您可以在"解析设置"选项卡上指定多个 IP 地址，并选择要对来自指定地址的事件使用的规范化器。可使用以下类型的规范化器：`json`、`cef`、`regexp`、`syslog`、`csv`、`kv`、`xml`。对于 `syslog` 和 `regexp` 类型的规范化器，您可以根据 DeviceProcessName 字段的值指定额外的规范化条件。

规范化器的创建分为几个步骤：

1. **准备创建规范化器**

   可以在 OSMP 控制台中创建规范化器：

   - 在"**监控**" → "**资源**" → "**规范化器**"部分创建。
   - 创建收集器时，在"**事件解析**"步骤创建。

   然后必须在规范化器中创建解析规则。

2. **为事件创建主解析规则**

   通过单击"**添加事件解析**"按钮来创建主解析规则。这将打开"**事件解析**"窗口，您可以在其中指定主解析规则的设置：

   - 指定事件解析设置。
   - 指定事件增强设置。

   事件的主解析规则在规范化器中显示为深色圆圈。您可以通过单击此圆圈来查看或修改主解析规则的设置。将鼠标悬停在圆圈上时，会显示一个加号。单击它即可添加解析规则。

   主解析规则的名称在 KUMA 中用作规范化器名称。

3. **创建附加事件解析规则**

将鼠标悬停在圆圈或与规范化器对应的区块上时，单击显示的加号图标将打开“**附加事件解析**”窗口，您可以在其中指定附加解析规则的设置：

- 指定将数据发送到新规范化器的条件。
- 指定事件解析设置。
- 指定事件增强设置。

附加事件解析规则在规范化器中显示为深色区块。该区块显示附加解析规则的触发条件、附加解析规则的名称和事件字段。当此事件字段可用时，数据将传递给规范化器。单击附加解析规则的区块以查看或修改其设置。

如果将鼠标悬停在附加规范化器上，将出现一个加号按钮。您可以单击此按钮来创建新的附加事件解析规则。要删除规范化器，请使用带有垃圾桶图标的按钮。

4. **完成规范化器的创建**

要完成规范化器的创建，请单击“**保存**”。

在右上角的搜索字段中，您可以按名称搜索其他解析规则。

对于规范化器资源，您可以在除“**描述**”字段之外的所有输入字段中启用控制字符的显示。

如果在更改收集器资源集的设置时，更改或删除与其连接的规范化器中的转换，则编辑不会被保存，且规范化器本身可能被损坏。若需修改已属于某个服务的规范化器中的转换规则，则必须在 OSMP 控制台的“**监控**” → “**资源**” → “**规范化器**”下直接对该规范化器进行更改。

事件解析设置

您可以在规范化器设置窗口的“**规范化方案**”选项卡中创建事件解析规则时，配置将传入事件转换为 KUMA 格式的规则。

要定义事件解析设置：

1. 在 **卡巴斯基存储库中的资源版本** 字段中，指定了资源版本号。

   此字段不可编辑。仅适用于卡巴斯基提供的资源，用于管理资源更新。

2. 在“**名称**”字段（必填）中，输入解析规则的唯一名称。必须包含 1 到 128 个 Unicode 字符。主解析规则的名称用作规范化器的名称。

3. 在“**租户**”字段（必填）中，输入资源所属的租户的名称。

   此设置不适用于额外的解析规则。

4. 在“**解析方法**”下拉列表中，选择要接收的事件类型。根据您的选择，您可以使用预配置的规则来匹配事件字段或设置您自己的规则。在选择某些解析方法时，可能需要填写额外的设置字段。

   可用的解析方法：

   - JSON

     此解析方法用于处理 JSON 数据，其中每个对象（包括其嵌套对象）均在文件中占用一行。

     在处理具有层次结构的数据文件时，可以通过指定参数名称并以句点分隔这些名称来访问嵌套对象的字段。例如，可以使用 `user.username` 查询来访问字符串 `"user": {"username": "system: node: example-01"}` 中的 `username` 参数。

将逐行处理文件。具有嵌套结构的多行对象可能会被错误规范化。

在使用附加规范化器的复杂规范化方案中，所有嵌套对象都在第一个规范化级别进行处理，但未指定额外规范化条件的情况除外。因此，正在处理的事件将被完整地传递给附加规范化器。

换行符可以是 `\n` 和 `\r\n`。字符串必须采用 UTF-8 编码。

如果要发送原始事件以进行高级规范化，请在“**高级事件解析**”窗口的每个嵌套级别上，在“**保留原始事件**”下拉列表中选择“**是**”。

- CEF

  此解析方法用于处理 CEF 数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。

- regexp

  此解析方法用于创建自定义规则，以使用正则表达式的格式处理数据。

  在“**规范化**”参数块的字段中，添加一个包含命名捕获组的正则表达式（RE2 语法）。组名及其值将分别被视为原始事件的字段及其值，该字段可转换为 KUMA 格式的事件字段。

  要添加事件处理规则：

  1. 将要处理的数据示例复制到“**事件示例**”字段。该步骤为可选步骤，但建议执行。

     您还可以单击“**通过 KIRA 生成正则表达式**”，根据已添加的示例生成正则表达式。在这种情况下，生成的正则表达式将自动添加到“**规范化**”参数块。

  2. 在“**规范化**”参数块的字段中，添加一个采用 RE2 语法、包含命名捕获组的正则表达式，例如“(?P<name>regexp)”。添加到“**规范化**”参数中的正则表达式必须与事件完全匹配。此外，编写正则表达式时，建议使用匹配文本起始和结束位置的特殊字符：^、$。

     您可以使用“**添加正则表达式**”按钮添加多个正则表达式。如果需要删除正则表达式，请单击 ✕ 按钮。

  3. 单击“**将字段名称复制到映射表**”按钮。

     捕获组名称显示在**映射**表的“**KUMA 字段**”列中。现在，您可以在每个捕获组旁边的列中选择对应的 KUMA 字段。否则，如果您按照 CEF 格式命名了捕获组，可以选中“**使用 CEF 语法进行规范化**”复选框，以使用自动 CEF 映射。

  已添加事件处理规则。

- Syslog

  此解析方法用于处理 syslog 格式的数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。

- csv

  此解析方法用于创建处理 CSV 数据的自定义规则。

  选择此方法时，必须在“**分隔符**”字段中指定字符串中各值的分隔符。任何单字节 ASCII 字符都可以用作分隔符。

- **kv**

  此解析方法用于处理键值对格式的数据。

  如果选择此方法，必须在以下必填字段中提供值：

  - "**配对分隔符**"——指定用作键值对分隔符的字符。您可以指定任意单字符（1字节）值，但该字符不能与值分隔符相同。
  - "**值分隔符**"——指定用作键和值之间分隔符的字符。您可以指定任意单字符（1字节）值，但该字符不能与键值对分隔符相同。

- **xml**

  此解析方法用于处理 XML 数据。在文件中，每个对象（包括其嵌套对象）各占一行。将逐行处理文件。

  如果要发送原始事件以进行高级规范化，请在"**高级事件解析**"窗口的每个嵌套级别上，在"**保留原始事件**"下拉列表中选择"**是**"。

  选择此方法后，您可以在"**XML 属性**"参数块中指定要从标签中提取的关键属性。如果 XML 结构的同一标签中有多个值不同的属性，您可以在"**映射**"表的"**源**"列中指定所需值对应的键。

  要添加关键 XML 属性，

  单击"**添加字段**"按钮，然后在显示的窗口中指定所需属性的路径。

  您可以添加多个属性。可以使用叉号图标逐个移除属性，也可以使用"**重置**"按钮一次性移除所有属性。

  如果未指定 XML 键属性，则在字段映射过程中，XML 值的唯一路径将由一系列标签表示。

  标签编号

  标签编号功能自 KUMA 2.1.3 起可用。此功能可自动为 XML 事件中的标签编号，以便解析包含相同标签或未命名标签（例如 <Data>）的事件。

  下面以 **Microsoft Windows PowerShell 事件 ID 800** 的 EventData 属性为例，使用**标签编号**功能为其中的标签编号。

  
  PowerShell 事件 ID 800

  要解析此类事件，您必须：

  - 配置标签编号。
  - 配置编号后的标签与 KUMA 事件字段之间的数据映射。

  KUMA 3.0.x 支持在同一个额外规范化器中同时使用**XML 属性**和**标签编号**功能。如果属性包含未命名标签或相同标签，建议使用**标签编号**功能。如果属性仅包含命名标签，请使用**XML 属性**功能。要在额外规范化器中使用此功能，您必须依次在事件到达目标额外规范化器所经过的每个额外规范化器中，以及目标额外规范化器本身，启用"保留原始事件"设置。

  有关此功能的使用示例，请参阅 MicrosoftProducts 规范化器 — 其中在"AD FS"和"424"额外规范化器中依次启用了"保留原始事件"设置。

要配置对包含同名标签或未命名标签的事件的解析：

1. 创建新的规范化器，或打开现有规范化器进行编辑。
2. 在规范化器的**基本事件解析**窗口中，从**解析方法**下拉列表中选择"xml"，然后在**标签编号**字段中点击**添加字段**。

   在显示的字段中，输入要为其元素编号的标签的完整路径。例如，Event.EventData.Data。为标签分配的第一个编号为 0。如果标签为空，例如 <Data />，也会为其分配编号。
3. 要配置数据映射，请在**映射**下点击**添加行**，然后执行以下操作：

   a. 在新行的**来源**字段中，输入标签的完整路径及其索引。对于上述示例中的 Microsoft Windows 事件，带索引的完整路径如下：

   - Event.EventData.Data.0,
   - Event.EventData.Data.1
   - Event.EventData.Data.2，依此类推

   b. 在"**KUMA 字段**"下拉列表中，选择 KUMA 事件中用于接收解析后带编号标签对应值的字段。
4. 要保存更改：

   - 如果您创建了新的规范化器，请单击"**保存**"。
   - 如果您编辑了现有的规范化器，请在该规范化器关联的收集器中单击"**更新配置**"。

已配置解析。

- **netflow5**

  此解析方法用于处理 NetFlow v5 格式的数据。

  选择此方法时，您可以单击"**应用默认映射**"按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 netflow5 类型进行主解析，则无法进行额外的规范化。

  > 在映射规则中，默认情况下不会在 KUMA 事件的字段中指明 **netflow5** 的协议类型。在解析 NetFlow 格式的数据时，在**增强**规范化器选项卡上，您必须创建一条**常量**数据增强规则，该规则会将 `netflow` 值添加到 `DeviceProduct` 目标字段。

- **netflow9**

  此解析方法用于处理 NetFlow v9 格式的数据。

  选择此方法时，您可以单击"**应用默认映射**"按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 netflow9 类型进行主解析，则无法进行额外的规范化。

  > 在映射规则中，默认情况下不会在 KUMA 事件的字段中指明 **netflow9** 的协议类型。在解析 NetFlow 格式的数据时，在**增强**规范化器选项卡上，您必须创建一条**常量**数据增强规则，该规则会将 `netflow` 值添加到 `DeviceProduct` 目标字段。

- **sflow5**

  此解析方法用于处理 sflow5 格式的数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 sflow5 类型进行主解析，则无法进行额外的规范化。

- **ipfix**

  此解析方法用于处理 IPFIX 数据。

  选择此方法时，您可以单击“**应用默认映射**”按钮，使用预配置规则将事件转换为 KUMA 格式。如果选择 ipfix 类型进行主解析，则无法进行额外的规范化。

  > 在映射规则中，默认情况下不会在 KUMA 事件的字段中指明 **ipfix** 的协议类型。在解析 NetFlow 格式的数据时，在**增强**规范化器选项卡上，您必须创建一条**常量**数据增强规则，该规则会将 `netflow` 值添加到 `DeviceProduct` 目标字段。

- sql — 仅在使用 sql 类型的连接器时，此方法才可用。

  规范化器使用此方法处理从数据库中查询得到的数据。

5. 在“**保留原始事件**”下拉列表中，指定是否将原始事件存储在新创建的规范化事件中。可用值：

   - **不保存** — 不保存原始事件。这是默认设置。
   - **仅出错时** — 如果解析原始事件时发生错误，将原始事件保存到规范化事件的 `Raw` 字段中。该值在调试服务时使用起来十分方便。在这种情况下，每当事件的 `Raw` 字段不为空时，您就知道出现了问题。

     > 如果包含名称 `*Address` 或 `*Date*` 的字段不符合规范化规则，这些字段会被忽略。在这种情况下，不会发生规范化错误，即使已选择“**保留原始事件**” → “**仅出错时**”选项，字段值也不会显示在规范化事件的 `Raw` 字段中。

   - **始终** — 始终将原始事件保存在规范化事件的 `Raw` 字段中。

   此设置不适用于额外的解析规则。

6. 在“**保留额外字段**”下拉列表中，选择当原始事件字段未配置映射规则时，是否要将其存储在规范化事件中（详见下文）。数据存储在 `Extra` 事件字段中。您可以根据 `Extra` 字段中存储的数据对规范化事件进行搜索和筛选。

   基于“Extra”事件字段数据的筛选

   基于 **Extra** 事件字段数据的筛选条件如下：

   - 条件 — **如果**。
   - 左操作数 — **事件字段**。
   - 在此事件字段中，您可以指定以下值之一：
     - **Extra** 字段。
     - Extra 字段中的值格式如下：

`Extra.<field name>`

例如，`Extra.app`。

此类型的值需手动指定。

- 写入 **Extra** 字段的数组值格式如下：

  `Extra.<field name>.<array element>`

  例如，`Extra.array.0`。

  数组中的值从 0 开始编号。

  此类型的值需手动指定。

  要使用 Extra 字段中第 3 层及更深层级的值，请使用反引号 ``。例如，`Extra.lev1.lev2.lev3`。

- 运算符 — =。
- 右操作数 — **常量**。
- 值 — 用于过滤事件的值。

默认情况下，字段不会被保存。

7. 在“**描述**”字段中，指定资源描述：最多 4,000 个 Unicode 字符。

   此设置不适用于额外的解析规则。

8. 在“**事件示例**”字段中，您可以提供要处理的数据示例。

   此设置不适用于以下解析方法：**netflow5**、**netflow9**、**sflow5**、**ipfix**、**sql**。

   如果事件解析成功，并且从原始事件获取的数据类型与 KUMA 字段的类型匹配，则“**事件示例**”字段将填充从原始事件获取的数据。

   例如，括在引号中的值“192.168.0.1”不会显示在 SourceAddress 字段中，而是会在“**事件示例**”字段中显示值 192.168.0.1。

9. 在“**映射**”表中，配置原始事件字段到 KUMA 格式事件字段的映射：

   a. 在“**源**”列中，提供要转换为 KUMA 事件字段的原始事件字段的名称。

   有关字段格式的详细信息，请参阅“规范化事件数据模型”文章。有关映射的说明，请参阅“预定义规范化器的字段映射”文章。

   单击“**源**”列中字段名称旁边的“🔧”按钮，将打开“**转换**”窗口。在该窗口中，您可以单击“**添加转换**”按钮，以创建在将原始数据写入 KUMA 事件字段之前进行修改的规则。

   可用转换

   转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

   可用转换：

   - **lower** — 用于将值的所有字符变为小写
   - **upper** — 用于将值的所有字符变为大写
   - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
   - **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。

- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除"**字符**"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
- **append** 用于将"**常量**"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

在“**转换**”窗口中，可以通过拖动 ⣿ 图标来交换添加的规则；您也可以使用 ✕ 图标来删除规则。

b. 在 **KUMA 字段**列中，从下拉列表中选择所需的 KUMA 事件字段。您可以通过在字段中输入名称来搜索字段。

有关 KUMA 字段列的建议

建议您配置以下 KUMA 字段的映射。否则，您将无法在警报详情和事故详情中查看可观察对象。

推荐的 KUMA 字段取决于可观察对象类型：

- 对于 MD5 哈希和 SHA256 类型的可观察对象：
  - FileHash
- 对于 URL 类型的可观察对象：
  - RequestUrl
- 对于 IP 地址类型的可观察对象：
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress
  - SourceTranslatedAddress
  - SourceAddress
- 对于域名类型的可观察对象：
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain

- SourceDnsDomain
- SourceNtDomain

- 对于 UserName 类型的可观察对象：
  - DestinationUserName
  - SourceUserName
- 对于 HostName 类型的可观察对象：
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. 如果上一步中选择的 KUMA 事件字段的名称以 `DeviceCustom*` 或 `Flex*` 开头，您可以在“**标签**”字段中添加唯一的自定义标签。

可以使用“**添加行**”按钮添加新的表格行。可以使用 ✕ 按钮逐行删除，也可以使用“**全部清除**”按钮一次性删除所有行。

如果希望 KUMA 使用资产信息增强事件数据，并在触发关联规则时在警报卡中显示资产信息，请在“**映射**”表中根据资产的用途配置主机地址和主机名字段的映射。例如，映射可以应用于 SourceAddress 和 SourceHostName，或 DestinationAddress 和 DestinationHostName 字段。进行事件增强后，事件卡将包含 SourceAssetID 或 DestinationAssetID 字段，以及指向资产卡的链接。此外，进行事件增强后，资产信息也将显示在警报卡中。

如果您已将数据加载到“**事件示例**”字段中，则该表将包含一个“**示例**”列，其中包含从原始事件字段转移到 KUMA 事件字段的值示例。

如果 KUMA 事件字段的大小小于其中放置值的长度，则该值将被截断为事件字段的大小。

扩展事件模式

在规范化事件时，除了标准 KUMA 事件模式字段外，还可以使用扩展事件模式字段。下表显示了有关扩展事件模式字段类型的信息。

使用扩展事件模式的多个唯一字段会降低系统性能、增加存储事件所需的磁盘空间，并导致信息难以理解。

建议您有意识地选择扩展事件模式中要在规范化器和关联中使用的最小附加字段集。

要使用扩展事件模式字段：

- 打开现有的事件规范化器或创建一个新的事件规范化器。
- 指定规范化器的基本设置。
- 单击“**添加行**”。
- 对于“**源**”设置，请输入原始事件中源字段的名称。

- 对于“**KUMA 字段**”设置，请输入您正在创建的扩展事件模式字段的名称（请参阅下表）。您也可以使用扩展事件模式的现有字段。

  规范化事件的扩展数据模型的字段：

字段名称 在“KUMA 字段”设置中指定	数据类型	在规范化器中的可用性	描述
S.<字段名称>	字符串	所有类型	`String` 类型的字段
N.<字段名称>	数字	所有类型	`Number` 类型的字段
F.<字段名称>	浮点数	所有类型	`Float` 类型的字段
SA.<字段名称>	字符串数组	KV、JSON	`Array of strings` 类型的字段。数组元素的顺序与原始事件的元素顺序相同。
NA.<字段名称>	整数数组	KV、JSON	`Array of integers` 类型的字段。数组元素的顺序与原始事件的元素顺序相同。
FA.<字段名称>	浮点数数组	KV、JSON	`Array of floats` 类型的字段。数组元素的顺序与原始事件的元素顺序相同。

在创建扩展事件模式的字段时，必须加上前缀`S.`、`N.`、`F.`、`SA.`、`NA.`、`FA.`；这些前缀必须严格使用大写表示。

将<字段名称>替换成实际的字段名称。您可以在字段名称中使用英文字母和数字。不允许使用空格字符。

- 单击“**确定**”。
- 单击“**保存**”，完成事件规范化器的编辑。

规范化器已保存，附加字段已创建。保存规范化器后，附加字段可在其他规范化器中使用。

注意：如果原始事件的字段中的数据与 KUMA 字段的类型不匹配，则在事件规范化期间不会保存该值。例如，字符串 `test` 无法写入 `Number` 类型的“DeviceCustomNumber1 KUMA”字段。

如果要在搜索事件、准备报告和对存储中的事件执行其他操作时最大限度地减少存储服务器的负载，请将 KUMA 事件模式字段作为首选，将扩展事件模式字段作为第二选择，将额外字段作为最后的选择。

扩展事件模式

您可以在规范化器中使用扩展事件模式字段来规范化事件，也可以在其他KUMA资源中使用，例如用作小部件字段或用于筛选和搜索事件。您可以在**设置→KUMA→打开KUMA设置→扩展字段集**部分查看KUMA中所有扩展事件模式字段的列表。所有租户的扩展事件模式字段列表均相同。

在该部分顶部，会显示扩展字段集的版本号。此版本号用于管理扩展字段的更新。

只有具有主管理员、租户管理员、二级分析师、一级分析师、初级分析师、读取共享资源和管理共享资源角色的用户才能查看扩展事件模式字段表。

扩展事件模式字段表包含以下信息：

- **类型**– 扩展事件模式字段的数据类型。

  可能的数据类型：

类型	在规范化器中的可用性	数据类型
S	所有类型	字符串。
N	所有类型	数字。

类型	在规范化器中的可用性	数据类型
F	所有类型	浮点数。
SA	KV、JSON	字符串数组。 数组元素的顺序与原始事件的元素顺序相同。
NA	KV、JSON	整数数组。 数组元素的顺序与原始事件的元素顺序相同。
FA	KV、JSON	浮点数数组。 数组元素的顺序与原始事件的元素顺序相同。

- **字段名称**– 扩展事件模式字段的名称（不包含类型）。

  您可以点击名称来编辑扩展事件模式字段的设置。

- **状态**– 扩展事件模式字段是否可用于资源。

  您可以**启用**或**禁用**切换开关，以允许或禁止在新资源中使用此扩展事件模式字段。但是，禁用字段仍然在已运行的资源配置中使用，直到您手动从配置中删除该字段；该字段仍然在**事件**部分的表格列列表中可用，用于管理旧事件。

  只有具有主管理员角色的用户才能禁用扩展事件模式字段。

- **更新日期**– 扩展事件模式字段的最后修改日期和时间。

- **创建者**– 创建扩展事件模式字段的用户的名称。

- **依赖关系**–使用该扩展事件模式字段的KUMA 资源、仪表盘布局、报告、预设以及用于搜索事件源的字段集的数量。

  您可以点击数字打开一个面板，其中包含一个表格，列出了所有使用此字段的资源和其他KUMA实体。对于每个依赖项，表格会显示名称、租户（仅适用于资源）和类型。表格中的依赖项按名称排序。点击依赖项的名称即可进入其页面（控制板布局、预设和已保存的用户查询除外）。

  您只能查看您有权访问的租户中的资源和实体的扩展事件模式字段的依赖项。如果您没有该租户的访问权限，则其资源不会显示在表格中，但仍计入依赖项的数量。

- **描述**– 字段的文本描述。

默认情况下，扩展事件模式字段表格按更新日期降序排列。如有必要，您可以点击列标题并选择**升序**或**降序**来对表格进行排序；您还可以按字段名称进行上下文搜索。

默认情况下，以下服务扩展事件模式字段会自动添加到KUMA：

- `KL_EventRoute`，类型为 `S`，用于存储事件路由信息。

  您可以在标准化器中使用此字段，在活动列表中将其用作密钥或值，在增强规则中使用，在数据收集和分析规则中将其用作查询字段，以及在关联规则中使用。此字段不能用于检测事件源。

- 以下字段将添加到关联事件中：

  - `KL_CorrelationRulePriority`，类型为 `N`
  - `KL_SourceAssetDisplayName`，类型为 `S`
  - `KL_DestinationAssetDisplayName`，类型为 `S`
  - `KL_DeviceAssetDisplayName`，类型为 `S`

- `KL_SourceAccountDisplayName`，类型为 `S`
- `KL_DestinationAccountDisplayName`，类型为 `S`

此服务字段不能用于搜索事件。

服务字段无法编辑、删除、导出或禁用。所有带有`KL_`前缀的扩展事件模式字段都是服务字段，只能从卡巴斯基服务器中进行管理。我们不建议在新增扩展事件模式字段时使用`KL_`前缀。

添加扩展事件模式字段

具有主管理员、租户管理员、二级分析师、一级分析师、初级分析师和管理共享资源角色的用户可以添加新的扩展事件模式字段。

若要添加扩展事件模式字段：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→**打开KUMA设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**其他**下，点击**扩展字段集**。
   这将打开**扩展字段集**窗口。
3. 点击表格上方的**添加**按钮。
   这将打开**创建扩展模式**窗格。
4. 启用或禁用**状态**切换开关，以启用或禁用此扩展事件模式字段。
   默认情况下，切换开关处于打开状态。禁用字段仍保留在**事件**部分的表格列列表中，用于管理旧事件。
5. 在**类型**字段中，选择扩展事件模式字段的数据类型。
   可能的数据类型

类型	在规范化器中的可用性	数据类型
`S`	所有类型	字符串。
`N`	所有类型	数字。
`F`	所有类型	浮点数。
`SA`	KV、JSON	字符串数组。 数组元素的顺序与原始事件的元素顺序相同。
`NA`	KV、JSON	整数数组。 数组元素的顺序与原始事件的元素顺序相同。
`FA`	KV、JSON	浮点数数组。 数组元素的顺序与原始事件的元素顺序相同。

6. 在**名称**字段中，指定扩展事件模式字段的名称。
   命名扩展事件模式字段时，请考虑以下事项：
   - 名称在KUMA实例中必须是唯一的。
   - 名称区分大小写。例如，`Field_name` 和 `field_name` 是不同的名称。
   - 您可以使用拉丁字母、西里尔字母和数字。不允许使用空格或"~`@#$%^&*()+-[]{}|\|/."<>:!,.?=字符。

- 如果要使用扩展事件模式字段搜索事件源，则只能使用拉丁字符和数字。
- 最大长度为 128 个字符。

7. 如有必要，请在**描述**字段中输入扩展事件模式字段的描述。

   我们建议描述扩展事件模式字段的用途。描述中只允许使用Unicode字符。最大长度为 256 个字符。

8. 单击“**保存**”按钮。

表格顶部随即新增一个扩展事件模式字段。创建扩展事件模式字段时会生成一个审计事件。如果已启用该字段，则可以在规范化器和配置资源时使用它。

编辑扩展事件模式字段

具有主管理员、租户管理员、二级分析师、一级分析师、初级分析师和管理共享资源角色的用户可以编辑现有的扩展事件模式字段。

若要编辑扩展事件模式字段：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→**打开KUMA设置**部分。

   这将打开 KUMA 设置窗口。

2. 在**其他**下，点击**扩展字段集**。

   这将打开**扩展字段集**窗口。

3. 点击要编辑的字段名称。

   这将打开**编辑扩展模式**面板。此面板显示所选字段的设置，以及**依赖项**表，其中包含资源列表、控制板布局、报告、预设和字段集，用于查找使用此字段的事件源。仅显示您有权访问的租户的资源。如果该字段被您无权访问的租户的资源使用，则此类资源不会显示在表中。表格中的资源按名称排序。

   点击资源或实体的名称即可进入其页面（控制板资源、预设和已保存的用户查询除外）。

4. 在可用设置中进行所需的更改：

   只有当扩展事件模式字段没有依赖项时，才能编辑**类型**和**字段名称**设置。您可以编辑任何扩展事件模式字段的**状态**和**描述**设置。但是，具有**禁用**状态的字段仍会在已运行的资源配置中使用，直到您手动从配置中删除该字段；该字段仍然在**事件**部分的表格列列表中可用，用于管理旧事件。

   使用**状态**字段禁用扩展事件模式字段需要具备主管理员角色。

5. 单击“**保存**”按钮。

扩展事件模式字段随即更新。系统会生成一条关于字段修改的审计事件。

导入和导出扩展事件模式字段

您可以通过从JSON文件导入，一次新增多个扩展事件模式字段。您还可以将所有扩展事件模式字段及其相关信息导出到文件中，例如，将字段列表传播到其他KUMA实例来维护资源。

具有主管理员、租户管理员、二级分析师、一级分析师、初级分析师和管理共享资源角色的用户可以导入和导出扩展事件模式字段。具有“读取共享资源”角色的用户只能导出扩展事件模式字段。

若要将扩展事件模式字段从文件导入KUMA：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→**打开KUMA设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**其他**下，点击**扩展字段集**。
   这将打开**扩展字段集**窗口。
3. 单击“**导入**”按钮。
4. 这将打开一个窗口；在该窗口中，选择一个包含扩展事件模式字段对象列表的JSON文件。
   JSON文件示例：

```
[
{"kind": "SA",
"name": "<fieldName1>",
"description": "<description1>",
"disabled": false},
{"kind": "N",
"name": "<fieldName2>",
"description": "<description2>",
"disabled": false},
....
{"kind": "FA",
"name": "<fieldNameX>",
"description": "<descriptionX>",
"disabled": false}
]
```

从文件中导入字段时，会检查字段名称是否与同类型字段存在冲突。如果KUMA中已存在同名同类型的字段，则不会从文件中导入此类字段。

扩展事件模式字段是从文件导入到KUMA的。系统会生成一个关于字段导入的审计事件，并且每个新增字段都会生成一个单独的审计事件。

若要将扩展事件模式字段导出到文件：

1. 在应用程序主窗口中，转到**设置**→**KUMA**→**打开KUMA设置**部分。
   这将打开 KUMA 设置窗口。
2. 在**其他**下，点击**扩展字段集**。
   这将打开**扩展字段集**窗口。

3. 如果要导出特定的扩展事件模式字段：

   a. 选中表格第一列中所需字段的复选框。

      您不能选择服务字段。

   b. 点击表格顶部的**导出所选项**按钮。

4. 如果要导出所有扩展事件模式字段，请点击表格顶部的**全部导出**按钮。

系统将下载一个包含扩展事件模式字段对象列表及其相关信息的JSON文件。

删除扩展事件模式字段

只有具有主管理员角色的用户才能删除扩展事件模式字段。

您只能删除非服务字段、状态为**已禁用**且未在KUMA资源和其他实体中使用（无依赖项）的扩展事件模式字段。我们建议在删除扩展事件模式字段之前等待足够长的时间，以确保所有使用该字段的事件都已从KUMA中删除。删除字段后，该字段将不再显示在事件提示中。

若要删除扩展事件模式字段：

1. 在应用程序主窗口中，转到**设置**→KUMA→**打开**KUMA**设置**部分。

   这将打开 KUMA 设置窗口。

2. 在**其他**下，点击**扩展字段集**。

   这将打开**扩展字段集**窗口。

3. 选中表格第一列中要删除的一个或多个字段旁边的复选框。

   要选择所有字段，您可以选中第一列标题中的复选框。

4. 点击表格顶部的**删除**按钮。

   仅当所有选定字段均已禁用且无依赖项时， **删除**按钮才处于活动状态。如果至少有一个字段已启用或存在依赖项，则该按钮处于非活动状态。

   如果您想删除至少一个KUMA资源中使用的字段（具有依赖项），但您没有访问其租户的权限，则选中该字段时**删除**按钮处于活动状态，但尝试删除时会显示错误。

选定的字段随即删除。系统会生成一条关于字段删除的审计事件。

在规范化器中使用扩展事件模式字段

使用扩展事件模式字段时，收集器可处理的事件最大大小的一般限制相同，均为 4 MB。下表显示了有关扩展事件模式字段类型的信息（说明的第6步）。

使用扩展事件模式的多个唯一字段会降低系统性能、增加存储事件所需的磁盘空间，并导致信息难以理解。

建议您有意识地选择扩展事件模式中要在规范化器和关联中使用的最小附加字段集。

若要使用扩展事件模式字段：

1. 打开现有的规范化器或创建一个新的规范化器。
2. 指定规范化器的基本设置。
3. 单击“**添加行**”。
4. 对于“**源**”设置，请输入原始事件中源字段的名称。
5. 对于**KUMA字段**设置，开始输入扩展事件模式字段的名称，然后从下拉列表中选择该字段。
   下拉列表中的扩展事件模式字段的名称采用 `<type>.<field name>` 格式。
6. 单击**保存**按钮以保存事件规范化器。

规范化器与选定的扩展事件模式字段一起保存。

如果原始事件字段中的数据与KUMA字段的类型不匹配，如果无法执行类型转换，则在事件规范化期间不会保存该值。例如，字符串 `test` 无法写入 Number 类型的 `DeviceCustomNumber1` KUMA 字段。

如果要在搜索事件、准备报告以及对存储中的事件执行其他操作时最大限度地减少存储服务器的负载，请将 KUMA 事件模式字段作为首选，将扩展事件模式字段作为第二选择，将 `Extra` 字段作为最后选择。

使用 KIRA 生成正则表达式

您可以借助卡巴斯基调查与响应助手，根据使用 **regexp** 解析方法的规范化器的事件示例，自动创建一个或多个正则表达式。此功能可供具有主管理员、租户管理员、二级分析师、一级分析师和初级分析师角色的用户使用。

要生成正则表达式：

1. 获取包含 AI 模块的授权许可，并在 KUMA 中激活该功能。
2. 配置 KIRA 集成，使用第三方 LLM 提供商（**自定义**模式）。
3. 开始创建规范化器或打开现有规范化器的设置。
4. 在 **规范化方案** 选项卡上的 **解析方式** 下拉列表中，选择 **regexp**。
5. 在 **事件示例** 字段中，添加一个或多个要从中创建正则表达式的示例事件。
   您最多可以添加 10 个单行事件。
6. 单击 **通过 KIRA 生成正则表达式** 按钮。
7. 确认您的请求。
   请求处理完毕后，将显示一个窗口，其中包含以下信息：
   - 生成所消耗的令牌数量
   - 生成的正则表达式，其中以颜色突出显示分组以及示例事件的相应片段。

   每个生成的正则表达式均以 (?:ai)? 字符组开头。

在包含已创建表达式的窗口中，您可以编辑和复制正则表达式，并通过单击 **应用** 按钮来应用生成结果。

如果正则表达式生成失败或未产生预期结果，则可能表示您使用的提供商模型无法正确识别事件的组成部分或生成正则表达式。尝试重新开始生成。如果错误再次出现，请在 **事件示例** 字段中添加更多类似示例，然后重新开始生成。发生错误后重新开始生成时，不会消耗额外的令牌。

应用结果后，生成的正则表达式会自动添加到 **规范化** 字段。如果生成了多个正则表达式，则会自动为每个表达式生成相应数量的字段。正则表达式会按生成顺序添加。如有必要，您可以使用 ⠿ 图标拖动表达式来更改顺序。

8. 应用生成的正则表达式后，依次单击 **确定** 按钮和 **保存** 按钮，以保存规范化器设置。

规范化器中的增强操作

在“规范化器设置”窗口的“**增强**”选项卡上创建事件解析规则时，您可以配置使用增强规则向规范化事件的字段添加额外数据的规则。这些增强规则存储在创建它们的规范化器设置中。

通过单击“**添加增强**”按钮可以创建增强功能。可以指定多个增强规则。您可以通过单击 ✕ 按钮来删除增强规则。

增强规则设置区块中的可用设置：

- **源类型**（必填） — 用于选择增强类型的下拉列表。根据所选类型，可能还会显示需要填写的高级设置。
  可用的增强规则源类型：
  - **常量**

    在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置：

    - 在“**常量**”字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。
    - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

    如果对 `String`、 `Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。

    如果对 `Array of strings`、`Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。

  - **词典**

    如果需要从“字典”类型的**字典**中添加值，则使用此类型的增强规则。

    在“**字典名称**”下拉列表中选择此类型后，必须选择用于提供值的字典。在“**键字段**”设置块中，您必须点击“**添加字段**”按钮，然后选择相应的事件字段，其值将用于词典条目选择。

    如果您使用事件增强功能，并在“源类型”设置中选择了“字典”类型，且在“键增强字段”设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。

    示例：“键增强字段”设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”。以下值作为键传递给字典：['a','b','c']。

如果“键增强字段”设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以“|”字符分隔。

示例：“键增强字段”设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”；Code 字符串字段包含字符序列“myCode”。以下值作为键传递给词典：['a','b','c']myCode。

- **表格**

  如果您需要从“表格”类型的**字典**中添加值，则需使用此类型的增强功能。

  在“**字典名称**”下拉列表中选择此增强类型后，选择用于提供值的字典。在“**键字段**”设置组中，单击“**添加字段**”按钮以选择其值用于字典条目选择的事件字段。

  在“**映射**”表格中，配置用于提供数据的字典字段和用于接收数据的事件字段：

  - 在“**字典字段**”列中，选择字典字段。可用字段取决于所选的字典资源。
  - 在“**KUMA 字段**”列中，选择要写入值的事件字段。对于某些所选字段（`*custom*` 和 `*flex*`），在“**标签**”列中，可以为写入其中的数据指定一个名称。

  可通过单击“**添加新元素**”按钮添加新的表行。可通过单击 ✕ 按钮删除列。

- **事件**

  若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置：

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
  - 在“**源字段**”下拉列表中，选择要将其值写入目标字段的事件字段。
  - 单击 🔧 按钮将打开“**转换**”窗口。您可以在该窗口中使用“**添加转换**”按钮创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。

    可用转换

    转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

    可用转换：

    - **lower** — 用于将值的所有字符变为小写
    - **upper** — 用于将值的所有字符变为大写
    - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
    - **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
    - **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
      - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
      - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。

- **trim** — 用于同时从值的开始和结束位置删除"**字符**"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。

- **append** 用于将"**常量**"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。

- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。

- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。

  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。

  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。

- 将编码字符串转换为文本：

  - **decodeHexString** — 用于将 HEX 字符串转换为文本。

  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。

  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。

- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。

- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。

- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

使用事件增强功能时，如果在"**源类型**"设置中选择了"**事件**"，并将扩展事件模式字段用作参数，则需要特别注意以下事项：

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `String` 类型的字段，则值会以 TSV 格式写入目标字段。

  例如：SA.StringArray 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 DeviceCustomString1 事件模式字段。操作后，DeviceCustomString1 字段包含 ["string1", "string2", "string3"]。

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `Array of strings` 类型的字段，则将源字段的值附加到目标字段的值之后，并将结果写入目标字段，使用逗号（","）作为分隔符。

  例如：SA.StringArrayOne 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 SA.StringArrayTwo 事件模式字段。操作后，SA.StringArrayTwo 字段包含 "string1"、"string2" 和 "string3"。

- **模板**

  在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

  - 在"**模板**"字段中，输入 Go 模板。

    事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。

    例如：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

  - 在"**目标字段**"下拉列表中，选择要写入数据的 KUMA 事件字段。

  要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

  如果您使用事件增强功能，并在"**源类型**"设置中选择了"**模板**"类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

  例如：

  {{.SA.StringArrayOne}}

  例如：

  {{- range $index, $element := .SA.StringArrayOne -}}

  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **目标字段**（必填）— 用于选择应接收数据的 KUMA 事件字段的下拉列表。

  此设置不适用于"**表格**"类型的增强源。

将数据发送到额外规范化器的条件

创建附加事件解析规则时，可以指定条件。满足这些条件时，事件将被发送到已创建的解析规则进行处理。可以在**附加事件解析**窗口的**额外规范化条件**选项卡中指定条件。此选项卡不适用于基本解析规则。

可用设置：

- **使用原始事件** — 如果要发送原始事件进行额外规范化处理，请在**保留原始事件**下拉列表中选择**是**。默认值是“**否**”。建议将原始事件传递给 json 和 xml 类型的规范化器。如果要将原始事件发送到第二、第三等嵌套级别进行额外规范化，请在每个嵌套级别的“**保留原始事件**”下拉列表中选择“**是**”。

- **要传入规范化器的字段** — 表示事件字段，仅在希望发送包含规范化器设置中配置的字段的事件进行额外解析时使用。

  如果此字段为空，则完整事件将发送到额外的规范化器进行处理。

- 过滤器集 — 用于定义规范化器接收的事件必须满足的复杂条件。

  您可以使用**添加条件**按钮添加一个包含用于标识条件的字段的字符串（见下文）。

  您可以点击**添加群组**按钮来添加过滤器群组。组运算符可以在 **AND**、**OR** 和 **NOT** 之间切换。您可以添加其他条件组，也可以将单个条件添加到过滤器组中。

  您可以通过使用 ⣿ 图标进行拖动操作来交换条件与条件组；也可使用 ✕ 图标将其删除。

过滤条件设置：

- **左操作数**和**右操作数** — 用于指定需要通过运算符处理的值。

  在左操作数中，必须指定进入规范化器的事件的源字段。例如，如果在**事件基础解析**窗口中配置了 eventType - DeviceEventClass 映射，则在**附加事件解析**窗口的**额外规范化条件**选项卡中，必须在过滤器的左操作数字段中指定eventType。数据仅作为文本字符串进行处理。

- 运算符：

  - **=** – 左右操作数完全匹配。

  - **startsWith** – 左操作数以右操作数中指定的字符开头。

  - **endsWith** – 左操作数以右操作数中指定的字符结尾。

  - **match** – 左操作数与右操作数中指定的正则表达式 (RE2) 匹配。

  - **in** – 左操作数与右操作数中指定的值之一匹配。

可以通过单击 🔧 按钮来转换传入的数据。**转换**窗口随即打开，您可以在其中单击**添加转换**按钮，创建用于在对源数据执行任何操作之前转换源数据的规则。在“**转换**”窗口中，可以通过拖动 ⣿ 图标来交换添加的规则；您也可以使用 ✕ 图标来删除规则。

可用转换

转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

可用转换：

- **lower** — 用于将值的所有字符变为小写

- **upper** — 用于将值的所有字符变为大写

- **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。

- **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。

- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除"**字符**"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
- **append** 用于将"**常量**"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

支持的事件源

KUMA 支持对来自下表所列系统的事件进行规范化处理。分发包中包含这些系统的规范化器。

支持的事件源

系统名称	规范化器名称	类型	规范化器描述
1C EventJournal	[OOTB] 1C EventJournal Normalizer	xml	用于处理 1C 系统的事件日志。事件源为 1C 日志。
1C TechJournal	[OOTB] 1C TechJournal Normalizer	regexp	用于处理技术事件日志。事件源为 1C 技术日志。
Absolute Data and Device Security (DDS)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
AhnLab Malware Defense System (MDS)	[OOTB] Syslog-CEF	Syslog	用于用于处理 CEF 格式的事件。
Ahnlab UTM	[OOTB] Ahnlab UTM	regexp	用于处理来自 Ahnlab 系统的事件。事件源包括系统日志、操作日志、连接日志和 IPS 模块。
AhnLabs MDS	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Alcatel AOS-W	[OOTB] Alcatel AOS-W syslog	regexp	用于处理通过 syslog 从 Alcatel AOS-W 6.4 接收的部分事件。
Alcatel Network Switch	[OOTB] Alcatel Network Switch syslog	Syslog	用于处理通过 syslog 从 Alcatel 网络交换机接收的某些类型的事件。
Apache Cassandra	[OOTB] Apache Cassandra 文件	regexp	用于处理 Apache Cassandra 数据库 4.0 版日志中的事件。
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Atlassian Confluence	[OOTB] Atlassian Jira Confluence 文件	regexp	用于处理存储在文件中的 Atlassian Jira、 Atlassian Confluence 系统（Jira 9.12、Confluence 8.5）的事件。
Atlassian Jira	[OOTB] Atlassian Jira Confluence 文件	regexp	用于处理存储在文件中的 Atlassian Jira、 Atlassian Confluence 系统（Jira 9.12、Confluence 8.5）的事件。
Avanpost FAM	[OOTB] Avanpost FAM syslog	regexp	用于处理通过 syslog 接收的 Avanpost Federated Access Manager (FAM) 1.9 事件。
Avanpost IDM	[OOTB] Avanpost IDM syslog	regexp	用于处理通过 syslog 接收的 Avanpost IDM 系统事件。
Avanpost PKI	[OOTB] Avanpost PKI syslog CEF	Syslog	用于处理通过 Syslog 以 CEF 格式从 Avanpost PKI 6.0 接收的事件。
Avaya Aura Communication Manager	[OOTB] Avaya Aura Communication Manager syslog	regexp	用于处理通过 Syslog 从 Avaya Aura Communication Manager 7.1 接收的某些事件。
Avigilon Access Control Manager (ACM)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Ayehu eyeShare	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Arbor Pravail	[OOTB] Arbor Pravail syslog	Syslog	用于处理通过 Syslog 接收的 Arbor Pravail 系统事件。

系统名称	规范化器名称	类型	规范化器描述
Aruba Aruba AOS-S	[OOTB] Aruba Aruba AOS-S syslog	regexp	用于处理通过 Syslog 从运行 Aruba AOS-S 16.10 固件的 Aruba 网络设备接收的特定类型事件。规范化器支持以下类型的事件：会计事件、ACL 事件、ARP 保护事件、身份验证事件、控制台事件、环路保护事件。
Barracuda Cloud Email Security Gateway	[OOTB] Barracuda Cloud Email Security Gateway syslog	regexp	用于处理通过 Syslog 从 Barracuda Cloud Email Security Gateway 接收的事件。
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Barracuda Web Security Gateway	[OOTB] Barracuda Web Security Gateway syslog	Syslog	用于处理通过 Syslog 从 Barracuda Web Security Gateway 15.0 接收的部分事件。
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
BeyondTrust's BeyondInsight	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	Syslog	用于处理通过 syslog 接收的 DDOS Mitigator 保护系统事件。
Bloombase StoreSafe	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
BMC CorreLog	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Bricata ProAccel	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Brinqa Risk Analytics	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	用于处理来自 Symantec Endpoint Protection 系统的事件。
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Brocade Fabric OS	[OOTB] Brocade Fabric OS syslog	Syslog	用于处理通过 Syslog 接收的 Brocade Fabric 9.1 的事件。
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	用于处理通过 Syslog 从 Canonical LXD 5.18 系统接收的事件。
Checkpoint	[OOTB] Checkpoint syslog	Syslog	[OOTB] Checkpoint syslog — 用于处理通过 Syslog 协议从 Checkpoint R81 防火墙接收的事件。
Cisco® Access Control Server (ACS)	[OOTB] Cisco ACS syslog	regexp	用于处理通过 Syslog 接收的 Cisco Access Control Server (ACS) 系统事件。
Cisco ASA	[OOTB] Cisco ASA and IOS® syslog	Syslog	用于处理通过 Syslog 接收的 Cisco ASA 和 Cisco IOS 设备的特定事件。
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	用于处理 Cisco Email Security Appliance (WSA) 代理服务器的事件日志（access.log 文件）。

系统名称	规范化器名称	类型	规范化器描述
Cisco ESA syslog	[OOTB] Cisco ESA syslog	Syslog	用于处理通过 syslog 从 Alcatel 网络交换机接收的某些类型的事件。
Cisco Firepower Threat Defense	[OOTB] Cisco ASA 和 IOS Syslog	Syslog	用于处理网络设备事件：通过 Syslog 接收的来自 Cisco ASA、Cisco IOS、Cisco Firepower Threat Defense（版本 7.2）的事件。
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	用于处理通过 syslog 接收的 Cisco Identity Services Engine (ISE) 系统事件。
Cisco IOS	[OOTB] Cisco ASA 和 IOS Syslog	Syslog	用于处理通过 Syslog 接收的 Cisco ASA 和 Cisco IOS 设备的特定事件。
Cisco Netflow v5	[OOTB] NetFlow v5	netflow5	用于处理来自 Cisco Netflow 版本 5 的事件。
Cisco NetFlow v9	[OOTB] NetFlow v9	netflow9	用于处理来自 Cisco Netflow 版本 9 的事件。
Cisco Prime	[OOTB] Cisco Prime syslog	Syslog	用于处理通过 syslog 接收的 Cisco Prime 系统版本 3.10 的事件。
Cisco Secure Email Gateway (SEG)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Cisco Secure Firewall Management Center	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Cisco Unified Communications Manager	[OOTB] Cisco Unified Communications Manager	regexp	用于处理 Cisco Unified Communications Manager 11.5.1 中的事件类型。
Cisco WLC	[OOTB] Cisco WLC syslog	regexp	该规范化器用于处理通过 Syslog 接收到的来自 Cisco WLC 网络设备（2500 系列无线控制器、5500 系列无线控制器、8500 系列无线控制器、Flex 7500 系列无线控制器）的特定类型事件。
Cisco WSA	[OOTB] Cisco WSA 文件, [OOTB] Cisco WSA syslog	regexp	[OOTB] Cisco WSA 文件。此规范化器用于处理 Cisco WSA 代理服务器（版本 14.2、15.0）的事件日志。该规范化器支持使用以下模板生成的处理事件：%t %e %a %w/%h %s %2r %A %H/%d %c %D %Xr %? BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%. %) %q %k %u %m [OOTB] Cisco WSA syslog.该规范化器用于处理通过 Syslog 从 Cisco WSA 系统（版本 15.0）接收的事件。
Citrix NetScaler®	[OOTB] Citrix NetScaler syslog	regexp	用于处理从 Citrix NetScaler 13.7 负载均衡器和 Citrix ADC NS13.0 接收的事件。
Claroty Continuous Threat Detection	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
CloudPassage Halo	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Codemaster Mirada	[OOTB] Codemaster Mirada syslog	Syslog	用于处理通过 syslog 接收的 Codemaster Mirada 系统事件。
CollabNet Subversion Edge	[OOTB] CollabNet Subversion Edge syslog	Syslog	用于处理通过 syslog 从 Subversion Edge（版本 6.0.2）系统接收的事件。
CommuniGate Pro	[OOTB] CommuniGate Pro	regexp	用于处理 KUMA 代理通过 TCP 发送的 CommuniGate Pro 6.1 系统的事件。
Corvil Network Analytics	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Cribl Stream	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
CrowdStrike Falcon Host	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。

系统名称	规范化器名称	类型	规范化器描述
CyberArk Privileged Threat Analytics (PTA)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
CyberPeak Spektr	[OOTB] CyberPeak Spektr syslog	Syslog	用于处理通过 syslog 接收的 CyberPeak Spektr 系统版本 3 的事件。
Cyberprotect Cyber Backup	[OOTB] Cyberprotect Cyber Backup SQL [OOTB] Cyberprotect Cyber Backup syslog	sql、regexp	[OOTB] Cyberprotect Cyber Backup SQL 是一个规范化器，用于处理连接器从 Cyber Backup 系统（版本 16.5）数据库接收的事件。 [OOTB] Cyberprotect Cyber Backup syslog 是一个规范化器，用于处理通过 Syslog 以 CEF 格式从 Cyber Backup 系统（版本 17.2、17.3、18.5）接收的事件。此软件包适用于 KUMA 3.2 或更高版本。
DeepInstinct	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Delinea Secret Server	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Dell Network Switch	[OOTB] Dell Network Switch syslog	regexp	用于处理通过 syslog 从 Dell 网络交换机接收的某些类型的事件。
Digital Guardian Endpoint Threat Detection	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
BIND DNS server	[OOTB] BIND syslog [OOTB] BIND 文件	Syslog regexp	[OOTB] BIND Syslog 用于处理通过 Syslog 接收的 BIND DNS 服务器的事件。[OOTB] BIND 文件用于处理 BIND DNS 服务器的事件日志。
Docsvision	[OOTB] Docsvision syslog	Syslog	用于处理通过 syslog 从 Docsvision 系统接收的审计事件。
Dovecot	[OOTB] Dovecot Syslog	Syslog	用于处理通过 syslog 接收的 Dovecot 邮件服务器事件。事件源为 POP3/IMAP 日志。
Dragos Platform	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Dr.Web Enterprise Security Suite	[OOTB] Syslog-CEF	Syslog	用于处理来自 Dr.Web Enterprise Security Suite 13.0.1 的 CEF 格式的事件。
EclecticIQ Intelligence Center	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Edge Technologies AppBoard and enPortal	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Eltex ESR	[OOTB] Eltex ESR syslog	Syslog	用于处理通过 syslog 从 Eltex ESR 网络设备接收的部分事件。
Eltex MES	[OOTB] Eltex MES syslog	regexp	用于处理通过 syslog 从 Eltex MES 网络设备接收的事件（支持的设备型号：MES14xx、MES24xx、MES3708P）。
ESET Protect	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Extreme Networks Summit Wireless Controller	[OOTB] Extreme Networks Summit Wireless Controller	regexp	该规范化器用于处理来自 Extreme Networks Summit 无线控制器（型号：WM3700，固件版本：5.5.5.0-018R）的特定审计事件。
Factor-TS Dionis NX	[OOTB] Factor-TS Dionis NX syslog	regexp	用于处理通过 syslog 从 Dionis-NX 系统（版本 2.0.3）接收的某些审计事件。
F5™ 高级 Web 应用程序防火墙	[OOTB] F5 Advanced Web Application Firewall syslog	regexp	用于处理通过 syslog 从 F5 高级 Web 应用程序防火墙系统接收的审计事件。
F5 BigIP Advanced Firewall Manager (AFM)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。

系统名称	规范化器名称	类型	规范化器描述
FFRI FFR yarai	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
FireEye CM Series	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
FireEye Malware Protection System	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Forcepoint NGFW	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Forcepoint SMC	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Fortinet FortiAnalyzer	[OOTB] Syslog-CEF	Syslog	用于处理通过 syslog 从 Fortinet FortiAnalyzer 7.0、7.2 接收的 CEF 格式事件。
Fortinet FortiADC	[OOTB] FortiADC syslog KV	regexp	用于处理通过 Syslog 从 Fortinet FortiADC 7.1 负载均衡器接收的键值格式事件。
Fortinet FortiGate®	[OOTB] Syslog-CEF	regexp	用于处理通过 Syslog 从 Fortinet FortiGate 7.0、7.2 接收的 CEF 格式事件。
Fortinet FortiGate	[OOTB] FortiGate syslog KV	Syslog	用于处理通过 Syslog 从 FortiGate 防火墙（版本 7.0）接收的事件。事件源为键值对格式的 FortiGate 日志。
Fortinet Fortimail	[OOTB] Fortimail	regexp	用于处理 FortiMail 电子邮件保护系统的事件。事件源为 FortiMail 邮件系统日志。
Fortinet FortiSOAR	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Fortinet FortiWeb	[OOTB] Syslog-CEF	Syslog	用于处理来自 Fortinet FortiWeb 7.6.1 系统的 CEF 格式事件。
FreeBSD™	[OOTB] FreeBSD 文件	regexp	用于处理存储在文件中的 FreeBSD 操作系统（版本 13.1-RELEASE）事件。 该规范化器可以处理由 praudit 实用程序生成的文件。 例如： praudit -xl /var/audit/AUDITFILE >> file_name.log
FreeIPA	[OOTB] FreeIPA	json	用于处理来自 FreeIPA 系统的事件。事件源为 Free IPA 目录服务日志。
FreeRADIUS	[OOTB] FreeRADIUS syslog	Syslog	用于处理通过 syslog 接收的 FreeRADIUS 系统事件。此规范化器支持 FreeRADIUS 3.0 版本的事件。
GajShield Firewall	[OOTB] GajShield Firewall syslog	regexp	用于处理通过 syslog 从 GAJ_OS_Bulwark_Firmware_v4.35 版本的 GajShield 防火墙接收的部分事件。
Garda Monitor	[OOTB] Garda Monitor syslog	Syslog	用于处理通过 syslog 从 3.4 版本的 Garda Monitor 系统接收的事件。
Gardatech GardaDB	[OOTB] Gardatech GardaDB syslog	Syslog	用于处理通过 syslog 从 5.3、5.4 版本的 Gardatech Perimeter 系统接收的事件。
Gardatech Perimeter	[OOTB] Gardatech Perimeter syslog	Syslog	用于处理通过 syslog 从 5.3 版本的 Gardatech Perimeter 系统接收的事件。
Gigamon GigaVUE	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
HAProxy	[OOTB] HAProxy syslog	Syslog	用于处理 HAProxy 系统的日志。该规范化器支持处理来自 HAProxy 版本 2.8 的 HTTP 日志、TCP 日志和错误日志类型的事件。
HashiCorp Vault	[OOTB] HashiCorp Vault json	json	用于处理从 HashiCorp Vault 系统 1.16 版本接收的 JSON 格式事件。该规范化器包可在 KUMA 3.0 及更高版本中使用。
Huawei Eudemon	[OOTB] Huawei Eudemon	regexp	用于处理来自 Huawei Eudemon 防火墙的事件。事件源为 Huawei Eudemon 防火墙的日志。
Huawei iManager 2000	[OOTB] Huawei iManager 2000 文件	regexp	该规范化器支持处理 Huawei iManager 2000 系统的部分事件，这些事件存储在 \client\logs\rpc、\client\logs\deploy\ossDeployment 文件中。
Huawei USG	[OOTB] Huawei USG Basic	Syslog	专用于处理通过 syslog 从 Huawei USG 安全网关接收的事件。

系统名称	规范化器名称	类型	规范化器描述
Huawei VRP	[OOTB] Huawei VRP syslog	regexp	专用于处理通过 syslog 接收的某些类型的 Huawei VRP 系统事件。该规范化器对事件数据进行部分提取。该规范化器可在 KUMA 3.0 及更高版本中使用。
IBM InfoSphere Guardium	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Ideco UTM	[OOTB] Ideco UTM Syslog	Syslog	用于处理通过 syslog 从 Ideco UTM 接收的事件。此规范化程序支持来自 Ideco UTM 14.7、14.10 和 17.5 的事件。
Illumio Policy Compute Engine (PCE)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Imperva Incapsula	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Imperva SecureSphere	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Indeed Access Manager	[OOTB] Indeed Access Manager syslog	Syslog	用于处理通过 syslog 从 Indeed Access Manager 系统接收的事件。
Indeed PAM	[OOTB] Indeed PAM syslog	Syslog	用于处理来自 Indeed PAM（特权访问管理器）2.6 版本的事件。
Indeed SSO	[OOTB] Indeed SSO xml	xml	用于处理来自 Indeed SSO（单点登录）系统的事件。该规范化器支持在 KUMA 2.1.3 及更高版本中使用。
InfoWatch Person Monitor	[OOTB] InfoWatch Person Monitor SQL	sql	用于处理来自 InfoWatch Person Monitor 10.2 版本 MS SQL 数据库的系统审计事件。
InfoWatch Traffic Monitor	[OOTB] InfoWatch Traffic Monitor SQL	sql	用于处理连接器从 InfoWatch Traffic Monitor 系统数据库接收的事件。
Intralinks VIA	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
IPFIX	[OOTB] IPFIX	ipfix	用于处理 IP 流信息导出 (IPFIX) 格式的事件。
Juniper JUNOS™	[OOTB] Juniper - JUNOS	regexp	用于处理从 Juniper 网络设备接收的审计事件。
Kaspersky Anti Targeted Attack (KATA)	[OOTB] KATA	cef	用于处理来自 Kaspersky Anti Targeted Attack 活动日志的警报或事件。
Kaspersky CyberTrace	[OOTB] CyberTrace	regexp	用于处理 Kaspersky CyberTrace 事件。
Kaspersky Endpoint Detection and Response (KEDR)	[OOTB] KEDR 遥测数据	JSON	用于处理经 KATA 标记的 Kaspersky EDR 遥测数据。事件源为 kafka、EnrichedEventTopic。
Kaspersky Endpoint Security for Linux	[OOTB] KESL syslog cef [OOTB] KESL json	Syslog、JSON	[OOTB] KESL syslog cef 规范化器用于处理通过 syslog 接收的来自 Kaspersky Endpoint Security for Linux (KESL) 12.2 的 CEF 格式事件。 [OOTB] KESL json 规范化器用于处理来自 Kaspersky Endpoint Security for Linux (KESL) 12.5 的 JSON 格式事件。
KICS/KATA	[OOTB] KICS4Net v2.x	CEF	用于处理 KICS/KATA 版本 2.x 的事件。
KICS/KATA	[OOTB] KICS4Net v3.x	Syslog	用于处理 KICS/KATA 版本 3.x 的事件。
KICS/KATA 4.2	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog	Syslog	用于处理通过 syslog 从 KICS/KATA 4.2 系统接收的事件。
Kaspersky KISG	[OOTB] Kaspersky KISG syslog	Syslog	用于处理通过 syslog 从 Kaspersky IoT Secure Gateway (KISG) 3.0 接收的事件。
Kaspersky NGFW	[OOTB] Kaspersky NGFW CEF	cef	用于处理从 Kaspersky NGFW 系统 1.0、1.2 版本接收的 CEF 格式事件。

系统名称	规范化器名称	类型	规范化器描述
Open Single Management Platform	[OOTB] KSC	CEF	用于处理以 CEF 格式接收的来自 Open Single Management Platform 的事件。
Open Single Management Platform	[OOTB] KSC from SQL	sql	用于处理连接器从 Open Single Management Platform 系统数据库接收的事件。
Kaspersky Security for Linux Mail Server	[OOTB] KLMS Syslog CEF	Syslog	用于处理通过 syslog 从 Kaspersky Security for Linux Mail Server 接收的 CEF 格式事件。
Kaspersky Security for MS Exchange SQL	[OOTB] Kaspersky Security for MS Exchange SQL	sql	该规范化器用于处理存储在数据库中的 Kaspersky Security for Exchange (KSE) 9.0 事件。
Kaspersky Secure Mail Gateway	[OOTB] KSMG Syslog CEF	Syslog	用于处理通过 Syslog 从 Kaspersky Secure Mail Gateway 2.0 版本接收的 CEF 格式事件。
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS Syslog CEF	Syslog	用于处理通过 Syslog 从 Kaspersky Web Traffic Security 接收的 CEF 格式事件。
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS (KV)	Syslog	用于处理 Kaspersky Web Traffic Security 键值对格式事件。
Kemptechnologies LoadMaster	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Kerio Control	[OOTB] Kerio Control	Syslog	用于处理 Kerio Control 防火墙的事件。
KUMA	[OOTB] KUMA forwarding	JSON	用于处理从 KUMA 转发的事件。
LastLine Enterprise	[OOTB] LastLine Enterprise syslog cef	Syslog	用于处理通过 syslog 以 CEF 格式从 LastLine Enterprise 7.3、8.1、9.1 接收的事件。
Libvirt	[OOTB] Libvirt syslog	Syslog	用于处理通过 syslog 接收的 Libvirt 8.0.0 版事件。
Lieberman Software ERPM	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Linux	[OOTB] Linux audit and iptables Syslog v1	Syslog	用于处理 Linux 操作系统的事件。此规范化器不支持处理 ENRICHED 格式的事件。
Linux auditd	[OOTB] Linux auditd syslog for KUMA 3.2	Syslog	用于处理通过 syslog 接收的 Linux 操作系统审计事件（auditd 包）。该规范化器支持处理由 KUMA 收集器版本 3.2 或更高版本处理过的事件。
Linux auditd	[OOTB] Linux auditd file for KUMA 3.2	regexp	用于处理保存到文件的 Linux 操作系统审计事件（auditd 包）。该规范化器支持处理由 KUMA 收集器版本 3.2 或更高版本处理过的事件。
MariaDB	[OOTB] MariaDB 审计插件 Syslog	Syslog	用于处理通过 syslog 从 MariaDB 审计插件接收的事件。
McAfee Endpoint DLP	[OOTB] McAfee Endpoint DLP syslog	Syslog	用于处理通过 Syslog 从 McAfee Endpoint DLP Windows 11.10.200 接收的事件。
Microsoft 365 (Office 365)	[OOTB] Microsoft Office 365 json	JSON	该规范化器用于处理 Microsoft 365 事件。
Active Directory 联合身份验证服务 (AD FS) 设置:	[OOTB] Microsoft Products for KUMA 3	xml	用于处理 Microsoft AD FS 事件。[OOTB] Microsoft Products for KUMA 3 规范化器在 KUMA 3.0.1 及更高版本中支持此事件源。
Microsoft Active Directory Domain Service (AD DS)	[OOTB] Microsoft Products for KUMA 3	xml	用于处理 Microsoft AD DS 事件。[OOTB] Microsoft Products for KUMA 3 规范化器在 KUMA 3.0.1 及更高版本中支持此事件源。

系统名称	规范化器名称	类型	规范化器描述
Microsoft Defender	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理 Microsoft Defender 事件。
Microsoft DHCP	[OOTB] MS DHCP 文件	regexp	用于处理 Microsoft DHCP 服务器事件。事件源为 Windows DHCP 服务器日志。
Microsoft DNS	[OOTB] DNS Windows	regexp	用于处理 Microsoft DNS 服务器事件。事件源为 Windows DNS 服务器日志。该规范化器不支持在启用"**详细信息**"选项的情况下处理调试日志事件。
Microsoft Exchange	[OOTB] Exchange CSV	csv	用于处理 Microsoft Exchange 系统的事件日志。事件源为 Exchange 服务器 MTA 日志。
Microsoft Hyper-V	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理 Microsoft Windows 事件。 事件源为 Microsoft Hyper-V 日志：Microsoft-Windows-Hyper-V-VMMS-Admin、Microsoft-Windows-Hyper-V-Compute-Operational、Microsoft-Windows-Hyper-V-Hypervisor-Operational、Microsoft-Windows-Hyper-V-StorageVSP-Admin、Microsoft-Windows-Hyper-V-Hypervisor-Admin、Microsoft-Windows-Hyper-V-VMMS-Operational、Microsoft-Windows-Hyper-V-Compute-Admin。
Microsoft IIS 设置	[OOTB] IIS Log File Format	regexp	该规范化器按照 https://learn.microsoft.com/en-us/windows/win32/http/iis-logging 中描述的格式处理事件。事件源为 Microsoft IIS 日志。
Microsoft Network Policy Server (NPS)	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	该规范化器用于处理 Microsoft Windows 操作系统的事件。事件源为网络策略服务器事件。
Microsoft SCCM	[OOTB] Microsoft SCCM 文件	regexp	该规范化器用于处理 Microsoft SCCM 系统版本 2309 的事件。该规范化器支持处理存储在 AdminService.log 文件中的部分事件。
Microsoft SharePoint® Server	[OOTB] Microsoft SharePoint Server 诊断日志文件	regexp	该规范化器支持处理诊断日志中存储的部分 Microsoft SharePoint Server 2016 事件。
Microsoft Sysmon	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	该规范化器用于处理 Microsoft Sysmon 模块事件。
Microsoft Windows 7, 8.1, 10, 11	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理来自 Microsoft Windows 操作系统的安全、系统、应用程序日志的部分事件。[OOTB] Microsoft 产品事件规范化器（经 KES WIN 转发的事件），支持处理 Kaspersky Endpoint Security 12.6 for Windows 经 Syslog 发送到 KUMA 的部分审计事件类型。
Microsoft-Windows-PowerShell™	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理 Microsoft Windows PowerShell 日志事件。
Microsoft-Windows-PowerShell-Operational	[OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理 Microsoft Windows PowerShell-Operational 日志事件。[OOTB] Microsoft 产品事件规范化器（经 KES WIN 转发的事件），支持处理 Kaspersky Endpoint Security 12.6 for Windows 经 Syslog 发送到 KUMA 的部分审计事件类型。

系统名称	规范化器名称	类型	规范化器描述
Microsoft → Windows → 系统日志 → Netlogon	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	用于处理 XML 格式的 Microsoft → Windows → 系统日志 → Netlogon 日志事件。
Microsoft → Windows → TaskScheduler → 操作	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	用于处理 XML 格式的 Microsoft → Windows → TaskScheduler → 操作日志事件。
Microsoft → Windows → WinRM → 操作	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	用于处理 XML 格式的 Microsoft → Windows → WinRM → 操作日志事件。
Microsoft SQL Server	[Deprecated] [OOTB] Microsoft SQL Server xml	xml	用于处理 MS SQL Server 版本 2008、2012、2014、2016 的事件。该规范化器支持在 KUMA 2.1.3 及更高版本中使用。
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理 Microsoft Windows 事件。事件源为位于"应用程序和服务日志 - Microsoft - Windows - TerminalServices-LocalSessionManager - Operational"中的日志。[OOTB] Microsoft 产品事件规范化器（经 KES WIN 转发的事件），支持处理 Kaspersky Endpoint Security 12.6 for Windows 经 Syslog 发送到 KUMA 的部分审计事件类型。
Microsoft Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	用于处理来自 Microsoft Windows Server 操作系统的安全、系统日志的部分事件。[OOTB] Microsoft 产品事件规范化器（经 KES WIN 转发的事件），支持处理 Kaspersky Endpoint Security 12.6 for Windows 经 Syslog 发送到 KUMA 的部分审计事件类型。
Microsoft Windows 8	[OOTB] SNMP.Windows {XP/2003}	JSON	用于处理通过 SNMP 协议从运行 Microsoft Windows XP、Microsoft Windows 2003 操作系统的工作站和服务器接收的事件。
Microsoft WSUS	[OOTB] Microsoft WSUS 文件	regexp	用于处理通过 syslog 从 5.3、5.4 版本的 Gardatech Perimeter 系统接收的事件。
MikroTik	[OOTB] MikroTik syslog	regexp	用于处理通过 syslog 从 MikroTik 设备接收的事件。
Minerva Labs Minerva EDR	[OOTB] Minerva EDR	regexp	用于处理来自 Minerva EDR 系统的事件。
MongoDb	[OOTB] MongoDb syslog	Syslog	用于处理通过 syslog 从 MongoDB 7.0 数据库接收的部分事件。
Multifactor Radius Server for Windows	[OOTB] Multifactor Radius Server for Windows syslog	Syslog	用于处理通过 Syslog 从适用于 Microsoft Windows 的 Multifactor Radius Server 1.0.2 接收的事件。

系统名称	规范化器名称	类型	规范化器描述
Aurora MySQL 5.7	[OOTB] MariaDB Audit Plugin Syslog	Syslog	用于处理 MariaDB 审计插件通过 Syslog 发送的事件。
NetApp ONTAP (AFF, FAM)	[OOTB] NetApp syslog, [OOTB] NetApp 文件	regexp	[OOTB] NetApp syslog — 用于处理通过 Syslog 接收的 NetApp 系统（版本 — ONTAP 9.12）的事件。 [OOTB] NetApp 文件 — 用于处理存储在文件中的 NetApp 系统（版本 — ONTAP 9.12）的事件。
NetApp SnapCenter	[OOTB] NetApp SnapCenter 文件	regexp	用于处理 NetApp SnapCenter 系统（SnapCenter Server 5.0）的部分事件。此规范化器支持处理来自 C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\napManagerWeb.*.log 文件的某些事件。SnapManagerWeb.*.log 文件中支持的 xml 格式的事件类型：SmDiscoverPluginRequest、SmDiscoverPluginResponse、SmGetDomainsResponse、SmGetHostPluginStatusRequest、SmGetHostPluginStatusResponse、SmGetHostRequest、SmGetHostResponse、SmRequest。该规范化器支持处理来自 C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\audit.log 文件的某些事件。
NetIQ Identity Manager	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
NetScout Systems nGenius Performance Manager	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Netskope Cloud Access Security Broker	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Netwrix Auditor	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Nextcloud	[OOTB] Nextcloud syslog	Syslog	专为处理通过 syslog 接收的 Nextcloud 26.0.4 版本事件而设计。该规范化器不会保存来自 Trace 字段的信息。
Nexthink Engine	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Nginx	[OOTB] nginx 正则表达式	regexp	用于处理 Nginx Web 服务器日志事件。
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
One Identity Privileged Session Management	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
OpenLDAP	[OOTB] OpenLDAP	regexp	用于逐行处理 auditlog.ldif 文件中 OpenLDAP 2.5 系统的某些事件。
Open VPN®	[OOTB] OpenVPN 文件	regexp	用于处理 OpenVPN 系统的事件日志。
Oracle	[OOTB] Oracle Audit Trail	sql	用于处理连接器直接从 Oracle 数据库接收的数据库审计事件。
OrionSoft Termit	[OOTB] OrionSoft Termit syslog	Syslog	用于处理通过 Syslog 从 OrionSoft Termit 2.2、2.3、2.4 系统接收的事件。
Orion soft zVirt	[OOTB] Orion Soft zVirt syslog	regexp	用于处理 Orion soft zVirt 3.1 虚拟化系统的事件。
PagerDuty	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Palo Alto Networks NGFW	[OOTB] PA-NGFW (Syslog-CSV)	Syslog	用于处理通过 Syslog 以 CSV 格式接收的来自 Palo Alto Networks 防火墙的事件。
Palo Alto Networks PANOS	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Parsec ParsecNET	[OOTB] Parsec ParsecNET	sql	用于处理连接器从 Parsec ParsecNET 3 系统数据库接收的事件。

系统名称	规范化器名称	类型	规范化器描述
Passwork	[OOTB] Passwork syslog	Syslog	用于处理通过 Syslog 从 Passwork 版本 050219 系统接收的事件。
Penta Security WAPPLES	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Positive Technologies ISIM	[OOTB] PTsecurity ISIM	regexp	用于处理来自 PT Industrial Security Incident Manager 系统的事件。
Positive Technologies Network Attack Discovery (NAD)	[OOTB] PT NAD json	JSON	用于处理来自 PT NAD 的 json 格式的事件。此规范化器支持处理来自 PT NAD 版本 11.1、11.0 的事件。
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	用于处理 PT Sandbox 系统的事件。
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF	Syslog	用于处理来自 PTsecurity（Web 应用程序防火墙）系统的事件。
Postfix	[OOTB] Postfix syslog	regexp	The [OOTB] Postfix package contains a resource set for processing Postfix 3.6 events. 支持处理通过 TCP 接收的 syslog 事件。该软件包适用于 KUMA 3.0 及更高版本。
PostgreSQL pgAudit	[OOTB] PostgreSQL pgAudit Syslog	Syslog	用于处理 PostgreSQL 数据库 pgAudit 审计插件的事件，这些事件通过 syslog 接收。
PowerDNS	[OOTB] PowerDNS syslog	Syslog	用于处理通过 syslog 接收的 PowerDNS Authoritative Server 4.5 事件。
Proftpd	[OOTB] Proftpd syslog	regexp	用于处理通过 Syslog 从 Proftpd 1.3.8c 接收的事件。
Proofpoint® 内部威胁管理	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Proxmox	[OOTB] Proxmox 文件	regexp	用于处理存储在文件中的 Proxmox 系统版本 7.2-3 的事件。该规范化器支持处理访问和 pveam 日志中的事件。
PT NAD	[OOTB] PT NAD json	JSON	用于处理来自 PT NAD 的 json 格式的事件。此规范化器支持处理来自 PT NAD 版本 11.1、11.0 的事件。
QEMU - hypervisor logs	[OOTB] QEMU - Hypervisor 文件	regexp	用于处理存储在文件中的 QEMU hypervisor 的事件。支持 QEMU 6.2.0 和 Libvirt 8.0.0。
QEMU - virtual machine logs	[OOTB] QEMU - Virtual Machine 文件	regexp	用于处理存储在文件中的 QEMU hypervisor 版本 6.2.0 的虚拟机日志事件。
Radware DefensePro AntiDDoS	[OOTB] Radware DefensePro AntiDDoS	Syslog	用于处理通过 Syslog 接收的来自 DDOS Mitigator 保护系统的事件。
Reak Soft Blitz Identity Provider	[OOTB] Reak Soft Blitz Identity Provider 文件	regexp	用于处理存储在文件中的 Reak Soft Blitz Identity Provider 系统版本 5.16 的事件。
RedCheck Desktop	[OOTB] RedCheck Desktop 文件	regexp	用于处理存储在文件中的 RedCheck Desktop 2.6 系统的日志。
RedCheck WEB	[OOTB] RedCheck WEB 文件	regexp	用于处理存储在文件中的 RedCheck Web 2.6 系统的日志。
RED SOFT RED ADM	[OOTB] RED SOFT RED ADM syslog	regexp	用于处理通过 syslog 从 RED ADM 系统（RED ADM：工业版 1.1）接收的事件。 该规范化器支持处理： - 管理子系统事件 - 控制器事件
ReversingLabs N1000 Appliance	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Rubicon Communications pfSense	[OOTB] pfSense Syslog	Syslog	用于处理通过 Syslog 接收的来自 pfSense 防火墙的事件。

系统名称	规范化器名称	类型	规范化器描述
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	用于处理来自 pfSense 防火墙的事件。这些事件的 Syslog 标头不包含主机名。
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
SecurityCode Continent 4	[OOTB] SecurityCode Continent 4 syslog	regexp	用于处理通过 syslog 接收的 SecurityCode Continent 系统版本 4 的事件。
Sendmail	[OOTB] Sendmail syslog	Syslog	用于处理通过 syslog 接收的 Sendmail 版本 8.15.2 的事件。
SentinelOne	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Skype™ for Business	[OOTB] Microsoft Products for KUMA 3	xml	用于处理来自 Skype for Business 系统日志和 Lync Server 日志的某些事件。
Snort	[OOTB] Snort 3 json 文件	JSON	用于处理 JSON 格式的 Snort 版本 3 的事件。
Sophos Central	[OOTB] Sophos Central syslog	Syslog	用于处理通过 Sophos-Central-SIEM-Integration 脚本，以 CEF 格式经由 syslog 从 Sophos Central 1.2 接收的部分事件。
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall	Syslog	用于处理通过 Syslog 从 SonicWall TZ 防火墙接收的事件。
Solar WebProxy	[OOTB] Solar WebProxy syslog	regexp	用于处理通过 Syslog 以 siem-log 格式从 Solar WebProxy 4.2 接收的事件。
SolarWinds DameWare® MRC	[OOTB] SolarWinds DameWare MRC xml	xml	该规范化器支持处理存储在 Windows 应用程序日志中的某些 DameWare Mini Remote Control (MRC) 7.5 事件。该规范化器处理由 dwmrcs 提供程序生成的事件。
Sophos Firewall	[OOTB] Sophos Firewall syslog	regexp	用于处理通过 syslog 从 Sophos Firewall 20 接收的事件。
Sophos XG	[OOTB] Sophos XG	regexp	用于处理来自 Sophos XG 防火墙的事件。
Squid	[OOTB] Squid access Syslog	Syslog	用于处理通过 syslog 协议接收的 Squid 代理服务器事件。
Squid	[OOTB] Squid access.log 文件	regexp	用于处理来自 Squid 代理服务器的 Squid 日志事件。事件源为 access.log 日志。
Staffcop Enterprise	[OOTB] Staffcop Enterprise syslog CEF	regexp	用于处理通过 syslog 从 Staffcop Enterprise 5.4、5.5 接收的 CEF 格式事件。
S-Terra VPN Gate	[OOTB] S-Terra	Syslog	用于处理来自 S-Terra VPN Gate 设备的事件。
Stormshield 防火墙	[OOTB] Stormshield 防火墙 syslog	Syslog	用于处理通过 Syslog 接收的来自 Stormshield 防火墙 4.8 和 5.0 的密钥-值格式事件。
Suricata	[OOTB] Suricata json 文件	JSON	此软件包中包含一个规范化器，用于处理存储在 JSON 文件中的 Suricata 7.0.1 事件。 该规范化器支持处理以下事件类型：flow、anomaly、alert、dns、http、ssl、tls、ftp、ftp_data、smb、rdp、pgsql、modbus、quic、dhcp、bittorrent_dht、rfb。
ThreatConnect Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
ThreatQuotient	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Tionix Cloud Platform	[OOTB] Tionix Cloud Platform syslog	Syslog	用于处理通过 syslog 接收的 Tionix Cloud Platform 系统 2.9 版本的事件。该规范化器对事件数据进行部分提取。该规范化器可在 KUMA 3.0 及更高版本中使用。
Tionix VDI	[OOTB] Tionix VDI 文件	regexp	该规范化器支持处理存储在 tionix_lntmov.log 文件中的 Tionix VDI 系统（2.8 版本）的部分事件。

系统名称	规范化器名称	类型	规范化器描述
TrapX DeceptionGrid	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Trend Micro™ Control Manager	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Trend Micro Deep Security	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Trend Micro NGFW	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Unbound	[OOTB] Unbound Syslog	Syslog	用于处理通过 syslog 接收的来自 Unbound DNS 服务器的事件。
UserGate	[OOTB] Syslog-CEF	Syslog	专为处理通过 syslog 从 UserGate 系统接收的 CEF 格式事件而设计。
Varonis DatAdvantage	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Veriato 360	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
ViPNet TIAS	[OOTB] ViPNet TIAS syslog	Syslog	用于处理通过 Syslog 接收的 ViPNet TIAS 3.8 的事件。
VMware ESXi	[OOTB] VMware ESXi syslog	regexp	用于处理通过 syslog 接收的 VMware ESXi 事件（支持的事件仅限于 ESXi 5.5、6.0、6.5 和 7.0 版本中的部分事件）。
VMWare Horizon	[OOTB] VMware Horizon - Syslog	Syslog	用于处理通过 syslog 从 VMware Horizon 2106 系统接收的事件。
VMwareCarbon Black EDR	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Vmware vCenter	[OOTB] VMware vCenter API	xml	用于处理通过 API 接收的 VMware vCenter 7 的事件。
Vormetric Data Security Manager	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Votiro Disarmer for Windows	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Vsftpd	[OOTB] Vsftpd syslog	regexp	用于处理通过 Syslog 从 Vsftpd 3.0.5 接收的事件。
Wallix AdminBastion	[OOTB] Wallix AdminBastion syslog	regexp	用于处理通过 syslog 从 Wallix AdminBastion 系统接收的事件。
WatchGuard - Firebox	[OOTB] WatchGuard Firebox	Syslog	用于处理通过 Syslog 接收的 WatchGuard Firebox 事件。
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Winchill Fracas	[OOTB] PTC Winchill Fracas	regexp	用于处理 Windchill FRACAS 故障登记系统的事件。
Yandex Browser corporate	[OOTB] Yandex Browser	JSON	用于处理从 Yandex Browser 23 或 24.4 企业版接收的事件。
Yandex Cloud	[OOTB] Yandex Cloud	regexp	用于处理部分 Yandex Cloud 审计事件。该规范化器支持处理配置级别的审计日志事件：IAM（Yandex 身份和访问管理）、Compute（Yandex 计算云）、Network（Yandex 虚拟私有云）、Storage（Yandex 对象存储）、Resourcemanager（Yandex 资源管理器）。
Zabbix	[OOTB] Zabbix SQL	sql	用于处理 Zabbix 6.4 的事件。
Zecurion DLP	[OOTB] Zecurion DLP syslog	regexp	用于处理通过 Syslog 接收的 Zecurion DLP 系统版本 12.0 的事件。

系统名称	规范化器名称	类型	规范化器描述
ZEEK IDS	[OOTB] ZEEK IDS json 文件	JSON	用于处理 JSON 格式的 ZEEK IDS 系统日志。该规范化器支持处理来自 ZEEK IDS 1.8 及以上版本的事件。
Zettaset BDEncrypt	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
Zscaler Nanolog Streaming Service (NSS)	[OOTB] Syslog-CEF	Syslog	用于处理 CEF 格式的事件。
IT-Bastion – SKDPU	[OOTB] Syslog-CEF	Syslog	用于处理通过 Syslog 从 IT-Bastion SKDPU 系统接收的 CEF 格式的事件。
A-Real Internet Control Server (ICS)	[OOTB] A-real IKS syslog	regexp	用于处理通过 syslog 接收的 A-Real Internet Control Server (ICS) 系统事件。该规范化器支持处理来自 A-Real ICS 7.0 及更高版本的事件。
Biznes Resheniya Compass	[OOTB] Biznes Resheniya Compass	regexp	用于处理通过 Kafka 接收的 Biznes Resheniya Compass 6.7.7 和 6.7.8 审计事件。
Apache web server	[OOTB] Apache HTTP Server 文件	regexp	用于处理存储在文件中的 Apache HTTP Server 2.4 的事件。该规范化器支持处理来自“应用程序”日志的“通用”或“合并日志”格式的事件，以及来自“错误”日志的事件。 错误日志事件的预期格式： `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Apache web server	[OOTB] Apache HTTP Server syslog	Syslog	用于处理通过 syslog 接收的 Apache HTTP Server 事件。该规范化器支持处理来自“访问”日志（“通用”或“合并日志”格式）以及“错误”日志的 Apache HTTP Server 2.4 事件。 错误日志事件的预期格式： `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Lighttpd web server	[OOTB] Lighttpd syslog	Syslog	用于处理通过 syslog 接收的 Lighttpd 系统访问事件。该规范化器支持处理 Lighttpd 1.4 版本的事件。 “访问”日志事件的预期格式： `$remote_addr $http_request_host_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"`
IVK Kolchuga-K	[OOTB] Kolchuga-K Syslog	Syslog	用于处理通过 syslog 接收的 IVK Kolchuga-K 系统（版本 LKNV.466217.002）事件。
InfoTeCS ViPNet IDS	[OOTB] Syslog-CEF	Syslog	用于处理通过 syslog 从 infotecs ViPNet IDS 系统接收的 CEF 格式事件。
InfoTeCS ViPNet Coordinator	[OOTB] VipNet Coordinator Syslog	Syslog	用于处理通过 syslog 接收的 ViPNet Coordinator 系统事件。
Kod Bezopasnosti —Continent	[OOTB][regexp] Continent IPS/IDS & TLS	regexp	用于处理 Continent IPS/IDS 设备日志的事件。
Kod Bezopasnosti —Continent	[OOTB] Continent SQL	sql	用于处理从数据库获取的 Continent 系统的事件。
Kod Bezopasnosti SecretNet 7	[OOTB] SecretNet SQL	sql	用于处理连接器从 SecretNet 系统数据库接收的事件。
Confident – Dallas Lock Unified Control Center	[OOTB] Confident Dallas Lock syslog CEF	regexp	用于处理从 Dallas Lock Unified Control Center 4.0 接收的 CEF 格式的事件。
CryptoPro NGate	[OOTB] Ngate Syslog	Syslog	用于处理通过 Syslog 从 CryptoPro NGate 系统接收的事件。
H3C (Huawei-3Com) routers	[OOTB] H3C Routers syslog	regexp	用于处理通过 Syslog 从 H3C（华为 3Com）SR6600 网络设备（Comware 7 固件）接收的特定类型事件的规范化器。该规范化器支持标准事件格式（符合 RFC 3164 的格式）。
NT Monitoring and Analytics	[OOTB] Syslog-CEF	Syslog	用于处理通过 syslog 从 NT Monitoring and Analytics 系统接收的 CEF 格式事件。

系统名称	规范化器名称	类型	规范化器描述
BlueCoat proxy server	[OOTB] BlueCoat Proxy v0.2	regexp	用于处理 BlueCoat 代理服务器事件。事件源为 BlueCoat 代理服务器事件日志。
SKDPU NT Access Gateway	[OOTB] Bastion SKDPU-GW	Syslog	用于处理通过 Syslog 接收的 SKDPU NT Access 网关系统的事件。
Solar Dozor	[OOTB] Solar Dozor Syslog	Syslog	用于处理通过 Syslog 从 Solar Dozor 7.9 版本系统接收的事件。该规范化器支持处理自定义格式事件，但不支持 CEF 格式事件。
-	[OOTB] Syslog header	Syslog	用于处理通过 Syslog 接收的事件。该规范化器会解析 Syslog 事件的标头，但不会解析事件的消息字段。如有必要，您可以使用其他规范化器来解析消息字段。

连接器

连接器用于在 KUMA 服务之间建立连接，以及主动和被动接收事件。

该程序提供以下连接器类型：

- tcp — 用于通过 TCP 被动接收数据。适用于 Windows 和 Linux 代理。
- udp — 用于通过 UDP 被动接收数据。适用于 Windows 和 Linux 代理。
- netflow — 用于被动接收 NetFlow 格式的事件。
- sflow — 用于被动接收 SFlow 格式的事件。
- nats-jetstream — 用于与 NATS 消息代理进行通讯。适用于 Windows 和 Linux 代理。
- kafka — 用于与 Apache Kafka 数据总线进行通讯。适用于 Windows 和 Linux 代理。
- http — 用于通过 HTTP 接收事件。适用于 Windows 和 Linux 代理。
- sql — 用于从数据库中选择数据。
  该程序支持以下类型的 SQL 数据库：
  - SQLite
  - MSSQL。
  - MySQL。
  - PostgreSQL。
  - Cockroach。
  - Oracle。
  - Firebird。
  - ClickHouse
- file — 用于从文本文件中检索数据。适用于 Linux 代理。
- 1c-log 和 1c-xml 用于从 1C 日志接收数据。适用于 Linux 代理。

- diode — 用于使用数据二极管在工业 ICS 网络中进行单向数据传输。
- ftp — 用于通过文件传输协议接收数据。适用于 Windows 和 Linux 代理。
- sftp — 用于通过安全文件传输协议接收数据。适用于 Windows 和 Linux 代理。
- nfs — 用于通过网络文件系统协议接收数据。适用于 Windows 和 Linux 代理。
- wmi — 用于使用 Windows Management Instrumentation 获取数据。适用于 Windows 代理。
- wec — 用于使用 Windows Event Forwarding (WEF) 或 Windows Event Collector (WEC) 或者 Windows 主机的本地操作系统日志接收数据。适用于 Windows 代理。
- snmp — 用于使用简单网络管理协议接收数据。适用于 Windows 和 Linux 代理。
- snmp-trap — 用于使用简单网络管理协议陷阱（SNMP 陷阱）接收数据。适用于 Windows 和 Linux 代理。
- kata/edr — 用于通过 API 接收 KEDR 数据。
- vmware — 用于通过 API 接收 VMware vCenter 数据。
- elastic — 用于接收 Elasticsearch 数据。
- etw — 用于接收扩展 DNS 服务器日志。
- universalAPI — 用于从任何支持 JSON 响应的 REST API 接收数据。支持按唯一 ID 和迭代模式进行筛选。
- smb — 用于通过 SMB（服务器消息块）协议接收数据。适用于 Linux 代理。
- http-streaming — 用于通过 HTTP 接收流式事件。该连接器分段处理请求正文，从而减少内存使用量。适用于 Windows 和 Linux 代理。

查看连接器设置

要查看连接器设置：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**连接器**”。
2. 在文件夹结构中，选择包含相关连接器的文件夹。
3. 选择要查看其设置的连接器。

连接器的设置显示在两个选项卡上：**基本设置**和**高级设置**。有关每个连接器设置的详细说明，请参阅“*连接器设置*”部分。

添加连接器

您可以为除“**描述**”字段之外的所有条目字段启用非打印字符显示功能。

要添加连接器：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**连接器**”。
2. 在文件夹结构中，选择要放置连接器的文件夹。

   根文件夹与租户相对应。要使连接器可供特定租户使用，必须在该租户的文件夹中创建资源。

   如果文件夹树中不存在所需的文件夹，则需要创建该文件夹。
   默认情况下，添加的连接器会创建在“**共享**”文件夹中。
3. 单击“**添加连接器**”按钮。
4. 请定义所选连接器类型的设置。
   “*连接器设置*”部分提供了您必须为每种类型的连接器指定的设置。
5. 单击“**保存**”按钮。

连接器设置

本部分介绍 KUMA 支持的所有连接器类型的设置。

Tcp 类型

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） — 拥有该资源的租户的名称。
- **类型**（必填）— 连接器类型：**tcp**。
- **URL**（必填）—您需要连接到的 URL。可用格式：hostname:port、IPv4:port、IPv6:port、:port。
- **Auditd** 是一项机制的切换开关，该机制可将从连接器接收的 auditd 日志事件记录合并为单个事件。Auditd 仅支持 \n 分隔符。如果启用切换开关，**分隔符**字段将不可用。如果在代理连接器中启用了“**Auditd**”切换开关，则必须在代理发送事件所至的收集器的连接器中配置 \n 分隔符。
- **分隔符**用于指定表示事件之间分隔符的字符。可用值：`\n`、`\t`、`\0`。如果未指定分隔符（即选择了空值），则默认值为 `\n`。
- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- “**缓冲区大小**”用于设置连接器的缓冲区大小。默认值为 1 MB，最大值为 64 MB。
- **字符编码** 设置项指定字符编码。默认值为 `UTF-8`。

- “**事件缓冲区 TTL**”是将记录合并为单个 auditd 事件的缓冲区的生存时间。如果启用了“**Auditd**”切换开关，则此字段可用。倒计时从收到第一个事件行时开始，或者在前一个 TTL 到期后立即开始。可能值：50 毫秒到 3000 毫秒。默认值是 2000 毫秒。

- **传输标头** — 对于 auditd 事件，必须指定一个正则表达式来标识 auditd 日志的各个部分。您可以使用默认值，也可以对其进行编辑。正则表达式必须包含 record_type_name、record_type_value 和 event_sequence_number 这三个捕获组。如果多行 auditd 事件包含前缀，则第一个记录将保留该前缀，对于后续条目，将丢弃该前缀。

  可以单击“**重置为默认值**”来恢复为原始值。

- **TLS 模式** — 使用 PEM x509 格式的证书的 TLS 加密模式：

  - **已禁用** （默认）—不使用 TLS 加密。

  - **已启用** — 使用不带证书验证的加密。

  - **带验证** — 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。

  - **自定义 PFX** — 使用加密。选择此选项后，必须在外部证书颁发机构中生成证书，该证书需包含私钥且采用 PKCS#12 容器格式。然后，必须将证书从密钥库中导出，并将其作为 PFX 机密上传到 KUMA 控制台。**添加 PFX 密钥**。

    要创建 PFX 密钥：

    1. 在“**名称**”字段中，输入 PFX 密钥的名称。

    2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。

    3. 在**“密码”**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。

    4. 然后单击**创建**按钮。

       PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。

    使用 TLS 时，无法将 IP 地址指定为 URL。

- **压缩** — 您可以使用 Snappy 压缩。默认情况下，压缩被**禁用**。

- **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

udp 类型

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。

- **租户**（必填） — 拥有该资源的租户的名称。

- **类型**（必需）—连接器类型：**udp**。

- **URL** （必填）—您需要连接到的 URL。可用格式：hostname:port、IPv4:port、IPv6:port、:port。

- **Auditd** 是一项机制的切换开关，该机制可将从连接器接收的 auditd 日志事件记录合并为单个事件。Auditd 仅支持 \n 分隔符。如果启用切换开关，**分隔符**字段将不可用。如果在代理连接器中启用了“**Auditd**”切换开关，则必须在代理发送事件所至的收集器的连接器中配置 \n 分隔符。

- **分隔符**用于指定表示事件之间分隔符的字符。可用值：`\n`、`\t`、`\0`。如果未指定分隔符（即选择了空值），则事件不会被分隔。

- **描述** – 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- “**缓冲区大小**”用于设置连接器的缓冲区大小。默认值为 16 KB，最大值为 64 KB。

- **处理程序数量**是指服务可以同时运行以并行处理响应规则的处理程序数量。您可以使用以下公式确定处理程序的数量：(<CPU 核心数>/2) + 2。

- **字符编码** 设置指定字符编码。默认值为 `UTF-8`。

- “**事件缓冲区 TTL**”是将记录合并为单个 auditd 事件的缓冲区的生存时间。如果启用了“**Auditd**”切换开关，则此字段可用。倒计时从收到第一个事件行时开始，或者在前一个 TTL 到期后立即开始。可能值：50 毫秒到 3000 毫秒。默认值是 2000 毫秒。

- **传输标头** – 对于 auditd 事件，必须指定一个正则表达式来标识 auditd 日志的各个部分。您可以使用默认值，也可以对其进行编辑。正则表达式必须包含 record_type_name、record_type_value 和 event_sequence_number 这三个捕获组。如果多行 auditd 事件包含前缀，则第一个记录将保留该前缀，对于后续条目，将丢弃该前缀。

  可以单击“**重置为默认值**”来恢复为原始值。

- **压缩** – 您可以使用 Snappy 压缩。默认情况下，压缩被**禁用**。

- **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

Netflow 类型

创建此类型的连接器时，您需要定义以下设置的值：

- “**基本设置**”选项卡

  - **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。

  - **租户**（必填） – 拥有该资源的租户的名称。

  - **类型**（必填）–连接器类型：**netflow**。

  - **URL**（必填）–您需要连接到的 URL。

  - **描述** – 资源描述：最多 4,000 个 Unicode 字符。

- “**高级设置**”选项卡

  - “**缓冲区大小**”用于设置连接器的缓冲区大小。默认值为 16 KB，最大值为 64 KB。

  - **工作进程数** – 用于设置连接器的工作进程数量。默认值是 1。

- **字符编码** 设置指定字符编码。默认值为 UTF-8。
- **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

Sflow 类型

附加规范化可用于以 sFlow 格式接收的事件。

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） – 拥有该资源的租户的名称。
- **类型**（必填）– 连接器类型：**sflow**。
- **URL**（必填）– 您需要连接到的 URL。可用格式：hostname:port、IPv4:port、IPv6:port、:port。
- **描述** – 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- “**缓冲区大小**”用于设置连接器的缓冲区大小。默认值为 1 MB，最大值为 64 MB。
- **工作进程数** – 用于设置连接器的工作进程数量。默认值是 1。
- **字符编码** 设置指定字符编码。默认值为 UTF-8。
- **调试**– 切换开关，用于启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

Nats-jetstream 类型

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） – 拥有该资源的租户的名称。
- **类型**（必填）–连接器类型：**nats-jetstream**。
- **URL**（必填）–您需要连接到的 URL。
- **主题**（必填）– NATS 消息的主题。必须包含 Unicode 字符。
- **分隔符**用于指定表示事件之间分隔符的字符。可用值：`\n`、`\t`、`\0`。如果未指定分隔符（即选择了空值），则事件不会被分隔。
- **描述** – 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- “**缓冲区大小**”用于设置连接器的缓冲区大小。默认值为 16 KB，最大值为 64 KB。
- **群组 ID** — NATS 消息的“组 ID”参数。必须包含 1 到 255 个 Unicode 字符。默认值为 `default`。
- **工作线程数** — 用于设置连接器的工作线程数量。默认值是 1。
- **字符编码** 设置指定字符编码。默认值为 `UTF-8`。
- **集群 ID**是NATS集群的ID。
- TLS **模式**指定是否使用 TLS 加密：
  - **已禁用** （默认）—不使用 TLS 加密。
  - **已启用** — 使用不带证书验证的加密。
  - **带验证** — 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。
  - **自定义 CA** — 使用加密并验证证书是否由证书颁发机构签名。包含证书的密钥从“**自定义 CA**”下拉列表中选择，选择此选项时会显示该列表。

    创建由证书颁发机构签名的证书

    您可以在 KUMA Core 服务器上创建 CA 签名的证书（以下命令示例使用 OpenSSL）。

    要创建由证书颁发机构签名的证书：

    1. 生成证书签发机构要使用的密钥，例如：

       ```
       openssl genrsa -out ca.key 2048
       ```

    2. 为生成的密钥创建证书，例如：

       ```
       openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 证书颁发机构的通用主机名 >" -out ca.crt
       ```

    3. 创建私钥并请求证书签发机构对其进行签名，例如：

       ```
       openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 服务器的通用主机名 >" -out server.csr
       ```

    4. 创建由证书签发机构签名的证书。您需要在 `subjectAltName` 变量中包含要为其创建证书的服务器的域名或 IP 地址，例如：

       ```
       openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
       ```

    5. 在 Open Single Management Platform Web 界面中，将创建的 `server.crt` 证书上传到 **证书** 类型的密钥，然后在 **自定义 CA** 下拉列表中选择 **证书** 类型的密钥。

    使用 TLS 时，无法将 IP 地址指定为 URL。

    要在第三方设备上使用 KUMA 证书，您必须将证书文件扩展名从 CERT 更改为 CRT。否则，可能会返回错误 x509：证书由未知机构签名。

- **压缩** – 您可以使用 Snappy 压缩。默认情况下，压缩被**禁用**。
- **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。

连接器，Kafka 类型

kafka 类型的连接器用于在使用 Windows 和 Linux 代理时与 Apache Kafka 数据总线进行通信。下表描述了"**kafka**"类型连接器的设置。

使用 **kafka** 类型的连接器，KUMA 可以接收未压缩和压缩形式的事件。压缩采用 **kafka** 支持的以下压缩算法：gzip、snappy、zstd 或 lz4。以压缩形式到达的事件会自动解压缩。

"基本设置"选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
类型	连接器类型：**kafka**。 必需设置。
标签	资源搜索的标签。 可选设置。
网址	URL（必填）–需要连接到的 URL。支持以下 URL 格式： • `<主机名>:<端口号>` • `<IPv4 地址>:<端口号>` • `<IPv6 地址>:<端口号>` 您可以按以下格式指定 IPv6 地址：`[<IPv6 地址>%<接口>:<端口号>`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以添加多个 URL，也可以删除一个 URL。如果 URL 字段包含制表符或空格字符，KUMA 不允许保存资源或服务。要添加 URL，请单击"**+ 添加**"按钮。要删除 URL，请单击旁边的删除 (✕) 图标。 必需设置。

设置	描述
授权	连接到 **URL** 字段中指定的 URL 时的授权类型： • **已停用**。默认选择此值。 • **Plain**。这种类型的授权使用 SASL/PLAIN 机制执行，该机制以明文形式传输用户名和密码。通常情况下，TLS 用于在 SASL/PLAIN 中提供传输安全（加密）。 如果选择此选项，请在**"Secret"**下拉列表中指定包含用户账户凭证的 Secret，以便在连接到目的地时进行授权。您可以选择现有 Secret 或创建新 Secret。要创建新 Secret，请选择"**新建**"。 如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (🖊) 图标。 **如何创建 Secret?** *要创建密钥：* 1. 在"**名称**"字段中，输入密钥的名称。 2. 在"**用户**"和"**密码**"字段中，输入代理将用于连接到连接器的用户账户的凭证。 3. 如有必要，请在"**描述**"字段中输入密钥的描述。 4. 单击"**创建**"按钮。 密钥将添加并显示在"**密钥**"下拉列表中。 • **PFX** 指的是使用 PFX 密钥的 TLS 加密。您必须在外部证书颁发机构中生成一个 PKCS#12 容器格式的私钥证书，从密钥库中导出 PFX 文件，并将 PFX 文件作为 PFX 密钥上传到 KUMA Web 界面。如果选择此值，请在**PFX 密钥**下拉列表中指定由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择"**新建**"。 如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (🖊) 图标。 **如何创建 PFX 密钥?** *要创建 PFX 密钥：* 1. 在"**名称**"字段中，输入 PFX 密钥的名称。 2. 单击"**上传 PFX**"并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。 3. 在**"密码"**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。 4. 然后单击**创建**按钮。 PFX 密钥已创建并显示在"**PFX 密钥**"下拉列表中。 如果您使用多个证书的链来验证服务器，我们建议使用 OpenSSL 构建 PFX 文件，以确保证书链中证书的顺序正确。 • **SCRAM-SHA-256**是一种使用安全连接机制进行的授权，它使用SHA256哈希值进行安全身份验证，防止数据被拦截。 • **SCRAM-SHA-512**是一种使用安全连接机制进行的授权，它使用SHA512哈希值进行安全身份验证，防止数据被拦截。 当在**密钥**下拉列表中选择**SCRAM-SHA-256**或**SCRAM-SHA-512**作为授权类型时，请指定一个带有密码的密钥进行授权。您可以选择现有 Secret 或创建新 Secret。要创建新的 Secret，请在**"Secret"**下拉列表中选择**"新建"** 。
主题	Kafka 消息的主题。消息的最大长度为 255 个字符。不允许使用空格和选项卡符。您可以使用以下字符：a–z、A–Z、0–9、"."、"_"、"-"。 必需设置。
组 ID。	Kafka 消息的 `GroupID` 参数的值。值的最大长度为 255 个字符。您可以使用以下字符：a–z、A–Z、0–9、"."、"_"和"-"。
分隔符	标志着事件之间界限的字符： • **\n** • **\t** • **\0** 如果您未在此下拉列表中选择值，则默认选择空值。在这种情况下，连接器不会将一个事件拆分成多个事件，而是原封不动地将其传递给规范化器。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

"高级设置"选项卡

设置	描述
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。
处理程序数	服务可以同时运行以并行处理响应规则的处理程序数量。 该值必须是正整数，最高到 999。 默认情况下，处理程序的数量为 256。

设置	描述
字符编码	字符编码。默认是 **UTF-8**。

TLS 模式	TLS 加密模式。使用 TLS 加密时，您不能在"基本设置"**基本设置URL** 字段中指定 IP 地址。可用值：
	• "**已禁用**"表示不使用 TLS 加密。默认选择此值。
	• "**已启用**"表示已使用 TLS 加密，但未验证证书。
	• "**自定义 CA**"表示使用 TLS 加密并验证证书是否由证书颁发机构签名。如果选择此值，请在**"自定义 CA"**下拉列表中指定一个由证书颁发机构签名的证书的密钥。您可以选择现有 Secret 或创建新 Secret。要创建新 Secret，请选择"**新建**"。
	如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (🖊) 图标。
	如何创建由证书颁发机构签名的证书?
	您可以在 KUMA Core 服务器上创建 CA 签名的证书（以下命令示例使用 OpenSSL）。
	要创建由证书颁发机构签名的证书：
	1. 生成证书签发机构要使用的密钥，例如：
	`openssl genrsa -out ca.key 2048`
	2. 为生成的密钥创建证书，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 证书颁发机构的通用主机名 >" -out ca.crt`
	3. 创建私钥并请求证书签发机构对其进行签名，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 服务器的通用主机名 >" -out server.csr`
	4. 创建由证书签发机构签名的证书。您需要在 `subjectAltName` 变量中包含要为其创建证书的服务器的域名或 IP 地址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform Web 界面中，将创建的 `server.crt` 证书上传到 **证书** 类型的密钥，然后在 **自定义 CA** 下拉列表中选择 **证书** 类型的密钥。
	要在第三方设备上使用 KUMA 证书，您必须将证书文件扩展名从 CERT 更改为 CRT。否则，您可能会收到 `x509: certificate signed by unknown authority` 错误。

要获取的消息大小	请求中单个消息的大小（以字节为单位）。如果未指定值或指定为 0，则应用默认值 16 MB。它不能超过 2147483647 字节。
最大获取等待时间	单条消息超时时间（秒）。如果没有指定值或指定为 0，则默认值为 5 秒。最大可能值为：2147483647。
连接超时时间	Kafka broker 连接超时时间（秒）。 最大可能值为：2147483647。默认值是 30 秒。
读取超时时间	读取操作超时时间（秒）。 最大可能值为：2147483647。默认值是 30 秒。
写入超时时间	写入操作超时时间（秒）。 最大可能值为：2147483647。默认值是 30 秒。
群组检测信号间隔	群组状态更新间隔（秒）。 更新间隔不能超过会话时间。推荐值为会话时间的 1/3。最大可能值为：2147483647。默认值是 3 秒。
会话超时时间	会话时间（秒）。 最大可能值为：2147483647。默认值是 10 秒。
最大处理时间	处理单个线程的一条消息的最大持续时间（以毫秒为单位）。 最大可能值为：2147483647。默认值是 100 毫秒。
已启用自动提交	默认启用。

设置	描述
自动提交间隔	自动提交间隔（秒）。默认值是1秒。 最大可能值为：18446744073709551615。可以指定任何正数。

kata/edr 类型

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） — 拥有该资源的租户的名称。
- **类型**（必填）—连接器类型：**kata/edr**。
- **URL**（必填）— 可从 KATA/EDR 服务器接收遥测数据的 URL。URL 必须包含主机和端口；默认端口为 443。如果 KATA/EDR 部署在集群中，则可以指定多个 URL 以确保连接的高可用性。
- **Secret**（必填）是一个下拉列表，您可以从中选择存储用于连接到 KATA/EDR 服务器的凭证的密钥。您可以从下拉列表中选择密钥资源，也可以通过单击加号图标 (+) 创建密钥。创建密钥时，您可以指定自定义证书和私钥，也可以自动生成新的自签名证书和私钥。可以通过点击铅笔图标 () 来更改所选密钥。
- **外部 ID** — 外部系统的 ID。KUMA 会自动在此字段中生成 ID。
- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。
- **字符编码** — 用于转换为 UTF-8 的源字符编码设置。仅建议在规范化事件的字段中发现无效字符时配置转换。默认值：未选择。
- **事件数** — 一个请求中的最大事件数。默认情况下，使用 KATA/EDR 服务器上设置的值。
- **事件获取超时时间**是等待从KATA/EDR服务器接收事件的时间（以秒为单位）。默认值为 0，这意味着使用了 KATA/EDR 服务器上指定的值。
- **客户端超时时间**是等待KATA/EDR服务器响应的时间（以秒为单位）。默认值为 1,800 秒，显示为 0。
- **KEDRQL 筛选器** — 用于过滤向 KATA/EDR 服务器发送的请求。有关查询语言的更多详细信息，请参阅 KEDR 帮助。

连接器，HTTP 类型

使用 Windows 和 Linux 代理时，**http** 类型的连接器用于通过 HTTP 接收事件。下表描述了“**http**”类型连接器的设置。

使用 **http** 类型的连接器，KUMA 可以接收未压缩和压缩形式的事件。以压缩形式到达的事件，例如 Kaspersky Endpoint Security for Windows 事件会自动解压缩。

“基本设置”选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
类型	连接器类型：**http**。 必需设置。
标签	资源搜索的标签。 可选设置。
网址	URL（必需）—需要连接到的 URL。您可以按以下格式之一输入 URL： • `< 主机名 >:< 端口号 >` • `< IPv4 地址 >:< 端口号 >` • `< IPv6 地址 >:< 端口号 >` • `:< 端口号 >` 要将事件源中的数据发送到连接器，指定的 URL 必须以 `/input` 结尾。 必需设置。
分隔符	标志着事件之间界限的字符： • **\n** • **\t** • **\0** 如果您未在此下拉列表中选择值，则默认选择空值。在这种情况下，连接器不会将一个事件拆分成多个事件，而是原封不动地将其传递给规范化器。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。
字符编码	字符编码。默认是 **UTF-8**。

设置	描述
TLS 模式	TLS 加密模式。使用 TLS 加密时，您不能在“基本设置”的 **URL** 字段中指定 IP 地址。可用值： • “**已禁用**”表示不使用 TLS 加密。默认选择此值。 • “**已启用**”表示已使用 TLS 加密，但未验证证书。 • “**带验证**”表示使用 TLS 加密并验证证书是否使用 KUMA 根证书进行签名。KUMA 的根证书和密钥在应用程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 目录中。 已过时的加密模式，已弃用。将在 KUMA 的未来版本中移除。 • **自定义 PFX** 指的是使用 PFX 密钥的 TLS 加密。您必须生成一个包含 PKCS#12 容器格式的私钥的 PFX 证书，然后将该 PFX 证书作为 PFX 密钥上传到 KUMA Web 界面。如果选择此值，请在 PFX 密钥下拉列表中指定由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择“新建”。 如果要编辑现有密钥的设置，请单击旁边的铅笔图标。 **如何创建 PFX 密钥?** *要创建 PFX 密钥：* 1. 在“**名称**”字段中，输入 PFX 密钥的名称。 2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。 3. 在**“密码”**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。 4. 然后单击**创建**按钮。 PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。 • **带客户端身份验证的自定义 PFX** 是指使用 PFX 密钥进行 TLS 加密。在此模式下，客户端将使用证书进行身份验证。 您必须生成一个包含 PKCS#12 容器格式的私钥的 PFX 证书，然后将该 PFX 证书作为 PFX 密钥上传到 KUMA Web 界面。如果选择此值，请在 PFX 密钥下拉列表中指定由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择“新建”。 如果要编辑现有密钥的设置，请单击旁边的铅笔图标。 **如何创建 PFX 密钥?** *要创建 PFX 密钥：* 1. 在“**名称**”字段中，输入 PFX 密钥的名称。 2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。 3. 在**“密码”**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。 4. 然后单击**创建**按钮。 PFX密钥随即创建并显示在**PFX 密钥**下拉列表中。

SQL 类型

sql 类型的连接器用于查询数据库。KUMA 支持多种数据库类型。

支持的数据库类型

该程序支持以下类型的 SQL 数据库：

- SQLite
- MSSQL。
- MySQL。
- PostgreSQL。
- Cockroach。

- Oracle。
- Firebird。

创建 **sql** 类型的连接器时，必须指定常规连接器设置和各个数据库的连接设置。下表描述了 **sql** 类型的连接器的设置。

“基本设置”选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
类型	连接器类型：**sql**。 必需设置。
标签	资源搜索的标签。 可选设置。
默认查询	连接到数据库时执行的 SQL 查询。 必需设置。
每次发送请求时都重新连接数据库	此切换开关用于在每次发送查询时重新将连接器连接到数据库。默认情况下，此切换开关处于关闭状态。
轮询间隔（秒）	执行 SQL 查询的时间间隔（以秒为单位）。默认值是 10 秒。

设置	描述
连接	此组中的设置取决于为连接选择的数据库类型： MySQL Postgres SQLite3 Oracle。 Firebird。 ClickHouse ODBC • **数据库类型** 是要连接的数据库的类型。选择数据库类型后，**URL** 字段中会显示与通信协议对应的前缀。例如，对于 **ClickHouse** 数据库，**URL** 字段包含 `clickhouse://` 前缀。 • 通过 **独立密钥** 复选框，您可以查看连接信息。如果选中 **独立密钥** 复选框，则凭据在 **密钥** 字段中指定，而连接字符串输入到 **URL** 字段中，且不指定用户的密码。 • 如果选中 **独立密钥复选框，则 URL 为连接 URL。** 这样一来，即便用于连接的用户账户密码发生更改，您也无需重新创建大量连接，即可查看连接信息。 创建连接时，如果在 URL 中指定连接信息，则包含特殊字符的凭据字符串可能无法正确处理。如果在创建连接时发生错误，但您确定指定的设置正确，请以百分比编码输入特殊字符。 **特殊字符代码** ! # $ % & ' ( ) * + %21 %23 %24 %25 %26 %27 %28 %29 %2A %2B , / : ; = ? @ [ ] \ %2C %2F %3A %3B %3D %3F %40 %5B %5D %5C 用于访问 SQL 数据库的密码不支持以下特殊字符：空格、[、]、:、/、#、%、\。 如果选中了 **独立密钥** 复选框，则不需要使用任何特殊字符代码。 在 **使用密钥中的 URL** 下拉列表中，您可以选择现有 URL 或创建新 URL。要创建新 URL，请选择“**新建**”。 如果要编辑现有 URL 的设置，请单击旁边的铅笔 (🖉) 图标。 • **Secret** 是一个 URL Secret，用于存储连接数据库的 URL 列表。如果选中了 **独立密钥** 复选框，则会显示此字段。 • **标识列** 是包含表每行 ID 的列的名称。 必需设置。 • **标识种子** 是标识列中的值，用于确定要从 SQL 表的哪一行开始读取数据。 • **查询** 是附加 SQL 查询，将代替默认 SQL 查询执行。 • **轮询间隔，秒** 是 SQL 查询执行间隔（以秒为单位）。连接器将使用指定的间隔，而不是默认间隔。默认值是 10 秒。 您可以添加多个连接或删除连接。要添加连接，请单击 **+ 添加连接** 按钮。要删除连接，请单击旁边的删除 (✕) 图标。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。
字符编码	字符编码。默认是 **UTF-8**。 KUMA 将 SQL 响应转换为 UTF-8 编码。您可以将 SQL 服务器配置为以 UTF-8 编码发送响应，或者更改 KUMA 端传入消息的编码。

在单个连接器中，您可以为多个受支持的数据库**创建连接**。如果无法启动带有 **sql** 类型连接器的收集器，请检查 /opt/kaspersky/kuma/collector/<收集器 ID>/sql/state-<文件 ID> 状态文件是否为空。如果状态文件为空，请将其删除并重新启动收集器。

要为多个 SQL 数据库创建连接，请执行以下操作：

1. 点击“**添加连接**”按钮。
2. 指定 **URL** 、**标识列**、**标识种子**、**查询**和**轮询间隔（秒）**的值。
3. 对每个所需的连接重复步骤 1-2。

支持的 SQL 类型及其特定使用功能

支持以下 SQL 类型：

- MSSQL。
  例如：
  - `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}`

  建议使用此 URL 变体。
  - `sqlserver://{user}:{password}@{server}?database={database}`

  字符 `@p1` 在 SQL 查询中用作占位符。

  > 如果要使用域账户凭证进行连接，请以 < 域 >`%5C`< 用户 > 格式指定账户名称。例如：`sqlserver://domain%5Cuser:password@ksc.example.com:1433/SQLEXPRESS?database=KAV`。

- MySQL/MariaDB
  例如：
  `mysql://{user}:{password}@tcp({server}:{port})/{database}`
  字符 `?` 在 SQL 查询中用作占位符。

- PostgreSQL。
  例如：`postgres://{user}:{password}@{server}/{database}?sslmode=disable`
  字符 `$1` 在 SQL 查询中用作占位符。

- CockroachDB
  例如：
  `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`
  字符 `$1` 在 SQL 查询中用作占位符。

- SQLite3
  例如：
  `sqlite3://file:{file_path}`
  问号 (`?`) 在 SQL 查询中用作占位符。
  查询 SQLite3 时，如果 ID 的初始值为 datetime 格式，则必须在 SQL 查询中添加使用 `sqlite datetime` 函数的日期转换。例如：
  `select * from connections where datetime(login_time) > datetime(?, 'utc') order by login_time`

在此示例中，`connections` 是 SQLite 表，变量 `?` 的值取自 **标识种子** 字段，并且必须以 `{<` 日期 `>}T{<` 时间 `>}Z` 格式指定，例如 `2021-01-01T00:10:00Z)`。

- Oracle DB

  使用“oracle”驱动程序的密钥的 URL 示例：

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}
  ```

  ```
  oracle://{user}:{password}@{server}:{port}/?SID={SID_VALUE}
  ```

  如果查询执行时间超过 30 秒，oracle 驱动程序将中止 SQL 请求，并且收集器日志中会出现以下错误：**user requested cancel of current operation**。要增加 SQL 查询的执行时间，请在连接字符串中指定 **timeout** 参数的值（以秒为单位），例如：

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}?timeout=300
  ```

  SQL 变量 `:val` 用作占位符。

  查询 Oracle DB 时，如果标识种子为 datetime 格式，则必须考虑数据库中字段的类型，并在必要时在 SQL 查询中添加时间字符串的转换，以确保 SQL 连接器正常工作。例如，如果数据库中的 `Connections` 表具有 `login_time` 字段，则可以进行以下转换：

  - 如果 **login_time** 字段的类型为 TIMESTAMP，则根据数据库的配置，**login_time** 字段可能包含 `YYYY-MM-DD HH24:MI:SS` 格式的值，例如 `2021-01-01 00:00:00`。在这种情况下，您需要在 **标识种子** 字段中指定 `2021-01-01T00:00:00Z`，并在 SQL 查询中使用 `to_timestamp` 函数执行转换，例如：

    ```
    select * from connections where login_time > to_timestamp(:val, 'YYYY-MM-DD"T"HH24:MI:SS"Z"')
    ```

  - 如果 **login_time** 字段的类型为 TIMESTAMP WITH TIME ZONE，则根据数据库的配置，**login_time** 字段可能包含 `YYYY-MM-DD"T"HH24:MI:SSTZH:TZM` 格式的值（例如 `2021-01-01T00:00:00+03:00`）。在这种情况下，您需要在标识种子字段中指定 `2021-01-01T00:00:00+03:00`，并在 SQL 查询中使用 `to_timestamp_tz` 函数执行转换，例如：

    ```
    select * from connections_tz where login_time > to_timestamp_tz(:val, 'YYYY-MM-DD"T"HH24:MI:SSTZH:TZM')
    ```

    有关 `to_timestamp` 和 `to_timestamp_tz` 函数的详细信息，请参阅 Oracle 官方文档。

  要与 Oracle DB 交互，必须安装 libaio1 Astra Linux 软件包。

- Firebird® SQL

  例如：

  ```
  firebirdsql://{user}:{password}@{server}:{port}/{database}
  ```

  问号 (`?`) 在 SQL 查询中用作占位符。

  如果在 Windows 上连接 Firebird 时出现问题，请使用数据库文件的完整路径，例如：

  ```
  firebirdsql://{user}:{password}@{server}:{port}/C:\Users\user\firebird\db.FDB
  ```

- ClickHouse

  例如：

  ```
  clickhouse://{user}:{password}@{server}:{port}/{database}
  ```

  问号 (`?`) 在 SQL 查询中用作占位符。

KUMA 支持以下数据类型：

- 可转换为字符串的数据（例如字符串、数值和 BLOB）将显示为字符串。
- 数组和映射将以 JSON 格式显示，或者使用内置 `go fmt.Sprintf("%v",v)` 函数以最佳方式显示。

连接到 ClickHouse 有两种方法：

- 不使用凭据，通过输入 URL： `clickhouse://host:port/database`
- 使用凭据，通过输入 URL： `clickhouse://user:password@host:port/database`

使用 TLS 加密时，默认情况下，连接器仅在端口 9440 上运行。如果未使用 TLS 加密，默认情况下，连接器只能通过端口 9000 与 ClickHouse 配合使用。

> 该连接器无法通过 HTTP 运行。

如果在 ClickHouse 服务器上配置了 TLS 加密模式，而在连接器设置的 **TLS 模式** 下拉列表中选择了 **已禁用**，或反之亦然，则无法建立数据库连接。

> 仅当指定 ClickHouse 驱动程序时，才使用 **TLS 模式**。

如果要连接到 KUMA ClickHouse，请在 **SQL** 连接器设置中指定 **PublicPKI** 密钥类型，其中包含 base64 编码的 PEM 私钥和公钥。

在 ClickHouse 连接类型的 **SQL** 连接器参数中，需要在 **TLS 模式** 下拉列表中选择 **已禁用**。如果使用证书进行身份验证，则不得指定此值。如果在 **TLS 模式** 下拉列表中选择 **自定义 CA**，则需要在 **密钥** 字段中指定 “certificate” 类型的密钥的 ID。您还需要在 **授权类型** 下拉列表中选择以下值之一：

- **已禁用**。如果选择此值，则需要将 **密钥** 字段留空。
- **Plain**。如果选中 **独立密钥** 复选框，并在 **密钥** 字段中指定“凭证”类型的密钥 ID，则选择此值。
- **PublicPKI**。如果选中 **独立密钥** 复选框，并在 **密钥** 字段中指定 PublicPKI 类型的密钥 ID，则选择此值。

如果 ID 的初始值包含时间指示 (`datetime`)，则在查询中必须使用用于时间转换的变量 (`parseDateTimeBestEffort`)。例如，如果时间指定为 `2021-01-01 00:10:00`，则可以使用以下查询：

```
select connections, username, host, login_time from connections where login_time >
parseDateTimeBestEffort(?) order by login_time
```

- ODBC

  例如：

  如果在配置连接设置时选中 **独立密钥** 复选框，则为 `odbc://{server}:{port}/{database}`。

  如果需要指定所有连接参数，则为 `odbc://{server}:{port}/{database}?params1=value1&params2=value2`。

  问号 (`?`) 在 SQL 查询中用作占位符。

  > 当收集器部署在 Kubernetes 中时，不支持 ODBC。

如果使用 ODBC，则需要为 **ODBC 驱动程序文件名** 设置指定 ODBC 数据库驱动程序的名称。然后，您需要将驱动程序文件保存在 `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` 目录中。

解决方案使用 ODBC Manager 系统实用程序 2.3.14 版来管理 ODBC 驱动程序和数据库连接。您需要使用与此版本的系统实用程序兼容的 ODBC 驱动程序。

指定 ODBC 数据库驱动程序的名称时，请考虑以下事项：

- 如果驱动程序有依赖项，则需要将这些依赖项保存在 `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` 或 `/opt/kaspersky/kuma/collector/<uuid_of_collector>/` 目录中（如果驱动程序要求如此）。
- 此设置区分大小写。
- 指定路径时，允许使用特殊字符。

ODBC 数据库驱动程序名称示例

```
psqlodbcw.so
```

要在现有收集器中使用 ODBC SQL 连接器，从 4.2 版升级解决方案后，您需要卸载并重新安装收集器。这样，您可以获取 ODBC 连接器正常工作所需的所有环境变量的值。

使用 ODBC 驱动程序配置 SQL 连接器的示例

要配置连接器以使用 ODBC 驱动程序（以 PostgreSQL 和 Astra Linux 的 ODBC 驱动程序为例）：

1. 检查是否有适用于您的数据库的 ODBC 驱动程序。如果存在这样的驱动程序，请在线查找此驱动程序的 .so 扩展名文件名。
2. 在 **监控** → **资源和服务** → **连接器** 部分，创建 SQL 连接器；在 **数据库类型** 字段中，选择 **ODBC**。
3. 填写新连接器的所有必填字段，并在 **ODBC 驱动程序文件名** 字段中指定 ODBC 驱动程序的名称。

   如有必要，您可以在使用指定连接器安装收集器后更改驱动程序的名称。
4. 在主机上安装带有 SQL 连接器的收集器。
5. 下载相应的 .so 文件。对于 PostgreSQL，可以使用以下命令下载此文件：

   ```
   apt download odbc-postgresql
   ```

   解决方案会下载适用于 Astra Linux 的 `ibpq5_15.17-astra.se2.3r2_amd64.deb` 软件包。
6. 执行以下操作：

   a. 通过运行以下命令解压 `ibpq5_15.17-astra.se2.3r2_amd64.deb` 软件包：

   ```
   ar x libpq5_15.17-astra.se2.3r2_amd64.deb
   ```

   b. 通过运行以下命令解压 `data.tar.xz` 压缩文件：

   ```
   tar -xf data.tar.xz
   ```

7. 在解压的文件中，通过运行以下命令查找 .so 文件：

```
find . -name ".so"
```

8. 通过运行以下命令，将 PostgreSQL ODBC 驱动程序复制到收集器目录内的 `driver` 目录：

```
cp ./usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so
```

9. 通过运行以下命令，验证主机上是否满足所有 ODBC 驱动程序依赖项：

```
LD_LIBRARY_PATH="/opt/kaspersky/kuma/collector/<ID>/deps/odbc:/opt/kaspersky/kuma/collector/<ID>/driver"
ldd /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so | grep "not found"
```

其中 `<ID>` 是已安装收集器的 ID。

如果该命令显示 `libpq.so.5 => not found`，您需要另外下载 `libpq.so.5` 依赖项。对于 Astra Linux，您也可以通过运行以下命令执行此操作：

```
apt download libpq5
```

之后，解压 deb 软件包并查找 .so 文件。将由此找到的 .so 文件移动到收集器文件夹（`cp ./usr/lib/x86_64-linux-gnu/libpq.so.5.15 /opt/kaspersky/kuma/collector/<ID>/driver/libpq.so.5`）中的 `driver` 目录。

10. 重新检查主机上的所有 ODBC 驱动程序依赖项。此外，请确保收集器的 `driver` 目录（`/opt/kaspersky/kuma/` collector/<ID>/driver/psqlodbcw.so）中的驱动程序文件名与配置文件中的文件名匹配。

为防止出现缺少依赖项错误，您可以将 `- Environment=LD_DEBUG=libs` 行添加到收集器的 systemd 文件中，并运行以下命令：

```
systemctl daemon-reload
```

然后重新启动收集器；`journalctl` 将显示有关 ODBC 驱动程序搜索依赖项的信息。

每种 ODBC 驱动程序都有其自己显示缺失依赖项相关信息的特殊方式。例如，MsSQL ODBC 驱动程序会在 `driver` 目录的上一级查找依赖项。您需要将缺失的 `share` 文件夹保存到 `/opt/kaspersky/kuma/collector/<ID>` 中，而不是保存到 `driver` 目录中。根据 ODBC 驱动程序的不同，指定 URL 时也可能存在一些特殊之处。例如，对于 Oracle ODBC 驱动程序，您需要在连接器配置文件中以 `odbc://?DBQ=//{server}:{port}/{database}` 格式指定 URL（用户账户单独指定）。

> 配置 ODBC 驱动程序时，建议遵循特定驱动程序的文档。

11. 重启收集器。

SQL 查询中支持对数据库信息的顺序请求。例如，如果您在 **查询** 字段中输入 `select * from <数据表名称> where id > <占位符>`，则首次查询该表时会将 **标识种子** 字段的值用作占位符值。此外，使用 SQL 连接器的服务会保存最后读取条目的 ID，并且该条目的 ID 将在下一次查询数据库时用作占位符值。

> 建议将 `order by` 命令添加到查询字符串中，后接排序字段。例如，`select * from table_name where id > ? order by id`。

SQL 请求示例

SQLite、Firebird—`select * from table_name where id > ?`

MSSQL—`select * from table_name where id > @p1`

MySQL—`select * from table_name where id > ?`

PostgreSQL、Cockroach—`select * from table_name where id > $1`

Oracle—`select * from table_name where id > :val`

文件类型

"**文件**"类型用于从任何文本文件中检索数据。文件中的一个字符串被视为一个事件。字符串分隔符：\n。此类连接器适用于 Linux 代理和 Windows 代理。

要读取 Windows 文件，您需要创建"文件"类型的连接器并在 Windows 上手动安装代理。在一个 Windows 代理中，您可以配置多个不同类型的连接，但只能有一个"文件"类型的连接。Windows 代理不得读取其安装目录下的文件。即使使用 FAT 文件系统，该连接器也能正常工作。如果磁盘进行了碎片整理，连接器会重新读取所有文件，因为所有文件的 inode 都会被重置。

我们不建议使用管理员帐户运行代理。代理的用户帐户必须具有文件夹和文件的读取权限。我们不建议在重要系统上安装代理。最好发送事件日志，并由专用设备上的代理读取这些日志。

创建此类型的连接器时，您需要定义以下设置的值：

- "**基本设置**"选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填）— 连接器类型：**文件**。
  - **文件路径**（必填）— 您需要操作的文件的完整路径。例如，`/var/log/*som?[1-9].log or c:\folder\logs.*.` 不允许使用以下路径：
    - `` `(?i)^[a-zA-Z]:\\Program Files` ``
    - `` `(?i)^[a-zA-Z]:\\Program Files \(x86\)` ``
    - `` `(?i)^[a-zA-Z]:\\Windows` ``
    - `` `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` ``

    文件和文件夹掩码模板

掩码：

- '*'—匹配任意字符序列。
- '[['^'] { 字符范围 } ']'—字符类（不能为空）。
- '?'—匹配任意单个字符。

字符范围：

- [0-9]—数字；
- [a-zA-Z]—拉丁字母字符。

示例：

- /var/log/*som?[1-9].log
- /mnt/dns_logs/*/dns.log
- /mnt/proxy/access*.log

在文件路径中使用前缀时的限制

指定文件路径时不能使用的前缀：

- `/*`
- `/bin`
- `/boot`
- `/dev`
- `/etc`
- `/home`
- `/lib`
- `/lib64`
- `/proc`
- `/root`
- `/run`
- `/sys`
- `/tmp`
- `/usr/*`
- `/usr/bin/`

- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。

文件可通过以下路径获取：

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/metrics/log/

按掩码限制要监控的文件的数量

可通过 Core 的 max_user_watches 设置限制同时按掩码监控的文件数量。要查看此设置的值，请运行以下命令：

```
cat /proc/sys/fs/inotify/max_user_watches
```

如果要监控的文件数量超过 max_user_watches 设置的值，收集器将无法继续从文件中读取事件，并会在收集器日志中记录以下错误：

```
Failed to add files for watching {"error": "no space left on device"}
```

为确保收集器继续正常运行，您可以配置适当的文件轮换，使文件数量不超过 max_user_watches 设置的值，或者增大 max_user_watches 的值。

要增大此设置的值：

```
sysctl fs.inotify.max_user_watches=<number of files>
```

```
sysctl -p
```

您还可以将 max_user_watches 设置的值添加到 sysctl.conf 中，以确保该值永久保留。

增大 max_user_watches 设置的值后，收集器将恢复正常运行。

- **Auditd** 是一项机制的切换开关，该机制可将从连接器接收的 auditd 日志事件记录合并为单个事件。Auditd 仅支持 \n 分隔符。如果启用切换开关，**分隔符**字段将不可用。如果在代理连接器中启用了“**Auditd**”切换开关，则必须在代理发送事件所至的收集器的连接器中配置 \n 分隔符。

- “**适用于 Windows**”是一个切换开关，打开后可以从 Windows 代理接收 Windows 事件日志事件。在这种情况下，必须关闭 **Auditd** 开关。默认情况下，“**适用于 Windows**”切换开关处于关闭状态。

- **描述** – 资源描述：最多 4,000 个 Unicode 字符。

- “**高级设置**”选项卡

  - **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

  - **缓冲区大小**是一种设置，允许您指定在将事件发送到存储或进一步处理之前，用于在 RAM 中累积事件的缓冲区大小（以字节为单位）。

    默认值：1048576 字节 (1 MB)。

    可能值：小于或等于 67108864 字节 (64 MB) 的正整数。

  - “**处理程序数量**”用于设置处理队列的服务数量。您可以使用以下公式确定处理程序的数量：(<CPU 核心数>/2) + 2。

  - **轮询间隔（毫秒）**是一种设置，用于设置连接器重新读取包含文件的目录的间隔。该值以毫秒为单位。仅当文件没有更改时，连接器才会等待指定的时长。如果文件被连续修改，且轮询间隔 = 5000 毫秒，则不会按照 5 秒间隔的设定来重新读取目录中的文件，而是连续重新读取。如果文件没有更改，连接器将等待 5 秒。如果在 Web 界面中设置了 0，则使用默认值 700 毫秒。我们建议将**轮询间隔（毫秒）**（毫秒）设置为不小于**事件缓冲区 TTL**的值。否则，**Auditd**选项可能会受到不利影响。

  - **字符编码** 设置用于指定字符编码。默认值是 UTF-8。

  - “**事件缓冲区 TTL**”是将记录合并为单个 auditd 事件的缓冲区的生存时间。如果启用了“**Auditd**”切换开关，则此字段可用。倒计时从收到第一个事件行时开始，或者在前一个 TTL 到期后立即开始。可能值：700 毫秒到 3000 毫秒。默认值是 2000 毫秒。

  - **传输标头** – 对于 auditd 事件，必须指定一个正则表达式来标识 auditd 日志的各个部分。您可以使用默认值，也可以对其进行编辑。正则表达式必须包含 record_type_name、record_type_value 和 event_sequence_number 这三个捕获组。如果多行 auditd 事件包含前缀，则第一个记录将保留该前缀，对于后续条目，将丢弃该前缀。

    可以单击“**重置为默认值**”来恢复为原始值。

类型 1c-xml

“**1c-xml**”类型用于从 1C 应用程序注册日志中检索数据。当连接器处理多行事件时，它会将其转换为单行事件。此类型的连接器适用于 Linux 代理。

创建此类型的连接器时，请指定以下设置的值：

- “**基本设置**”选项卡

  - **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。

  - **租户**（必填） – 拥有该资源的租户的名称。

  - **类型**（必填） – 连接器类型：**1c-xml**。

- **URL**（必填） — 包含需要交互的文件的目录的完整路径。例如，`/var/log/1c/logs/`。

  在文件路径中使用前缀时的限制

  指定文件路径时不能使用的前缀：

  - `/*`
  - `/bin`
  - `/boot`
  - `/dev`
  - `/etc`
  - `/home`
  - `/lib`
  - `/lib64`
  - `/proc`
  - `/root`
  - `/run`
  - `/sys`
  - `/tmp`
  - `/usr/*`
  - `/usr/bin/`
  - `/usr/local/*`
  - `/usr/local/sbin/`
  - `/usr/local/bin/`
  - `/usr/sbin/`
  - `/usr/lib/`
  - `/usr/lib64/`
  - `/var/*`
  - `/var/lib/`
  - `/var/run/`
  - `/opt/kaspersky/kuma/`

系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。

文件可通过以下路径获取：

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

- "**高级设置**"选项卡
  - **字符编码** 设置指定字符编码。默认值为 `UTF-8`。
  - **缓冲区大小**是一种设置，允许您指定在将事件发送到存储或进一步处理之前，用于在 RAM 中累积事件的缓冲区大小（以字节为单位）。

    默认值：1048576 字节 (1 MB)。

    可能的值：小于或等于 67108864 字节 (64 MB) 的正整数。
  - **轮询间隔（毫秒）**是一种设置，用于设置连接器重新读取包含文件的目录的间隔。该值以毫秒为单位。仅当文件没有更改时，连接器才会等待指定的时长。如果文件被连续修改，且轮询间隔 = 5000 毫秒，则不会按照 5 秒间隔的设定来重新读取目录中的文件，而是连续重新读取。如果文件没有更改，连接器将等待 5 秒。如果在 Web 界面中设置了 0，则使用默认值 700 毫秒。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。

连接器工作流程图：

1. 在指定目录中搜索扩展名为 XML 的 1C 日志文件。日志可以手动放置在目录中，也可以使用以 1C 语言编写的应用程序放置，例如，使用 `DownloadRegistrationLog()` 函数。连接器仅支持以这种方式接收的日志。有关如何获取 1C 日志的更多信息，请参阅官方 1C 文档。
2. 文件按上次修改时间升序排序。上次读取之前修改的所有文件都将被丢弃。

   有关已处理文件的信息存储在 /<收集器工作目录>/1c_xml_connector/state.ini 文件中，格式如下：`offset=<number>\ndev=<number>\ninode=<number>`。
3. 事件在每个未读文件中定义。
4. 文件中的事件被逐一处理。多行事件将转换为单行事件。

连接器限制：

- Windows 操作系统不支持安装带有 1c-xml 连接器的收集器。要设置 1C 日志文件的文件传输以供 KUMA 收集器处理：
  1. 在 Windows 服务器上，授予对包含 1C 日志文件的文件夹的网络读取权限。
  2. 在 Linux 服务器上，将包含 1C 日志文件的共享文件夹挂载到 Windows 服务器上（请参阅支持的操作系统列表）。
  3. 在 Linux 服务器上，安装要从已挂载的共享文件夹处理 1C 日志文件的收集器。
- 不会读取事件格式不正确的文件。例如，如果文件中的事件标签是俄语，收集器就不会读取此类事件。

包含事件的正确 XML 文件示例。

```
<?xml version="1.0" encoding="UTF-8"?>
<v8e:EventLog xmlns:v8e="http://v8.1c.ru/eventLog"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <v8e:Event>
                <v8e:Level>Information</v8e:Level>
                <v8e:Date>2022-12-07T01:55:44+03:00</v8e:Date>
                <v8e:ApplicationName>generator.go</v8e:ApplicationName>

<v8e:ApplicationPresentation>generator.go</v8e:ApplicationPresentation>
                <v8e:Event>Test event type: Count test</v8e:Event>
                <v8e:EventPresentation></v8e:EventPresentation>
                <v8e:User>abcd_1234</v8e:User>
                <v8e:UserName>TestUser</v8e:UserName>
                <v8e:Computer>Test OC</v8e:Computer>
                <v8e:Metadata></v8e:Metadata>
                <v8e:MetadataPresentation></v8e:MetadataPresentation>
                <v8e:Comment></v8e:Comment>
                <v8e:Data>
                        <v8e:Name></v8e:Name>
                        <v8e:CurrentOSUser></v8e:CurrentOSUser>
                </v8e:Data>
                <v8e:DataPresentation></v8e:DataPresentation>
                <v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus>
                <v8e:TransactionID></v8e:TransactionID>
                <v8e:Connection>0</v8e:Connection>
                <v8e:Session></v8e:Session>
                <v8e:ServerName>kuma-test</v8e:ServerName>
                <v8e:Port>80</v8e:Port>
                <v8e:SyncPort>0</v8e:SyncPort>
        </v8e:Event>
</v8e:EventLog>
```

已处理事件的示例。

```
<v8e:Event><v8e:Level>Information</v8e:Level><v8e:Date>2022-12-
07T01:55:44+03:00</v8e:Date><v8e:ApplicationName>generator.go</v8e:ApplicationName><v8e:ApplicationPresentation>generator.go
</v8e:ApplicationPresentation><v8e:Event>Test event type: Count
test</v8e:Event><v8e:EventPresentation></v8e:EventPresentation><v8e:User>abcd_1234</v8e:User><v8e:UserName>TestUser</v8e:Use
rName><v8e:Computer>Test
OC</v8e:Computer><v8e:Metadata></v8e:Metadata><v8e:MetadataPresentation></v8e:MetadataPresentation><v8e:Comment></v8e:Commen
t><v8e:Data><v8e:Name></v8e:Name><v8e:CurrentOSUser></v8e:CurrentOSUser></v8e:Data><v8e:DataPresentation></v8e:DataPresentat
ion><v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus><v8e:TransactionID></v8e:TransactionID><v8e:Connection>0</v8
e:Connection><v8e:Session></v8e:Session><v8e:ServerName>kuma-
test</v8e:ServerName><v8e:Port>80</v8e:Port><v8e:SyncPort>0</v8e:SyncPort></v8e:Event>
```

- 如果连接器读取的文件中增加了新事件，并且此文件不是目录中读取的最后一个文件，则会重新处理该文件中的所有事件。

类型 1c-log

1c-log 类型用于从 1C 应用程序技术日志中检索数据。字符串分隔符：\n。连接器仅接受多行事件记录的第一行。此类型的连接器适用于 Linux 代理。

创建此类型的连接器时，请指定以下设置的值：

- “**基本设置**”选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填） — 连接器类型：**1c-log**。
  - **URL**（必填） — 包含需要交互的文件的目录的完整路径。例如，`/var/log/1c/logs/`。

    在文件路径中使用前缀时的限制

指定文件路径时不能使用的前缀：

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。

文件可通过以下路径获取：

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

- “**高级设置**”选项卡
  - **字符编码** 设置指定字符编码。默认值为 `UTF-8`。
  - **缓冲区大小**是一种设置，允许您指定在将事件发送到存储或进一步处理之前，用于在 RAM 中累积事件的缓冲区大小（以字节为单位）。

    默认值：1048576 字节 (1 MB)。

    可能的值：小于或等于 67108864 字节 (64 MB) 的正整数。
  - **轮询间隔（毫秒）**是一种设置，用于设置连接器重新读取包含文件的目录的间隔。该值以毫秒为单位。仅当文件没有更改时，连接器才会等待指定的时长。如果文件被连续修改，且轮询间隔 = 5000 毫秒，则不会按照 5 秒间隔的设定来重新读取目录中的文件，而是连续重新读取。如果文件没有更改，连接器将等待 5 秒。如果在 Web 界面中设置了 0，则使用默认值 700 毫秒。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

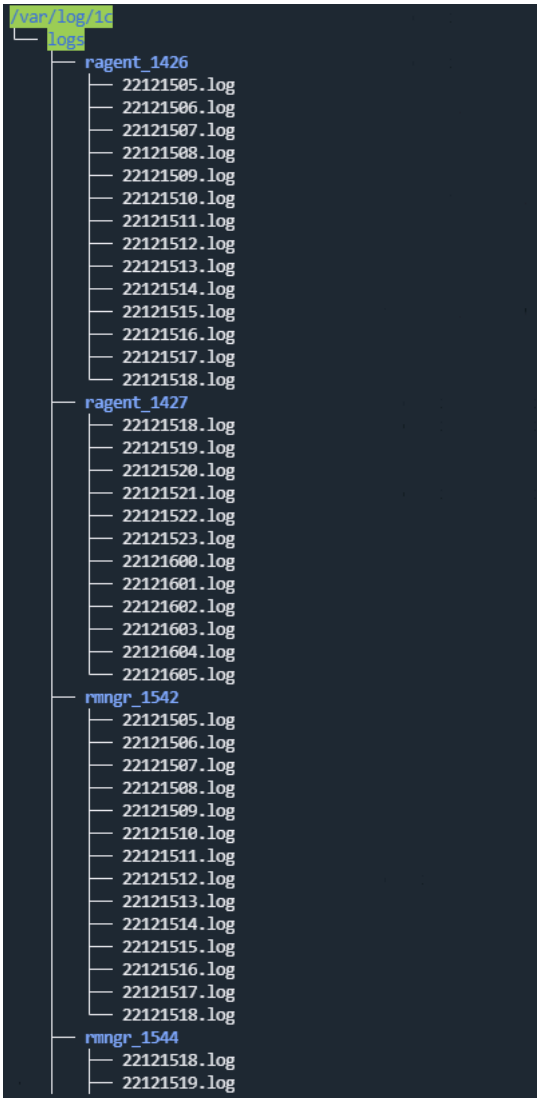
连接器工作流程图：

1. 搜索所有 1C 技术日志文件。

   日志文件要求：

   - 扩展名为 LOG 的文件在日志目录中创建（默认路径为 `/var/log/1c/logs/`），每个进程都有一个对应的子目录来存放这些文件。

支持的 1C 技术日志结构示例



- 事件将记录到文件中，持续一小时；之后会创建下一个日志文件。
- 文件名格式如下：`<YY><MM><DD><HH>.log`。例如，`22111418.log` 是 2022 年 11 月 14 日 18:00 创建的文件。
- 每个事件都采用以下格式的事件时间开头：<mm>:<ss>.<microseconds>-<duration_in_microseconds>。

2. 已处理的文件将被丢弃。

   已处理文件的相关信息存储在文件 /<收集器工作目录>/1c_log_connector/state.json 中。

3. 新事件开始处理，事件时间转换为 RFC3339 格式。

4. 队列中的下一个文件将被处理。

连接器限制：

- Windows 操作系统不支持安装带有 1c-log 连接器的收集器。要设置 1C 日志文件的文件传输以供 KUMA 收集器处理：

  1. 在 Windows 服务器上，授予对包含 1C 日志文件的文件夹的网络读取权限。
  2. 在 Linux 服务器上，将包含 1C 日志文件的共享文件夹挂载到 Windows 服务器上（请参阅支持的操作系统列表）。
  3. 在 Linux 服务器上，安装要从已挂载的共享文件夹处理 1C 日志文件的收集器。

- 仅处理多行事件记录的第一行。
- 规范化器仅处理以下类型的事件：
  - ADMIN
  - ATTN
  - CALL
  - CLSTR
  - CONN
  - DBMSSQL
  - DBMSSQLCONN
  - DBV8DBENG
  - EXCP
  - EXCPCNTX
  - HASP
  - LEAKS
  - LIC
  - MEM
  - PROC
  - SCALL
  - SCOM
  - SDBL
  - SESN
  - SINTEG

- SRVC
- TLOCK
- TTIMEOUT
- VRSREQUEST
- VRSRESPONSE

二极管类型

用于通过数据二极管传输事件。

创建此类型的连接器时，您需要定义以下设置的值：

- “**基本设置**”选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填） — 连接器类型：**二极管**。
  - **数据二极管目标目录**（必填） — KUMA 收集器服务器目录的完整路径，数据二极管将包含来自隔离网段的事件的文件移动到该目录。连接器读取这些文件后，将从目录中删除这些文件。路径最多可包含 255 个 Unicode 字符。

    在路径中使用前缀的限制

    指定文件路径时不能使用的前缀：

    - `/*`
    - `/bin`
    - `/boot`
    - `/dev`
    - `/etc`
    - `/home`
    - `/lib`
    - `/lib64`
    - `/proc`
    - `/root`
    - `/run`
    - `/sys`

- `/tmp`
- `/usr/*`
- `/usr/bin/`
- `/usr/local/*`
- `/usr/local/sbin/`
- `/usr/local/bin/`
- `/usr/sbin/`
- `/usr/lib/`
- `/usr/lib64/`
- `/var/*`
- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。

文件可通过以下路径获取：

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

- **分隔符**用于指定表示事件之间分隔符的字符。可用值：`\n`、`\t`、`\0`。如果未指定分隔符（即选择了空值），则默认值为 `\n`。

  要通过数据二极管从隔离网段转发事件时，连接器与所使用的目标资源的此项配置必须保持一致。

- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

- "**高级设置**"选项卡
  - **工作进程数** — 处理请求队列的服务数量。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
  - **轮询间隔（秒）** — 从包含来自数据二极管的事件的目录读取文件的频率。默认值是 2。以秒为单位指定该值。
  - **字符编码** 设置指定字符编码。默认值为 `UTF-8`。
  - **压缩** — 您可以使用 Snappy 压缩。默认情况下，压缩被**禁用**。

    要通过数据二极管从隔离网段转发事件，连接器与所使用的目标资源的此项设置必须保持一致。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。

Ftp 类型

创建此类型的连接器时，您需要定义以下设置的值：

- "**基本设置**"选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填）— 连接器类型：**ftp**。
  - **URL** （必填）—文件或文件掩码的实际 URL，以"ftp://"开头。对于文件掩码，您可以使用"*"、"?"、"[...]"。
    文件掩码模板

    掩码：

    - '*'—匹配任意字符序列。
    - '[' ['^'] { 字符范围 } ']'—字符类（不能为空）。
    - '?'—匹配任意单个字符。

    字符范围：

    - [0-9]—数字；
    - [a-zA-Z]—拉丁字母字符。

    示例：

    - /var/log/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log

    如果 URL 不包含 FTP 服务器端口，则插入端口 21。
  - **URL 凭证** — 用于指定 FTP 服务器的用户名和密码。如果没有用户名和密码，则该行留空。
  - **描述** — 资源描述：最多 4,000 个 Unicode 字符。
- "**高级设置**"选项卡
  - **字符编码** 设置指定字符编码。默认值为 UTF-8。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。

Sftp 类型

"**sftp**"类型的连接器用于在使用 Windows 和 Linux 代理时通过安全文件传输协议 (SFTP) 获取数据。

下表描述了“**sftp**”类型连接器的设置。

“基本设置”选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
类型	连接器类型：**sftp**。 必需设置。
标签	资源搜索的标签。 可选设置。
网址	以 `'sftp://'` 架构开头的日志文件或文件掩码的网址，例如 `sftp://example.ru:22/path/to/file.log`。您可以将 `* ? [...]` 用于文件掩码。 **文件掩码模板** 掩码： • '*'—匹配任意字符序列。 • '[' ['^'] { 字符范围 } ']'—字符类（不能为空）。 • '?'—匹配任意单个字符。 字符范围： • [0-9]—数字； • [a-zA-Z]—拉丁字母字符。 示例： • /var/log/*som?[1-9].log • /mnt/dns_logs/*/dns.log • /mnt/proxy/access*.log 如果 URL 不包含 SFTP 服务器的端口号，则会自动指定端口 `22`。 必需设置。

SSH 服务器公钥	用于在建立 SSH 连接时验证 SFTP 服务器身份的公钥。您可以指定多个不同类型的密钥，连接器将自动选择合适的密钥。
	格式：`<key_type> <base64-value>`
	密钥示例：ssh-ed25519 ABCD...
	在服务器上，公钥存储在以下路径：
	`/etc/ssh/ssh_host_*_key.pub`
	您也可以通过运行以下命令获取公钥：
	`ssh-keyscan [-p port] [-t type] [host | addrlist namelist]`
	命令示例：
	`ssh-keyscan example.com`
	`ssh-keyscan -p 2222 -t rsa,ed25519 example.com`
	必需设置。

设置	描述
Secret	存储用于连接 SFTP 服务器的凭据的 Secret。支持 **凭据**和 **SSH 私钥**类型的 Secret。Secret 必须包含用户名和密码，或 SSH 私钥。如果连接到 SFTP 服务器不需要凭据，请将用户名和密码字段留空。 您可以选择现有 Secret 或创建新 Secret。要创建新 Secret，请选择“**新建**”。 如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (🖉) 图标。 **如何创建 Secret?** *要创建密钥：* 1. 在“**名称**”字段中，输入密钥的名称。 2. 在“**用户**”和“**密码**”字段中，输入代理将用于连接到连接器的用户账户的凭证。 3. 如有必要，请在“**描述**”字段中输入密钥的描述。 4. 单击“**创建**”按钮。 密钥将添加并显示在“**密钥**”下拉列表中。 必需设置。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。
字符编码	从 SFTP 服务器接收的文件的编码。默认编码为 UTF-8。 可选设置。

smb 类型

smb 类型的连接器用于在使用 Linux 代理时通过 SMB（Server Message Block）协议接收数据。下表描述了 **smb** 类型连接器的可用设置。

“基本设置”选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
类型	连接器类型：**smb**。 必需设置。
标签	资源搜索的标签。 可选设置。
网址	远程目录路径，格式如下： • `smb://< ip_address 或 host_name >:< port >/< shared_resource_name >` • `smb://< ip_address 或 host_name >:< port >/< shared_resource_name >/< directory_path >` KUMA 仅从路径最终目录中的文件获取信息。假设您指定以下路径： `smb://< ip_address 或 host_name >:< port >/< shared_resource_name >/< directory1 >/< directory2 >` 在这种情况下，KUMA 仅从 directory2 中的文件获取信息。如果 directory2 中还有下级子目录，则不会读取这些子目录中的文件。 如果未指定端口，KUMA 将自动使用端口 445。 必需设置。

设置	描述
文件名掩码	用于筛选包含事件的文件的掩码。可使用以下通配符：“*”、“?”、“[...]”。 示例：*.json 必需设置。
Secret	用于存储连接 SMB 服务器的凭据的 Secret。支持 **credentials** 类型的 Secret。身份验证使用 NTLMv2 协议。 您可以选择现有 Secret 或创建新 Secret。要创建新 Secret，请选择“**新建**”。 如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (🖉) 图标。 **如何创建 Secret?** *要创建密钥：* 1. 在“**名称**”字段中，输入密钥的名称。 2. 在“**用户**”和“**密码**”字段中，输入代理将用于连接到连接器的用户账户的凭证。 3. 如有必要，请在“**描述**”字段中输入密钥的描述。 4. 单击“**创建**”按钮。 密钥将添加并显示在“**密钥**”下拉列表中。 必需设置。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。
缓冲区大小	在发送事件作进一步处理或存储之前，用于在服务器 RAM 中累积事件的缓冲区大小（以字节为单位）。该值必须是正整数。 最小值是 16。 最大值：67,108,864 (64 MB)。 默认缓冲区大小：1,048,576 (1 MB)；在界面中显示为 **自动**。
处理程序数	服务可以同时运行以并行处理响应规则的处理程序数量。 该值必须是正整数，最高到 999。
轮询间隔（毫秒）	连接器重新读取目录中的文件的间隔（以毫秒为单位）。默认值为 `0`。使用此值时，连接器每 700 毫秒重新读取目录中的文件。
字符编码	从 SMB 服务器接收的文件的编码。默认编码为 UTF-8。 必需设置。

Nfs 类型

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） – 拥有该资源的租户的名称。
- **类型**（必填）– 连接器类型：**nfs**。
- **URL**（必填）–远程文件夹的路径，格式为 nfs://host/path。
- **文件名掩码**（必填）– 用于筛选包含事件的文件。可以使用掩码：“*”、“?”、“[...]”。

- **轮询间隔（秒）** – 轮询间隔。在此时间间隔后从远程系统重新读取文件。以秒为单位指定该值。默认值是 0。
- **描述** – 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- **字符编码** 设置指定字符编码。默认值为 UTF-8。
- **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

vmware 类型

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） – 拥有该资源的租户的名称。
- **类型**（必填）– 连接器类型：**vmware**。
- **URL** （必填）– VMware API 可访问的 URL。URL 必须包含主机和端口。只能指定一个 URL。
- **VMware 凭证**（必填）– 存储用于连接到 VMware API 的用户名和密码的密钥。
- **客户端超时时间**是指请求未返回事件后，等待多长时间再发起新请求。以秒为单位指定该值。默认值是 5 秒。如果指定 0，则使用默认值。
- **最大事件数** – 一次请求中从 VMware API 请求的事件数。默认值是 100。最大值是 1000。
- **开始时间戳** – 您要从 VMware API 读取事件的开始日期和时间。默认值是收集器启动的时间。如果在收集器停止后启动，则从上次保存的日期开始读取事件。

“**高级设置**”选项卡

- **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。
- **字符编码** – 指定字符编码。默认值是 UTF-8。
- **TLS 模式** – 使用 PEM x509 格式的证书的 TLS 加密模式：
  - **已禁用** （默认）–不使用 TLS 加密。
  - “**已启用**”表示已使用加密，但未验证证书。
  - **自定义 CA** – 此选项要求您向收集器添加带有证书的密钥。非自签名证书。服务器的证书必须使用收集器设置中指定的证书进行签名。
- **自定义 CA** （如果为 TLS 模式设置选择了“**自定义 CA**”，则必填）是存储证书的密钥。

Wmi 类型

创建此类型的连接器时，您需要定义以下设置的值：

- "**基本设置**"选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填）— 连接器类型：**wmi**。
  - **URL** （必填）—正在创建的收集器的 URL，例如：`kuma-collector.example.com:7221`。

    在使用 Windows Management Instrumentation 创建用于接收数据的收集器时，会自动创建一个代理，该代理在远程设备上接收必要的数据，并将这些数据转发至收集器服务。您必须在 **URL** 中指定此收集器的地址。如果您已确定要在哪台服务器上安装该服务，则可以提前知道 URL。但也可以在安装向导完成后，通过从"**资源**" → "**活动服务**"部分复制 URL 数据来填写此字段。
  - **描述** — 资源描述：最多 4,000 个 Unicode 字符。
  - **默认凭证** — 无需选择任何值的下拉列表。必须在**远程主机**表中提供用于连接主机的账户凭证（见下文）。
  - **远程主机**表列出了您可以连接的远程Windows资产。可用列：
    - "**主机**"（必填）是要从中接收数据的设备的 IP 地址或名称。例如，`machine-1`。
    - **域**（必填）— 远程设备所在域的名称。例如，`example.com`。
    - **日志类型** — 用于选择需要检索的Windows日志名称的下拉列表。默认情况下，列表中仅显示预配置的日志，但您可以通过在"**Windows 日志**"字段中输入其名称，然后按下 **ENTER** 键，将自定义日志添加到列表中。为了正确处理自定义日志，KUMA 服务和资源配置可能需要进行额外调整。

      默认可用的日志包括：
      - 应用程序
      - 转发的事件
      - 安全性
      - 系统
      - 硬件事件

    如果 WMI 连接至少使用一个名称不正确的日志，则使用该连接器的代理不会接收来自此连接内所有日志的事件，即使其他日志的名称指定正确。所有日志名称均指定正确的 WMI 代理连接将正常运行。
  - **密钥** — 用于访问具有读取日志权限的远程 Windows 资产的凭证。如果将此字段留空，则使用从**默认凭证**下拉列表中选择的密钥中的凭证。必须指定密钥中的登录名而不指定域。用于访问主机的域值取自**远程主机**表的**域**列。

    您可以从下拉列表中选择密钥资源，也可以通过单击加号图标 (+) 创建密钥。可以通过点击铅笔图标 (✎) 来更改所选密钥。

- “**高级设置**”选项卡
  - **字符编码** 设置指定字符编码。默认值为 UTF-8。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

从远程设备接收事件

从托管 KUMA 代理的远程 Windows 设备接收事件的条件：

- 要在远程设备上启动 KUMA 代理，您必须使用具有“**作为服务登录**”权限的账户。
- 要接收来自 KUMA 代理的事件，您必须使用具有“事件日志读取器”权限的账户。对于域服务器，可以创建一个这样的用户账户，以便使用组策略将其读取日志的权限分配给域中的所有服务器和工作站。
- 必须在远程 Windows 设备上打开 TCP 端口 135、445 和 49152-65535。
- 您必须在远程计算机上运行以下服务：
  - 远程过程调用 (RPC)
  - RPC 端点映射器

Wec 类型

创建此类型的连接器时，您需要定义以下设置的值：

- “**基本设置**”选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填）—连接器类型：**wec**。
  - **URL** （必填）—正在创建的收集器的 URL，例如：`kuma-collector.example.com:7221`。

    在使用 Windows Event Collector 创建用于接收数据的收集器时，会自动创建一个代理，该代理在远程设备上接收必要的数据并将该数据转发至收集器服务。您必须在 **URL** 中指定此收集器的地址。如果您已确定要在哪台服务器上安装该服务，则可以提前知道 URL。但也可以在安装向导完成后，通过从“**资源**” → “**活动服务**”部分复制 URL 数据来填写此字段。
  - **描述** — 资源描述：最多 4,000 个 Unicode 字符。
  - **Windows 日志**（必需） — 从此下拉列表中选择要检索的 Windows 日志的名称。默认情况下，列表中仅显示预配置的日志，但您可以通过在“**Windows 日志**”字段中输入其名称，然后按下“**ENTER**”键，将自定义日志添加到列表中。为了正确处理自定义日志，KUMA 服务和资源配置可能需要进行额外调整。

    预配置日志：
    - 应用程序
    - 转发的事件
    - 安全性

- 系统
- 硬件事件

> 如果至少一个日志的名称指定不正确，使用连接器的代理不会从任何日志接收事件，即使其他日志的名称正确。

- “**高级设置**”选项卡
  - **字符编码** 设置指定字符编码。默认值为 UTF-8。
  - **调试** – 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

要在远程设备上启动 KUMA 代理，必须使用具有“作为服务登录”权限的服务账户。要接收来自操作系统日志的事件，服务用户账户还必须具有“事件日志读取器”权限。

您可以创建一个具有“作为服务登录”和“事件日志读取器”权限的用户账户，然后使用组策略，将此账户的日志读取权限扩展到域中的所有服务器和工作站。

建议您禁用服务账户的交互式登录。

SNMP 类型

> 要处理通过 SNMP 接收的事件，必须使用 json 规范化器。

它适用于 Windows 和 Linux 代理。支持的协议版本：

- snmpV1
- snmpV2
- snmpV3

创建此类型的连接器时，您需要定义以下设置的值：

- “**基本设置**”选项卡
  - **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填）– 拥有该资源的租户的名称。
  - **类型**（必填）– 连接器类型：**snmp**。
  - **SNMP 版本**（必填）– 此下拉列表用于选择要使用的协议版本。
  - **主机**（必填）– 主机名或其 IP 地址。可用格式：主机名、IPv4、IPv6。
  - **端口**（必填）– 用于连接到主机的端口。通常使用 161 或 162。

SNMP 版本、**主机**和**端口**设置定义与SNMP资源的一个连接。您可以通过单击**SNMP 资源**按钮来添加新连接，从而在一个连接器中创建多个这样的连接。您可以通过单击垃圾桶图标 ( ) 来删除连接。

- **密钥**（必填）— 用于选择密钥的下拉列表，该密钥用于存储通过简单网络管理协议进行连接的凭证。密钥类型必须与 SNMP 版本匹配。如果需要，可以通过在连接器创建窗口中单击加号图标 ( ) 来创建密钥。可以通过点击铅笔图标 ( ) 来更改所选密钥。
- **源数据** — 一个表格，您可以在其中指定接收数据的命名规则，并根据这些规则将OID（对象标识符）转换为规范化器可以交互的密钥。可用的表格列：
  - **参数名称**（必填）— 数据类型的任意名称。例如，`Site name` 或 `Site uptime`。
  - **OID** （必填）— 唯一标识符，用于确定在事件源中查找所需数据的位置。例如，`1.3.6.1.2.1.1.5`。
  - **密钥**（必填）— 唯一标识符，在对资产的请求做出响应时返回，包含所请求设置的值。例如，`sysName`。在规范化数据时可以访问此密钥。
  - **MAC 地址** — 如果启用此功能，KUMA 会正确解码数据，其中 OID 包含 OctetString 格式的 MAC 地址信息。解码后，MAC 地址将转换为 XX:XX:XX:XX:XX:XX 格式的字符串值。
- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

- "**高级设置**"选项卡
  - **字符编码** 设置指定字符编码。默认值为 `UTF-8`。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。

SNMP 陷阱类型

snmp-trap 连接器用于在代理和收集器中被动接收 SNMP 陷阱消息。连接器通过将 SNMP 对象 ID 映射到临时密钥来接收并准备要规范化的消息。然后，消息被传递给 JSON 规范化器，在此处临时密钥被映射到 KUMA 字段并生成事件。

要处理通过 SNMP 接收的事件，必须使用 json 规范化器。

它适用于 Windows 和 Linux 代理。支持的协议版本：

- snmpV1
- snmpV2

创建此类型的连接器时，您需要定义以下设置的值：

- "**基本设置**"选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填）— 连接器类型：**snmp-trap**。

- **SNMP 版本**（必填）— 在此下拉列表中，选择要使用的协议版本：**snmpV1**或**snmpV2**。

  例如，Windows 默认使用 **snmpV2** 版本。

- **URL**（必填）— 用于接收 SNMP 陷阱消息的 URL。可用格式：hostname:port、IPv4:port、IPv6:port、:port。

SNMP 版本和**URL**参数定义了用于接收SNMP陷阱消息的连接。您可以通过单击**SNMP 资源**按钮来添加新连接，从而在一个连接器中创建多个这样的连接。您可以通过单击 ✕ 按钮来删除连接。

- **源数据** — 一个表，您可以在其中指定接收数据的命名规则，根据该规则，OID（对象标识符）将转换为规范化器可以交互的键。

  您可以单击**应用 WinEventLog 的 OID**，用WinEventLog日志中接收的OID值映射来填充表格。如果需要在传入事件中确定和规范化更多数据，请向表中添加包含 OID 对象及其键的行。

  可用的表格列：

  - **参数名称**— 数据类型的任意名称。例如，`Site name` 或 `Site uptime`。
  - **OID**（必填）— 唯一标识符，用于确定在事件源中查找所需数据的位置。例如，`1.3.6.1.2.1.1.1`。
  - **密钥**（必填）— 唯一标识符，在对资产的请求做出响应时返回，包含所请求设置的值。例如，`sysDescr`。在规范化数据时可以访问此密钥。
  - **MAC 地址** — 如果启用此功能，KUMA 会正确解码数据，其中 OID 包含 OctetString 格式的 MAC 地址信息。解码后，MAC 地址将转换为 XX:XX:XX:XX:XX:XX 格式的字符串值。

  数据根据允许列表原则进行处理：表中未指定的对象不会发送到规范化器作进一步处理。

- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

- "**高级设置**"选项卡
  - **字符编码** 设置指定字符编码。默认值为 `UTF-8`。当从俄语本地化的 Windows 设备接收 snmp-trap 事件时，如果在事件中遇到无效字符，建议将 snmp-trap 连接器中的字符编码改为 Windows 1251。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。

配置 Windows 的 SNMP 陷阱消息源

将 Windows 设备配置为向 KUMA 收集器发送 SNMP 陷阱消息，需执行以下步骤：

1. **配置和启动 SNMP 和 SNMP 陷阱服务**
2. **配置"事件转陷阱转换器"服务**

KUMA 收集器必须接收来自 SNMP 陷阱消息源的事件，该收集器使用 snmp-trap 类型的连接器和 json 规范化器。

配置和启动 SNMP 和 SNMP 陷阱服务
要在 Windows 10 中配置和启动 SNMP 和 SNMP 陷阱服务：

1. 打开"**设置**" → "**应用**" → "**应用和功能**" → "**可选功能**" → "**添加功能**" → "**简单网络管理协议 (SNMP)**"，然后单击"**安装**"。
2. 等待安装完成后，重新启动计算机。

3. 确保 SNMP 服务正在运行。如果以下任何服务未运行，请启用该服务：

   - “**服务**” → “**SNMP 服务**”。
   - “**服务**” → “**SNMP 陷阱**”。

4. 右键单击“**服务**” → “**SNMP 服务**”，然后在上下文菜单中选择“**属性**”。指定下列设置：

   - 在“**登录**”选项卡上，选中“**本地系统账户**”复选框。
   - 在“**代理**”选项卡上，填写“**联系人**”（例如，指定 `User-win10`）和“位置”（例如，指定 `detroit`）字段。
   - 在“**陷阱**”选项卡上：
     - 在“**团体名称**”字段中，输入“**团体 public**”，然后单击“**添加到列表**”。
     - 在“**陷阱目标**”字段中，单击“**添加**”，指定部署了等待 SNMP 事件的收集器所在的 KUMA 服务器的 IP 地址或主机名，然后单击“**添加**”。
   - 在“**安全**”选项卡上：
     - 选中“**发送身份验证陷阱**”复选框。
     - 在“**接受的团体名称**”表中，单击“**添加**”，输入“**团体名称 public**”并指定“READ WRITE”作为**团体权限**。
     - 选中“**接受来自任何主机的 SNMP 数据包**”复选框。

5. 单击“**应用**”并确认您的选择。

6. 右键单击“**服务**”→ “**SNMP 服务**”并选择“**重新启动**”。

要在 Windows XP 中配置和启动 SNMP 和 SNMP 陷阱服务：

1. 打开“**开始**”→“**控制面板**”→“**添加或删除程序**”→“**添加/删除 Windows 组件**”→“**管理和监控工具**”→“**详细信息**”。

2. 选择“**简单网络管理协议**”和“**WMI SNMP 提供程序**”，然后单击“**确定**”→“**下一步**”。

3. 等待安装完成后，重新启动计算机。

4. 确保 SNMP 服务正在运行。如果以下任何服务未运行，请通过将“**启动类型**”设置为“**自动**”来启用该服务：

   - “**服务**” → “**SNMP 服务**”。
   - “**服务**” → “**SNMP 陷阱**”。

5. 右键单击“**服务**” → “**SNMP 服务**”，然后在上下文菜单中选择“**属性**”。指定下列设置：

   - 在“**登录**”选项卡上，选中“**本地系统账户**”复选框。
   - 在“**代理**”选项卡上，填写“**联系人**”（例如，指定 `User-win10`）和“位置”（例如，指定 `detroit`）字段。

- 在“**陷阱**”选项卡上：
  - 在“**团体名称**”字段中，输入“**团体 public**”，然后单击“**添加到列表**”。
  - 在“**陷阱目标**”字段中，单击“**添加**”，指定部署了等待 SNMP 事件的收集器所在的 KUMA 服务器的 IP 地址或主机名，然后单击“**添加**”。
- 在“**安全**”选项卡上：
  - 选中“**发送身份验证陷阱**”复选框。
  - 在“**接受的团体名称**”表中，单击“**添加**”，输入“**团体名称 public**”并指定“READ WRITE”作为**团体权限**。
  - 选中“**接受来自任何主机的 SNMP 数据包**”复选框。

6. 单击“**应用**”并确认您的选择。
7. 右键单击“**服务**”→ “**SNMP 服务**”并选择“**重新启动**”。

更改 SNMP 陷阱服务的端口

如有必要，您可以更改 SNMP 陷阱服务端口。

要更改 SNMP 陷阱服务的端口：

1. 打开 C:\Windows\System32\drivers\etc 文件夹。
2. 以管理员身份在记事本中打开“**services**”文件。
3. 在文件的“**服务名称**”部分，指定为“**SNMP 陷阱**”服务添加到 KUMA 收集器的 snmp-trap 连接器端口。
4. 保存该文件。
5. 打开控制面板并选择“**管理工具**” → “**服务**”。
6. 右键单击“**SNMP 服务**”并选择“**重新启动**”。

配置“事件转陷阱转换器”服务

要配置将 Windows 事件转换为 SNMP 陷阱消息的“事件转陷阱转换器”服务：

1. 在命令行中输入 `evntwin`，然后按 **Enter** 键。
2. 在“**配置类型**”下，选择“**自定义**”，然后单击“**编辑**”按钮。
3. 在“**事件源**”设置组中，单击“**添加**”按钮以查找并添加要发送到安装了 SNMP 陷阱连接器的 KUMA 收集器的事件。
4. 单击“**设置**”按钮，在打开的窗口中，选中“**不应用节流**”复选框，然后单击“**确定**”。
5. 单击“**应用**”并确认您的选择。

elastic 类型

明确支持 Elasticsearch 7.0.0 版本。

创建此类型的连接器时，您需要定义以下设置的值：

- “**基本设置**”选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填） — 连接器类型，**elastic**。
  - **URL** （必填） — Elasticsearch 服务器的有效 URL。
  - **Elastic 凭证** — 下拉列表，您可以在其中选择存储用于连接到 Elasticsearch 服务器的凭证的密钥。
  - **Elastic 指纹** — 此下拉列表用于选择一个密钥，该密钥存储两种类型的密钥：一种是用于连接 Elasticsearch 服务器的 `fingerprint` 类型，另一种是用于使用 CA 证书的 `certificate` 类型。
  - **索引**（必填） — Elasticsearch 中的索引名称。
  - **查询**（必填）— 向 Elasticsearch 进行查询。建议在查询中指定 `size` 参数，以防止 KUMA 和 Elasticsearch 出现性能问题。

    查询示例：

    ```
    "query" : { "match_all" : {} },"size" : 25
    ```

  - **排序**（必填） — 排序顺序。可能值：升序、降序。
  - **轮询间隔（秒）** — 如果前一个查询未返回任何事件，对 Elasticsearch 服务器进行查询的时间间隔（以秒为单位）。如果 Elasticsearch 在请求时包含事件，连接器将接收事件，直到从 Elasticsearch 收到所有可用事件。
  - **描述** — 资源描述：最多 4,000 个 Unicode 字符。
- “**高级设置**”选项卡
  - **字符编码** 设置用于指定字符编码。默认值是 UTF-8。
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于“**已禁用**”位置。

etw 类型

创建此类型的连接器时，您需要定义以下设置的值：

- "**基本设置**"选项卡
  - **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
  - **租户**（必填） — 拥有该资源的租户的名称。
  - **类型**（必填） — 连接器类型，**etw**。
  - **URL**（必填） — DNS 服务器的有效 URL。
  - **会话名称**（必填） — 您只能指定一个会话名称，该名称对应于Microsoft-Windows-DNSServer ETW提供者{EB79061A-A566-4698-9119-3ED2807060E7}。
  - **提取事件信息**— 如果切换开关处于关闭状态，则仅会提取无需从磁盘下载第三方元数据即可获取的最基本事件信息集。此方法有助于节省代理所在的计算机的 CPU 资源。默认情况下，将提取有关事件的所有数据。
  - **提取事件属性** — 如果切换开关处于关闭状态，则不会提取事件属性，这有助于节省代理程序所在计算机的CPU使用率。默认情况下，会提取事件属性。仅当**提取事件信息**切换开关打开时，才可以使用**提取事件属性**切换开关。
  - **描述** — 资源描述：最多 4,000 个 Unicode 字符。
- "**高级设置**"选项卡
  - **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于"**已禁用**"位置。
  - **字符编码** — 用于指定源编码为 UTF-8。建议仅当规范化事件的字段中显示乱码时才编辑此设置。默认情况下，未设置任何值。
  - **TLS 模式** — 使用 PEM x509 格式的证书的 TLS 加密模式：
    - **已禁用**（默认） — 不使用 TLS 加密。
    - **已启用** — 使用不带证书验证的加密。
    - **带验证** — 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器的文件夹 /opt/kaspersky/kuma/core/certificates/ 中。
  - **压缩** — 您可以使用 Snappy 压缩。默认情况下，压缩处于禁用状态。

universalAPI类型

universalAPI类型的连接器用于从任何支持JSON响应的REST API接收数据。

这种连接器类型仅适用于可通过用户界面进行配置的 REST API。这些连接器始终使用 **JSON** 规范化器。一个连接器只能创建一个连接。一个连接只能配置一个 URL。

universalAPI 连接器仅支持从嵌套级别为 1 的 JSON 结构中收集事件。如果响应结构包含嵌套列表（例如，一个对象列表，其中每个对象又包含另一个对象列表），则连接器不支持从此类列表中收集事件。在这种情况下，我们建议收集顶层数据并在规范化器级别处理嵌套结构。

运行收集器后，您可以通过分析其日志来测试与源的连接。如果连接出现问题或授权出现问题，收集器将在**资源和服务→活动服务**部分以黄色状态显示。

> **universalAPI** 连接器不会取代其他现有的 API 连接器，例如 **office365**。

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称** – 资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。必需设置。
- **租户** – 拥有资源的租户的名称。必需设置。
- **类型** – 连接器的类型，**universalAPI**。必需设置。
- **标签** – 用于资源搜索。
- **描述** – 资源的描述。描述的最大长度为 4,000 个 Unicode 字符。
- REST API 服务器的 **URL**。您无需指定连接协议（http 或 https）。它是根据 tlsMode 设置自动推断的。您只能指定一个 URL。必需设置。
- **请求间隔（秒）**，用于指定URL。请输入 60 到 3600 之间的数字（即 1 分钟到 60 分钟之间的数字）。默认值是 3600。
- **HTTP 方法**，用于API请求。可用值：
  - **GET**
  - **POST**
  - **PUT**
  - **DELETE**

  必需设置。
- 连接 API 的**授权**方法。以下授权方法可用：
  - **已停用**。未经授权。
  - **Plain**。登录名和密码授权。您需要使用**凭证**类型的密钥。
  - **令牌**。令牌授权。您需要使用**令牌**类型的密钥。

  有关详细信息，请参阅密钥部分。
  默认值是**已停用**。
  如果在**高级设置**选项卡上，**TLS模式**字段设置为**自定义PFX**，则**授权**字段不可用。

- 如果**授权**字段设置为**Plain**，则**密钥 ID**字段可用。您需要选择**凭证**类型的密钥。必需设置。
- 如果**授权**字段设置为**令牌**，则**令牌**字段可用。您需要选择"**令牌**"类型的密钥。必需设置。
- 如果**授权**字段设置为**令牌**，则**令牌名称**字段可用。可用值：
  - **持有人**
  - **OAuth**

  您也可以手动指定名称。必需设置。
- **查询主体**是HTTP请求的主体部分。您还可以使用变量：`$token`、`$username`、`$password`、`$identityValue`。如果启用了迭代功能，并且状态具有迭代密钥，则会自动将其替换到请求参数中。
- **JSONPath 格式的数据路径**是指API响应结构中指向对象或对象列表的数据路径。路径以JSONPath格式指定（例如，`$.data`、`$.data.edges[0].node.event`、`$.data.edges[*].node.event`）。`$` 字符会自动替换到该字段中，您无需手动输入。必需设置。
- **标识字段**切换开关允许使用唯一ID来选择事件。默认情况下，此切换开关处于关闭状态。
- 如果选中**标识字段**复选框，则**JSONPath 格式的字段路径**可用。API响应元素结构中ID字段的路径以JSONPath格式指定（例如，`$.id`）。`$` 字符会自动替换到该字段中，您无需手动输入。必需设置。
- 如果启用了**标识字段**切换开关，则**类型**字段可用。用于选择事件的 ID 字段类型。可用值：
  - **int**
  - **float**
  - **字符串**
  - **date**

  在内部，该值存储为以毫秒为单位的时间戳。必需设置。
- 如果**类型**字段设置为**date**，则**日期格式**字段可用。日期格式可以包括日期、时间、秒的小数部分和时区，例如：`YYYY-MM-DDTHH:mm:ssX`。使用指定的格式：
  - 用于解析 ID 的初始值。
  - 用于解析 REST API 响应中的 ID 值。如果日期格式包含时区，则该值将按照指定的时区进行处理。如果日期格式不包括时区，则该值将被处理为 UTC。
  - 用于为查询参数生成日期字符串（例如 `queryParams`、`headers`、`body` 中的 `$identityValue`）。如果日期格式包含时区，则字符串将以服务器的时区生成。如果日期格式不包含时区，则字符串将以 UTC 时间生成。
- 如果启用了**标识字段**切换开关，则**初始值**字段可用。身份种子以字符串形式指定，其格式与所选**类型**相对应。对于**date**类型，您需要以**日期格式**字段中指定的格式指定值。此值可以包含 Unicode 字符。最小长度是 1 个字符。
- **迭代参数**切换开关启用用于具有分阶段数据输出的API的迭代模式。默认情况下，此切换开关处于关闭状态。
- **JSONPath 格式的迭代键字段路径**是API响应元素结构中迭代密钥字段的JSONPath格式路径。`$` 字符会自动插入到字段中。必需设置。

- **迭代模式下的请求间隔（秒）**是指迭代模式下的URL轮询间隔，单位为秒。默认值为 `60`。

- **迭代键的 URL 参数**是指向API发出请求时传递迭代密钥的URL参数名称。

- **可选查询参数**是`map[string][]string`格式的附加请求参数。您还可以使用变量：`$token`、`$username`、`$password`、`$identityValue`。要添加参数，请单击**"+ 添加"**按钮，然后填写**"密钥"**和**"值"**字段。要删除参数，请选中其旁边的复选框，然后单击**"删除"**。

- **查询标头**是`map[string][]string`格式的可选HTTP请求标头。您还可以使用变量：`$token`、`$username`、`$password`、`$identityValue`。要添加参数，请单击**"+ 添加"**按钮，然后填写**"密钥"**和**"值"**字段。要删除参数，请选中其旁边的复选框，然后单击**"删除"**。

- **附加字段**是以`map[string][]string`格式添加到每个数据元素的字段。要添加字段，请单击**+添加**按钮，然后填写**字段名称**和**JSONPath**字段。要删除字段，请选中字段旁边的复选框，然后单击**"删除"**。

"**高级设置**"选项卡

- "**调试**"切换开关用于启用连接器的调试模式。默认情况下，此切换开关处于关闭状态。

- **字符编码**。默认是 **UTF-8**。

- "**代理**"用于指定连接到 API 时所需的代理服务器设置（如果需要）。您可以选择现有的代理服务器或创建新的代理服务器。

- **TLS 模式**。使用 TLS 加密时，您不能在"基本设置"**基本设置URL** 字段中指定 IP 地址。可用值：

  - "**已禁用**"表示不使用 TLS 加密。默认选择此值。

  - "**已启用**"表示已使用 TLS 加密，但未验证证书。

  - "**自定义 CA**"启用 TLS 加密，并验证由证书颁发机构签名的证书。如果选择此值，请在**"自定义 CA"**下拉列表中指定一个由证书颁发机构签名的证书的密钥。您可以选择现有 Secret 或创建新 Secret。要创建新 Secret，请选择"**新建**"。

    如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (✎) 图标。

    如何创建由证书颁发机构签名的证书?

    您可以在 KUMA Core 服务器上创建 CA 签名的证书（以下命令示例使用 OpenSSL）。

    要创建由证书颁发机构签名的证书：

    1. 生成证书签发机构要使用的密钥，例如：

       ```
       openssl genrsa -out ca.key 2048
       ```

    2. 为生成的密钥创建证书，例如：

       ```
       openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 证书颁发机构的通用主机名 >"
       -out ca.crt
       ```

    3. 创建私钥并请求证书签发机构对其进行签名，例如：

       ```
       openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 服务器的通
       用主机名 >" -out server.csr
       ```

4. 创建由证书签发机构签名的证书。您需要在 `subjectAltName` 变量中包含要为其创建证书的服务器的域名或 IP 地址，例如：

   ```
   openssl x509 -req -extfile <(printf
   "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in
   server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. 在 Open Single Management Platform Web 界面中，将创建的 `server.crt` 证书上传到 **证书** 类型的密钥，然后在 **自定义 CA** 下拉列表中选择 **证书** 类型的密钥。

- **自定义 PFX**使用 PFX 密钥启用 TLS 加密。您必须生成一个包含私钥的 PFX 证书（采用 PKCS#12 容器格式），然后将该 PFX 证书作为 PFX 密钥上传到 OSMP 控制台。如果选择此值，请在“**自定义 PFX**”下拉列表中指定由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择“**新建**”。

  如果要编辑现有 Secret 的设置，请单击旁边的铅笔 (✎) 图标。

  如何创建 PFX 密钥?

  要创建 PFX 密钥：

  1. 在“**名称**”字段中，输入 PFX 密钥的名称。
  2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。
  3. 在**“密码”**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。
  4. 然后单击**创建**按钮。

     PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。

- **请求超时时间（秒）**是指等待API请求响应的时间，以秒为单位。默认响应超时是 30 秒。
- **请求重试次数**是指发生错误时重复尝试发出请求的次数。默认值为 `1`。
- “**重试间隔（秒）**”是指两次请求重试之间的间隔，以秒为单位。默认值为 `0`。

promtail类型

Promtail连接器用于从OSMP组件传输审计事件。

创建此类型的连接器时，您需要定义以下设置的值：

“**基本设置**”选项卡

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） — 拥有该资源的租户的名称。
- **类型**（必填）—连接器类型，promtail。

- **URL** （必填）— 您需要连接到的 URL。可用格式：hostname:port、IPv4:port、IPv6:port、:port。

  您可以按以下格式指定 IPv6 地址：`[<IPv6 address>%<interface>:<port number>`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。您可以添加多个 URL 或删除一个 URL。如果URL字段包含制表符或空格字符，KUMA不允许保存资源或服务。要添加 URL，请单击“**+ 添加**”按钮。要删除 URL，请单击旁边的删除 (×) 图标。

- **描述** — 资源描述：最多 4,000 个 Unicode 字符。

“**高级设置**”选项卡

- **调试** — 切换开关，用于指定是否必须启用资源日志记录。默认情况下，此切换开关处于关闭状态。
- **字符编码** 设置项指定字符编码。默认值是 UTF-8。
- **TLS 模式** — 使用 PEM x509 格式的证书的 TLS 加密模式：
  - **已禁用**（默认）—不使用TLS加密。
  - **已启用** — 使用不带证书验证的加密。
  - **使用验证** — 使用加密并验证证书时是否使用KUMA根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器的文件夹 /opt/kaspersky/kuma/core/certificates/ 中。
  - **自定义PFX** —使用加密。选择此选项后，必须在外部证书颁发机构中生成证书，该证书需包含私钥且采用 PKCS#12 容器格式。然后，证书必须从密钥库导出，并作为PFX密钥上传到OSMP控制台。**添加 PFX 密钥**。

    要创建 PFX 密钥：

    1. 在“**名称**”字段中，输入 PFX 密钥的名称。
    2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。
    3. 在**“密码”**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。
    4. 然后单击**创建**按钮。

    PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。

    使用 TLS 时，无法将 IP 地址指定为 URL。
  - **带客户端身份验证的自定义 PFX** 是指使用 PFX 密钥进行 TLS 加密。在此模式下，客户端将使用证书进行身份验证。

    您必须使用PKCS#12容器格式的私钥生成PFX证书，然后将PFX证书作为PFX密钥上传到OSMP网页界面。如果选择此值，请在 PFX 密钥下拉列表中指定由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择“**新建**”。

    如果要编辑现有密钥的设置，请单击旁边的铅笔图标。

http-streaming 类型

http-streaming 类型的连接器用于在使用 Windows 和 Linux 代理时通过 HTTP 接收事件。

连接器接受 HTTP 请求，并按如下方式处理请求正文：读取请求正文（并在必要时进行解压缩），将正文拆分为事件，然后逐个发送事件进行处理。这种处理方法有助于减少内存使用，但当少量来源产生大量事件时，连接器的性能可能会降低。

http-streaming 类型连接器的设置如下表所述。

“基本设置”选项卡

设置	描述
名称	连接器的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	连接器所属租户的名称。 必需设置。
类型	连接器类型：**http-streaming**。 必需设置。
标签	用于搜索连接器的标签。 可选设置。
网址	URL（必需）—需要连接到的 URL。您可以按以下格式之一输入 URL： • `< 主机名 >:< 端口号 >` • `< IPv4 地址 >:< 端口号 >` • `< IPv6 地址 >:< 端口号 >` 要将事件源中的数据发送到连接器，指定的 URL 必须以 `/input` 结尾。 必需设置。
分隔符	标志着事件之间界限的字符： • **\n** • **\t** • **\0** 如果您未在此下拉列表中选择值，则默认选择空值。在这种情况下，连接器不会将一个事件拆分成多个事件，而是原封不动地将其传递给规范化器。
缓冲区大小	设置单个事件的最大大小（以字节为单位）。事件的最大大小为 1 字节。 如果 HTTP 请求正文中没有分隔符，则整个请求正文将被视为一个事件。在这种情况下，缓冲区大小必须大于请求正文的大小。 我们建议根据最大事件的大小（而不是一批事件的大小）设置缓冲区大小，并留出至少 2 字节的安全余量。 默认值：4096 字节（4 KB）。最大值：67108864 字节（64 MB）。 如果设置为 0，则使用默认值。
描述	连接器的描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
调试	此切换开关用于启用或禁用资源的日志记录。默认情况下，此切换开关处于关闭状态。
字符编码	字符编码。默认是 UTF-8。

设置	描述
TLS 模式	TLS 加密模式。使用 TLS 加密时，您不能在“基本设置”的 **URL** 字段中指定 IP 地址。可用值： • “**已禁用**”表示不使用 TLS 加密。默认选择此值。 • “**已启用**”表示已使用 TLS 加密，但未验证证书。 • **自定义 PFX** 指的是使用 PFX 密钥的 TLS 加密。您必须生成一个包含 PKCS#12 容器格式的私钥的 PFX 证书，然后将该 PFX 证书作为 PFX 密钥上传到 KUMA Web 界面。如果选择此值，请在“**带有客户端身份验证的自定义 PFX**”下拉列表中指定一个包含由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择“**新建**”。 如果要编辑现有密钥的设置，请单击旁边的铅笔图标。 **如何创建 PFX 密钥?** *要创建 PFX 密钥：* 1. 在“**名称**”字段中，输入 PFX 密钥的名称。 2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。 3. 在“**密码**”字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。 4. 然后单击**创建**按钮。 PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。 • **带客户端身份验证的自定义 PFX** 是指使用 PFX 密钥进行 TLS 加密。在此模式下，客户端将使用证书进行身份验证。 您必须生成一个包含 PKCS#12 容器格式的私钥的 PFX 证书，然后将该 PFX 证书作为 PFX 密钥上传到 KUMA Web 界面。如果选择此值，请在“**带有客户端身份验证的自定义 PFX**”下拉列表中指定一个包含由证书颁发机构签名的证书的 PFX 密钥。您可以选择现有的 PFX 密钥或创建新的 PFX 密钥。要创建新 PFX 密钥，请选择“**新建**”。 如果要编辑现有密钥的设置，请单击旁边的铅笔图标。 **如何创建 PFX 密钥?** *要创建 PFX 密钥：* 1. 在“**名称**”字段中，输入 PFX 密钥的名称。 2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。 3. 在“**密码**”字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。 4. 然后单击**创建**按钮。 PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。
队列中的传入请求数量	连接器可同时处理的最大 HTTP 请求数。 达到指定限制时，新的 HTTP 请求将被拒绝，并返回代码 `429 Too Many Requests`。被拒绝的请求的正文不会被处理。 实际同时处理的请求数取决于此设置的值以及收集器上通过“**工作进程**”设置指定的工作进程数。 默认值是 32768。最大值是 65535。 如果设置为 0，则使用默认值。 增大此值可以同时处理更多请求，但可能会增加内存使用量。

预定义连接器

下表列出的连接器包含在 OSMP 分发包中。

预定义连接器

连接器名称	注释
[OOTB] Continent SQL	从 Continent 硬件和软件加密系统的数据库中获取事件。 要使用它，您必须配置相应密钥类型的设置。
[OOTB] InfoWatch Trafic Monitor SQL	从 InfoWatch Traffic Monitor 系统的数据库中获取事件。 要使用它，您必须配置相应密钥类型的设置。
[OOTB] KSC MSSQL	从 Kaspersky Security Center 应用程序的 MS SQL 数据库中获取事件。 要使用它，您必须配置相应密钥类型的设置。
[OOTB] KSC MySQL	从 Kaspersky Security Center 应用程序的 MySQL 数据库中获取事件。 要使用它，您必须配置相应密钥类型的设置。

[OOTB] KSC PostgreSQL	从 Kaspersky Security Center 15.0 应用程序的 PostgreSQL 数据库中获取事件。 要使用它，您必须配置相应密钥类型的设置。
[OOTB] Oracle Audit Trail SQL	从 Oracle 数据库中获取审计事件。 要使用它，您必须配置相应密钥类型的设置。
[OOTB] SecretNet SQL	从 SecretNet SQL 数据库中获取事件。 要使用它，您必须配置相应密钥类型的设置。

目标位置

目标位置定义用于发送规范化事件的网络设置。收集器和关联器使用目标位置来指定已处理事件的发送位置。目标位置通常是关联器和存储器。

目标位置的设置在两个选项卡上配置：**基本设置**和**高级设置**。可用设置取决于所选的目标位置类型：

- **内部** — 用于使用"内部"协议从 KUMA 服务接收数据。
- **nats-jetstream** — 用于 NATS 通信。
- **tcp** — 用于 TCP 通信。
- **udp**— 用于通过UDP进行通信。
- **http** — 用于 HTTP 通信。
- **diode** — 用于使用数据二极管传输事件。
- **kafka** — 用于 Kafka 通信。
- **file** — 用于写入文件。
- **存储** — 用于将数据传输到存储。
- **关联器** — 用于将数据传输到关联器。
- **事件路由器** — 用于将事件发送到事件路由器。

目标位置，内部类型

内部类型的目标位置用于通过"内部"协议接收来自 KUMA 服务的数据。您可以使用内部协议传输以下数据：

- 内部数据，例如事件路由。
- 文件属性。如果在创建收集器期间，您在安装过程的传输步骤中指定了文件类型的连接器、1c-xml或1c-log，则在事件解析步骤的**映射**表中，您可以使用 KUMA 事件字段传递收集器所处理文件的名称或路径。为此，需要在"**源**"列中，指定以下值之一：
  - `$kuma_fileSourceName` 用于在 KUMA 事件字段中传入收集器正在处理的文件名。
  - `$kuma_fileSourcePath` 用于在 KUMA 事件字段中传入收集器正在处理的文件路径。

当您使用“**文件**”、“**1c-xml**”或“**1c-log**”连接器时，规范化器中的新变量将仅适用于**内部类型的目标位置**。

- 事件发送到事件路由器。事件路由器只能通过“内部”协议接收事件，因此在将事件发送到事件路由器时只能使用“**内部**”类型的目标位置。

下表描述了“**内部**”类型目标位置的设置。

“基本设置”选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
状态	此切换开关用于将事件发送到目标位置。默认情况下，此切换开关处于开启状态。
类型	目标位置类型：**内部**。 必需设置。
网址	URL（必填）—需要连接到的 URL。支持以下 URL 格式： • `< 主机名 >:< 端口号 >` • `< IPv4 地址 >:< 端口号 >` • `< IPv6 地址 >:< 端口号 >` 您可以按以下格式指定 IPv6 地址：`[< IPv6 地址 >%< 接口 >:< 端口号 >`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以添加多个 URL，也可以删除一个 URL。如果 URL 字段包含制表符或空格字符，KUMA 不允许保存资源或服务。要添加 URL，请单击“**+ 添加**”按钮。要删除 URL，请单击旁边的删除 (✕) 图标。 必需设置。
标签	资源搜索的标签。 可选设置。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
缓冲区大小	在发送事件作进一步处理或存储之前，用于在服务器 RAM 中累积事件的缓冲区大小（以字节为单位）。该值必须是正整数。默认缓冲区大小：67,108,864（64MB），在界面中显示为0。
缓冲区刷新间隔	向目标位置发送事件的间隔（以秒为单位）。默认值是 1 秒。
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。默认值：10GB，在界面中显示为0。
处理程序	服务可以同时运行以并行处理响应规则的处理程序数量。 该值必须是正整数，最高到 999。
代理服务器	目标位置的代理服务器。您可以选择现有的代理服务器或创建新的代理服务器。要创建新的代理服务器，请选择“**新建**”。 如果要编辑现有代理服务器的设置，请单击旁边的铅笔 (🖉) 图标。

设置	描述
URL 选择策略	如果您在“**基本设置**”选项卡的“**URL**”字段中添加了多个 URL，确定必须优先将事件发送到哪些 URL 的方法： • “**任意**”表示只要 URL 接受事件，事件就会发送到随机选择的可用 URL。如果该 URL 不可用，事件就会发送到另一个随机选择的可用 URL。默认选择此值。 • “**首选第一个**”表示事件会优先发送到第一个添加的 URL。如果该 URL 变得不可用，事件就会发送到下一个添加的可用 URL。如果第一个添加的 URL 重新变得可用，事件会再次发送到第一个添加的 URL。 • “**轮询**”表示事件在可用的 URL 之间均匀分布。此方法不能保证事件在 URL 之间均匀分布，因为缓冲区可能发生溢出或事件可能会发送到目标位置。您可以在“**缓冲区大小限制**”字段中指定缓冲区大小（以字节为单位）；您还可以在“**缓冲区刷新间隔**”字段中指定将事件发送到目标的间隔（以秒为单位）。
健康检查超时	检查目标位置健康状况的间隔（以秒为单位）。
磁盘缓冲区已禁用	此切换开关用于启用磁盘缓冲区。默认情况下，此切换开关处于开启状态。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。您可以在“**磁盘缓冲区大小限制**”字段中指定磁盘缓冲区的大小。如果磁盘缓冲区的可用空间不足，新的规范化事件将从最早的事件开始覆盖旧的规范化事件。
超时	目标位置等待其他服务或组件响应的时间（以秒为单位）。
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。

设置	描述
过滤器	用于确定资源必须处理哪些事件的过滤器。您可以选择现有过滤器或创建新过滤器。要创建新过滤器，请选择“**新建**”。 如果要编辑现有过滤器的设置，请单击旁边的铅笔 (🖉) 图标。 **如何创建过滤器?** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**“条件”**下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是**”。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“🔗”按钮查看嵌套过滤器设置。

设置	描述

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

Nats-jetstream 类型

“**nats-jetstream**”类型用于 NATS 通讯。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**nats-jetstream**。
网址	必需设置。 要连接到的 URL。
主题	必需设置。 NATS 消息的主题。必须包含 Unicode 字符。
分隔符	指定一个字符，用于定义一个事件的结束位置和另一个事件的开始位置。默认情况下，使用 `\n`。

设置	描述
授权	连接到指定 URL 时的授权类型 可能值： • "**已禁用**"是默认值。 • **纯文本**：如果选择此选项，则必须指明包含用户账户凭证的密钥，以便在连接到连接器时进行授权。 **添加密钥** *要创建密钥：* 1. 在"**名称**"字段中，输入密钥的名称。 2. 在"**用户**"和"**密码**"字段中，输入代理将用于连接到连接器的用户账户的凭证。 3. 如有必要，请在"**描述**"字段中输入密钥的描述。 4. 然后单击**创建**按钮。 密钥将添加并显示在"**密钥**"下拉列表中。
描述	资源描述：最多 4,000 个 Unicode 字符。

"高级设置"选项卡

设置	描述
压缩	您可以使用 Snappy 压缩。默认情况下，压缩处于**禁用**状态。
缓冲区大小	设置缓冲区的大小。 默认值是 1 KB，最大值为 64 MB。
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。
集群 ID	NATS 集群的 ID。
输出格式	将事件发送到外部目标位置的格式。可用值： • JSON • CEF 如果选择 CEF 格式，则发送的事件包含 CEF 标头和仅非空字段。

设置	描述

TLS 模式	使用 TLS 加密。可用值：
	• **已禁用**（默认）表示不使用 TLS 加密。
	• "**已启用**"表示使用加密，但不验证证书。
	• **带验证** – 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。
	• "**自定义 CA**"表示使用加密并验证证书是否由证书颁发机构签名。从"**自定义 CA**"下拉列表中可选择包含证书的密钥，选择此选项时会显示该列表。
	创建由证书颁发机构签名的证书
	您可以在 KUMA Core 服务器上创建 CA 签名的证书（以下命令示例使用 OpenSSL）。
	要创建由证书颁发机构签名的证书：
	1. 生成证书签发机构要使用的密钥，例如：
	`openssl genrsa -out ca.key 2048`
	2. 为生成的密钥创建证书，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 证书颁发机构的通用主机名 >" -out ca.crt`
	3. 创建私钥并请求证书签发机构对其进行签名，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 服务器的通用主机名 >" -out server.csr`
	4. 创建由证书签发机构签名的证书。您需要在 `subjectAltName` 变量中包含要为其创建证书的服务器的域名或 IP 地址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform Web 界面中，将创建的 `server.crt` 证书上传到 **证书** 类型的密钥，然后在 **自定义 CA** 下拉列表中选择 **证书** 类型的密钥。
	使用 TLS 时，无法将 IP 地址指定为 URL。

分隔符	在下拉列表中，您可以选择用于标记事件之间分隔的字符。默认情况下，使用 `\n`。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是"**已禁用**"。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受"**磁盘缓冲区大小限制**"设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在"**过滤器**"部分，您可以指定识别资源必须处理的事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是**"。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

Tcp 类型

“**tcp**”类型用于 TCP 通讯。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**tcp**。
网址	必需设置。 要连接到的 URL。可用格式： `host:port`、 `IPv4:port`、 `:port`。 IPv6 地址也受到支持。使用 IPv6 地址时，您还必须按照 `[address%interface]:port` 格式指定接口。 例如， `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`)。
描述	资源描述：最多 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
压缩	您可以使用 Snappy 压缩。默认情况下，压缩处于**禁用**状态。
缓冲区大小	设置缓冲区的大小。 默认值为 1 KB，最大值为 64 MB。
超时	等待另一个服务或组件响应的时间（以秒为单位）。 默认值为 `30`。
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。

设置	描述
输出格式	将事件发送到外部目标位置的格式。可用值： • JSON • CEF 如果选择 CEF 格式，则发送的事件包含 CEF 标头和仅非空字段。
TLS 模式	使用 pem x509 格式证书的 TLS 加密模式。可用值： • “**已禁用**”表示不使用 TLS 加密。默认值。 • **已启用** – 使用不带证书验证的加密。 • **自定义CA**表示使用加密，并验证您提供的证书文件。选择此值后，将显示**自定义CA**附加参数。使用此参数指定证书。 • **自定义PFX**表示使用加密，并验证您提供的PFX格式证书。选择此值后，将显示**PFX密钥**附加参数。使用此参数指定证书。 使用 TLS 时，无法将 IP 地址指定为 URL。
自定义CA	此字段允许您选择包含证书文件的证书类型密钥。您可以选择现有密钥或新建密钥。要新建密钥，请选择**新建**值，然后在打开的窗口中上传TLS证书文件。
PFX密钥	此字段允许您选择包含证书文件的PFX类型密钥。您可以选择现有密钥或新建密钥。要新建密钥，请选择**新建**值，然后在打开的窗口中上传包含TLS证书的PFX文件。
分隔符	在下拉列表中，您可以选择用于标记事件之间分隔的字符。默认情况下，使用 `\n`。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是“**已禁用**”。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受“**磁盘缓冲区大小限制**”设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在此部分中，您可以指定识别资源必须处理的事件的标准。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是**"。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

udp 类型

udp 类型的目标位置用于 UDP 通信。下表描述了“**udp**”类型目标位置的设置。

“基本设置”选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
状态	此切换开关用于将事件发送到目标位置。默认情况下，此切换开关处于开启状态。
类型	目标位置类型，**udp**。 必需设置。
网址	URL（必填）—需要连接到的 URL。支持以下 URL 格式： • `< 主机名 >:< 端口号 >` • `< IPv4 地址 >:< 端口号 >` • `< IPv6 地址 >:< 端口号 >` 您可以按以下格式指定 IPv6 地址：`[< IPv6 地址 >%< 接口 >:< 端口号 >`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以添加多个 URL，也可以删除一个 URL。如果 **URL** 字段包含制表符或空格字符，您无法保存资源或服务。要添加 URL，请单击“**+添加**”按钮。要删除 URL，请单击旁边的删除 (✕) 图标。 必需设置。
标签	资源搜索的标签。 可选设置。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
缓冲区大小	在发送事件作进一步处理或存储之前，用于在服务器 RAM 中累积事件的缓冲区大小（以字节为单位）。该值必须是正整数。默认缓冲区大小：67,108,864（64MB），在界面中显示为0。
缓冲区刷新间隔	向目标位置发送事件的间隔（以秒为单位）。默认值是 1 秒。

设置	描述
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。默认值：10GB，在界面中显示为0。
处理程序	服务可以同时运行以并行处理响应规则的处理程序数量。 该值必须是正整数，最高到 999。
输出格式	事件发送到目标位置的格式： • JSON。 • CEF。如果选择此值，则传输的事件包含 CEF 标头和仅非空字段。 • Syslog-CEF
TLS 模式	TLS 加密模式。使用 TLS 加密时，您不能在“基本设置”**基本设置URL** 字段中指定 IP 地址。可用值： • “**已禁用**”表示不使用 TLS 加密。默认选择此值。 • “**已启用**”表示已使用 TLS 加密，但未验证证书。 • “**带验证**”表示使用 TLS 加密并验证证书是否使用 KUMA 根证书进行签名。KUMA 的根证书和密钥在应用程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 目录中。 已过时的加密模式，已弃用。
压缩	用于配置 Snappy 压缩的下拉列表： • **已禁用**。默认选择此值。 • **使用 Snappy**。
URL 选择策略	如果您在“**基本设置**”选项卡的“**URL**”字段中添加了多个 URL，确定必须优先将事件发送到哪些 URL 的方法： • “**任意**”表示只要 URL 接受事件，事件就会发送到随机选择的可用 URL。如果该 URL 不可用，事件就会发送到另一个随机选择的可用 URL。默认选择此值。 • “**首选第一个**”表示事件会优先发送到第一个添加的 URL。如果该 URL 变得不可用，事件就会发送到下一个添加的可用 URL。如果第一个添加的 URL 重新变得可用，事件会再次发送到第一个添加的 URL。 • “**轮询**”表示事件在可用的 URL 之间均匀分布。此方法不能保证事件在 URL 之间均匀分布，因为缓冲区可能发生溢出或事件可能会发送到目标位置。您可以在“**缓冲区大小限制**”字段中指定缓冲区大小（以字节为单位）；您还可以在“**缓冲区刷新间隔**”字段中指定将事件发送到目标的间隔（以秒为单位）。
分隔符	标志着事件之间界限的字符： • \n • \t • \0 如果您未在此下拉列表中选择值，则默认选择空值。在这种情况下，连接器不会将一个事件拆分成多个事件，而是原封不动地将其传递给规范化器。
磁盘缓冲区已禁用	此切换开关用于启用磁盘缓冲区。默认情况下，此切换开关处于开启状态。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。您可以在“**磁盘缓冲区大小限制**”字段中指定磁盘缓冲区的大小。如果磁盘缓冲区的可用空间不足，新的规范化事件将从最早的事件开始覆盖旧的规范化事件。
超时	目标位置等待其他服务或组件响应的时间（以秒为单位）。
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。

设置	描述
过滤器	用于确定资源必须处理哪些事件的过滤器。您可以选择现有过滤器或创建过滤器。要创建新过滤器，请选择“**新建**”。 如果要编辑现有过滤器的设置，请单击旁边的铅笔 (🖉) 图标。 **如何创建过滤器?** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**“条件”**下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“🔗”按钮查看嵌套过滤器设置。

设置	描述

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

Http 类型

“**http**”类型用于 HTTP 通讯。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**http**。
网址	必需设置。 要连接到的 URL。 可用格式：`host:port`、`IPv4:port`、`:port`。 也支持 IPv6 地址，但是使用 IPv6 地址时，还必须指定接口：`[address%interface]:port`。 示例：`[fe80::5054:ff:fe4d:ba0c%eth0]:4222`）。
授权	连接到指定 URL 时的授权类型 可能值： • “**已禁用**”是默认值。 • **明文** – 如果选择此选项，则必须指明包含用户账户凭证的密钥，以便在连接到连接器时进行授权。 **添加密钥** *要创建密钥：* 1. 在“**名称**”字段中，输入密钥的名称。 2. 在“**用户**”和“**密码**”字段中，输入代理将用于连接到连接器的用户账户的凭证。 3. 如有必要，请在“**描述**”字段中输入密钥的描述。 4. 然后单击**创建**按钮。 密钥将添加并显示在“**密钥**”下拉列表中。
描述	资源描述：最多 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
压缩	您可以使用 Snappy 压缩。默认情况下，压缩处于**禁用**状态。
缓冲区大小	设置缓冲区的大小。 默认值为 1 KB，最大值为 64 MB。
超时	等待另一个服务或组件响应的时间（以秒为单位）。 默认值为 `30`。
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。
输出格式	将事件发送到外部目标位置的格式。可用值： • JSON • CEF 如果选择 CEF 格式，则发送的事件包含 CEF 标头和仅非空字段。

TLS 模式	使用 TLS 加密。可用值：
	• **已禁用** （默认）表示不使用 TLS 加密。
	• “**已启用**”表示使用加密，但不验证证书。
	• **带验证** – 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。
	• “**自定义 CA**”表示使用加密并验证证书是否由证书颁发机构签名。从“**自定义 CA**”下拉列表中可选择包含证书的密钥，选择此选项时会显示该列表。
	创建由证书颁发机构签名的证书
	您可以在 KUMA Core 服务器上创建 CA 签名的证书（以下命令示例使用 OpenSSL）。
	要创建由证书颁发机构签名的证书：
	1. 生成证书签发机构要使用的密钥，例如：
	`openssl genrsa -out ca.key 2048`
	2. 为生成的密钥创建证书，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 证书颁发机构的通用主机名 >" -out ca.crt`
	3. 创建私钥并请求证书签发机构对其进行签名，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 服务器的通用主机名 >" -out server.csr`
	4. 创建由证书签发机构签名的证书。您需要在 `subjectAltName` 变量中包含要为其创建证书的服务器的域名或 IP 地址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform Web 界面中，将创建的 `server.crt` 证书上传到 **证书** 类型的密钥，然后在 **自定义 CA** 下拉列表中选择 **证书** 类型的密钥。
	使用 TLS 时，无法将 IP 地址指定为 URL。

URL 选择策略	如果指定了多个 URL，您可以从下拉列表中选择决定将事件发送到哪个 URL 的方法。可用值： • **任何**。只要此 URL 可以接收事件，就会将事件发送到其中一个可用的 URL。如果连接断开（例如，接收节点断开连接），将选择其他 URL 作为事件目标位置。 • **第一个优先**。事件将发送到所添加地址列表中的第一个 URL。如果该 URL 不可用，则事件将按顺序发送到下一个可用节点。当第一个 URL 再次可用时，将再次开始向其发送事件。 • **均衡**意味着包含事件的包会在列表中所有可用的 URL 之间进行平均分配。由于数据包是在目标位置缓冲区溢出或刷新计时器触发时发送的，因此该 URL 选择策略无法保证事件均匀分布到目标位置。
分隔符	在下拉列表中，您可以选择用于标记事件之间分隔的字符。默认情况下，使用 \n。
路径	必须为 URL 请求添加的路径。例如，如果指定路径 `/input`，并输入 `10.10.10.10` 作为 URL，则会从目标位置发送对 `10.10.10.10/input` 的请求。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	正在处理队列的服务数量。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。

设置	描述
健康检查路径	用于发送请求以获取有关目标位置资源所连接的系统健康信息的 URL。
健康检查超时	健康检查的频率（以秒为单位）。
健康检查已禁用	禁用健康检查的复选框。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是“**已禁用**”。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受“**磁盘缓冲区大小限制**”设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在"**过滤器**"部分，您可以指定识别资源必须处理的事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是**"。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

二极管类型

“**二极管**”类型用于通过数据二极管传输事件。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**二极管**。

设置	描述
数据二极管源目录	必需设置。 数据二极管将事件从中移出的目录。路径最多可包含 255 个 Unicode 字符。 **在 Windows 服务器上的路径中使用前缀时的限制** 在 Windows 服务器上，必须指定目录的绝对路径。不能使用名称与以下正则表达式匹配的目录： • `^[a-zA-Z]:\\Program Files` • `^[a-zA-Z]:\\Program Files \(x86\)` • `^[a-zA-Z]:\\Windows` • `^[a-zA-Z]:\\Program Files\\Kaspersky Lab\\KUMA` **在 Linux 服务器上的路径中使用前缀时的限制** 指定文件路径时不能使用的前缀： • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` 系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。 文件可通过以下路径获取： • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/`

设置	描述
临时目录	准备将事件传输到数据二极管的目录。 当发生超时（默认为 10 秒）或缓冲区溢出时，事件存储在文件中。准备好的文件将移动到"**数据二极管源目录**"字段中指定的目录。文件内容的校验和（SHA256）用作包含事件的文件的名称。 临时目录必须与数据二极管源目录不同。
描述	资源描述：最多 4,000 个 Unicode 字符。

"高级设置"选项卡

设置	描述
压缩	您可以使用 Snappy 压缩。默认情况下，压缩处于**禁用**状态。 要通过数据二极管从隔离网段转发事件，连接器与所使用的目标资源的此项设置必须保持一致。
缓冲区大小	设置缓冲区的大小。 默认值是 1 KB，最大值为 64 MB。
分隔符	在下拉列表中，您可以选择用于标记事件之间分隔的字符。默认情况下，使用 `\n`。 要通过数据二极管从隔离网段转发事件时，连接器与所使用的目标资源的此项设置必须保持一致。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是"**已禁用**"。

设置	描述
过滤器	在"**过滤器**"部分，您可以指定识别资源必须处理的事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是** 。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

Kafka 类型

“**kafka**”类型用于 Kafka 通讯。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**kafka**。
网址	必需设置。 要连接到的 URL。可用格式： `host:port`、 `IPv4:port`、 `:port`。也支持 IPv6 地址，但是使用 IPv6 地址时，还必须指定接口： `[address%interface]:port`。 示例： `[fe80::5054:ff:fe4d:ba0c%eth0]:4222` ）。 您可以通过单击“URL”按钮来添加多个地址。
主题	必需设置。 Kafka 消息的主题。必须包含 1 到 255 个以下字符中：a–z、A–Z、0–9、“.”、“_”、“-”。
分隔符	指定一个字符，用于定义一个事件的结束位置和另一个事件的开始位置。默认情况下，使用 `\n`。

设置	描述
授权	连接到指定 URL 时的授权类型 可能值： • “**已禁用**”是默认值。 • **PFX** — 必须在外部证书颁发机构中使用 PKCS#12 容器格式的私钥生成证书。然后，必须将证书从密钥库中导出，并将其作为 PFX 机密上传到 KUMA 控制台。 • **添加 PFX 密钥** *要创建 PFX 密钥：* 1. 在“**名称**”字段中，输入 PFX 密钥的名称。 2. 单击“**上传 PFX**”并选择将带有私钥的 PFX 文件导出至的 PKCS#12 容器文件。 3. 在**“密码”**字段中，输入在 PFX 导出向导中设置的 PFX 文件的密码。 4. 然后单击**创建**按钮。 PFX 密钥已创建并显示在“**PFX 密钥**”下拉列表中。 • **纯文本** — 必须指明包含用户账户凭证的密钥，以便在连接到连接器时进行授权。 **添加密钥** *要创建密钥：* 1. 在“**名称**”字段中，输入密钥的名称。 2. 在“**用户**”和“**密码**”字段中，输入代理将用于连接到连接器的用户账户的凭证。 3. 如有必要，请在“**描述**”字段中输入密钥的描述。 4. 然后单击**创建**按钮。 密钥将添加并显示在“**密钥**”下拉列表中。
描述	资源描述：最多 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
缓冲区大小	设置缓冲区的大小。 默认值为 1 KB，最大值为 64 MB。
超时	等待另一个服务或组件响应的时间（以秒为单位）。 默认值为 `30`。
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。
输出格式	将事件发送到外部目标位置的格式。可用值： • JSON • CEF 如果选择 CEF 格式，则发送的事件包含 CEF 标头和仅非空字段。

设置	描述

TLS 模式	使用 TLS 加密。可用值：
	• "**已禁用**"（默认）表示不使用 TLS 加密。
	• **已启用** – 使用不带证书验证的加密。
	• **带验证** – 使用加密并验证证书是否使用 KUMA 根证书签名。KUMA 的根证书和密钥在程序安装期间自动创建，并存储在 KUMA Core 服务器上的 /opt/kaspersky/kuma/core/certificates/ 文件夹中。
	• "**自定义 CA**"表示使用加密并验证证书是否由证书颁发机构签名。从"**自定义 CA**"下拉列表中可选择包含证书的密钥，选择此选项时会显示该列表。
	创建由证书颁发机构签名的证书
	您可以在 KUMA Core 服务器上创建 CA 签名的证书（以下命令示例使用 OpenSSL）。
	要创建由证书颁发机构签名的证书：
	1. 生成证书签发机构要使用的密钥，例如：
	`openssl genrsa -out ca.key 2048`
	2. 为生成的密钥创建证书，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 证书颁发机构的通用主机名 >" -out ca.crt`
	3. 创建私钥并请求证书签发机构对其进行签名，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 服务器的通用主机名 >" -out server.csr`
	4. 创建由证书签发机构签名的证书。您需要在 `subjectAltName` 变量中包含要为其创建证书的服务器的域名或 IP 地址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform Web 界面中，将创建的 `server.crt` 证书上传到 **证书** 类型的密钥，然后在 **自定义 CA** 下拉列表中选择 **证书** 类型的密钥。
	使用 TLS 时，无法将 IP 地址指定为 URL。

分隔符	在下拉列表中，您可以选择用于标记事件之间分隔的字符。默认情况下，使用 `\n`。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是"**已禁用**"。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受"**磁盘缓冲区大小限制**"设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在此部分中，您可以指定识别资源必须处理的事件的标准。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**“条件”**下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是**”。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

文件类型

“**文件**”类型用于将数据写入文件。

> 如果删除服务中使用的“文件”类型的目标位置，则必须重新启动该服务。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**文件**。

设置	描述
网址	必需设置。 事件必须写入的文件路径。 **在文件路径中使用前缀时的限制** 指定文件路径时不能使用的前缀： • /* • /bin • /boot • /dev • /etc • /home • /lib • /lib64 • /proc • /root • /run • /sys • /tmp • /usr/* • /usr/bin/ • /usr/local/* • /usr/local/sbin/ • /usr/local/bin/ • /usr/sbin/ • /usr/lib/ • /usr/lib64/ • /var/* • /var/lib/ • /var/run/ • /opt/kaspersky/kuma/ 系统使用这些前缀作为正则表达式来检查路径。前缀中的 * 字符匹配任何字符序列，如果路径本身不是有效路径的一部分，则不得手动指定该字符。 文件可通过以下路径获取： • /opt/kaspersky/kuma/clickhouse/logs/ • /opt/kaspersky/kuma/metrics/log/
描述	资源描述：最多 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
缓冲区大小	设置缓冲区的大小。 默认值是1KB，最大值为 64 MB。
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。
分隔符	在下拉列表中，您可以选择用于标记事件之间分隔的字符。默认情况下，使用 \n。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
输出格式	将事件发送到外部目标位置的格式。可用值： • JSON • CEF 如果选择 CEF 格式，则发送的事件包含 CEF 标头和仅非空字段。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是“**已禁用**”。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受“**磁盘缓冲区大小限制**”设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在“**过滤器**”部分，您可以指定识别资源必须处理的事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**“条件”**下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是**”。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

存储类型

“**存储**”类型用于将数据传输到存储。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**存储**。
网址	必需设置。 要连接到的 URL。可用格式： `host:port`、 `IPv4:port`、 `:port`。也支持 IPv6 地址，但是使用 IPv6 地址时，还必须指定接口： `[address%interface]:port`。 示例： `[fe80::5054:ff:fe4d:ba0c%eth0]:4222` ）。 您可以通过单击“**URL**”按钮来添加多个地址。 “**URL**”字段支持通过 FQDN、IP 地址和名称搜索服务。搜索字符串格式： • `<Search value>` — 按 FQDN、IP 地址和服务名称执行搜索。 • `<First search value ending in one or more digits>:<second search value>` — 第一个值用于按服务 FQDN 或 IP 地址搜索，第二个值用于按端口搜索。 • `:<value>` — 按端口执行搜索。
描述	资源描述：最多 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
代理服务器	用于选择代理服务器的下拉列表。
缓冲区大小	设置缓冲区的大小。 默认值是 1 KB，最大值为 64 MB。

设置	描述
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。
URL 选择策略	如果指定了多个 URL，您可以在下拉列表中选择确定将事件发送到哪个 URL 的方法： • **任何**。只要此 URL 可以接收事件，就会将事件发送到其中一个可用的 URL。如果连接断开（例如，接收节点断开连接），将选择其他 URL 作为事件目标位置。 • **第一个优先**。事件将发送到所添加地址列表中的第一个 URL。如果该 URL 不可用，则事件将按顺序发送到下一个可用节点。当第一个 URL 再次可用时，将再次开始向其发送事件。 • **均衡**意味着包含事件的包会在列表中所有可用的 URL 之间进行平均分配。由于数据包是在目标位置缓冲区溢出或刷新计时器触发时发送的，因此该 URL 选择策略无法保证事件均匀分布到目标位置。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
健康检查超时	健康检查的频率（以秒为单位）。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是“**已禁用**”。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受“**磁盘缓冲区大小限制**”设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在此部分中，您可以指定识别资源必须处理的事件的标准。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是**"。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

关联器类型

“**关联器**”类型用于将数据传输到关联器。

“基本设置”选项卡

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
“**状态**”切换开关	必须将事件发送到目标位置时使用。 默认情况下，发送事件处于启用状态。
类型	必需设置。 目标位置类型，**关联器**。
网址	必需设置。 要连接到的 URL。可用格式： `host:port`、 `IPv4:port`、 `:port`。也支持 IPv6 地址，但是使用 IPv6 地址时，还必须指定接口：`[address%interface]:port`。 示例： `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`）。 您可以通过单击“**URL**”按钮来添加多个地址。 “**URL**”字段支持通过 FQDN、IP 地址和名称搜索服务。搜索字符串格式： • `<Search value>` — 按 FQDN、IP 地址和服务名称执行搜索。 • `<First search value ending in one or more digits>:<second search value>` — 第一个值用于按服务 FQDN 或 IP 地址搜索，第二个值用于按端口搜索。 • `:<value>` — 按端口执行搜索。
描述	资源描述：最多 4,000 个 Unicode 字符。

“高级设置”选项卡

设置	描述
代理服务器	用于选择代理服务器的下拉列表。
缓冲区大小	设置缓冲区的大小。 默认值是 1 KB，最大值为 64 MB。

设置	描述
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。 默认值是 10 GB。
URL 选择策略	如果指定了多个 URL，您可以在下拉列表中选择确定将事件发送到哪个 URL 的方法： • **任何**。只要此 URL 可以接收事件，就会将事件发送到其中一个可用的 URL。如果连接断开（例如，接收节点断开连接），将选择其他 URL 作为事件目标位置。 • **第一个优先**。事件将发送到所添加地址列表中的第一个 URL。如果该 URL 不可用，则事件将按顺序发送到下一个可用节点。当第一个 URL 再次可用时，将再次开始向其发送事件。 • **均衡**意味着包含事件的包会在列表中所有可用的 URL 之间进行平均分配。由于数据包是在目标位置缓冲区溢出或刷新计时器触发时发送的，因此该 URL 选择策略无法保证事件均匀分布到目标位置。
缓冲区刷新间隔	将批量数据发送到目标位置的时间间隔（以秒为单位）。默认值为 `1 second`。
处理程序数量	此字段用于设置处理队列的服务数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
健康检查超时	健康检查的频率（以秒为单位）。
调试	此切换开关可让您指定是否必须启用资源日志记录。默认值是“**已禁用**”。
磁盘缓冲区已禁用	下拉列表，可让您启用或禁用磁盘缓冲区。默认情况下，启用磁盘缓冲区。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。分配的磁盘空间量受“**磁盘缓冲区大小限制**”设置的值的限制。 如果分配给磁盘缓冲区的磁盘空间耗尽，则事件将按如下方式覆盖：新事件替换写入缓冲区的最早事件。

设置	描述
过滤器	在“**过滤器**”部分，您可以指定识别资源必须处理的事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**“条件”**下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是**”。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击"**确定**"。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**"删除"**，然后确认与该服务取消链接。

目标位置，"事件路由器"类型

eventRouter 类型的目标位置用于将事件发送到事件路由器。下表描述了"**事件路由器**"类型的目标位置设置。

"基本设置"选项卡

设置	描述
名称	资源的唯一名称。名称的最大长度为 128 个 Unicode 字符。 必需设置。
租户	拥有该资源的租户的名称。 必需设置。
状态	此切换开关用于将事件发送到目标位置。默认情况下，此切换开关处于开启状态。
类型	目标位置类型：**事件路由器**。 必需设置。
网址	URL（必填）—需要连接到的 URL。支持以下 URL 格式： • `< 主机名 >:< 端口号 >` • `< IPv4 地址 >:< 端口号 >` • `< IPv6 地址 >:< 端口号 >` 您可以按以下格式指定 IPv6 地址：`[< IPv6 地址 >%< 接口 >:< 端口号 >`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以添加多个 URL，也可以删除一个 URL。如果 URL 字段包含制表符或空格字符，KUMA 不允许保存资源或服务。要添加 URL，请单击"**+ 添加**"按钮。要删除 URL，请单击旁边的删除 (✕) 图标。 必需设置。
标签	资源搜索的标签。 可选设置。
描述	资源描述。描述的最大长度为 4,000 个 Unicode 字符。

"高级设置"选项卡

设置	描述
缓冲区大小	在发送事件作进一步处理或存储之前，用于在服务器 RAM 中累积事件的缓冲区大小（以字节为单位）。该值必须是正整数。默认缓冲区大小：67,108,864（64MB），在界面中显示为0。
缓冲区刷新间隔	向目标位置发送事件的间隔（以秒为单位）。默认值是 1 秒。

设置	描述
磁盘缓冲区大小限制	磁盘缓冲区的大小（以字节为单位）。默认值：10GB，在界面中显示为0。
处理程序	服务可以同时运行以并行处理响应规则的处理程序数量。 该值必须是正整数，最高到 999。
代理服务器	目标位置的代理服务器。您可以选择现有的代理服务器或创建新的代理服务器。要创建新的代理服务器，请选择“**新建**”。 如果要编辑现有代理服务器的设置，请单击旁边的铅笔 (🖉) 图标。
URL 选择策略	如果您在“**基本设置**”选项卡的“**URL**”字段中添加了多个 URL，确定必须优先将事件发送到哪些 URL 的方法： • “**任意**”表示只要 URL 接受事件，事件就会发送到随机选择的可用 URL。如果该 URL 不可用，事件就会发送到另一个随机选择的可用 URL。默认选择此值。 • “**首选第一个**”表示事件会优先发送到第一个添加的 URL。如果该 URL 变得不可用，事件就会发送到下一个添加的可用 URL。如果第一个添加的 URL 重新变得可用，事件会再次发送到第一个添加的 URL。 • “**轮询**”表示事件在可用的 URL 之间均匀分布。此方法不能保证事件在 URL 之间均匀分布，因为缓冲区可能发生溢出或事件可能会发送到目标位置。您可以在“**缓冲区大小限制**”字段中指定缓冲区大小（以字节为单位）；您还可以在“**缓冲区刷新间隔**”字段中指定将事件发送到目标的间隔（以秒为单位）。
健康检查超时	检查目标位置健康状况的间隔（以秒为单位）。
磁盘缓冲区已禁用	此切换开关用于启用磁盘缓冲区。默认情况下，此切换开关处于开启状态。 如果收集器无法将规范化事件发送到目标位置，则会使用磁盘缓冲区。您可以在“**磁盘缓冲区大小限制**”字段中指定磁盘缓冲区的大小。如果磁盘缓冲区的可用空间不足，新的规范化事件将从最早的事件开始覆盖旧的规范化事件。
超时	目标位置等待其他服务或组件响应的时间（以秒为单位）。
调试	此开关用于启用资源日志记录。默认情况下，此切换开关处于关闭状态。

设置	描述
过滤器	用于确定资源必须处理哪些事件的过滤器。您可以选择现有过滤器或创建新过滤器。要创建新过滤器，请选择“**新建**”。 如果要编辑现有过滤器的设置，请单击旁边的铅笔 (🖉) 图标。 **如何创建过滤器?** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**“条件”**下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 检查右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是**”。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“🔗”按钮查看嵌套过滤器设置。

设置	描述

服务选项卡

仅在管理目标位置设置时显示此选项卡，用于链接到服务，即收集器、关联器和事件路由器。

若要将目标位置关联到服务，请点击**关联到服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个服务，然后单击“**确定**”。该目标位置被关联到所选服务。

如有必要，您可以将目标位置与服务取消链接。要执行此操作，请选中服务旁边的复选框，单击**“删除”**，然后确认与该服务取消链接。

预定义目标位置

下表列出的目标位置包含在 OSMP 分发包中。

预定义目标位置

目标位置名称	描述
[OOTB] 关联器	将事件发送到关联器。
[OOTB] 存储	将事件发送到存储。

过滤器

过滤器允许您根据指定条件来选择事件。

收集器服务使用过滤器来选择要发送到 KUMA 的事件。也就是说，符合过滤条件的事件将被发送到 KUMA 作进一步处理。

过滤器可用于以下 KUMA 服务和功能：

- 收集器。
- 关联器。
- 存储。
- KUMA 代理。
- 关联规则。
- 增强规则。
- 聚合规则。
- 目标位置。

- 响应规则。
- 分段规则。

您可以使用独立过滤器或内置过滤器，这些过滤器存储在创建它们的服务或资源中。

对于这些资源，您可以在除“**描述**”字段之外的所有输入字段中启用控制字符的显示。

过滤器的可用设置：

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。内联过滤器是在其他资源或服务中创建的，没有名称。
- **租户**（必填） — 拥有该资源的租户的名称。
- 描述 — 最多 4,000 个 Unicode 字符，用于描述过滤器。
- “**条件**”设置组允许您通过创建过滤条件和过滤器组，或添加现有过滤器来制定过滤条件。

  要创建过滤条件，您可以使用*构建器模式*或*源代码模式*。默认情况下使用构建器模式。

  在构建器模式下，您可以通过从下拉列表中选择过滤条件和运算符来创建或编辑过滤条件。

  在源代码模式下，您可以使用文本命令来创建和编辑搜索查询。

  创建过滤条件时，您可以自由地在模式之间切换。要切换到源代码模式，请单击“**代码**”按钮。在模式之间切换时，创建的条件过滤器会被保留。如果将创建的过滤器关联到资源后，“**代码**”选项卡上未显示过滤器代码，请转到“**构建器**”选项卡，然后返回到“**代码**”选项卡。过滤器代码将会显示。

在构建器模式下创建条件

您可以通过单击以下按钮，在构建器模式下创建过滤条件：

- “**添加条件**” — 添加带有用于定义条件的字段的字符串。
- “**添加组**” — 添加一组过滤器。组运算符可以在 **AND**、**OR** 和 **NOT** 之间切换。您可以将组、条件和现有过滤器添加到过滤器组。“**NOT**”组中的条件将与“**AND**”运算符进行组合。

要替换创建的条件中的运算符，请单击要替换的运算符，然后从下拉列表中选择新的运算符。

要删除创建的条件中的运算符，请单击要删除的运算符，然后按下“**Backspace**”键。

要更改过滤条件的顺序，请单击 ⣿ 并将条件拖放到新位置。

可以通过单击 ✕ 按钮来删除条件、条件组和过滤器。

条件设置：

- **当**（必填） — 在此下拉列表中，您可以指定是否使用运算符的反转函数。
- **左操作数**和**右操作数**（必填） — 用于指定运算符将处理的值。可用的类型取决于所选的运算符。

过滤器的操作数

- **事件字段** – 用于将事件字段值分配给操作数。高级设置：
  - **事件字段**（必填） – 此下拉列表用于选择要从中提取操作数值的字段。
- **活动列表** – 用于将活动列表记录值分配给操作数。高级设置：
  - **活动列表**（必填） – 此下拉列表用于选择活动列表。
  - **键字段**（必填） – 这是用于创建活动列表条目并用作活动列表条目键的事件字段列表。
  - **字段**（必填，除非选择了 **inActiveList** 操作符） – 用于输入要从中提取操作数值的活动列表字段名称。
- **上下文表** – 用于将上下文表值分配给操作数。高级设置：
  - **上下文表名称**（必填） – 此下拉列表用于选择上下文表。
  - **键字段**（必填） – 是用于创建上下文表记录并作为上下文表记录键的事件字段列表或本地变量。
  - **字段** – 用于输入必须从中提取操作数值的上下文表字段的名称。
  - **索引** – 用于输入必须从中提取操作数值的表的列表字段的索引。
- **字典** – 用于将词典资源值分配给操作数。高级设置：
  - **词典**（必填） – 此下拉列表用于选择词典。
  - **键字段**（必填） – 这是用于形成词典值键的事件字段列表。
- **常量** – 用于将自定义值分配给操作数。高级设置：
  - **值**（必填） – 在此处输入要分配给操作数的常量。
- **表** – 用于将多个自定义值分配给操作数。高级设置：
  - **词典**（必填） – 此下拉列表用于选择“**表**”类型词典。
  - **键字段**（必填） – 这是用于形成词典值键的事件字段列表。
- **列表** – 用于将多个自定义值分配给操作数。高级设置：
  - **值**（必填） – 在此处输入要分配给操作数的常量列表。在字段中键入值并按下“**ENTER**”键后，该值将添加到列表中，您可以输入新值。
- **TI** – 用于从事件中读取 CyberTrace 威胁情报 (TI) 数据。高级设置：
  - **Feed**（必填） – 此字段用于指定 CyberTrace 威胁类别。
  - **键字段**（必填） – 此下拉列表用于选择包含 CyberTrace 威胁指标的事件字段。
  - **字段**（必填） – 此字段用于指定包含威胁指标的 CyberTrace Feed 字段。
- “**运算符**”（必填）– 用于选择条件运算符。

在此下拉列表中，如果运算符应忽略值的大小写，则可以选中“**大小写不匹配**”复选框。如果选择了“**inSubnet**”、“**inActiveList**”、“**inCategory**”、“**InActiveDirectoryGroup**”、“**hasBit**”、“**inDictionary**”运算符，则此复选框将被忽略。默认情况下，此复选框未被选中。

过滤器运算符

- **=** — 左操作数等于右操作数。
- **<** — 左操作数小于右操作数。
- **<=** — 左操作数小于或等于右操作数。
- **>** — 左操作数大于右操作数。
- **>=** — 左操作数大于或等于右操作数。
- **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
- **contains** — 左操作数包含右操作数的值。
- **startsWith** — 左操作数以右操作数的某个值开头。
- **endsWith** — 左操作数以右操作数的某个值结尾。
- **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 右操作数中指定的列表项是否存在于左操作数中。

可用操作数类型取决于操作数是左 (L) 还是右 (R)。

左 (L) 和右 (R) 操作数的可用操作数类型

运算符	事件字段类型	活动列表类型	字典类型	上下文表类型	表类型	TI 类型	常量类型	列表类型
=	L、R	L、R	L、R	L、R	L、R	L、R	R	R
>	L、R	L、R	L、R	L、R（仅当通过索引查找表值时）	L、R	L	R	—
>=	L、R	L、R	L、R	L、R（仅当通过索引查找表值时）	L、R	L	R	—
<	L、R	L、R	L、R	L、R（仅当通过索引查找表值时）	L、R	L	R	—
<=	L、R	L、R	L、R	L、R（仅当通过索引查找表值时）	L、R	L	R	—
inSubnet	L、R	L、R	L、R	L、R	L、R	L、R	R	R
包含	L、R	L、R	L、R	L、R	L、R	L、R	R	R
startsWith	L、R	L、R	L、R	L、R	L、R	L、R	R	R
endsWith	L、R	L、R	L、R	L、R	L、R	L、R	R	R
match	L	L	L	L	L	L	R	R
hasVulnerability	L	L	L	L	L	—	—	—
hasBit	L	L	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—	—	—
inDictionary	—	—	—	—	—	—	—	—
inCategory	L	L	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—	—	—
inActiveDirectoryGroup	L	L	L	L	L	—	R	R
TIDetect	—	—	—	—	—	—	—	—

管理过滤器时可使用快捷键。热键如下表所述。

热键及其功能

键	功能
e	按事件字段调用过滤器
天	按字典字段调用过滤器
a	按活动列表字段调用过滤器
c	按上下文表字段调用过滤器
t	按表字段调用过滤器
f	调用过滤器
t+i	使用 TI 调用过滤器
Ctrl+Enter	完成条件编辑

`string`、`number` 或 `float` 类型的扩展事件模式字段的用法与 KUMA 事件模式字段的用法相同。

当使用包含 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的扩展事件模式字段的过滤器时，可以使用以下操作：

- 如果指定的子字符串存在于数组中，则 `contains` 操作返回 `True`，否则返回 `False`。
- `match` 操作将字符串与正则表达式进行匹配。
- `intersec` 操作。

当使用包含 `Array of numbers` 和 `Array of floats` 类型的扩展事件模式字段的过滤器时，可以使用以下比较运算：`<`、`>`、`=`、`>=`、`<=`。

如果要在过滤器中引用数组的特定元素，可以使用以下语法：`NA.<` 数组名称 `>.<` 元素索引 `>`

数组从 0 开始。

例如：

`NA.ArrayOne.0` — 访问 ArrayOne 整数数组的第一个元素。

`FA.ArrayTwo.2` — 访问 ArrayTwo 浮点数数组的第三个元素。

在源代码模式下创建条件

代码编辑器模式允许您快速编辑条件、选择和复制代码块。

在构建器的右侧，您可以找到用于导航过滤器代码的导航器。

在 **AND**、**OR**、**NOT** 逻辑运算符处或分隔值列表中各项的逗号处自动换行。

过滤器中使用的资源名称是自动指定的。包含已关联资源名称的字段无法编辑。如果您没有"**访问共享资源**"角色，则共享资源类别的名称不会显示在过滤器中。

下表列出的过滤器包含在 OSMP 分发包中。

预定义过滤器

过滤器名称	描述
[OOTB][AD] 向启用安全的全局组添加了一个成员 (4728)	选择将用户添加到启用安全的 Active Directory 全局组的事件。
[OOTB][AD] 向启用安全的通用组添加了一个成员 (4756)	选择将用户添加到启用安全的 Active Directory 通用组的事件。
[OOTB][AD] 已从启用安全的全局组中删除一个成员 (4729)	选择将用户从 Active Directory 启用安全的全局组中删除的事件。
[OOTB][AD] 已从启用安全的通用组中删除成员 (4757)	选择将用户从 Active Directory 启用安全的通用组中删除的事件。
[OOTB][AD] 已创建账户	选择 Windows 用户账户创建事件。
[OOTB][AD] 已删除账户	选择 Windows 用户账户删除事件。
[OOTB][AD] 账户登录失败 (4625)	选择 Windows 登录失败事件。
[OOTB][AD] Kerberos 身份验证成功（4624、4768、4769、4770）	选择 Windows 登录成功事件和在域控制器上记录的 ID 为 4769、4770 的事件。
[OOTB][AD][Technical] 4768。已请求 TGT	选择 ID 为 4768 的 Microsoft Windows 事件。
[OOTB][Net] 可能的端口扫描	选择可能指示端口扫描的事件。
[OOTB][SSH] 接受的密码	选择使用密码成功建立 SSH 连接的事件。
[OOTB][SSH] 失败的密码	选择使用密码通过 SSH 建立连接的尝试。

活动列表

活动列表是 KUMA 关联器用于根据关联规则分析事件的数据存储桶。

例如，对于信誉不佳的 IP 地址列表，您可以：

1. 创建“操作”类型的关联规则并将这些 IP 地址添加到活动列表中。
2. 创建“标准”类型的关联规则并将活动列表指定为过滤条件。
3. 使用此规则创建关联器。
   在这种情况下，KUMA 会选择所有包含活动列表中 IP 地址的事件，并创建关联事件。

您可以使用简单类型的关联规则自动填充活动列表，也可以导入包含活动列表数据的文件。

您可以添加、复制或删除活动列表。

活动列表可用于以下 KUMA 服务和功能：

- 关联规则。
- 仪表板。

不同的关联器可以使用相同的活动列表。但是，每个关联器都会创建一个单独的活动列表实体。因此，即使活动列表具有相同的名称和 ID，不同关联器使用的活动列表内容也会有所不同。

只有基于关联器关联规则的数据才会添加到活动列表中。

您可以在活动关联器表中添加、编辑、复制、删除和导出记录。

在关联过程中，当从活动列表中删除条目时，会在关联器中生成服务事件。这些事件仅存在于关联器中，不会重定向到其他目标位置。可以配置关联规则来跟踪这些事件，从而借助它们来识别威胁。用于从活动列表中删除条目的服务事件字段如下所述。

事件字段	值或注释
`ID`	事件标识符
`Timestamp`	过期条目被删除的时间
`Name`	`"active list record expired"`
`DeviceVendor`	`"Kaspersky"`
`DeviceProduct`	`"KUMA"`
`ServiceID`	关联器 ID
`ServiceName`	关联器名称
`DeviceExternalID`	活动列表 ID
`DevicePayloadID`	过期条目的键
`BaseEventCount`	已删除条目更新次数增加了一次
`S.<active list field>`	活动列表中丢弃的条目，格式如下： S.<活动列表字段> = <活动列表字段的值>

查看活动列表的表格

要查看关联器活动列表的表格：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。

   系统将显示“**关联器活动列表**”表。

该表包含以下数据：

- **名称** — 关联器列表的名称。
- **记录** — 活动列表包含的记录数。
- **磁盘占用大小** — 活动列表的大小。
- **目录** — KUMA Core 服务器上活动列表的路径。

添加活动列表

要添加活动列表：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**活动列表**”。
2. 单击“**添加活动列表**”按钮。
3. 执行以下操作：

   a. 在“**名称**”字段中，输入活动列表的名称。

   b. 在“**租户**”下拉列表中，选择拥有该资源的租户。

   c. 在“**TTL**”字段中，指定添加到活动列表中的记录的存储时间。
   当指定时间到期时，记录将被删除。以秒为单位指定时间。
   默认值是 0。如果该字段的值为 0，则记录将保留 36,000 天（大约 100 年）。

   d. 在“**描述**”字段中，提供任何附加信息。
   最多可以使用 4,000 个 Unicode 字符。
   该字段是可选的。
4. 单击“**保存**”按钮。

   活动列表已添加。

查看活动列表的设置

要查看活动列表的设置：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**活动列表**”。
2. 在“**名称**”列中，选择要查看其设置的活动列表。

这将打开活动列表设置窗口。它显示以下信息：

- **ID** – 所选活动列表的标识符。
- **名称** – 资源的唯一名称。
- **租户** – 拥有资源的租户的名称。
- **TTL** – 记录添加到活动列表在系统中保留的有效时长。以秒为单位指定该值。
- **描述** – 有关资源的任何额外信息。

更改活动列表的设置

要更改活动列表的设置：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**活动列表**”。
2. 在“**名称**”列中，选择要更改其设置的活动列表。
3. 指定以下参数的值：
   - **名称** – 资源的唯一名称。
   - **TTL** – 记录添加到活动列表在系统中保留的有效时长。以秒为单位指定该值。
     如果该字段设置为 0，则记录将无限期保留。
   - **描述** – 有关资源的任何额外信息。

> “ID”和“**租户**”字段不可编辑。

复制活动列表的设置

要复制活动列表：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**活动列表**”。
2. 选中要复制的活动列表旁边的复选框。

3. 单击“**复制**”。
4. 指定必要设置。
5. 单击“**保存**”按钮。

活动列表即被复制。

删除活动列表

要删除活动列表：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**活动列表**”。
2. 选中要删除的活动列表旁边的复选框。
   要删除所有列表，请选中“**名称**”列旁边的复选框。

   > 必须至少选中一个复选框。

3. 单击“**删除**”按钮。
4. 单击“**确定**”。

活动列表即被删除。

查看活动列表中的记录

要查看活动列表中的记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。
5. 在“**名称**”列中，选择所需的活动列表。

所选列表的记录表将打开。

该表包含以下数据：

- **密钥** – 记录密钥的值。
- **记录重复** – 事件中提及该记录以及将活动列表导入 KUMA 时下载相同记录的总次数。

- **到期日期** – 必须删除记录的日期和时间。
  如在创建活动列表时，“**TTL**”字段的值为 0，则此活动列表的记录将保留 36,000 天（大约 100 年）。
- **创建时间** – 创建活动列表的时间。
- **更新时间** – 活动列表最后更新的时间。

搜索活动列表中的记录

要查找活动列表中的记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。
5. 在“**名称**”列中，选择所需的活动列表。
   将打开一个包含所选列表记录的窗口。
6. 在“**搜索**”字段中，输入记录键值或键中的几个字符。

活动列表的记录表仅显示密钥包含输入字符的记录。

将记录添加到活动列表

要将记录添加到活动列表：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中所需关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。
5. 在“**名称**”列中，选择所需的活动列表。
   将打开一个包含所选列表记录的窗口。
6. 然后单击“**添加**”按钮。
   “**创建记录**”窗口随即打开。
7. 指定以下参数的值：
   a. 在“**密钥**”字段中，输入记录的名称。
      您可以指定多个值，用“|”字符分隔。

"**密钥**"字段不能为空。如果未填写该字段，KUMA 在尝试保存更改时将返回错误。

b. 在"**值**"字段中，指定"**字段**"列中字段的值。

KUMA 从与活动列表关联的关联规则中获取字段名称。这些名称不可编辑。如有必要，您可以删除这些字段。

c. 单击"**添加新元素**"按钮以添加更多值。

d. 在"**字段**"列中，指定字段名称。

该名称必须满足以下要求：

- 具备唯一性。
- 不包含制表符。
- 不得包含除下划线以外的特殊字符。
- 最大字符数为 128。

名称不得以下划线开头，且只能包含数字。

e. 在"**值**"列中，指定此字段的值。

它必须满足以下要求：

- 不包含制表符。
- 不得包含除下划线以外的特殊字符。
- 最大字符数为 1024。

该字段是可选的。

8. 单击"**保存**"按钮。

记录已添加。保存后，活动列表中的记录将按字母顺序排序。

复制活动列表中的记录

要复制活动列表中的记录：

1. 在主菜单中，转到"**监控**" → "**资源**"。
2. 在"**服务**"部分中，单击"**活动服务**"按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击"**转至活动列表**"按钮。

系统将显示"**关联器活动列表**"表。

5. 在“**名称**”列中，选择所需的活动列表。
   将打开一个包含所选列表记录的窗口。
6. 选择要复制的记录旁边的复选框。
7. 单击“**复制**”。
8. 指定必要设置。

   > ”**密钥**“字段不能为空。如果未填写该字段，KUMA 在尝试保存更改时将返回错误。

   > 对于之前已添加到活动列表中的记录，无法编辑“**字段**”列中的字段名称。您只能更改编辑时添加的记录的名称。名称不得以下划线开头，且只能包含数字。

9. 单击“**保存**”按钮。

记录已复制。保存后，活动列表中的记录将按字母顺序排序。

更改活动列表中的记录

要编辑活动列表中的记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。
5. 在“**名称**”列中，选择所需的活动列表。
   将打开一个包含所选列表记录的窗口。
6. 单击“**键**”列中的记录名称。
7. 指定所需的值。
8. 单击“**保存**”按钮。

该记录将被覆盖。保存后，活动列表中的记录将按字母顺序排序。

编辑记录时的限制：

- 记录名称无法编辑。您可以通过导入具有不同名称的相同数据来进行更改。
- 对于之前已添加到活动列表中的记录，无法编辑“**字段**”列中的字段名称。您只能更改编辑时添加的记录的名称。名称不得以下划线开头，且只能包含数字。

- “**值**”列中的值必须满足以下要求：
  - 不得包含西里尔字符。
  - 不得包含空格或制表符。
  - 不得包含除下划线以外的特殊字符。
  - 最大字符数为 128。

从活动列表中删除记录

要从活动列表中删除记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。
5. 在“**名称**”列中，选择所需的活动列表。
   将打开一个包含所选列表记录的窗口。
6. 选中要删除的记录旁边的复选框。
   要删除所有记录，请选中“**密钥**”列旁边的复选框。

   > 必须至少选中一个复选框。

7. 单击“**删除**”按钮。
8. 单击“**确定**”。

记录将被删除。

将数据导入活动列表

要导入活动列表：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。

5. 将鼠标指向所需活动列表所在的行。
6. 单击活动列表名称左侧的 ...。
7. 选择“**导入**”。
   “活动列表导入”窗口将打开。
8. 在“**文件**”字段中选择要导入的文件。
9. 在“**格式**”下拉列表中，选择文件格式：
   - **csv**
   - **tsv**
   - **内部**
10. 在**键字段**下，输入包含活动列表记录键的列的名称。
11. 单击“**导入**”按钮。

文件中的数据将导入到活动列表中。之前列表中包含的记录将被保存。

从文件导入的数据不会检查无效字符。当您在小部件中使用此数据时，如果数据中存在无效字符，小部件将无法正确显示。

从活动列表中导出数据

要导出活动列表：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 选中要查看活动列表的关联器旁边的复选框。
4. 单击“**转至活动列表**”按钮。
   系统将显示“**关联器活动列表**”表。
5. 将鼠标指向所需活动列表所在的行。
6. 单击位于所需活动列表的左侧的 ...。
7. 单击“**导出**”按钮。

活动列表将使用您的浏览器设置以 JSON 格式下载。下载文件的名称反映了活动列表的名称。

预定义活动列表

下表列出的活动列表包含在 OSMP 分发包中。

活动列表名称	描述
[OOTB][AD] 最终用户技术支持账户	此活动列表用作"[OOTB][AD] 在多个主机上使用同一用户账户成功进行身份验证"关联规则的过滤器。技术支持人员的账户可以添加到活动列表中。记录不会从活动列表中删除。
[OOTB][AD] 已请求 TGT 的列表。EventID 4768	此活动列表由"[OOTB][AD][技术] 4768.TGT 请求"规则填充；此活动列表还用于"[OOTB][AD] 未请求 TGT 即授予 TGS（黄金票证）"规则的选择器中。记录会在录入 10 小时后从列表中删除。
[OOTB][AD] 敏感组列表	此活动列表用作"[OOTB][AD] 敏感组成员身份已修改"关联规则的过滤器。必须监控其成员的关键域组可以添加到活动列表中。记录不会从活动列表中删除。
[OOTB][Linux] 被入侵的主机	此活动列表由"[OOTB] 可能遭入侵的 Linux 主机成功执行了暴力破解"规则填充。记录在录入 24 小时后从列表中删除。

字典

参数描述

字典是存储数据的资源，可供其他 KUMA 资源和服务使用。

字典可用于以下 KUMA 服务和功能：

- 收集器。
- 关联规则。
- 规范化器。

可用设置：

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） — 拥有该资源的租户的名称。
- **描述** — 最多 4,000 个 Unicode 字符，用于描述资源。
- **类型**（必填）— 字典类型。所选类型决定了字典可包含的数据格式：
  - 您可以向"**字典**"类型添加键值对。
    建议不要向此类字典添加超过 50,000 个条目。

    > 向字典中添加含相同键的行时，每新增一行都会覆盖具有相同键的现有行。这意味着只会向字典中添加一行。

  - 可以将复杂表格形式的数据添加到"**表**"类型。您可以使用 REST API 与此类字典交互。
- "**值**"设置区块 — 包含一个字典数据表：

对于“**字典**”类型，此区块显示**键–值**对的列表。您可以单击 + 按钮向表格中添加行。您可以通过单击当鼠标悬停在某一行上时出现的按钮 × 来删除该行。在“**键**”字段中，您可以选择性地指定一个唯一值：最多 128 个 Unicode 字符，第一个字符不能是 $。在“**值**”字段中，您可以选择指定一个值：最多 255 个 Unicode 字符，第一个字符不能是 $。您可以添加一个或多个**键–值**对。

- 对于“**表**”类型，此区块显示包含数据的表。您可以单击 + 按钮来向表中添加行和列。您可以通过单击当鼠标光标悬停在行或列标题上时显示的 × 按钮来删除该行或该列。可以编辑列标题。

如果字典包含超过 5,000 个条目，则它们不会显示在 KUMA 控制台中。要查看此类字典的内容，必须将内容导出为 CSV 格式。如果您编辑 CSV 文件并将其导回 KUMA，字典会随之更新。

导入和导出字典

您可以通过单击“**导入 CSV**”或“**导出 CSV**”按钮，以 CSV 格式（UTF-8 编码）导入或导出字典数据。

CSV 文件的格式取决于字典类型：

- “**字典**”类型：

  ```
  {KEY},{VALUE}\n
  ```

- **表**类型：

  ```
  {Column header 1}, {Column header N}, {Column header N+1}\n
  {Key1}, {ValueN}, {ValueN+1}\n
  {Key2}, {ValueN}, {ValueN+1}\n
  ```

  CSV 文件和字典中的键都必须唯一。在表格中，键在第一列中指定。键必须包含 1 到 128 个 Unicode 字符。值必须包含 0 到 256 个 Unicode 字符。

导入过程中，字典的内容会被导入的文件覆盖。导入字典后，资源名称也会更改，以反映所导入文件的名称。

如果键或值包含逗号或引号字符（, 和 "），则导出时会将它们括在引号 (") 中。此外，引号字符 (") 会通过使用额外的引号 (") 来进行转义。

如果在导入的文件中检测到错误的行（例如，无效的分隔符），则在导入字典时将忽略这些行，而导入表时的导入过程会中断。

通过 API 与字典交互

您可以使用 REST API 读取“**表**”类型字典的内容。即使这些资源正在被活动服务使用，您也可以对其进行修改。例如，您可以利用从第三方应用程序导出的动态变更表格数据来配置事件增强功能。

预定义字典

下表列出的字典包含在 OSMP 分发包中。

字典名称	类型	描述
[OOTB] Ahnlab。严重级别	词典	包含优先级 ID 与其名称之间的对应关系表。
[OOTB] Ahnlab。SeverityOperational	词典	包含 SeverityOperational 参数的值及其相应的描述。
[OOTB] Ahnlab。VendorAction	词典	包含正在执行的操作的 ID 与其名称之间的对应关系表。
[OOTB] Cisco ISE 消息代码	词典	包含 Cisco ISE 事件代码及其对应的名称。
[OOTB] DNS。操作码	词典	包含 DNS 操作的十进制操作码与其在 IANA 注册的描述之间的对应关系表。
[OOTB] IANAProtocolNumbers	词典	包含由 IANA 注册的传输协议（TCP、UDP）的端口号及其对应的服务名称。
[OOTB] Juniper - JUNOS	词典	包含 JUNOS 事件 ID 及其对应的描述。
[OOTB] KEDR。AccountType	词典	包含用户账户类型的 ID 及其对应的类型名称。
[OOTB] KEDR。FileAttributes	词典	包含文件系统存储的文件属性的 ID 及其对应的描述。
[OOTB] KEDR。FileOperationType	词典	包含来自 KATA API 的文件操作的 ID 及其对应的操作名称。
[OOTB] KEDR。FileType	词典	包含来自 KATA API 的已修改文件 ID 及其对应的文件类型描述。
[OOTB] KEDR。IntegrityLevel	词典	包含 Microsoft Windows INTEGRITY LEVEL 参数的 SID 及其对应的描述。
[OOTB] KEDR。RegistryOperationType	词典	包含来自 KATA API 的注册表操作 ID 及其对应的值。
[OOTB] Linux。Sycall 类型	词典	包含 Linux 调用 ID 及其对应的名称。
[OOTB] MariaDB 错误代码	词典	该字典包含 MariaDB 错误代码，并被 [OOTB] MariaDB 审计插件 syslog 规范化器用于增强事件。
[OOTB] Microsoft SQL Server 代码	词典	包含 MS SQL Server 错误 ID 及其对应的描述。
[OOTB] MS DHCP 事件 ID 描述	词典	包含 Microsoft Windows DHCP 服务器事件 ID 及其对应的描述。
[OOTB] S-Terra。MSG ID 与名称间映射的字典	词典	包含 S-Terra 设备事件的 ID 及其对应的事件名称。
[OOTB] S-Terra。MSG_ID 与严重级别间的映射	词典	包含 S-Terra 设备事件的 ID 及其对应的严重级别值。
[OOTB] Syslog 优先级与设施和严重级别间的映射	表格	该表包含**优先级**值和对应的**设施和严重级别**字段值。
[OOTB] VipNet Coordinator Syslog Direction	词典	包含 ViPNet Coordinator 中用于指定方向的方向 ID（特殊字符序列）及其对应的值。
[OOTB] Wallix EventClassId - DeviceAction	词典	包含 Wallix AdminBastion 事件 ID 及其对应的描述。
[OOTB] Windows.Codes (4738)	词典	包含 ID 为 4738 的 MS Windows 审计事件中存在的操作代码及其对应的名称。
[OOTB] Windows.Codes (4719)	词典	包含 ID 为 4719 的 MS Windows 审计事件中存在的操作代码及其对应的名称。
[OOTB] Windows.Codes (4663)	词典	包含 ID 为 4663 的 MS Windows 审计事件中存在的操作代码及其对应的名称。
[OOTB] Windows.Codes (4662)	词典	包含 ID 为 4662 的 MS Windows 审计事件中存在的操作代码及其对应的名称。
[OOTB] Windows。EventIDs 和事件名称映射	词典	包含 Windows 事件 ID 及其对应的事件名称。
[OOTB] Windows。FailureCodes (4625)	词典	包含 Microsoft Windows 事件 4625 的"**失败信息 \ 状态**"和"**失败信息 \ 子状态**"字段中的 ID 及其对应的描述。
[OOTB] Windows。ImpersonationLevels (4624)	词典	包含 Microsoft Windows 事件 4624 的"**模拟级别**"字段中的 ID 及其对应的描述。
[OOTB] Windows。KRB ResultCodes	词典	包含 Kerberos v5 错误代码及其对应的描述。
[OOTB] Windows。LogonTypes（所有 Windows 事件）	词典	包含用户登录类型的 ID 及其对应的名称。
[OOTB] Windows_Terminal Server。EventIDs 和事件名称映射	词典	包含 Microsoft Terminal Server 事件 ID 及其对应的名称。
[OOTB] Windows。验证凭证。错误代码	词典	包含用户登录类型的 ID 及其对应的名称。
[OOTB] ViPNet Coordinator Syslog Direction	词典	包含 ViPNet Coordinator 中用于指定方向的方向 ID（特殊字符序列）及其对应的值。
[OOTB] Syslog 优先级与设施和严重级别间的映射	表格	包含"优先级"值和对应的"设施和严重级别"字段值。

密钥

密钥用于安全地存储机密信息，例如 KUMA 必须使用用户名和密码才能与外部服务交互。如果密钥存储了用户登录名和密码等账户数据，则当收集器连接到事件源时，该密钥中指定的用户账户可能会按照事件源系统中配置的密码策略被阻止。

密钥可用于以下 KUMA 服务和功能：

- 收集器（使用 TLS 加密时）。
- 连接器（使用 TLS 加密时）。
- 目标（使用 TLS 加密或授权时）。
- 代理服务器。

可用设置：

- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填） — 拥有该资源的租户的名称。
- **类型**（必填）— 密钥类型。

  在下拉列表中选择类型时，还会显示用于配置此密钥类型的参数。这些参数如下所述。
- **描述** — 最多 4,000 个 Unicode 字符。

根据密钥类型，有不同的字段可用。您可以选择以下密钥类型之一：

- **凭证** — 这种类型的密钥用于存储连接到外部服务（如 SMTP 服务器）所需的账户凭证。如果选择这种类型的密钥，则必须填写“**用户**”和“**密码**”字段。如果“**密钥**”资源使用“凭证”类型将收集器连接到事件源（例如数据库管理系统），则密钥中指定的用户账户可能会按照事件源系统中配置的密码策略被阻止。

  更改之前保存的凭证类型密钥时，用户名和密码字段显示为空。这些字段的值会保留，您无需重新输入。
- **令牌** — 这种类型的密钥用于存储 API 请求的令牌。例如，在连接到 IRP 系统时会使用令牌。如果选择这种类型的密钥，则必须填写“**令牌**”字段。
- **ktl** — 这种类型的密钥用于存储卡巴斯基威胁情报门户账户凭证。如果您选择这种类型的密钥，则必须填写以下字段：
  - **用户**和**密码**（必填字段）— 您的卡巴斯基威胁情报门户账户的用户名和密码。
  - **PFX 文件**（必填）— 用于上传卡巴斯基威胁情报门户证书密钥。
  - **PFX 密码**（必填）— 用于访问卡巴斯基威胁情报门户证书密钥的密码。
- **urls** — 这种类型的密钥用于存储连接到 SQL 数据库和代理服务器的 URL。在“**描述**”字段中，您必须提供使用“**urls**”类型密钥的连接的描述。

  您可以采用以下格式指定 URL：hostname:port、IPv4:port、IPv6:port、:port。

- **pfx** — 这种类型的密钥用于导入包含证书的 PFX 文件。如果您选择这种类型的密钥，则必须填写以下字段：
  - **PFX 文件**（必填）— 用于上传 PFX 文件。该文件必须包含证书和密钥。PFX 文件可能包含用于服务器证书验证的 CA 签名证书。
  - **PFX 密码**（必填）— 用于输入访问证书密钥的密码。
- **kata/edr** — 这种类型的密钥用于存储连接到 Kaspersky Endpoint Detection and Response 服务器时所需的证书文件和私钥。如果选择这种类型的密钥，则必须上传以下文件：
  - 证书文件 — KUMA 服务器证书。

    该文件必须为 PEM 格式。您只能上传一个证书文件。
  - 用于加密连接的私钥 — KUMA 服务器 RSA 密钥。

    该密钥必须为无密码保护，但带有 PRIVATE KEY 标头。您只能上传一个密钥文件。

    > 您可以通过单击 ⭳ 按钮来生成证书和密钥文件。
- **snmpV1** — 这种类型的密钥用于存储通过简单网络管理协议进行交互所需的 **社群** 值（例如，`public` 或 `private`）。
- **snmpV3** — 这种类型的密钥用于存储通过简单网络管理协议进行交互所需的数据。如果您选择这种类型的密钥，则必须填写以下字段：
  - **用户** — 不带域的用户名。
  - **安全级别** — 用户的安全级别。
    - **NoAuthNoPriv** — 转发消息时无需身份验证，也不保证机密性。
    - **AuthNoPriv** — 转发消息时进行身份验证，但不保证机密性。
    - **AuthPriv** — 转发消息时进行身份验证并保证机密性。

    根据所选级别，可能会显示其他设置。
  - **密码** — SNMP 用户身份验证密码。选择“**AuthNoPriv**”或“**AuthPriv**”安全级别时，此字段可用。
  - **认证协议** — 以下协议可用：MD5、SHA、SHA224、SHA256、SHA384、SHA512。选择“**AuthNoPriv**”或“**AuthPriv**”安全级别时，此字段可用。
  - **隐私协议** — 用于加密消息的协议。可用协议：DES、AES。选择“**AuthPriv**”安全级别时，此字段可用。
  - **隐私密码** — 创建SNMP用户时设置的加密密码。选择“**AuthPriv**”安全级别时，此字段可用。
- **证书** — 这种类型的密钥用于存储证书文件。单击“**上传证书文件**”按钮即可将文件上传到资源。支持 Base64 编码的 X.509 证书公钥。
- **SSH 私钥** — 这种类型的密钥在 SFTP 连接器中用于连接 SFTP 服务器。如果选择这种类型的密钥，您必须指定用户名以及包含 SSH 私钥的文件。

预定义密钥

下表列出的密钥包含在 OSMP 分发包中。

预定义密钥

密钥名称	描述
[OOTB] Continent SQL 连接	存储用于连接到 APKSh Kontinent 数据库的机密数据和设置。要使用它，您必须指定数据库的登录名和密码。
[OOTB] KSC MSSQL 连接	存储用于连接到 Kaspersky Security Center (KSC) 的 MS SQL 数据库的机密数据和设置。要使用它，您必须指定数据库的登录名和密码。
[OOTB] KSC MySQL 连接	存储用于连接到 Kaspersky Security Center (KSC) 的 MySQL 数据库的机密数据和设置。要使用它，您必须指定数据库的登录名和密码。
[OOTB] Oracle Audit Trail SQL 连接	存储用于连接到 Oracle 数据库的机密数据和设置。要使用它，您必须指定数据库的登录名和密码。
[OOTB] SecretNet SQL 连接	存储用于连接到 SecretNet 系统的 MS SQL 数据库的机密数据和设置。要使用它，您必须指定数据库的登录名和密码。

上下文表

*上下文表*是数据数组的容器，KUMA 关联器使用它来根据关联规则分析事件。您可以在“**监控**” → “**资源**”部分创建上下文表。上下文表数据仅存储在通过关联规则中的过滤器或操作添加了该数据的关联器中。

您可以通过“简单”和“操作”类型的关联规则自动填充上下文表，也可以导入包含上下文表数据的文件。

您可以添加、复制和删除上下文表，以及编辑其设置。

上下文表可用于以下 KUMA 服务和功能：

- 关联规则。
- 仪表板。

同一个上下文表可用于多个关联器。但是，每个关联器都会创建一个单独的上下文表实体。因此，即使上下文表具有相同的名称和 ID，不同关联器使用的上下文表的内容也不同。

只有基于关联器关联规则的数据才会添加到上下文表中。

您可以在关联器的上下文表中添加、编辑、删除、导入和导出记录。

在关联过程中，当从上下文表中删除条目时，会在关联器中生成服务事件。这些事件仅存在于关联器中，不会重定向到其他目标位置。服务事件将发送至使用该上下文表的关联器，由其关联规则进行处理。可以配置关联规则来跟踪这些事件，从而借助它们来识别威胁。

用于从上下文表中删除条目的服务事件字段如下所述。

事件字段	值或注释
ID	事件 ID

Timestamp	过期条目被删除的时间
Name	"context table record expired"
DeviceVendor	"Kaspersky"
DeviceProduct	"KUMA"
ServiceID	关联器 ID
ServiceName	关联器名称
DeviceExternalID	上下文表ID
DevicePayloadID	过期条目的键
BaseEventCount	已删除条目的更新次数加一
FileName	上下文表的名称。
S.< 上下文表字段 > SA.< 上下文表字段 > N.< 上下文表字段 > NA.< 上下文表字段 > F.< 上下文表字段 > FA.< 上下文表字段 >	根据从上下文表中删除的条目的类型，删除的上下文表条目会记录在相应类型的事件中： 例如，S.< 上下文表字段 > = < 上下文表字段值 > SA.< 上下文表字段 > = < 上下文表字段值数组 > 布尔型上下文表记录采用以下格式： S.< 上下文表字段 > = true/false SA.< 上下文表字段 > = false,true,false

查看上下文表列表

要查看关联器的上下文表列表：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 在要查看其上下文表的关联器的上下文菜单中，选择**转至上下文表**。

   将显示**关联器上下文表**列表。

该表包含以下数据：

- **名称** – 上下文表的名称。
- **磁盘占用大小** – 上下文表的大小。
- **目录** – KUMA 关联器服务器上的上下文表路径。

添加上下文表

要添加上下文表：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**上下文表**”。
2. 在“**上下文表**”窗口中，单击“**添加**”。
   这将打开**创建上下文表**窗口。

3. 在“**名称**”字段中，输入上下文表的名称。

4. 在“**租户**”下拉列表中，选择拥有该资源的租户。

5. 在“**TTL**”字段中，指定添加到上下文表的记录存储在其中的时间。
   当指定时间到期时，记录将被删除。以秒为单位指定时间。最大值为 `31536000`（1年）。
   默认值为 `0`。如果该字段的值为 0，则记录将无限期存储。

6. 在“**描述**”字段中，提供任何附加信息。
   最多可以使用 4,000 个 Unicode 字符。
   该字段是可选的。

7. 在“**架构**”部分中，指定上下文表具有哪些字段以及字段的数据类型。
   根据数据类型，字段可能是或可能不是关键字段。表中必须至少有一个字段是关键字段。所有字段的名称必须是唯一的。
   要添加表行，请单击“**添加**”并填写表字段：

   a. 在“**名称**”字段中，输入字段的名称。最大长度为 128 个字符。

   b. 在“**类型**”下拉列表中，选择字段的数据类型。
   可能的字段数据类型

   可能的上下文表字段数据类型

字段数据类型	可以是关键字段	注释
整数	是	—
浮点数	是	—
字符串	是	—
布尔	是	—
时间戳	是	对于这种类型的字段，会检查字段值是否大于或等于零。未提供其他操作。
IP 地址	是	对于此类型的字段，将检查字段值是否符合 IPv4、IPv6 格式。未提供其他操作。
整数列表	否	—
浮点数列表	否	—
字符串列表	否	—
布尔列表	否	—
时间戳列表	否	对于此类型的字段，将检查列表中的每一项是否大于或等于零。未提供其他操作。
IP 列表	否	对于此类型的字段，将检查列表中的每一项是否符合 IPv4、IPv6 格式。未提供其他操作。

   c. 如果要将某个字段设为关键字段，请选中“**关键字段**”复选框。
   一个表可以有多个关键字段。关键字段在创建上下文表时选择，唯一标识一个表条目并且不能更改。
   如果上下文表有多个关键字段，则每个表条目由多个字段（复合键）唯一标识。

8. 添加所需数量的上下文表行。

> 保存上下文表后，无法更改架构。

9. 单击“**保存**”按钮。

上下文表已添加。

查看上下文表设置

要查看上下文表设置：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**上下文表**”。
2. 在“**上下文表**”窗口的列表中，选择要查看其设置的上下文表。

这将打开上下文表设置窗口。它显示以下信息：

- **名称** – 资源的唯一名称。
- **租户** – 拥有资源的租户的名称。
- **TTL** – 添加到上下文表的记录存储的时长。以秒为单位指定该值。
- **描述** – 有关资源的任何额外信息。
- **架构**是字段及其数据类型的有序列表，其中标记了关键字段。

编辑上下文表设置

要编辑上下文表设置：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**上下文表**”。
2. 在“**上下文表**”窗口的列表中，选择要编辑其设置的上下文表。
3. 指定以下参数的值：
   - **名称** – 资源的唯一名称。
   - **TTL** – 添加到上下文表的记录存储的时长。以秒为单位指定该值。
   - **描述** – 有关资源的任何额外信息。
   - **架构**是字段及其数据类型的有序列表，其中标记了关键字段。如果关联规则中未使用上下文表，则可以编辑字段列表。

     如果要编辑关联规则中已使用的上下文表中的架构，请按照以下步骤操作。

   “**租户**”字段不可编辑。
4. 单击“**保存**”按钮。

要编辑关联器先前使用的上下文表的设置：

1. 从表中导出数据。
2. 复制并保存关联器磁盘上包含表数据的文件路径。此路径在**关联器上下文表**窗口的**目录**列中指定。稍后您将需要此路径，以从关联器磁盘中删除文件。
3. 从关联器中删除上下文表。
4. 根据需要编辑上下文表设置。
5. 删除关联器磁盘上、步骤 2 中指定路径下的表格数据文件。
6. 将您在其中编辑设置的上下文表添加到关联器。
7. 要重新启动关联器，请在“**资源**”→ “**活动服务**”部分的服务列表中，选中相关关联器旁边的复选框，单击工具栏上的三个点图标，然后在显示的菜单中选择“**重新启动**”。
8. 调整已导出表中的字段（参见步骤 1），使其与步骤 6 中上传到关联器的表的字段匹配。
9. 将调整后的数据导入上下文表。

复制上下文表设置

要复制上下文表：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**上下文表**”。
2. 选择您要复制的上下文表旁边的复选框。
3. 点击“**复制**”。
4. 指定必要设置。
5. 单击“**保存**”按钮。

上下文表将被复制。

删除上下文表

只能删除未用于任何关联器的上下文表。

要删除上下文表：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**上下文表**”。
2. 选中要删除的上下文表旁边的复选框。

   要删除所有上下文表，请选中“**名称**”列旁边的复选框。

> 必须至少选中一个复选框。

3. 单击“**删除**”按钮。

4. 单击“**确定**”。

上下文表被删除。

查看上下文表记录

要查看上下文表记录列表：

1. 在主菜单中，转到“**监控**” → “**资源**”。

2. 在“**服务**”部分中，单击“**活动服务**”按钮。

3. 在您要查看上下文表的关联器的上下文菜单中，选择“**转至上下文表**”。

   这将打开“**关联器上下文表**”窗口。

4. 在“**名称**”列中，选择相关的上下文表。

将显示所选上下文表的记录列表。

列表包含以下数据：

- “**键**”是指记录的复合键。它由一个或多个关键字段的值组成，用“|”字符分隔。如果其中一个关键字段值不存在，仍会显示分隔符。

  例如，记录键由三个字段组成：`DestinationAddress`、`DestinationPort` 和 `SourceUserName`。如果后两个字段不包含值，则记录键显示如下：`43.65.76.98| |` 。

- “**记录重复次数**”是该记录在事件中被提及的次数以及将上下文表导入 KUMA 时下载相同记录的次数之和。

- **到期日期** – 必须删除记录的日期和时间。

  如果创建上下文表时“**TTL**”字段的值为 0，则此上下文表的记录将保留 36,000 天（约 100 年）。

- “**更新**”是上下文表更新的日期和时间。

搜索上下文表记录

要在上下文表中查找记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。

2. 在“**服务**”部分中，单击“**活动服务**”按钮。

3. 在您想要查找记录的关联器的上下文菜单中，选择“**转至上下文表**”。

   这将打开“**关联器上下文表**”窗口。

4. 在“**名称**”列中，选择所需的上下文表。
   这将打开一个窗口，其中包含所选上下文表的记录。
5. 在“**搜索**”字段中，输入记录键值或键中的几个字符。
   上下文表记录列表仅显示键包含输入字符的记录。

如果您的搜索查询与键值为空的记录匹配，则“**仪表板**”上的小部件中会显示文本 <未找到任何内容>。建议明确搜索查询的条件。

添加上下文表记录

要将记录添加到上下文表：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 在要向其上下文表中添加记录的关联器的上下文菜单中，选择“**转至上下文表**”。
   这将打开“**关联器上下文表**”窗口。
4. 在“**名称**”列中，选择相关的上下文表。
   将显示所选上下文表的记录列表。
5. 然后单击“**添加**”按钮。
   “**创建记录**”窗口随即打开。
6. 在“**值**”字段中，指定“**字段**”列中字段的值。
   KUMA 从与上下文表关联的关联规则中获取字段名称。这些名称不可编辑。字段列表无法编辑。
   如果您未指定某些字段值，则缺少的字段（包括关键字段）将使用默认值填充。记录的键由完整的字段集确定，然后将记录添加到表中。如果表中已存在相同的键，则会显示错误。

   默认字段默认值列表

字段类型	默认值
整数	0
浮点数	0.0
字符串	""
布尔	false
IP 地址	"0.0.0.0"
时间戳	0
整数列表	[]
浮点数列表	[]
字符串列表	[]
布尔列表	[]

时间戳列表	[]
IP 列表	[]

7. 单击“**保存**”按钮。

记录已添加。

编辑上下文表记录

要编辑上下文表中的记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。
3. 在要编辑上下文表的关联器的上下文菜单中，选择“**转至上下文表**”。
   这将打开“**关联器上下文表**”窗口。
4. 在“**名称**”列中，选择相关的上下文表。
   将显示所选上下文表的记录列表。
5. 单击要编辑的记录所在行。
6. 在“**值**”列中指定所需值。
7. 单击“**保存**”按钮。

该记录将被覆盖。

编辑记录时的限制：

- 记录的关键字段值不可编辑。您可以通过导出和导入记录来更改值。
- “**字段**”列中的字段名称不可编辑。
- “**值**”列中的值必须满足以下要求：
  - 对于“**时间戳**”和“**时间戳列表**”类型的字段，其值大于或等于 0。
  - 对于“**IP 地址**”和“**IP 列表**”类型的字段，其值为 IPv4 或 IPv6 格式。
  - 对于**布尔值**字段，其值必须为**true**或**false**。

删除上下文表记录

要从上下文表中删除记录：

1. 在主菜单中，转到“**监控**” → “**资源**”。
2. 在“**服务**”部分中，单击“**活动服务**”按钮。

3. 在要从其上下文表中删除记录的关联器的上下文菜单中，选择“**转至上下文表**”。
   这将打开“**关联器上下文表**”窗口。

4. 在“**名称**”列中，选择相关的上下文表。
   将显示所选上下文表的记录列表。

5. 选中要删除的记录旁边的复选框。
   要删除所有记录，请选中“**密钥**”列旁边的复选框。

   > 必须至少选中一个复选框。

6. 单击“**删除**”按钮。

7. 单击“**确定**”。

记录将被删除。

将数据导入上下文表

要将数据导入上下文表：

1. 在主菜单中，转到“**监控**” → “**资源**”。

2. 在“**服务**”部分中，单击“**活动服务**”按钮。

3. 在要将数据导入到其上下文表的关联器的上下文菜单中，选择“**转至上下文表**”。
   这将打开“**关联器上下文表**”窗口。

4. 选中上下文表旁边的复选框，然后单击“**导入**”。
   这将打开上下文表数据导入窗口。

5. 单击“**添加**”，然后选择要导入的文件。

6. 在“**格式**”下拉列表中，选择文件格式：

   - **csv**
   - **tsv**
   - **内部**

7. 点击“**导入**”按钮。

文件中的数据将导入上下文表。上下文表中先前存在的记录将被保留。

导入时，KUMA 会检查每条记录键的唯一性。如果记录已存在，则其字段将填充新值，新值是通过将先前的值与导入记录的字段值合并得出的。

如果上下文表中不存在记录，则将创建新记录。

> 从文件导入的数据不会检查无效字符。当您在小部件中使用此数据时，如果数据中存在无效字符，小部件将无法正确显示。

从上下文表中导出数据

要从上下文表中导出数据：

1. 在主应用程序窗口中，前往**资源和服务→活动服务**部分。
2. 选择要导出其上下文表的关联器，然后在工具栏或菜单 (⋮) 中，单击“**转至上下文表**”。
   这将打开“**关联器上下文表**”窗口。
3. 选中您要导出的上下文表旁边的复选框。
   您不能同时导出多个上下文表。每个表格都必须单独导出。
4. 单击“**导出**”按钮，然后从“**格式**”下拉列表中选择一种格式：
   - **内部**
     上下文表以 JSON 格式导出。
   - **csv**
   - **tsv**
5. 单击“**导出**”按钮。

上下文表将以所选格式下载到您的设备中。导出文件的名称遵循以下模板：<上下文表名称>_<导出日期 (YYYY-MM-DD)>_<导出时间 (HH-MM-SS)>。文件中导出的数据按“**键**”字段排序。

以 JSON（**内部**）格式导出时：

- 文件中各字段的顺序未定义。
- “数组”类型的字段会以值数组的形式导出到文件中，例如：`["val1","val2","val3","val4"]`。
- “**时间戳**”类型字段中的日期和时间格式取决于所选的应用程序界面语言：
  - 俄语：DD.MM.YYYY HH:MM:SS，例如：`18.02.2025 16:09:58`
  - 英语：YYYY-MM-DD HH:MM:SS，例如：`2025.02.18 16:09:58`

导出为 CSV 和 TSV 格式时：

- 文件的第一行包含字段名称，后续行包含数据。
- 在 CSV 格式中，逗号用作字段分隔符；而在 TSV 格式中，使用制表符作为分隔符。

您还可以在上下文表设置窗口中将数据导出到上下文表中。

关联规则

关联规则用于识别已处理事件的特定序列，并在识别后采取某些操作，例如创建关联事件/警报或与活动列表交互。

关联规则可用于以下 KUMA 服务和功能：

- 关联器。
- 通知规则。
- 分段规则的链接。
- 回溯扫描。

可用的关联规则设置取决于所选类型。关联规则的类型：

- 标准 – 用于查找多个事件之间的关联。此类资源可以创建关联事件。

  此规则类型用于确定复杂的关联模式。对于更简单的模式，您应该使用其他需要较少资源来操作的关联规则类型。

- 简单 – 用于在发现某个事件时创建关联事件。
- 操作 – 用于与活动列表和上下文表相关的操作。此规则类型无法创建关联事件。
- 周期性 – 用于基于周期性分析的累积数据检测异常用户活动。当两个指标超过阈值时，即检测到异常：**相对分数**和标准分数（**Z 分数**）。

  此类规则仅在使用 correlator-ng 关联器时可用。无法在 OSMP Console 中创建此类规则。

  更改 correlator-ng 配置时，您可能需要删除 correlation/ 和 containers/ 目录。删除这些目录会导致所有累积的关联器数据丢失，包括统计信息、关联规则存储桶、活动列表和上下文表。

对于这些资源，您可以在除“**描述**”字段之外的所有输入字段中启用控制字符的显示。

如果在关联器中使用了关联规则并基于该规则创建了警报，则即使重启关联器服务，对关联规则的任何更改也不会导致现有警报发生变化。例如，如果更改了关联规则的名称，警报的名称将保持不变。如果关闭现有警报，则会创建一个新警报，该警报会将对关联规则所做的更改纳入考虑。

标准关联规则

标准关联规则用于识别已处理事件中的复杂模式。

模式搜索是通过使用存储桶进行的

*存储桶*是一个数据容器，关联规则资源使用它来确定是否应该创建关联事件。它具有以下功能：

- 将与关联规则资源设置的“**选择器**”组中的过滤器匹配的事件分组在一起。事件按用户在“**相同字段**”字段中选择的字段分组。
- 确定关联规则应触发的实例，这将影响存储桶中已分组的事件。
- 执行在设置“**操作**”组中选择的操作。
- 创建关联事件。

存储桶的可用状态：

- `Empty` — 存储桶中没有事件。这种情况只有在通过关联规则触发进行创建时才会发生。
- `Partial Match` — 存储桶中存在一些预期事件（恢复事件不计入在内）。
- `Full Match` — 存储桶中存在所有预期事件（恢复事件不计入在内）。当达到此条件时：
  - 关联规则触发器
  - 事件从存储桶中清除
  - 存储桶的触发计数器会更新
  - 存储桶的状态变为 `Empty`
- `False Match` — 在以下情况下，存储桶可能出现这种状态：
  - 达到 `Full Match` 状态，但连接筛选器返回 false 时。
  - 当选中“**恢复**”复选框并收到恢复事件时。

  达到此条件时，关联规则不会触发。事件从存储桶中清除，触发计数器进行更新，存储桶的状态变为 `Empty`。

关联规则窗口包含以下选项卡：

- **常规** — 用于指定关联规则的主要设置。在此选项卡上，您可以选择关联规则的类型。
- **选择器** — 用于定义已处理的事件必须满足才能触发关联规则的条件。可用设置因所选规则类型而异。
- **操作** — 用于设置在满足“**选择器**”设置区块中配置的条件时将激活的触发器。关联规则资源必须至少有一个触发器。可用设置因所选规则类型而异。
- **关联器** — 用于链接关联器。仅适用于已创建且处于可供编辑状态的关联规则。

“**常规**”选项卡

- **卡巴斯基存储库中的资源版本** — 资源版本号。此字段不可编辑。仅适用于卡巴斯基提供的资源，用于管理资源更新。
- **名称**（必填） — 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。

- **租户**（必填）– 关联规则所属的租户。
- **类型**（必填）– 用于选择关联规则类型的下拉列表。如果要创建标准关联规则，请选择“**标准**”。
- **相同字段**（必填）– 应分组到存储桶中的事件字段。所选字段值的哈希将用作存储桶的密钥。如果触发了选择器（见下文），所选字段将被复制到关联事件中。

  如果关联规则的不同选择器使用的字段在事件中具有不同的值，请勿在“**相同字段**”部分中指定这些字段。
- **唯一字段** – 应发送到存储桶的事件字段。如果设置了此参数，存储桶将仅接收唯一事件。所选字段值的哈希将用作存储桶的键。

  > 您可以在“**相同字段**”和“**唯一字段**”部分中使用局部变量。要访问变量，其名称必须以“$”字符开头。
  > 有关在这些部分中使用局部变量的示例，请参阅 KUMA 提供的规则：R403_从禁用保护或反病毒数据库过期的主机访问恶意资源。

- **频率限制** – 每秒可触发关联规则的最大次数。默认值是 100。

  > 如果采用复杂逻辑进行模式检测的关联规则未被触发，这可能是由于 KUMA 中用于计算规则触发次数的特定方法造成的。在这种情况下，可以尝试将“**频率限制**”的值增加到 `1000000`。

- **时间窗口（秒）**（必填）– 存储桶生命周期，以秒为单位。默认值：86,400 秒（24 小时）。此计时器在创建存储桶时启动（当它收到第一个事件时）。生命周期不会更新，当其到期时，将激活“**操作**”设置组中的“**超时触发**”触发器并删除存储桶。“**达到每个阈值时**”和“**后续达到阈值时**”触发器可在存储桶的生命周期内多次激活。
- **基础事件保留策略** – 此下拉列表用于指定必须存储在关联事件中的基础事件：
  - **首个事件**（默认值）– 此选项用于存储触发关联事件创建的事件集合中的第一个基础事件。
  - **最后事件** – 此选项用于存储触发关联事件创建的事件集合中的最后一个基础事件。
  - **全部事件** – 此选项用于存储触发关联事件创建的事件集合中的所有基础事件。
- **优先级** – 用来确定关联规则重要性的基础系数。默认值是“**低**”。
- **排序依据** – 在此下拉列表中，您可以选择关联规则选择器将用于跟踪情况变化的事件字段。例如，如果您要将一个关联规则配置成在几种类型的事件依次发生时触发，这可能很有用。
- **描述** – 资源的描述。最多 4,000 个 Unicode 字符。

“**选择器**”选项卡

“**标准**”类型的规则可以有多个选择器。您可以通过单击“**添加选择器**”按钮来添加选择器，也可以通过单击“**删除选择器**”按钮来进行移除。可以通过单击 ⣿ 按钮来移动选择器。

对于每个选择器，以下两个选项卡可用：“**设置**”和“**局部变量**”。

"**设置**"选项卡包含以下设置：

- **别名**（必填）— 满足选择器条件的事件组的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **选择器阈值（事件计数）**（必填）— 选择器必须接收才能触发的事件数量。默认值是 1。
- "**过滤器**"（必填） — 用于设置确定应触发选择器的事件的条件。您可以从下拉列表中选择一个现有过滤器，也可以创建新过滤器。

  在资源中创建过滤器

  KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

  要创建过滤器：

  1. 在"**过滤器**"下拉列表中，选择"**新建**"。
  2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
  3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
  4. 在**"条件"**下，指定事件必须满足的条件：
     a. 单击"**添加条件**"按钮。
     b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。
     c. 在"**运算符**"下拉列表中，选择一个运算符。

     过滤器运算符

     - **=** — 左操作数等于右操作数。
     - **<** — 左操作数小于右操作数。
     - **<=** — 左操作数小于或等于右操作数。
     - **>** — 左操作数大于右操作数。
     - **>=** — 左操作数大于或等于右操作数。
     - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
     - **contains** — 左操作数包含右操作数的值。
     - **startsWith** — 左操作数以右操作数的某个值开头。
     - **endsWith** — 左操作数以右操作数的某个值结尾。
     - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。

- **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

  待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

  如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。

- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。

- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。

- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。

- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。

- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。

- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。

- **inContextTable** — 检查指定的上下文表中是否存在该条目。

- **intersect** — 右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。

6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

基于“Extra”事件字段数据的筛选

基于 **Extra** 事件字段数据的筛选条件如下：

- 条件 — **如果**。
- 左操作数 — **事件字段**。
- 在此事件字段中，您可以指定以下值之一：
  - **Extra** 字段。
  - Extra 字段中的值格式如下：

    `Extra.<field name>`

    例如，`Extra.app`。

    此类型的值需手动指定。

- 写入 **Extra** 字段的数组值格式如下：

  `Extra.<field name>.<array element>`

  例如，`Extra.array.0`。

  数组中的值从 0 开始编号。

  此类型的值需手动指定。

  要使用 Extra 字段中第 3 层及更深层级的值，请使用反引号 ``。例如，`Extra.lev1.lev2.lev3`。

- 运算符 — =。

- 右操作数 — **常量**。

- 值 — 用于过滤事件的值。

关联规则的选择器过滤器中指定的条件顺序非常重要，它会影响系统性能。建议将最具唯一性的条件放在选择器过滤器的第一位。

以下为两个选择器筛选器示例，用于筛选 Microsoft Windows 中的身份验证成功事件。

选择器过滤器 1：

条件 1。DeviceProduct = Microsoft Windows

条件 2。DeviceEventClassID = 4624

选择器过滤器 2：

条件 1。DeviceEventClassID = 4624

条件 2。DeviceProduct = Microsoft Windows

选择器过滤器 2 中的条件顺序更可取，因为它对系统造成的负载更低。

- **恢复** — 当从选择器接收到一定数量的事件时不得触发关联规则，则必须选中此复选框。默认情况下，此复选框未被选中。

选择**局部变量**选项卡，然后单击**添加变量**以声明您想要在此关联规则限制内使用的变量。

在关联规则的选择器中，您可以使用符合 RE2 标准的正则表达式。

与其他操作相比，在关联规则中使用正则表达式的计算量很大。因此，在设计关联规则时，建议将正则表达式的使用限制在必要的最小范围内，并采用其他可用操作。

要使用正则表达式，您必须使用 `match` 比较运算符。正则表达式必须写在常量中。可以选择在正则表达式中使用捕获组。与正则表达式匹配的字段文本必须与正则表达式完全匹配，才会触发关联规则。

有关语法的入门知识以及在选择器中使用正则表达式的关联规则示例，请查看 KUMA 随附的以下规则：

- R105_04_Suspicious PowerShell 命令。疑似混淆。

- R333_在自动运行文件夹中创建文件的行为可疑。

“**操作**”选项卡

“**标准**”类型的规则可以有多个触发器。

- **达到第一个阈值时** – 在存储桶的生命周期内，当存储桶注册选择器的第一次触发时，此触发器激活。
- **达到后续阈值时** – 在存储桶的生命周期内，当存储桶注册选择器的第二次和所有后续触发时，此触发器激活。
- **达到每个阈值时** – 每次存储桶注册选择器的触发时，此触发器激活。
- **超时触发** – 触发器在存储桶的生命周期结束时激活，并通过选中“**恢复**”复选框来关联到选择器。换言之，如果关联规则检测到的情况未在定义的时间内解决，此触发器会激活。

每个触发器都表示为一组设置，其中包含以下可用参数：

- **输出** – 如果选中此复选框，则会发送关联事件进行后处理，包括关联规则之外的外部增强、响应和发送到目标位置。
- **循环至关联器** – 如果选中此复选框，则创建的关联事件将由当前关联器的规则链处理。这可用于分层关联。

  如果选中**输出**和**循环至关联器**复选框，则关联规则将首先发送到后处理，然后再发送到当前关联规则的选择器。
- **不创建警报** – 如果选中此复选框，则触发此关联规则时不会创建警报。如果不想在触发关联规则时创建警报，但仍想将关联事件发送到存储，请选中**输出**和**不触发警报**复选框。如果仅选中“**不触发警报**”复选框，则关联事件不会保存在存储中。
- 在“**增强**”下，您可以使用增强规则修改关联事件的字段。这些增强规则存储在创建它们的关联规则中。您可以创建多个增强规则。可以分别通过单击**添加增强功能**或**移除数据增强**按钮来添加或删除增强规则。
  - **源类型** – 您可以在此下拉列表中选择增强的类型。根据所选类型，可能还会显示需要填写的高级设置。

    可用的增强类型：
    - **常量**

      在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置：
      - 在“**常量**”字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。
      - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

      如果对 `String`、 `Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。

      如果对 `Array of strings`、 `Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。
    - **词典**

      如果需要从“字典”类型的**字典**中添加值，则使用此类型的增强规则。

      在“**字典名称**”下拉列表中选择此类型后，必须选择用于提供值的字典。在“**键字段**”设置块中，您必须点击“**添加字段**”按钮，然后选择相应的事件字段，其值将用于词典条目选择。

如果您使用事件增强功能，并在“源类型”设置中选择了“字典”类型，且在“键增强字段”设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。

示例：“键增强字段”设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”。以下值作为键传递给字典：['a','b','c']。

如果“键增强字段”设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以“|”字符分隔。

示例：“键增强字段”设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”；Code 字符串字段包含字符序列“myCode”。以下值作为键传递给词典：['a','b','c']myCode。

- **表格**

  如果您需要从“表格”类型的**字典**中添加值，则需使用此类型的增强功能。

  在“**字典名称**”下拉列表中选择此增强类型后，选择用于提供值的字典。在“**键字段**”设置组中，单击“**添加字段**”按钮以选择其值用于字典条目选择的事件字段。

  在“**映射**”表格中，配置用于提供数据的字典字段和用于接收数据的事件字段：

  - 在“**字典字段**”列中，选择字典字段。可用字段取决于所选的字典资源。
  - 在“**KUMA 字段**”列中，选择要写入值的事件字段。对于某些所选字段（`*custom*` 和 `*flex*`），在“**标签**”列中，可以为写入其中的数据指定一个名称。

  可通过单击“**添加新元素**”按钮添加新的表行。可通过单击 ✕ 按钮删除列。

- **事件**

  若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置：

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
  - 在“**源字段**”下拉列表中，选择要将其值写入目标字段的事件字段。
  - 单击 🔧 按钮将打开“**转换**”窗口。您可以在该窗口中使用“**添加转换**”按钮创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。

    可用转换

    转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

    可用转换：

    - **lower** — 用于将值的所有字符变为小写
    - **upper** — 用于将值的所有字符变为大写
    - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。
    - **substring** — 用于提取“**开始**”和“**结束**”字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。

- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除“**字符**”字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
- **append** 用于将“**常量**”字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将“**常量**”字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

使用事件增强功能时，如果在“**源类型**”设置中选择了“**事件**”，并将扩展事件模式字段用作参数，则需要特别注意以下事项：

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `String` 类型的字段，则值会以 TSV 格式写入目标字段。

  例如：SA.StringArray 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 DeviceCustomString1 事件模式字段。操作后，DeviceCustomString1 字段包含 ["string1", "string2", "string3"]。

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `Array of strings` 类型的字段，则将源字段的值附加到目标字段的值之后，并将结果写入目标字段，使用逗号（“,”）作为分隔符。

  例如：SA.StringArrayOne 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 SA.StringArrayTwo 事件模式字段。操作后，SA.StringArrayTwo 字段包含 "string1"、"string2" 和 "string3"。

- **模板**

  在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

  - 在“**模板**”字段中，输入 Go 模板。

    事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。

    例如：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

  要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

  如果您使用事件增强功能，并在“**源类型**”设置中选择了“**模板**”类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

  例如：

  {{.SA.StringArrayOne}}

  例如：

  {{- range $index, $element := .SA.StringArrayOne -}}

  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **调试** — 您可以使用此切换开关来启用服务操作的日志记录。

- **描述** — 资源的描述。最多 4,000 个 Unicode 字符。

- “**分类**”设置组 – 用于更改事件中指示的资产类别。可以有多个分类规则。您可以通过单击**添加分类**或**移除分类**按钮来进行添加或删除。只有响应式类别才能添加到资产中或从资产中删除。

  - **操作** – 此下拉列表用于选择要对类别执行的操作：

    - **添加** – 将类别分配给资产。

    - **删除** – 取消资产与类别的绑定。

  - **事件字段** – 指示需要操作的资产的事件字段。

  - **类别 ID** – 下拉列表显示类别树，您可以在其中选择要对其执行操作的类别。单击行可展开列表。

- “**活动列表更新**”设置组 – 用于为一个或多个活动列表操作分配触发器。您可以单击“**添加活动列表操作**”和“**删除活动列表操作**”按钮分别添加或删除活动列表操作。

  可用设置：

  - **名称**（必填） – 此下拉列表用于选择活动列表资源。

  - **操作**（必填） – 此下拉列表用于选择必须执行的操作：

    - **求和** – 将常量、关联事件字段的值或局部变量的值添加到活动列表的值中。

    - **获取** – 获取活动列表条目，并将所选字段的值写入关联事件。

    - **设置** – 通过创建新的或更新现有的活动列表条目，将关联事件的选定字段的值写入活动列表。更新活动列表条目时，数据将合并，且仅覆盖指定字段。

    - **删除** – 删除活动列表条目。

  - **键字段**（必填） – 这是用于创建活动列表条目的事件字段列表。该列表亦用作活动列表条目的键。

    > 活动列表条目键取决于可用字段，而不取决于它们在 KUMA 控制台中的显示顺序。

  - **映射**（“**获取**”和“**设置**”操作必填） – 用于将活动列表字段与事件字段进行映射。可以设置多个映射规则。

    - 左侧字段用于指定活动列表字段。

      > 该字段不能仅包含特殊字符或数字。

    - 中间下拉列表用于选择事件字段。

    - 如果选择了“**设置**”操作，右侧字段可用于将常量分配给活动列表字段。

    - 在“上下文表更新”下，您可以为一个或多个上下文表操作分配触发器。您可以单击**添加上下文表操作**或**删除上下文表操作**来添加或删除上下文表操作。

    - 可用设置：

    - 名称（必填） – 此下拉列表用于选择上下文表资源。

    - 操作（必填）– 此下拉列表用于选择必须执行的操作。

- 求和 — 将常量、关联事件字段的值或局部变量的值添加到上下文表的值中。此操作仅用于数字和浮点类型的字段。
- 设置 — 通过创建新的或更新现有的上下文表条目，将关联事件的所选字段值写入上下文表。更新上下文表条目时，数据将合并，并且仅覆盖指定的字段。
- 获取 — 获取上下文表的字段并将指定字段的值写入关联事件。布尔类型的表字段和布尔值列表将从映射中排除，因为事件不包含布尔字段。
- 合并 — 将关联事件字段、局部变量或常量的值附加到上下文表字段的当前值。
- 删除 — 删除上下文表条目。
- 键字段（必填） — 这是用于创建上下文表条目的事件字段列表。该列表亦用作上下文表条目的键。作为键字段，您可以指定一个事件字段，或在"**选择器**"选项卡上声明的局部变量。
- 上下文表条目的复合键仅取决于字段的值，而不取决于它们在 KUMA 控制台中的显示顺序。
- 映射（除"**删除**"外的所有操作均为必填项） — 用于将上下文表字段映射到事件字段或变量。可以设置多个映射规则。您可以多次指定相同的上下文表字段。
- 左侧字段用于指定上下文表字段。
- 该字段不得包含映射中已使用的字段名称、制表符、特殊字符，也不能仅包含数字。最大字符数为128。名称不能以下划线开头。
- 中间的下拉列表用于选择事件字段或局部变量。
- 如果选择了"**设置**"操作，则可以使用右侧字段为上下文表字段分配常量。"**合并**"或"**求和**"。最大字符数为1,024。

"**关联器**"选项卡

- **添加** — 在编辑已创建的关联规则时使用。您可以单击"**添加**"以打开"**关联器**"窗口，然后从列表中选择一个关联器。单击"**确定**"后，规则将关联到所选的关联器。您可以同时选择多个关联器。规则将添加到执行队列的末尾。如果要在执行队列中上移规则，请前往**资源** - **关联器** - <所选关联器> - **编辑关联器** - **关联**，选中相关规则旁边的复选框，然后单击**上移**或**下移**按钮来根据需要调整规则顺序。
- **删除** — 用于取消关联规则与关联器之间的关联。

简单关联规则

"**简单**"关联规则用于定义简单的事件序列。

关联规则窗口包含以下设置选项卡：

- **常规** — 用于指定关联规则的主要设置。在此选项卡上，您可以选择关联规则的类型。
- **选择器** — 用于定义已处理的事件必须满足才能触发关联规则的条件。可用设置因所选规则类型而异。

- **操作** – 用于设置在满足"**选择器**"设置区块中配置的条件时将激活的触发器。关联规则必须至少有一个触发器。可用设置因所选规则类型而异。
- **关联器** – 用于链接关联器。仅适用于已创建且处于可供编辑状态的关联规则。

"**常规**"选项卡

- **卡巴斯基存储库中的资源版本** – 资源版本号。此字段不可编辑。仅适用于卡巴斯基提供的资源，用于管理资源更新。
- **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填）– 关联规则所属的租户。
- **类型**（必填）– 用于选择关联规则类型的下拉列表。如果要创建简单的关联规则，请选择"**简单**"。
- **传播字段**（必填）– 用于事件分类的事件字段。如果触发了选择器（见下文），这些字段将写入关联事件。
- **频率限制** – 每秒可触发关联规则的最大次数。默认值是 100。

  如果采用复杂逻辑进行模式检测的关联规则未被触发，这可能是由于 KUMA 中用于计算规则触发次数的特定方法造成的。在这种情况下，可以尝试将"**频率限制**"的值增加到 `1000000`。

- **优先级** – 用来确定关联规则重要性的基础系数。默认值为 `Low`。
- **描述** – 资源的描述。最多 4,000 个 Unicode 字符。

"**选择器**"选项卡

"**简单**"类型的规则只能有一个选择器，"**设置**"和"**局部变量**"选项卡可用于该选择器。

"**设置**"选项卡包含带有"**过滤器**"设置组的设置：

- "**过滤器**"（必填） – 用于设置确定应触发选择器的事件的条件。您可以从下拉列表中选择一个现有过滤器，也可以创建新过滤器。

  在资源中创建过滤器

  KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

  要创建过滤器：

  1. 在"**过滤器**"下拉列表中，选择"**新建**"。
  2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。

3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。

4. 在**“条件”**下，指定事件必须满足的条件：

   a. 单击“**添加条件**”按钮。

   b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。

   c. 在“**运算符**”下拉列表中，选择一个运算符。

   过滤器运算符

   - **=** — 左操作数等于右操作数。
   - **<** — 左操作数小于右操作数。
   - **<=** — 左操作数小于或等于右操作数。
   - **>** — 左操作数大于右操作数。
   - **>=** — 左操作数大于或等于右操作数。
   - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
   - **contains** — 左操作数包含右操作数的值。
   - **startsWith** — 左操作数以右操作数的某个值开头。
   - **endsWith** — 左操作数以右操作数的某个值结尾。
   - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
   - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。

     待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

     如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
   - **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

     如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
   - **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
   - **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
   - **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
   - **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。

- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
- **inContextTable** — 检查指定的上下文表中是否存在该条目。
- **intersect** — 右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

基于“Extra”事件字段数据的筛选

基于 **Extra** 事件字段数据的筛选条件如下：

- 条件 — **如果**。
- 左操作数 — **事件字段**。
- 在此事件字段中，您可以指定以下值之一：
  - **Extra** 字段。
  - Extra 字段中的值格式如下：

    `Extra.<field name>`

    例如，`Extra.app`。

    此类型的值需手动指定。
  - 写入 **Extra** 字段的数组值格式如下：

    `Extra.<field name>.<array element>`

    例如，`Extra.array.0`。

    数组中的值从 0 开始编号。

    此类型的值需手动指定。

    要使用 Extra 字段中第 3 层及更深层级的值，请使用反引号 ``。例如，`Extra.lev1.lev2.lev3`。
- 运算符 — =。
- 右操作数 — **常量**。
- 值 — 用于过滤事件的值。

关联规则的选择器过滤器中指定的条件顺序非常重要，它会影响系统性能。建议将最具唯一性的条件放在选择器过滤器的第一位。

以下为两个选择器筛选器示例，用于筛选 Microsoft Windows 中的身份验证成功事件。

选择器过滤器 1：

条件 1。DeviceProduct = Microsoft Windows

条件 2。DeviceEventClassID = 4624

选择器过滤器 2：

条件 1。DeviceEventClassID = 4624

条件 2。DeviceProduct = Microsoft Windows

选择器过滤器 2 中的条件顺序更可取，因为它对系统造成的负载更低。

选择**局部变量**选项卡，然后单击**添加变量**以声明您想要在此关联规则限制内使用的变量。

“**操作**”选项卡

“**简单**”类型的规则只能有一个触发器：**每次事件发生时**。每次选择器触发时都会激活它。

触发器的可用参数：

- **输出** — 如果选中此复选框，则会发送关联事件进行后处理，包括增强、响应和发送到目标位置。
- **循环至关联器** — 如果选中此复选框，则创建的关联事件将由当前关联器的规则链处理。这可用于分层关联。

  如果选中**输出**和**循环至关联器**复选框，则关联规则将首先发送到后处理，然后再发送到当前关联规则的选择器。
- **不创建警报** — 如果选中此复选框，则触发此关联规则时不会创建警报。如果不想在触发关联规则时创建警报，但仍想将关联事件发送到存储，请选中**输出**和**不触发警报**复选框。如果仅选中“**不触发警报**”复选框，则关联事件不会保存在存储中。
- “**增强**”设置组 — 您可以使用增强规则来修改关联事件的字段。这些增强规则存储在创建它们的关联规则中。您可以创建多个增强规则。可以分别通过单击**添加增强功能**或**移除数据增强**按钮来添加或删除增强规则。
  - **源类型** — 您可以在此下拉列表中选择增强的类型。根据所选类型，可能还会显示需要填写的高级设置。

    可用的增强类型：
    - **常量**

      在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置：
      - 在“**常量**”字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。
      - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

      如果对 `String`、 `Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。

      如果对 `Array of strings`、 `Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。
    - **词典**

      如果需要从“字典”类型的**字典**中添加值，则使用此类型的增强规则。

在“**字典名称**”下拉列表中选择此类型后，必须选择用于提供值的字典。在“**键字段**”设置块中，您必须点击“**添加字段**”按钮，然后选择相应的事件字段，其值将用于词典条目选择。

如果您使用事件增强功能，并在“源类型”设置中选择了“字典”类型，且在“键增强字段”设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。

示例：“键增强字段”设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”。以下值作为键传递给字典：['a','b','c']。

如果“键增强字段”设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以“|”字符分隔。

示例：“键增强字段”设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素：“a”、“b”和“c”；Code 字符串字段包含字符序列“myCode”。以下值作为键传递给词典：['a','b','c']myCode。

- **表格**

  如果您需要从“表格”类型的**字典**中添加值，则需使用此类型的增强功能。

  在“**字典名称**”下拉列表中选择此增强类型后，选择用于提供值的字典。在“**键字段**”设置组中，单击“**添加字段**”按钮以选择其值用于字典条目选择的事件字段。

  在“**映射**”表格中，配置用于提供数据的字典字段和用于接收数据的事件字段：

  - 在“**字典字段**”列中，选择字典字段。可用字段取决于所选的字典资源。
  - 在“**KUMA 字段**”列中，选择要写入值的事件字段。对于某些所选字段（`*custom*` 和 `*flex*`），在“**标签**”列中，可以为写入其中的数据指定一个名称。

  可通过单击“**添加新元素**”按钮添加新的表行。可通过单击 ✕ 按钮删除列。

- **事件**

  若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置：

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。
  - 在“**源字段**”下拉列表中，选择要将其值写入目标字段的事件字段。
  - 单击 🔧 按钮将打开“**转换**”窗口。您可以在该窗口中使用“**添加转换**”按钮创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。

    可用转换

    转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。

    可用转换：

    - **lower** — 用于将值的所有字符变为小写
    - **upper** — 用于将值的所有字符变为大写
    - **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。

- **substring** — 用于提取"**开始**"和"**结束**"字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。
- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除"**字符**"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对 `Microsoft-Windows-Sysmon` 应用值为 `Micromon` 的 **trim** 转换后，结果为 `soft-Windows-Sys`。
- **append** 用于将"**常量**"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将"**常量**"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。

  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。

  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。
- **hexToDecimal** 将十六进制数值转换为其十进制表示形式。该转换适用于包含十六进制值（包括 0x 前缀，如有）的字符串或数字字段，结果会作为整数存储在目标 KUMA 事件字段中。该转换返回十进制数。例如，值 0x00FF 会转换为 255。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

使用事件增强功能时，如果在“**源类型**”设置中选择了“**事件**”，并将扩展事件模式字段用作参数，则需要特别注意以下事项：

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `String` 类型的字段，则值会以 TSV 格式写入目标字段。

  例如：SA.StringArray 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 DeviceCustomString1 事件模式字段。操作后，DeviceCustomString1 字段包含 ["string1", "string2", "string3"]。

- 如果源字段是 `Array of strings` 类型的字段，目标字段是 `Array of strings` 类型的字段，则将源字段的值附加到目标字段的值之后，并将结果写入目标字段，使用逗号（“,”）作为分隔符。

  例如：SA.StringArrayOne 扩展事件模式字段包含值："string1"、"string2" 和 "string3"。对事件执行增强操作。该操作的结果会写入 SA.StringArrayTwo 事件模式字段。操作后，SA.StringArrayTwo 字段包含 "string1"、"string2" 和 "string3"。

- **模板**

  在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

  - 在“**模板**”字段中，输入 Go 模板。

    事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。

    例如：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

  - 在“**目标字段**”下拉列表中，选择要写入数据的 KUMA 事件字段。

  要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

  如果您使用事件增强功能，并在“**源类型**”设置中选择了“**模板**”类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

  例如：

  {{.SA.StringArrayOne}}

例如：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **调试** — 您可以使用此切换开关来启用服务操作的日志记录。
- **描述** — 资源的描述。最多 4,000 个 Unicode 字符。
- "**过滤器**"设置区块 — 用于选择要转发哪些事件进行增强。配置按上述说明执行。

- "**分类**"设置组 — 用于更改事件中指示的资产类别。可以有多个分类规则。您可以通过单击**添加分类**或**移除分类**按钮来进行添加或删除。只有响应式类别才能添加到资产中或从资产中删除。
  - **操作** — 此下拉列表用于选择要对类别执行的操作：
    - **添加** — 将类别分配给资产。
    - **删除** — 取消资产与类别的绑定。
  - **事件字段** — 指示需要操作的资产的事件字段。
  - **类别 ID** — 下拉列表显示类别树，您可以在其中选择要对其执行操作的类别。单击行可展开列表。
- "**活动列表更新**"设置组 — 用于为一个或多个活动列表操作分配触发器。您可以单击"**添加活动列表操作**"和"**删除活动列表操作**"按钮分别添加或删除活动列表操作。

  可用设置：
  - **名称**（必填） — 此下拉列表用于选择活动列表。
  - **操作**（必填） — 此下拉列表用于选择必须执行的操作：
    - **求和** — 将常量、关联事件字段的值或局部变量的值添加到活动列表的值中。
    - **获取** — 获取活动列表条目，并将所选字段的值写入关联事件。
    - **设置** — 通过创建新的或更新现有的活动列表条目，将关联事件的选定字段的值写入活动列表。更新活动列表条目时，数据将合并，且仅覆盖指定字段。
    - **获取** — 获取活动列表条目，并将所选字段的值写入关联事件。
    - **删除** — 删除活动列表条目。
  - **键字段**（必填） — 这是用于创建活动列表条目的事件字段列表。该列表亦用作活动列表条目的键。

    活动列表条目键取决于可用字段，而不取决于它们在 KUMA 控制台中的显示顺序。

- **映射**（“**获取**”和“**设置**”操作必填） — 用于将活动列表字段与事件字段进行映射。可以设置多个映射规则。
  - 左侧字段用于指定活动列表字段。

    该字段不能仅包含特殊字符或数字。

  - 中间下拉列表用于选择事件字段。
  - 如果选择了“**设置**”操作，右侧字段可用于将常量分配给活动列表字段。
- 在“上下文表更新”下，您可以为一个或多个上下文表操作分配触发器。您可以单击**添加上下文表操作**或**删除上下文表操作**来添加或删除上下文表操作。
- 可用设置：
- 名称（必填） — 此下拉列表用于选择上下文表资源。
- 操作（必填）— 此下拉列表用于选择必须执行的操作。
- 求和 — 将常量、关联事件字段的值或局部变量的值添加到上下文表的值中。此操作仅用于数字和浮点类型的字段。
- 设置 — 通过创建新的或更新现有的上下文表条目，将关联事件的所选字段值写入上下文表。更新上下文表条目时，数据将合并，并且仅覆盖指定的字段。
- 获取 — 获取上下文表的字段并将指定字段的值写入关联事件。布尔类型的表字段和布尔值列表将从映射中排除，因为事件不包含布尔字段。
- 合并 — 将关联事件字段、局部变量或常量的值附加到上下文表字段的当前值。
- 删除 — 删除上下文表条目。
- 键字段（必填） — 这是用于创建上下文表条目的事件字段列表。该列表亦用作上下文表条目的键。作为键字段，您可以指定一个事件字段，或在“**选择器**”选项卡上声明的局部变量。
- 上下文表条目的复合键仅取决于字段的值，而不取决于它们在 KUMA 控制台中的显示顺序。
- 映射（除“**删除**”外的所有操作均为必填项） — 用于将上下文表字段映射到事件字段或变量。可以设置多个映射规则。您可以多次指定相同的上下文表字段。
- 左侧字段用于指定上下文表字段。
- 该字段不得包含映射中已使用的字段名称、制表符、特殊字符，也不能仅包含数字。最大字符数为 128。名称不能以下划线开头。
- 中间的下拉列表用于选择事件字段或局部变量。
- 如果选择了“**设置**”操作，则可以使用右侧字段为上下文表字段分配常量。“**合并**”或“**求和**”。最大字符数为 1,024。

“关联器”选项卡

- **添加** – 在编辑已创建的关联规则时使用。您可以单击“**添加**”以打开“**关联器**”窗口，然后从列表中选择一个关联器。单击“**确定**”后，规则将关联到所选的关联器。您可以同时选择多个关联器。规则将添加到执行队列的末尾。如果要在执行队列中上移规则，请转到“**资源**” - “**关联器**” -“<所选关联器>” - “**编辑关联器**” - “**关联**”，选中相关规则旁边的复选框，然后单击“上移”或“下移”按钮来根据需要调整规则顺序。
- **删除** – 用于取消关联规则与关联器之间的关联。

操作关联规则

“**操作**”关联规则用于处理活动列表。

关联规则窗口包含以下选项卡：

- **常规** – 用于指定关联规则的主要设置。在此选项卡上，您可以选择关联规则的类型。
- **选择器** – 用于定义已处理的事件必须满足才能触发关联规则的条件。可用设置因所选规则类型而异。
- **操作** – 用于设置在满足“**选择器**”设置区块中配置的条件时将激活的触发器。关联规则必须至少有一个触发器。可用设置因所选规则类型而异。
- **关联器** – 用于链接关联器。仅适用于已创建且处于可供编辑状态的关联规则。

“**常规**”选项卡

- **卡巴斯基存储库中的资源版本** – 资源版本号。此字段不可编辑。仅适用于卡巴斯基提供的资源，用于管理资源更新。
- **名称**（必填） – 此类资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
- **租户**（必填）– 关联规则所属的租户。
- **类型**（必填）– 用于选择关联规则类型的下拉列表。如果要创建操作关联规则，请选择“**操作**”。
- **频率限制** – 每秒可触发关联规则的最大次数。默认值是 100。

  如果采用复杂逻辑进行模式检测的关联规则未被触发，这可能是由于 KUMA 中用于计算规则触发次数的特定方法造成的。在这种情况下，可以尝试将“**频率限制**”的值增加到 `1000000`。

- **描述** – 资源的描述。最多 4,000 个 Unicode 字符。

“**选择器**”选项卡

“**操作**”类型的规则只能有一个选择器，该选择器支持“**设置**”和“**局部变量**”选项卡。

“**设置**”选项卡包含带有“**过滤器**”设置组的设置：

- “**过滤器**”（必填） — 用于设置确定应触发选择器的事件的条件。您可以从下拉列表中选择一个现有过滤器，也可以创建新过滤器。

  在资源中创建过滤器

  KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

  要创建过滤器：

  1. 在“**过滤器**”下拉列表中，选择“**新建**”。
  2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
  3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
  4. 在**“条件”**下，指定事件必须满足的条件：
     a. 单击“**添加条件**”按钮。
     b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。
     c. 在“**运算符**”下拉列表中，选择一个运算符。

     过滤器运算符

     - **=** — 左操作数等于右操作数。
     - **<** — 左操作数小于右操作数。
     - **<=** — 左操作数小于或等于右操作数。
     - **>** — 左操作数大于右操作数。
     - **>=** — 左操作数大于或等于右操作数。
     - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
     - **contains** — 左操作数包含右操作数的值。
     - **startsWith** — 左操作数以右操作数的某个值开头。
     - **endsWith** — 左操作数以右操作数的某个值结尾。
     - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
     - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。

如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。

- **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。

  如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。

- **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。

- **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。

- **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。

- **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。

- **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。

- **inContextTable** — 检查指定的上下文表中是否存在该条目。

- **intersect** — 右操作数中指定的列表项是否存在于左操作数中。

d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。

e. 如果要添加否定条件，请从**“If”**下拉列表中选择“**如果不是** 。

您可以添加多个条件或一组条件。

5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。

6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

基于“Extra”事件字段数据的筛选

基于 **Extra** 事件字段数据的筛选条件如下：

- 条件 — **如果**。
- 左操作数 — **事件字段**。
- 在此事件字段中，您可以指定以下值之一：
  - **Extra** 字段。
  - Extra 字段中的值格式如下：

    `Extra.<field name>`

    例如，`Extra.app`。

    此类型的值需手动指定。
  - 写入 **Extra** 字段的数组值格式如下：

`Extra.<field name>.<array element>`

例如，`Extra.array.0`。

数组中的值从 0 开始编号。

此类型的值需手动指定。

要使用 Extra 字段中第 3 层及更深层级的值，请使用反引号 ``。例如，`Extra.lev1.lev2.lev3`。

- 运算符 – =。
- 右操作数 – **常量**。
- 值 – 用于过滤事件的值。

在**局部变量**选项卡上，单击**添加变量**以声明要在此关联规则限制内使用的变量。

"**操作**"选项卡

"**操作**"类型的规则只能有一个触发器：**每次事件发生时**。每次选择器触发时都会激活它。

触发器的可用参数：

- **活动列表更新**设置组 – 用于为一个或多个活动列表操作指定触发器。您可以单击"**添加活动列表操作**"和"**删除活动列表操作**"按钮分别添加或删除活动列表操作。

  可用设置：

  - **名称**（必填） – 此下拉列表用于选择活动列表。
  - **操作**（必填） – 此下拉列表用于选择必须执行的操作：
    - **求和** – 将常量、关联事件字段的值或局部变量的值添加到活动列表的值中。
    - **设置** – 通过创建新的或更新现有的活动列表条目，将关联事件的选定字段的值写入活动列表。更新活动列表条目时，数据将合并，且仅覆盖指定字段。
    - **删除** – 删除活动列表条目。
  - **键字段**（必填） – 这是用于创建活动列表条目的事件字段列表。该列表亦用作活动列表条目的键。

    > 活动列表条目键取决于可用字段，而不取决于它们在 KUMA 控制台中的显示顺序。

  - **映射**（"**设置**"操作必填） – 用于将活动列表字段与事件字段进行映射。可以设置多个映射规则。
    - 左侧字段用于指定活动列表字段。

      > 该字段不能仅包含特殊字符或数字。

    - 中间下拉列表用于选择事件字段。
    - 如果选择了"**设置**"操作，右侧字段可用于将常量分配给活动列表字段。

- 在“**上下文表更新**”下，您可以为一个或多个上下文表操作分配触发器。您可以单击**添加上下文表操作**或**删除上下文表操作**来添加或删除上下文表操作。

  可用设置：

  - **名称**（必填） – 此下拉列表用于选择上下文表资源。
  - **操作**（必填）– 此下拉列表用于选择必须执行的操作。
    - **求和** – 将常量、关联事件字段的值或局部变量的值添加到上下文表的值中。此操作仅用于数字和浮点类型的字段。
    - **设置** – 通过创建新的或更新现有的上下文表条目，将关联事件的所选字段值写入上下文表。更新上下文表条目时，数据将合并，并且仅覆盖指定的字段。
    - **合并** – 将关联事件字段、局部变量或常量的值附加到上下文表字段的当前值。
    - **删除** – 删除上下文表条目。
  - **键字段**（必填） – 这是用于创建上下文表条目的事件字段列表。该列表亦用作上下文表条目的键。作为密钥字段，您可以指定事件字段或在“选择器”选项卡上声明的局部变量。

    > 上下文表条目的复合键仅取决于字段的值，而不取决于它们在 KUMA 控制台中的显示顺序。

  - **映射**（除“**删除**”外的所有操作均为必填项）– 用于将上下文表字段映射到事件字段或变量。可以设置多个映射规则。您可以多次指定相同的上下文表字段。
    - 左侧字段用于指定上下文表字段。

      该字段不得包含映射中已使用的字段名称、制表符、特殊字符，也不能仅包含数字。最大字符数为 128。名称不能以下划线开头。
    - 中间的下拉列表用于选择事件字段或局部变量。
    - 您可以使用右侧字段将常量分配给上下文表字段。最大字符数为 1024。

“关联器”选项卡

- **添加** – 在编辑已创建的关联规则时使用。您可以单击“**添加**”以打开“**关联器**”窗口，然后从列表中选择一个关联器。单击“**确定**”后，规则将关联到所选的关联器。您可以同时选择多个关联器。规则将添加到执行队列的末尾。如果要在执行队列中上移规则，请转到“**资源**” - “**关联器**” -“<所选关联器>” - “**编辑关联器**” - “**关联**”，选中相关规则旁边的复选框，然后单击“上移”或“下移”按钮来根据需要调整规则顺序。
- **删除** – 用于取消关联规则与关联器之间的关联。

关联器中的变量

如果跟踪事件字段、活动列表或字典中的值不足以涵盖某些特定的安全场景，则可以使用全局变量和局部变量。您可以使用这些变量对关联器接收到的值执行各种操作，以实施复杂的威胁检测逻辑。变量可以在关联器（*全局变量*）或关联规则（*局部变量*）中声明，方法是为其分配一个函数，之后即可像查询普通事件字段一样从关联规则中查询这些变量，并在响应中接收触发后的函数结果。

变量的使用范围：

- 在关联规则中搜索分组字段值或唯一字段值时。
- 在关联规则选择器中，用于设置关联规则触发条件的过滤器中。
- 增强关联事件时。选择“**事件**”作为源类型。
- 向活动列表填充值时。

变量的查询方式与事件字段相同，只需在其名称前加上“$”字符即可。

相同和唯一字段中的局部变量

您可以在“标准”类型关联规则的“**相同字段**”和“**唯一字段**”部分中使用局部变量。要使用局部变量，其名称前面必须带有“$”字符。

有关在“**相同字段**”和“**唯一字段**”部分中使用局部变量的示例，请参阅 KUMA 提供的规则：R403_从保护被禁用或反病毒数据库过期的主机访问恶意资源。

选择器中的局部变量

要在选择器中使用局部变量：

1. 将局部变量添加到规则中。
2. 在“**关联规则**”窗口中，转到“**常规**”选项卡，并将创建的局部变量添加到“**相同字段**”部分。在局部变量名称前添加“$”字符。
3. 在“**关联规则**”窗口中，转到“**选择器**”选项卡，选择现有过滤器或创建新过滤器，然后单击“**添加条件**”。
4. 选择“**事件字段**”作为操作数。
5. 选择局部变量作为事件字段值，并在变量名称前添加“$”字符。
6. 指定其余过滤器设置。
7. 单击“**保存**”按钮。

有关使用局部变量的示例，请参阅 KUMA 提供的规则：R403_从禁用保护或反病毒数据库过期的主机访问恶意资源。

事件增强中的局部变量

您可以使用“标准”和“简单”关联规则，通过局部变量来增强事件。

使用文本和数字实现增强

您可以使用文本（字符串）来增强事件。为此，您可以使用修改字符串的函数：to_lower、to_upper、str_join、append、prepend、substring、tr、replace、str_join。

您可以使用数字来增强事件。为此，您可以使用以下函数：addition（“+”）、subtraction（“-”）、multiplication（“*”）、division（“/”）、round、ceil、floor、abs、pow。

您还可以使用正则表达式来管理局部变量中的数据。

与其他操作相比，在关联规则中使用正则表达式的计算量很大。因此，在设计关联规则时，建议将正则表达式的使用限制在必要的最小范围内，并采用其他可用操作。

时间戳增强

您可以使用时间戳（日期和时间）来增强事件。为此，您可以使用以下函数来获取或修改时间戳：now、extract_from_timestamp、parse_timestamp、format_timestamp、truncate_timestamp 和 time_diff。

活动列表和表格操作

您可以使用局部变量以及来自活动列表和表格的数据来增强事件。

要使用来自活动列表的数据增强事件，请使用 active_list、active_list_dyn 函数。

要使用来自表格的数据增强事件，请使用 table_dict、dict 函数。

您可以使用局部变量中的“conditional”函数来创建条件语句。这样一来，变量可以根据收到的要处理的数据返回其中一个值。

使用局部变量增强事件

要使用局部变量增强事件：

1. 将局部变量添加到规则中。
2. 在“**关联规则**”窗口中，转到“**常规**”选项卡，并将创建的局部变量添加到“**相同字段**”部分。在局部变量名称前添加“$”字符。
3. 在“**关联规则**”窗口中，转到“**操作**”选项卡，然后在“**增强**”下的“**源类型**”下拉列表中，选择“**事件**”。
4. 从“**目标字段**”下拉列表中，选择要将局部变量的值传递给哪个 KUMA 事件字段。
5. 从“**源字段**”下拉列表中，选择一个局部变量。在局部变量名称前添加“$”字符。
6. 指定其余规则设置。
7. 单击“**保存**”按钮。

活动列表增强中的局部变量

您可以使用局部变量来增强活动列表。

要使用局部变量增强活动列表：

1. 将局部变量添加到规则中。
2. 在“**关联规则**”窗口中，转到“**常规**”选项卡，并将创建的局部变量添加到“**相同字段**”部分。在局部变量名称前添加“$”字符。

3. 在“**关联规则**”窗口中，转到“**操作**”选项卡，在“**活动列表更新**”下，将局部变量添加到“**键字段**”字段。在局部变量名称前添加“$”字符。

4. 在“**映射**”下，指定事件字段和活动列表字段之间的对应关系。

5. 单击“**保存**”按钮。

变量的属性

局部变量和全局变量

全局变量的属性与局部变量的属性不同。

全局变量：

- 全局变量在关联器级别声明，仅在该关联器的范围内应用。
- 可以从关联器中指定的所有关联规则查询该关联器的全局变量。
- 在“标准”关联规则中，同一个全局变量在每个选择器中可以取不同的值。
- 无法在不同的关联器之间传输全局变量。

局部变量：

- 局部变量在关联规则级别声明，并且仅在该规则的范围内应用。
- 在“标准”关联规则中，局部变量的作用域仅由声明该变量的选择器组成。
- 局部变量可以在任何类型的关联规则中声明。
- 局部变量不能在规则或选择器之间传递。
- 局部变量不能用作全局变量。

各种关联规则中使用的变量

- 在“**操作**”关联规则中，在“**操作**”选项卡上，您可以指定此规则中所有可用或声明的变量。
- 在“**标准**”关联规则中，在“**操作**”选项卡上，您只能提供这些规则在“**常规**”选项卡的“**相同字段**”字段中指定的变量。
- 在“**简单**”关联规则中，在“**操作**”选项卡上，您只能提供这些规则在“**常规**”选项卡的“**继承字段**”字段中指定的变量。

变量的要求

添加变量函数时，必须首先指定函数的名称，然后在括号中列出其参数。基本数学运算（加、减、乘、除）不受此要求限制。使用这些操作时，括号用于指定操作的严重级别。

函数名称的要求：

- 在关联器内必须是唯一的。
- 必须包含 1 到 128 个 Unicode 字符。
- 不能以 $ 字符开头。
- 必须用 camelCase 或 CamelCase 形式书写。

指定变量函数时的特殊注意事项：

- 参数的顺序很重要。
- 参数以逗号分隔： `,`。
- 字符串参数用单引号传递： `'`。
- 指定事件字段名称和变量时不带引号。
- 当查询一个变量并将其作为参数使用时，在其名称前添加 `$` 字符。
- 参数之间无需添加空格。
- 所有可以使用变量作为参数的函数都可以创建嵌套函数。

变量函数

活动列表和字典的相关操作

active_list 和 active_list_dyn

这些函数允许您从活动列表接收信息，并动态生成活动列表和密钥的字段名称。

您必须按以下顺序指定参数：

1. 活动列表名称。
2. 返回活动列表字段名称的表达式
3. 一个或多个表达式，其结果构成密钥

使用示例	结果
`active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2), to_lower(DeviceCustomString1))`	获取活动列表的字段值。

使用这些函数从变量中查询共享租户的活动列表。为此，请在活动列表名称后添加 @Shared 后缀（区分大小写）。例如，active_list('exampleActiveList@Shared', 'score', SourceAddress, SourceUserName)。

table_dict

获取表类型字典中指定列的值信息。

您必须按以下顺序指定参数：

1. 字典名称
2. 字典列名称
3. 一个或多个表达式，其结果构成字典字符串密钥

使用示例	结果
`table_dict('exampleTableDict', 'office', SourceUserName)`	从 `exampleTableDict` 字典中具有 `SourceUserName` 密钥的行的 `office` 列获取数据。
`table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))`	从 `exampleTableDict` 字典中获取由 `SourceAddress` 字段值和 `SourceUserName` 字段的小写值组成的复合密钥字符串对应的行的 `office` 列数据。

使用此函数从变量访问共享租户的字典。为此，请在活动列表的名称后添加“`@Shared`”后缀（区分大小写）。例如，`table_dict('exampleTableDict@Shared', 'office', SourceUserName)`。

字典

获取有关字典类型字典中指定列的值的信息。

您必须按以下顺序指定参数：

1. 字典名称
2. 一个或多个表达式，其结果用于生成字典行密钥

使用示例	结果
`dict('exampleDictionary', SourceAddress)`	从 `exampleDictionary` 中密钥为 `SourceAddress` 的行获取数据。
`dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))`	根据由 `SourceAddress` 字段值和 `SourceUserName` 字段的小写值组成的复合密钥字符串，从 `exampleDictionary` 中获取数据。

使用此函数从变量访问共享租户的字典。为此，请在活动列表的名称后添加“`@Shared`”后缀（区分大小写）。例如，`dict('exampleDictionary@Shared', SourceAddress)`。

上下文表的相关操作

context_table

返回基本类型中指定字段的值（例如，整数、整数数组）。

您必须按以下顺序指定参数：

1. 上下文表的名称。名称必须指定。
2. 返回上下文表的字段名称的表达式。
3. 返回上下文表的键字段 1 的名称的表达式。
4. 返回上下文表的键字段 1 的值的表达式。

该函数必须包含至少 4 个参数。

使用示例	结果
`context_table('tbl1', 'list_field1', 'key1', 'key1_val')`	`Get the value of the specified field. If the context table or context table field does not exist, an empty string is returned.`

len

返回字符串或数组的长度。

如果传递的数组属于以下类型之一，则该函数返回数组的长度：

- 整数数组
- 浮点数数组
- 字符串数组
- 布尔值数组

如果传递了不同类型的数组，则数组的数据将转换为字符串类型，并且函数返回结果字符串的长度。

使用示例
`len(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`len(DeviceCustomString1)`

distinct_items

返回数组中唯一元素的列表。

如果传递的数组属于以下类型之一，则该函数返回数组的唯一元素列表：

- 整数数组
- 浮点数数组
- 字符串数组
- 布尔值数组

如果传递了不同类型的数组，则数组的数据将转换为字符串类型，并且函数返回由原始字符串中唯一字符组成的字符串。

使用示例
`distinct_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`distinct_items(DeviceCustomString1)`

sort_items

返回数组元素的排序列表。

您必须按以下顺序指定参数：

1. 返回排序对象的表达式
2. 排序顺序可能的值： `asc`、 `desc`。如果未指定该参数，则默认值为 `asc`。

如果传递的数组属于以下类型之一，函数将返回数组的排序元素列表：

- 整数数组
- 浮点数数组
- 字符串数组

对于布尔数组，该函数按原始顺序返回数组元素列表。

如果传递了不同类型的数组，则数组的数据将转换为字符串类型，并且函数将返回排序后的字符串。

使用示例
`sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')`
`sort_items(DeviceCustomString1)`

元素

如果传递的是整数、浮点数、字符串或布尔值数组，则返回具有指定索引的数组元素或具有指定索引的字符串字符。

您必须按以下顺序指定参数：

1. 返回被索引对象的表达式
2. 返回元素或字符索引的表达式

该函数必须至少包含 2 个参数。

如果索引在数组范围内，且传入的数组属于以下类型之一，则函数返回指定索引的数组元素，或者返回指定索引的字符串字符：

- 整数数组
- 浮点数数组
- 字符串数组
- 布尔值数组

如果传递了不同类型的数组，并且索引落在数组范围内，则数据将转换为字符串类型，并且函数返回具有指定索引的字符串字符。如果传递了不同类型的数组，并且索引超出了数组范围，则函数返回空字符串。

使用示例
`item(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 1)`
`item(DeviceCustomString1, 0)`

字符串相关操作

to_lower

将字符串中的字符转换为小写。支持“`string`”类型的标准字段和扩展事件模式字段。

字符串可以作为字符串、字段名称或变量传递。

使用示例
`to_lower(SourceUserName)`
`to_lower('SomeText')`
`to_lower($otherVariable)`

to_upper

将字符串中的字符转换为大写。支持“`string`”类型的标准字段和扩展事件模式字段。字符串可以作为字符串、字段名称或变量传递。

使用示例
`to_upper(SourceUserName)`
`to_upper('SomeText')`
`to_upper($otherVariable)`

append

将字符添加到字符串的末尾。支持“`string`”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 添加的字符串

字符串可以作为字符串、字段名称或变量传递。

使用示例	使用结果
`append(Message, '123')`	字符串“`123`”从“`Message`”字段添加到此字符串的末尾。
`append($otherVariable, 'text')`	字符串“`text`”从变量 `otherVariable` 添加到此字符串的末尾。
`append(Message, $otherVariable)`	来自 `otherVariable` 的字符串被添加到来自“`Message`”字段的此字符串的末尾。

prepend

将字符添加到字符串的开头。支持“`string`”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 添加的字符串

字符串可以作为字符串、字段名称或变量传递。

使用示例	使用结果
`prepend(Message, '123')`	将字符串“`123`”添加至来自“`Message`”字段的此字符串的开头。
`prepend($otherVariable, 'text')`	将字符串“`text`”添加至来自 `otherVariable` 的此字符串的开头。
`prepend(Message, $otherVariable)`	将来自 `otherVariable` 的字符串添加至来自“`Message`”字段的此字符串的开头。

substring

返回来自字符串的子字符串。支持“`string`”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 子字符串起始位置（自然数或 0）。
3. 子字符串结束位置（可选）。

字符串可以作为字符串、字段名称或变量传递。如果位置编号大于原始数据字符串长度，则返回空字符串。

使用示例	使用结果
`substring(Message, 2)`	返回“`Message`”字段中的一部分字符串：从第 3 个字符到结尾。
`substring($otherVariable, 2, 5)`	返回“`otherVariable`”变量中的一部分字符串：从第 3 个字符到第 6 个字符。
`substring(Message, 0, len(Message) - 1)`	返回“`Message`”字段中除最后一个字符之外的整个字符串。

index_of

“`index_of`”函数返回字符串中字符或子字符串的字节偏移量；字符串中第一个字符的索引为 0。如果函数没有找到子字符串，则函数返回负值。

如果字符串包含非 ASCII 字符，则返回的字节偏移量将与您正在搜索的子字符串之前的字符数不对应。

该函数接受以下参数：

- 作为源数据的事件字段、其他变量或常量
- 任何可在局部变量中使用的表达式。

要使用此函数，必须按以下顺序指定参数：

1. 要查找其位置的字符或子字符串。
2. 要搜索的字符串。

使用示例	使用结果
`index_of('@', SourceUserName)`	该函数在“`SourceUserName`”字段中查找“`@`”字符。“`SourceUserName`”字段包含“`user@example.com`”字符串。 结果 = 4。 该函数返回字符串中字符第一次出现的索引。字符串中第一个字符的索引为 0。

index_of('m', SourceUserName)	该函数在“SourceUserName”字段中查找“m”字符。“SourceUserName”字段包含“user@example.com”字符串。 结果 = 8。 该函数返回字符串中字符第一次出现的索引。字符串中第一个字符的索引为 0。

last_index_of

“last_index_of”函数返回字符串中字符或子字符串最后一次出现的位置；字符串中第一个字符的索引为 0。如果该函数没有找到子字符串，则返回“-9223372036854775807”。

该函数接受以下参数：

- 作为源数据的事件字段、其他变量或常量
- 任何可在局部变量中使用的表达式。

要使用此函数，必须按以下顺序指定参数：

1. 要查找其位置的字符或子字符串。
2. 要搜索的字符串。

使用示例	使用结果
last_index_of('m', SourceUserName)	该函数在“SourceUserName”字段中查找“m”字符。“SourceUserName”字段包含“user@example.com”字符串。 结果 = 15。 该函数返回字符串中字符最后一次出现的索引。字符串中第一个字符的索引为 0。

tr

删除字符串开头和结尾的指定字符。支持“string”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 要从原始字符串的开头和结尾删除的子字符串（可选）

字符串可以作为字符串、字段名称或变量传递。如果不指定要删除的字符串，则会从原始字符串的开头和结尾删除空格。

使用示例	使用结果
tr(Message)	“Message”字段中字符串开头和结尾的空格已被删除。
tr($otherVariable, '_')	如果otherVariable变量的值为_test_，则返回字符串 _test_。
tr(Message, '@example.com')	如果Message事件字段包含字符串user@example.com，则返回字符串user。

replace

将字符串中出现的所有字符序列 A 替换为字符序列 B。支持“string”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 搜索字符串：要替换的字符序列。
3. 替换字符串：用于替换搜索字符串的字符序列。

字符串可以作为表达式传递。

使用示例	使用结果
`replace(Name, 'UserA', 'UserB')`	返回“Name”事件字段的一个字符串，其中所有出现的“UserA”均被替换为“UserB”。
`replace($otherVariable, ' text ', '_text_')`	返回 otherVariable 中的一个字符串，其中所有出现的“' text'”均被替换为“'_text_'。

regexp_replace

将与正则表达式匹配的字符序列替换为字符序列和正则表达式捕获组。支持“string”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 搜索字符串：正则表达式。
3. 替换字符串：用于替换搜索字符串的字符序列，以及正则表达式捕获组的 ID。字符串可以作为表达式传递。

字符串可以作为字符串、字段名称或变量传递。可以使用未命名的捕获组。

在变量函数所使用的正则表达式中，每个反斜杠字符都必须另外转义。例如，必须使用 `^example\\\\`，而不是正则表达式 `^example\\`。

使用示例	使用结果
`regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')`	返回“SourceAddress”事件字段的一个字符串，其中在 IP 地址之前插入文本“newIP”。此外，地址的最后几位数字被替换为“10”。

regexp_capture

从原始字符串中获取与正则表达式条件匹配的结果。支持“string”类型的标准字段和扩展事件模式字段。

您必须按以下顺序指定参数：

1. 原始字符串
2. 搜索字符串：正则表达式。

字符串可以作为字符串、字段名称或变量传递。可以使用未命名的捕获组。

在变量函数所使用的正则表达式中，每个反斜杠字符都必须另外转义。例如，必须使用 `^example\\\\`，而不是正则表达式 `^example\\`。

使用示例	示例值	使用结果
`regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})')`	`Message = 'Access from 192.168.1.1 session 1'` `Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'`	`'192.168.1.1'` `'45.45.45.45'`

模板

返回函数中指定的字符串，其中变量被替换为其值。可以通过以下方式传递用于替换的变量：

- 在字符串中。
- 字符串之后。在这种情况下，在字符串内部，必须以 `{{index.<n>}}` 表示法指定变量，其中 <n> 是在字符串之后传递的变量的索引。该索引从 0 开始计数。

使用示例
`template('Very long text with values of rule={{.DeviceCustomString1}} and {{.Name}} event fields, as well as values of {{index.0}} and {{index.1}} local variables and then {{index.2}}', $var1, $var2, $var10)`

时间戳的相关操作

now 函数

获取纪元格式的时间戳。无需参数即可运行。

使用示例
`now()`

extract_from_timestamp

从具有纪元格式时间的字段和变量中获取原子时间表示（年、月、日、小时、分钟、秒、星期几）。

必须按以下顺序指定参数：

1. 时间戳类型的事件字段或变量。
2. 原子时间表示的符号。此参数区分大小写。

原子时间表示法的可能变体：

- y 表示数字格式的年份。
- M 表示用数字表示的月份。
- d 表示月份的数字。
- wd 表示星期几：周一、周二、周三、周四、周五、周六、周日。
- h 表示 24 小时格式的小时。
- m 表示分钟。
- s 表示秒。

3. 时区标识（可选）。

   参数可以指定为字符串（例如， `Europe/Moscow`）或指定为变量（`$timezone`）。变量必须在关联规则的局部变量中声明。该变量的值必须包含时区的字符串标识符。也允许使用从其他变量和字典值派生的变量。

   如果不指定该参数，则以 UTC 格式计算时间。

使用示例
`extract_from_timestamp(Timestamp, 'wd')`
`extract_from_timestamp(Timestamp, 'h')`
`extract_from_timestamp($otherVariable, 'h')`
`extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')`
`extract_from_timestamp(Timestamp, 'h', $timezone)`

使用示例：使用从字典中获取的变量

`$key_timezone = 'timezone'`
 	
`$timezone = dict('UEBA.Timezone', $key_timezone)`
 	
`extract_from_timestamp(EndTime, 'h', $timezone)`

在本例中， `$timezone`变量由另一个变量和一个字典值派生而来，并用作`timezone`参数。

parse_timestamp

将时间从 RFC3339 格式（例如 `2022-05-24 00:00:00`、 `2022-05-24 00:00:00+0300`）转换为 epoch 格式。

使用示例
`parse_timestamp(Message)`
`parse_timestamp($otherVariable)`

format_timestamp

将时间从纪元格式转换为 RFC3339 格式。

必须按以下顺序指定参数：

1. 时间戳类型的事件字段或变量。
2. 时间格式表示法：RFC3339。
3. （可选）时区表示法。如果不指定该参数，则以 UTC 格式计算时间。

使用示例
`format_timestamp(Timestamp, 'RFC3339')`
`format_timestamp($otherVariable, 'RFC3339')`
`format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')`

truncate_timestamp

将时间以纪元格式四舍五入。四舍五入后，以纪元格式返回时间。时间向下舍入。

必须按以下顺序指定参数：

1. 时间戳类型的事件字段或变量。
2. 舍入参数：
   - 1s 四舍五入到最接近的秒。
   - 1m 四舍五入到最接近的分钟。
   - 1h 四舍五入到最接近的小时。
   - 24h 四舍五入到最接近的天。
3. 时区标识（可选）。如果不指定该参数，则以 UTC 格式计算时间。

使用示例	四舍五入值示例	使用结果
`truncate_timestamp(Timestamp, '1m')`	1654631774175 (2022 年 6 月 7 日，19:56:14.175)	1654631760000 (2022 年 6 月 7 日，19:56:00)
`truncate_timestamp($otherVariable, '1h')`	1654631774175 (2022 年 6 月 7 日，19:56:14.175)	1654628400000 (2022 年 6 月 7 日，19:00:00)
`truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')`	1654631774175 (2022 年 6 月 7 日，19:56:14.175)	1654560000000 (2022 年 6 月 7 日，0:00:00)

time_diff

以纪元格式获取两个时间戳之间的时间间隔。

必须按以下顺序指定参数：

1. 间隔结束时间。时间戳类型的事件字段或变量。
2. 间隔开始时间。时间戳类型的事件字段或变量。

3. 时间间隔表示方法：

- ms 表示毫秒。
- s 表示秒。
- m 表示分钟。
- h 表示小时。
- d 表示天。

使用示例
`time_diff(EndTime, StartTime, 's')`
`time_diff($otherVariable, Timestamp, 'h')`
`time_diff(Timestamp, DeviceReceiptTime, 'd')`

数学运算

这些由基本的数学运算和函数组成。

基本的数学运算

支持扩展事件模式的整数和浮点字段。

操作：

- 附加
- 减法
- 乘法
- 除法
- 模除

括号确定操作顺序

可用参数：

- 数字事件字段
- 数字变量
- 实数
  模除时，只有自然数可以用作参数。

使用限制：

- 除以零返回零。
- 对数字和字符串执行数学运算时，返回的数字保持不变。例如，1 + abc 返回 1。

- 返回运算结果的整数，不带小数点。

使用示例 (Type=3; otherVariable=2; Message=text)	使用结果
Type + 1	4
$otherVariable - Type	-1
2 * 2.5	5
2 / 0	0
Type * Message	0
(Type + 2) * 2	10
Type % $otherVariable	1

round

对数字进行四舍五入。支持扩展事件模式的整数和浮点字段。

可用参数：

- 数字事件字段
- 数字变量
- 数字常量

使用示例 (DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)	使用结果
round(DeviceCustomFloatingPoint1)	8
round(DeviceCustomFloatingPoint2)	8
round($otherVariable)	7

ceil

对数字进行向上取整。支持扩展事件模式的整数和浮点字段。

可用参数：

- 数字事件字段
- 数字变量
- 数字常量

使用示例 (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	使用结果
ceil(DeviceCustomFloatingPoint1)	8
ceil($otherVariable)	9

floor

对数字进行向下取整。支持扩展事件模式的整数和浮点字段。

可用参数：

- 数字事件字段
- 数字变量
- 数字常量

使用示例 (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	使用结果
floor(DeviceCustomFloatingPoint1)	7
floor($otherVariable)	8

abs

获取数字的模数。支持扩展事件模式的整数和浮点字段。

可用参数：

- 数字事件字段
- 数字变量
- 数字常量

使用示例 (DeviceCustomNumber1=-7; otherVariable=-2)	使用结果
abs(DeviceCustomFloatingPoint1)	7
abs($otherVariable)	2

pow

对数字求幂。支持扩展事件模式的整数和浮点字段。

必须按以下顺序指定参数：

1. 底数 – 实数。
2. 幂 – 自然数。

可用参数：

- 数字事件字段
- 数字变量
- 数字常量

使用示例
pow(DeviceCustomNumber1, DeviceCustomNumber2)
pow($otherVariable, DeviceCustomNumber1)

str_join

使用分隔符将多个字符串合并为一个。支持扩展事件模式的整数和浮点字段。

必须按以下顺序指定参数：

1. 分隔符。字符串。
2. 字符串 1、字符串 2、字符串 N。至少 2 个表达式。

使用示例	使用结果
`str_join('|', to_lower(Name), to_upper(Name), Name)`	字符串。

条件式

如果满足条件，则获取一个值；如果不满足条件，则获取另一个值。支持扩展事件模式的整数和浮点字段。

必须按以下顺序指定参数：

1. 条件。字符串。语法类似于 SQL 中 Where 语句的条件。您可以在条件中使用 KUMA 变量的函数以及引用其他变量。
2. 满足条件时的值。表达式。
3. 不满足条件时的值。表达式。

支持的运算符：

- `AND`
- `OR`
- `NOT`
- `=`
- `!=`
- `<`
- `<=`
- `>`
- `>=`
- `LIKE`（传递 RE2 正则表达式，而不是 SQL 表达式）
- `ILIKE`（传递 RE2 正则表达式，而不是 SQL 表达式）
- `BETWEEN`
- `IN`
- `IS NULL`（检查是否为空值，例如 0 或空字符串）

用法示例（值取决于参数 2 和 3）
`conditional('SourceUserName = \\'root\\' AND DestinationUserName = SourceUserName', 'match', 'no match')`
`conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no match')`
`conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no match')`

扩展事件模式字段的操作

对于 `string` 类型的扩展事件模式字段，支持以下操作：

- `len`
- `to_lower`
- `to_upper`
- `append`
- `prepend`
- `substring`
- `tr`
- `replace`
- `regexp_replace`
- `regexp_capture`

对于整数或浮点数类型的扩展事件模式字段，支持以下类型的操作：

- 基本的数学运算：
- `round`
- `ceil`
- `floor`
- `abs`
- `pow`
- `str_join`
- `conditional`

对于 `array of integers`、`array of floats` 和 `array of strings` 类型的扩展事件模式字段，KUMA 支持以下函数：

- 获取数组的第 i 个元素。例如：`item(<type>.someStringArray)`。
- 获取一个值数组。例如：`<type>.someStringArray`。返回 `["string1", "string2", "string3"]`。

- 获取数组中元素的数量。例如：`len(<type>.someStringArray)`。返回 `["string1", "string2"]`。
- 获取数组中的唯一元素。例如：`distinct_items(<type>.someStringArray)`。
- 生成数组元素的 TSV 字符串。例如：`to_string(<type>.someStringArray)`。
- 对数组元素进行排序。例如：`sort_items(<type>.someStringArray)`。
  在示例中，您必须指定数组类型，而不是 `<type>`：NA 表示整数数组，FA 表示浮点数数组，SA 表示字符串数组。

对于 `array of integers` 和 `array of floats` 类型的字段，支持以下函数：

- `math_min` – 返回数组的最小元素。例如：`math_min(NA.NumberArray)`、`math_min(FA.FloatArray)`。
- `math_max` 返回数组的最大元素。例如：`math_max(NA.NumberArray)`、`math_max(FA.FloatArray)`。
- `math_avg` – 返回数组的平均值。例如：`math_avg(NA.NumberArray)`、`math_avg(FA.FloatArray)`。

声明变量

要声明变量，必须将变量添加到关联器或关联规则中。

要将全局变量添加到现有关联器：

1. 在主菜单中，转到“**监控**”→ “**资源**” → “**关联器**”。
2. 选择相关关联器的资源集。
   “关联器安装向导”随即打开。
3. 选择安装向导的“**全局变量**”步骤。
4. 单击**添加变量**按钮并指定以下参数：
5. 在“**变量**”窗口中，输入变量的名称。
   变量命名要求
   - 在关联器内必须是唯一的。
   - 必须包含 1 到 128 个 Unicode 字符。
   - 不能以 $ 字符开头。
   - 必须用 camelCase 或 CamelCase 形式书写。
   - 在“**值**”窗口中，输入变量函数。
     变量函数描述。

   可以添加多个变量。可使用 ✕ 图标编辑或删除已添加变量。
6. 选择安装向导的“**设置验证**”步骤，然后单击“**保存**”。

全局变量将添加到关联器。可在变量名称前添加“$”符号，使其能像事件字段一样被查询。重新启动关联器服务后，该变量将用于关联。

要将局部变量添加到现有关联规则：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**关联规则**”。
2. 选择相关的关联规则。

   关联规则设置窗口打开。还可以通过继续执行安装向导的**关联**步骤，从添加关联规则的关联器中打开关联规则的参数。
3. 单击**选择器**选项卡。
4. 在选择器中，打开**局部变量**选项卡，单击**添加变量**按钮并指定以下参数：
   - 在“**变量**”窗口中，输入变量的名称。

     变量命名要求
     - 在关联器内必须是唯一的。
     - 必须包含 1 到 128 个 Unicode 字符。
     - 不能以 $ 字符开头。
     - 必须用 camelCase 或 CamelCase 形式书写。
   - 在“**值**”窗口中，输入变量函数。

     变量函数描述。

   可以添加多个变量。可使用 ✕ 图标编辑或删除已添加变量。

   对于“标准”关联规则，请对每个要在其中声明变量的选择器重复此步骤。
5. 单击“**保存**”按钮。

局部变量将添加到关联规则中。可在变量名称前添加“$”符号，使其能像事件字段一样被查询。重新启动关联器服务后，该变量将用于关联。

添加的变量可以编辑或删除。如果关联规则查询未声明的变量（例如，如果其名称已更改），则会返回空字符串。

如果更改变量的名称，则需要在使用它的所有关联规则中手动更改此变量的名称。

预定义关联规则

OSMP 分发包中包含下表中列出的关联规则。

预定义关联规则

关联规则名称	描述
[OOTB] KATA 警报	用于增强 KATA 事件。
[OOTB] 成功执行了暴力破解	在多次身份验证尝试失败后检测到成功的身份验证尝试时触发。此规则基于 sshd 守护进程的事件运行。
[OOTB][AD] 短时间内创建和删除的账户	检测在 Microsoft Windows 主机上创建和随后删除账户的实例。

[OOTB][AD] 从不同主机登录失败的账户	检测在不同主机上多次身份验证失败的尝试。
[OOTB][AD] 在没有 TGT 的情况下授予 TGS（黄金票证）	检测可疑的"黄金票证"类型攻击。此规则基于 Microsoft Windows 事件运行。
[OOTB][AD][技术] 4768。已请求 TGT	用于填充活动列表的技术规则是 [OOTB][AD] 已请求 TGT 的列表。EventID 4768。此规则基于 Microsoft Windows 事件运行。
[OOTB][AD] 敏感组的成员已修改	基于 Microsoft Windows 事件运行。
[OOTB][AD] 多个账户从同一主机登录失败	在同一主机的不同账户上检测到多次身份验证尝试失败后触发。
[OOTB][AD] 可能的 Kerberoasting 攻击	检测疑似 Kerberoasting 类型的攻击。此规则基于 Microsoft Windows 事件运行。
[OOTB][AD] 在多个主机上使用同一账户身份验证成功	检测使用同一账户连接到不同主机的情况。此规则基于 Microsoft Windows 事件运行。
[OOTB][AD] 短时间内从组中添加和删除的账户	检测用户被添加到组后随即被删除的情况。此规则基于 Microsoft Windows 事件运行。
[OOTB][Net] 可能的端口扫描	检测可疑的端口扫描。此规则基于 Netflow、Ipfix 事件运行。
[OOTB] EDR IOA警报	监控EDR事件，并在检测到具有触发IOA规则的迹象并标记为警报的EDR事件时创建警报。
[OOTB] EDR IOA沙盒警报	监控EDR事件，并在检测到来自自动沙盒扫描的EDR事件时创建警报。
[OOTB] OSMP扫描程序检测	并监控IRP组件生成的安全审计事件，并在收到以下类型之一的事件时创建警报："YARA扫描主机"、"沙盒检测"、"反恶意软件检测"、"IOC扫描主机"、"YARA扫描服务器"。
[OOTB] KEDR事件监控	监控审计事件，并在事件源监控策略触发时创建警报。
[OOTB] 使用同一帐户多次登录OSMP控制台	检测使用同一帐户登录OSMP控制台的尝试，如果发生三次身份验证失败，则生成警报。

为关联规则添加临时排除列表

没有在 OSMP 控制台中编辑关联规则权限的用户可以创建临时排除列表（例如，在管理警报时为误报创建排除项）。拥有编辑关联规则权限的用户随后可以将排除项添加到规则中，并将其从临时列表中移除。

要在管理警报时向关联规则添加排除项：

1. 转至"**警报**"区域并选择一个警报。
2. 单击"**在事件中查找**"按钮。

   警报的事件会显示在事件页面上。
3. 打开关联事件。

   这将打开事件卡片，其中每个字段都有一个 （箭头）按钮，可用于添加排除项。
4. 单击 按钮，然后选择"**添加到排除项**"。

   随即显示一个侧边栏，其中包含以下字段："**关联规则**"、"**排除项**"、"**警报**"、"**注释**"。
5. 点击"**创建**"按钮。

   已添加排除规则。

该排除项已添加到临时列表。任何拥有关联规则读取权限的人员都可以使用此列表：在"**资源**" → "**关联规则**"区域的规则列表工具栏中，单击"**排除项列表**"按钮。如果要查看特定规则的排除项，请打开该规则的卡片并选择"**排除项**"选项卡。

排除列表包含具有以下参数的条目：

- `Exclusion`
  排除条件。
- `Correlation rule`
  关联规则的名称。
- `Alert`
  添加排除项所依据的警报的名称。
- `Tenant`
  规则和排除项适用的租户。
- `Condition`
  根据关联事件的选定字段自动生成。
- `Creation date`
  添加排除项的日期和时间。
- `Expires`

排除项将自动从列表中移除的日期和时间。

- `Created by`
  添加该排除项的用户的名称。
- `Comment`

添加排除项后，默认情况下，关联规则会在 7 天内考虑该排除项。在 **选项** → **常规** 部分中，您可以通过编辑 **核心属性** 部分中的 `corr_rule_exclusion_ttl_hours` 参数来配置排除项的有效期。您可以按小时和天配置排除项的有效期。最小值为 1 小时，最大值为 365 天。此设置仅适用于具有主管理员角色的用户。

要将基础事件中的字段传播到关联事件，必须在关联规则卡片的 **常规** 选项卡上的 **传播字段** 字段中指定这些字段。如果基础事件的字段未映射到关联事件，则无法将这些字段添加到排除项。

要从关联规则中移除排除项：

1. 转到 **资源** → **关联规则** 部分。
2. 在规则列表的工具栏中，单击**排除项列表**按钮。
   这将打开包含排除项列表的窗口。
3. 选择要删除的排除项，然后单击**删除**按钮。

异常将从关联规则中删除。

每当创建或删除异常时，KUMA 都会生成审计事件。您可以在**事件详细信息**窗口中查看事件设置的更改。

Sigma 规则转换器

Sigma 规则转换器可将关联规则转换为 OSMP 支持的格式，并便于导入简单规则以供分析师完善。

支持 Sigma 规则转换器的操作系统列表在“软件要求”部分中提供。

要使用 Sigma 规则转换器转换关联规则，请执行以下步骤：

1. 安装 Sigma 规则转换器。可使用以下安装选项：

- **使用 Docker 和 Bash 安装 Sigma 规则转换器**

  此安装方法适用于在本地安装转换器 Web 界面。

  安装需要最新版本的 Bash 和 Docker。有关部署 Bash 和 Docker 的详细信息，请参阅官方文档。

  不支持 Astra Linux 1.7。

  要执行安装，请执行以下操作：

  1. 进入已解压压缩文件所在的目录，并执行以下命令之一：

     - 要在具有以下地址的主机上安装转换器：

       `0.0.0.0:8000`
       运行以下命令：

       ```
       ./run.sh
       ```

     - 要在具有以下地址的主机上安装转换器：

       `0.0.0.0:8888`
       运行以下命令：

       ```
       ./run.sh <port>
       ```

       其中：
       <port> 是端口（默认端口为 `8000`）。

     - 要在具有以下地址的主机上安装转换器：

       `127.0.0.1:9999`
       运行以下命令：

       ```
       ./run.sh <IP address>:<port>
       ```

       其中：

- <IP address> 是监听接口的 IP 地址，默认值为

  `0.0.0.0`
  .指定

  `127.0.0.1`
  以仅在本地接口上运行。

- <port> 是端口。

转换器已安装。

- **在允许运行 Docker 镜像的环境中安装 Sigma 规则转换器**

  此安装方法使用所提供的容器，允许您创建 systemd 服务并使用 Kubernetes 部署 Web 界面。

  任何容器化工具均可：docker、podman、cri-o。安装过程包括下载容器镜像，然后在指定端口的情况下运行该镜像。

  要使用 podman 安装转换器：

  1. 下载容器镜像：

     ```
     podman load --input "kuma-sigma-converter-x.x.x.tar
     ```

  2. 以下列方式之一运行该镜像：

     - 运行直到按下 Ctrl+C：

       ```
       podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm -it kuma-sigma-converter:x.x.x
       ```

     - 在后台运行：

       ```
       podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm kuma-sigma-converter:x.x.x
       ```

  转换器已安装。

- **使用 Python 3.10 或更高版本安装 Sigma 规则转换器**

  此安装方法最灵活，适合有经验的用户，因为它允许您根据自己的具体需求调整转换器。与其他方法不同，此方法需要连接互联网才能下载 Python 包。

  要安装转换器：

  1. 确保您已安装 Python 3.10 或更高版本。

  2. 安装 poetry 以管理 Python 依赖项。对于 Ubuntu 或 Debian，您可以使用软件包管理器：

     ```
     sudo apt-get update
     sudo apt install pipx
     pipx install poetry
     ```

  3. 使用 poetry 配置并运行 Sigma 规则转换器的 Web 界面：

     ```
     cd sigconverter.io
     poetry install
     ```

```
poetry run ./run.py
```

4. 在浏览器中，转到安装了 Sigma 规则转换器 Web 界面的主机。对于本地安装，地址为 http://127.0.0.1:8000 或 http://0.0.0.0:8000。

5. 如有必要，您可以指定 `HOST` 和 `PORT` 环境变量以配置监听接口并设置端口号。

转换器已安装。

Sigma 规则转换器是 pySigma 框架的插件，这意味着它

pySigma-backend-kuma

可以与其他标准 Sigma 工具一起使用，而不仅限于定制版本
sigconverter.io

。例如：
sigma-cli 是带有命令行界面的转换器。

sigconverter.io 是原始的通用 Web 界面。

以下是以源代码形式提供的库的 README 文件：

src/pySigma/README.md，适用于行业标准 Sigma 转换框架和库。

src/pySigma-backend-kuma/README.md——适用于可实现 OSMP 过滤器和查询转换的 pySigma 插件。

src/sigconverter.io/README.md——Web 用户界面。

安装后，登录转换器的 Web 界面。

2. 根据需要在 Sigma 规则转换器中调整关联规则，并将调整后的规则复制或导入 OSMP。

3. 重启关联器以应用更改。

调整后的关联规则已应用于关联器。

准备 Sigma 规则

将 Sigma 规则转换为关联规则：

1. 修改规则前，请确保满足以下要求：

   - 预定义规范化器对包含用户名、主机名和进程名的字段使用事件扩充 `to lower case`，因此建议在源 Sigma 规则中将相关字段转换为小写。

   - 不建议在 `contains` 条件及类似位置编写注释或附加信息。如果需要留下注释，建议使用 `#` 字符，此类注释不会影响条件。

   - 规则必须以单词 `title` 开头，其前不得有连字符。

2. 从 OSMP Web 界面复制要编辑的关联规则，将其转换为 YML 格式，然后粘贴到转换器的 **rule.yml** 选项卡中。根据需要在下拉列表中选择设置。必要时修正所有错误。

3. 在 Sigma 规则转换器的 **后端** 字段中，选择 **kuma**；在 **格式** 字段中，选择 **default**；并将 **管道** 字段留空。
可用值如下：

   - 后端：kuma，格式：default — 无格式设置的可直接运行 SQL 查询。
   - 后端：kuma，格式：SQL_formatted — 带格式设置的可直接运行 SQL 查询。
   - 后端：kuma_filter，格式：default — 关联规则的即用型选择器。
   - 后端：kuma_filter，格式：correlation — JSON 格式的可直接导入关联规则。要执行导入，可以使用 REST API 方法 /xdr/api/v3/kuma/resources/{kind}/create，并指定用于导入的 tenantID 和租户名称。

4. 转到转换器的 **custom_pipeline.yml** 选项卡，并将针对 pySigma 调整的示例字典复制到该选项卡中。
针对 pySigma 调整的示例字典

Windows process_creation 映射

product: windows

category: process_creation

DeviceEventClassID = 4688

Windows sysmon EVENT=11 映射

product: windows

service: Sysmon

EventID = 11

Windows security

product: windows

service: security

EventID = 4624|4662|4104|4698

```
name: KUMA windows
priority: 30
transformations:
### Windows process_creation mapping
  - id: MAPPING_logsource_windows_process_creation
    type: field_name_mapping
    mapping:
      ParentImage: SourceProcessName
      Image: DestinationProcessName
      CommandLine: DeviceCustomString4
    rule_conditions:
      - type: logsource
        product: windows
        category: process_creation
  - id: DEFAULT_FOR_logsource_windows_process_creation
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
```

```
      DeviceProduct: Windows
      DeviceEventClassID: '4688'
    rule_conditions:
       - type: logsource
         product: windows
         category: process_creation
### Windows sysmon EventID=11 mapping
  - id: DEFAULT_FOR_logsource_windows_sysmon
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Sysmon
    rule_conditions:
       - type: logsource
         product: windows
         service: Sysmon
  - id: MAPPING_logsource_windows_sysmon
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Image: OldFilePath
      CommandLine: DeviceCustomString4
      TargetFilename: FilePath
    rule_conditions:
      - type: logsource
        product: windows
        service: Sysmon
### Windows security mapping
  - id: DEFAULT_FOR_logsource_windows_security
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
    rule_conditions:
       - type: logsource
         product: windows
         service: security
  - id: DEFAULT_MAPPING_FOR_logsource_windows_security
    type: field_name_mapping
    mapping:
      Computer: DestinationHostName
      LogonID: FlexString1
    rule_conditions:
       - type: logsource
         product: windows
         service: security
  - id: 4624_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      LogonType: DeviceCustomNumber1
      SourceIP: SourceAddress
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4624
  - id: 4662_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Properties: FilePermission
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4662
  - id: 4104_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      ScriptBlockText: Message
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4104
  - id: 4698_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      TaskName: SourceProcessName
    rule_conditions:
      - type: contains_detection_item
```

```
        field: "EventID"
        value: '4698'
```

转换后的规则显示在**查询**选项卡上。转换结果是用于 SQL 查询的 WHERE 子句。

如果最终结果是查询或筛选器，您可以将其复制到 OSMP。如果要在 OSMP 中使用规则，可以逐条将规则导入 OSMP。

支持的 Sigma 规则转换示例

支持的 Sigma 规则转换示例

Sigma 规则	映射到 OSMP 对象	
title: Generic-DCSync Execution id: 9107f781-c984-436a-8093-1aaa64c70c49 description: Detects access to DC with "DS-Replication-Get-Changes" or "DS-Replication-Get-Changes-All" rights author: Kaspersky status: stable modified: 2023-08-02 tags: - attack.credential_access - attack.t1003.006 logsource: product: windows service: security detection: selection1: EventID: 4662 Properties|contains: - 'DS-Replication-Get-Changes' - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' selection2: EventID: 4624 LogonType: 3 filter: EventID: 4624 LogonType: 3 SourceIP: - '<ip address of DC servers>' timeframe: 1m condition: selection1 or (selection2 and not filter) | count(EventID) by Computer,LogonID = 2 fields: - SourceIP - Computer - LogonID - Username - Properties falsepositives: - Unknown level: high	"Microsoft 产品"规范化器 tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows selection1: DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '' selection2 DeviceEventClassID=4624 DeviceCustomNumber1 = 3 filter DeviceEventClassID=4624 DeviceCustomNumber1 = 3 SourceAddress = <IP> condition: DeviceVendor = Microsoft AND DeviceProduct = Windows AND ((DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '') OR ((DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3) NOT (DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3 AND SourceAddress = <IP>))) everything inside Count() Put EventID in Unique fields, everything after 'by' Computer → DestinationHostName LogonID → FlexString1 put in Aggregation fields, everything after '=' or '>' 2 put in threshold. timeframe put in time window	这是一条包含关联 OSMP 规则。目前 Sigma 规则中移除 件，或用于威胁搜

Sigma 规则	映射到 OSMP 对象	
title: Lsass Dump via LOLBin id: 2fe9cd33-d7f1-4d52-ab11-e40cb359ad02 description: detects lsass dump via lolbins such as procdump.exe, dotnet-dump.exe, dumpminitool.exe references: - https://twitter.com/bohops/status/1635288066909966338 - https://twitter.com/mrd0x/status/1511415432888131586 modified: 2023-07-18 author: Kaspersky status: stable tags: - attack.credential_access - attack.t1003.001 logsource: product: windows category: process_creation detection: selection_procdump: Image|endswith: - '\procdump.exe' - '\procdump64.exe' CommandLine|contains: 'lsass' selection_dotnet: Image|endswith: '\dotnet-dump.exe' CommandLine: ' collect ' selection_dumpminitool: Image|endswith: '\dumpminitool.exe' condition: 1 of selection* falsepositives: - Unknown level: high	转换方式与表格第 3 行中的规则相同。 差异：“选择条件 1*”中的条件是命名集合之一。	DeviceVendor=' DeviceProduct= DeviceEventCla (((Desti '\\procdump.ex '\\procdump64. 'lsass') OR (Destinati dump.exe' AND De) OR Destinati '\\dumpminitoo)
title: Generic-Clearing Windows Event Logs via Command Line id: a903492e-da40-4ab4-a92d-306a4799d973 description: Detects Clear Windows Event Logs via Command Line author: Kaspersky status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1070.001 logsource: product: windows category: process_creation detection: selection1: Image|endswith: '\wevtutil.exe' CommandLine|contains: - ' cl ' - 'clear' selection2: Image|endswith: - '\powershell.exe' - '\powershell_ise.exe' - '\pwsh.exe' CommandLine|contains: - 'Clear-EventLog' - 'Remove-EventLog' selection3: Image|endswith: '\wmic.exe' CommandLine|contains: - 'ClearEventLog' condition: 1 of them falsepositives: - Legitimate System Administrator actions level: high	"Microsoft products" normalizer tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows DeviceEventClassID=4688 selection1: DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" Selection2 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" selection3 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" condition DeviceVendor = Microsoft AND DeviceProduct = Windows AND DeviceEventClassID=4688 AND ((DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains ""))) identical fields - specify the fields from the condition, except Name, deviceProduct, deviceVendor	DeviceVendor=' DeviceProduct= DeviceEventCla ((Destinati '\\wevtutil.ex (Devic DeviceCustomSt) OR ((Destin '\\powershell. Des '\\powershell\ '\\pwsh.exe') A (Device EventLog' OR D 'Remove-EventL) OR (Destinatio AND DeviceC 'ClearEventLog)

Sigma 规则	映射到 OSMP 对象	
title: 0021-0002.1204.003 Execution - PowerExchangeDropper description: Detect the dropping of PowerExchange components. status: experimental logsource: product: windows service: Sysmon detection: selection1: EventID: 11 selection2: TargetFilename|contains: - 'c:\users\public\microsoftedge\autosave.exe' - 'c:\users\public\microsoftedge\wsdl.ps1' selection3: Image|endswith: "brochure.exe" condition: selection1 and selection2 and selection3 falsepositives: - Unknown level: high	Based on: Normalizer 11 of Sysmon event. title → name author → description description→ description status → description logsource DeviceVendor = Microsoft DeviceProduct = Sysmon selection1 DeviceEventClassID=11 selection2 FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '' if the file path contains * format in regexp selection3 OldFilePath endswith "" condition: DeviceVendor = Microsoft AND DeviceProduct = Sysmon AND (DeviceEventClassID=11) AND (FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '') AND (OldFilePath endswith "") identical fields—specify the fields from the condition, except Name, deviceProduct, deviceVendor level →severity falsepositive → Description	DeviceVendor=' DeviceProduct= DeviceEventCla (FilePath con 'c:\\users\\pu OR FilePath c 'c:\\users\\pu) AND OldFilePath en
标题：已加入域的主机发现 描述：检测攻击者使用 PowerShell 枚举已加入域的计算机的行为。 状态：稳定 日志源： product: windows service: security 检测： 选择： 事件 ID：4104 ScriptBlockText|包含|全部： - 'System.DirectoryServices.DirectorySearcher' - 'Properties.operatingsystem' 条件：选择 误报： - "管理脚本或工具，例如漏洞扫描工具" 级别：中	ScriptBlockText → 消息	

Sigma 规则	映射到 OSMP 对象	
标题：0022-0002.1053.005 执行 - PowerExchange 任务 描述：检测 PowerExchange 创建计划任务的行为。 状态：实验性 logsource: product: windows service: security 检测： 选择： 事件 ID： - '4698' TaskName|包含： - 'MicrosoftEdgeUpdateService' 条件：选择 falsepositives: - 未知 级别：中	TaskName → SourceProcessName	

Sigma 规则	映射到 OSMP 对象	
标题：从严重 Windows 进程创建 Windows Shell 描述：严重 Windows 进程的异常行为 status: stable 修改日期：2023-07-18 标签： - attack.defense_evasion - attack.t1036 logsource: product: windows category: process_creation detection: 选择： ParentImage|endswith： - '\searchindexer.exe' - '\lsaiso.exe' - '\lsm.exe' - '\spoolsv.exe' - '\wininit.exe' - '\smss.exe' - '\csrss.exe' - '\lsass.exe' - '\services.exe' - '\winlogon.exe' Image|endswith： - '\powershell_ise.exe' - '\cmstp.exe' - '\appvlp.exe' - '\mftrace.exe' - '\scriptrunner.exe' - '\forfiles.exe' - '\msiexec.exe' - '\rundll32.exe' - '\mshta.exe' - '\hh.exe' - '\wmic.exe' - '\regsvr32.exe' - '\scrcons.exe' - '\bash.exe' - '\sh.exe' - '\cscript.exe' - '\wscript.exe' - '\powershell.exe' - '\cmd.exe' 条件：选择 falsepositives: - Unknown 级别：高	ParentImage → SourceProcessName	

MITRE ATT&CK 矩阵覆盖范围

如果要通过关联规则评估 MITRE ATT&CK 矩阵的覆盖范围：

1. 从官方 MITRE ATT&CK 存储库下载 MITRE 技术列表并将其导入 KUMA。
2. 将 MITRE 技术映射到关联规则。
3. 将关联规则导出至 MITRE ATT&CK Navigator。

这样，您就可以直观地评估 MITRE ATT&CK 矩阵的覆盖范围。

导入 MITRE 技术列表

仅具有主管理员角色的用户才能导入 MITRE 技术列表。

要导入 MITRE ATT&CK 技术列表：

1. 从 GitHub 门户 下载 MITRE ATT&CK 技术列表。

   > KUMA 仅支持 MITRE ATT&CK 技术列表版本 14.1。

2. 在应用程序主窗口中，转到**设置**→**KUMA**→ **打开 KUMA 设置**部分。
   这将打开 KUMA 设置窗口。
3. 在“**其他**”下，单击“**通用**”。
4. 在 **MITRE 技术列表设置**中，单击“**从文件导入**”。
   将打开文件选择窗口。
5. 选择下载的 MITRE ATT&CK 技术列表，然后单击“**打开**”。

MITRE ATT&CK 技术列表将导入到 KUMA 中。您可以通过单击**查看列表**来查看导入的技术列表和MITRE ATT&CK 技术列表的版本。

将 MITRE 技术映射到关联规则

要将 MITRE ATT&CK 技术映射到关联规则：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**关联规则**”。
2. 单击关联规则的名称以打开关联规则编辑窗口。
   关联规则编辑窗口将打开。

3. 在“**常规**”选项卡上，单击“**MITRE 技术**”字段将打开可用技术的列表。为方便搜索，系统提供了过滤器，您可在其中输入技术名称、技术 ID 或战术 ID。您可以将一种或多种 MITRE ATT&CK 技术关联到相应的关联规则。

4. 单击“**保存**”按钮。

MITRE ATT&CK 技术已映射到关联规则。在 KUMA 控制台的“**监控**” → “**资源**” → “**关联规则**”部分中，已编辑规则的“**MITRE 技术**”列会显示所选技术的 ID，在将鼠标悬停在该 ID 上时，会显示该技术的全名，包括技术 ID 和战术 ID。

将关联规则导出至 MITRE ATT&CK Navigator

要将映射了 MITRE 技术的关联规则导出至 MITRE ATT&CK Navigator：

1. 在主菜单中，转到“**监控**” → “**资源**” → “**关联规则**”。

2. 单击右上角的省略号按钮 (...)。

3. 在下拉列表中，单击“**导出至 MITRE ATT&CK Navigator**”。

4. 在打开的窗口中，选择要导出的关联规则。

5. 单击“**确定**”。
   包含所导出规则的文件将下载到您的计算机上。

6. 将文件从计算机上传到“MITRE ATT&CK Navigator”，以评估 MITRE ATT&CK 矩阵的覆盖范围。

您可以评估 MITRE ATT&CK 矩阵的覆盖范围。

聚合规则

聚合规则允许您整合相同类型的重复事件，并将其替换为一个通用事件。聚合规则支持标准 KUMA 事件模式的字段以及扩展事件模式的字段。通过这种方式，您可以减少发送到存储和/或关联器的类似事件的数量，减少服务负载，节省数据存储空间和授权许可配额 (EPS)。当达到时间或事件数量阈值（以先发生者为准）时，将创建聚合事件。

对于聚合规则，您可以配置过滤器，并仅将其应用于符合指定条件的事件。

您可以在“**监控**”→ “**资源**”→ “**聚合规则**”下配置聚合规则，然后从收集器设置的下拉列表中选择已创建的聚合规则。您也可以直接在收集器设置中配置聚合规则。

可用的聚合规则设置

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
阈值	事件数量的阈值。当具有相同字段的事件累积到指定数量后，收集器便会生成一个聚合事件，并开始重新累积事件，以生成下一个聚合事件。默认值为 `100`。

设置	描述
触发后规则有效期	必需设置。 时间阈值（以秒为单位）。当指定的时间到期时，基础事件停止累积，收集器会创建一个聚合事件，并开始重新累积事件，以生成下一个聚合事件。默认值为 `60`。
描述	资源描述：最多 4,000 个 Unicode 字符。
相同字段	必需设置。 此下拉列表列出了必须具有相同值的规范化事件的字段。例如，对于网络事件，您可以使用 SourceAddress、DestinationAddress 和 DestinationPort 字段。在聚合事件中，这些字段将填充基础事件的值。
唯一字段	此下拉列表列出了必须在聚合事件中保存其值范围的字段。例如，如果在"**唯一字段**"中指定了 DestinationPort 字段，而未在"**相同字段**"中未指定，则聚合事件将整合多个端口的基础连接事件，并且聚合事件的 DestinationPort 字段包含所有已建立连接的端口的列表。
求和字段	在此下拉列表中，您可以选择在聚合过程中求和的字段，其求和结果将写入聚合事件中的同名字段。

设置	描述
过滤器	用于指定需由此资源处理的事件识别条件的设置组。您可以从下拉列表中选择现有过滤器，也可以**创建**新过滤器。 在聚合规则中，请勿使用带有“**TI**”操作数或“**TIDetect**”、“**inActiveDirectoryGroup**”或“**hasVulnerability**”运算符的过滤器。可以使用“**inActiveDirectoryGroup**”运算符的 Active Directory 字段将在增强阶段（执行聚合规则之后）显示。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在“**过滤器**”下拉列表中，选择“**新建**”。 2. 如果要将过滤器保留为单独的资源，请选中“**保存过滤器**”复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了“**保存过滤器**”复选框，请在“**名称**”字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在“**条件**”下，指定事件必须满足的条件： a. 单击“**添加条件**”按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在“**右操作数**”字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择“**活动列表**”时，必须指定活动列表的名称、条目键和条目键字段。 c. 在“**运算符**”下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中“**大小写不匹配**”复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从“**If**”下拉列表中选择“**如果不是** 。 您可以添加多个条件或一组条件。

设置	描述
	5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

服务选项卡

此选项卡仅在您编辑已创建的聚合规则的设置时显示；在此选项卡上，您可以将规则关联到收集器。

若要将聚合规则关联到收集器，请点击**关联至服务→关联至收集器**。这将打开一个窗口；在该窗口中，选择一个或多个收集器，然后点击**确定**。聚合规则将关联到所选收集器，并根据其配置应用。

如有必要，您可以将聚合规则与收集器取消关联。要执行此操作，请选中收集器旁边的复选框，单击**删除**，然后确认与该服务取消关联。

预定义聚合规则

OSMP 分发包中包含下表所列的聚合规则。

聚合规则名称	描述
[OOTB] Netflow 9	该规则在达到 100 个事件或 10 秒后触发。 事件按以下字段聚合： • DestinationAddress • DestinationPort • SourceAddress • TransportProtocol • DeviceVendor • DeviceProduct 对“DeviceCustomString1”和“BytesIn”字段进行求和。

增强规则

*事件增强*涉及向事件添加可用于识别和调查事故的信息。

增强规则允许您通过转换字段中已有的数据或查询外部系统的数据来向事件字段添加补充信息。例如，假设事件中记录了用户名。您可以使用增强规则将有关此用户的部门、职位和经理的信息添加到事件字段。

增强规则可用于以下 KUMA 服务和功能：

- 收集器。
- 关联器。
- 规范化器。

可用的增强规则设置列于下表。

"基本设置"选项卡

设置	描述

源类型	必需设置。 用于选择传入事件类型的下拉列表。根据所选类型，将显示以下附加设置： • **常量** 在需要将常量添加到事件字段时，将使用此类型的增强规则。此类增强功能的设置： • 在"**常量**"字段中，指定应添加到事件字段的值。该值的长度不得超过 255 个 Unicode 字符。如果将此字段留空，则会清除现有的事件字段值。 • 在"**目标字段**"下拉列表中，选择要写入数据的 KUMA 事件字段。 如果对 `String`、`Number` 或 `Float` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到字段中。 如果对 `Array of strings`、`Array of numbers` 或 `Array of floats` 类型的扩展模式字段使用事件增强函数并指定常量，则该常量会被添加到数组元素中。 • **词典** 如果需要从"字典"类型的**字典**中添加值，则使用此类型的增强规则。 在"**字典名称**"下拉列表中选择此类型后，必须选择用于提供值的字典。在"**键字段**"设置块中，您必须点击"**添加字段**"按钮，然后选择相应的事件字段，其值将用于词典条目选择。 如果您使用事件增强功能，并在"源类型"设置中选择了"字典"类型，且在"键增强字段"设置中指定了数组字段，则在数组作为字典键进行查询时，将按照 TSV 格式序列化单个值的规则，将该数组转化成一个字符串。 示例："键增强字段"设置使用 SA.StringArrayOne 扩展架构字段。SA.StringArrayOne 扩展架构字段包含 3 个元素："a"、"b"和"c"。以下值作为键传递给字典：['a','b','c']。 如果"键增强字段"设置使用扩展架构数组字段和常规事件模式字段，则在查询词典时，字段值将以"|"字符分隔。 示例："键增强字段"设置使用两个字段：SA.StringArrayOne 扩展架构字段和 Code 字段。SA.StringArrayOne 扩展架构字段包含 3 个元素："a"、"b"和"c"；Code 字符串字段包含字符序列"myCode"。以下值作为键传递给词典：['a','b','c']myCode。 • **表格** 如果您需要从"表格"类型的**字典**中添加值，则需使用此类型的增强功能。 在"**字典名称**"下拉列表中选择此增强类型后，选择用于提供值的字典。在"**键字段**"设置组中，单击"**添加字段**"按钮以选择其值用于字典条目选择的事件字段。 在"**映射**"表格中，配置用于提供数据的字典字段和用于接收数据的事件字段： • 在"**字典字段**"列中，选择字典字段。可用字段取决于所选的字典资源。 • 在"KUMA **字段**"列中，选择要写入值的事件字段。对于某些所选字段（`*custom*` 和 `*flex*`），在"**标签**"列中，可以为写入其中的数据指定一个名称。 可通过单击"**添加新元素**"按钮添加新的表行。可通过单击 ✕ 按钮删除列。 • **事件** 若需要将值从另一个事件字段写入当前事件字段时，可使用此类增强类型。此类增强功能的设置： • 在"**目标字段**"下拉列表中，选择要写入数据的 KUMA 事件字段。 • 在"**源字段**"下拉列表中，选择要将其值写入目标字段的事件字段。 • 在"**转换**"下，您可以创建规则，以便在将原始数据写入 KUMA 事件字段之前对其进行修改。可以从下拉列表中选择转换类型。您可以使用"**添加转换**"和"**删除转换**"按钮来添加或删除转换。转换的顺序很重要。 **可用转换** 转换是在将值写入事件字段之前可以应用于该值的更改。转换类型可以从下拉列表中选择。 可用转换： • **entropy** 用于使用信息熵计算函数转换源字段的值，并将转换结果放置在浮点类型的目标字段中。转换结果是一个数字。计算信息熵可以检测 DNS 隧道或已泄露的密码，例如，当用户输入密码而不是登录名时，该密码会以明文形式记录下来。 • **lower** — 用于将值的所有字符变为小写 • **upper** — 用于将值的所有字符变为大写 • **regexp** — 用于使用正则表达式 RE2 来转换值。选择此转换类型后，会出现一个字段，应该在其中添加正则表达式。 • **substring** — 用于提取"**开始**"和"**结束**"字段中指定位置范围内的字符。选择此转换类型时，这些字段会出现。

- **replace** — 用于将指定的字符序列替换为其他字符序列。选择此转换类型时，会出现新字段：
  - **Replace chars** — 您可以在此字段中指定要替换的字符序列。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- **trim** — 用于同时从值的开始和结束位置删除"字符"字段中指定的字符。选择此转换类型时，会出现此字段。例如，对"Microsoft-Windows-Sysmon"应用"Micromon"值的去除首尾字符转换后，结果为"soft-Windows-Sys"。
- **append** 用于将"常量"字段中指定的字符添加到事件字段值的末尾。选择此转换类型时，会出现此字段。
- **prepend** — 用于将"常量"字段中指定的字符添加到事件字段值的开头。选择此转换类型时，会出现此字段。
- **replace with regexp** — 用于将 RE2 正则表达式结果替换为字符序列。
  - **Expression** — 您可以在此字段中指定应替换结果的正则表达式。
  - **With chars** — 您可以在此字段中指定应使用的字符序列，而不是替换的字符。
- 将编码字符串转换为文本：
  - **decodeHexString** — 用于将 HEX 字符串转换为文本。
  - **decodeBase64String** — 用于将 Base64 字符串转换为文本。
  - **decodeBase64URLString** — 用于将 Base64url 字符串转换为文本。

  转换损坏的字符串或发生转换错误时，损坏的数据可能会被写入事件字段。
  在事件增强期间，如果编码字符串的长度超过了规范化事件字段的大小，则字符串会被截断并且不会被解码。
  如果解码字符串的长度超出了要写入解码值的事件字段的大小，则会截断该字符串以适应事件字段的大小。

使用扩展事件模式时的转换

是否可以使用转换取决于所使用的扩展事件模式字段的类型：

- 对于 `String` 类型的附加字段，所有类型的转换均可用。
- 对于 `Number` 和 `Float` 类型的字段，可进行以下类型的转换：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 对于 `Array of strings`、`Array of numbers` 和 `Array of floats` 类型的字段，可进行以下类型的转换：append、prepend。

- **模板**

  在需要将通过处理 Go 模板获得的值写入事件字段时，可使用这种类型的增强功能。此类增强功能的设置：

  - 在"**模板**"字段中，输入 Go 模板。
    事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是需要将其值传递给脚本的事件字段名称。
    例如： `Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。
  - 在"**目标字段**"下拉列表中，选择要写入数据的 KUMA 事件字段。

  要将模板中的数组字段数据转换为 TSV 格式，必须使用 toString 函数。

  如果您使用事件增强功能，并在"**源类型**"设置中选择了"**模板**"类型，且目标字段的类型为 `String`、源字段是包含字符串数组的扩展事件架构字段，则可以使用以下任一模板示例。

  例如：

  {{.SA.StringArrayOne}}

  例如：

  {{- range $index, $element := .SA.StringArrayOne -}}

  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

  这种类型的增强功能用于向私有网络 DNS 服务器发送请求，以实现 IP 地址与域名之间的相互转换。仅对以下私有地址进行 IP 地址到 DNS 名称的转换：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、100.64.0.0/10、fd00::/8。

  下表介绍了此类增强功能的设置。

"dns"类型的增强功能参数

设置	描述
网址	要向其发送请求的 DNS 服务器的 URL。 您可以使用 **添加 URL** 按钮指定多个 URL。 如果未指定 **URL** 设置，KUMA 将从本地主机的 `/etc/resolv.conf` 文件中获取 DNS 服务器列表。在这种情况下，您需要启用 **递归查询** 选项。否则，将不会执行增强操作。
每秒请求数	每秒向 DNS 服务器发送的最大查询数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
工作进程	服务可以同时运行以并行处理响应规则的处理程序数量。请指定一个介于 0 到 999 之间的正整数。如果指定为 0，则使用逻辑 CPU 核心数。默认值为 `1`。
数据增强队列中的最大事件数	重新提交队列中可容纳的最大事件数。默认值为 `1,000,000`。
超时时间	等待 DNS 服务器响应的时间（以秒为单位）。默认值为 `5`。
DNS 模式覆盖	使用的解析方法： • **仅正向 DNS**将域名解析为 IP 地址。 • **仅反向 DNS**将 IP 地址解析为域名。 • **正向和反向 DNS**将域名解析为 IP 地址，或将 IP 地址解析为域名。
缓存 TTL	缓存中存储的值的生存时间（以秒为单位）。默认值为 `60` 秒。
缓存已停用	您可以使用此设置启用或禁用缓存。默认情况下启用缓存。
缓存刷新已停用	如果启用了缓存更新，当缓存的 TTL 到期时，收集器会多次向 DNS 服务器发送请求，以更新缓存中存储的数据。此设置仅在启用缓存时可用。默认情况下，缓存更新已启用。
递归查询	允许收集器向权威 DNS 服务器发送递归查询，以进行数据增强。默认值是"**已禁用**"。

- **cybertrace**

  此类增强功能用于将 CyberTrace 数据流中的信息添加到事件字段。

  可用设置：

  - **URL**（必填）— 在此字段中，您可以指定要向其发送请求的 CyberTrace 服务器的 URL。
  - **连接数** — KUMA 可与 CyberTrace 服务器建立的最大同时连接数。默认情况下，此值等于 KUMA Core 服务器的 vCPU 数量。
  - **RPS** — 每秒向服务器发送的最大请求数。默认值为 `1000`。
  - **超时** — 等待 CyberTrace 服务器响应的时间（以秒为单位）。默认值为 `30`。
  - **映射**（必需）— 此设置块包含用于将 KUMA 事件字段映射到 CyberTrace 指标类型的映射表。**KUMA 字段**列显示 KUMA 事件字段的名称，**CyberTrace 指标**列显示 CyberTrace 指标的类型。
    可用的 CyberTrace 指标类型：
    - **ip**
    - **url**
    - **哈希**

    在映射表中，您必须提供至少一个字符串。您可以单击"**添加行**"按钮来添加字符串，也可以单击 ✕ 按钮来删除字符串。

- **cybertrace-http**

  此类增强功能用于使用 REST API 将 CyberTrace 数据流中的信息添加到事件字段。

  可用设置：

  - **URL**（必填）— 在此字段中，您可以指定要向其发送请求的 CyberTrace 服务器的 URL。
  - "**密钥**"（必填）是一个下拉列表，您可以在其中选择存储连接凭证的密钥。
  - **超时** — 等待 CyberTrace 服务器响应的时间（以秒为单位）。默认值是 30。
  - "**键字段**"（必填）是用于通过 CyberTrace 数据丰富来增强事件的事件字段列表。
  - **增强队列中的最大事件数量** — 存储在增强队列中用于重新发送的最大事件数量。默认值是 1000000000。从 CyberTrace 服务器接收的事件达到 100 万个后，事件增强将停止，直到接收的事件数量减少到 50 万个以下。

  > 当队列中接收的事件数达到 100 万个时，事件增强将停止，并且事件将以未增强状态记录在存储中，直到队列中接收的事件数量少于 50 万个。

- **时区**

  这种类型的增强功能在收集器和关联器中用于为事件分配特定的时区。在搜索发生在异常时间（例如夜间）的事件时，时区信息可能很有用。

选择这种类型的增强功能时，必须从“**时区**”下拉列表中选择所需的时区。

确保在增强功能服务的托管服务器上，已设置所需的时区。例如，您可以使用 `timedatectl list-timezones` 命令，该命令显示服务器上设置的所有时区。有关设置时区的更多详细信息，请参阅您的操作系统文档。

对事件进行增强后，所选时区相对于世界协调时 (UTC) 的时间偏移量会以 `+-hh:mm` 格式写入 DeviceTimeZone 事件字段。例如，如果您选择 **Asia/Yekaterinburg** 时区，则值 `+05:00` 将被写入 DeviceTimeZone 字段。如果经过增强的事件在 DeviceTimeZone 字段中已经存在值，则该值将被覆盖。

默认情况下，如果未在正在处理的事件中指定时区，并且未配置按时区增强规则，则将为事件分配处理事件的服务（收集器或关联器）所在服务器的时区。如果服务器时间被更改，则必须重启服务。

丰富 DeviceTimeZone 字段时允许的时间格式

在收集器中处理传入的原始事件时，以下时间格式可以自动转换为 +-hh:mm 格式：

已处理事件中的时间格式	示例
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

如果 `DeviceTimeZone` 字段中的日期格式与上述所列格式不同，那么在使用时区信息对事件进行增强时，收集器服务器的时区将会被写入该字段。您可以为非标准时间格式创建自定义规范化规则。

- **geographic data**

  这种类型的增强功能用于将 IP 地址的地理数据添加到事件字段。了解有关将 IP 地址关联到地理数据的更多信息。

  选择此类型后，在**将地理数据映射到事件字段**下，您必须指定从哪个事件字段读取 IP 地址，选择所需的地理数据属性，并定义要将地理数据写入的事件字段：

  1. 在**带有 IP 地址的事件字段**下拉列表中，选择从中读取 IP 地址的事件字段。上传到 KUMA 的地理数据与此 IP 地址匹配。

     您可以使用“**添加带有 IP 地址的事件字段**”按钮来指定需要增强地理数据的多个带有 IP 地址的事件字段。单击“**删除带有 IP 地址的事件字段**”按钮，即可删除以这种方式添加的事件字段。

     选择 `SourceAddress`、`DestinationAddress` 和 `DeviceAddress` 事件字段后，“**应用默认映射**”按钮将变为可用。您可以点击此按钮来添加地理数据属性和事件字段的预配置映射对。

  2. 对于需要从中读取 IP 地址的每个事件字段，选择地理数据的类型以及要将地理数据写入其中的事件字段。

     您可以使用“**添加地理数据属性**”按钮来添加“**地理数据属性 - 目标事件字段**”的字段对。您还可以为一个 IP 地址配置不同类型的地理数据，以将其写入不同的事件字段。要删除字段对，请单击 ❌。

     - 在“**地理数据属性**”字段中，选择与所读取的 IP 地址对应且应该被写入事件的地理数据。可用的地理数据属性：**国家/地区**、**地区**、**城市**、**经度**、**纬度**。
     - 在**目标“事件”字段**中，选择必须写入所选地理数据属性的事件字段。

     您可以将相同的地理数据属性写入不同的事件字段。如果配置了多个地理数据属性写入同一事件字段，则事件将以序列中最后一个映射的结果为准。

名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
调试	您可以使用此切换开关来启用服务操作的日志记录。日志记录默认被禁用。
描述	资源描述：最多 4,000 个 Unicode 字符。

过滤器

用于指定需由此资源处理的事件识别条件的设置组。您可以从下拉列表中选择现有过滤器，也可以**创建**新过滤器。

在资源中创建过滤器

KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。

要创建过滤器：

1. 在"**过滤器**"下拉列表中，选择"**新建**"。
2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。
3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。
4. 在**"条件"**下，指定事件必须满足的条件：
   a. 单击"**添加条件**"按钮。
   b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。
   c. 在"**运算符**"下拉列表中，选择一个运算符。
   过滤器运算符
   - **=** — 左操作数等于右操作数。
   - **<** — 左操作数小于右操作数。
   - **<=** — 左操作数小于或等于右操作数。
   - **>** — 左操作数大于右操作数。
   - **>=** — 左操作数大于或等于右操作数。
   - **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。
   - **contains** — 左操作数包含右操作数的值。
   - **startsWith** — 左操作数以右操作数的某个值开头。
   - **endsWith** — 左操作数以右操作数的某个值结尾。
   - **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。
   - **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。
     待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。
     如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。
   - **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。
     如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。
   - **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。
   - **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。
   - **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。
   - **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。
   - **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。
   - **inContextTable** — 检查指定的上下文表中是否存在该条目。
   - **intersect** — 右操作数中指定的列表项是否存在于左操作数中。
   d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。
   e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是** 。

   您可以添加多个条件或一组条件。
5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。
6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

此选项卡仅在您编辑已创建的增强规则的设置时显示；在此选项卡上，您可以将规则链接到服务，即关联器和收集器。

要将增强规则关联到收集器或关联器，请单击**关联至服务**按钮→**关联到<服务名称>**。这将打开一个窗口；在该窗口中，选择一个或多个关联器或收集器，然后单击“**确定**”。增强规则将链接到所选服务，并根据其配置应用。

如有必要，您可以将聚合规则与服务取消链接。为此，请选中关联器或收集器旁边的复选框，单击“**删除**”，然后确认取消与服务的链接。

预定义的增强规则

OSMP 分发包中包含下表所列的增强规则。

预定义的增强规则

增强规则名称	描述
[OOTB] KATA 警报	用于以指向警报的超链接形式来增强从 KATA 接收的事件。超链接放在“DeviceExternalId”字段中。

响应规则

借助响应规则，您可以启动 Kaspersky Security Center 任务的自动运行、针对 Kaspersky Endpoint Detection and Response、KICS for Networks、Active Directory 的威胁响应操作以及针对特定事件运行自定义脚本。

与相关程序集成后，可以根据响应规则自动执行 Kaspersky Security Center 任务、Kaspersky Endpoint Detection and Response 任务以及 KICS for Networks 和 Active Directory 任务。

您可以在“**监控**”→ “**资源**”→ “**响应规则**”下配置响应规则，然后从关联器设置的下拉列表中选择已创建的响应规则。您还可以直接在关联器设置中配置响应规则。

Kaspersky Security Center 的响应规则

您可以配置响应规则以自动启动反病毒扫描任务和 Kaspersky Security Center 资产的更新。

在创建和编辑 Kaspersky Security Center 的响应规则时，您需要定义以下设置的值。

“常规”选项卡

响应规则设置

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
类型	必需设置，当 KUMA 与 Kaspersky Security Center 集成时可用。 响应规则 **osmptasks**。
Open Single Management Platform 任务	必需设置。 要运行的 Kaspersky Security Center 任务的名称。任务必须提前创建，并且其名称必须以“`KUMA`”开头。例如，`KUMA antivirus check`（不区分大小写且不带引号）。 您可以使用 KUMA 运行以下类型的 Kaspersky Security Center 任务： • 更新 • 病毒扫描
事件字段	必需设置。 定义应为其启动 Kaspersky Security Center 任务的资产的事件字段。可能值： • SourceAssetID • DestinationAssetID • 设备资产 ID
工作进程数	服务可以同时运行的进程数。默认情况下，工作进程数与安装程序服务的服务器上的虚拟处理器数相同。
描述	响应规则的描述。您最多可以添加 4,000 个 Unicode 字符。

设置	描述
过滤器	用于定义使用响应规则处理事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是** 。 您可以添加多个条件或一组条件。

设置	描述
	5. 如果您添加了多个条件或条件组，请单击“**AND**”按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从“**选择筛选器**”下拉列表中选择的现有过滤器，请单击“**添加过滤器**”按钮。您可以通过单击“”按钮查看嵌套过滤器设置。

要向 Kaspersky Security Center 发送请求，您必须确保 Kaspersky Security Center 可通过 UDP 协议使用。

如果响应规则属于共享租户，则主租户所连接的 Kaspersky Security Center 服务器上的任务将显示为可供选择的 Kaspersky Security Center 任务。

如果响应规则选择了租户连接到的 Kaspersky Security Center 服务器中不存在的任务，则不会针对此租户的资产执行该任务。例如，当两个租户使用同一个关联器时，可能会出现这种情况。

服务选项卡

此选项卡仅在您编辑已创建的响应规则的设置时显示；在此选项卡上，您可以将规则关联到关联器。

要将目标位置链接到关联器，请单击**关联至服务”**按钮 → **关联至关联器**。这将打开一个窗口；在该窗口中，选择一个或多个关联器，然后点击**确定**。响应规则将关联到所选关联器，并根据其配置应用。

如有必要，您可以将响应规则与服务取消关联。要执行此操作，请选中关联器旁边的复选框，单击**删除**，然后确认与该服务取消关联。

自定义脚本的响应规则

您可以创建一个脚本，其中包含在检测到选定事件时在 KUMA 服务器上执行的命令，并配置响应规则以自动运行此脚本。在这种情况下，程序将在收到与响应规则匹配的事件时运行该脚本。

脚本文件存储在安装了使用响应资源的关联器服务的服务器上：/opt/kaspersky/kuma/correlator/<关联器 ID>/scripts。此服务器的 kuma 用户需要运行该脚本的权限。

创建和编辑自定义脚本的响应规则时，需要定义以下参数的值。

“常规”选项卡

响应规则设置

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。

设置	描述
类型	必需设置。 响应规则类型：**脚本**。
超时	分配给脚本完成的秒数。如果超过此时间量，脚本将终止。
脚本名称	必需设置。 脚本文件的名称。 如果响应资源已附加到关联器服务，但 /opt/kaspersky/kuma/correlator/<关联器 ID>/scripts 文件夹中没有脚本文件，则关联器将无法运行。
脚本参数	必须传递给脚本的参数或事件字段值。 如果脚本包含对文件采取的操作，则应指定这些文件的绝对路径。 参数可以用引号 (") 括起书写。 事件字段名称以 `{{.EventField}}` 格式传递，其中 `EventField` 是其值必须传递给脚本的事件字段的名称。 例如： `-n "\"usr\": {{.SourceUserName}}"`
工作进程数	服务可以同时运行的进程数。默认情况下，工作进程数与安装程序服务的服务器上的虚拟处理器数相同。
描述	资源描述。您最多可以添加 4,000 个 Unicode 字符。

设置	描述
过滤器	用于定义使用响应规则处理事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在"**条件**"下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是** 。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

此选项卡仅在您编辑已创建的响应规则的设置时显示；在此选项卡上，您可以将规则关联到关联器。

要将目标位置链接到关联器，请单击**关联至服务"**按钮 → **关联至关联器**。这将打开一个窗口；在该窗口中，选择一个或多个关联器，然后点击**确定**。响应规则将关联到所选关联器，并根据其配置应用。

如有必要，您可以将响应规则与服务取消关联。要执行此操作，请选中关联器旁边的复选框，单击**删除**，然后确认与该服务取消关联。

KICS for Networks 的响应规则

您可以配置响应规则以自动触发对 KICS for Networks 资产执行的响应操作。例如，您可以在 KICS for Networks 中更改资产状态。

在创建和编辑 KICS for Networks 的响应规则时，您需要定义以下设置的值。

"常规"选项卡

响应规则设置

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
类型	必需设置。 响应规则类型：**kics**。
事件字段	必需设置。 指定必须执行响应操作的资产的事件字段。可能值： • SourceAssetID • DestinationAssetID • 设备资产 ID
KICS for Networks 任务	收到与过滤器匹配的数据时要执行的响应操作。可用的响应操作类型如下： • **将资产状态更改为已授权**。 • **将资产状态更改为未授权**。 当触发响应规则时，KUMA 将向 KICS for Networks 发送 API 请求，以将指定设备的状态更改为"**已授权**"或"**未授权**"。
工作进程数	服务可以同时运行的进程数。默认情况下，工作进程数与安装程序服务的服务器上的虚拟处理器数相同。
描述	资源描述。您最多可以添加 4,000 个 Unicode 字符。

设置	描述
过滤器	用于定义使用响应规则处理事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** – 左操作数等于右操作数。 • **<** – 左操作数小于右操作数。 • **<=** – 左操作数小于或等于右操作数。 • **>** – 左操作数大于右操作数。 • **>=** – 左操作数大于或等于右操作数。 • **inSubnet** – 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** – 左操作数包含右操作数的值。 • **startsWith** – 左操作数以右操作数的某个值开头。 • **endsWith** – 左操作数以右操作数的某个值结尾。 • **match** – 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** – 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** – 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** – 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** – 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** – 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** – 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** – 检查指定的上下文表中是否存在该条目。 • **intersect** – 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是**"。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

此选项卡仅在您编辑已创建的响应规则的设置时显示；在此选项卡上，您可以将规则关联到关联器。

要将目标位置链接到关联器，请单击**关联至服务"**按钮 → **关联至关联器**。这将打开一个窗口；在该窗口中，选择一个或多个关联器，然后点击**确定**。响应规则将关联到所选关联器，并根据其配置应用。

如有必要，您可以将响应规则与服务取消关联。要执行此操作，请选中关联器旁边的复选框，单击**删除**，然后确认与该服务取消关联。

Kaspersky Endpoint Detection and Response 的响应规则

您可以配置响应规则，以自动触发针对 Kaspersky Endpoint Detection and Response 资产的响应操作。例如，您可以配置资产网络自动隔离。

在创建和编辑 Kaspersky Endpoint Detection and Response 的响应规则时，您需要定义以下设置的值。

"常规"选项卡

响应规则设置

设置	描述
事件字段	必需设置。 指定必须执行响应操作的资产的事件字段。可能值： • SourceAssetID • DestinationAssetID • 设备资产 ID

设置	描述
任务类型	收到与过滤器匹配的数据时要执行的响应操作。可用的响应操作类型如下： • 启用网络隔离。选择此类型的响应时，您需要定义以下设置的值： • **隔离超时** — 资产的网络隔离处于活动状态的小时数。您可以设置 1 到 9,999 小时之间的数值。如有必要，您可以**添加网络隔离排除项**。 *要添加网络隔离排除项：* a. 单击"**添加排除项**"按钮。 b. 选择不得阻止的网络流量方向： • 入站。 • 出站。 • 入站/出站。 c. 在"**资产 IP**"字段中，输入不得阻止其网络流量的资产的 IP 地址。 d. 如果选择了"**入站**"或"**出站**"，请在"**远程端口**"和"**本地端口**"字段中指定连接端口。 e. 如果要添加多个排除项，请单击"**添加排除项**"，然后重复相关步骤填写"**流量方向**"、"**资产 IP**"、"**远程端口**"和"**本地端口**"字段。 f. 如果要删除某个排除项，请单击相关排除项下方的"**删除**"按钮。 在向网络隔离规则添加排除项时，Kaspersky Endpoint Detection and Response 可能会错误显示规则详细信息中的端口值。这不会影响应用程序性能。有关查看网络隔离规则的更多详细信息，请参阅 *Kaspersky Anti Targeted Attack Platform 帮助指南*。 • 禁用网络隔离。 • 添加预防规则。选择此类型的响应时，您需要定义以下设置的值： • **要从中提取哈希的事件字段** — KUMA 从中提取 SHA256 或 MD5 哈希值的事件字段，所对应的文件必须被阻止运行。必须将选定的事件字段以及在**事件字段**中选择的值添加到关联规则的传播字段中。 • **文件哈希值 #1** — 要阻止的文件的 SHA256 或 MD5 哈希值。 必须至少填写上述字段之一。 • 删除预防规则。 • 启动应用程序。选择此类型的响应时，您需要定义以下设置的值： • **文件路径** — 要启动的进程的文件路径。 • **命令行参数** — 要用来启动文件的参数。 • **工作目录** — 启动时文件所在的目录。 针对具有主管理员角色的用户触发响应规则时，将在程序控制台的"**任务管理器**"部分显示"**运行程序**"任务。对于此任务，**任务表**的创建者列中显示**已排定的任务**。您可以查看任务完成结果。 所有列出的操作都可以在安装了 Kaspersky Endpoint Agent for Windows 的资产上执行。在安装了 Kaspersky Endpoint Agent for Linux 的资产上，该程序仅可执行启动操作。 在软件层面，针对已安装 Kaspersky Endpoint Agent for Linux 的资产，创建防护规则和网络隔离规则的能力不受限制。KUMA 和 Kaspersky Endpoint Detection and Response 不提供任何有关这些规则应用失败的通知。
工作进程数	服务可以同时运行的进程数。默认情况下，工作进程数与安装程序服务的服务器上的虚拟处理器数相同。
描述	响应规则的描述。您最多可以添加 4,000 个 Unicode 字符。

设置	描述
过滤器	用于定义使用响应规则处理事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在"**条件**"下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在"**左操作数**"和"**右操作数**"下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是** 。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

此选项卡仅在您编辑已创建的响应规则的设置时显示；在此选项卡上，您可以将规则关联到关联器。

要将目标位置链接到关联器，请单击**关联至服务"**按钮 → **关联至关联器**。这将打开一个窗口；在该窗口中，选择一个或多个关联器，然后点击**确定**。响应规则将关联到所选关联器，并根据其配置应用。

如有必要，您可以将响应规则与服务取消关联。要执行此操作，请选中关联器旁边的复选框，单击**删除**，然后确认与该服务取消关联。

Active Directory 响应规则

Active Directory 响应规则定义在触发规则时要应用于账户的操作。

使用 Active Directory 创建和编辑响应规则时，请指定以下设置的值。

"常规"选项卡

响应规则设置

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。
类型	必需设置。 响应规则类型：**通过 Active Directory 响应**。
账户 ID 源	从中获取 Active Directory 账户 ID 值的事件字段。可能值： • SourceAccountID • 目标账户 ID
AD 命令	触发响应规则时应用于账户的命令。 可用值： • **将账户添加到组** 要将账户移出或移入的 Active Directory 组。 在必填字段"**可分辨名称**"中，您必须指定组的完整路径。 例如，CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。 一次操作中只能指定一个组。 • **从组中删除账户** 要将账户移出或移入的 Active Directory 组。 在必填字段"**可分辨名称**"中，您必须指定组的完整路径。 例如，CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。 一次操作中只能指定一个组。 • 重置账户密码 如果您的 Active Directory 域允许选择"**用户不能更改密码**"复选框，则以重置用户账户密码作为响应操作将导致与用户账户的要求冲突：用户将无法进行身份验证。域管理员需要清除受影响的用户账户的复选框之一："**用户不能更改密码**"或"**用户必须在下次登录时更改密码**"。 • 阻止账户(B)

设置	描述
过滤器	用于定义使用响应规则处理事件的条件。您可以从下拉列表中选择现有过滤器，也可以创建新过滤器。 **在资源中创建过滤器** KUMA事件的所有字段都有默认值。对于所有数值字段，默认值为0。对于所有字符串字段，默认值为空字符串。如果事件没有某个字段，则该字段使用默认值。因此，即使事件本身不包含筛选器中指定的字段，该事件也可以触发筛选器。例如，如果您在筛选器中指定了 `DestinationPort <= 1024` 条件，但事件不包含 `DestinationPort` 字段，筛选器仍会被触发，因为默认情况下 `DestinationPort = 0`。 *要创建过滤器：* 1. 在"**过滤器**"下拉列表中，选择"**新建**"。 2. 如果要将过滤器保留为单独的资源，请选中"**保存过滤器**"复选框。在这种情况下，您将能够在各种服务中使用创建的过滤器。默认情况下，此复选框未被选中。 3. 如果您选中了"**保存过滤器**"复选框，请在"**名称**"字段中输入创建的过滤器资源的名称。名称的最大长度：128 个 Unicode 字符。 4. 在**"条件"**下，指定事件必须满足的条件： a. 单击"**添加条件**"按钮。 b. 在**左操作数**和**右操作数**下拉列表中，指定搜索参数。根据在"**右操作数**"字段中选择的数据源，可能会显示用于标识要传递给过滤器的值的附加参数字段。例如，当您选择"**活动列表**"时，必须指定活动列表的名称、条目键和条目键字段。 c. 在"**运算符**"下拉列表中，选择一个运算符。 **过滤器运算符** • **=** — 左操作数等于右操作数。 • **<** — 左操作数小于右操作数。 • **<=** — 左操作数小于或等于右操作数。 • **>** — 左操作数大于右操作数。 • **>=** — 左操作数大于或等于右操作数。 • **inSubnet** — 左操作数（IP 地址）位于右操作数（子网）的子网中。 • **contains** — 左操作数包含右操作数的值。 • **startsWith** — 左操作数以右操作数的某个值开头。 • **endsWith** — 左操作数以右操作数的某个值结尾。 • **match** — 左操作数与右操作数的正则表达式匹配。使用 RE2 正则表达式。 • **hasBit** — 检查左操作数（字符串或数字）是否包含其位置列于右操作数（常量或列表中）的位。 待检查的值将转换为二进制，并从右到左进行处理。检查其索引被指定为常量或列表的字符。 如果检查的值是字符串，则尝试将其转换为整数并按照上面描述的方式进行处理。如果字符串无法转换为数字，则过滤器返回 `False`。 • **hasVulnerability** — 检查左操作数是否包含具有右操作数中指定的漏洞和漏洞严重级别的资产。 如果没有指定漏洞的 ID 和严重级别，则当所检查事件中的资产存在任何漏洞时，会触发过滤器。 • **inActiveList** — 此运算符只有一个操作数。其值在**键字段**中选择，并与从活动列表下拉列表中选择的活动列表中的条目进行比较。 • **inDictionary** 检查指定的字典是否包含由选定事件字段的串联值组成的键所定义的条目。 • **inCategory** — 左操作数中的资产至少分配有右操作数的一个资产类别。 • **inActiveDirectoryGroup** — 左操作数中的 Active Directory 账户属于右操作数中的某个 Active Directory 组。 • **TIDetect** — 此运算符用于使用 CyberTrace 威胁情报 (TI) 数据查找事件。此运算符只能用于已使用 CyberTrace 威胁情报数据完成增强的事件。换言之，它只能在收集器的目标位置选择阶段以及关联器中使用。 • **inContextTable** — 检查指定的上下文表中是否存在该条目。 • **intersect** — 右操作数中指定的列表项是否存在于左操作数中。 d. 如果您希望运算符不区分大小写，请选中"**大小写不匹配**"复选框。此复选框不适用于 **InSubnet**、**InActiveList**、**InCategory** 或 **InActiveDirectoryGroup** 运算符。默认情况下，此复选框未被选中。 e. 如果要添加否定条件，请从**"If"**下拉列表中选择"**如果不是**"。 您可以添加多个条件或一组条件。 5. 如果您添加了多个条件或条件组，请单击"**AND**"按钮来选择逻辑条件（**and**、**or**、**not**）。 6. 如果您要添加从"**选择筛选器**"下拉列表中选择的现有过滤器，请单击"**添加过滤器**"按钮。您可以通过单击"↗"按钮查看嵌套过滤器设置。

服务选项卡

此选项卡仅在您编辑已创建的响应规则的设置时显示；在此选项卡上，您可以将规则关联到关联器。

要将目标位置链接到关联器，请单击**关联至服务"**按钮 → **关联至关联器**。这将打开一个窗口；在该窗口中，选择一个或多个关联器，然后点击**确定**。响应规则将关联到所选关联器，并根据其配置应用。

如有必要，您可以将响应规则与服务取消关联。要执行此操作，请选中关联器旁边的复选框，单击**删除**，然后确认与该服务取消关联。

数据收集和分析规则

数据挖掘规则用于通过分析保存在 OSMP 数据库中的事件来检测事故。

与流式关联和回溯扫描不同，数据挖掘规则会使用 SQL 查询对数据进行预处理（包括使用 SQL 执行额外计算、分组和聚合），并按计划定期运行。正确配置数据挖掘规则后，SIEM 可以帮助您检测高级威胁。

> 要管理此部分，您需要具备以下角色之一：主管理员、租户管理员、一级分析师或二级分析师。

在创建或编辑数据收集和分析规则时，您需要指定下表中列出的设置。

数据挖掘规则的设置

设置	描述
名称	必需设置。 资源的唯一名称。必须包含 1 到 128 个 Unicode 字符。
租户	必需设置。 拥有该资源的租户的名称。 如果您只能访问一个租户，则此字段会自动填写。如果您可以访问多个租户，则会填入可用租户列表中第一个租户的名称。您可以从此列表中选择任意租户。

SQL	必需设置。
	SQL 查询必须包含带 LIMIT 的聚合函数和/或带 LIMIT 的数据分组。
	必须使用 1 到 10,000 之间的 LIMIT 值。
	SQL 查询示例
	• 仅包含聚合函数的查询：
	`SELECT count(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
	• 仅包含数据分组的查询：
	`SELECT SourceAddress, DeviceCustomFloatingPoint1 FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• 包含聚合函数和数据分组的查询：
	`SELECT SourceAddress, sum(DeviceCustomFloatingPoint1) FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• 包含使用聚合函数的表达式的查询：
	`SELECT stddevPop(DeviceCustomFloatingPoint1) + avg(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`

查询间隔	必需设置。 执行 SQL 查询的间隔。可以分钟、小时和天为单位指定间隔。最短间隔为 1 分钟。 SQL 查询的默认超时时间等于您在此字段中指定的时间间隔。 如果 SQL 查询的执行时间超过超时时间，则会发生错误。在这种情况下，我们建议增加时间间隔。例如，如果时间间隔为 1 分钟，而查询执行需要 80 秒，我们建议将时间间隔设置为至少 90 秒。
标签	可选设置。 资源搜索的标签。

设置	描述
深度	可选设置。 用于定义在数据库中搜索事件的时间间隔下限的表达式。 要从列表中选择值或将深度指定为相对时间间隔，请将光标置于该字段中。例如，如果要查找从一小时前到现在的所有事件，请将相对时间间隔设置为 now-1h。
描述	可选设置。 数据收集和分析规则的描述。
映射	将 SQL 查询结果字段映射到 KUMA 事件的设置： **源字段**是 SQL 查询结果中要转换为 KUMA 事件的字段。 **事件字段**是 KUMA 事件字段。将鼠标光标置于此字段中，即可从列表中选择一个值。 **标签**是为以 `DeviceCustom*` 开头的事件字段指定的唯一自定义标签。 您可以添加或删除表格行。要添加新的表格行，请单击**添加映射**。要删除一行，请选中该行旁边的复选框，然后单击 按钮。 如果不想手动填写字段，可以单击**从 SQL 更新映射**按钮。字段映射表中将填充 SQL 查询字段的值，包括别名（如果有）。例如，如果 SQL 查询字段的值为 `SourceAddress`，并且该值与某个事件字段的名称相同，则会将该值插入字段映射表的**事件字段**列中。 再次单击**从 SQL 更新映射**按钮不会刷新表格，而是会将 SQL 查询中的字段再次添加到表格中。

您可以通过以下方式之一创建数据收集和分析规则：

- 在**仪表板 → 资源和服务 → 数据挖掘规则**部分中。

1. 在**仪表板 → 威胁搜索**部分中。

*要在**威胁搜索**部分中创建数据收集和分析规则：*

1. 创建或生成 SQL 查询，然后单击**创建数据挖掘规则**按钮。

   浏览器中将打开一个用于创建数据收集和分析规则的新标签页，其中已预填充**SQL 查询**和**深度**字段。如果 SQL 查询中未使用星号 (*)，字段映射表也会自动填充。

2. 填写必填字段。

   如有必要，您可以更改**SQL 查询周期**字段中的值。

3. 保存设置。

数据收集和分析规则将被保存，并可在**监控 → 资源和服务 → 数据收集和分析规则**部分中找到。要应用数据挖掘规则，您需要为其创建计划。

虚拟管理服务器

虚拟管理服务器（也称为*虚拟服务器*） 是 Kaspersky Next XDR Expert 的一个组件，用于管理客户端组织网络的反病毒保护。

虚拟管理服务器是从属管理服务器的一种特殊类型，与物理管理服务器相比，存在以下限制：

- 只能在主管理服务器上创建虚拟管理服务器。
- 虚拟管理服务器依赖于主管理服务器的数据库。虚拟管理服务器不支持数据备份和恢复任务，也不支持更新、扫描和下载任务。
- 虚拟管理服务器不支持创建从属管理服务器（包括虚拟服务器）。

此外，虚拟管理服务器具有以下限制：

- 在虚拟管理服务器属性窗口中，区域的数量是有限的。
- 要在虚拟管理服务器管理的客户端设备上远程安装卡巴斯基应用程序，您必须确保已在其中一台客户端设备上安装网络代理，以确保与虚拟管理服务器通信。在第一次连接到虚拟管理服务器时，该设备会被自动分配为分发点，并充当客户端设备与虚拟管理服务器的连接网关。
- 虚拟服务器只能通过分发点进行网络轮询。
- 要重启出现故障的虚拟服务器，Kaspersky Next XDR Expert 会重启主管理服务器和所有虚拟管理服务器。
- 在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

虚拟管理服务器的管理员在该特定虚拟服务器上具有所有权限。

构建 OSMP 实例层次结构

您可以将 Open Single Management Platform (OSMP) 实例排列成两级层次结构，父实例位于顶部。这样，您可以将父实例的设置分发给子实例，同时保持子实例的设置不变。

例如，用户 A 和用户 B 已部署 OSMP。每个用户都有一个独立的 OSMP 实例，并管理各自实例的 OSMP 控制台。

为了实现实例之间的数据交换，用户 A 和用户 B 必须将他们的实例排列成一个层次结构。为此，未来子实例的用户 A 向未来的父实例发送连接请求，未来父实例的用户 B 批准该请求。

如有必要，您可以断开子实例的连接。

构建层次结构后，实例中的实体按如下方式在层次结构中进行管理：

- **管理服务器**

  在实例层次结构中，您必须手动分配从属管理服务器。

- **租户**

  子实例的租户层次结构构建于父实例的租户层次结构之中。子实例的租户设置和集成租户设置可以从子实例和父实例进行编辑。只能从父实例编辑父实例的租户设置和集成租户设置。

  在父实例上，您可以查看子实例的租户层级结构；并在子实例上创建、编辑和删除租户；但无法删除子实例的根租户。

- **资产（设备）和资产类别**

  父实例和子实例的设置彼此独立。如果对父实例进行更改，则更改不会应用到子实例，反之亦然。

  父实例的资产不会显示在子实例中。在子实例中，可以查看父实例的资产类别、将这些类别关联到子实例资产，以及对子实例资产执行响应操作。例如，在父实例和子实例上都有 NNN 资产类别。如果您从子实例运行针对 NNN 类别的响应操作，则只有子实例的资产会受到该响应操作的影响。但是，您无法编辑父实例的类别，无法将这些类别分配给子实例的设备，也无法创建继承类别的子类别。

  在父实例上，会显示子实例的资产类别。如果您选择一个资产类别，则会显示子实例的资产。您可以对子实例类别的资产执行响应操作。如果与子实例没有连接，父实例的用户可以发起响应操作，该操作将在连接重新建立后对子实例设备执行。如果从父实例中删除某个类别，则该类别在子实例上会变为本地类别，并移动到子实例根租户的“已分类资产”类别中。如果资产类别已被 KUMA 资源使用，则无法删除该类别。子实例的资产类别不能被父实例的 KUMA 资源使用。

- **用户和用户角色**

  所有用户都是从父实例管理的。用户和用户角色会从父实例复制到子实例（管理员帐户除外）。在子实例中，现有用户将被删除，用户角色将保留，但不会复制到父实例。

  管理员帐户对于每个 OSMP 实例都是唯一的，不会在实例之间复制。因此，无法使用父实例的管理员帐户执行以下操作：

  - 在父实例的**威胁搜索**部分中管理子实例的事件
  - 从父实例查看子实例的资源信息
  - 从父实例查看和管理子实例的服务

- **文件**

  在子实例上执行响应操作后下载和获取的文件会显示在父实例上的文件表中，并且在**租户**字段中带有以下图标：(⛁)。当您在父实例上打开子实例文件的详细信息时，您会被重定向到子实例，以便对该文件执行进一步操作。

- KUMA **实体**

  - **事件**

    子实例事件存储在子实例上，父实例事件存储在父实例上。在父实例上，您可以搜索子实例的事件。

  - **关联规则和 IOA 规则**

    IOA 规则在构建层次结构后会转换为 KUMA 关联规则。

    层次结构中关联规则的使用模式如下：

    - **本地**。如果关联规则是在子实例上创建的，则该规则也会在子实例上进行管理。如果关联规则继承自父实例，则在子实例上，您只能向关联规则添加排除项，而不能编辑规则本身。

      关联规则及其排除项仅应用于连接到子实例管理服务器的设备。

    - **全局**。关联规则是在父实例上创建的。规则及其排除项将应用于您在配置规则设置时指定的子实例设备。

  - **关联规则排除项**

    添加到父实例关联规则中的临时排除项不会被继承。在子实例上，您可以向继承的关联规则添加临时排除项。过滤器会继承关联规则。

- **警报和事故**

  子实例的警报和事故会复制到父实例，并在子实例和父实例中同时显示。父实例的警报和事故仅在父实例中显示。在父实例上，您无法编辑、链接和合并子实例的警报或事故。

  当删除子实例上的警报或事故时，它们也会从父实例中删除。

  警报和事故设置及其保留期限不会被继承。如果保留期限到期，并且子实例上的警报或事故被删除，则相应的事件将被发送到父事故，然后父实例上的警报或事故也会被删除。

- **事故类型**、**工作流**和 SLA

  > 为避免数据不一致，事故类型、工作流和 SLA 会作为一个整体复制到子实例中。

  - SLA

    在子实例上，您无法创建 SLA。当尝试从父实例查看子实例的 SLA 时，您将被重定向到子实例。

  - **工作流**

    在子实例中，您可以创建工作流，也可以查看和应用从父实例继承的工作流。当尝试从父实例查看子实例的工作流时，您将被重定向到子实例。在父实例上，您可以删除父实例工作流；如果该工作流在父实例上没有关联实体，则不再显示该工作流，并在 90 天后将其彻底删除。您无法删除有关联实体的工作流。

  - **事故类型**

    事故类型从父实例继承，在父实例中默认处于禁用状态。如果继承了默认事故类型，则在子实例中，该事故类型不再是默认类型。

    在子实例上，您可以创建新的事故类型，以及查看和应用继承的事故类型。您无法编辑继承的事故类型。此外，您可以为继承的事故类型和在子实例上本地创建的事故类型设置默认属性。

- **聚合规则**

  手动创建的聚合规则从父实例继承。预定义的聚合规则不会被继承。

  在父实例上，您可以查看子实例的所有聚合规则。编辑规则的权限取决于您的 XDR 角色。

  在子实例上，继承的聚合规则会按照它们在父实例上的显示顺序显示在规则表的顶部。默认情况下，继承的规则处于禁用状态。您可以查看、启用和禁用继承的聚合规则。

  已启用的聚合规则将根据其优先级应用：规则在表中的位置越高，其优先级越高。

- **分段规则**

  手动创建的分段规则会从父实例继承。预定义的分段规则不会被继承。

  在父实例上，您可以查看子实例的所有分段规则。编辑规则的权限取决于您的 XDR 角色。

  在子实例上，继承的分段规则会按照它们在父实例上的显示顺序显示在规则表的顶部。默认情况下，继承的规则处于禁用状态。您可以查看、启用和禁用继承的分段规则。

  已启用的分段规则将根据其优先级应用：规则在表中的位置越高，其优先级越高。

- **防御规则**

  阻止规则会从父实例继承。

  在父实例上，您可以查看和编辑子实例的阻止规则，以及将子实例规则应用于子实例的资产。您无法将子实例的阻止规则应用于父实例的资产。

  在子实例上，您可以查看从父实例继承的防御规则。您无法编辑这些规则，也无法在从父实例继承的防御规则中添加或删除子实例资产。

- **YARA 和 IOC 规则**

  YARA 和 IOC 规则列表继承自父实例。

  在父实例上，您可以查看和编辑子实例规则，以及将子实例规则应用于子实例资产。您无法将子实例规则应用于父实例资产。

  在子实例上，您可以查看从父实例继承的 YARA 和 IOC 规则，但您无法编辑这些规则。要运行响应操作，您可以同时使用子实例的规则和从父实例继承的规则。

- **沙盒规则**

  Sandbox 规则继承自父实例。

  在父实例上，您可以查看和编辑子实例 Sandbox 规则，以及将子实例规则应用于子实例资产。

  在子实例上，您可以查看从父实例继承的 Sandbox 规则，但您无法编辑这些规则。

- **行动手册**

  从父实例，您可以创建子实例上的行动手册，并手动启动子实例的警报和事故的行动手册。

- **授权许可**

  授权许可管理和授权许可配置由各实例独立处理，不会在实例层次结构中继承。

  授权许可密钥需分别添加到每个实例。您可以将同一个授权许可密钥添加到所有实例中。

- **政策和任务**

  政策和任务继承自父实例。

- KSN/KPSN设置、凭据和通知模板不会被继承。

将子实例连接到父实例

未来子实例的用户发送连接请求，未来父实例的用户批准该请求。

两个用户都必须在各自的实例中拥有主管理员 XDR 角色。
如果您向在另一个层级结构中充当子实例的实例发送连接请求，该请求将被取消。
一个父实例最多可以有 150 个子实例。

从子实例发送连接请求

要发送连接请求：

1. 在未来子实例上，在主菜单中，转到**设置 → 租户。**
   屏幕上将显示租户列表。
2. 在工具栏上，单击“**请求连接**”按钮。
3. 在打开的右侧窗格中，执行以下操作：
   - 在**父实例的 API URL**字段中，指定父实例公共 API 的地址，例如：`https://api.xdr-hier-1.kuma.example.com`。
   - 在**父实例证书的指纹**字段中，指定父实例证书的哈希值。
     您可以单击**获取指纹**将父实例证书的哈希值插入到**父实例证书的指纹**字段中。如果父实例具有证书链，则 Kaspersky Next XDR Expert使用中间证书。我们不建议您使用叶证书，因为它的轮换频率比中间证书更高。指定的证书轮换后，您需要恢复实例层次结构。
   - 在**API 令牌**字段中，指定用于外部集成的公共 API 令牌。

     必须在父实例上预先生成 API 令牌。
     配置令牌参数时，必须使用 GET:/api/hierman/v1/* 和 POST:/api/hierman/v1/* API 方法来构建实例层次结构。
   - 如果必要，配置以下设置：
     - 在“**子实例的 API URL**”字段中，指定子实例公共 API 的地址，例如：*https://api.xdr-hier-2.kuma.example.com*。
     - 在**选择租户共享 SIEM 资源**部分，选中要在父实例中显示其 SIEM 资源的租户旁边的复选框。

4. 单击“**请求**”按钮。
   窗格关闭。

5. 在确认对话框中，单击“**请求**”。

确认对话框将关闭，屏幕上将显示“**您的连接请求正在等待批准**状态消息。

父实例上的用户批准或拒绝请求后，您将收到电子邮件通知，并且屏幕上显示的状态消息也会发生变化。

如果父实例上的用户批准了请求，则父实例的 ID 和父实例租户的名称将显示在子实例中。

批准来自父实例的连接请求

当子实例的用户发送连接请求后，您会收到相应的电子邮件通知。

要批准连接请求：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 在页面顶部，单击有关待处理连接请求的消息中显示的“**查看请求**”链接。
3. 在打开的**连接请求**窗格中，单击要批准的请求的**批准**按钮。
4. 在打开的“**批准连接请求**”窗格中，执行以下操作：
   - 在**根租户名称**字段中，为要连接的子实例租户指定一个新名称。
   - 在**根租户名称**部分，从父实例的租户层次结构中，选择一个租户作为子实例租户的父租户。
   - 点击**批准**按钮。
     窗格关闭。

子实例被添加到父实例的租户层次结构中。屏幕上会显示相应消息。

重启子实例上的活动服务

子实例与父实例建立连接后，重新启动子实例上的活动服务。之后，子实例的活动服务将显示在父实例上。

结果

现在您可以按如下方式管理子实例的租户树：

- 查看子实例租户树
- 在子实例上创建租户

- 编辑子实例上的租户
- 从子实例中删除除根租户之外的所有租户
- 断开子实例的连接

子实例的用户只能查看、编辑和删除子实例的租户。

在 OSMP 实例层次结构中分配从属管理服务器

构建 OSMP 实例层次结构后，必须通过手动分配从属管理服务器来手动建立“主/从属”关系。

要分配可通过 OSMP 控制台连接的从属管理服务器：

1. 在将来的主管理服务器上，确保端口 13000 可用于接收来自从属管理服务器的连接。
2. 在主菜单中，单击管理服务器名称以打开属性窗口，然后单击 **管理服务器** 选项卡。
3. 选择您要向其添加管理服务器的管理组名称旁边的复选框。
4. 在菜单行中，单击“**连接从属管理服务器**”。
   “添加从属管理服务器向导”启动。使用**下一步**按钮进行向导。
5. 指定将来的从属管理服务器的连接设置：

   - **连接主管理服务器到 DMZ 中的从属管理服务器**

     如果从属管理服务器位于隔离区 (DMZ)，选择该选项。

     如果选择此选项，主管理服务器将发起与从属管理服务器的连接。否则，从属管理服务器将发起与主管理服务器的连接。

   - **从属管理服务器地址(可选)**

     指定从属管理服务器的 IP 地址或域名。

     如果启用了“**连接主管理服务器到 DMZ 中的从属管理服务器**”选项，则需要此参数。

   - **从属管理服务器显示名称**

     从属管理服务器将显示在层级的名称。如果需要，您可以输入 IP 地址作为名称，也可以使用名称，例如“组 1 的从属服务器”。

   - **管理服务器 SSL 端口**

     指定主管理服务器上的 SSL 端口号。默认端口号是 13000。

     端口 13000 用于根管理服务器；此端口号无法更改。

   - **管理服务器 API 端口**

     Web Console 将用于通过 OpenAPI 接收来自从属管理服务器的连接的端口号。默认端口号是 13299。

     构建层级结构时，Web Console 会连接到未来的从属服务器，请求凭证，检索公共证书并执行初始设置。

     管理服务器层级结构构建完成后，将不再使用端口 13299。管理服务器将通过端口 13000 进行交互。

6. 指定未来从属服务器的证书。

   如果选择了 **从属管理服务器地址(可选)** 参数，则必须单击 **从从属管理服务器获取** 按钮以获取证书，或单击 **浏览证书文件** 并手动添加证书。

7. 指定未来主服务器的地址。

8. 如果通过代理服务器连接到未来主管理服务器，请选中 **使用代理服务器** 复选框并指定连接设置。

9. 指定对将来的从属管理服务器具有访问权限的用户的凭证。

10. 如果已启用并配置了 双重身份验证，请指定认证应用生成的 secret key。

11. 保存设置。

12. 切换到未来从属管理服务器并打开其属性窗口。

13. 在 **常规** 选项卡上，转到 **管理服务器层级** 部分并执行以下操作：

    - 选中 **该管理服务器是服务器层级中的从属** 复选框。
    - 在 **主管理服务器地址** 字段中，指定未来主管理服务器的网络名称。
    - 通过单击“浏览”，选择先前保存的包含未来主管理服务器证书的文件。
    - 如有必要，请选中 **连接主管理服务器到 DMZ 中的从属管理服务器** 复选框。
    - 如果通过代理服务器连接到未来主管理服务器，请选中 **使用代理服务器** 复选框并指定连接设置。

14. 保存设置。

    管理服务器的“主/从属”层次结构已构建。主管理服务器开始使用端口 13000 从从属管理服务器接收连接。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

将子实例与父实例断开连接

子实例与其父实例断开连接后，您无法将子实例连接到另一个层次结构。

断开与父实例的连接

要断开子实例的连接：

1. 在父实例的主菜单中，转到**设置 → 租户**。

   屏幕上将显示租户列表。

2. 选中要断开连接的子实例根租户旁边的复选框。

3. 在工具栏中，单击**断开连接**按钮，然后在显示的确认对话框中，单击**断开连接**。

子实例与父实例断开连接，屏幕上会显示相应的消息。子实例的用户将收到电子邮件通知。

如果在断开连接时子实例被关闭，则该实例将被强制断开连接。总之，要完成断开连接，请打开子实例，然后按照以下说明将子实例与父实例断开连接。

断开实例连接时，Kaspersky Next XDR Expert 会创建一个审计事件从 PCN 断开 SCN 连接。无论在断开连接时子实例是开启还是关闭，审计事件都是相同的。

出于诊断目的，如果子实例在断开连接时处于关闭状态，Kaspersky Next XDR Expert 会将错误写入hierman 组件的日志文件，例如“disconnect on secondary failed”错误。使用审计事件中 `trace_id` 字段的值来查找日志文件中的错误。

断开与子实例的连接

要断开子实例的连接：

1. 在子实例的主菜单中，转到**设置** → **租户**。
   屏幕上将显示租户列表。

2. 选中要断开连接的根租户旁边的复选框。

3. 在工具栏中，单击**断开连接**按钮，然后在显示的确认对话框中，单击**断开连接**。

子实例与父实例断开连接，屏幕上会显示相应的消息。父实例的用户将收到电子邮件通知。

断开连接结果

由于子实例断开连接，OSMP 层次结构被破坏。

在父实例中：

- 断开连接的实例的资源和设置将被删除。
- 已复制到父实例的子实例数据现在已从父实例中删除。

在子实例中：

- 父实例的信息将被删除，并且父实例不会显示在子实例租户层次结构中。
- 子实例租户层次结构的管理追溯到子实例。
- Identity and Access Manager 仍以只读模式可用。
  子实例的用户仍然可以登录到该实例，但不能执行任何其他操作（创建用户、分配权限、更改密码等）。
  在子实例连接到层次结构之前在该子实例上创建的用户将从子实例中删除。

- 如果从父实例继承的实体在父实例上没有链接对象，则这些实体会立即从子实例中删除。否则，该实体将不再显示在子实例上，但仍以只读模式保留 90 天。该期限结束后，实体将被删除。
- 从父实例继承的资产类别现在由子实例进行管理。
- 父实例管理的服务将被删除。

层次结构中关联规则的分布

OSMP 支持在合并成层次结构的 OSMP 实例之间集中管理和分发关联规则。

您可以在 OSMP 父实例上创建关联规则，并自动将其分发到子实例。在 OSMP 子实例上，继承的关联规则可供使用，但无法修改。若要进行更改，您需要创建继承规则的本地副本（复制该关联规则）。之后，更改仅会应用于本地副本。OSMP 父实例和子实例上的资源路径不同，因为文件夹名称不同；但是，资源本身及其包含的更改是同步的。

集中管理可确保在具有多个 OSMP 实例的分布式基础架构中统一使用关联规则，降低规则维护成本，并支持一致的威胁检测。

关键术语

*全局规则*是在OSMP父实例上创建并分发到子实例的关联规则。

*本地规则*是在子OSMP实例上创建的规则。

*继承的关联器*是指OSMP子实例上的关联器服务，它使用在父实例上创建的关联器配置。

*继承的资源*是指从层次结构中的OSMP父实例获取的资源。

在您开始之前

要使规则继承机制正常工作，必须满足以下条件：

1. 已配置OSMP实例层次结构。

   OSMP实例组织成一个层次结构，包含一个父实例和一个或多个子实例。

2. OSMP子实例连接到OSMP父实例。

此功能可实现的操作

OSMP父实例可以执行以下操作：

- 创建全局关联规则，并将这些规则分发到OSMP子实例。
- 查看在OSMP子实例上创建的资源和服务。

以下操作位于**活动服务**部分：

- 添加服务
- 更新服务设置
- 重启服务
- 删除子实例的服务
- 查看服务事件
- 查看活动列表
- 查看上下文表
- 查看部分
- 下载日志和转储文件
- 复制服务ID
- 复制集群ID
- 重置证书

OSMP子实例可以执行以下操作：

- 使用继承的规则，但无法编辑它们
- 创建全局规则的本地副本

以下针对继承服务的操作位于**活动服务**部分：

- 查看服务日志
- 更新服务设置
- 查看服务配置

限制

对于OSMP子实例上继承的关联规则，规则无法编辑或删除，无法更改链接到的服务，也无法修改关联器设置。

要编辑继承的关联规则，需要在OSMP子实例上创建一个复制规则。

副本规则将成为可编辑的本地资源。

规则生命周期

更新父规则

全局规则修改后，变更不会自动分发。如需应用变更，您需要重启关联器服务或

更新服务设置。

之后，变更才会应用到OSM子实例。

删除父实例上的规则

如果在OSMP父实例上删除了全局规则，则OSMP子实例上继承的规则不会自动删除。继承的规则会成为本地资源，OSMP子实例将获得对该资源的完全权限。

复制规则

如果在OSMP子实例上复制全局规则，则会创建该规则的本地副本，OSMP子实例将获得对该副本的完全权限（读取、写入、删除）。

导出和导入

可以将继承的规则导出到另一个OSMP实例，或从另一个OSMP实例导入。

导入后，该规则将成为可编辑的本地资源。

连接暂时中断

如果OSMP实例之间的连接暂时中断，则会立即传输最大64MB的数据包，更大的数据包将被拒绝并传回错误。

连接恢复后，子实例将收到丢失的变更。

层次结构拆分

如果子实例从层次结构中分离出来，其继承的服务和规则将变为本地规则，并可进行编辑和删除。

用例

您可以执行以下操作：

- 将全局关联器配置与全局关联规则一起分发。
- 分发全局关联规则以供本地使用
- 在子实例上复制继承的关联规则
- 查看在OSMP子实例上创建的规则

分发全局关联器配置以及全局关联规则

将全局规则作为继承关联器的一部分分发到OSMP子实例：

1. 在OSMP父实例上：

   a. 创建全局关联规则：

      1. 转到**资源和服务→关联规则**部分。
      2. 创建关联规则。
      3. 在关联规则的设置中，启用**在子节点上启用继承**切换开关。
      4. 在下拉列表中，指定要将规则分发到的一个或多个OSMP子实例的租户。
      5. 保存关联规则。

   创建的关联规则必须关联到关联器服务。

   b. 创建一个将在OSMP子实例上继承的关联器服务，并关联全局关联规则：

      1. 转到**资源和服务→关联器**部分。
      2. 创建一个关联器，并在安装程序向导的**常规**步骤中，开启**在子节点上启用继承**切换开关。
      3. 在下拉列表中，指定要将关联器配置分发到的一个或多个OSMP子实例的租户。
      4. 在安装程序的**关联**步骤中，关联全局关联规则。
      5. 保存关联器服务的设置。

   保存设置后，关联器服务和全局关联规则的配置将保存在OSMP父实例上，并传播到OSMP子实例。关联器服务的进一步配置和安装在OSMP子实例上执行。

2. 在OSMP子实例上：

   a. 在卡巴斯基安全管理中心子实例上，转到**资源和服务→关联器**部分，并在服务表中打开继承的关联器服务。

      1. 在关联器的安装程序的**路由**步骤中，指定目标位置：

      - 用于保存事件和警报的存储。
      - OSMP父实例上的关联器，用于进一步处理事件。

      1. 在**设置验证**步骤中，单击**创建并保存服务**。
      2. 复制**关联器安装推荐命令**下的安装命令，并在OSMP子实例的主机上安装关联器服务。

因此，在OSMP子实例上：

- 会创建关联规则的副本。
- 会创建关联的依赖资源。
- 会创建继承的关联器配置。关联器内部使用的资源也会被继承，即使它们没有单独继承，例如响应规则。
- 关联规则和关联器服务的配置以读取模式提供，并可指定目标点。
- 该服务显示在OSMP父实例的**活动服务**部分，并标明它是继承的服务。
- 在OSMP父实例上所做的更改会自动向下继承到层级结构中。

分发全局关联规则以供本地使用

将全局规则分发给OSMP子实例并将它们关联到本地关联器：

1. 在OSMP父实例上：

   a. 转到**资源和服务→关联规则**部分。

   b. 创建关联规则。

   c. 在关联规则的设置中，启用**在子节点上启用继承**切换开关。

   d. 在下拉列表中，指定要将规则分发到的一个或多个OSMP子实例的租户。

   e. 填写其余必填字段。

   f. 保存规则。
   创建的全局关联规则将传播到OSMP子实例。继承的关联规则必须关联到关联器服务。

2. 在OSMP子实例上：

   a. 转到**资源和服务→关联器**部分。

   b. 创建关联器服务或打开现有服务的设置。

c. 在关联器的安装程序向导中，在**关联**步骤中，将全局关联规则关联到本地关联器服务。

d. 管理其余必填设置：

e. 在**设置验证**步骤中，执行以下操作之一：

- 如果要创建关联器，请单击**保存并创建服务**，然后使用生成的命令在OSMP子实例的主机上安装该服务。
- 如果要更新活动关联器的设置，请单击**保存并更新服务配置**。

因此，在OSMP子实例上：

- 会创建关联规则的副本。
- 关联器服务将显示在OSMP父实例的**活动服务**部分中，并且可以查看。
- 对OSMP父实例上的关联规则所做的更改会自动向下继承。

继承的关联规则为只读。

如果您需要编辑规则以供本地使用，请复制该关联规则，并在本地使用该副本，使其独立于OSMP父实例。

复制继承的关联规则以供本地使用

先决条件：

- 已配置OSMP实例层次结构。
- OSMP子实例连接到父实例。
- 已在OSMP父实例上创建关联规则。
- 全局关联规则的继承配置在OSMP子实例上。

要复制继承的关联规则以供本地使用：

1. 在OSMP子实例上，转到**资源和服务→关联规则**部分。
2. 在关联规则表中，找到继承的规则，并选中它旁边的复选框。
3. 在工具栏或菜单中（⋮），点击**复制**。
4. 输入新关联规则名称。
5. 保存关联规则的副本。
6. 打开已创建的本地关联规则副本。

7. 进行必要的更改。
8. 保存关联规则。

因此，OSMP子实例上的关联规则本地副本将独立于OSMP父实例，您可以编辑、删除、导出和更改本地副本的依赖资源。

限制：

复制后，对父规则所做的更改不会应用到本地副本，也不会同步。

查看在 OSMP 子实例中创建的资源和服务

先决条件：

- 已配置OSMP实例层次结构。
- OSMP子实例连接到OSMP父实例。
- 在OSMP子实例上创建资源或服务。

查看在OSMP子实例上创建的资源：

1. 在OSMP父实例上，转到**资源和服务→关联规则**部分。
2. 打开资源列表。
3. 查看可用的基本信息：
   - ID。
   - Name。
   - 租户 ID
   - 租户名称。
   - 远程租户（OSMP子实例的租户）指示器
   - 规则类型
   - 上次更新: {date}
   - 标签
   - MITRE 技术
   - 包名称（如果资源是通过卡巴斯基更新服务器获取的）
   - 描述

- 资源路径
  父实例和子实例上的文件夹名称不同，因此路径也不同。但是，更改会在适用情况下同步。

要查看完整信息，请打开关联规则的卡片。

要查看在OSMP子实例上创建的关联器服务：

1. 在OSMP父实例中，前往**资源和服务→活动服务**部分。
2. 在服务表中，打开一个服务进行查看。

因此，在OSMP父实例上：

- 将显示子实例的资源和服务。
- 资源和服务为只读。
- 可以使用搜索和筛选功能。
- 打开资源卡片时，关联规则的完整信息将直接从OSMP子实例加载。

在OSMP父实例上，无法对OSMP子实例的资源执行以下操作：

- 复制
- 删除
- 查看依赖项列表
- 分配标签
- 关联到关联器
- 分配和查看排除项列表
- 查看历史版本
- 使用父实例的关联器中的资源

在层次结构中分发资源时的文件夹行为

资源会与分发时的文件夹路径关联。如果您未手动重命名或移动文件夹，则路由不会改变。文件夹结构的更改不会在 OSMP 实例之间同步。

在层次结构中分发资源时，适用以下规则：

1. 仅传输包含至少一个已分发资源的文件夹。
2. 实例之间的文件夹按其完整路径进行映射。
3. 不会传输文件夹 ID：在目标实例上，将使用新的 ID 创建文件夹。

4. 导入期间，现有文件夹结构不会被替换，而是会与导入的文件夹结构合并。
5. 文件夹操作（创建、重命名和移动）不会直接同步。只有在分发位于相应文件夹中的资源后，更改才会变为可见。

创建文件夹

在子实例上创建的新文件夹只有在该文件夹中至少创建了一个已分发资源后，才会在父 OSMP 实例上可见。

重命名文件夹

重命名文件夹不会自动更新其他 OSMP 实例上的文件夹结构。

重命名后，预期行为如下：

- 在文件夹名称更改之前分发的资源仍然与旧路径关联。
- 重命名后分发的资源使用新路径。

示例

初始状态：

- 父实例：文件夹 A 包含资源 R1。
- 子实例会继承 R1 资源。

更改：

- 在子实例上，文件夹 A 被重命名为 B。
- 在文件夹 B 中创建新的资源 R2，并将其分发到父实例。

结果：

- 在父实例上，R1 位于文件夹 A；R2 位于文件夹 B。
- 在子实例上：R1 和 R2 位于文件夹 B。

每个资源都与资源分发时存在的文件夹路径关联。因此，为了保持稳定的路由，建议不要手动重命名或移动文件夹。

将 OSMP 实例组合成层次结构

本节介绍如何将 OSMP 实例组合成层次结构。

1 先决条件

至少需要两个 OSMP 实例：一个父实例和一个子实例。

本节使用以下域名作为示例：

- 对于父实例：
  - Web 界面：`console.edrparent.organization.acme`
  - API：`api.edrparent.organization.acme`
- 对于子实例：
  - Web 界面：`console.edrchild1.organization.acme`
  - API：`api.edrchild1.organization.acme`
- 对于所有实例：
  - 必须与每个实例 IP 地址的 443 端口建立双向通信。
  - 父实例必须能够访问子实例的 API 域名，并且所有子实例都必须能够访问父实例的 API 域名。

2 准备父实例

1. 在将作为父实例的实例的主菜单中，转到**设置** → **API 令牌**部分，然后单击**添加令牌**按钮。
2. 在**名称**字段中，输入 API 令牌的名称（例如，`edrparenthierarchy`）。
   完成与子节点的连接后，您可以撤销此令牌。
3. 在**到期日**字段中，指定令牌到期日。设置此日期时，请考虑完成层次结构构建所需的最短时间（至少一天）。
4. 在"**API 方法**"部分，选中以下方法对应的复选框：
   - **GET:/api/hierman/v1/***
   - **POST:/api/hierman/v1/***

5. 单击“**生成**”，然后单击“**复制并关闭**”。

   API 令牌随即被创建并复制到剪贴板。请妥善保存，因为之后将无法复制。

6. 获取证书指纹，以验证与实例的连接。为此，请在浏览器中打开父实例的 API 域名（`api.edrparent.organization.acme`），并查看证书详细信息。

   确保指纹是从可信来源获取的。检查其 IP 地址，确保域名未被伪造。

❸ 每个子实例的操作步骤

1. 转到未来子实例的 Web 界面（在本例中为 `console.edrchild1.organization.acme`）。
2. 在主菜单中，转到“**设置**” → “**租户**”。
3. 在工具栏上，单击“**请求连接**”按钮。
4. 在打开的右侧窗格中，执行以下操作：
   - 在“**父实例的 API URL**”字段中，指定父实例的 API 地址（在本例中为 `api.edrparent.organization.acme`）。
   - 在**父实例证书的指纹**字段中，指定父实例证书的哈希值。
   - 在“**API 令牌**”字段中，指定之前在父实例中创建的 API 令牌。
5. 单击“**请求**”按钮。

   如果所有字段均填写正确，则会显示“*您的请求已发送*”消息。
6. 导航到**父**实例（本例中为 `console.edrparent.organization.acme`）。
7. 在主菜单中，转到“**设置**” → “**租户**”。

   会显示“*正在等待连接请求*”消息。如果未显示该消息，请刷新页面。
8. 单击“**查看请求**。

   这将打开一个显示子实例详细信息的窗口。
9. 仔细检查已填写的字段和地址。尤其要注意“**证书指纹**”字段：必须使用可信来源提供的子实例证书验证其值。检查 IP 地址，确保域名（本例中为 `api.edrchild1.organization.acme`）未遭到欺骗。
10. 如果所有字段均已正确填写，请单击“**批准**”按钮。
11. 在打开的“**批准连接请求**”窗格中，执行以下操作：
    - 在**根租户名称**字段中，为要连接的子实例租户指定一个新名称。子实例的根租户将以此名称注册到父实例。
    - 在**根租户名称**部分，从父实例的租户层次结构中，选择一个租户作为子实例租户的父租户。

- 点击**批准**按钮。

  窗格关闭。子实例被添加到父实例的租户层次结构中。屏幕上会显示*根租户已连接到实例*消息。

12. 刷新页面后，您将在租户树中看到一个包含子实例层次结构的新节点。

证书轮换后修复实例层次结构

当您构建OSMP实例的层次结构时，请在**父实例证书的指纹**字段中指定父实例的证书。指定的证书轮换后，层次结构会断开。例如，以下原因可能导致这种情况：

- 您将Kaspersky Next XDR Expert从早期版本升级，或在同一主版本内进行更新。
- 证书在到期后会自动替换。
- 您手动替换了证书。

当层次结构断开时，OSMP会在hierman组件的日志文件中添加以下错误："证书链中没有证书与预期指纹匹配"。

要在证书轮换后修复实例结构，请执行以下操作：

1. 在OSMP父实例的管理员主机上，运行以下命令：

```
./kdt invoke hierman --action hiermanRepairTrust
```

2. 在层次结构中包含的OSMP子实例的管理员主机上运行相同的命令。

层次结构随即修复。

与其他解决方案集成

通过与其他解决方案集成，可丰富 Kaspersky Next XDR Expert 的功能。

Kaspersky Next XDR Expert 支持与以下卡巴斯基解决方案和第三方解决方案集成：

- Kaspersky Automated Security Awareness Platform
- 卡巴斯基威胁情报门户
- Kaspersky Anti Targeted Attack Platform/Kaspersky Endpoint Detection and Response
- 活动目录
- UserGate
- Ideco NGFW
- Ideco UTM
- Redmine
- Check Point NGFW
- Sophos Firewall
- Continent 4
- SKDPU NT
- FortiGate
- Palo Alto NGFW

Kaspersky Next XDR Expert 还支持 100 多个事件源。有关受支持事件源的完整列表，请参阅“受支持事件源”部分。

可以为任何级别的租户指定集成设置。父租户集成设置将被复制到子租户。您可以编辑所复制的子集成设置，因为子租户设置和父租户设置不相关，子租户设置的更改不会影响父租户的设置。

对于共享租户，您无需配置集成设置。

如需禁用集成，可以在“**设置**” → “**租户**”中手动执行此操作。

若所指定集成的租户被删除，则其与卡巴斯基解决方案的集成也会被自动删除。数据删除延迟最长可达 24 小时。不支持恢复集成设置。

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform（以下也称为 KASAP）是一个在线学习平台，可让用户学习日常工作中的信息安全规则及相关威胁知识，并通过真实案例进行实践。

完成集成配置后，您可以在 Kaspersky Next XDR Expert 中执行以下任务：

- 为与警报和事故相关的用户分配学习课程。
- 更改用户的学习分组。
- 查看用户参加的课程及其获得的证书信息。

配置 KASAP 与 KUMA 的集成后，KASAP 即视为已与 Kaspersky Next XDR Expert 集成。

> 在配置 KASAP 与 KUMA 的集成之前，您需要在 KASAP 中创建授权令牌并获取用于 API 请求的 URL。

创建令牌

要授权从 KUMA 到 KASAP 的 API 请求，必须使用在 KASAP 中创建的令牌对请求进行签名。

> 只有公司管理员才能创建令牌。

要创建令牌：

1. 登录 KASAP Web 界面。
2. 在“**仪表板**”部分，选择“**导入并同步**”部分，然后打开“**OpenAPI**”选项卡。
3. 单击“**新建令牌**”按钮。
4. 在打开的窗口中，选择集成时可用的令牌权限：
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
5. 单击“**生成令牌**”按钮。
   生成的令牌将显示在屏幕上。

6. 复制令牌并以任何方便的方式保存。此令牌是配置 KASAP 和 KUMA 之间集成所必需的。

> 令牌无法以明文形式存储在 KASAP 系统中。关闭“**创建令牌**”窗口后，将无法查看令牌。如果您关闭窗口而不复制令牌，则需要单击“**重新签发令牌**”按钮，系统才会生成新令牌。

签发的令牌有效期为 12 个月。

获取 API 请求的 URL

该 URL 用于通过 OpenAPI 与 KASAP 交互。您必须在配置 KASAP 和 KUMA 之间的集成时指定此 URL。

要获取 KASAP 中用于 API 请求的 URL：

1. 登录 KASAP Web 界面。
2. 在“**仪表板**”部分，选择“**导入并同步**”部分，然后打开“**OpenAPI**”选项卡。
3. 在“**OpenAPI URL**”字段中，复制 URL，然后以任何方便的方式进行保存。

配置与 Kaspersky Threat Intelligence Portal 的集成

您必须配置与 Kaspersky 威胁情报门户（以下也称为 Kaspersky TIP）的集成，才能获取有关可观察对象的信誉信息。

> 在配置设置之前，您必须在 Kaspersky TIP 或 Kaspersky OpenTIP 上为 API 请求创建授权令牌。

要配置 Kaspersky Next XDR Expert 与 Kaspersky TIP 之间的集成：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   屏幕上将显示租户列表。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 转到“**设置**”选项卡，然后选择“**Kaspersky TIP**”部分。

> 要编辑 **Kaspersky TIP** 部分，您必须被分配以下 XDR 角色之一：主管理员、租户管理员或 SOC 管理员。

4. 如果您在步骤 2 中选择了“根租户”，则可以打开“**代理**”切换按钮，以使用代理服务器与 Kaspersky TIP 进行交互。
   代理服务器在根管理服务器属性中进行配置。
5. 在“**缓存 TTL**”字段中，指定缓存存储期限和单位（天或小时）。
   默认设置为 7 天。如果您未指定任何值，则缓存存储期限不受限制。

您可以为所有连接设置缓存存储期限。

6. 打开以下服务之一的“**集成**”切换按钮：

   - **Kaspersky TIP (常规访问)**

     添加授权令牌后，则可以从 Kaspersky TIP 获取有关警报或事故详情中“**可观察对象**”选项卡上列出的以下可观察对象类型的信息：域、URL、IP、MD5、SHA256。该信息会在“**增强**”列中更新。请求数据时会消耗配额。

   - **Kaspersky TIP (高级访问)**

     添加授权令牌后，即可执行以下操作：

     - 从 Kaspersky TIP 获取有关警报或事故详情中“**可观察对象**”选项卡上列出的以下可观察对象类型的信息：域、URL、IP、MD5、SHA256。该信息会在“**增强**”列中更新。请求数据时会消耗配额。
     - 从 Kaspersky TIP 获取有关警报或事故详情中“**可观察对象**”选项卡上列出的以下可观察对象类型的信息：域、URL、IP、MD5、SHA256。该信息会在“**状态更新**”列中更新。请求数据时不会消耗配额。

7. 单击“**添加令牌**”按钮。

8. 在打开的窗口中，输入授权令牌，然后单击“**添加**”按钮。

   有关为 API 请求生成授权令牌的详细信息，请参阅 Kaspersky TIP 或 Kaspersky OpenTIP 帮助。

   添加令牌后，通过单击“**替换**”按钮，然后在打开的窗口中输入新令牌，即可更改令牌。如果令牌过期，则可能需要执行此操作。

9. 单击“**保存**”按钮。

与 KATA/KEDR 集成

如果从KEDR 7.1迁移后，您拥有的端点代理程序不支持与Kaspersky Next XDR Expert 2.0或2.1集成，则可能需要此说明。

Kaspersky Endpoint Detection and Response（以下也称为 KEDR）是 Kaspersky Anti Targeted Attack Platform（以下也称为 KATA）的一个功能块，用于保护企业局域网中的资产。

您可以配置 Kaspersky Next XDR Expert 与 KATA/KEDR 之间的集成，以管理连接到 Kaspersky Endpoint Detection and Response 服务器的资产上的威胁响应操作。执行操作的命令由 Kaspersky Endpoint Detection and Response 服务器接收，然后将这些命令转发到安装在资产上的 Kaspersky Endpoint Agent。

要配置 Kaspersky Next XDR Expert 与 KATA/KEDR 之间的集成：

1. 在主菜单中，转到“**设置**” → “**租户**”。

   屏幕上将显示租户列表。

2. 单击所需租户的名称。

   该租户的属性窗口将打开。

3. 转到“**设置**”选项卡，然后选择“**KATA/KEDR**”部分。

> 如果您被分配了以下 **XDR 角色**之一，则可以编辑“KATA/KEDR”部分：主管理员、租户管理员或 SOC 管理员。

4. 打开“**KATA 集成**”切换按钮。

5. 单击“**添加连接**”按钮，然后在打开的窗口中执行以下操作：

   a. 在“**IP 地址或主机名**”字段中，输入以下内容之一：

   - hostname
   - IPv4
   - IPv6

   b. 在“**端口**”字段中，设置一个端口。

   c. 单击“**保存**”按钮。

   窗口将被关闭。

   如果连接添加失败，将显示错误消息。

   如果连接添加成功，屏幕上会显示相应的消息。将生成 XDR ID、证书和私玥，并显示在相应的字段中。如有需要，您可以单击“**生成**”按钮以生成新的证书和私钥。

   为确保连接建立成功，请单击“**检查连接**”按钮。结果将显示在“**连接状态**”参数中。

6. 单击“**保存**”按钮以保存设置。

   添加连接后，您可以单击相应图标进行编辑或删除。也可以通过执行步骤 1 至 6 来添加其他连接。

如果要接收有关 Kaspersky Endpoint Detection and Response 警报的信息，则需要配置 KUMA 组件与 KATA/KEDR 之间的集成。

如果尚未在所有受管理主机上将端点安全应用程序升级到新版本，则在升级完成之前，威胁响应操作仍通过与 Kaspersky Anti Targeted Attack Platform (KATA) 的集成进行管理。在这种情况下，事故响应平台会向 KATA 发送请求，然后 KATA 会向端点安全应用程序发送请求。

配置 Kaspersky Next XDR Expert 与脚本启动服务的集成

您可以借助外部系统，通过在远程客户端设备上启动第三方脚本来响应警报和事故。要启用此选项，您必须配置环境以及 Kaspersky Next XDR Expert 与脚本启动服务之间的集成。

要配置启动第三方自定义脚本的环境，您必须：

- 设置启动第三方自定义脚本的设备。
- 配置 Kaspersky Next XDR Expert 与脚本启动服务之间的集成。
- 创建将用于启动脚本的行动手册。

客户提供对第三方自定义脚本的访问权限并更新脚本。

要配置 Kaspersky Next XDR Expert 与脚本启动服务的集成：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
   屏幕上将显示租户列表。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 转到“**设置**”选项卡，然后在“**自定义集成**”部分中：
   - 打开“**自定义集成**”切换按钮。
   - 在“**远程主机验证**”部分中，打开“**连接前验证主机**”切换按钮，然后填写“**公钥**”字段，以在 Kaspersky Next XDR Expert 中启用客户端设备验证。
   - 在“**远程主机连接**”部分，执行以下操作：
     - 填写“IP **地址或主机名**”和“**端口**”字段。
     - 选择将用于与远程设备建立安全连接的 SSH **身份验证方法**：
       - **用户名和密码**。如果选择此身份验证方法，则下一步必须输入用户名和密码。
       - **SSH 密钥**。如果选择此身份验证方法，则下一步必须输入用户名和 SSH 密钥的私钥部分。
     - 单击“**添加数据**”按钮。
4. 在打开的窗口中，输入所需数据，然后单击“**保存**”按钮。
   如果要编辑已保存的数据，请单击“**替换**”按钮，在打开的窗口中输入新数据，然后保存编辑的内容。
   为确保连接建立成功，请单击“**检查连接**”按钮。结果将显示在“**连接状态**”参数中。
5. 单击“**保存**”按钮以保存设置。

Kaspersky Next XDR Expert 与脚本启动服务之间的集成已配置。您可以通过启动行动手册在远程设备上执行响应操作。

威胁检测

Kaspersky Next XDR Expert 使用警报和事故作为由分析师处理的工作项。

如果满足以下条件，则“**警报**”和“**事故**”部分将显示在主菜单中：

- 拥有 Kaspersky Next XDR Expert 的授权许可密钥。
- 已连接到 OSMP 控制台中的根管理服务器。
- 您拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、1 级分析师、2 级分析师、SOC 经理、审批人、审计员。

处理警报

本部分包含有关警报、其属性、典型生命周期以及与事故的联系的一般信息。提供的说明将帮助您分析警报表、根据生命周期的当前状态更改警报属性，以及通过关联或取消关联将警报合并为事故。

如满足以下条件，“**警报**”部分将显示在主菜单中：

- 拥有 Kaspersky Next XDR Expert 的授权许可密钥。
- 已连接到 OSMP 控制台中的根管理服务器。
- 您拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、1 级分析师、2 级分析师、SOC 经理、审批人、审计员。

关于警报

*警报*是组织 IT 基础架构中被 Kaspersky Next XDR Expert 标记为异常或可疑的事件，可能会对组织 IT 基础架构的安全构成威胁。

当 EPP 应用程序（例如 Kaspersky Endpoint Security for Windows）检测到基础架构中符合检测规则所定义条件的特定活动时，Kaspersky Next XDR Expert 会生成警报。

警报在 KUMA 关联事件发生后 30 秒内创建。如果您之前配置了通知模板，则会收到相应的电子邮件通知。

您也可以从一组事件中手动创建警报。

检测后，Kaspersky Next XDR Expert 会将警报作为待分析人员处理的工作项添加到警报表中。您无法删除警报。您只能关闭这些警报。

事故只能分配给具有警报和事故读取及修改权限的分析人员。

您可以使用以下警报属性将警报作为工作项进行管理：

- **警报状态。**

  可能值：**新建**、**进行中**、**已关闭**或**事故中**。

  警报状态显示了警报在其生命周期中的当前状态。您可以根据需要更改状态，但以下情况除外：

  - 您不能将已关闭的警报更改为“**进行中**”状态。已关闭的警报只能先返回至“*新建*”状态，然后才能更改为“**进行中**”状态。
  - 您不能手动设置“**事故中**”状态。当警报关联到事故时，它们会获得此状态。
  - 您只能将关联的警报设置为“**已关闭**”状态。要设置“**新建**”或“**进行中**”状态，您必须首先取消警报与事故的关联。

- **警报严重级别。**

  可能值：“**低**”、“**中**”、“**高**”或“**严重**”。

  警报严重级别基于卡巴斯基的经验显示了此警报可能对计算机安全或企业 LAN 安全产生的影响。严重级别是自动定义的，不能手动更改。

- **警报负责人**

  该角色为警报所有者，即负责警报调查和处理的分析师。您可以随时更改警报负责人。您无法更改已关闭警报的负责人。

您可以合并警报并将其关联到更大的工作项（称为*事故*）。您可以手动将警报关联到事故，也可以启用规则来创建事故并自动关联警报。通过使用事故，分析师可以将多个警报作为单个问题进行调查。将当前未关联的警报关联到事故时，警报将失去其当前状态并获得“**事故中**”状态。您可以将当前关联的警报关联到另一个事故。在这种情况下，将保留警报的“**事故中**”状态。您最多可以将 200 个警报关联到一个事故。

每个警报都具有*警报详情*，其中提供了与该警报相关的所有信息。您可以使用这些信息来调查警报、追踪警报之前的事件、查看检测工件、受影响的资产或将警报关联到事故。

警报数据模型

警报的结构由包含值的字段表示（见下表）。有些字段是对象或对象数组，具有自己的一组字段（例如，`Assignee`和`Assets`字段）。

警报

字段	值类型	是否必需	Description
`InternalID`	字符串	是	内部警报 ID，采用 UUID 格式。字段值可能与 `SourceID` 值匹配。
`ID`	整数	是	短格式的内部警报 ID。
`TenantID`	字符串	是	与警报关联的租户的 ID，采用 UUID 格式。
`CreatedAt`	字符串	是	警报生成的日期和时间，采用 RFC 3339 格式。
`UpdatedAt`	字符串	是	上次警报更改的日期和时间，采用 RFC 3339 格式。
`StatusChangedAt`	字符串	否	上次警报状态更改的日期和时间，采用 RFC 3339 格式。

Severity	字符串	是	警报的严重级别。 可能值： • critical • high • medium • low
IntegrationID	字符串	是	OSMP 中集成的卡巴斯基应用程序管理插件的 ID。
IntegrationCompatibilityVersion	字符串	是	OSMP 中集成的卡巴斯基应用程序管理插件的版本。
SourceID	字符串	否	集成组件中的唯一警报标识符。
SourceCreatedAt	字符串	否	集成组件中警报生成的日期和时间，采用 RFC 3339 格式。
FirstEventTime	字符串	是	与警报相关的第一个遥测事件的日期和时间，采用 RFC 3339 格式。
LastEventTime	字符串	是	与警报相关的最后一个遥测事件的日期和时间，采用 RFC 3339 格式。
DetectSource	字符串	否	检测并生成警报的组件。
DetectionTechnologies	字符串数组	否	触发的检测技术。
State	字符串	是	警报状态。 可能值： • new • inProgress • inIncident • closed
StatusResolution	字符串	否	警报状态解析。 可能值： • truePositive • falsePositive • lowPriority • merged
IncidentID	字符串	否	与警报关联的事故的内部 ID。
IncidentLinkType	字符串	否	将警报添加到事故的方式。 可能值： • manual • auto
Assignee	Assignee 对象	否	被分配负责处理该警报的操作员。
MITRETactics	MITRETactic 对象数组	否	与警报中所有触发的 IOA 规则相关的 MITRE 战术。
MITRETechniques	MITRETechnique 对象数组	否	与警报中所有触发的 IOA 规则相关的 MITRE 技术。
Observables	Observable 对象数组	否	与警报相关的可观察对象。
Assets	Asset 对象数组	否	受警报影响的资产。
Rules	Rule 对象数组	否	触发的关联规则，警报是基于此生成的。
OriginalEvents	对象数组	否	事件，警报以此为基础生成。
ExternalRef	字符串	是	指向外部系统中实体的链接（例如，指向 Jira 工单的链接）。
Extra	对象	否	与警报相关的数据，采用 JSON 格式。这些数据是在事件转换为警报时从受管理的卡巴斯基应用程序中获取的。该字段未在接口中使用。
AdditionalData	对象	否	有关警报的附加信息，采用 JSON 格式。此信息可由用户或行动手册填写。
IsCII	布尔	是	指示受影响资产（设备或账户）是否为严重信息基础设施对象的标志。

`Name`	字符串	是	警报名称。
`Attachments`	`UnkeyedAttachment` 对象数组	否	与事故相关的附件。

负责人

字段	值类型	是否必需	Description
`ID`	字符串	是	被分配负责处理该警报的操作员的用户账户 ID。
`Name`	字符串	是	被分配负责处理该警报的操作员的姓名。

MITRE 战术

字段	值类型	是否必需	Description
`ID`	字符串	是	与警报中所有触发的 IOA 规则相关的 MITRE 战术的 ID。
`Name`	字符串	是	与警报中所有触发的 IOA 规则相关的 MITRE 战术的名称。

MITRE 技术

字段	值类型	是否必需	Description
`ID`	字符串	是	与警报中所有触发的 IOA 规则相关的 MITRE 技术的 ID。
`Name`	字符串	是	与警报中所有触发的 IOA 规则相关的 MITRE 技术的名称。

可观察对象

字段	值类型	是否必需	Description
`Type`	字符串	是	观察点类型 可能值： • `ip` • `md5` • `sha256` • `url` • `domain` • `UserName` • `hostName`
`Value`	字符串	是	可观察对象的值。
`Details`	字符串	否	有关可观察对象的附加信息。

规则

字段	值类型	是否必需	Description
ID	字符串	是	触发规则的 ID。
Name	字符串	否	触发规则的名称。
Severity	字符串	否	触发规则的严重级别。 可能值： • critical • high • medium • low
Confidence	字符串	否	触发规则的置信度。 可能值： • high • medium • low
Custom	布尔	否	指示警报基于自定义规则的标志。

资产

字段	值类型	是否必需	Description
Type	字符串	是	受影响资产（设备或账户）的类型。 可能值： • host • user
ID	字符串	是	受影响资产（设备或账户）的 ID。
Name	字符串	否	与警报关联的受影响设备的名称（如果将 Type 设置为 host）。 与事件关联的受影响用户账户的用户名，基于这些事件生成警报（如果将 Type 设置为 user）。
IsAttacker	布尔	否	指示受影响资产（设备或账户）是攻击者的标志。
IsVictim	布尔	否	指示受影响资产（设备或账户）是受害者的标志。
CIICategory	字符串	否	作为严重信息基础设施对象的受影响资产（设备或账户）的重要性类别。 可能值： • notCII • ciiWithoutCategory • ciiFirstCategory • ciiSecondCategory • ciiThirdCategory

无键附件

字段	值类型	是否必需	Description
AttachmentID	字符串	是	附件 ID，采用 UUID 格式。
Name	字符串	是	附件名称。
CreatedAt	字符串	是	附件创建的日期和时间，采用 UTC 格式。

`UpdatedAt`	字符串	是	附件最后更改的日期和时间，采用 UTC 格式。
`CreatedBy`	字符串	是	指示受影响资产（设备或账户）是受害者的标志。
`Size`	整数	是	附件大小，以字节为单位。
`State`	字符串	是	附件状态，指示附件上传是正在进行、已完成还是因错误而中止。 可能值： • `completed` • `error` • `uploading`
`Description`	字符串	否	附件描述。
`StatusCode`	字符串	否	向用户显示的状态文本（例如，附件上传失败时显示的错误消息）。

查看警报表

警报表显示在 **监控** → **警报**部分，其中概述了 Kaspersky Next XDR Expert 中记录的所有警报。默认情况下，该表显示与您有访问权限的所有租户相关的警报。如有必要，您可以配置警报表。

要配置警报表，请执行以下操作之一：

- 应用租户过滤器：
  a. 单击“**租户过滤器**”设置旁边的链接。
  租户过滤器将打开。
  b. 选中相应租户旁边的复选框。
- 使用以下方法之一过滤警报表中的数据：
  - 使用主过滤器：
    a. 单击筛选 ( ) 图标。
    b. 单击“**过滤器**”选项卡，然后在调用的菜单中指定并应用筛选条件。
  - 过滤出重新扫描的警报：
    a. 单击“**名称**”列的标题。
    b. 勾选“**仅重新扫描的警报**”或“**排除重新扫描的警报**”复选框。
  - 使用单元格上下文过滤器可以快速添加新的过滤条件：
    a. 找到包含您要添加为过滤条件的值的单元格。请注意，有些列没有单元格上下文过滤器。
    b. 单击单元格中的值。

c. 在打开的列表中，选择以下操作之一：

- **添加到过滤器**中，将该值添加到过滤条件中。
- **从过滤器中排除**，将该值从过滤条件中排除。
- **复制**，将值复制到剪贴板。

- 如果要隐藏或显示某一列，请单击设置 (⚙) 图标，然后选择必要的列。

警报表已配置并显示您需要的数据。

警报表具有以下列：

- **已注册**。警报添加到警报表的日期和时间。
- **更新时间**。警报历史记录中最后更改的日期和时间。
- **警报 ID**。警报的唯一 ID。
- **状态**。警报的当前状态。
- **事故关联类型**。将警报添加到事故的方式。
- **严重级别**。警报的严重级别。
- **名称**。警报名称。
- **已检测到**。已检测到的对象的一个或多个类别。例如，当 Kaspersky Next XDR Expert 检测到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的文件时，“**已检测到**”字段会显示此警报的 Trojan-Downloader.JS.Cryptoload.ad 类别。
- **受影响资产**。受警报影响的设备和用户。

  从将资产添加到 OSMP 时起，大约需要 2 分钟，解决方案才能开始使用该资产丰富事件信息。例如，如果在添加资产后的两分钟内发生关联事件，则生成的警报中不会显示该资产。
- **已分配**。警报的当前负责人。
- **可观察对象**。检测工件，例如 IP 地址或文件的 MD5 哈希。
- **详细信息**。警报简述。
- **状态已更改**。上次警报状态更改的日期和时间。
- **租户**。所检测到的警报的租户名称。
- **外部引用**。外部系统中的警报编号。
- **CII 对象**。用于指示警报是否与 CII 对象相关资产关联的指标。
- **技术**。扫描过程中生成警报的模块或组件的名称。

此列的可能值：

- IOA
- SB（沙盒）
- AM（反恶意软件引擎）
- IOC
- YARA
- KUMA

IOA 规则触发的警报中的事件聚合的特殊注意事项

如果 Kaspersky Next XDR Expert 创建了一个由 IOA 规则触发的警报，并且同一天该主机或其他主机上的其他事件触发了同一 IOA 规则，则 Kaspersky Next XDR Expert 会将这些事件聚合到一个警报中。如果警报已关闭，Kaspersky Next XDR Expert 会重新打开它。事件聚合周期于次日 00:00 结束。

查看警报详情

警报详情是界面中的一个页面，其中包含与警报相关的所有信息，包括警报属性。

要查看警报详情：

1. 在主菜单中，转到“**监控**” → “**Alerts**”。
2. 在警报表中，单击所需警报的 ID。

   警报详情将显示。

如有必要，您可以通过单击警报名称旁边的刷新 (↻) 图标来刷新警报详情中的信息。

您可以使用警报详情上部的工具栏执行以下操作：

- 编辑“**外部参考**”字段值
- 将警报分配给分析师
- 更改警报状态
- 将警报关联到事故
- 取消警报与事故的关联
- 选择行动手册
- 创建新事故并将警报关联到该事故

根据警报类型，警报详情包含以下几个部分：

- **概要**

  根据警报类型，摘要部分可能包含以下警报属性：

  - **分析师**。向其分配了警报的分析师。
  - **名称**。警报名称。如果未指定警报名称，则不显示此字段。
  - **租户**。所检测到的警报的租户名称。
  - **资产**。与警报相关的用户账户和设备的数量。
  - **严重级别**。可能值："**低**"、"**中**"、"**高**"或"**严重**"。警报严重级别基于卡巴斯基的经验显示了此警报可能对计算机安全或企业 LAN 安全产生的影响。
  - **规则**。触发以检测警报的规则。单击规则名称旁边的省略号图标，即可打开快捷菜单。使用此菜单可以了解有关规则的更多详细信息，查找由相同规则检测到的警报或事故，或在"**威胁搜索**"中搜索触发规则的事故，以查找警报的第一个事件和最后一个事件之间的时间段。

    单击菜单中的"**前往威胁搜索**"时，"**威胁搜索**"部分将在同一选项卡中打开。本部分的标题显示您从中下钻到此处的警报的 ID 和名称。如果要在新的浏览器选项卡中打开"**威胁搜索**"部分，请按住 `Ctrl` 密钥，然后在菜单中单击"**前往威胁搜索**"部分。

  - **已注册**。警报添加到警报表的日期和时间。
  - **第一个事件**。与警报相关的第一个事件的日期和时间。
  - **Last event**。与警报相关的最近事件的日期和时间。
  - **外部参考**。指向外部系统中实体的链接（例如，指向 Jira 工单的链接）。您可以单击顶部的"**编辑**"按钮以指定外部参考。如果警报是从 Kaspersky Endpoint Detection and Response 警报创建的，则字段中将显示指向此警报的链接。
  - **已关联到**。与警报相关联的事故。
  - **MITRE 战术**。警报中检测到的一个或多个战术。单击 MITRE 战术名称即可打开上下文菜单。使用快捷菜单，您可以执行以下操作：
    - 点击**在 Kaspersky TIP 中查找**按钮，即可在Kaspersky TIP中查看MITRE战术的详细信息。
    - 点击**在 MITRE ATTCK 中查找**按钮，即可在MITRE ATT&CK知识库中查看MITRE战术的详细信息。
    - 复制MITRE战术名称。
  - **MITRE 技术**。警报中检测到的一种或多种技术。单击 MITRE 技术名称即可打开上下文菜单。使用快捷菜单，您可以执行以下操作：
    - 点击**在 Kaspersky TIP 中查找**按钮，即可在Kaspersky TIP中查看MITRE技术的详细信息。
    - 点击**在 MITRE ATTCK 中查找**按钮，即可在MITRE ATT&CK知识库中查看MITRE技术的详细信息。
    - 复制 MITRE 技术名称。

- **关联规则**。触发用于检测威胁并创建警报的关联规则。
- **IOA 规则**。触发用于检测威胁并创建警报的IOA规则。单击IOA规则名称即可打开快捷菜单。使用快捷菜单，您可以执行以下操作：
  - 单击**打开属性**按钮，查看该IOA规则的详细信息。
  - 单击**前往威胁搜索**按钮，查看相关事件。

    您将被重新导向到**威胁搜索**部分，其中仅显示此IOA规则跟踪的事件。事件的默认显示时间间隔为24小时。本部分的标题显示您从中下钻到此处的警报的 ID 和名称。
  - 查找类似事故。
  - 单击**在 Kaspersky TIP 中查找**按钮，在Kaspersky TIP中查看IOA规则的详细信息。
  - 复制IOA规则名称。
- **技术**。用于检测威胁的检测技术。
- **检测源**。已检测到的对象的来源。例如，如果从某个主机向 Sandbox 发送文件进行扫描，则该主机就是检测源。
- **附加数据**。有关警报的附加信息。您只能使用行动手册编辑此字段中的值。如果添加了值，则会显示该字段。

- **扫描结果**

  “**扫描结果**”部分包含有关已扫描文件和触发警报创建的扫描结果的信息。

- **IOC 扫描结果**

  “**IOC 扫描结果**”部分包含有关扫描期间触发的 IOC 规则的信息。

  单击 IOC 规则名称，即可查看有关该 IOC 规则的详细信息。

  单击“**扫描结果**”列中的“**查看报告**”，即可查看有关扫描结果的详细信息，包括扫描过程中涉及的网络和系统信息、进程和文件。

- **Kaspersky Sandbox 扫描结果**

  “**Kaspersky Sandbox 扫描结果**”部分包含有关 Sandbox 中对象处理结果的信息，包括：
  - 已检测到的对象数量及其类型。
  - 提取的文件数量及其类型。
  - 已检测到的对象的哈希值。

  单击“**导出结果**”，即可查看有关在 Sandbox 可用操作系统中对象处理结果的详细信息，包括：
  - 包含检测统计信息的图表。
  - 包含对象活动树的图表。
  - MITRE 策略和技术（参见 MITRE ATT&CK 知识库）。

- 操作系统中的可疑活动列表。
- 操作系统中文件执行的屏幕截图。
- 系统活动。
- 网络活动。

要在 Sandbox 扫描结果窗口中获取完整信息，请在不同操作系统间切换，同时切换“**快速扫描模式**”与“**完整日志模式**”下的结果。

- YARA **扫描结果**

  YARA **扫描结果**部分包含有关主机上 YARA 扫描结果的信息。

  单击“**扫描结果**”列中的“**查看报告**”，即可查看扫描结果的详细信息。要在 YARA 扫描结果窗口中获取完整信息，请在“**进程和内存转储**”、“**文件**”和“**规则条件**”选项卡之间切换。

- **扫描的文件**

  在“**扫描的文件**”部分，您可以找到有关已扫描文件的信息。要了解更多关于在卡巴斯基威胁情报门户上检测到的文件威胁的信息，请单击“**判定**”列中的威胁名称。

- **详细信息**

  在“**详情**”部分，您可以追踪与警报相关的遥测事件。

  事件表显示您通过 SQL 查询定义的搜索结果。

  可以通过事件表的工具栏执行以下操作：

  - **下载事件**。您可以单击此按钮将相关事件的信息下载为 CSV 文件（UTF-8 编码）。
  - **在“威胁搜索”中查找**。您可以单击此按钮以打开“**威胁搜索**”部分。此部分允许您搜索与您有权访问的租户相关的所有事件，而不仅仅是与当前警报相关的事件。本部分的标题显示您从中下钻到此处的警报的 ID 和名称。

    默认情况下，此部分中打开的事件表包含警报的第一个事件与最后一个事件之间的时间段内发生的所有事件。例如，您可以运行搜索查询来查找设备受到影响的所有事件。

    在“**威胁搜索**”部分，您可以手动将事件关联到警报。如果您发现某些事件与警报相关，但未自动关联到警报，此功能可能会有所帮助。有关详情，请参阅将事件关联到警报或取消关联到警报的说明。

    您可以单击**警报调查**或浏览器中的后退按钮，返回事故详情。
  - **从警报取消关联**。您可以在表中选择一个或多个事件，然后单击此按钮以取消所选事件与警报的关联。

- **资产**

  在**资产**部分，您可以完成以下操作：

  - 查看受警报影响或涉及的设备和用户。
  - 执行响应操作。为此，请选中资产旁边的复选框，然后在**选择响应操作**下拉列表中选择所需的响应操作。
  - 通过点击**导出为CSV**按钮，将有关受影响资产的信息导出为CSV文件。
  - 使用远程终端连接到资产。为此，请点击**打开远程终端**按钮。

资产表包含以下列：

- **资产类型**

  可能值：设备或用户。

- **资产名称**

- **资产 ID**

- **有迹象**

  可能值：攻击者或受害者。

- **授权状态**

  此参数仅适用于设备资产类型。设备授权状态由 KICS for Networks 定义。您可以通过对设备应用相应的响应操作来更改授权状态。

- **管理服务器**

  管理设备的管理服务器。

- **管理组**

  设备所属的管理组。

- **类别**

  包含资产的资产类别。

- **Archived**

  资产的归档状态。可能的值：是或否。

通过单击用户名或设备名称，您可以：

- 查看用户或设备属性。

  > 要查看与设备相关的警报或事故列表，请在设备属性窗口中，单击“**显示相关**”按钮，然后根据要查看的内容选择“**警报**”或“**事故**”。

- 将用户名或设备名称复制到剪贴板。

- 在其他警报中搜索用户名或设备 ID。

- 在其他事故中搜索用户名或设备 ID。

- 在“**威胁搜索**”中搜索用户名或设备 ID，以查找警报的第一个事件与最后一个事件之间的时间间隔。

  > 单击用户名或设备名称后，在菜单中选择“**前往威胁搜索**”，“**威胁搜索**”部分将在同一选项卡中打开。本部分的标题显示您从中下钻到此处的警报的 ID 和名称。如果要在新的浏览器选项卡中打开“**威胁搜索**”部分，请按住 `Ctrl` 密钥，然后在菜单中单击“**前往威胁搜索**”部分。

通过单击用户 ID 或设备 ID，您可以：

- 查看用户或设备属性。

  要查看与设备相关的警报或事故列表，请在设备属性窗口中，单击“**显示相关**”按钮，然后根据要查看的内容选择“**警报**”或“**事故**”。

- 将用户 ID 或设备 ID 复制到剪贴板中。
- 在其他警报中搜索用户 ID 或设备 ID。
- 在其他事故中搜索用户 ID 或设备 ID。
- 在“**威胁搜索**”中搜索用户 ID 或设备 ID，搜索时间范围限定为该警报首个事件到最后一个事件之间的时间段内。

  单击用户 ID 或设备 ID 后，在菜单中选择“**前往威胁搜索**”，“**威胁搜索**”部分将在同一选项卡中打开。本部分的标题显示您从中下钻到此处的警报的 ID 和名称。如果要在新的浏览器选项卡中打开“**威胁搜索**”部分，请按住 `Ctrl` 密钥，然后在菜单中单击“**前往威胁搜索**”部分。

从将资产添加到 OSMP 时起，大约需要 2 分钟，解决方案才能开始使用该资产丰富事件信息。例如，如果在添加资产后的两分钟内发生关联事件，则生成的警报中不会显示该资产。

- **文件**

文件部分包含通过响应操作获取的文件或手动添加到此警报的文件。您可以上传、下载、删除与警报相关的文件，或编辑文件描述。

您可以上传任何扩展名的文件。允许重复的文件名。您可以附加到事故的最大文件数和您可以在配置文件中指定的最大文件总大小。

默认限制：

- 每个警报的文件数量不能超过 100 个。
- 每个警报的文件总大小不得超过 25 MB。

要上传文件，请单击“**上传**”按钮并选择一个或多个文件。如果您尝试上传的文件超出此限制，则会出现显示警告消息的“**上传文件**”面板。在此面板中，您可以从上传队列中删除文件，直到警告消息消失，然后单击“**上传**”按钮上传文件。如果您忽略警告消息，上传将失败，文件列表将包含无法上传的文件，文件名旁边会显示警告图标。

单击“**上传**”按钮后，窗格将关闭，上传的文件将显示在警报详情以及主菜单的“**文件**”部分中的文件表格中。上传大文件或多个文件时，您需要刷新表格以显示新文件。如果文件正在上传，则**名称或完整路径**列会显示加载指示器， **大小**列会显示已上传的文件大小占总文件大小的比例。

单击一个文件以打开显示文件详情的“**编辑文件**”面板。在此面板中，您可以编辑文件描述。

使用复选框来选择一个或多个文件。选择一个或多个文件，然后单击**下载**按钮，以ZIP格式将它们下载为存档文件。该存档受密码*infected*保护。选择一个或多个文件，然后单击“**删除**”按钮来删除所选的文件。

要上传、删除文件、编辑文件描述，需要具备“**警报和事故**”功能区中的“**写入**”权限。要下载文件，需要具备“**警报和事故**”功能区中的“**读取**”权限。

- **Observables**

  在**可观察对象**部分，您可以：

  - 查看与警报相关的可观察对象。
  - 单击**导出到 CSV**按钮，将相关可观察对象的信息导出到 CSV 文件。
  - 使用**值**列中的数据搜索可观测对象表。

    为此，请开始在搜索字段中输入所需可观测对象的数据。如果未找到与**值**列中的可观测对象值匹配的项，则显示空表。

  可观察值可能包括：

  - MD5 hash
  - 网址
  - 域名
  - SHA256
  - 用户名
  - HostName
  - 本地 IP 地址
  - 远程 IP 地址

    以下私有 IP 地址未包含在与警报相关的可观察对象中：
    从 10.0.0.0 到 10.255.255.255，子网掩码为 255.0.0.0 或 /8
    从 172.16.0.0 到 172.31.255.255，子网掩码为 255.240.0.0 或 /12
    从 192.168.0.0 到 192.168.255.255，子网掩码为 255.255.0.0 或 /16
    从 100.64.0.0 到 100.127.255.255，子网掩码为 255.192.0.0 或 /10

    要在可观察对象中包含私有 IP 地址，请在管理员主机上运行以下命令：

    ```
    k0s kubectl -n irp set env deploy/transformer -c transformer
    OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
    ```

    ```
    k0s kubectl -n irp set env deploy/incident -c incident
    OSMP_FILTER_PRIVATE_IPS_DISABLED=true
    ```

  - 本地端口
  - 远程端口
  - 系统进程 ID

- 唯一 PID
- 文件全名

通过单击“**值**”列中的链接，您可以：

- 在“**威胁搜索**”中搜索警报事件首次与末次发生期间的可观察值。

  > 单击“**值**”列中的链接后，在菜单中选择“**前往威胁搜索**”，“**威胁搜索**”部分将在同一选项卡上打开。本部分的标题显示您从中下钻到此处的警报的 ID 和名称。如果要在新的浏览器选项卡中打开“**威胁搜索**”部分，请按住 `Ctrl` 密钥，然后在菜单中单击“**前往威胁搜索**”部分。

- 在其他警报中搜索可观察值。
- 在其他事故中搜索可观察值。
- 将可观察值复制到剪贴板中。

此部分的工具栏包含以下按钮：

- **来自 Kaspersky TIP 的请求状态**。使用此按钮可从 Kaspersky 威胁情报门户 (Kaspersky TIP) 获取有关所选可观察值的详细信息。最终，“**状态更新**”列中的信息将会更新。需要与 Kaspersky 威胁情报门户集成（需要高级访问权限）。
- **来自 Kaspersky TIP 的丰富数据**。使用此按钮可从 Kaspersky TIP 获取有关所有列出的可观察对象的详细信息。最终，“**丰富**”列中的信息将会更新。使用“**丰富**”列中的链接打开已获取的可观察对象的数据增强详情。需要与 Kaspersky 威胁情报门户集成（需要高级访问权限）。
- **移动到隔离区**。使用此按钮将文件所在的设备移动到隔离区。此按钮仅适用于哈希（MD5 或 SHA256）可观察对象。
- **添加防护规则**。使用此按钮可添加阻止文件运行的规则。此按钮仅适用于哈希（MD5 或 SHA256）可观察值。
- **删除防护规则**。使用此按钮可删除阻止文件运行的规则。此按钮仅适用于哈希（MD5 或 SHA256）可观察对象。
- **终止进程**。使用此按钮可终止与文件关联的进程。此按钮仅适用于哈希（MD5 或 SHA256）可观察对象。

- **相似的关闭警报**

  在“**类似的已关闭警报**”部分，您可以查看与当前警报具有相同受影响工件的已关闭警报列表。受影响的工件包括可观察对象和受影响的设备。类似的已关闭警报可以帮助您调查当前警报。

  通过此列表，您可以评估当前警报与其他警报的相似程度。相似度计算公式如下：

  相似度 = M / T * 100

  这里，“M”表示当前警报和类似警报中匹配的工件数量，而“T”表示当前警报中的工件总数。

  如果相似度为 100%，则当前警报与类似警报相比没有任何新内容。如果相似度为 0%，则当前警报与类似警报完全不同。相似度为 0% 的警报不会包含在列表中。

  计算结果将四舍五入为最接近的整数。如果相似度等于 0% 到 1% 之间的值，则应用程序不会将该值向下舍入为 0%。在这种情况下，该值将显示为小于 1%。

单击警报 ID，即可打开警报详情。

自定义相似的已关闭警报列表

您可以使用以下选项来自定义表格：

- 通过选择已更新警报的术语来过滤警报。默认情况下，该列表包含过去 30 天内已更新的警报。
- 单击**列设置**图标（⚙），然后选择要显示的列及其显示顺序。
- 单击**过滤器**图标（▽），然后选择并配置要应用的过滤器。如果选择多个过滤器，它们将通过逻辑运算符“AND”同时应用。
- 单击列标题，然后选择排序选项。您可以按升序或降序对警报进行排序。

- **相似事故**

在“**类似事故**”部分，您可以查看与当前警报具有相同受影响工件的事故列表。受影响的工件包括可观察值和受影响的设备。类似事故可以帮助您判断当前警报是否可能与现有事故相关联。

通过该列表，您可以评估当前警报和事故的相似度。相似度计算公式如下：

相似度 = M / T * 100

其中，“M”表示当前警报与类似事故中匹配的工件数量，“T”表示当前警报中工件的总数。

如果相似度为 100%，则当前警报与类似事故相比没有任何新内容。如果相似度为 0%，则当前警报与类似事故完全不同。相似度为 0% 的事故不包含在列表中。

计算结果将四舍五入为最接近的整数。如果相似度等于 0% 到 1% 之间的值，则应用程序不会将该值向下舍入为 0%。在这种情况下，该值将显示为小于 1%。

单击事故 ID 将打开事故详情。

自定义类似事故列表

您可以使用以下选项来自定义表格：

- 通过选择更新事故的条件，对事故进行过滤。默认情况下，列表包含过去 30 天内更新的事故。
- 单击**列设置**图标（⚙），然后选择要显示的列及其显示顺序。
- 单击**过滤器**图标（▽），然后选择并配置要应用的过滤器。如果选择多个过滤器，它们将通过逻辑运算符“AND”同时应用。
- 单击列标题，然后选择排序选项。您可以按升序或降序对事故进行排序。

- **注释**

在“**注释**”部分，您可以留下与警报相关的注释。例如，您可以输入有关调查结果或更改警报属性（如警报负责人或状态）时的评论。

要保存您的注释，请按 **Enter**。要换行，请按 **Shift+Enter**。要编辑或删除您的注释，请使用右上角的按钮。

您只能在留下注释后的指定时间段内编辑或删除自己的注释。默认间隔是 15 分钟。

如果要更改此设置，请在管理员主机上运行以下命令：

```
k0s kubectl -n irp set env deploy/comment -c comment
OSMP_COMMENT_LOCK_AFTER_DURATION=Nx
```

其中，`N` 表示时间间隔，`x` 表示计量单位：`h`（小时）或 `m`（分钟）。

其他用户的注释无法修改或删除。输入注释需要“**警报和事故**”功能区中的“**写入**”权限。

- **历史记录**

  在“**警报事件日志**”部分，您可以追踪作为工作项对警报所做的更改：

  - 更改警报状态
  - 更改警报负责人
  - 将警报关联到事故
  - 取消警报与事故的关联
  - 将文件上传到警报
  - 从警报中删除文件

  在“**响应历史**”部分，您可以查看手动操作和行动手册响应操作的日志。资源表包含以下各列：

  - **时间**。事件发生的时间。
  - **启动者**。启动响应操作的用户名称。
  - **事件**。事件描述。
  - **响应参数**。响应操作中指定的响应操作参数。
  - **资产**。启动响应操作的资产数量。您可以单击包含资产数量的链接来查看资产详情。
  - **操作状态**。响应操作的执行状态。此列可显示以下值：
    - **等待批准** – 响应操作正在等待启动审批。
    - **已推出** – 响应操作正在执行中。
    - **成功** – 响应操作执行完成，无错误或警告。
    - **警告** – 响应操作已完成，但存在警告。
    - **错误** – 响应操作已完成，但存在错误。
    - **已终止** – 由于用户中断了执行，响应操作停止执行。
    - **批准时间已过** – 由于审批等待超时，响应操作停止执行。
    - **被拒绝**– 由于用户拒绝了启动，响应操作停止执行。
  - **行动手册**。在其中启动响应操作的行动手册的名称。您可以单击链接以查看行动手册详情。

- **响应操作**。已执行的响应操作的名称。
- **资产类型** 为其启动响应操作的资产类型。可能值：**设备**或**用户**。
- **资产租户**。租户是为其启动响应操作的资产的所有者。

向分析师分配警报

作为工作项，可以将警报分配给 SOC 分析师或用户组以进行检查和可能的调查。如果要将警报自动分配给选定组内的分析师，可以将警报分配给用户组。有关详情，请参阅“配置警报和事故的自动分配”。

您可以随时更改活动警报的负责人。您无法更改已关闭警报的负责人。

> 警报只能分配给具有读取和修改警报和事故的访问权限的分析师和用户组。

要分配一个或多个警报：

1. 在主菜单中，转到“**监控**” → “**警报**”。
2. 选择您要分配的警报旁边的复选框。

   您只能选择在同一租户中检测到的警报。否则，“**分配**”按钮将被禁用。

   或者，您可以从“警报详情”中将警报分配给分析师或用户组。要打开警报详情，请单击包含所需警报 ID 的链接。
3. 单击“**分配**”按钮。
4. 在打开的“**分配给分析师**”窗口中，选择是否将警报分配给用户或用户组。
5. 开始输入分析师或用户组的名称，然后从列表中选择负责人。

   如果要取消分配警报，请选择“**未分配**”。

   > 您可以为所有警报选择“**未分配**”，但“**已关闭**”状态的警报除外。
6. 单击“**分配**”按钮。

警报已分配。

您还可以通过使用行动手册来分配警报。

更改警报状态

作为工作项，警报具有一个状态，显示其在生命周期中的当前状态。

仅当您具有读取和修改警报和事故的访问权限时，才能更改您自己或其他分析师的警报的状态。

如果手动更改警报状态，行动手册将不会自动启动。您可以手动为此类警报启动行动手册。

警报可以具有以下状态之一：

- **新建**

  当 Kaspersky Next XDR Expert 登记新警报时，该警报的状态为“*新建*”。您可以将其状态更改为“*进行中*”或“*已关闭*”。当您更改“*新建*”状态更改为“*已关闭*”且警报没有负责人时，警报将自动分配给您。

- **进行中**

  此状态表示分析师已开始处理该警报。您可以将“*进行中*”状态更改为“*新建*”或“*已关闭*”。

- **已关闭**

  真阳性警报将被关联到事故并在事故内进行调查。关闭事故时，所关联的警报也会获得“*已关闭*”状态。您只能将未关联的警报作为误报或低优先级警报对其进行关闭。关闭警报时，您必须选择解决方案。

  “*已关闭*”状态只能更改为“*新建*”。如果要将已关闭的警报恢复为活动状态，请按如下所示更改其状态：“*已关闭*” → “*新建*” → “*进行中*”。

  关闭与事故关联的警报时，该警报将自动与事故取消关联。如果要关闭的警报没有负责人，则警报将被自动分配给关闭该警报的分析师。

- **事故中**

  警报关联到事故时，将获得此状态。此状态无法手动选择。“*关闭*”状态只能分配给关联的警报。要将此状态更改为“*新的*”或“*进行中*”，您必须先取消警报与事故的关联。

要更改一个或多个警报的状态：

1. 在主菜单中，转到“**监控**” → “**警报**”。
2. 执行以下操作之一：
   - 选择您要更改状态的警报旁边的复选框。
   - 单击要更改状态的警报 ID 链接。

     “**警报详情**”窗口将打开。
3. 单击“**更改状态**”按钮。
4. 在“**更改状态**”窗格中，选择要设置的状态。

   如果选择“*已关闭*”状态，则必须选择解决方式。

> 如果将警报状态更改为“*已关闭*”，并且此警报包含未完成的行动手册或响应操作，则所有相关的行动手册和响应操作都将被终止。

5. 单击“**保存**”按钮。

   所选警报的状态已更改。

如果已将警报添加到调查图，则您也可以通过图更改警报状态。

您也可以使用行动手册来更改警报状态。

手动创建警报

您可以从一组事件手动创建警报。您可以使用此功能来检查尚未自动检测到的假设性事故。

> 如果手动创建警报，行动手册不会自动启动。您可以手动为此类警报启动行动手册。

要手动创建警报：

1. 在主菜单中，转到**“监控”** → **“威胁搜索”。**
2. 选择您要为其创建警报的事件。事件应属于同一租户。
3. 单击“**创建警报**”按钮。

   此时将显示一个窗口，其中显示已创建的警报，如果已配置通知模板，您将收到相应的电子邮件通知。“**严重级别**”字段的值对应于所选事件中的最高严重级别。

在“**监控→警报**”表格中，手动创建的警报对应的“**规则**”值为空白。

将警报添加到事故

您可以将一个或多个警报关联到一个事故，原因如下：

- 多个警报可能被视为组织 IT 基础设施中同一问题的指标。如果是这种情况，则可以将事故中的警报作为单个问题进行调查。最多可以将 200 个警报关联到一个事故。
- 如果警报被定义为真阳性，则可以将单个警报关联到一个事故。

如果警报具有除“*已关闭*”以外的任何状态，则可以将警报关联到事故。当关联到事故时，警报将失去其当前状态并获得“*事故中*”的特殊状态。如果您对当前已关联到其他事故的警报进行关联，则该警报将与当前事故取消关联，因为一个警报只能关联到一个事故。

> 警报只能与属于同一租户的事故相关联。

可以手动或自动将警报关联到事故。

手动关联警报

要将警报关联到现有事故或新事故：

1. 在主菜单中，转到**监控 → "警报"**。
2. 选中要关联到事故的警报旁边的复选框。
3. 如果您想将警报关联到现有事故：
   a. 单击"**关联到事故**"按钮。
   b. 选择警报要关联到的事故。

   或者，单击某个警报以显示其详情，然后单击顶部工具栏中的"**关联到事故**"按钮。
4. 如果想将警报关联到新事故：
   a. 单击"**创建事故**"按钮。
   b. 填写新事故的属性：名称、负责人、优先级和描述。

   或者，单击某个警报显示其详情，然后单击顶部工具栏中的"**创建事故**"按钮。
5. 单击"**保存**"按钮。

选定的警报将关联到现有事故或新事故。

自动关联警报

如果您希望警报自动关联到事故，则必须配置分段规则。

解除警报与事故的关联

您可能需要取消警报与事故的关联，例如，如果警报分析和调查显示该警报未与事故中的其他警报关联。当您取消警报与事故的关联时，Kaspersky Next XDR Expert 将执行以下操作：

- 刷新与事故相关的所有数据，以反映警报不再属于该事故。例如，您可以在事故详情中查看更改。
- 将取消关联的警报的状态重置为"*新建*"。

要取消警报与事故的关联：

1. 打开警报详情。
2. 单击顶部工具栏中的"**取消事故关联**"按钮。
   此时将打开"**取消警报关联**"窗口。

3. 如果要更改负责人，请选择“**将警报分配给**”，然后指定新的负责人。
4. 如果要添加注释，请在“**注释**”部分中指定。您指定的注释将显示在“**历史记录**”部分的“**详情**”列中。

选定的警报已与事故取消关联。

将事件关联到警报

如果在调查期间发现与正在调查的警报相关的事件，则可以手动将此事件关联到警报。

> 您可以将事件链接到除“**已关闭**”之外的任何状态的警报。

要将事件关联到警报：

1. 在主菜单中，前往**监控→警报**部分。
2. 在警报列表中，单击要将事件链接到的警报 ID 的链接。
   “**警报详情**”窗口将打开。
3. 转到“**详细信息**”部分，然后单击“**在威胁搜索中查找**”按钮。
   “**威胁搜索**”部分随即打开。默认情况下，事件表包含与所选警报相关的事件。

   > 事件表仅包含与您有权访问的租户相关的事件。

4. 在窗口上部，打开第一个下拉列表，然后选择“**存储**”。
5. 打开第三个下拉列表，然后指定时间范围。
   您可以选择相对于当前日期和时间的预定义范围，使用“**范围开始**”和“**范围结束**”字段来指定自定义范围，或者通过选择日历中的日期来指定。
6. 单击“**运行查询**”按钮。
7. 在更新的事件列表中，选择要关联到警报的事件，然后单击“**关联到警报**”。

所选事件将关联到警报。

解除事件与警报的关联

您可能需要解除事件与警报的关联，例如，如果警报分析和调查显示事件与警报无关。

要解除事件与警报的关联：

1. 在主菜单中，前往**监控→警报**部分。
2. 在警报列表中，单击要解除事件关联的警报 ID 的链接。
   “**警报详情**”窗口将打开。
3. 在“**详细信息**”部分中，选择要解除关联的事件，然后单击“**解除与警报的关联**”按钮。

   所选事件与警报之间的关联将被解除。

在调查图上处理警报

在调查图上，您可以对警报执行以下操作：

- 向图中添加警报。
- 从图中隐藏警报。
- 通过从警报节点的上下文菜单中选择相应项目来查看警报详情。
- 更改警报状态。
- 查看与警报相关的事件。
- 查看与警报相关的资产。
- 查看与警报相关的可观察对象。

向调查图添加警报

您可以通过以下方式之一将警报添加到调查图：

- 从“常规警报表”中添加警报，当您单击调查图上的“**添加警报**”按钮时，该表格将会打开。您必须选中要在调查图上显示的警报旁边的复选框，然后单击“**在图表上显示**”按钮。
- 从类似警报表中。

要从类似警报表中将警报添加到调查图：

1. 执行以下操作之一：
   - 如果调查图上存在资产、可观察对象或分段规则，请单击其节点，然后在上下文菜单中单击“**查找类似警报**”。
   - 如果调查图上存在事件，请单击其节点，然后在上下文菜单中单击“**查看详情**”。在打开的窗口中，单击“**在图表上显示**”按钮。

- 如果调查图上存在警报，请单击其节点，然后在上下文菜单中单击“**事件**”。在事件表中，单击要打开其详情的事件。如果事件详情包含可观察对象、资产或分段规则，请单击相应字段中的链接，然后在上下文菜单中单击“**查找类似警报**”。

- 在调查图上，单击“**威胁搜索**”按钮，然后在常规事件表中，单击要打开其详情的事件。如果事件详情包含可观察对象、资产或分段规则，请单击相应字段中的链接，然后在上下文菜单中单击“**查找类似警报**”。

将显示类似警报的表格。

2. 选中要在调查图上显示的警报旁边的复选框，然后单击“**在图表上显示**”按钮。

选中的警报将添加到调查图中。

从调查图中隐藏警报

您可以通过以下其中一种方式隐藏调查图上的警报：

- 单击警报节点，然后在上下文菜单中选择“**隐藏**”。
- 通过警报表。

要通过警报表从图中隐藏警报：

1. 执行以下操作之一：

   - 在调查图顶部的工具栏中，单击“**添加警报**”按钮。
   - 如果图上显示了可观察对象、资产或事件节点，请单击要为其添加警报的节点，然后在上下文菜单中选择“**查找类似警报**”。

   显示警报表。

2. 选中要从调查图上隐藏的警报旁边的复选框，然后单击“**在图表上显示**”按钮。

选中的警报及其链接将从调查图中隐藏。相关节点仍保留在调查图上。

更改警报状态

要更改警报状态：

1. 单击警报节点，然后在上下文菜单中选择“**更改状态**”。
2. 在打开的“**更改状态**”窗格中，选择状态，然后单击“**保存**”。
   如果选择“*已关闭*”状态，则必须选择解决方式。

所选警报的状态已更改。

查看与警报相关的事件

要查看与警报相关的事件，请执行以下操作之一：

- 单击要显示事件的警报节点旁边的数字。该数字代表与警报相关的事件数。
- 单击要显示事件的警报节点，然后在上下文菜单中单击“**事件**”。

如果要将表中的事件添加到调查图上，请选中事件旁边的复选框，然后单击“**在图表上显示**”按钮。

如果要隐藏调查图上的事件，请选中事件旁边的复选框，然后单击“**在图表上隐藏**”按钮。

查看与警报相关的资产

要查看与警报相关的资产，请单击警报节点。

在上下文菜单中，菜单项“**设备**”和“**用户**”旁边的数字代表与警报相关的设备和用户的数量。

如果要将设备或用户添加到调查图上，请单击相应的菜单项。

查看与警报相关的可观察对象

要查看与警报相关的可观察对象，请单击警报节点，然后在上下文菜单中单击“**事件**”。

在打开的菜单中，菜单项旁边的数字代表与警报相关的可观察对象的数量。

如果要将可观察对象（例如，**哈希**、**域**、**IP 地址**）添加到调查图上，请单击相应的菜单项。

将IOA规则添加到排除项

如果您不想为组织正常资产活动产生警报，可以将IOA规则添加到排除项。

若要将IOA规则添加到警报表中的排除项：

1. 在主菜单中，前往**监控→警报**。
2. 点击过滤器图标。
3. 在**过滤器**选项卡上，指定并应用所需IOA规则的**检测日期**过滤条件。
4. 在警报表中，点击警报的ID。
   警报详情将显示。
5. 在**概要**部分中，点击IOA规则名称。

6. 在IOA规则面板中，点击**添加到排除**。
   此时将打开**添加到排除**面板。

7. 在**添加到排除**面板中，选择要将IOA规则添加到排除项的政策或配置文件。单击"**下一个**"。

8. 指定排除规则属性，然后点击**添加**。
   IOA规则随即被添加到排除项。

若要查看和编辑政策的IOA排除项列表：

1. 在主菜单中，前往**策略**。

2. 请点击所需的政策。

3. 选择**应用程序设置**选项卡。展开左侧的**常规设置**菜单，然后选择**遥测设置**。
   在**EDR Expert（本地部署）遥测数据**选项卡中， **一般排除项**选项卡显示IOA排除项。

   - 若要禁用排除规则，请关闭其**状态**切换开关。
   - 若要删除排除规则，请选中排除规则旁边的复选框，然后单击**删除**。
   - 若要查看排除规则的详细信息，请点击排除规则名称。

管理聚合规则

本部分包含有关聚合规则的常规信息，并提供有关如何创建、编辑、复制、复制到另一个租户以及删除聚合规则的说明。

> 要管理聚合规则，您必须具有以下 XDR 角色之一：主管理员、租户管理员、SOC 管理员。

*聚合规则*允许您将其他卡巴斯基解决方案的重复事件整合到 Open Single Management Platform 警报中。警报要么关联至现有事故，要么生成新事故。

您可以在 **监控 → 资源和服务 → 聚合规则** 中创建和管理聚合规则。聚合规则显示在表中。规则在聚合规则表中的位置越高，其优先级就越高。如果要更改聚合规则优先级，则必须通过单击拖动 (⠿) 图标来拖放该规则进行操作。

对于继承的规则，您只能在父租户中更改优先级。在子租户中，继承的规则的优先级始终高于在该子租户中创建的规则的优先级。此外，继承的规则会保持其在父租户中的相同优先级顺序。

此外，该表还包含由卡巴斯基专家创建的预定义聚合规则。此规则将整合在默认聚合时间间隔（30 秒）内触发了相同关联规则的各项事件。

您无法删除预定义聚合规则，但可以编辑。默认情况下，该规则处于启用状态。

默认情况下，会在所有租户中创建预定义规则，并且会为这些规则禁用继承。如果您为父租户中的规则启用继承，子租户中的相应规则将被父租户设置覆盖。如果您禁用继承，来自父租户的规则将被删除。但是，由于租户不能没有预定义规则，系统会在子租户中自动创建新的本地预定义规则。

聚合规则将根据指定的优先级按顺序进行处理。当满足**触发器**部分中设置的条件时，聚合规则将被触发，并继续搜索其他适用的聚合规则。仅当处理完表中的所有规则后，搜索才会停止。

检测技术相关的限制

根据检测技术的不同，警报聚合存在一些限制：

- 针对文件的 YARA、Sandbox 和反恶意软件检测：
  - 您可以将这些技术的检测结果聚合到同一个文件中。
  - 您无法添加 IOA 检测结果或 IOC 或 YARA 扫描结果。
- IOA 检测：
  - 您可以将由一条或多条 IOA 规则触发的检测结果聚合到一个警报中。
  - 您无法添加所有其他技术的检测结果。
- IOC 扫描：
  - 您可以聚合 IOC 扫描结果（例如，由同一 IOC 规则、不同 IOC 规则、相同或不同主机触发的检测结果）。
  - 您无法添加所有其他技术的检测结果。
- YARA 扫描：
  - 您可以聚合 YARA 扫描结果（例如，由同一 YARA 规则、不同 YARA 规则、相同或不同主机触发的检测结果）。
  - 您无法添加所有其他技术的检测结果。

创建聚合规则

聚合规则可帮助您将其他卡巴斯基解决方案的重复事件整合到 Open Single Management Platform 警报中。

要创建聚合规则，您必须具有以下 XDR 角色之一：主管理员、租户管理员、SOC 管理员。

要创建聚合规则：

1. 在主菜单中，前往**监控→资源和服务→警报聚合**。
   聚合规则表随即打开。
2. 单击“**创建**”按钮。
   “**创建聚合规则**”窗口随即打开。
3. 在“**状态**”字段中，启用要创建的聚合规则。
   默认情况下，该规则处于禁用状态。
4. 在**租户所有者**字段中，指定聚合规则所属的租户。

5. 在“**名称**”字段中，指定聚合规则名称。

   规则名称必须唯一。

6. 在“**警报中的最大事件数**”字段中，指定整合到警报中的事件最大数量。

   该值必须介于 1 到 100 之间。默认值是 100。

7. 在“**聚合间隔**”字段中，指定搜索间隔（以分钟或秒为单位）。

   最大值是 1,500 秒。默认值是 30。

8. 如有必要，请在“**继承者**”字段中更改继承设置。

   默认情况下，层次结构中父租户下的所有子租户都会继承该父租户的规则。您可以通过选择 **仅限当前租户** 选项来禁用继承，或者单击 **特定租户**，然后从下拉列表中选择必须继承该规则的租户。

   > 您只能指定您拥有以下 XDR 角色的租户：主管理员、租户管理员、SOC 管理员。
   > 只能从父租户编辑继承设置、更改规则优先级、复制或删除继承的规则。可以从父租户和子租户更改继承规则的状态。

   在子租户中，继承的规则的优先级始终高于在该子租户中创建的规则的优先级。此外，继承的规则会保持其在父租户中的相同优先级顺序。复制继承的规则时，会连同其作用域一起复制。将继承的规则复制到另一个租户时，不会复制规则作用域。

9. 在“**警报名称**”部分中，指定定义用于创建新警报名称的模板的 jq 表达式。该表达式还用于将多个事件合并到一个警报中。

   默认情况下，指定了以下表达式：`([.Rules[]?.Name // empty] | sort | join(","))`

   创建新警报时，名称将根据模板中指定的字段值来生成。

   如有必要，您可以从另一个聚合规则复制“**警报名称**”部分的 jq 表达式。为此，请单击“**从另一条规则复制**”按钮。

   “警报名称”部分的 jq 表达式示例

   ```
   if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "Brute force
   admin" else "Brute force not admin" end
   ```

10. 在“**触发器**”部分中，指定定义从事件创建警报的条件的 jq 表达式。

    如有必要，您可以从另一个聚合规则复制“**触发器**”部分的 jq 表达式。为此，请单击“**从另一条规则复制**”按钮。

    “触发器”部分的 jq 表达式示例

    ```
    .AggregationID | startswith("bruteforce_DestinationUserName")
    ```

11. 如有必要，在“**描述**”字段中指定聚合规则的描述。

12. 单击“**创建**”按钮。

    聚合规则被创建。

默认情况下，聚合规则创建时优先级设为最低。要更改聚合规则优先级，请在聚合规则表中单击规则名称，然后拖放规则。规则在聚合规则表中的位置越高，其优先级就越高。

编辑聚合规则

您可以编辑聚合规则设置。

对于继承的规则，您在子租户中只能更改规则状态。如果要编辑其他设置，必须在父租户中进行编辑，之后更改将传播到子租户。

要编辑聚合规则：

1. 在主菜单中，前往**监控→资源和服务→聚合规则**。
2. 在打开的聚合规则表中，单击您想要编辑的聚合规则的名称。
3. 在打开的“**编辑聚合规则**”窗口中，编辑聚合规则属性。有关您可以编辑的规则属性的更多详细信息，请参阅“创建聚合规则”。
4. 单击“**应用**”按钮。
5. 如果要更改聚合规则优先级，请在聚合规则表中单击规则名称，然后拖放规则。
   规则在聚合规则表中的位置越高，其优先级就越高。

聚合规则的属性将被修改并保存。

将聚合规则复制到另一个租户

您可以将现有的聚合规则复制到另一个租户。

如果已构建OSMP 实例层次结构，则您只能在单个实例内复制规则。

要复制聚合规则：

1. 在主菜单中，前往**监控→资源和服务→聚合规则**。
2. 在聚合规则表中，选择要复制的规则，然后单击“**复制到租户**”。
3. 选择一个或多个目标租户，然后单击“**复制**”。
4. 如果目标租户包含同名的聚合规则，则会显示“**覆盖或重命名聚合规则?** ”窗口：
   - 如果要删除之前为目标租户创建的规则并将其替换为要复制的规则，请单击“**覆盖**”。
   - 如果要保留之前创建的规则并复制指定规则（在其标题后添加“copy”），请单击“**复制和重命名**”。

   如果您复制继承的规则，而目标租户已存在同名规则，则不会覆盖此规则。您必须更改正在复制的规则的名称。此外，复制继承的规则时会保留其状态，但不包含其作用域。

单击关闭 (✕) 按钮，窗口将关闭，并且不会复制名称与目标租户中相同的聚合规则。但是，如果在步骤 2 中您还选择了目标租户中不存在的聚合规则，则会复制这些规则。

聚合规则将复制到其他租户。

删除聚合规则

您可以一次永久删除一个或多个聚合规则。

如果某个聚合规则是继承的，则您只能从其父租户中删除该规则。

您无法删除预定义的聚合规则。由于租户不能在没有预定义规则的情况下存在，因此删除该规则后，将自动创建一个新的本地预定义规则。

要删除聚合规则：

1. 在主菜单中，前往**监控→资源和服务→聚合规则**。
2. 在聚合规则表中，选择一个或多个要删除的聚合规则，然后单击“**删除**”。
3. 在确认对话框中，单击“**删除**”。

聚合规则被删除。

处理事故

本部分包含有关事故、事故的属性、典型生命周期和警报连接的一般信息。本部分还提供有关如何创建事故、分析事故表、根据生命周期的当前状态更改事故属性以及合并事故的说明。

如满足以下条件，“**事故**”部分将显示在主菜单中：

- 拥有 Kaspersky Next XDR Expert 的授权许可密钥。
- 已连接到 OSMP 控制台中的根管理服务器。
- 您拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、1 级分析师、2 级分析师、SOC 经理、审批人、审计员、与子事故交互的角色。

关于事故

*事故*是警报的容器，通常表明组织 IT 基础设施中存在真实的问题。一个事故可能包含一个或多个警报。通过使用事故，分析师可以将多个警报作为单个问题进行调查。

您可以手动创建事故，也可以启用事故自动创建规则。创建事故后，您可以将警报关联到该事故。最多可以将 200 个警报关联到一个事故。

创建后，Kaspersky Next XDR Expert 会将事故作为需要由分析师处理的工作项添加到事故表中。

只能将事故分配给具有读取和修改警报和事故的访问权限的分析师。

您可以使用以下事故属性将事故作为工作项进行管理：

- **事故状态**

  可能值："*新建*"、"*进行中*"、"*搁置*"或"*已关闭*"。

  事故状态显示了事故在其生命周期中的当前状态。您可以根据需要更改状态，但以下情况除外：

  - "*新建*"状态不能被更改为"*搁置*"。
  - "*已关闭*"状态只能更改为"*新建*"。

- **事故严重级别**

  可能值："**低**"、"**中**"、"**高**"或"**严重**"。

  事故严重级别基于卡巴斯基的经验显示了此事故可能对计算机安全或企业 LAN 安全产生的影响。事故严重级别对应于所关联警报的最高严重级别，不能手动更改。

- **事故优先级**

  可能值："**低**"、"**中**"、"**高**"或"**严重**"。

  事故优先级定义了分析师调查事故的顺序。优先级为"**严重**"的事故是最紧急的事故，必须优先调查。您可以手动更改事故优先级。

- **事故负责人**

  该角色为事故所有者，即负责事故调查和处理的分析师。如果"**状态**"参数未设置为"**已关闭**"，则您可以随时更改事故负责人。

两个或多个事故可能被解释为组织 IT 基础设施中同一问题的指标。如果是这种情况，您可以合并这些事故以将它们作为单个问题进行调查。

每个事故都具有*事故详情*，其中提供了与该事故相关的所有信息。您可以使用这些信息来调查事故或合并事故。

对于每个事故，您可以创建子事故。您可以根据子事故来调查不同租户中的事故并做出响应。您还可以创建另一个子事故的子事故。一个父事故最多可以包含 200 个子事故。

事故数据模型

事故的结构由包含值的字段表示（见下表）。有些字段是对象或对象数组，具有自己的一组字段（例如，`Assignee` 和 `Alerts` 字段）。

事故

字段	值类型	是否必需	Description
`InternalID`	字符串	是	内部事故 ID，采用 UUID 格式。

ID	整数	是	短格式的内部事故 ID。
TenantID	字符串	是	与事故关联的租户的 ID，采用 UUID 格式。
IncidentType	IncidentType 对象	是	事故类型
Name	字符串	是	事故名称。
WorkflowName	字符串	是	事故工作流的名称。
WorkflowUUID	字符串	是	事故工作流的唯一标识符，采用 UUID 格式。
Description	字符串	否	事故描述。
CreatedAt	字符串	是	事故创建日期和时间，采用 RFC 3339 格式。
UpdatedAt	字符串	是	上次事故更改的日期和时间，采用 RFC 3339 格式。
StatusChangedAt	字符串	否	事故状态更改的日期和时间，采用 RFC 3339 格式。
Severity	字符串	否	事故的严重级别。 可能值： • critical • high • medium • low
Priority	字符串	是	事故优先级 可能值： • critical • high • medium • low
Assignee	Assignee 对象	否	被分配负责处理该事故的操作员。
FirstEventTime	字符串	否	与事故相关的警报的第一个遥测事件的日期和时间，采用 RFC 3339 格式。
LastEventTime	字符串	否	与事故相关的警报的最后一个遥测事件的日期和时间，采用 RFC 3339 格式。
State	字符串	是	事故状态 可能值： • open • inProgress • hold • closed
StatusUUID	字符串	是	事故状态 ID，采用 UUID 格式。
StatusResolution	字符串	否	事故状态的解析。 可能值： • truePositive • falsePositive • lowPriority • merged
DetectSources	字符串数组	否	检测并生成事故的组件。
DetectionTechnologies	字符串数组	否	触发的检测技术。
Alerts	警报 对象数组	否	事故中包含的警报。
AdditionalData	对象	否	有关警报的附加信息，采用 JSON 格式。此信息可由用户或行动手册填写。
ExternalRef	字符串	是	指向外部系统中实体的链接（例如，指向 Jira 工单的链接）。
SignOfCreation	字符串	是	创建事故的方法。
IsCII	布尔	是	指示受影响资产（设备或账户）是否为严重信息基础设施对象的标志。
Attachments	UnkeyedAttachment 对象数组	否	与事故相关的附件。

IncidentType

字段	值类型	是否必需	Description
ID	字符串	是	事故类型 ID，采用 UUID 格式。
Name	字符串	是	事故类型的名称。
Description	字符串	是	事故类型描述。

负责人

字段	值类型	是否必需	Description
ID	字符串	是	被分配负责处理该事故的操作员的用户账户 ID。
Name	字符串	是	被分配负责处理该事故的操作员的姓名。

无键附件

字段	值类型	是否必需	Description
AttachmentID	字符串	是	附件 ID，采用 UUID 格式。
Name	字符串	是	附件名称。
CreatedAt	字符串	是	附件创建的日期和时间，采用 UTC 格式。
UpdatedAt	字符串	是	附件最后更改的日期和时间，采用 UTC 格式。
CreatedBy	字符串	是	指示受影响资产（设备或账户）是受害者的标志。
Size	整数	是	附件大小，以字节为单位。
State	字符串	是	附件状态，指示附件上传是正在进行、已完成还是因错误而中止。 可能值： • completed • error • uploading
Description	字符串	否	附件描述。
StatusCode	字符串	否	向用户显示的状态文本（例如，附件上传失败时显示的错误消息）。

创建事故

您可以手动创建事故，也可以启用事故自动创建规则。本主题介绍了如何手动创建事故。

要创建事故，您必须具有读取和修改警报和事故的访问权限。

如果手动创建事故，行动手册将不会自动启动。您可以手动为此类事故启动行动手册。

您可以使用事故表或警报表创建事故。

使用事故表创建事故

要创建事故：

1. 在主菜单中，转到“**监控**” → “**事故**”。单击“**创建事故**”按钮。
2. 在“**常规设置**”步骤中，指定以下设置：
   - 事故名称。
   - **租户**

     与事故关联的租户。警报只能与属于同一租户的事故相关联。之后，您将无法更改事故的租户。
   - **负责人**

     该角色为事故所有者，即负责事故调查和处理的分析师。如果“**状态**”参数未设置为“**已关闭**”，则您可以随时更改事故负责人。
   - **优先级**

     可能值：“**低**”、“**中**”、“**高**”或“**严重**”。

     事故优先级定义了分析师调查事故的顺序。优先级为“**严重**”的事故是最紧急的事故，必须优先调查。您可以手动更改事故优先级。
   - **描述**

     在此字段中，您可以输入事故的描述。例如，您可以描述问题或提供所关联警报的调查结果。描述将被添加到事故详情的“**描述**”部分。

     该字段是可选的。
3. 单击“**确定**”。

   事故已创建。

使用警报表创建事故

您可以通过选择要关联到新事故的警报来创建事故。请参阅将警报关联到事故。

创建子事故

通过子事故可以监控调查进度并针对不同租户的各类事故执行响应。您还可以创建另一个子事故的子事故。一个父事故最多可以有 200 个子事故。

> 您必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、1 级分析师、2 级分析师、SOC 经理、审批人、与子事故交互的角色。

要创建子事故：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在事故表中，单击相应事故的 ID。
   “**事故详情**”窗口打开。
3. 在“**子事故**”部分中，单击“**创建**”按钮。
   将打开“**创建子事故**”窗口。
4. 如有必要，可以在“**名称**”字段中更改子事故的名称。
   默认情况下，子事故名称包含 [Child] 标签和父事故名称。
5. 在“**租户**”下拉列表中，选择要将子事故分配给哪个租户。
6. 在“**分析师**”下拉列表中，输入分析师的姓名，然后从列表中选择分析师。
   您也可以选择“**未分配**”选项。
7. 如有必要，请在“**优先级**”下拉列表中更改事故优先级。
   默认情况下，子事故会继承父事故的优先级。
8. 如有必要，请在“**描述**”字段中指定子事故的描述。
9. 如果要复制父事故的所有信息，请选中“**从父事故复制信息**”复选框。
   如果选中此复选框，则将复制父事故中的所有信息（包括可观察对象、资产和已关联的警报）。复制的警报将分配给子事故的租户。
   如果取消选中此复选框，则子事故不会包含来自父事故的资产、可观察对象和已关联警报的信息。
10. 单击“**创建**”按钮。

子事故将创建完成并关联到父事故。您可以在“**事故详情**”窗口的“**子事故**”部分中找到子事故。

如果将子事故分配给不具有父事故所属事故类型的租户，则将为子事故分配默认事故类型和默认事故工作流。如有必要，您可以更改事故类型。

查看事故表格

事故表显示在“**监控**” → “**事故**”部分，并提供了所有已创建事故的概览。默认情况下，该表显示与您拥有访问权限的所有租户相关的事故。如有必要，您可以配置事故表。

要配置事故表，请执行以下操作之一：

- 应用租户过滤器：
  a. 单击“**租户过滤器**”设置旁边的链接。
     租户过滤器将打开。
  b. 选中相应租户旁边的复选框。

- 过滤警报表的数据：

  a. 单击筛选 ( ) 图标。

  b. 单击“**过滤器**”选项卡，然后在调用的菜单中指定并应用筛选条件。

- 如果要隐藏或显示某一列，请单击设置 ( ) 图标，然后选择必要的列。

事故表已配置并显示您需要的数据。

事故表包含以下列：

- **创建日期**。创建事故的日期和时间。
- **威胁持续时间**。与事故关联的所有警报中，最早事故与最近事故之间的时间间隔。
- **更新日期**。事故历史记录中最后更改的日期和时间。
- **事故 ID**。事故的唯一标识符。
- **状态**。事故的当前状态。
- **分类时间**。接受事故的时间限制，以天、小时和分钟为单位。
- **响应所花的时间**。对事故进行初始响应的时间限制，以天、小时和分钟为单位。
- **解决时间**。解决事故的时间限制，以天、小时和分钟为单位。
- **状态已改变**。事故状态更改的日期和时间。
- **严重级别。**事故的严重级别。
- **优先级**。事故的优先级。
- **已关联的警报**。事故中包含的警报数量。
- **名称**。事故名称。
- **规则**。触发创建事故的规则。
- **受影响的资产**。受事故影响的设备和用户。如果受事故影响或涉及事故的资产数量大于或等于三，则会显示受影响设备的数量。
- **租户**。检测到事故的租户名称。
- **外部引用**。The incident number in an external system.
- **被分配者**。事故的当前负责人。

- **具有父事故**。显示事故是否具有父事故。如果显示值为“**是**”，则该事故为子事故。
- **子事故的状态**。第一级子事故的结果状态。可能值：“**已关闭**”、“**进行中**”、“**无子事故**”。
- **创建方法**。事故的创建方式：手动或自动。
- **可观察对象**。检测工件的数量，例如 IP 地址或文件的 MD5 哈希值。如果可观察对象的数量大于或等于 3，则显示可观察对象的数量。

如有必要，您可以将事故表中显示的所有事故的信息导出到 JSON 文件。

查看事故详情

事故详情是界面中的一个页面，其中包含与事故相关的所有信息，包括事故属性等。

要查看事故详情：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在事故表中，单击相应事故的 ID。

   将显示包含事故详情的窗口。

如有必要，您可以单击事故名称旁边的刷新 (↻) 图标，刷新事故详情中的信息。

事故详情上部的工具栏允许您执行以下操作：

- 编辑“**名称**”、“**描述**”和“**外部参考**”字段值
- 在调查图上查看事故
- 更改事故状态
- 更改事故优先级
- 将事故分配给分析师
- 选择行动手册
- 将警报关联至事故
- 将该事故与其他事故合并

事故详情包含以下部分：

- **概要**

  摘要部分包含以下事故属性：

  - **类型**。事故类型
  - **分析师**。事故的当前负责人。

- **创建方法**。事故的创建方式：手动或自动。
- **名称**。事故创建时指定的名称。您可以单击顶部的“**编辑**”按钮来更改事故名称。
- **租户**。检测到事故的租户名称。
- **资产**。受事故影响的用户和设备数量。
- **注册日期**。创建事故的日期和时间。
- **更新日期**。事故历史记录中最后更改的日期和时间。
- **第一个事件**。与事故相关的第一个事件的日期和时间。这是与该事故关联的所有警报中，警报详情的“详情部分”里时间最早的事件。
- **最近的事件。**与事故相关的最新事件的日期和时间。这是与该事故关联的所有警报中，警报详情的“详情部分”里时间最新的事件。
- **描述。**事故描述。您可以单击顶部的“**编辑**”按钮以指定描述。
- **外部引用。**关联到外部系统中的实体。您可以单击顶部的“**编辑**”按钮以指定外部参考。
- **优先级**。可能值：**低**、**中**、**高**或**严重**。事故优先级决定了调查事故的顺序。优先级为“**严重**”的事故是最紧急的事故，可以首先进行调查。您可以通过单击当前优先级值来更改优先级。
- **严重级别**。可能值：**低**、**中**、**高**或**严重**。事故严重级别基于卡巴斯基的经验显示了此事故可能对计算机安全或企业 LAN 安全产生的影响。
- **分类时间** – 接受事故的时间限制，以天、小时和分钟为单位。
- **响应时间** – 对事故进行初始响应的时间限制，以天、小时和分钟为单位。
- **解决时间** – 解决事故的时间限制，以天、小时和分钟为单位。
- **相关规则**。被触发用于检测已关联警报的规则。单击规则名称旁边的省略号图标，即可打开快捷菜单。使用此菜单可以了解有关规则的更多详细信息，查找由同一规则检测到的警报或事故，或在“**威胁搜索**”中搜索事故首次与末次发生期间触发该规则的相关事件。“**威胁搜索**”部分的标题显示您深入查看到此部分时所源自的事故 ID 和名称。

  > 当您点击菜单中的“**前往威胁搜索**”时，“**威胁搜索**”部分将在同一选项卡中打开。如果您想在新浏览器选项卡中打开“**威胁搜索**”部分，请点击并按住“Ctrl”键，然后单击菜单中的“**前往威胁搜索**”。

- IOA **规则**。触发用于检测威胁并创建警报的IOA规则。单击IOA规则名称即可打开快捷菜单。使用快捷菜单，您可以执行以下操作：
  - 单击**打开属性**按钮，查看该IOA规则的详细信息。
  - 单击**前往威胁搜索**按钮，查看相关事件。

    您将被重新导向到**威胁搜索**部分，其中仅显示此IOA规则跟踪的事件。事件的默认显示时间间隔为24小时。该部分标题显示您从中深入查看的事故的ID和名称。
  - 查找类似事故。

- 单击**在 Kaspersky TIP 中查找**按钮，在Kaspersky TIP中查看IOA规则的详细信息。
- 复制IOA规则名称。

- **MITRE 战术**。在关联到该事故的警报中检测到的一种或多种战术。单击MITRE战术名称即可打开上下文菜单。使用快捷菜单，您可以执行以下操作：
  - 点击**在 Kaspersky TIP 中查找**按钮，即可在Kaspersky TIP中查看MITRE战术的详细信息。
  - 点击**在 MITRE ATTCK 中查找**按钮，即可在MITRE ATT&CK知识库中查看MITRE战术的详细信息。
  - 复制MITRE战术名称。
- **MITRE 技术**。在关联到该事故的警报中检测到的一种或多种技术。单击MITRE技术名称即可打开上下文菜单。使用快捷菜单，您可以执行以下操作：
  - 点击**在 Kaspersky TIP 中查找**按钮，即可在Kaspersky TIP中查看MITRE技术的详细信息。
  - 点击**在 MITRE ATTCK 中查找**按钮，即可在MITRE ATT&CK知识库中查看MITRE技术的详细信息。
  - 复制MITRE技术名称。
- **附加数据**。有关事故的其他信息。您只能使用行动手册编辑此字段中的值。如果添加了值，则会显示该字段。

- **详细信息**

  在“**详情**”部分中，您可以跟踪与事故相关的遥测事件。

  要查看与事故相关的事件，请单击“**在威胁搜索中查找**”按钮。打开的表显示与事故相关的警报。“**威胁搜索**”部分的标题显示您深入查看到此部分时所源自的事故 ID 和名称。

  可以通过事件表的工具栏执行以下操作：

  - **下载事件**。单击此按钮可将有关相关事件的信息下载为 TSV 文件。
  - **取消与事故的关联**。您可以在表中选择一个或多个事件，然后单击此按钮，将解除所选事件与该事故相关警报之间的关联。

  您可以单击**事故调查**或浏览器中的后退按钮，返回事故详情。

- **相似事故**

  在“**类似事故**”部分，您可以查看与当前事故具有相同受影响工件的事故列表。受影响的工件包括与事故关联的警报的可观察对象和受影响的设备。该列表包含任何状态的事故。

  通过该列表，您可以评估当前事故与其他事故的相似度。相似度计算公式如下：

  相似度 = M / T * 100

  其中，M 表示当前事故和类似事故中匹配的工件数量，T 表示当前事故中的工件总数。

  如果相似度为 100%，则表示当前事故与类似事故相比没有任何新内容。如果相似度为 0%，则表示当前事故和类似事故完全不同。相似度为 0% 的事故不包含在列表中。

  计算结果将四舍五入为最接近的整数。如果相似度等于 0% 到 1% 之间的值，则应用程序不会将该值向下舍入为 0%。在这种情况下，该值将显示为小于 1%。

单击事故 ID 将打开事故详情。

自定义类似事故列表

您可以使用以下选项来自定义表格：

- 通过选择更新事故的条件，对事故进行过滤。默认情况下，列表包含过去 30 天内更新的事故。
- 单击**列设置**图标（⚙），然后选择要显示的列及其显示顺序。
- 单击**过滤器**图标（▽），然后选择并配置要应用的过滤器。如果选择多个过滤器，它们将通过逻辑运算符“AND”同时应用。
- 单击列标题，然后选择排序选项。您可以按升序或降序对事故进行排序。

- **警报**

  在“**警报**”部分，您可以查看关联至当前事故的警报列表。

  通过单击警报 ID，您可以打开“警报详情”。您还可以使用工具栏按钮以解除警报与事故的关联。

- **资产**

  在**资产**部分，您可以完成以下操作：

  - 查看受警报影响或涉及的设备和用户。
  - 执行响应操作。为此，请选中资产旁边的复选框，然后在**选择响应操作**下拉列表中选择所需的响应操作。
  - 通过点击**导出为CSV**按钮，将有关受影响资产的信息导出为CSV文件。
  - 使用远程终端连接到资产。为此，请点击**打开远程终端**按钮。

  资产表包含以下列：

  - **资产类型**
    可能值：设备或用户。
  - **资产名称**
  - **资产 ID**
  - **授权状态**
    此参数仅适用于设备资产类型。设备授权状态由 KICS for Networks 定义。您可以通过对设备应用相应的响应操作来更改授权状态。
  - **有迹象**
    可能值：攻击者或受害者。
  - **管理服务器**
    管理设备的管理服务器。

- **类别**
  包含资产的资产类别。

- **Archived**
  资产的归档状态。可能的值：是或否。

- **计数**
  受事故影响或涉及事故且具有相同 ID、类型和名称的设备和用户的数量。

- **管理组**
  设备所属的管理组。

通过单击用户名或设备名称，您可以：

- 查看用户或设备属性。

  > 要查看与设备相关的警报或事故列表，请在设备属性窗口中，单击“**显示相关**”按钮，然后根据要查看的内容选择“**警报**”或“**事故**”。

- 将用户名或设备名称复制到剪贴板。
- 在其他警报中搜索用户名或设备 ID。
- 在其他事故中搜索用户名或设备 ID。
- 在“**威胁搜索**”中搜索事故首次与末次发生期间的用户名或设备 ID。

  > 单击用户名或设备名称后，在菜单中选择“**前往威胁搜索**”，“**威胁搜索**”部分将在同一选项卡中打开。如果您想在新浏览器选项卡中打开“**威胁搜索**”部分，请点击并按住“`Ctrl`”键，然后单击菜单中的“**前往威胁搜索**”。

通过单击用户 ID 或设备 ID，您可以：

- 查看用户或设备属性。

  > 要查看与设备相关的警报或事故列表，请在设备属性窗口中，单击“**显示相关**”按钮，然后根据要查看的内容选择“**警报**”或“**事故**”。

- 将用户 ID 或设备 ID 复制到剪贴板中。
- 在其他警报中搜索用户 ID 或设备 ID。
- 在其他事故中搜索用户 ID 或设备 ID。

- 在“**威胁搜索**”中搜索事故首次与末次发生期间的用户 ID 或设备 ID。

  点击用户 ID 或设备 ID 后，在菜单中选择“**前往威胁搜索**”，“**威胁搜索**”部分将在同一选项卡中打开。如果您想在新浏览器选项卡中打开“**威胁搜索**”部分，请点击并按住“Ctrl”键，然后单击菜单中的“**前往威胁搜索**”。

- **子事故**

  在“**子事故**”部分中，您可以查看当前浏览的事故的子事故列表。

- **文件**

  文件部分包含通过响应操作获取的文件或手动添加到此事故的文件。您可以上传、下载、删除与事故相关的文件，或编辑文件描述。

  您可以上传任何扩展名的文件。允许重复的文件名。您可以附加到事故的最大文件数和您可以在配置文件中指定的最大文件总大小。

  默认限制：

  - 每个事故的文件数不能超过 100 个。
  - 每个事故的文件总大小不能超过 25 MB。

  要上传文件，请单击“**上传**”按钮并选择一个或多个文件。如果您尝试上传的文件超出此限制，则会出现显示警告消息的“**上传文件**”面板。在此面板中，您可以从上传队列中删除文件，直到警告消息消失，然后单击“**上传**”按钮上传文件。如果您忽略警告消息并单击“**上传**”按钮，上传将失败，文件列表将包含无法上传的文件，文件名旁边会显示警告图标。

  单击“**上传**”按钮后，窗格将关闭，上传的文件会同时显示在事故详细信息的文件表格中以及主菜单的“**文件**”部分中。上传大文件或多个文件时，您需要刷新表格以显示新文件。如果文件正在上传，则**名称或完整路径**列会显示加载指示器， **大小**列会显示已上传的文件大小占总文件大小的比例。

  单击一个文件以打开显示文件详情的“**编辑文件**”面板。在此面板中，您可以编辑文件描述。

  使用复选框来选择一个或多个文件。选择一个或多个文件，然后单击**下载**按钮，以ZIP格式将它们下载为存档文件。该存档受密码*infected*保护。选择一个或多个文件，然后单击“**删除**”按钮来删除所选的文件。

  要上传、删除文件、编辑文件描述，需要具备“**警报和事故**”功能区中的“**写入**”权限。要下载文件，需要具备“**警报和事故**”功能区中的“**读取**”权限。

- Observables

  在**可观测对象**部分中，您可以：

  - 查看属于与当前事故关联的警报的可观测对象。
  - 单击**导出到 CSV**按钮，将相关可观测对象的信息导出到 CSV 文件。
  - 使用**值**列中的数据搜索可观测对象表。

    为此，请开始在搜索字段中输入所需可观测对象的数据。如果未找到与**值**列中的可观测对象值匹配的项，则显示空表。

  可观察值可能包括：

  - MD5 hash
  - 网址
  - 域名

- SHA256
- 用户名
- HostName
- IP 地址

以下私有 IP 地址不会纳入与关联至当前事故的警报相关的可观察对象中：
10.0.0.0 至 10.255.255.255，子网掩码为 255.0.0.0 或 /8
172.16.0.0 至 172.31.255.255，子网掩码为 255.240.0.0 或 /12
192.168.0.0 至 192.168.255.255，子网掩码为 255.255.0.0 或 /16
100.64.0.0 至 100.127.255.255，子网掩码为 255.192.0.0 或 /10

要在可观察值中包含私有 IP 地址，请在管理员主机上运行以下命令：

```
k0s kubectl -n irp set env deploy/transformer -c transformer
OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
```

```
k0s kubectl -n irp set env deploy/incident -c incident
OSMP_FILTER_PRIVATE_IPS_DISABLED=true
```

通过单击“**值**”列中的链接，您可以：

- 在事故的第一个事件和最后一个事件之间的时间段内，在**威胁搜索**中搜索可观察值。

单击“**值**”列中的链接后，在菜单中选择“**前往威胁搜索**”，“**威胁搜索**”部分将在同一选项卡上打开。该部分标题显示您从中深入查看的事故的ID和名称。如果要在新的浏览器选项卡中打开**威胁搜索**部分，请按住`Ctrl`密钥，然后在菜单中单击**前往威胁搜索**。

- 在其他警报中搜索可观察值。
- 在其他事故中搜索可观察值。
- 将可观察值复制到剪贴板中。

此部分的工具栏包含以下按钮：

- **来自 Kaspersky TIP 的请求状态**。使用此按钮可从 Kaspersky 威胁情报门户 (Kaspersky TIP) 获取有关所选可观察值的详细信息。最终，“**状态更新**”列中的信息将会更新。需要与 Kaspersky 威胁情报门户集成（需要高级访问权限）。
- **来自 Kaspersky TIP 的丰富数据**。使用此按钮可从 Kaspersky TIP 获取有关所有列出的可观察对象的详细信息。最终，“**丰富**”列中的信息将会更新。使用“**丰富**”列中的链接打开已获取的可观察对象的数据增强详情。需要与 Kaspersky 威胁情报门户集成（需要高级访问权限）。
- **移动到隔离区**。使用此按钮将文件所在的设备移动到隔离区。此按钮仅适用于哈希（MD5 或 SHA256）可观察对象。

- **添加防护规则**。使用此按钮可添加阻止文件运行的规则。此按钮仅适用于哈希（MD5 或 SHA256）可观察值。
- **删除防护规则**。使用此按钮可删除阻止文件运行的规则。此按钮仅适用于哈希（MD5 或 SHA256）可观察对象。
- **终止进程**。使用此按钮可终止与文件关联的进程。此按钮仅适用于哈希（MD5 或 SHA256）可观察对象。

- **历史记录**

  在"**事故日志**"部分，您可以跟踪该事故作为工作项所发生的变更：
  - 更改事故状态
  - 更改事故负责人
  - 将警报关联到事故
  - 解除警报与事故的关联
  - 创建子事故
  - 将事故与其他事故合并
  - 将文件上传到事故
  - 从事故中删除文件

  在"**响应历史**"部分，您可以查看手动操作和行动手册响应操作的日志。资源表包含以下各列：
  - **时间**。事件发生的时间。
  - **启动者**。启动响应操作的用户名称。
  - **事件**。事件描述。
  - **响应参数**。响应操作中指定的响应操作参数。
  - **资产**。启动响应操作的资产数量。您可以单击包含资产数量的链接来查看资产详情。
  - **操作状态**。响应操作的执行状态。此列可显示以下值：
    - **等待批准** – 响应操作正在等待启动审批。
    - **已推出** – 响应操作正在执行中。
    - **成功** – 响应操作执行完成，无错误或警告。
    - **警告** – 响应操作已完成，但存在警告。
    - **错误** – 响应操作已完成，但存在错误。
    - **已终止** – 由于用户中断了执行，响应操作停止执行。
    - **批准时间已过** – 由于审批等待超时，响应操作停止执行。
    - **被拒绝**– 由于用户拒绝了启动，响应操作停止执行。

- **行动手册**。在其中启动响应操作的行动手册的名称。您可以单击链接以查看行动手册详情。
- **响应操作**。已执行的响应操作的名称。
- **资产类型** 为其启动响应操作的资产类型。可能值：**设备**或**用户**。
- **资产租户**。租户是为其启动响应操作的资产的所有者。

- **工作量日志**

  在“**工作量日志**”部分，您可以查看分析师在事故相关工作上所投入的工作量。

  在此部分，您可以管理您的工作量。您无法修改或删除其他分析师添加的工作量。

  通过单击“**数据**”列中的链接，您可以查看和编辑您的工作量。

- **注释**

  在“**注释**”部分，您可以留下与事故相关的评论。例如，您可以输入关于调查结果的评论，或在修改事故属性（如事故负责人、事故状态）时添加注释。

  要保存您的注释，请按 **Enter**。要换行，请按 **Shift+Enter**。要编辑或删除您的注释，请使用右上角的按钮。

  您只能在留下注释后的指定时间段内编辑或删除自己的注释。默认间隔是 15 分钟。

  如果要更改此设置，请在管理员主机上运行以下命令：

  ```
  k0s kubectl -n irp set env deploy/comment -c comment
  OSMP_COMMENT_LOCK_AFTER_DURATION=Nx
  ```

  其中，`N` 表示时间间隔，`x` 表示计量单位：`h`（小时）或 `m`（分钟）。

  其他用户的注释无法修改或删除。输入注释需要“**警报和事故**”功能区中的“**写入**”权限。

将事故分配给分析师

作为工作项，必须将事故分配给 SOC 分析师或用户组以进行检查和可能的调查。如果要将事故自动分配给所选组内的分析师，则可以将事故分配给用户组。有关详情，请参阅“配置警报和事故的自动分配”。

您可以随时更改事故的负责人。

> 事故只能分配给具有读取和修改警报和事故的访问权限的分析师和用户组。

要分配一个或多个事故：

1. 在主菜单中，转到“**监控**” → “**事故**”。
2. 选择您要分配的事故旁边的复选框。

   您只能选择在同一租户中检测到的事故。否则，“**分配给我**和“**分配**”按钮将被禁用。

   或者，您可以从事故详情中将事故分配给分析师或用户组。要打开事故详情，请单击包含事故 ID 的链接。

3. 执行以下操作之一：

- 要将事故分配给您，请单击“**分配给我**”按钮。
- 要将事故分配给其他分析师或用户组：

  a. 单击“**分配**”按钮。

  b. 在打开的“**分配**”窗口中，选择将事故分配给用户或用户组。

  c. 开始输入分析师或用户组的名称，然后从列表中选择负责人。

  d. 单击“**分配**”按钮。

如果要取消分配事故，请选择“**未分配**”。

事故已分配。

您还可以使用行动手册将事故分配给分析师。

更改事故状态

作为工作项，事故状态显示了事故在其生命周期中的当前状态。

仅当您具有读取和修改警报和事故的访问权限时，才能更改您自己或其他分析师的事故状态。

在更改事故状态时，事故和任何未分配的已关联警报都会自动分配给您。

如果手动更改事故状态，行动手册将不会自动启动。您可以手动为此类事故启动行动手册。

事故可以具有以下状态之一：

- **新建**

  当您创建事故或事故自动创建时，事故状态为“*新建*”。您可以将其状态更改为“*进行中*”或“*已关闭*”。将“*新建*”状态更改为“*已关闭*”，且该事故无负责人时，则该事故将被自动分配给您。

- **进行中**

  此状态表示分析师已开始处理该事故，或通过更改“*搁置*”状态恢复工作。您可以将“*进行中*”状态更改为任何其他状态。

- **保持**

  此状态表示分析师暂停了事故的工作。通常，在恢复工作时，您会将“*搁置*”状态更改为“*进行中*”，但您也可以将“*搁置*”状态更改为其他状态。

- **已关闭**

  当预计事故不需要额外工作时，您可以关闭事故。您可以使用以下解决方案之一关闭事故：

  - 真实
  - 误报。
  - 低优先级。

  关闭事故时，关联的警报也会获得“*已关闭*”状态并继承事故的解决方案。如果事故没有负责人，则已关闭的事故会自动分配给您。如果已关闭的事故有未分配的关联警报，则这些警报会自动分配给您。

  “*已关闭*”状态只能更改为“*新建*”。如果您想将已关闭的事故重新设为活动状态，请按以下顺序更改其状态：*已关闭 → 新建 → 进行中*。

要更改一个或多个事故的状态：

1. 在主菜单中，转到“**监控**” → “**事故**”。
2. 执行以下操作之一：
   - 选择要更改其状态的事故旁边的复选框。
   - 单击要更改状态的事故 ID 的关联。

     “**事故详情**”窗口打开。
3. 单击“**更改状态**”按钮。
4. 在“**更改状态**”窗格中，选择要设置的状态。

   选择“*已关闭*”状态时，必须选择一个解决方案。

   如果某个事故至少违反了一项 SLA 指标，则关闭该事故时会显示“**SLA 违规原因**”字段。您需要在此字段中指定 SLA 违规的原因。

   > 如果在事故工作流中编辑“*已关闭*”状态时选中了“**仅允许具有特定权限的用户关闭此事故**”复选框，则您必须拥有主管理员或审批者 XDR 角色才能关闭该事故。

   > 如果将事故状态更改为“*已关闭*”，并且此事故包含未完成的行动手册或响应操作，则所有相关的行动手册和响应操作都将被终止。

5. 单击“**保存**”按钮。

所选事故的状态已被更改。

您还可以使用行动手册更改事故状态。

更改事故优先级

作为工作项，事故具有优先级，该优先级定义了分析师必须调查事故的顺序。您可以手动更改事故优先级。

> 如果您具有读取和修改警报和事故的权限，则可以更改您自己或其他分析师的事故优先级。

事故可以具有以下优先级之一：

- **低**
- **中**（默认值）
- **高**
- **严重**

优先级为“**严重**”的事故是最紧急的事故，必须优先调查。**低**优先级通常意味着事故被放置在积压工作中。您可以定义自己的标准来确定应为哪个事故设置哪个优先级。

要更改事故优先级：

1. 在主菜单中，转到**监控** → **“事故”**。
2. 执行以下操作之一：
   - 选择您要更改其优先级的事故旁边的复选框。
   - 单击事故 ID 以打开要更改优先级的事故的详细信息。
3. 单击“**更改优先级**”按钮。
4. 在“**更改优先级**”窗口中，选择要设置的优先级。
5. 单击“**保存**”按钮。

   所选事故的优先级已被更改。

您也可以使用行动手册更改事故优先级。

对于处于**新建**状态的事故（无论是刚创建的事故，还是从任何其他状态切换到此状态的事故）：

- 您可以编辑优先级，但在向此事故添加警报或从中移除警报时，系统会自动重新评估其优先级。
  优先级将设置为**事故严重性**值。
- 如果您手动更改没有任何关联警报的事故的优先级（事故创建时没有警报，或者所有警报均已从事故中移除），则**事故严重性**将设置为优先级值。
- 重新评估事故优先级时，系统还会自动重新评估事故 SLA。

合并事故

两个或多个事故可能被解释为组织 IT 基础架构中同一问题的指标。如果是这种情况，您可以合并这些事故以将它们作为单个问题进行调查。

合并事故时，您需要从中选择一个目标事故。事故合并后，将在目标事故中调查问题。目标事故的状态不能是“*已关闭*”。其他事故将被合并到目标事故中，合并后，这些事故将获得“*已关闭*”状态和“**已合并**”处理结果。

关联到合并事故的所有警报都会被自动关联到目标事故。由于一个事故的关联警报不能超过 1,000 个，因此应用程序会计算关联到要合并的事故的警报。如果关联警报的总数超过 1,000，则无法合并选定的事故。选择目标事故时，将显示合并后的警报总数量。

> 您无法合并子事故或包含子事故的事故。

要合并事故表中的事故：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 选中要合并到目标事故的事故旁边的复选框。您将在向导的第一步中选择目标事故。
3. 单击“**合并到事故**”按钮。
4. “**合并事故**”向导将打开。
5. 选择目标事故。
6. 单击“**合并**”按钮。

   事故已合并。

要使用事故详情合并事故：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 单击事故 ID 以打开事故详情。此事故将被合并到目标事故中。您将在向导的第一步中选择目标事故。
3. 单击“**合并到事故**”按钮。
   “**合并事故**”向导将打开。
4. 选择目标事故。
5. 单击“**合并**”按钮。

   事故已合并。

将事故导出到文件

您可以将事故导出为 PDF 或 JSON 文件。

要将事故导出为 PDF 文件：

1. 在主菜单中，转到“**监控**” → “**事故**”，调用事故表。
2. 单击要导出的事故的 ID。
3. 单击事故详情窗口中的“**导出为 PDF**”按钮。
   “**打印**”窗口随即打开。
4. 在“**打印**”窗口中，展开“**打印机**”列表并选择“**另存为 PDF**”。
5. 单击“**保存**”按钮以将事故保存为 PDF 文件。
   如果按“**类型**”或“**名称**”字段对事故表进行排序，则导出的 PDF 文件也会使用此排序。

要将所有事故导出为 JSON 文件：

1. 在主菜单中，转到“**监控**” → “**事故**”，调用事故表。
2. 单击表格上方面板中的“**导出**”按钮。
3. 指定文件名并选择要将事故导出至哪个文件夹。
4. 单击“**保存**”以将所有事故保存为 JSON 文件。

从 XDR 事故创建 Managed Detection and Response 事故

如果在OSMP中启用了Managed Detection and Response集成，并且事件的警报满足以下条件，您可以从XDR事件创建Managed Detection and Response：

- 检测源为端点。
- 所选事故必须至少有一个具有相关资产的警报。
- 检测技术为以下任一技术：
  - IOA规则
  - IOC
  - YARA
  - SB（沙盒）
  - AM（反恶意软件引擎）

有关如何在OSMP中启用受管理的检测和响应集成的信息，请参阅以下文章：与卡巴斯基应用程序和解决方案集成。

要将事故导出到 Managed Detection and Response：

1. 在主菜单中，转到“**监控**” → “**事故**”。
2. 在事故表中，单击相应事故的 ID。将显示包含事故详情的窗口。

3. 单击工具栏上的三点图标，然后选择“**创建 MDR 事故**”。

4. 在“**创建 MDR 事故**”面板中，指定事故名称和描述，然后单击“**创建**”。

如果事故创建成功，则会显示相应的消息。现在，您可以在 MDR Web Console 中访问事故。事故链接位于 XDR 事故的“摘要”部分。

调查图

*调查图*是一种可视化分析工具，可显示以下对象之间的关系：

- 事件
- 警报
- 用户
- Observables
- 资产（设备）
- 分段规则

该图显示事故的详细信息：相应的警报及其共同属性。

要打开调查图：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在事故表中，单击相应事故的 ID。
   将显示包含事故详情的窗口。
3. 单击“**在图表上查看**按钮。

要查看图，需要“**警报和事故**”功能区域中的“**写入**”权限。有关详细信息，请参阅以下主题：预定义用户角色。

您可以使用右下角的平移和缩放面板来浏览复杂图。

此外，您可以通过单击撤销图标 (↶) 来取消调查图上的任意操作，并通过单击重做图标 (↷) 来恢复之前撤销的操作。您可以撤消或重做的最大操作次数为 10。

如果您在调查图中执行操作时关闭调查图，您的更改历史记录将被清除。这意味着在您再次打开调查图后，无法撤消和重做在关闭之前执行的操作。

与其他用户同时编辑调查图时，您可以查看用户所做的更改，但无法撤消和重做其操作。

显示模式

调查图有两种显示模式：自动模式（图节点沿时间线显示）和手动模式。默认情况下，应用自动模式。

时间线是屏幕下方的一个刻度，它以图形方式可视化构成事故背景的对象、这些对象出现的时间以及它们出现的整个时期。

刻度的左端代表时间段的开始：事故中包含的所有警报中的最早事件或最早警报。刻度的右端代表时间段的结束：事故中包含的所有警报中的最新事件或最新警报。

在分析完事故中的所有警报后，系统会自动计算整个持续时间。如果在调查图中添加或删除新对象，或者生成进程树时，时间线会自动重新排列。

与刻度上一个分度相对应的区间 (|) 取决于整个时期的持续时间。

计算区间

如果整个时期是……	除法值为……
大于或等于 1 年	1 年
大于或等于 28 天但小于 1 年	1 个月
大于或等于 1 周但小于 28 天	7 天
大于或等于 24 小时但小于 1 周	24 小时
大于或等于 1 小时但小于 24 小时	1 小时
大于或等于 10 分钟但小于 1 小时	5 分钟
从 100 秒到 10 分钟	1 分钟
从 1 秒到 1.6 分钟	10 秒
少于 1 秒	100 毫秒

在自动模式下，调查图上节点的位置取决于相应对象被检测和定义的日期和时间，具体如下：

- 资产位于刻度的开头。
- 警报根据其创建时间放置。
- 事件根据其时间戳放置。
- 可观察对象根据其添加到调查图的方式放置：
  - 通过警报节点添加时，可观察对象根据警报创建时间放置。
  - 通过事件节点添加时，可观察对象根据事件时间戳放置。

  可观察对象的日期和时间与其关联的警报或事件的日期和时间相同。

将鼠标光标悬停在节点上时，将显示该节点的创建日期和时间。

警报或事件在图表上的位置对应于刻度上的列元素 (▮)。当您将鼠标光标悬停在列元素上时，将显示有关事故中同时检测到的警报和事件的信息。

自动模式存在以下限制：

- 您无法移动图表节点。
- 手动创建的链接不会显示。
- 当一个对象有多个链接时（例如，一个可观察对象链接到多个警报），图表上只会显示来自最老对象（创建时间最早的对象）的链接。
- 您无法手动添加与事故自动定义的上下文无关的对象。

  您只能通过已显示对象的上下文菜单添加新对象（与警报相关的事件和可观察对象，或与事件相关的警报和可观察对象）。将模式切换到手动后，在自动模式下添加的对象将放置在与其相关的节点附近。如果对象链接到多个节点，则必须将其放置在时间戳最新的节点附近。

如有需要，您可以通过点击图标在调查图表模式之间切换。在手动模式下，不会显示时间线，您可以移动节点。

> 如果在手动显示模式下添加一个没有时间戳的对象，则在将模式切换到自动模式后，该对象将不会显示。

与图节点交互

您可以使用顶部的工具栏来添加警报和可观察对象。

您可以单击并拖动图节点进行重新排列。

您可以单击图节点以调出上下文菜单。

常见的上下文菜单项：

- **查看详情**

  打开所选节点的详细信息窗口。
- **复制**

  将节点值复制到剪贴板。
- **隐藏**

  从图中移除选定节点。
- **添加注释/编辑评论**

  调用文本字段以输入注释。单击“**发送**”确认更改。单击“**取消**”还原更改。

特定于事件的上下文菜单项：

进程树

仅适用于特定事件类型。为事件生成流程树。事件的蓝色指示表示您可以为其生成流程树。

特定于警报的上下文菜单项：

- **更改状态**

  调用“**更改状态**”面板，以更改警报状态。

- **事件**

  子菜单允许您将事件添加为图节点。

- **可观察对象**

  子菜单允许您将常见的可观察对象添加为图节点。

- **设备**

  子菜单允许您将常见的设备添加为图节点。

  通过使用此子菜单，您也可以查看与设备相关的警报或事故列表。要执行此操作，请在子菜单中，单击“**查看详情**”以打开“**设备详情**”窗口，然后单击“**显示相关**”按钮并选择“**警报**”或“**事故**”。

- **用户**

  子菜单允许您将用户添加为图节点。

特定于可观察对象的上下文菜单项：

- **查找类似事件**

  调用“**威胁搜索**”面板，以显示类似事件。

- **查找类似警报**

  调用“**警报**”面板，以显示类似警报。

- **来自 Kaspersky TIP 的请求状态**

  允许您从 Kaspersky 威胁情报门户 (Kaspersky TIP) 获取有关所选可观察对象的详细信息。有关详细信息，请参阅以下主题：与 Kaspersky 威胁情报门户集成。

- **来自 Kaspersky TIP 的丰富数据**

  使用此按钮可从 Kaspersky TIP 获取有关所选可观察对象的详细信息。有关详细信息，请参阅以下主题：与 Kaspersky 威胁情报门户集成。

特定于分段规则的上下文菜单项：

- **在 KUMA 中编辑**

  在浏览器的新选项卡中打开 KUMA 控制台，该选项卡中将显示规则详细信息。

- **查找类似警报**

  调用“**警报**”面板，以显示类似警报。

您也可以单击警报或事件来添加可观察对象。为此，在打开的上下文菜单中，您需要选择“**可观察对象**”，然后单击该可观察对象。可观察对象将被添加到调查图中。如有需要，您可以从调查图中删除可观察对象。为此，您必须单击可观察对象，然后在打开的上下文菜单中单击“**隐藏**”。

对图元素进行分组

调查图会自动对具有共同属性的警报进行分组。

要取消警报分组：

1. 单击与警报组对应的图元素。
   将显示一个列出警报的表格。
2. 选择要在图上显示的警报。
3. 单击表格工具栏中的“**在图表上显示**”按钮。
   警报将作为图节点添加。
4. 如果要隐藏警报，请单击“**在图表上隐藏**”按钮。

连接图元素

调查图在适用时会自动为新条目创建链接。可以手动添加连接。

要手动添加链接：

1. 单击“**链接节点**”按钮。
   链接点会出现在图节点周围。
2. 从一个节点的链接点单击并拖动到另一个节点的链接点。

手动创建的连接带有颜色指示。

要删除手动创建的连接：

1. 将鼠标悬停在手动创建的连接上。
   链接中间会出现一个十字图标。
2. 单击十字图标即可删除链接。

威胁搜索

您可以通过分析事件来搜索尚未自动检测到的威胁和漏洞。为此，请单击顶部工具栏中的“**威胁搜索**”按钮，或调用图节点的上下文菜单，然后单击“**事件**”或“**查找类似事件**”。将打开“**威胁搜索**”面板。请参阅以下部分了解详情：“威胁搜索”。

导出图

您可以将图保存为 SVG 格式。为此，请单击顶部工具栏中的“**导出**”按钮。

查看和编辑注释

您可以为任何图节点或链接留下注释。

要添加或编辑注释：

1. 单击图元素并选择“**添加注释**”或“**编辑评论**”。
2. 单击“**保存**”保存更改。

   消息 ( ) 图标将出现在图元素旁边。单击消息 ( ) 图标即可显示注释。

要显示所有注释，

请单击顶部工具栏中的“**注释**”按钮。右侧会出现一个包含注释的面板。您可以单击面板中的注释以突出显示图上的相应消息 ( ) 图标。您可以使用面板对整个图表发表评论。

要删除某条注释，

请在图上或带有注释的面板中选择一条注释。单击省略号 (⋮) 图标并选择“**删除**”。

进程树状图

在Kaspersky Next XDR Expert中进行事故调查时，您可以使用进程树状图来可视化事件链。进程树状图显示父进程和子进程，以帮助您更详细地检查事故并跟踪事件的确切顺序。

每个事件最多可以构建和保存五个进程树。进程树状图一旦构建完成，就会自动保存。之后，您可以从**威胁搜索**部分或特定事件详情中访问已保存的进程树状图。

构建进程树状图

您可以从事件或警报详情、调查图表或威胁搜寻部分构建进程树。

若要根据事件详情构建进程树状图：

1. 在主菜单中，前往**监控→ 事故**。
2. 在事故表中，单击相应事故的 ID。

   “**事故详情**”窗口随即显示。
3. 单击“**在图表上查看**按钮。
4. 切换到**手动**显示模式。
5. 点击**威胁搜索**按钮。
6. 在**威胁搜索**面板中，指定所需事件的参数。
7. 单击“**运行查询**”按钮。

8. 点击包含所需事件的行。
9. 点击**构建进程树状图**按钮。

   进程树随即构建。

若要根据调查图表构建进程树状图：

1. 在主菜单中，前往**监控→ 事故**。
2. 在事故表中，单击相应事故的 ID。
   “**事故详情**”窗口随即显示。
3. 单击“**在图表上查看**按钮。
4. 切换到**手动**显示模式。
5. 右击要为其构建进程树状图的事件。
6. 点击**在图表上显示**按钮。

   进程树随即构建。

若要从“威胁搜索”部分中构建进程树：

1. 在主菜单中，转到“**监控**”→“**威胁搜索**”。
2. 指定查询语句，然后点击“**运行查询**”按钮。
3. 在“**事件**”部分，单击包含所需事件的行。
4. 单击“**在图表上查看**按钮。

   进程树随即构建。

删除进程树状图

若要删除进程树状图：

1. 点击**查看保存的树**按钮。
2. 点击进程树状图名称左侧的按钮。
3. 单击“**删除**”按钮。

   进程树被删除，无法恢复。

对进程树状图进行备注

您可以向进程树状图中的特定节点或链接添加备注，并提供该树状图的描述。所有备注都会显示在**注释**部分。

若要添加备注：

1. 右击要添加备注的节点或链接。
2. 输入您的备注。
3. 单击“**保存**”按钮。

要显示所有注释，

请单击顶部工具栏中的“**注释**”按钮。右侧会出现一个包含注释的面板。您可以单击面板中的注释，以突出显示进程树状图上的相应消息（  ）图标。您可以使用面板对整个进程树状图进程备注。

若要编辑或删除备注：

1. 单击备注。
2. 点击省略号（⋮）图标。
3. 选择**编辑**或**删除**。

分段规则

*分段规则*允许您根据创建规则时指定的条件自动将相关警报拆分为不同的事故。

使用分段规则可以根据相关警报创建不同的事故。例如，您可以将具有重要区别特征的多个警报合并成一个单独的事故。

警报只能与属于同一租户的事故相关联。

分段规则根据指定的优先级触发。在分段规则表中，规则的位置越靠上，优先级就越高。如果要更改分段规则优先级，请单击规则名称并拖放规则。

建议您同时使用分段规则与聚合规则，以定义用于创建事故的更精确的规则。

要创建分段规则：

1. 在主菜单中，前往**监控→资源和服务→分段规则**。
   将打开分段规则表。
2. 单击“**创建**”按钮。
   将显示“**创建分段规则**”窗口。
3. 输入分段规则设置。

   - **规则状态**
     启用或禁用该规则。默认情况下，该规则处于禁用状态。
   - **租户所有者**
     指定您希望分段规则所属的租户。

- **名称**

  规则的唯一名称。

- **事故中的警报**

  单个事故中的最大和最小警报数量。指定1到200之间的值。默认值为：最小值1，最大值200。最小数量必须小于或等于最大数量。如果警报数量未达到最小值，则不会创建事故。最大数量必须大于或等于最小数量。如果警报数量超过最大值，则会创建另一个事故。

- **搜索间隔**

  用于选择警报和事故的时间间隔。您可以指定以天或小时为单位的值。默认值是30天。

- **继承者**

  可选设置。继承该规则的租户。默认情况下，规则由所有子租户沿层级结构从父租户继承。您可以通过选择 **仅限当前租户** 选项来禁用继承，或者单击 **特定租户**，然后从下拉列表中选择必须继承该规则的租户。

  > 您只能指定您拥有以下 XDR 角色的租户：主管理员、租户管理员、SOC 管理员。
  > 只能从父租户编辑继承设置、更改规则优先级、复制或删除继承的规则。可以从父租户和子租户更改继承规则的状态。

  在子租户中，继承的规则的优先级始终高于在该子租户中创建的规则的优先级。此外，继承的规则会保持其在父租户中的相同优先级顺序。

  复制继承的规则时，会连同其作用域一起复制。将继承的规则复制到另一个租户时，不会复制规则作用域。

- **组**

  一个 jq 表达式，用于定义用于将警报分配给事故的字符串标识符数组。

  如有必要，您可以从另一个分段规则复制“**组**”部分的 jq 表达式。为此，请单击“**从另一条规则复制**”按钮。

  例如：`if any(.Observables[]? | select(.Type | ascii_downcase == "username") | .Value; startswith("adm_")) then ["Brute force admin"] else ["Brute force not admin"] end`

- **事故名称**

  jq 表达式，用于定义根据此细分规则所创建事故的命名模板。默认情况下，指定以下表达式：`"\(.Rules[]?.Name), \(.SourceCreatedAt)"`

  如有必要，您可以从另一个分段规则复制“**事故名称**”部分的 jq 表达式。为此，请单击“**从另一条规则复制**”按钮。

  例如：`if any(.Observables[]? | select(.Type | ascii_downcase == "username") | .Value; startswith("adm_")) then "Brute force admin" else "Brute force not admin" end`

- **触发器**

  一个 jq 表达式，用于定义将警报纳入事故的条件。

  如有必要，您可以从另一个分段规则复制“**触发器**”部分的 jq 表达式。为此，请单击“**从另一条规则复制**”按钮。

  例如：`any(.Rules[]?; .ID == "123")`

- **描述**

  可选设置。规则描述。

4. 单击“**创建**”按钮。

分段规则将保存并显示在分段规则表中。如有必要，您可以通过单击表中的名称来编辑规则设置。

您可以在 jq 表达式中使用 `inSubnet` 逻辑运算符，以测试左操作数（IP 地址）是否位于右操作数（子网）内。

例如：`any(.Observables[]? | select(.Type == "ip") | .Value // empty; inSubnet("11.11.11.1/11"))`

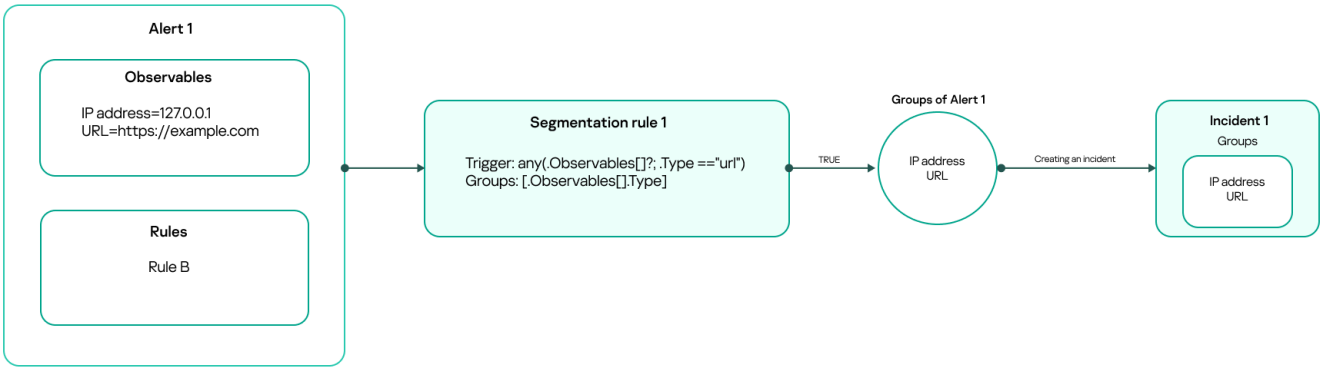
以下预定义的分段规则可用：

- 连接至现有事故：相同的MD5文件哈希值
- 连接至现有事故：同一主机资产
- 连接至现有事故：相同的IOA、IOC或Yara规则
- 创建事故：相同的MD5文件哈希值
- 创建事故：同一主机资产
- 创建事故：相同的IOA、IOC或Yara规则

预定义的规则会自动应用于租户。

默认情况下，会在所有租户上创建预定义的规则，并且这些规则的继承会被禁用。如果您为父租户中的规则启用继承，子租户中的相应规则将被父租户设置覆盖。如果您禁用继承，来自父租户的规则将被删除。但是，由于租户不能没有预定义的规则，因此会在子租户上自动创建一个新的本地预定义规则。

创建警报时，所有活动的分段规则都会根据其优先级进行检查。触发第一个规则后，将为警报形成一个字符串标识符数组，并开始搜索将与警报关联的事故。

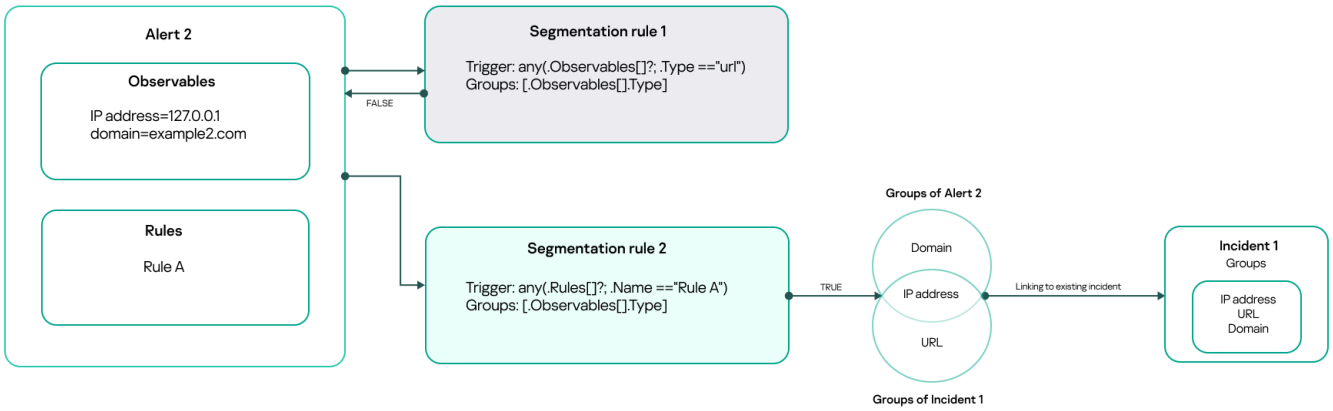


在触发第一个分段规则后创建新事故

如果在**触发器部分**中指定的jq表达式返回`true`，则规则会被触发。

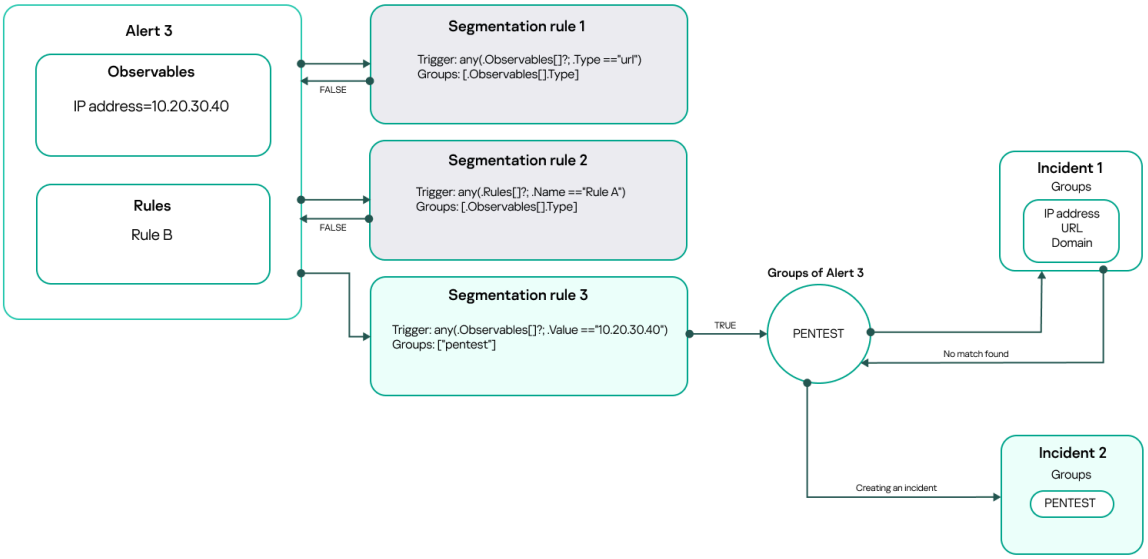
警报无法关联到手动创建的事故。

事故还具有一个字符串标识符数组，其中包括已关联到此事故的警报数组。如果触发分段规则的警报在其数组中至少有一个元素与事故数组中的任意元素匹配，则将该警报关联到该事故。最终，此警报的数组将添加到事故数组中。



检测到匹配元素后将警报关联到现有事故

如果有多个事故满足条件，则警报关联到最近更新的事故。如果数组中不存在具有匹配元素的事故，则将创建一个新事故。



根据前两个分段规则未找到匹配元素后创建新事故

如果事故是新事故，其数组为空。关联警报后，新事故将从警报中获取字符串标识符数组。

分段规则。示例

从“聚合规则”部分配置聚合规则。本主题中的示例部分。

下表说明了如何将所有渗透测试警报合并成单个事故。

分段规则

属性	值
触发	.AggregationID == "Pentest"
组	["渗透测试"]
事故名称	"渗透测试事故"

聚合和分段规则。示例

下表说明了如何根据用户名前缀，将两个事故中具有相同规则 ID 的警报合并。

聚合规则

属性	值	描述
触发	any(.Rules[]?; .ID == "123")	搜索规则 ID 为 "123"的警报。
聚合 ID	if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "rule123_DestinationUserName_adm" else "rule123_DestinationUserName_not_adm" end	搜索带有"adm_" 前缀的用户名。
警报名称	if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "Rule123 admin" else "Rule123 not admin" end	根据用户名前缀设置警报名称。

分段规则

属性	值
触发	.AggregationID | startswith("rule123_DestinationUserName")
组	[.AggregationID]
事故名称	.Name

将分段规则复制到另一个租户

您可以将现有的分段规则复制到另一个租户。

如果构建了OSMP 实例层次结构，则只能在一个实例内复制规则。

要复制分段规则：

1. 在主菜单中，前往**监控→资源和服务→分段规则**。
   将打开分段规则表。
2. 选择要复制的分段规则，然后单击"**复制到租户**"。
3. 选择一个或多个目标租户，然后单击"**复制**"。
4. 如果目标租户包含同名的分段规则，则会出现"**覆盖或重命名分段规则?** "窗口。
   单击"**覆盖**"可删除之前为目标租户创建的规则，并将其替换为要复制的规则。
   单击"**复制并重命名**"可保留先前创建的规则，并复制指定的规则，在其标题末尾附加`(copy)`。
   如果您复制继承的规则，而目标租户已存在同名规则，则不会覆盖此规则。您必须更改正在复制的规则的名称。此外，复制继承的规则时会复制其状态，但不会复制其作用域。

单击关闭 (✕) 按钮时，窗口会关闭，并且不会复制名称与目标租户中的分段规则相同的分段规则。但是，如果在步骤 2 中您还选择了目标租户中不存在的分段规则，则会复制这些规则。

分段规则将复制到其他一个或多个租户。

管理服务水平协议 (SLA)

Kaspersky Next XDR Expert 可用于配置服务水平协议 (SLA) 条目，这些条目定义处理事故的时间限制。

您可以为事故工作流和优先级的组合定义 SLA 条目。

“**事故**”表和事故详情显示 SLA 条目的剩余时间。

您可以配置电子邮件通知模板，其中包含“**事故 SLA 即将到期**”和“**事故 SLA 已更改**”类型。

当事故状态恢复时重新开始计算 SLA 指标

当某一事故被认定为已响应完毕时，该事故的 SLA 指标便停止计算。默认情况下，恢复事故状态会重新启动 SLA 指标。

要在事故状态恢复时防止重新启动 SLA 指标：

1. 确保在管理员主机上安装了 kubectl 实用程序。
2. 执行以下命令：

   ```
   kubectl -n irp set env deploy/incident
   OSMP_INCIDENT_SLA_DISABLE_RESTART_CALCULATION_ON_START_TRIGGER=true
   ```

3. 重新启动事故服务。

创建服务水平协议 (SLA) 条目

创建 SLA 条目需要以下 XDR 角色之一：主管理员、租户管理员、SOC 管理员。

要创建 SLA 条目：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   这将打开“租户属性”窗口。
3. 单击“**设置**”选项卡，然后单击“**事故管理**”。
4. 选择“**SLA**”选项卡，然后单击“**创建**”按钮。

5. 在打开的“**创建 SLA**”窗格中，配置以下设置：

   - **SLA 名称** – 条目的显示名称。
   - **优先级** – 应用条目的事故优先级。
   - **工作流** – 应用条目的事故工作流。

     您只能将单个条目分配给“**工作流**”和“**优先级**”的组合。您不能选择在具有相同优先级的其他 SLA 中使用的事故工作流。
   - **分类时间** – 接受事故的时间限制，以天、小时和分钟为单位。当事故从一种状态转换为另一种状态时，即认为该事故已被接受。

     要定义此转换，请选择“**从状态**”和“**至状态**”值。
   - **响应时间** – 对事故进行初始响应的时间限制，以天、小时和分钟为单位。

     选择停止条件：

     - 如果您希望在应用响应操作后事故被视为已响应，请选择“**首次响应操作**”。之后，在“**从状态**”字段中选择一个或多个值。
     - 如果您希望在事故更改为另一个状态后事故被视为已响应，请选择“**当状态变为**”。之后，在“**从状态**”和“**至状态**”字段中选择一个或多个值。
   - **解决时间** – 解决事故的时间限制，以天、小时和分钟为单位。当事故从一种状态变为另一种状态时，即认为事故已解决。

     要定义此转换，请选择“**从状态**”和“**至状态**”值。

6. 单击“**创建**”按钮。

   创建的 SLA 条目显示在表中。

删除服务水平协议 (SLA) 条目

删除 SLA 条目需要以下 XDR 角色之一：主管理员、租户管理员、 SOC 管理员。

要删除 SLA 条目：

1. 在主菜单中，转到“**设置**” → “**租户**”。

   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。

   这将打开“租户属性”窗口。
3. 单击“**设置**”选项卡，然后单击“**事故管理**”。
4. 选择“**删除**”选项卡。
5. 选中您要删除的 SLA 条目旁边的复选框。
6. 单击“**删除**”按钮。
7. 在打开的确认窗口中，单击“**删除**”。

删除某一项 SLA 条目时，对于与该条目中“**事故类型**”和“**优先级**”相匹配的事故，其时间限制将不再进行计算。

管理事故类型

Kaspersky Next XDR Expert 允许您根据事故类型来管理事故并自定义事故处理流程。

事故类型是一组属性，您可以为其配置不同流程，例如，为事故类型分配工作流、配置触发器或配置行动手册算法。

您可以创建事故类型，或使用可以自定义的预定义事故类型。

事故类型可以是活动状态，也可以是非活动状态。如果事故类型处于活动状态，您将能够在事故详细信息窗口中选择此类型。

标记为默认类型的事故类型会自动分配给所有新事故。您无法将默认事故类型切换为非活动状态。

> “**通用**”事故类型设置为默认类型。您可以编辑此设置。

> 您只能在一个租户中创建一个默认事故类型。

查看事故类型表

要查看事故类型表：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”。
   将显示“**类型**”选项卡和事故类型表。
4. 如果要配置事故类型表，请执行以下操作之一：
   - 单击过滤图标（ ），然后在调用的菜单中指定并应用过滤条件。
   - 要隐藏或显示某一列，请单击设置图标（ ），然后选择必要的列。

事故类型表包含以下信息：

- **名称**。自定义或预定义事故类型的名称。

该表包含以下预定义事故类型：

- 普通

  > 默认情况下，此类型在“**默认值**”列中的取值为“**是**”。

- 信息收集
- 入侵
- 未经授权访问
- 恶意软件攻击
- 网络钓鱼
- 可用性
- 内部威胁
- 数据泄露
- 配置错误
- 供应链攻击
- Web 应用程序攻击
- 漏洞利用

- **活动类型**。如果事故类型处于活动状态，您将能够在事故详细信息窗口中选择此类型。
- **默认**。创建事故时，将自动为其分配默认类型。可能值：
  - True
  - False
- **工作流**。事故工作流。
- **租户**。事故类型所属租户的名称。
- **创建类型**。事故类型的创建方式。可能值：
  - **自定义**
  - **预定义**
- ID。自定义或预定义事故类型的唯一标识符。默认情况下，此列处于隐藏状态。
- **描述**。事故类型描述。默认情况下，此列处于隐藏状态。

如有必要，您可以创建新的事故类型，以及编辑和删除预定义及自定义事故类型。

创建事故类型

要创建事故类型：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”，然后选择“**类型**”选项卡。
4. 单击“**创建**”按钮。
   “**创建事故类型**”窗口随即打开。
5. 如果希望新事故类型处于活动状态，请启用“**活动类型**”切换开关。
6. 在“**名称**”字段中，输入新事故类型的名称。
7. 如果要默认为所有新事故分配此类型，请选中“**设置为默认**”复选框。

   > 租户中只能有一个默认事故类型。这意味着如果租户已经有默认事故类型，则选中此复选框后，此类型将不再是默认类型。

8. 在“**工作流**”字段中，选择事故工作流。
9. 如有必要，在“**描述**”字段中输入事故类型描述或注释。
10. 单击“**创建**”按钮。

    新事故类型将显示在事故类型表中。

编辑事故类型

如有必要，您可以编辑事故类型。

要编辑事故类型：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”。
   将显示“**类型**”选项卡和事故类型表。

4. 单击您要编辑的事故类型名称。
   将打开“**编辑事故类型**”窗口。
5. 进行编辑，然后单击“**保存**”。有关可以编辑的事故类型属性的更多详细信息，请参阅“创建事故类型”。

事故类型属性已编辑并保存。

删除事故类型

如果要删除行动手册中使用的事故类型，则必须从行动手册触发器和/或算法中删除此事故类型以避免产生错误。

在以下情况下，无法删除事故类型：

- 在创建此事故类型的租户中，事故类型已设置为默认类型。
  尝试删除此事故类型时，系统会提示您设置新的默认事故类型。在打开的窗口中，您必须从列表中选择事故类型。
- 在子租户中，事故类型已设置为默认类型。
- 当前租户或子租户包含您要删除的类型的事故。
  在删除这种类型之前，您必须为该事故指定另一种类型。
- 已针对该事故类型定义了服务级别协议 (SLA) 规则。

要删除事故类型：

1. 在主应用程序窗口中，转到**设置** → **租户**部分。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”。
   将显示“**类型**”选项卡和事故类型表。
4. 执行以下操作之一：
   - 选择要删除的事故类型，然后单击“**删除**”。
   - 单击要删除的事故类型的名称，然后在“**编辑事故类型**”窗口中，单击“**删除**”。
5. 在确认对话框中，单击“**删除**”。

事故类型已删除。

管理事故工作流

您可以通过 Kaspersky Next XDR Expert 来配置灵活的事故工作流。Kaspersky Next XDR Expert 还会在可视化编辑器中显示工作流。

事故工作流是事故在其生命周期中经历的一系列状态和转换。“*状态*”是事故处理流程中的一个步骤。“*转换*”可帮助事故在不同状态之间切换。转换是一种关联，可用于配置从一个事故状态转换到另一个事故状态并返回。如有必要，您可以将转换用作单向关联。

您可以创建事故工作流，或使用可以自定义的预定义工作流。

您还可以为事故类型分配工作流。这将帮助您以最便捷的方式管理事故生命周期。

查看事故工作流表

要查看事故工作流表：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击目标租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”，然后选择“**工作流**”选项卡。
   要隐藏或显示某一列，请单击设置图标 (⚙)，然后选择必要的列。

将显示事故工作流表。

事故工作流表包含以下信息：

- **名称**。自定义或预定义事故工作流的名称。
- **链接的类型**。关联的事故类型数量。
- **租户名称**。事故工作流所属的租户的名称。
- **创建类型**。事故工作流的创建方式。可能值：
  - **自定义**。
  - **预定义**。
- **工作流 ID**。事故工作流的唯一标识符。默认情况下，此列处于隐藏状态。
- **描述**。事故工作流描述。默认情况下，此列处于隐藏状态。

预定义事故工作流

Kaspersky Next XDR Expert 支持您使用预定义事故工作流来管理事故。在事故工作流表中，此类工作流名为“**标准**”。在“**创建类型**”列中，这些工作流标记为“**预定义**”。

如有必要，您可以编辑预定义工作流，对其进行自定义。

下表显示了预定义工作流的状态，以及事故切换为这些状态的原因。

状态	原因
新建	• 新事故已创建（手动或自动）。 • 事故状态已从以下状态之一更改为“**新建**”：“**进行中**”、“**搁置中**”，或“**已关闭**”。
进行中	用户手动将事故状态从“**新建**”或“**搁置中**”更改为“**进行中**”。
搁置中	用户手动将事故状态从“**进行中**”更改为“**搁置中**”。
已关闭	• 用户关闭了该事故。 • 用户将该事故关联到另一个尚未关闭的类似事故。

创建事故工作流

事故工作流可用于管理事故生命周期。

要创建事故工作流：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”，然后选择“**工作流**”选项卡。
4. 单击“**创建**”按钮。
   这将打开“**创建工作流**”窗口。

   > 默认情况下，每个事故工作流都包含预定义状态“**新建**”和“**已关闭**”。您无法删除或编辑这些状态。

5. 在“**名称**”字段中，指定新工作流的名称。
6. 如有必要，在“**描述**”字段中输入工作流描述或注释。
7. 要添加新状态，在“**工作流**”部分中单击“**添加状态**”。
8. 在打开的窗口，指定以下设置：
   a. 在“**状态名称**”字段中，输入新状态的名称。
   b. 在“**类别**”字段中，选择以下状态类别之一：
      - **新建**
      - **进行中**
      - **已解决**
      - **已关闭**

      类别决定状态图标的颜色。
   c. 在“**传入转换**”字段中，选择一个或多个传入状态。
      如果要配置从所有状态到传入状态的转换，请选择“**允许所有状态转换为此状态**”选项。

d. 在“**传出转换**”字段中，选择一个或多个传出状态。
如果要配置从传出状态到所有状态的转换，请选择“**允许此状态转换为所有状态**”选项

e. 单击**添加**。
可视化工作流显示在“**创建工作流**”窗口中
如有必要，重复步骤 7-8e 以添加新状态。

9. 在“**创建工作流**”窗口中，单击“**保存**”按钮。

新的事故工作流显示在表中。

编辑事故工作流和状态

您可以编辑工作流属性以及工作流的状态和转换。

要编辑事故工作流：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”，然后选择“**工作流**”选项卡。
4. 单击要编辑的工作流名称。
这将打开 **编辑工作流** 窗口。
5. 编辑工作流属性。有关您可以编辑的工作流属性的更多详细信息，请参阅“创建事故工作流”。

工作流的属性将被修改并保存。

要编辑事故工作流的状态：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”，然后选择“**工作流**”选项卡。
4. 单击要编辑的工作流名称。
这将打开 **编辑工作流** 窗口。
5. 单击要编辑的状态名称。
将打开“**编辑状态**”窗口。
6. 编辑状态和转换设置。有关您可以编辑的状态设置的更多详细信息，请参阅“创建事故工作流”。
如有必要，您可以通过单击“**删除**”按钮来删除状态。

您无法编辑以下预定义状态的名称和类别：“**新建**”和“**已关闭**”状态。您也无法删除这些预定义状态。

如果状态已分配给事故，则此状态将无法删除。

7. 单击“**保存**”按钮。

工作流状态将被修改和保存。

删除事故工作流

如果存在属于父租户或子租户的已关联的事故类型，则无法删除事故工作流。在这种情况下，您需要为关联的事故类型分配不同的工作流，然后再次尝试删除事故工作流。

如果要删除行动手册中使用的工作流，请在删除之前编辑行动手册的触发器和/或算法，以避免出现错误。

要删除事故工作流：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击目标租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**事故管理**”，然后选择“**工作流**”选项卡。
4. 在工作流列表中，选择要删除的工作流，然后单击“**删除**”。
5. 在确认对话框中，单击“**删除**”。

事故工作流将被删除。

管理事故工作量

Kaspersky Next XDR Expert 可以跟踪与处理事故相关的工作量。这有助于计算分析师在事故分析和响应上花费的时间，评估分析师的工作量，并有效分配劳动力资源。

分析师可以手动添加在事故相关工作上所投入的工作量详情，包括花费的时间，以及必要时的工作量类别。

可以通过 API 查看、添加、编辑或删除工作量类别。要管理工作量类别，您必须具有以下 XDR 角色之一：主管理员、租户管理员、SOC 管理员。

要管理事故工作量，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、1级分析师、2级分析师、SOC 经理、审批人。

Kaspersky Next XDR Expert 还支持您按分析师或小组来生成并导出工作量报告以供进一步分析。

添加事故工作量

您可以将事故相关工作量添加到事故详情的“**工作量日志**”部分。这有助于评估分析师处理事故所花费的时间、规划其工作量以及计算工资成本。

要添加事故工作量：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在事故表中，单击相应事故的 ID。
   将显示包含事故详情的窗口。
3. 转到“**工作量日志**”选项卡，然后单击“**添加**”按钮。
   将打开“**增加工作量**”窗格。
4. 如有必要，请在“**类别**”下拉列表中，选择工作量类别。
5. 在“**小时**”和“**分钟**”字段中，指定您花在事故相关工作上的时间。

   > “**分钟**”字段的最大值为 59。

6. 单击**添加**。

将添加您的事故相关工作量。

编辑事故工作量

您可以编辑之前添加的工作量。

> 您无法编辑其他分析师添加的工作量。

要编辑事故工作量：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在事故表中，单击相应事故的 ID。
   将显示包含事故详情的窗口。
3. 转到“**工作量日志**”选项卡。
4. 在“**日期**”列中，单击包含待编辑工作量日期和时间的链接。
   “**编辑工作量**”窗格随即打开。
5. 编辑工作量属性，然后单击“**保存**”按钮。

工作量属性将被修改并保存。

删除事故工作量

您可以删除之前添加的工作量。

> 您无法删除其他分析师添加的工作量。

要删除事故的工作量：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在事故表中，单击相应事故的 ID。
   将显示包含事故详情的窗口。
3. 转到“**工作量日志**”选项卡。
4. 在工作量列表中，选中要删除的工作量旁边的复选框，然后单击“**删除**”按钮。

   工作量将被删除。

生成和导出事故报告

您可以生成和导出有关分析师处理事故所花费的工作量以及事故符合 SLA 指标的报告。报告以 CSV 格式保存。

要生成事故报告，您必须具有：

- 访问事故所属租户的权限。
- 以下 XDR 角色之一：主管理员、SOC 管理员、租户管理员、初级分析师、一级分析师、二级分析师、SOC 经理、与 NCIRCC 交互、审批人、审计员。

要生成和导出报告：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。
2. 在工具栏中，单击“**导出**”按钮，然后在下拉菜单中选择以下选项之一：
   - **工作量报告**，用于导出有关分析师处理事故所花费的工作量的报告。
   - **事故指标报告**，用于导出有关事故符合 SLA 指标的报告。
3. 在打开的右侧窗格中，指定要在报告中显示的数据所对应的时间段。为此，请在“**从**”和“**到**”字段中选择日期和时间。
   默认情况下，“**从**”字段中选定当前月份的第一天，时间设置为 00:00。在“**到**”字段中，选择当前日期，并将时间设置为 23:59。

4. 如有必要，请根据您在步骤 3 中选择的报告类型指定其他设置：

   - 对于**工作量报告**：
     - 如果您希望报告包含需要您指定的用户投入工作量的事故，请选择分析师或用户组。
     - 如果您希望工作量报告包含这些详细信息，请启用“**包括事故 ID 和工作量类别详细信息**”切换开关。
       默认情况下，此切换开关处于关闭状态。
   - 对于**事故指标报告**：
     - 选择要包含在报告中的事故的优先级。可能值：**低**、**中**、**高**、**严重**。
     - 如果您希望仅在报告中包含违反 SLA 的事故，请启用“**仅导出违反 SLA 的事故**”切换开关。
       如果事故至少有一个已过期的 SLA 条目，则该事故将包含在报告中。当 SLA 条目中至少一个时间限制（**分类时间**、**响应所花的时间** 或 **解决时间**）小于 0 时，该 SLA 条目则被视为过期。

5. 单击“**导出**”按钮。

窗格关闭，报告随即生成并下载到您的计算机中。

配置警报和事故的保留期

通过 Kaspersky Next XDR Expert，您可以根据需要缩短或延长警报和事故的保留期。默认情况下，警报和事故的保留期为 360 天。

子租户从父租户复制警报和事故的保留期。如有必要，您可以编辑子租户的保留期。

要配置警报或事故保留期：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**警报和事故**”。
4. 在“**保留期**”部分中，在以下一个或两个字段中指定新的保留期：
   - **警报保留期(天)**
   - **事故保留期(天)**

   最小值是 1。
5. 单击“**保存**”按钮。

新的保留期已配置。

无论配置的保留期如何，如果已过期警报关联至未过期事故，则只有在已关联事故的保留期到期后，才会删除警报。如果已过期事故包含未过期的已关联警报，则只有在已关联警报的保留期到期后，才会删除事故。

如果已过期父事故包含未过期的子事故，则只有在最后一个子事故的保留期到期后，才会删除父事故。

配置警报和事故的自动分配

Kaspersky Next XDR Expert 可用于配置警报、事故和子事故自动分配给分析师。如果启用自动分配，已手动或使用行动手册分配给用户组的警报或事故将自动分配给该组中的分析师。被分配了警报或事故的分析师必须满足以下条件：

- 工作状态为“**可用**”。
- 组中活动警报和事故最少。
- 用户会话持续时间等于或长于配置的最小值。

如果多位分析师符合自动分配的条件，应用程序会随机将警报或事故分配给其中一位分析师。

如果组中没有用户被分配警报或事故，或者没有符合条件的用户（例如，所有用户的状态均为“**忙碌**”），则警报或事故仍将分配给该组。

自动分配仅在警报或事故分配给用户组时运行一次。如果应用程序在首次尝试期间无法将警报或事故分配给用户，则警报或事故仍将分配给该组。不会再尝试分配警报或事故。

要配置自动分配，您必须拥有以下 XDR 角色之一：主管理员、SOC 管理员、租户管理员。

要配置警报和事故的自动分配：

1. 在主菜单中，转到“**设置**” → “**租户**”。
2. 单击目标租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡上，单击“**警报和事故**”。
4. 在“**自动分配**”部分中，为以下一个或多个选项启用自动分配：
   - **警报**
   - **事故**
   - **子事故**

5. 在“**用户活动的最短时长(分钟)**”字段中，指定分析师用户会话的最短持续时间。

   一旦达到此值，分析师就会被列入有资格获得警报和/或事故分配的用户列表中。默认情况下，该值为 5。

6. 单击“**应用**”按钮。

自动分配已配置。

将警报或事故自动分配给用户后，分配信息将显示在“**历史记录**”部分下的警报或事故详情中。自动分配警报或事故后，日志记录会将“**系统**”标注为作者。

如果自动分配失败，错误消息将显示在警报或事故详情的“**历史记录**”部分下。

查看资产详情

资产详情是一个窗口，其中包含与资产相关的所有信息。

您可以通过以下方式之一查看资产详情：

- 从警报详情中查看
- 从事故详情中查看
- 从事件详情中查看（如果事件包含资产）
- 从调查图表

要查看资产详情：

1. 在主菜单中，转到“**监控**”，然后执行以下操作之一：

   - 如果要从警报详情中查看资产详情，请单击“**警报**”，然后在“ID”列中，单击包含要查看其详情的资产的警报 ID。在打开的窗口中，转到“**资产**”选项卡。
   - 如果要从事故详情中查看资产详情，请单击“**事故**”，然后在“ID”列中，单击包含要查看其详情的资产的事故 ID。在打开的窗口中，转到“**资产**”选项卡。
   - 如果要从事件详情中查看资产详情，请单击“**威胁搜索**”，然后单击包含要查看其详情的资产的事件。
   - 如果要从调查图中查看资产详情，请单击“**事故**”，然后在“ID”列中，单击包含要查看其详情的资产的事故 ID。在打开的窗口中，单击“**在图表上查看**”按钮。单击警报节点，然后在上下文菜单中，选择“**设备**”或“**用户**”。

2. 执行以下操作之一：

   - 单击所需资产的名称，然后在下拉列表中选择“**查看属性**”。
   - 在调查图上，单击资产节点，然后在上下文菜单中选择“**查看详情**”。

将显示资产详情窗口。

在“资产详情”窗口中，您可以在**常规**和**防护规则**选项卡之间切换。

“常规”选项卡

常规选项卡包含以下部分：

- **资产属性** — 有关资产的信息，例如资产名称、ID 和资产所属的租户。

  如果 KUMA 中的当前授权许可包含 AI 模块，则会显示“**人工智能分数**”字段，该字段会显示资产分数。该字段展示资产上非典型活动的程度，取值范围为 0 到 1。其中，0 代表行为符合预期，1代表该资产在基础架构内的行为完全不符合预期。如果带有内置代理的 Kaspersky Endpoint Security 已安装在资产（设备上），则会显示“**隔离状态**”字段。您可以通过点击状态旁边的**设置**链接来查看和更改设备的网络隔离状态。

- **类别** — 有关与资产关联的类别的信息。

- **自定义字段** — 您在 KUMA 控制台中创建的资产字段。

- **已安装的软件** — 有关资产上安装的软件的信息。

  您可以使用“**搜索**”字段快速查找所需的应用程序。开始输入以下任一信息后，即会显示所需的应用程序：应用程序名称、版本、供应商或安装日期。

- **KSC：漏洞** — 资产漏洞（如有）。此信息适用于从 Kaspersky Security Center 导入的资产。

- **卡巴斯基应用程序** — 有关资产上安装的卡巴斯基应用程序的信息。

- **设备保护状态** — 资产状态；可能值包括：*正常*、*严重*、*警告*。此信息适用于从 Kaspersky Security Center 导入的资产。

- **KICS for Networks: 资产参数** — 有关资产的信息。此信息从 KICS for Networks 导入。

- **KICS for Networks：漏洞** — 资产的漏洞（如有）。此信息适用于从 KICS for Networks 导入的资产。

您可以单击其名称旁边的 V 形图标 (>)。

在工具栏中，您可以执行以下操作：

- 通过点击**编辑**按钮来编辑资产详细信息。

- 点击**响应**按钮，然后从下拉列表中选择响应操作，即可执行响应操作。

- 通过点击**关联至类别**按钮来为资产分配类别。

- 点击**响应历史**按钮，然后从下拉列表中选择要跳转到的位置，即可跳转到**威胁搜索**部分、**参看于**部分、相关警报列表或相关事故列表。

  响应历史部分、 **威胁搜索**部分中的事件、警报或事故将根据您跳转到的资产进行筛选。

- 使用远程终端连接到资产。为此，请点击**打开远程终端**按钮。

- 通过点击**导出到 CSV**按钮，将有关资产的信息导出为CSV文件。

“防护规则”选项卡

该选项卡包含应用于设备的防护规则表。

该表显示以下规则进程的状态之一： **已应用** 、 **正在应用**或**错误**。

若要查看防护规则列表，您必须具有以下XDR角色之一：主管理员、租户管理员、SOC管理员、SOC经理、一级分析师、二级分析师、初级分析师、批准人、审计员。

该表的列与您从资源和服务部分打开的表相同。

您可以查看和编辑防护规则设置。为此，请点击**名称**列中带有规则名称的链接，打开防护规则详细信息。打开**编辑防护规则**面板，并选中了**详细信息**选项卡。您可以编辑阻止规则设置。

此外，您可以单击**前往威胁搜索**按钮，以查看触发防护规则时获得的事件。在**更改日志**选项卡上，您可以查看应用于防护规则的所有更改。

要打开防御规则详细信息，您必须具有以下XDR角色之一：主管理员、租户管理员、一级分析师、二级分析师。
如果防御规则属于您没有权限的父租户，则您无法编辑该防御规则。

通过远程终端进行调查和响应

Kaspersky Next XDR Expert 允许您使用远程终端连接到资产。连接成功后，您可以实时与操作系统 Shell 进行交互，以调查警报和事故、执行诊断并响应威胁。

通过远程终端，您可以使用资产上安装的操作系统支持的命令来管理资产。

通过使用远程终端，您可以同时连接到多个资产。在这种情况下，OSMP 控制台中的每个资产都会打开一个单独的远程终端窗口。

如果满足以下条件，您可以使用远程终端连接到该资产：

- 您已在Kaspersky Next XDR Expert授权许可下激活了该应用程序。
- 您拥有以下 XDR 角色之一：主管理员、1 级分析师、2 级分析师。
- 资产上已安装 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows。

您不能使用远程终端连接到您访问 OSMP 控制台的资产。

如果资产遭到泄露，通过远程终端管理该资产可能会导致恶意代码的意外执行。仅使用远程终端连接到您信任的设备。

管理远程终端连接

您可以使用远程终端实时调查资产上的威胁并做出响应。

您可以通过以下方式访问远程终端：

- 从事故详情。
- 从警报详情。
- 从资产详情。
- 从资产表（**检测和响应**选项卡）中。

使用远程终端连接到资产

要连接到资产：

1. 在主菜单中，执行以下操作之一：
   - 要从事故详情访问远程终端，请前往**监控**，然后单击**事故**。在事故表中，单击所需事故的 ID，然后在打开的窗口中，转到**资产**选项卡。
   - 要从警报详情访问远程终端，请前往**监控**，然后单击**警报**。在警报表中，单击所需警报的 ID，然后在打开的窗口中，转到**资产**选项卡。
   - 要从资产详情访问远程终端，请前往**资产管理**，然后单击**资产(设备)**。选择 **检测和响应** 选项卡，然后在资产表中，单击所需资产的名称。在上下文菜单中，选择**详细信息**。在打开的资产详细信息窗格中，单击省略号（⋮）图标。
   - 要从资产表访问远程终端，请前往**资产管理**，然后单击**资产(设备)**。选择 **检测和响应** 选项卡，然后在资产表中，选择所需的资产。
2. 点击**打开远程终端**按钮。
3. 如果要对资产执行响应操作，请执行以下步骤：
   a. 在打开的**远程终端**窗口中，执行以下其中一项操作：
      - 对于运行Windows的设备：

        ```
        response.exe
        ```

      - 对于运行Linux的设备：

        ```
        responser
        ```

b. 按下“**Enter**”。

c. 点击**复制密码**链接复制密码，然后将密码粘贴到远程终端中。

与资产建立远程会话后，您可以调查威胁并在需要时执行响应操作。

远程终端上执行的所有操作都会被记录。

如果超过 10 分钟没有任何活动，则与资产的连接将被终止。

查看远程终端中的活动连接

使用远程终端，您可以同时连接和操作多个资产。如果您没有手动结束与某个资产的会话，或者会话没有因不活动而过期，即使您导航到 OSMP Console 的其他部分，该会话仍保持活动。

要查看活动的远程终端会话，

在 OSMP Console 的右上角，单击“**N 个连接**”。

“**远程终端**”窗口打开。

使用远程终端断开与资产的连接

要断开与资产的连接，

请在**“远程终端”**窗口中单击叉号 (✕) 图标断开与资产的连接。

或者，如果要断开与多个资产的连接，请点击“**全部断开连接**”按钮。

资产已与远程终端断开连接。

通过远程终端执行响应操作

通过远程终端连接到资产后，您可以使用命令行界面调查威胁并做出响应。

要运行命令，请使用以下语法：

```
<common> <parameter> <argument> [--option=value] [--flag]
```

请注意，`--flag` 是布尔标志。如果指定，则设置为`true`。您也可以将其显式设置为`true`或`false`。如果未指定，则设置为`false`。`--case-sensitive` 标志是此规则的一个异常，其行为在本页下方有更详细的描述。

通用命令行参数

设置	类型	描述
help	字符串	打开在线帮助。
task-timeout	整数	任务执行时间限制（秒）。
storage-path	字符串	用于存储响应操作结果的文件共享路径。

响应操作参数

您可以根据要对资产执行的响应操作使用以下参数：

删除文件

要从设备中删除文件，请使用以下响应操作参数：

设置	参数	可能值	类型	描述
`delete-file`	[filePath]	`md5`	字符串	MD5 文件哈希值。与文件路径搭配使用。可以指定是否附带 SHA256。
		`sha256`	字符串	SHA256 文件哈希值。与文件路径搭配使用。可以指定是否附带 MD5。
		`skip`	枚举数组	跳过响应操作的条件。 可能值： • `self-defence` • `sco` • `kl-signed` • `kl-by-trusted-app`
		`with-subfolders`	标志	如果`filePath`指定的是目录，则执行递归搜索。
		`case-sensitive`	标志	指定路径是否区分大小写。 如果未指定`--case-sensitive`标志，任务将使用操作系统的区分大小写行为，并以区分大小写的形式运行。要以不区分大小写的方式运行任务，请指定`--case-sensitive=false`。

示例

```
delete-file "C:/file path.txt" --md5=12345 --case-sensitive --skip=self-defence --skip=sco --skip=kl-signed --
skip=kl-by-trusted-app
```

管理服务

此响应操作仅适用于 Windows 设备。

要管理设备上的服务，请使用以下响应操作参数：

设置	参数	可能值	类型	描述
change-service	[operationType] 可能值： • start • stop • pause • resume • delete • change-startup-type	startup-type	enum	指定 change-startup-type 操作的启动类型。此参数在其他操作中将被忽略。 可能值： • Boot • System • Automatic • Manual • Disabled
		service-name	字符串	服务名称。支持掩码。
		md5	字符串	MD5 文件哈希值。可以指定是否附带 SHA256。
		sha256	字符串	SHA256 文件哈希值。可以指定是否附带 MD5。

示例

```
change-service change-startup-type --startup-type=auto --service-name=ServiceName --md5=12345
```

将文件移动至隔离区

为防止威胁传播，您可以将受感染的文件移至隔离区。为此，请使用以下响应操作参数：

设置	参数	可能值	类型	描述
quarantine-file	[filePath]	skip	枚举数组	跳过响应操作的条件。 可能值： • self-defence • sco • kl-signed • kl-by-trusted-app
		legacy-file-id	标志	指定后，返回遗留的 64 位隔离区 ID 而不是 GUID。
		case-sensitive	标志	指定路径是否区分大小写。 如果未指定 --case-sensitive 标志，任务将使用操作系统的区分大小写行为，并以区分大小写的形式运行。要以不区分大小写的方式运行任务，请指定 --case-sensitive=false。
		delete	标志	隔离文件后将其删除。
		md5	字符串	MD5 文件哈希值。与文件路径搭配使用。可以指定是否附带 SHA256。
		sha256	字符串	SHA256 文件哈希值。与文件路径搭配使用。可以指定是否附带 MD5。

示例

```
quarantine-file C:/filePath --skip=self-defence --skip=sco --skip=kl-signed --skip=kl-by-trusted-app
```

从隔离区中删除文件

要从设备上的隔离区目录中删除受感染的文件，请使用以下响应操作参数：

设置	可能值	类型	描述
delete-quarantined-file	file-id	字符串	隔离文件的 ID。
	legacy-file-id	整数	遗留的隔离区 ID。

示例

```
delete-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0
```

从隔离区恢复文件

如果您有理由相信隔离区中的文件是安全的，则可以将该文件恢复到设备上。为此，请使用以下响应操作参数：

设置	可能值	类型	描述
restore-quarantined-file	file-id	字符串	隔离文件的 ID。
	legacy-file-id	整数	遗留的隔离区 ID。
	replace	标志	替换现有文件。
	remove	标志	恢复后，将文件从隔离区移除。
	destination	字符串	指定用于从备份恢复对象的目标路径。如果未指定，则对象将恢复到原始路径。
	fallback-destination	字符串	指定备用目标路径。仅在恢复到原始路径失败（因为路径不存在或访问被拒绝）时使用。

示例

```
restore-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0 --replace --fallback-destination="C:/path"
```

从隔离区获取文件

可以从隔离区目录中获取设备上的隔离文件，以便进一步分析。要从隔离区获取文件，请使用以下响应操作参数：

设置	可能值	类型	描述
get-quarantined-file	file-id	字符串	隔离文件的 ID。
	legacy-file-id	整数	遗留的隔离区 ID。
	stream-index	整数	要检索的文件流索引。

响应操作完成后，获取的文件将显示在 OSMP 控制台的“**文件**”部分。

示例

```
get-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0 --stream-index=0
```

终止进程

要终止设备上的进程，请使用以下响应操作参数：

设置	可能值	类型	描述
terminate-process	path	字符串	进程可执行文件的路径。
	pid	整数	系统进程 ID。
	unique-pid	整数	进程 ID。
	md5	字符串	MD5 文件哈希值。与文件路径搭配使用。可以指定是否附带 SHA256。
	sha256	字符串	SHA256 文件哈希值。与文件路径搭配使用。可以指定是否附带 MD5。
	case-sensitive	标志	指定路径是否区分大小写。 如果未指定 `--case-sensitive` 标志，任务将使用操作系统的区分大小写行为，并以区分大小写的形式运行。要以不区分大小写的方式运行任务，请指定 `--case-sensitive=false`。
	expand-env	标志	展开路径中的环境变量。
	skip	枚举数组	跳过响应操作的条件。 可能值： • self-defence • sco • kl-signed • kl-by-trusted-app
	limit	整数	进程终止尝试的最大次数。如果未指定，则尝试次数不受限制。

示例

```
terminate-process --pid=1234 --limit=100
```

获取文件

要从设备获取文件，请使用以下响应操作参数：

设置	参数	可能值	类型	描述
get-file	[filePath]	md5	字符串	MD5 文件哈希值。与文件路径搭配使用。可以指定是否附带 SHA256。
		sha256	字符串	SHA256 文件哈希值。与文件路径搭配使用。可以指定是否附带 MD5。
		max-size	整数	文件最大大小（以字节为单位）。如果文件大小超过此限制，则响应操作将失败。默认情况下，文件大小不受限制。
		case-sensitive	标志	指定路径是否区分大小写。 如果未指定 `--case-sensitive` 标志，任务将使用操作系统的区分大小写行为，并以区分大小写的形式运行。要以不区分大小写的方式运行任务，请指定 `--case-sensitive=false`。

响应操作完成后，文件将保存到受密码保护的 ZIP 压缩包中。密码已*感染*。

示例

```
get-file C:/file --md5=1234567890 --max-size=1000 --case-sensitive
```

启用网络隔离

要为设备启用网络隔离，请使用以下响应操作参数：

设置	可能值	类型	描述
start-network-isolation	timeout	整数	网络隔离持续时间。超时到期后，隔离将自动解除。默认情况下，隔离持续时间不受限制。
	expand-env	标志	展开路径中的环境变量。
	no-notify-user	标志	禁用有关网络隔离操作的用户通知。
	exclude		网络排除规则。 此选项不能单独使用。要配置排除项，请指定一个或多个子选项： • process • direction • remote-ip-v4 • remote-ip-v6 • local-port-from • local-port-to • remote-port-from • remote-port-to • protocol
	process	字符串	指定可选的接收或发送进程。该值必须是可执行文件的完整路径。不支持掩码。环境变量仅在 Windows 系统上受支持。
	direction	enum	指定基于连接的协议（例如 TCP）的连接方向或基于数据报的协议（例如 UDP）的数据包方向。如果未指定，则同时使用两个方向。 可能值： • inbound • outbound • both
	remote-ip-v4	字符串	远程 IPv4 地址，格式为 xxx.xxx.xxx.xxx。支持子网前缀。如果未指定 IPv4 或 IPv6，则匹配任意 IP 地址。
	remote-ip-v6	字符串	远程 IPv6 地址，格式为 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。支持子网前缀。如果未指定 IPv4 或 IPv6，则匹配任意 IP 地址。
	local-port-from	整数	本地端口范围的下限。如果未指定，则匹配任意端口。如果端口不适用于数据包协议，则该规则不生效。
	local-port-to	整数	本地端口范围的上限。如果未指定，则匹配任意端口。如果端口不适用于数据包协议，则该规则不生效。
	remote-port-from	整数	远程端口范围的下限。如果未指定，则匹配任意端口。如果端口不适用于数据包协议，则该规则不生效。
	remote-port-to	整数	远程端口范围的上限。如果未指定，则匹配任意端口。如果端口不适用于数据包协议，则该规则不生效。
	protocol	整数	IANA 协议标识符（例如，TCP = 6）。如果未指定，则匹配任意协议。

示例

```
start-network-isolation --timeout=300 exclude --process="C:/process.exe" exclude --local-port-from=1 --local-port-to=10 --direction=inbound --no-notifyuser
```

禁用网络隔离

要禁用设备的网络隔离，请使用以下响应操作参数：

设置	可能值	类型	描述
stop-network-isolation	no-notify-user	标志	禁用设备的网络隔离。 默认情况下，当网络隔离被禁用时，用户会收到通知。 如果指定了 --no-notify-user 选项，则不会通知用户。 --no-notify-user 选项仅适用于运行 Windows 的设备。

示例

```
stop-network-isolation --no-notify-user
```

取证信息

获取文件列表

要获取存储在磁盘上的文件和文件夹列表，请使用以下响应操作参数。

设置	可能值	类型	描述
get-forensic files	case-sensitive	标志	指定路径是否区分大小写。 仅适用于运行Windows系统的设备。 如果未指定 --case-sensitive 标志，任务将使用操作系统的区分大小写行为，并以区分大小写的形式运行。要以不区分大小写的方式运行任务，请指定 --case-sensitive=false 。
	with-data-streams	标志	指定是否将备用数据流包含在取证报告中。
	max-depth	整数	最大搜索深度。0 表示无限制深度。1 表示仅搜索指定目录。
	max-files	整数	要查找的文件或备用数据流的最大数量。达到限制后，搜索将停止。
	include-dir	字符串数组	要包含在扫描中的目录。目录路径可以包含环境变量（例如，%TMP% 或 %TEMP%）。如果未指定，则包含所有本地目录。
	exclude-dir	字符串数组	要从扫描中排除的目录。目录路径可以包含环境变量（例如，%TMP% 或 %TEMP%）。
	include-files	字符串数组	要包含在搜索范围内的文件名掩码（例如，*.ps1）。如果未指定，则包含所有文件。
	exclude-files	字符串数组	要从搜索中排除的文件名掩码（例如，*.ps1）。如果未指定且指定了 exclude-dir ，则所有文件都将被排除。

示例

```
get-forensic files --max-depth=3 --max-files=1000 --include-dir="C:/include1" --include-dir=D:/include2
```

获取进程列表

要获取设备上正在运行的进程列表，请运行以下命令：

```
get-forensic processes
```

获取自动运行点列表

要获取自动运行点列表，请运行以下命令：

```
get-forensic autoruns
```

获取进程内存转储

要获取进程内存转储，请使用以下响应操作参数：

设置	可能值	类型	描述
get-forensic process-dump	pid	整数	系统进程 ID。
	unique-pid	整数	唯一进程 ID。
	md5	字符串	MD5 文件哈希值。与文件路径搭配使用。
	sha256	字符串	SHA256 文件哈希值。与文件路径搭配使用。

示例

```
get-forensic process-dump --pid=123 --md5=abcdef123456
```

获取文件转储

要获取文件转储，请使用以下响应操作参数：

设置	可能值	类型	描述
get-forensic files-dump	case-sensitive	标志	指定路径是否区分大小写。默认情况下，由文件系统决定。 仅适用于运行Windows系统的设备。 如果未指定 --case-sensitive 标志，任务将使用操作系统的区分大小写行为，并以区分大小写的形式运行。要以不区分大小写的方式运行任务，请指定 --case-sensitive=false。
	path	字符串数组	要转储的文件的完整路径。支持通用文件和元数据文件（例如，$Mft、$Boot）。不支持掩码。
	with-data-streams	标志	指定是否将备用数据流包含在取证报告中。
	sha256	字符串	SHA256 文件哈希值。与文件路径搭配使用。

示例

```
get-forensic files-dump --path="C:/path1"--path="D:/path2" --with-data-streams
```

获取注册表键

仅适用于运行Windows系统的设备。

要获取注册表项，请使用以下响应操作参数：

设置	可能值	类型	描述
get-forensic registry-dump	path	字符串数组	要转储的注册表项的完整路径。不支持掩码。

示例

```
get-forensic registry-dump --path="C:/path1" --path="D:/path2"
```

获取系统信息

要获取设备的系统信息，请运行以下命令：

```
get-forensic system-info
```

获取环境变量

> 仅适用于运行Windows系统的设备。

要获取环境变量，请运行以下命令：

```
get-forensic environment-variables
```

获取内存转储

要获取内存转储，请使用以下响应操作参数：

设置	可能值	类型	描述
`get-forensic memory-dump`	`compress`	标志	指定是否使用 gzip 以快速压缩级别对转储文件进行压缩。
	`segment-size`	整数	指定转储文件分段的大小（以字节为单位）。转储文件将被分割成指定大小的分段。如果值为 0 或未指定，则不会分割转储文件。

示例

```
get-forensic memory-dump --compress --segment-size=1000
```

获取磁盘映像

要获取磁盘映像，请使用以下响应操作参数：

设置	可能值	类型	描述
`get-forensic disk-dump`	`logical`	字符串	操作系统特定格式的逻辑驱动器名称（例如，Windows 系统中的 C:、D:、E:）。
	`physical`	字符串	操作系统特定格式的物理驱动器名称（例如，Windows 系统上的 \\.\PHYSICALDRIVE0）。
	`compress`	标志	指定是否使用 gzip 以快速压缩级别对转储文件进行压缩。
	`segment-size`	整数	指定转储文件分段的大小（以字节为单位）。转储文件将被分割成指定大小的分段。如果值为 0 或未指定，则不会分割转储文件。

示例

```
get-forensic disk-dump --logical="C:" --segment-size=1000 --compress
```

威胁搜索

“**威胁搜索**”页面提供了相关工具，可帮助您分析事件以排查未被自动检测到的威胁和漏洞。要基于一组事件创建警报，先选择事件，然后单击“**创建警报**”按钮。

您可以通过以下任一方式打开**威胁搜索**页面：

- 在主菜单中，转到**“监控” → “威胁搜索”。**
- 在警报或事故详情中，调用属性的上下文菜单，然后选择“**在威胁搜索中查找**”。
- 在“事故”详细信息中，单击“**在图表上查看**”按钮。在打开的调查图中，单击“**威胁搜索**”按钮。

威胁搜索页面将显示事件。您可以通过以下方式筛选事件：

- 编辑 SQL 查询
- 更改时间范围
- 选择事件所属租户

处理事件

“**威胁搜索**”部分包含可帮助您通过分析事件来搜索威胁和漏洞的工具。

事件数据模型

端点代理会将以下事件的信息发送到OSMP：

- Process
- File Create
- File Modify
- File Rename
- File Read
- File Delete
- File Attributes Modify
- 文件创建时间。
- File Hardlink Created
- File Symlink Created

- 模组
- Registry Create
- Registry Delete
- Registry Modify
- Registry Rename
- Registry Query
- Registry Save
- 连接
- Port Listen
- AMSI Scan
- Process Console Input
- 驱动器
- Process Interpreted File Run
- DNS
- Pipe Create
- Pipe Connect
- LDAP
- WMI Activity
- WMI Consumer Register
- Code Injection
- Process Access
- Threat Detect
- Threat Detect Processing Result
- Linux Event Log
- Windows Event Log
- Blocked Document
- Applock
- Process Terminated

- Device
- File System Mount
- File System Unmount
- Bits Job Create
- Bits Job Complete
- Bits Job Start
- Bits Job Stop
- Bits Job Add File
- Bits Job Error
- Service Create
- Service Modify
- Service Delete
- Scheduled Task Create
- Scheduled Task Modify
- Scheduled Task Delete
- File Owner Change
- File ACL Change
- Registry Owner Change
- Registry ACL Change
- Executable Memory Mapped
- Agent Start
- Agent Stop
- Agent Install
- Agent Uninstall
- Agent Action
- System Startup
- System Shutdown

- 连接关闭

> 启用 `Connection Close` 事件可能会显著增加受保护设备的资源使用。

Process

Windows、 Linux和macOS操作系统均支持此事件类型。

Process 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
ProcessUniqueid	int	进程唯一ID

字段	类型	描述
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessCalltrace	string	进程堆栈跟踪
ProcessFileLnkName	string	用于进程执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	用于进程执行的可执行文件（LNK 文件）路径（不含文件名）
ProcessFileLnkFullname	string	用于进程执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	用于进程执行的LNK文件命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限

字段	类型	描述
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）

字段	类型	描述
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS

字段	类型	描述
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）

字段	类型	描述
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表

字段	类型	描述
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Create

Windows操作系统支持此事件类型。

Registry Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegValueName	string	注册表值的名称
RegValueType	string	注册表值的类型
RegValueData	string	注册表值中的数据
RegValueFileMd5 [保留供将来使用]	string	RegValueData字段的文件的MD5哈希值
RegValueFileFullname [保留供将来使用]	string	RegValueData字段中的文件完整路径
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型

字段	类型	描述
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行

字段	类型	描述
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值

字段	类型	描述
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Create

Windows、 Linux和macOS操作系统均支持此事件类型。

File Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值

字段	类型	描述
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称

字段	类型	描述
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID

字段	类型	描述
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。适用于Linux和macOS
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件的名称（不包含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不包括文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间

字段	类型	描述
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。

字段	类型	描述
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Modify

Windows、 Linux和macOS操作系统均支持此事件类型。

File Modify 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。

字段	类型	描述
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称

字段	类型	描述
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID

字段	类型	描述
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间

字段	类型	描述
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段

字段	类型	描述
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Rename

Windows、 Linux和macOS操作系统均支持此事件类型。

File Rename 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
FileOldName	string	文件的先前名称
FileOldPath	string	文件的先前路径
FileOldFullname	string	文件的先前完整路径
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）

字段	类型	描述
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本

字段	类型	描述
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL

字段	类型	描述
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径

字段	类型	描述
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS

字段	类型	描述
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Read

Windows和Linux操作系统均支持此事件类型（Linux仅支持集成eBPF的版本）。

File Read 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。

字段	类型	描述
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称

字段	类型	描述
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID

字段	类型	描述
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间

字段	类型	描述
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段

字段	类型	描述
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Delete

Windows、 Linux和macOS操作系统均支持此事件类型。

File Delete 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。

字段	类型	描述
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称

字段	类型	描述
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID

字段	类型	描述
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间

字段	类型	描述
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段

字段	类型	描述
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Attributes Modify

Windows和Linux操作系统均支持此事件类型。

File Attributes Modify 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。

字段	类型	描述
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称

字段	类型	描述
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID

字段	类型	描述
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间

字段	类型	描述
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段

字段	类型	描述
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Creation Time Modify

Windows操作系统支持此事件类型。

File Creation Time Modify 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileDelafterreboot	string	如果重启后文件将被删除，则为true。指定用于删除操作。仅适用于Windows
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）

字段	类型	描述
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行

字段	类型	描述
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值

字段	类型	描述
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值

字段	类型	描述
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Hardlink Created

Windows操作系统支持此事件类型。

File Hardlink Created 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileTargetName	string	目标文件的名称
FileTargetPath	string	目标文件的路径
FileTargetFullname	string	目标文件的完整路径
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间

字段	类型	描述
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）

字段	类型	描述
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）

字段	类型	描述
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径

字段	类型	描述
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少 CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Symlink Created

Windows操作系统支持此事件类型。

File Symlink Created 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileTargetName	string	目标文件的名称
FileTargetPath	string	目标文件的路径
FileTargetFullname	string	目标文件的完整路径
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间

字段	类型	描述
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）

字段	类型	描述
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）

字段	类型	描述
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径

字段	类型	描述
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少 CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Module

Windows和Linux操作系统均支持此事件类型。

Module 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileAttr	int	文件系统属性
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileSignSubjectname	string	关于签署文件的组织的信息
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileType	string	文件的类型
FileAttrModificationtime	int	上次修改文件属性时
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
FileHijackingpath	string	原始DLL的路径
DotnetFileAssemblyName	string	完全限定的程序集名称。包含证书哈希值（用于筛选）
DotnetFileAssemblyFlags	int	.NET程序集标志
DotnetFileModuleFlags	int	.NET程序模组集标志
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS

字段	类型	描述
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS

字段	类型	描述
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名

字段	类型	描述
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL

字段	类型	描述
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径

字段	类型	描述
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Create

Windows 操作系统支持此事件类型。

Registry Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标的唯一标识符
IoAName	string array	攻击指标的名称
IoAVersion	整数数组	攻击指标版本
IoAAlert	string array	触发警报的属性
IoAConfidence	string array	攻击指标检测置信度级别（高、中、低）
IoASeverity	string array	攻击指标的严重级别（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	整数数组	与当前攻击指标相关的事件数量
IoASB	string array	根据攻击指标逻辑将发送到沙箱的文件的完整路径
EventType	字符串	通知类型
EventId	字符串	唯一事件 ID
EventTimestamp	int	客户端上的日期和时间（最初为 UTC）
EventReceivedtimestamp	int	服务器接收通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	字符串	主机唯一 ID
HostKscId	字符串	通过 KSC 进行管理的主机 ID
HostMdrId	字符串	MDR 解决方案中的受保护主机 ID
HostOsmpId	字符串	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器标识符列表
HostOsFamily	字符串	操作系统系列 (Windows)
HostOsName	字符串	操作系统名称
HostOsVersion	字符串	操作系统版本
hostName	字符串	生成事件的主机名
HostIp	字符串	主机的 IP 地址

字段	类型	描述
AgentVersion	字符串	计算机上安装的产品
AgentKdbTimestamp	int	组件 KDB 更新的时间戳
AgentSw2Timestamp	int	组件 sw2 库更新的时间戳
AgentIndexTimestamp	int	所有组件上次数据库更新的时间戳
RegKeyName	字符串	受操作影响的注册表密钥的完整路径和名称
RegValueName	字符串	注册表值的名称
RegValueType	字符串	注册表值的类型
RegValueData	字符串	注册表值中的数据
ProcessUniqueid	int	进程唯一 ID
ProcessId	int	进程 ID
ProcessCmdline	字符串	进程的命令行
ProcessCreationflags	字符串	进程创建标志列表
ProcessDirectory	字符串	进程初始目录
ProcessProperties	字符串	运行进程的帐户属性列表
ProcessFileLnkName	字符串	已执行的 LNK 文件名（不含路径）
ProcessFileLnkPath	字符串	已执行的 LNK 文件的完整路径（不含文件名）
ProcessFileLnkFullname	字符串	已执行的 LNK 文件的完整路径
ProcessFileLnkCmdline	字符串	已执行的 LNK 文件的命令行
ProcessFileLnkMd5	字符串	已执行的 LNK 文件的 MD5 哈希值
ProcessFileLnkSha256	字符串	已执行的 LNK 文件的 SHA256 哈希值
ProcessIntegritylevel	int	进程完整性级别
ProcessFileName	字符串	进程可执行文件的名称（不含路径）
ProcessFilePath	字符串	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	字符串	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	上次修改进程可执行文件的时间
ProcessFileMd5	字符串	进程可执行文件的 MD5 哈希值
ProcessFileSha256	字符串	进程可执行文件的 SHA256 哈希值
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	字符串	进程可执行文件的类型
ProcessFileUrl	字符串	下载进程可执行文件的 URL
ProcessFileEmailSrcAddress	字符串	接收进程可执行文件附件的发件人地址
ProcessFileZoneidentifier	int	从与文件关联的备用流 Zone.Identifier 中获取的区域 ID
ProcessFileProductname	字符串	VERSIONINFO 资源中的应用程序名称
ProcessFileProductversion	字符串	VERSIONINFO 资源中的应用程序版本
ProcessFileOriginalname	字符串	VERSIONINFO 资源中的原始文件名
ProcessFileProductvendor	字符串	VERSIONINFO 资源中的公司名称值
ProcessFileDescription	字符串	VERSIONINFO 资源中的描述
ProcessFileVersion	字符串	VERSIONINFO 资源中的文件版本
ProcessFileSignResult	字符串	签名验证结果：通过为 true，否则为 false

字段	类型	描述
ProcessFileSignTimestamp	int	文件签名的日期和时间
ProcessFileSignSubjectname	字符串	用于签署文件的证书的主题名称
ProcessLogonType	字符串	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话 ID
ProcessUserType	int	运行该进程的账户的属性列表
ProcessUserName	字符串	执行进程的域和用户名
ParentProcessUniqueid	int	父进程的唯一 ID
ParentProcessId	int	父进程 ID
ParentProcessCmdline	字符串	父进程的命令行
ParentProcessCreationflags	字符串	父进程的创建标志
ParentProcessFileLnkName	字符串	启动父进程的 LNK 文件名称（不含路径）
ParentProcessFileLnkPath	字符串	启动父进程的 LNK 文件路径（不含文件名）
ParentProcessFileLnkFullname	字符串	启动父进程的 LNK 文件的完整路径
ParentProcessFileLnkCmdline	字符串	启动父进程的 LNK 文件的命令行
ParentProcessFileLnkMd5	字符串	启动父进程的 LNK 文件的 MD5 哈希值
ParentProcessFileLnkSha256	字符串	启动父进程的 LNK 文件的 SHA256 哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	字符串	父进程的类型
ParentProcessFileName	字符串	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	字符串	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	字符串	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	字符串	父进程可执行文件的 MD5 哈希值
ParentProcessFileSha256	字符串	父进程可执行文件的 SHA256 哈希值
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	字符串	父进程可执行文件的类型
ParentProcessFileUrl	字符串	父进程可执行文件的下载来源 URL
ParentProcessFileEmailSrcAddress	字符串	父进程可执行文件作为附件接收时的发件人地址
ParentProcessFileCapEffective	字符串	父进程可执行文件的有效权限
ParentProcessFileProductname	字符串	父进程可执行文件的 VERSIONINFO 资源中的产品名称值
ParentProcessFileOriginalname	字符串	父进程可执行文件的 VERSIONINFO 资源中的原始文件名
ParentProcessFileProductvendor	字符串	父进程可执行文件的 VERSIONINFO 资源中的公司名称值
ParentProcessFileDescription	字符串	父进程可执行文件的 VERSIONINFO 资源中的描述
ParentProcessFileSignResult	字符串	签名验证结果：通过为 true，否则为 false
ParentProcessFileSignTimestamp	int	文件签名的日期和时间
ParentProcessFileSignSubjectname	字符串	用于签署文件的证书的主题名称
ParentProcessLogonType	字符串	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程访问令牌中的登录会话 ID
ParentProcessProperties	int	运行父进程的帐户的属性列表
ParentProcessUserName	字符串	执行父进程的用户所在的域及其用户名

字段	类型	描述
GrandParentProcessUniqueid	int	祖父进程的唯一 ID
GrandParentProcessId	int	祖父进程 ID
GrandParentProcessCmdline	字符串	祖父进程的命令行
GrandParentProcessCreationflags	字符串	祖父进程创建标志
GrandParentProcessFileLnkName	字符串	启动祖父进程的 LNK 文件的名称（不含路径）
GrandParentProcessFileLnkPath	字符串	启动祖父进程的 LNK 文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	字符串	启动祖父进程的 LNK 文件的完整路径
GrandParentProcessFileLnkCmdline	字符串	启动祖父进程的 LNK 文件的命令行
GrandParentProcessFileLnkMd5	字符串	启动祖父进程的 LNK 文件的 MD5 哈希值
GrandParentProcessFileLnkSha256	字符串	启动祖父进程的 LNK 文件的 SHA256 哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	字符串	祖父进程的类型
GrandParentProcessFileName	字符串	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	字符串	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	字符串	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的最后修改时间
GrandParentProcessFileMd5	字符串	祖父进程可执行文件的 MD5 哈希值
GrandParentProcessFileSha256	字符串	祖父进程可执行文件的 SHA256 哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	字符串	祖父进程可执行文件的类型
GrandParentProcessFileUrl	字符串	祖父进程可执行文件的下载来源 URL
GrandParentProcessFileEmailSrcAddress	字符串	以附件形式接收祖父进程可执行文件时的发件人地址
GrandParentProcessFileCapEffective	字符串	祖父进程可执行文件的有效权能
GrandParentProcessFileProductname	字符串	祖父进程可执行文件的 VERSIONINFO 资源中的产品名称值
GrandParentProcessFileOriginalname	字符串	祖父进程可执行文件的 VERSIONINFO 资源中的原始文件名
GrandParentProcessFileProductvendor	字符串	祖父进程可执行文件的 VERSIONINFO 资源中的公司名称值
GrandParentProcessFileDescription	字符串	祖父进程可执行文件的 VERSIONINFO 资源中的描述
GrandParentProcessFileSignResult	字符串	签名验证结果：通过为 true，否则为 false
GrandParentProcessFileSignTimestamp	int	文件签名的日期和时间
GrandParentProcessFileSignSubjectname	字符串	用于签署文件的证书的主题名称
GrandParentProcessLogonType	字符串	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程访问令牌中的登录会话 ID
GrandParentProcessProperties	int	运行祖父进程的帐户的属性列表
GrandParentProcessUserName	字符串	执行祖父进程的域和用户名
CreatorProcessUniqueid	int	当前进程的真正发起进程的唯一 ID。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessId	int	当前进程的真正发起进程的 ID。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessCmdline	字符串	当前进程的真正发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。

字段	类型	描述
CreatorProcessCreationflags	字符串	当前进程的真正发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessDirectory	字符串	当前进程的真正发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileLnkName	字符串	启动当前进程的真正发起进程的 LNK 文件名（不含路径）。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileLnkPath	字符串	启动当前进程的真正发起进程的 LNK 文件完整路径（不含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileLnkFullname	字符串	启动当前进程的真正发起进程的 LNK 文件完整路径。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileLnkCmdline	字符串	启动当前进程的真正发起进程的 LNK 文件命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileLnkMd5	字符串	启动当前进程的真正发起进程的 LNK 文件的 MD5 哈希值。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileLnkSha256	字符串	启动当前进程的真正发起进程的 LNK 文件的 SHA256 哈希值。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessIntegritylevel	int	当前进程的真正发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileName	字符串	当前进程的真正发起进程的可执行文件名。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFilePath	字符串	当前进程的真正发起进程的可执行文件所在目录的完整路径（不含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileFullname	字符串	当前进程的真正发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileCreationtime	int	当前进程的真正发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileModificationtime	int	当前进程的真正发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileMd5	字符串	当前进程的真正发起进程的可执行文件的 MD5 哈希值。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileSha256	字符串	当前进程的真正发起进程的可执行文件的 SHA256 哈希值。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileAttr	int	当前进程的真正发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileType	字符串	当前进程的真正发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileUrl	字符串	当前进程的真正发起进程的下载源 URL。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileEmailSrcAddress	字符串	当前进程的真正发起进程所对应的可执行文件作为附件接收时的发件人地址。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。

字段	类型	描述
CreatorProcessFileProductname	字符串	当前进程的真正发起进程文件的 VERSIONINFO 资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileOriginalname	字符串	当前进程的真正发起进程文件的 VERSIONINFO 资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileProductvendor	字符串	当前进程的真正发起进程文件的 VERSIONINFO 资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileDescription	字符串	当前进程的真正发起进程的 VERSIONINFO 资源中的描述。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileSignResult	字符串	当前进程的真正发起进程的可执行文件的签名验证结果：通过为 true，否则为 false。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileSignTimestamp	int	当前进程的真正发起进程文件的签名日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessFileSignSubjectname	字符串	用于签署当前进程的真正发起进程文件的证书的使用者名称。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessLogonType	字符串	当前进程的真正发起进程的启动用户的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessLogonSessionId	int	当前进程的真正发起进程的访问令牌中的登录会话 ID。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessProperties	int	当前进程的真正发起进程的启动用户的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。
CreatorProcessUserName	字符串	当前进程的真正发起进程的启动用户的域和用户名。通常，“ParentProcess”与“CreatorProcess”相同。在这种情况下，遥测中将不包含 CreatorProcess* 字段，需要查看 ParentProcess* 字段。

Registry Delete

Windows操作系统支持此事件类型。

Registry Delete 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegValueName	string	注册表值的名称
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名

字段	类型	描述
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径

字段	类型	描述
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）

字段	类型	描述
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Modify

Windows操作系统支持此事件类型。

Registry Modify 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegValueName	string	注册表值的名称
RegValueType	string	注册表值的类型
RegValueData	string	注册表值中的数据
RegValueFileMd5 [保留供将来使用]	string	RegValueData字段的文件的MD5哈希值
RegValueFileFullname [保留供将来使用]	string	RegValueData字段中的文件完整路径
RegOldValueData	string	注册表值中的先前数据
RegOldValueMd5	string	RegValueData字段中文件的先前MD5哈希值
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID

字段	类型	描述
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false

字段	类型	描述
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID

字段	类型	描述
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少 CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	执行运行子进程的进程的域和用户名。

Registry Rename

Windows操作系统支持此事件类型。

Registry Rename 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	
HostOsmpId	string	
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegValueName	string	注册表值的名称
RegValueType	string	注册表值的类型
RegValueData	string	注册表值中的数据
RegOldKeyName	string	注册表项的先前名称
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型

字段	类型	描述
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志

字段	类型	描述
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别

字段	类型	描述
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Query

Windows操作系统支持此事件类型。

Registry Query 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegValueName	string	注册表值的名称
RegValueType	string	注册表值的类型
RegValueData	string	注册表值中的数据
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID

字段	类型	描述
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）

字段	类型	描述
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型

字段	类型	描述
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Save

Windows操作系统支持此事件类型。

Registry Save 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegValueName	string	注册表值的名称
RegValueType	string	注册表值的类型
RegValueData	string	注册表值中的数据
FileFullname	string	文件的完整路径
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称

字段	类型	描述
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行

字段	类型	描述
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值

字段	类型	描述
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Connection

Windows、 Linux和macOS操作系统均支持此事件类型。

Connection 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
NetSrcIp	string	来源的IPv4/IPv6地址

字段	类型	描述
NetSrcPort	int	源端口号
NetDstIp	string	目标位置的IPv4/IPv6地址
NetDstPort	int	目标位置的端口号
NetUrlHostname	string	远程主机名
NetUrlPort	int	远程主机端口
NetUri	string	HTTP的目标位置URI
NetHttpMethod	string	HTTP方法
NetHttpUseragent	string	发起请求的客户端程序的标识符
NetHttpReferrer	string	指向获取目标位置URI的资源的URI引用
NetProtocol	string	IP协议
NetDirection	string	网络连接方向（入站、出站）
NetHttpHeaderName	string	HTTP标头的名称
NetHttpHeaderValue	string	HTTP标头的值
NetRaw	string	标记是否使用了原始套接字
NetTlsVersion	string	TLS 版本
NetTlsSni	string	TLS服务器名称指示
NetTlsSniEncrypted	string	TLS加密服务器名称指示
NetTlsCertificateMd5	string	TLS证书的MD5哈希值
NetTlsCertificateSha1	string	TLS证书的SHA1哈希值
NetTlsCertificateSubjectname	string	TLS主题备用名称（SAN）
NetTlsCertificateIssuername	string	TLS证书的签发者名称
NetTlsCertificateSerialnumber	string	TLS证书的序列号
NetTlsCertificateCheckresult	string	TLS证书验证结果
NetTlsCertificateValidfrom	int	TLS证书生效日期
NetTlsCertificateValidto	int	TLS证书有效期结束日期
NetTlsCiphersuite	int	TLS支持的算法
NetTlsJa3	string	TLS证书的JA3指纹
NetTlsJa3s	string	TLS证书的JA3s指纹
NetTlsJa3Md5	string	TLS证书的Ja3指纹的MD5哈希值
NetTlsJa3sMd5	string	TLS证书的Ja3s指纹的MD5哈希值
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行

字段	类型	描述
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间

字段	类型	描述
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID

字段	类型	描述
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间

字段	类型	描述
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段

字段	类型	描述
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Port Listen

Windows和Linux操作系统均支持此事件类型。

Port Listen 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
NetDstIp	string	来源的IPv4/IPv6地址

字段	类型	描述
NetDstPort	int	源端口号
NetProtocol	int	IP协议
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名

字段	类型	描述
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段

字段	类型	描述
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型

字段	类型	描述
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段

字段	类型	描述
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型

字段	类型	描述
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少 CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

AMSI Scan

Windows操作系统支持此事件类型。

AMSI Scan 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
AmsiContentType	string	发送到AMSI扫描的对象类型。

字段	类型	描述
AmsiContentData	string	检测到的对象的内容。
AmsiContentName	string	发送到AMSI扫描的对象名称。
AmsiContentMd5	string	发送到AMSI扫描的对象的MD5哈希值。
AmsiContentSha256	string	发送到AMSI扫描的对象的SHA256哈希值。
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型

字段	类型	描述
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行

字段	类型	描述
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值

字段	类型	描述
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Process Console Input

Windows和Linux操作系统均支持此事件类型。

Process Console Input 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
InputText	string	交互式输入文本

字段	类型	描述
InputType	string	输入对象的类型
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称

字段	类型	描述
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）

字段	类型	描述
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS

字段	类型	描述
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）

字段	类型	描述
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID

字段	类型	描述
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Driver

Windows操作系统支持此事件类型。

Driver 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间

字段	类型	描述
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址

Process Interpreted File Run

Windows操作系统支持此事件类型。

Process Interpreted File Run 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	解释器将执行的文件名（不含路径）

字段	类型	描述
FilePath	string	解释器将执行的文件路径（不含文件名）
FileFullname	string	解释器将执行的文件的完整路径
FileSize	int	解释器将执行的文件的大小（以字节为单位）
FileCreationtime	int	解释器将执行的文件的创建时间
FileModificationtime	int	解释器将执行的文件的上次修改时间
FileAttrModificationtime	int	解释器将执行的文件属性的上次修改时间
FileMd5	string	解释器将执行的文件的MD5哈希值
FileSha256	string	解释器将执行的文件的SHA256哈希值
FileAttr	int	解释器将执行的文件的文件系统属性列表
FileType	string	解释器将执行的文件的类型
FileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
FileProductname	string	VERSIONINFO资源中的应用程序名称
FileProductvendor	string	VERSIONINFO资源中的公司名称
FileDescription	string	VERSIONINFO资源中的描述
FileOriginalname	string	VERSIONINFO资源中的原始文件名
FileSignSubjectname	string	用于签署文件的证书的主题名称
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	解释器将执行的文件的下载URL
FileEmailSrcAddress	string	作为附近接受解释器将执行的文件的发件人地址
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群組ID。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群組名称。适用于Linux和macOS
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别

字段	类型	描述
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID

字段	类型	描述
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称

字段	类型	描述
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值

字段	类型	描述
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段

字段	类型	描述
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

DNS

Windows和Linux操作系统支持此事件类型（仅在Linux上用于外部连接）。

DNS 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
DnsServerIp	string	正在查询DNS服务器

字段	类型	描述
DnsQueryOptions	string	执行的DNS查询的选项
DnsQueryStatus	int	操作的错误代码
DnsResourceName	string	正在查询的URL
DnsResourceType	string	执行的DNS查询类型
DnsAnswer	string	DNS查询结果
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址

字段	类型	描述
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段

字段	类型	描述
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值

字段	类型	描述
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID

字段	类型	描述
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false

字段	类型	描述
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Pipe Create

Windows操作系统支持此事件类型。

Pipe Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
PipeName	string	创建或已建立连接的命名管道的名称

字段	类型	描述
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述

字段	类型	描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述

字段	类型	描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false

字段	类型	描述
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间

字段	类型	描述
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Pipe Connect

Windows操作系统支持此事件类型。

Pipe Connect 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
PipeName	string	创建或已建立连接的命名管道的名称

字段	类型	描述
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述

字段	类型	描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述

字段	类型	描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false

字段	类型	描述
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间

字段	类型	描述
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

LDAP

Windows操作系统支持此事件类型。

LDAP 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
LdapSearchScope	string	要搜索的目录树状图区域或范围

字段	类型	描述
LdapSearchFilter	string	LDAP搜索查询将用于匹配目录中的条目的条件或标准
LdapSearchDn	string	搜索操作将开始的目录树状图中的起点或基点
LdapSearchAttr	string	用于筛选或搜索的特定属性列表
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID

字段	类型	描述
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志

字段	类型	描述
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值

字段	类型	描述
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

WMI Activity

除Windows XP外，所有Windows操作系统均支持此事件类型。

WMI Activity 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
WmiRemote	string	远程WMI操作标志

字段	类型	描述
WmiHostName	string	WMI活动的源主机名称
WmiUserName	string	执行WMI操作的用户帐户名称
WmiNamespacename	string	查询的WMI命名空间
WmiQuery	string	WMI查询
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型

字段	类型	描述
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志

字段	类型	描述
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别

字段	类型	描述
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

WMI Consumer Register

除Windows XP外，所有Windows操作系统均支持此事件类型。

WMI Consumer Register 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
WmiNamespacename	string	查询的WMI命名空间

字段	类型	描述
WmiFiltername	string	事件使用者使用的筛选器名称
WmiConsumerName	string	创建事件的使用者名称。
WmiConsumerText	string	事件使用者的MOF代码
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表

字段	类型	描述
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）

字段	类型	描述
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）

字段	类型	描述
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Code Injection

Windows和Linux操作系统均支持此事件类型。

Code Injection 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
TargetProcessUniqueid	int	目标进程唯一ID

字段	类型	描述
TargetProcessId	int	目标进程ID（PID）
TargetProcessCmdline	string	传递给目标进程的命令行参数
TargetProcessFileName	string	目标进程（执行代码注入的进程）可执行文件的名称
TargetProcessFilePath	string	目标进程（执行代码注入的进程）可执行文件的完整路径（不包含文件名）。
TargetProcessFileFullname	string	目标进程（执行代码注入的进程）可执行文件的完整路径
TargetProcessFileMd5	string	目标进程可执行文件的MD5哈希值
TargetProcessFileSha256	string	目标进程可执行文件的SHA256哈希值
TargetProcessIntegritylevel	int	目标进程的完整性级别
TargetProcessFileUrl	string	目标进程可执行文件的下载URL
TargetProcessFileEmailSrcAddress	string	作为附件接收目标进程可执行文件的发件人地址
SyscallArgs	string	系统调用参数仅适用于Linux
ProcessCalltrace	string	进程堆栈跟踪
ProcessModifiedcmdline	string	进程的命令行
InjectMethod	string	注入方法
InjectAddress	string	字段包含有关注入后执行开始的地址的信息
InjectImageFileName	string	仅用于SET_WINDOWS_HOOK
InjectImageFileFullname	string	仅用于SET_WINDOWS_HOOK
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）

字段	类型	描述
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）

字段	类型	描述
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID

字段	类型	描述
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值

字段	类型	描述
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型

字段	类型	描述
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Process Access

Windows操作系统支持此事件类型。

Process Access 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
AccessOperationtype	string	在进程句柄上执行的访问操作类型（由一个进程在另一个进程上）。

字段	类型	描述
AccessRights	string	进程对象的所需访问权限
ProcessCalltrace	string	进程堆栈跟踪
TargetProcessFileName	string	目标进程（执行代码注入的进程）可执行文件的名称
TargetProcessFilePath	string	目标进程（执行代码注入的进程）可执行文件的完整路径（不包含文件名）。
TargetProcessFileFullname	string	目标进程（执行代码注入的进程）可执行文件的完整路径
TargetProcessFileMd5	string	目标进程可执行文件的MD5哈希值
TargetProcessFileSha256	string	目标进程可执行文件的SHA256哈希值
TargetProcessFileCreationtime	int	目标进程可执行文件的创建时间
TargetProcessFileModificationtime	int	目标进程可执行文件的上次修改时间
TargetProcessFileAttrModificationtime	int	目标进程可执行文件属性的上次修改时间
TargetProcessFileSize	int	目标进程可执行文件的大小（以字节为单位）
TargetProcessUniqueid	int	目标进程唯一ID
TargetProcessId	int	目标进程ID（PID）
TargetProcessCmdline	string	传递给目标进程的命令行参数
TargetProcessFileUrl	string	目标进程可执行文件的下载URL
TargetProcessFileEmailSrcAddress	string	作为附件接收目标进程可执行文件的发件人地址
HandleProcessSrcFileName	string	复制句柄的进程名称
HandleProcessSrcFilePath	string	复制句柄的进程的完整路径（不含文件名）
HandleProcessSrcFileFullname	string	复制句柄的进程的完整路径
HandleProcessSrcFileMd5	string	复制句柄的进程的MD5哈希值
HandleProcessSrcFileSha256	string	复制句柄的进程的SHA256哈希值
HandleProcessSrcFileCreationtime	int	复制句柄的进程的创建时间
HandleProcessSrcFileModificationtime	int	复制句柄的进程的上次修改时间
HandleProcessSrcFileAttrModificationtime	int	复制句柄的进程属性的上次修改时间
HandleProcessSrcFileSize	int	复制句柄的进程可执行文件的大小
HandleProcessSrcUniqueid	int	复制句柄的进程的唯一PID
HandleProcessSrcId	int	复制句柄的进程的进程标识符（PID）
HandleProcessSrcIntegritylevel	int	复制句柄的进程的完整性级别
HandleProcessSrcCmdline	string	复制句柄的进程的命令行选项
HandleProcessSrcFileUrl	string	源进程的下载URL
HandleProcessSrcFileEmailSrcAddress	string	作为附件接收源进程可执行文件的发件人地址
HandleProcessDstFileName	string	复制句柄的进程名称
HandleProcessDstFilePath	string	复制句柄的进程的完整路径（不含文件名）
HandleProcessDstFileFullname	string	复制句柄的进程的完整路径
HandleProcessDstFileMd5	string	复制句柄的进程的MD5哈希值
HandleProcessDstFileSha256	string	复制句柄的进程的SHA256哈希值
HandleProcessDstFileCreationtime	int	复制句柄的进程的创建时间
HandleProcessDstFileModificationtime	int	复制句柄的进程的上次修改时间
HandleProcessDstFileAttrModificationtime	int	复制句柄的进程属性的上次修改时间
HandleProcessDstFileSize	int	复制句柄的进程的可执行文件的大小
HandleProcessDstUniqueid	int	复制句柄的进程的唯一PID

字段	类型	描述
HandleProcessDstId	int	复制句柄的进程的进程标识符（PID）
HandleProcessDstIntegritylevel	int	复制句柄的进程的完整性级别
HandleProcessDstCmdline	string	复制句柄的进程的命令行选项
HandleProcessDstFileUrl	string	源进程的下载URL
HandleProcessDstFileEmailSrcAddress	string	作为附件接收源进程可执行文件的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID

字段	类型	描述
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称

字段	类型	描述
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限

字段	类型	描述
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值

字段	类型	描述
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Threat Detect

Windows、 Linux和macOS操作系统均支持此事件类型。

Threat Detect 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
ThreatObjectFullname	string	文件的完整路径

字段	类型	描述
ThreatObjectMd5	string	文件内容的MD5哈希值
ThreatObjectSha256	string	文件内容的SHA256哈希值
ThreatObjectType	string	检测到的对象的类型
ThreatVerdictname	string	威胁判定名称
ThreatRecordid	int	检测到威胁的记录ID
ThreatDatabaseTimestamp	int	数据库上次更新的日期和时间
ThreatProcessingmode	int	检测到对象的处理模式
ThreatSilent	string	True，用于静默检测
NetProtocol	int	IP协议
NetDstIp	string	本地（受攻击）IPv4/IPv6 地址
NetDstPort	int	本地（受攻击）端口号
NetSrcIp	string	远程（攻击者）IPv4/IPv6 地址
NetSrcPort	int	远程（攻击者）端口号。
ThreatEmailAddress	string	作为附件接收检测到的文件的发件人地址
ThreatEmailDestination	string	检测到的电子邮件的目标地址
ThreatEmailSubject	string	检测到的电子邮件的主题
ThreatEmailMessageid	string	检测到的电子邮件的邮件ID
ThreatEmailReceivedtimestamp	string	检测到的电子邮件的接收时间
ThreatDownloaderFileFullname	string	下载检测到的文件的进程的可执行文件的路径
AmsiContentType	string	发送到AMSI扫描的对象类型。
AmsiContentData	string	检测到的对象的内容。
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS

字段	类型	描述
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID

字段	类型	描述
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false

字段	类型	描述
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID

字段	类型	描述
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间

字段	类型	描述
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Threat Detect Processing Result

Windows、 Linux和macOS操作系统均支持此事件类型。

Threat Detect Processing Result 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
ThreatObjectFullname	string	文件的完整路径

字段	类型	描述
ThreatObjectMd5	string	文件内容的MD5哈希值
ThreatObjectSha256	string	文件内容的SHA256哈希值
ThreatObjectType	string	检测到的对象的类型
ThreatVerdictname	string	威胁判定名称
ThreatRecordid	int	检测到威胁的记录ID
ThreatDatabaseTimestamp	int	数据库上次更新的日期和时间
ThreatProcessingmode	int	检测到对象的处理模式
NetProtocol	int	IP协议
NetDstIp	string	本地（受攻击）IPv4/IPv6 地址
NetDstPort	int	本地（受攻击）端口号
NetSrcIp	string	远程（攻击者）IPv4/IPv6 地址
NetSrcPort	int	远程（攻击者）端口号。
ThreatEmailAddress	string	作为附件接收检测到的文件的发件人地址
ThreatDownloaderFileFullname	string	下载检测到的文件的进程的可执行文件的路径
ThreatAction	string	对精确检测检测到的对象采取的行动类型
ThreatActionresult	string	采取的行动的结果，在ThreatAction字段中指定。
ThreatActionreason	string	如果操作成功，该字段包含0。如果操作失败，此字段包含失败原因。
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）

字段	类型	描述
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）

字段	类型	描述
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID

字段	类型	描述
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值

字段	类型	描述
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型

字段	类型	描述
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Linux Event Log

Linux操作系统支持此事件类型。

Linux Event Log 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
LinuxEventType	string	事件类型。

字段	类型	描述
LinuxEventMessage	string	日志消息
LinuxOperationResult	string	操作结果——例如，成功或失败
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名

字段	类型	描述
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段

字段	类型	描述
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型

字段	类型	描述
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段

字段	类型	描述
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型

字段	类型	描述
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少 CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Windows Event Log

Windows操作系统支持此事件类型。

Windows Event Log 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
SystemLogEventXml	string	来自系统事件日志的XML
SystemLogEventId [包含过滤字段，名称为常量]	int	系统日志中的事件ID
SystemLogChannelName [包含过滤字段，名称为常量]	string	系统日志中的通道名称
SystemLogProviderName [包含过滤字段，名称为常量]	string	系统日志中的提供者名称
OmitQualifiers [包含过滤字段，名称为常量]		
WinBinary	string	正在处理的对象的文件属性
WinData	string	Windows事件日志事件的主要数据

字段	类型	描述
WinAccessGranted	string	来自Windows事件日志事件的安全参数
WinAccessList	string	正在处理的对象的访问权限
WinAccessMask	string	正在处理的对象的访问权限
WinAccessReason	string	将文件移动到类别的原因
WinAccessRemoved	string	从对象中删除的访问权限
WinAccountDomain	string	用于验证登录会话所有者的域名
WinAccountExpires	string	Active Directory对象参数
WinAccountName	string	启动受控进程的帐户ID
WinAccountSessionIdentifier	string	网络政策服务器事件中的身份验证会话标识符
WinAction	string	事件中的系统或安全操作
WinActionID	string	事件期间执行的操作标识符
WinActionName	string	事件期间执行的操作名称
WinActiveProfile	string	活动配置或网络配置文件
WinAddedCAPs	string	添加的中央访问政策列表
WinAdditionalActionsID	string	与事件相关的其他操作的标识符
WinAdditionalActionsString	string	与事件相关的其他操作的描述或字符串
WinAdditionalDetails	string	查询字符串
WinAdditionalInfo	string	关于事件或对象的其他信息
WinAdditionalInfo2	string	关于事件或对象的其他信息（第二个字段）
WinAdvancedOptions	string	高级配置选项
WinAlgorithmName	string	使用的加密算法名称
WinAllowedToDelegateTo	string	启动受控进程的帐户ID
WinAppCorrelationID	string	对象类型代码
WinApplication	string	正在处理的对象的名称
WinAppName	string	软件名称
WinAppVersion	string	软件组件的版本
WinAsIsCAPs	string	未修改的中央访问政策列表
WinAttributeLDAPDisplayName	string	正在处理的可执行文件的属性
WinAttributes	string	对象或事件的属性
WinAttributeSyntaxOID	string	正在处理的对象的文件属性
WinAttributeValue	string	正在处理的可执行文件的属性
WinAuditPolicyChanges	string	来自Windows事件日志事件的安全参数
WinAuditSourceName	string	正在处理的对象的名称
WinAuditStatusCode	string	事件审计状态代码
WinAuthenticationLevel	string	请求或连接的身份验证级别
WinAuthenticationPackageName	string	正在处理的对象的名称
WinAuthenticationProvider	string	事件的身份验证提供者
WinAuthenticationServer	string	执行身份验证的服务器
WinAuthenticationService	string	事件中使用的身份验证验证服务
WinAuthenticationType	string	事件的身份验证类型
WinBackupType	string	备份类型

字段	类型	描述
WinBcdCCID	string	智能卡设备设置和属性
WinBMaxSlotIndex	string	智能卡设备设置和属性
WinBNumClockSupported	string	智能卡设备设置和属性
WinBNumDataRateSupported	string	智能卡设备设置和属性
WinBootMode	string	windows事件日志事件的用户会话参数
WinBuildVersion	string	正在发送的统计信息的版本
WinBVoltageSupport	string	智能卡设备设置和属性
WinCalledStationID	string	身份验证中被调用的站标识符
WinCallerProcessId	string	父进程系统进程ID（PID）
WinCallerProcessName	string	正在处理的对象的名称
WinCallingStationID	string	身份验证中调用的站标识符
WinCalloutKey	string	调用的函数或规则的密钥
WinCalloutName	string	调用的函数或规则的名称
WinCategoryId	string	Windows事件日志事件的操作参数
WinCategoryName	string	事件或威胁的类别
WinCertificateTemplate	string	事件中使用的证书模板
WinCertIssuerName	string	证书签发者名称
WinCertSerialNumber	string	证书序列号
WinCertThumbprint	string	扫描对象和散列算法的数字证书指纹
WinChangeType	string	更改类型
WinClassId	string	对象类型代码
WinClassName	string	正在处理的对象的名称
WinClientAddress	string	本地IP地址
WinClientIPAddress	string	发起事件的客户端IP地址
WinClientName	string	启动受控进程的帐户ID
WinClientProcessId	string	客户端进程标识符
WinClientProcessStartKey	string	创建任务的进程的唯一键
WinCommandLine	string	启动进程的命令行
WinCompatibleIds	string	Windows事件日志事件的其他参数
WinComputerAccountChange	string	Windows事件日志事件的操作参数
WinComputerName	string	发生事件的计算机的名称
WinConditions	string	与事件或筛选器相关的条件
WinConfigAccessPolicy	string	配置访问政策
WinConfiguredNames	string	配置资源或对象的名称
WinContextInfo	string	Windows事件日志事件中记录的任务参数
WinCountOfCredentialsReturned	string	返回的凭证数量
WinCrashOnAuditFailValue	string	审计失败时崩溃设置的值
WinCredType	string	凭证类型
WinCurrentEngineVersion	string	安全引擎的当前版本
WinCurrentSignatureVersion	string	当前签名版本
WinCVEID	string	Windows事件日志事件的其他参数

字段	类型	描述
WinDCDNSName	string	域控制器DNS名称
WinDCOMorRPC	string	使用的DCOM或RPC协议
WinDeletedCAPs	string	已删除的中央访问政策列表
WinDestAddress	string	网络事件的目标地址
WinDestinationDRA	string	Windows事件日志事件的网络连接参数
WinDestPort	string	网络事件的目标端口
WinDetectionID	string	检测到的威胁标识符
WinDetectionSource	string	威胁检测的来源
WinDetectionSourceIndex	string	检测来源索引
WinDetectionTime	string	检测到威胁的时间
WinDetectionType	string	威胁检测的类型
WinDetectionTypeIndex	string	检测类型的索引
WinDetectionUser	string	检测到威胁的用户
WinDeviceClaims	string	参与身份验证的设备
WinDeviceDescription	string	正在处理的对象的描述，如对象属性中所定义。
WinDeviceId	string	设备ID
WinDirection	string	网络流量的方向
WinDisabledPrivilegeList	string	已禁用权限列表
WinDisableIntegrityChecks	string	标记以禁用完整性检查
WinDisplayName	string	启动受控进程的帐户ID
WinDisposition	string	事件或对象的处理结果
WinDnsHostName	string	用户设备名称
WinDnsName	string	用户设备名称
WinDomain	string	与事件或对象关联的域
WinDomainBehaviorVersion	string	Active Directory对象参数
WinDomainName	string	用于验证登录会话所有者的域名
WinDomainPolicyChanged	string	Active Directory对象参数
WinDomainSid	string	用户帐户安全标识符（SID）
WinDSName	string	正在处理的对象的名称
WinDSType	string	软件检测到的对象类型
WinDummy	string	Windows事件日志事件的其他参数
WinDuration	string	事件的持续时间
WinDwDataRate	string	智能卡设备设置和属性
WinDwDefaultClock	string	智能卡设备设置和属性
WinDwFeatures	string	智能卡设备设置和属性
WinDwMaxDataRate	string	智能卡设备设置和属性
WinDwMaxIFSD	string	智能卡设备设置和属性
WinDwMaximumClock	string	智能卡设备设置和属性
WinDwMechanical	string	智能卡设备设置和属性
WinDwProtocols	string	智能卡设备设置和属性
WinDwSyncProtocols	string	智能卡设备设置和属性

字段	类型	描述
WinEAPErrorCode	string	EAP错误代码
WinEAPReasonCode	string	EAP原因代码
WinEapRootCauseString	string	EAP错误根本原因描述
WinEAPType	string	EAP身份验证的类型
WinEffectiveState	string	对象或系统的当前状态
WinElevatedToken	string	来自Windows事件日志事件的安全参数
WinEnabledPrivilegeList	string	已启用权限列表
WinEndUSN	string	USN日志中结束更改标识符
WinEngineVersion	string	事件发生时的引擎版本
WinEntryType	string	软件检测到的对象类型
WinErrorCode	string	Windows事件日志事件的操作参数
WinErrorDescription	string	事件期间发生的错误描述
WinEventCount	string	事件重复次数
WinEventCountTotal	string	相关事件总数
WinEventId	string	事件标识符
WinEventIdx	string	序列中的事件索引
WinEventSourceId	string	对象类型代码
WinExecutionID	string	生成事件的进程标识符
WinExecutionName	string	生成事件的进程名称
WinExecutionStatus	string	操作的执行状态
WinExecutionStatusIndex	string	执行状态索引
WinExeFileName	string	正在处理的对象的名称
WinFailureId	string	故障标识符
WinFailurePoint	string	故障点
WinFailureReason	string	将文件移动到类别的原因
WinFileName	string	正在处理的对象的名称
WinFilterId	string	筛选器标识符
WinFilterKey	string	筛选键
WinFilterName	string	筛选器名称
WinFilterRTID	string	Windows事件日志事件的网络连接参数
WinFilterType	string	筛选器类型
WinFlags	string	Windows事件日志事件的操作参数
WinFlightSigning	string	飞行建造签名标志
WinForceLogoff	string	Active Directory对象参数
WinForestRoot	string	启动受控进程的帐户ID
WinForestRootSid	string	用户帐户安全标识符（SID）
WinFQDN	string	发起事件的主机或计算机的完全限定域名（FQDN）
WinFullyQualifiedSubjectMachineName	string	主题的完全限定计算机名称
WinFullyQualifiedSubjectUserName	string	主体的完全限定用户名
WinFWLink	string	指向描述威胁的页面链接
WinGPOList	string	正在处理的对象的访问权限

字段	类型	描述
WinGroupDomainName	string	群组域名
WinGroupMembership	string	群组成员身份
WinGroupName	string	组名称
WinGroupPolicyApplied	string	应用的群组政策
WinGroupSid	string	群组SID
WinGroupTypeChange	string	有关用户群组的信息
WinHandleId	string	对象类型代码
WinHangType	string	软件检测到的对象类型
WinHardwareIds	string	硬件标识符
WinHomeDirectory	string	正在处理对象的路径
WinHomePath	string	正在处理对象的路径
WinHypervisorDebug	string	虚拟机管理程序调试标志
WinHypervisorLaunchType	string	虚拟机监控程序启动类型
WinHypervisorLoadOptions	string	虚拟机监控程序加载选项
WinIdentity	string	用户或设备标识符
WinImagePath	string	正在处理对象的路径
WinImpersonationLevel	string	来自Windows事件日志事件的安全参数
WinInitiatorCookie	string	发起程序操作Cookie
WinInterfaceName	string	网络接口名称
WinIntfGuid	string	网络接口GUID
WinIpAddress	string	本地IP地址
WinIpAddresses	string	与对象关联的IP地址
WinIpPort	string	正在处理的网络连接的来源端口号和目标端口号
WinKerberosPolicyChange	string	来自Windows事件日志事件的安全参数
WinKernelDebug	string	卷积核调试标志
WinKeyFilePath	string	密钥文件路径
WinKeyLength	string	Active Directory对象参数
WinKeyModName	string	键控模块名称
WinKeyName	string	加密密钥名称
WinKeyType	string	加密密钥类型
WinLayerId	string	筛选层标识符
WinLayerKey	string	筛选层密钥
WinLayerName	string	Windows事件日志事件的网络连接参数
WinLayerRTID	string	Windows事件日志事件的网络连接参数
WinLinkName	string	正在处理的对象的名称
WinLmPackageName	string	正在处理的对象的名称
WinLoadOptions	string	加载选项
WinLocalAddress	string	网络事件中的本机地址
WinLocalKeyModPort	string	本地密钥模块端口
WinLocalMac	string	本机MAC地址
WinLocalMMPrincipalName	string	IPsec主模式身份验证过程中使用的本地安全主体

字段	类型	描述
WinLocationInformation	string	windows事件日志事件的用户会话参数
WinLockoutDuration	string	Active Directory对象参数
WinLockoutObservationWindow	string	Active Directory对象参数
WinLockoutThreshold	string	Active Directory对象参数
WinLogDroppedPacketsEnabled	string	指示是否启用了丢弃的网络数据包的日志记录的标志
WinLoggingResult	string	日志记录结果
WinLogonGuid	string	有关用户群组的信息
WinLogonHours	string	Active Directory对象参数
WinLogonID	string	用户帐户安全标识符（SID）
WinLogonProcessName	string	从Windows事件日志派生的对象名称
WinLogonType	string	登录会话类型
WinLogSuccessfulConnectionsEnabled	string	指示是否启用了成功网络连接的日志记录的标志
WinMachineAccountQuota	string	Active Directory对象参数
WinMachineInventory	string	计算机清单
WinMajorVersion	string	正在发送的统计信息的版本
WinMandatoryLabel	string	进程的强制安全标签
WinMasterKeyId	string	数据加密的主密钥标识符
WinMaxPasswordAge	string	Active Directory对象参数
WinMemberName	string	启动受控进程的帐户ID
WinMemberSid	string	用户帐户安全标识符（SID）
WinMessageNumber	string	Windows事件日志事件的其他参数
WinMessageTotal	string	Windows事件日志事件的其他参数
WinMinorVersion	string	正在发送的统计信息的版本
WinMinPasswordAge	string	Active Directory对象参数
WinMinPasswordLength	string	Active Directory对象参数
WinMixedDomainMode	string	Active Directory对象参数
WinMMAuthMethod	string	IPSec主模式协商期间使用的身份验证方法
WinMMFilterID	string	Windows分配给特定IPSec主模式筛选器的标识符
WinMMImpersonationState	string	字段显示IPSec主模式身份身份验证过程中是否使用了模拟
WinModifiedCAPs	string	已修改的中央访问政策列表
WinModifiedObjectProperties	string	正在处理的对象的描述，如对象属性中所定义。
WinMulticastFlowsEnabled	string	已启用的多播流标志
WinNamingContext	string	Windows事件日志事件的网络连接参数
WinNASIdentifier	string	网络访问服务器（NAS）标识符
WinNASIPv4Address	string	网络访问服务器（NAS）IPv4地址
WinNASIPv6Address	string	网络访问服务器（NAS）IPv6 地址
WinNASPort	string	网络访问服务器（NAS）连接的端口
WinNASPortType	string	网络访问服务器（NAS）端口类型
WinNetbiosName	string	正在处理的对象的名称
WinNetworkPolicyName	string	应用的网络政策名称
WinNewMaxUsers	string	分布式文件系统资源属性

字段	类型	描述
WinNewObjectDN	string	对象可分辨名称
WinNewProcessId	string	新进程ID
WinNewProcessName	string	新进程名称
WinNewRemark	string	分布式文件系统资源属性
WinNewSd	string	来自Windows事件日志事件的安全参数
WinNewShareFlags	string	分布式文件系统资源属性
WinNewState	string	对象或系统的新状态
WinNewTargetUserName	string	启动受控进程的帐户ID
WinNewTime	string	事件时间
WinNewUacValue	string	用户账户控制组件的属性
WinNewValue	string	正在处理的对象的文件属性
WinNewValueType	string	软件检测到的对象类型
WinNotificationPackageName	string	正在处理的对象的名称
WinObjectClass	string	应用程序更新组件中应用程序类别的位掩码
WinObjectCollectionName	string	正在处理的对象的名称
WinObjectDN	string	对象可分辨名称
WinObjectGUID	string	有关用户群组的信息
WinObjectIdentifyingProperties	string	Windows事件日志事件的其他参数
WinObjectName	string	从Windows事件日志派生的对象名称
WinObjectProperties	string	Windows事件日志事件中记录的任务参数
WinObjectServer	string	Windows事件日志事件中记录的任务参数
WinObjectType	string	软件检测到的对象类型
WinObjectValueName	string	正在处理的对象的名称
WinOemInformation	string	正在处理的对象的描述，如对象属性中所定义。
WinOldMaxUsers	string	分布式文件系统资源属性
WinOldObjectDN	string	对象可分辨名称
WinOldRemark	string	分布式文件系统资源属性
WinOldSd	string	来自Windows事件日志事件的安全参数
WinOldShareFlags	string	分布式文件系统资源属性
WinOldTargetUserName	string	启动受控进程的帐户ID
WinOldUacValue	string	用户账户控制组件的属性
WinOldValue	string	正在处理的对象的文件属性
WinOldValueType	string	软件检测到的对象类型
WinOpCorrelationID	string	对象类型代码
WinOperation	string	操作执行类型
WinOperationId	string	Windows事件日志事件的操作参数
WinOperationMode	string	操作执行模式
WinOperationType	string	软件检测到的对象类型
WinOptions	string	Windows事件日志事件的操作参数
WinOriginID	string	对象来源标识符
WinOriginName	string	对象来源名称

字段	类型	描述
WinPackage	string	与事件相关的程序包名称或标识符
WinPackageFullName	string	正在处理的对象的名称
WinPackageName	string	正在处理的对象的名称
WinPackageRelativeAppId	string	对象类型代码
WinPackageSid	string	与事件相关的程序包SID
WinParam1	string	查询字符串
WinParam2	string	查询字符串
WinParam3	string	查询字符串
WinParam4	string	查询字符串
WinParam5	string	查询字符串
WinParentProcessId	string	创建任务时启动当前进程的父进程ID
WinParentProcessName	string	父进程名称
WinPasswordHistoryLength	string	Active Directory对象参数
WinPasswordLastSet	string	Active Directory对象参数
WinPasswordProperties	string	正在处理的对象的描述，如对象属性中所定义。
WinPath	string	正在处理对象的路径
WinPathFound	string	检测到的文件或对象的路径
WinPayload	string	正在处理的对象的文件属性
WinPeerMac	string	对等设备MAC地址
WinPostCleanStatus	string	威胁修复后状态
WinPreAuthType	string	软件检测到的对象类型
WinPreExecutionStatus	string	操作执行前状态
WinPreviousEngineVersion	string	安全引擎的先前版本
WinPreviousSignatureVersion	string	先前签名版本
WinPreviousTime	string	事件时间
WinPrimaryGroupId	string	有关用户群组的信息
WinPrivilegeList	string	正在处理的对象的访问权限
WinProcessCreationTime	string	进程创建时间
WinProcessId	string	进程ID（PID）
WinProcessName	string	正在处理的对象的名称
WinProductName	string	生成事件的安全产品名称
WinProductVersion	string	安全产品版本
WinProfile	string	用户或系统配置文件名称/ID
WinProfileChanged	string	Windows事件日志事件的操作参数
WinProfilePath	string	正在处理对象的路径
WinProfiles	string	已应用配置文件列表
WinProfileUsed	string	事件中使用的配置文件
WinProperties	string	正在处理的对象的描述，如对象属性中所定义。
WinPropertyName	string	对象的属性名称
WinProtocol	string	Windows事件日志事件的网络连接参数
WinProviderKey	string	筛选器或操作员的提供者键

字段	类型	描述
WinProviderName	string	操作或事件的提供者名称
WinProxyPolicyName	string	代理政策名称
WinPuaCount	string	Windows事件日志事件的其他参数
WinPuaPolicyId	string	对象类型代码
WinQfeVersion	string	正在发送的统计信息的版本
WinQuarantineSessionIdentifier	string	隔离区会话标识符
WinQuarantineState	string	隔离中的对象状态
WinReadOperation	string	读取操作标志
WinReason	string	事件或操作的原因
WinReasonCode	string	事件原因代码
WinReasonForRejection	string	操作被拒的原因
WinReasonText	string	事件原因的文本描述
WinRecoveryKeyId	string	恢复密钥标识符
WinRecoveryReason	string	使用恢复密钥的原因
WinRecoveryServer	string	数据恢复服务器
WinRelativeTargetName	string	正在处理的对象的名称
WinRemediationUser	string	发起补救措施的用户
WinRemoteAddress	string	连接或操作的远程地址
WinRemoteAdminEnabled	string	已启用远程管理的标志
WinRemoteEventLogging	string	远程事件日志标志
WinRemoteKeyModPort	string	远程键模块端口
WinRemoteMachineID	string	远程计算机标识符
WinRemoteMMPrincipalName	string	IPsec主模式身份验证过程中使用的远程安全主体
WinRemoteUserID	string	远程用户标识符
WinReplicationEvent	string	复制事件标志
WinReportId	string	对象类型代码
WinRequestClientInfo	string	发送请求的客户端信息
WinRequestCSPProvider	string	事件中请求的CSP提供者
WinRequester	string	请求者
WinRequestId	string	请求ID
WinRequestOSVersion	string	发出请求客户端的操作系统版本
WinResource	string	操作中涉及的资源或对象
WinResourceAttributes	string	正在处理的对象的文件属性
WinResourceManager	string	负责对象的资源管理器
WinResponderCookie	string	响应器操作cookie
WinRestrictedAdminMode	string	来自Windows事件日志事件的安全参数
WinRestrictedSidCount	string	操作的受限SID数量
WinReturnCode	string	操作结果的返回代码
WinRole	string	主体在操作中的作用
WinRpcCallClientLocality	string	发起事件的RPC客户端位置，表明调用是本地还是远程的
WinRuleAttr	string	安全规则或筛选器属性

字段	类型	描述
WinRuleId	string	对象类型代码
WinRuleName	string	正在处理的对象的名称
WinRunspaceId	string	PowerShell运行空间ID
WinSamAccountName	string	启动受控进程的帐户ID
WinScanID	string	扫描标识符
WinScanParameters	string	扫描参数
WinScanParametersIndex	string	扫描参数索引
WinScanResources	string	扫描的资源
WinScanTimeHours	string	扫描耗费的小时数
WinScanTimeMinutes	string	扫描耗费的分钟数
WinScanTimeSeconds	string	扫描耗费的秒数
WinScanType	string	扫描类型
WinScanTypeIndex	string	扫描类型的索引
WinSchema	string	对象或事件的模式
WinSchemaFriendlyName	string	模式的友好名称
WinScriptBlockId	string	对象类型代码
WinScriptBlockText	string	windows事件日志事件的用户会话参数
WinScriptPath	string	正在处理对象的路径
WinSecurityDescriptor	string	对象的安全描述符
WinSecurityPackageName	string	正在处理的对象的名称
WinSerialNumber	string	证书或安全对象的序列号
WinServerNames	string	操作中涉及的服务器名称列表
WinService	string	与事件关联的服务或服务组件的名称
WinServiceAccount	string	启动受控进程的帐户ID
WinServiceFileName	string	正在处理的对象的名称
WinServiceName	string	从Windows事件日志派生的对象名称
WinServicePrincipalNames	string	正在处理的对象的名称
WinServiceSid	string	用户帐户安全标识符（SID）
WinServiceStartType	string	Windows服务的启动类型
WinServiceType	string	软件检测到的对象类型
WinServiceVersion	string	正在发送的统计信息的版本
WinSessionId	string	登录会话的唯一ID
WinSessionName	string	windows事件日志事件的用户会话参数
WinSettingType	string	软件检测到的对象类型
WinSettingValue	string	正在处理的对象的文件属性
WinSeverityID	string	威胁严重级别的标识符
WinSeverityName	string	威胁严重级别的名称
WinShareLocalPath	string	正在处理对象的路径
WinShareName	string	启动受控进程的帐户ID
WinSID	string	与用户或对象相关的安全标识符（SID）
WinSidFilteringEnabled	string	来自Windows事件日志事件的安全参数

字段	类型	描述
WinSidHistory	string	用户帐户安全标识符（SID）
WinSidList	string	用户帐户安全标识符（SID）
WinSignatureType	string	威胁签名类型
WinSignatureTypeIndex	string	签名类型的索引
WinSignatureVersion	string	事件发生时的签名版本
WinSourceAddr	string	Windows事件日志事件的网络连接参数
WinSourceAddress	string	本地IP地址
WinSourceDRA	string	Windows事件日志事件的网络连接参数
WinSourceHandleId	string	来源对象的句柄ID
WinSourceID	string	事件或操作来源的标识符
WinSourceName	string	事件或操作来源的名称
WinSourcePort	string	正在处理的网络连接的来源端口号和目标端口号
WinSourceProcessId	string	来源进程ID
WinSourceSid	string	发起操作的主体的SID
WinSourceUserName	string	来源用户名
WinSpnName	string	用于身份验证的SPN（服务主体名称）
WinSSID	string	无线网络标识符（SSID）
WinStagingReason	string	将对象分阶段进行审计的原因
WinStartTime	string	事件时间
WinStartType	string	软件检测到的对象类型
WinStartUSN	string	Windows事件日志事件的网络连接参数
WinState	string	事件发生时对象或系统的状态
WinStatus	string	正在处理的对象的描述，如对象属性中所定义。
WinStatusCode	string	Windows事件日志事件的操作参数
WinStatusDescription	string	事件或操作的当前状态描述
WinStopTime	string	事件时间
WinSubcategoryGuid	string	有关用户群组的信息
WinSubcategoryId	string	对象类型代码
WinSubject	string	有关发起操作的主体信息
WinSubjectAlternativeName	string	包含备用身份的证书SAN（主题备用名称）字段
WinSubjectDomainName	string	用于验证登录会话所有者的域名
WinSubjectKeyIdentifier	string	证书主题键标识符
WinSubjectLogonId	string	用户帐户安全标识符（SID）
WinSubjectMachineName	string	代表其执行操作的计算机名称
WinSubjectMachineSID	string	执行操作的系统的计算机SID
WinSubjectUserDomainName	string	用于验证登录会话所有者的域名
WinSubjectUserName	string	启动受控进程的帐户ID
WinSubjectUserSid	string	用户帐户安全标识符（SID）
WinSubStatus	string	Windows事件日志事件的操作参数
WinTargetDomainName	string	用于验证登录会话所有者的域名
WinTargetHandleId	string	目标对象的句柄ID

字段	类型	描述
WinTargetInfo	string	正在处理的对象的描述，如对象属性中所定义。
WinTargetLinkedLogonId	string	用户帐户安全标识符（SID）
WinTargetLogonGuid	string	有关用户群组的信息
WinTargetLogonId	string	用户帐户安全标识符（SID）
WinTargetName	string	目标对象或资源的名称
WinTargetOutboundDomainName	string	用于验证登录会话所有者的域名
WinTargetOutboundUserName	string	启动受控进程的帐户ID
WinTargetProcessId	string	进程ID（PID）
WinTargetProcessName	string	正在处理的对象的名称
WinTargetServer	string	事件的目标服务器
WinTargetServerName	string	用户设备名称
WinTargetSid	string	用户帐户安全标识符（SID）
WinTargetState	string	操作后目标对象的状态
WinTargetUserDomain	string	目标用户的域
WinTargetUserName	string	启动受控进程的帐户ID
WinTargetUserSid	string	用户帐户安全标识符（SID）
WinTaskContent	string	与事件相关的预定任务的原始内容
WinTaskContentActionsContext	string	操作系统任务调度器任务参数
WinTaskContentActionsExecCommand	string	进程的命令行参数
WinTaskContentPrincipalsPrincipalid	string	用户帐户安全标识符（SID）
WinTaskContentPrincipalsPrincipalLogonType	string	登录会话类型
WinTaskContentPrincipalsPrincipalRunLevel	string	操作系统任务调度器任务参数
WinTaskContentPrincipalsPrincipalUserId	string	用户帐户安全标识符（SID）
WinTaskContentRegistrationInfoAuthor	string	启动受控进程的帐户ID
WinTaskContentRegistrationInfoDate	string	事件日期
WinTaskContentSettingsAllowHardTerminate	string	操作系统任务调度器任务参数
WinTaskContentSettingsAllowStartOnDemand	string	操作系统任务调度器任务参数
WinTaskContentSettingsDisallowStartIfOnBatteries	string	操作系统任务调度器任务参数
WinTaskContentSettingsEnabled	string	操作系统任务调度器任务参数
WinTaskContentSettingsExecutionTimeLimit	string	事件时间
WinTaskContentSettingsHidden	string	操作系统任务调度器任务参数
WinTaskContentSettingsIdleSettingsRestartOnIdle	string	操作系统任务调度器任务参数
WinTaskContentSettingsIdleSettingsStopOnIdleEnd	string	操作系统任务调度器任务参数
WinTaskContentSettingsMultipleInstancesPolicy	string	操作系统任务调度器任务参数
WinTaskContentSettingsPriority	string	操作系统任务调度器任务参数
WinTaskContentSettingsRunOnlyIfIdle	string	操作系统任务调度器任务参数
WinTaskContentSettingsRunOnlyIfNetworkAvailable	string	操作系统任务调度器任务参数
WinTaskContentSettingsStartWhenAvailable	string	操作系统任务调度器任务参数
WinTaskContentSettingsStopIfGoingOnBatteries	string	操作系统任务调度器任务参数
WinTaskContentSettingsWakeToRun	string	操作系统任务调度器任务参数
WinTaskContentTriggers	string	Windows事件日志事件中记录的任务参数

字段	类型	描述
WinTaskContentversion	string	原始内容中的任务版本
WinTaskContentNew	string	已更新定时任务的内容
WinTaskContentNewActionsContext	string	操作系统任务调度器任务参数
WinTaskContentNewActionsExecCommand	string	进程的命令行参数
WinTaskContentNewPrincipalsPrincipalid	string	用户帐户安全标识符（SID）
WinTaskContentNewPrincipalsPrincipalLogonType	string	登录会话类型
WinTaskContentNewPrincipalsPrincipalRunLevel	string	操作系统任务调度器任务参数
WinTaskContentNewPrincipalsPrincipalUserId	string	用户帐户安全标识符（SID）
WinTaskContentNewRegistrationInfoAuthor	string	启动受控进程的帐户ID
WinTaskContentNewRegistrationInfoDate	string	事件日期
WinTaskContentNewSettingsAllowHardTerminate	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsAllowStartOnDemand	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsDisallowStartIfOnBatteries	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsEnabled	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsExecutionTimeLimit	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsHidden	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsIdleSettingsRestartOnIdle	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsIdleSettingsStopOnIdleEnd	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsMultipleInstancesPolicy	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsPriority	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsRunOnlyIfIdle	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsRunOnlyIfNetworkAvailable	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsStartWhenAvailable	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsStopIfGoingOnBatteries	string	操作系统任务调度器任务参数
WinTaskContentNewSettingsWakeToRun	string	操作系统任务调度器任务参数
WinTaskContentNewTriggers	string	Windows事件日志事件中记录的任务参数
WinTaskContentNewversion	string	更新内容中的任务版本
WinTaskName	string	正在处理的对象的名称
WinTdoAttributes	string	正在处理的对象的文件属性
WinTdoDirection	string	Windows事件日志事件的网络连接参数
WinTdoType	string	软件检测到的对象类型
WinTemplateContent	string	证书模板的内容
WinTemplateDSObjectFQDN	string	Active Directory中模板对象的FQDN
WinTemplateInternalName	string	证书模板的内部名称
WinTemplateOID	string	证书模板的OID（对象标识符）
WinTemplateSchemaVersion	string	证书模板的模式版本
WinTemplateVersion	string	证书模板版本
WinTerminationTime	string	事件时间
WinTestSigning	string	指示系统上是否启用了测试签名模式的标志
WinThreatID	string	威胁标识符
WinThreatName	string	威胁名称

字段	类型	描述
WinTicketEncryptionType	string	软件检测到的对象类型
WinTicketOptions	string	Active Directory对象参数
WinTokenElevationType	string	安全令牌提升类型
WinTopLevelName	string	正在处理的对象的名称
WinTransactionId	string	对象类型代码
WinTransitionsToOn	string	对象或组件过渡到"开启"状态
WinTransmittedServices	string	Windows事件日志事件的操作参数
WinTreeDelete	string	Windows事件日志事件的其他参数
WinType	string	事件或对象的类型
WinTypeID	string	事件或威胁类型的标识符
WinTypeName	string	事件或威胁类型的名称
WinUnused	string	保留或未使用的字段
WinUnused2	string	活动未使用的其他预留字段
WinUnused3	string	活动未使用的其他预留字段
WinUnused4	string	活动未使用的其他预留字段
WinUnused5	string	活动未使用的其他预留字段
WinUnused6	string	活动未使用的其他预留字段
WinUpdateType	string	产品类型或签名更新
WinUpdateTypeIndex	string	更新类型的索引
WinUser	string	与事件关联的用户名
WinUserAccountControl	string	用户账户控制组件的属性
WinUserClaims	string	新登录会话的用户声明列表
WinUserData	string	windows事件日志事件的用户会话参数
WinUserName	string	用户名
WinUserParameters	string	启动受控进程的帐户ID
WinUserPrincipalName	string	启动受控进程的帐户ID
WinUserSid	string	与事件关联的用户的SID
WinUserUPN	string	用户的用户主体名称（UPN）
WinUserWorkstations	string	用户设备名称
WinVendorIds	string	windows事件日志事件的用户会话参数
WinVirtualAccount	string	启动受控进程的帐户ID
WinVsmLaunchType	string	虚拟安全模式（VSM）的启动类型
WinWakeFromState	string	系统被唤醒的电源状态（睡眠、休眠等）
WinWakeRequesterTypeAc	string	在交流电源上运行时唤醒请求者类型
WinWakeRequesterTypeDc	string	在直流电源上运行时唤醒请求者类型
WinWeight	string	与事件对象关联的权重或优先级
WinWorkstation	string	用户设备名称
WinWorkstationName	string	用户设备名称
WinProcessingErrorDataDataItemName	string	导致处理错误的数据项名称
WinProcessingErrorDataErrorCode	string	事件处理期间发生的错误代码
WinProcessingErrorDataEventPayload	string	导致错误的原始事件有效负载

字段	类型	描述
WinSystemChannel	string	记录事件的Windows事件日志频道
WinSystemComputer	string	生成事件的计算机名称
WinSystemEventID	string	定义系统中发生的事件类型的事件标识符
WinSystemEventIDQualifiers	string	提供有关事件的扩展信息的其他事件限定符
WinSystemEventRecordID	string	日志中的唯一记录标识符
WinSystemExecutionProcessID	string	与事件执行关联的进程标识符（PID）
WinSystemExecutionThreadID	string	触发事件的线程标识符（TID）
WinSystemKeywords	string	用于对事件进行分类和筛选的事件关键字
WinSystemLevel	string	指示其严重等级或重要等级的事件级别
WinSystemOpcode	string	描述与事件关联的操作类型的事件操作代码
WinSystemProviderEventSourceName	string	生成事件的来源名称
WinSystemProviderGuid	string	事件提供者的全局唯一标识符
WinSystemProviderName	string	事件提供者名称
WinSystemSecurityUserID	string	与事件关联的用户标识符
WinSystemTask	string	与事件关联的任务标识符
WinSystemTimeCreatedSystemTime	string	创建事件的时间戳
WinSystemVersion	string	事件模式的版本
WinAutoBackupBackupPath	string	存储自动备份的文件或文件夹路径
WinAutoBackupChannel	string	用于自动备份的通道或来源
WinEventProcessingFailureErrorCode	string	事件处理期间遇到的错误代码
WinEventProcessingFailureEventID	string	导致处理失败的事件ID
WinEventProcessingFailurePublisherID	string	尝试记录失败事件的应用程序或服务的标识符
WinEventXMLAddress	string	与事件相关的地址
WinEventXMLParam1	string	其他事件信息字段
WinEventXMLParam2	string	其他事件信息字段
WinEventXMLParam3	string	其他事件信息字段
WinEventXMLSessionID	string	与事件关联的用户会话ID
WinEventXMLSource	string	事件来源
WinEventXMLTargetSession	string	与事件相关的目标会话
WinEventXMLUser	string	与事件关联的用户
WinFileIsFull	string	日志已满且无法再接受新条目的指示符
WinLogFileClearedSubjectDomainName	string	清除事件日志的用户的域
WinLogFileClearedSubjectLogonId	string	清除事件日志的用户的登录ID
WinLogFileClearedSubjectUserName	string	清除事件日志的用户的用户名
WinLogFileClearedSubjectUserSid	string	清除事件日志的用户SID
WinOperationClientFailureClientMachine	string	发生操作失败的客户端计算机名称
WinOperationClientFailureClientProcessId	string	导致操作故障的客户端进程ID
WinOperationClientFailureComponent	string	发生操作故障的系统组件
WinOperationClientFailureId	string	操作故障的唯一标识符
WinOperationClientFailureOperation	string	故障操作的名称或描述
WinOperationClientFailurePossibleCause	string	操作故障的可能原因

字段	类型	描述
WinOperationClientFailureResultCode	string	指示成功或故障原因的操作结果代码
WinOperationClientFailureUser	string	发起故障操作的用户
WinOperationStartedOperationalCode	string	已启动操作的代码
WinOperationStartedOperationalHostProcess	string	发起操作的主机进程
WinOperationStartedOperationalProcessID	string	与已启动操作员关联的进程ID
WinOperationStartedOperationalProviderName	string	提供者或事件来源的名称
WinOperationStartedOperationalProviderPath	string	提供者或事件来源的路径
WinServiceShutdown	string	Windows服务已停止

Blocked Document

Windows和Linux操作系统均支持此事件类型。

Blocked Document 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）

字段	类型	描述
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL

字段	类型	描述
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS

字段	类型	描述
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行

字段	类型	描述
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID

字段	类型	描述
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述

字段	类型	描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Applock

Windows、 Linux和macOS操作系统均支持此事件类型。

Applock 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
ProcessUniqueid	int	进程唯一ID

字段	类型	描述
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessCalltrace	string	进程堆栈跟踪
ProcessFileLnkName	string	用于进程执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	用于进程执行的可执行文件（LNK 文件）路径（不含文件名）
ProcessFileLnkFullname	string	用于进程执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	用于进程执行的LNK文件命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限

字段	类型	描述
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）

字段	类型	描述
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS

字段	类型	描述
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）

字段	类型	描述
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表

字段	类型	描述
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Process Terminated

Windows、 Linux和macOS操作系统均支持此事件类型。

Process Terminated 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
ProcessUniqueid	int	进程唯一ID

字段	类型	描述
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessCalltrace	string	进程堆栈跟踪
ProcessFileLnkName	string	用于进程执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	用于进程执行的可执行文件（LNK 文件）路径（不含文件名）
ProcessFileLnkFullname	string	用于进程执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	用于进程执行的LNK文件命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限

字段	类型	描述
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）

字段	类型	描述
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS

字段	类型	描述
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）

字段	类型	描述
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表

字段	类型	描述
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
ProcessTerminationtime	int	进程完成时间

Device

Windows操作系统支持此事件类型。

Device 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventVersion	string	事件架构版本
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
DeviceId	string	设备ID
DeviceName	string	设备名称
DevicePath	string	设备路径
DeviceOperationtype	string	设备操作类型（例如1 - 连接）
DeviceType	string	设备类型
DeviceSystemflag	string	标记设备是否为系统设备

File System Mount

Windows和Linux操作系统均支持此事件类型。

File System Mount 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
VolumeName	string	磁盘卷名称
VolumePath	string	磁盘卷挂载点
DeviceClass	string	根据官方规范的设备类别GUID
DeviceId	string	设备ID
DeviceBustype	string	连接设备使用的总线类型
DeviceType	string	设备类型
DeviceHotpluggable	string	设备是否支持热插拔（true或false）

字段	类型	描述
DeviceSerialnumber	string	制造商设备ID
VolumeFilesystemtype	string	磁盘卷的文件系统类型
DeviceSpaceTotal	uint	磁盘总容量（MB）
DeviceSpaceUsed	uint	磁盘上的已用空间（MB）
DeviceSpaceFree	uint	磁盘上的可用空间（MB）

File System Unmount

Windows和Linux操作系统均支持此事件类型。

File System Unmount 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
VolumeName	string	磁盘卷名称
VolumePath	string	磁盘卷挂载点
DeviceClass	string	根据官方规范的设备类别GUID
DeviceId	string	设备ID
DeviceBustype	string	连接设备使用的总线类型
DeviceType	string	设备类型
DeviceHotpluggable	string	设备是否支持热插拔（true或false）

字段	类型	描述
DeviceSerialnumber	string	制造商设备ID
VolumeFilesystemtype	string	磁盘卷的文件系统类型
DeviceSpaceTotal	uint	磁盘总容量（MB）
DeviceSpaceUsed	uint	磁盘上的已用空间（MB）
DeviceSpaceFree	uint	磁盘上的可用空间（MB）

Bits Job Create

Windows操作系统支持此事件类型。

Bits Job Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
BitsjobId	string	作业标识符（GUID）

字段	类型	描述
BitsjobName	string	作业名称
BitsjobOwnerUserName	string	作业所有者的用户名
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名

字段	类型	描述
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值

字段	类型	描述
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件的名称（不包含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不包括文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名

字段	类型	描述
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Bits Job Complete

Windows操作系统支持此事件类型。

Bits Job Complete 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
BitsjobId	string	作业标识符（GUID）
BitsjobName	string	作业名称
BitsjobOwnerUserName	string	作业所有者的用户名
BitsjobUserName	string	执行操作的用户名
BitsjobFilestotal	int	作业中的文件总数
BitsjobBytestransferred	int	作业中传输的字节总数
BitsjobPeerBytestransferred	int	通过p2p传输的字节数

Bits Job Start

Windows操作系统支持此事件类型。

Bits Job Start 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
BitsjobId	string	作业标识符（GUID）
BitsjobName	string	作业名称
BitsjobTransferid	string	作业中传输文件的唯一标识符（GUID）
BitsjobRemotename	string	数据源URL
BitsjobDatasourceCreationtime	int	数据源创建时间
BitsjobDatasourceSize	int	数据源大小
BitsjobBytestotal	int	作业中的文件总数

字段	类型	描述
BitsjobBytestransferred	int	作业中传输的字节总数
BitsjobPeerHostname	int	P2P数据源的主机名
BitsjobPeerBytestransferred	int	通过p2p传输的字节数

Bits Job Stop

Windows操作系统支持此事件类型。

Bits Job Stop 事件字段

字段	类型	描述
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
BitsjobId	string	作业标识符（GUID）
BitsjobName	string	作业名称
BitsjobTransferid	string	作业中传输文件的唯一标识符（GUID）
BitsjobRemotename	string	数据源URL
BitsjobDatasourceCreationtime	int	数据源创建时间
BitsjobDatasourceSize	int	数据源大小
BitsjobBytestotal	int	作业中的文件总数
BitsjobBytestransferred	int	作业中传输的字节总数

字段	类型	描述
BitsjobResultStatuscode	int	通过BITS进行数据传输操作的结果
BitsjobResultAdditionalinfo	int	有关通过BITS进行数据传输结果的其他信息
BitsjobPeerHostname	string	P2P数据源的主机名
BitsjobPeerContextinfo	int	p2p数据源的标识信息
BitsjobPeerProtocolflags	int	用于确定计算机是否向对等体提供内容以及可以从对等体下载内容的配置标志
BitsjobPeerBytestransferred	int	通过p2p传输的字节数
BitsjobProxy	string	用于传输数据的代理服务器
BitsjobBandwidthLimit	int	BITS作业可用于下载或上传数据的最大速度
BitsjobBandwidthIgnoreonlan	int	该参数确定如果来源或目标位置位于本地网络上是否忽略速度限制

Bits Job Add File

Windows操作系统支持此事件类型。

Bits Job Add File 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
BitsjobId	string	作业标识符（GUID）

字段	类型	描述
BitsjobName	string	作业名称
BitsjobOwnerUserName	string	作业所有者的用户名
BitsjobUserName	string	执行操作的用户名
BitsjobFilestotal	int	作业中的文件总数
BitsjobRemotename	string	数据源URL
BitsjobLocalname	string	用于保存作业数据的文件的本地路径
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限

字段	类型	描述
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型

字段	类型	描述
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型

字段	类型	描述
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Bits Job Error

Windows操作系统支持此事件类型。

Bits Job Error 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
BitsjobErrorid	int	错误标识符
BitsjobId	string	作业标识符（GUID）
BitsjobName	string	作业名称
BitsjobTransferid	string	作业中传输文件的唯一标识符（GUID）
BitsjobRemotename	string	数据源URL
BitsjobDatasourceCreationtime	int	数据源创建时间
BitsjobDatasourceSize	int	数据源大小

字段	类型	描述
BitsjobBytestotal	int	作业中的总字节数
BitsjobBytestransferred	int	作业中传输的字节总数
BitsjobResultStatuscode	int	通过BITS进行数据传输操作的结果
BitsjobResultAdditionalinfo	int	有关通过BITS进行数据传输结果的其他信息
BitsjobPeerHostname	string	P2P数据源的主机名
BitsjobPeerContextinfo	int	p2p数据源的标识信息
BitsjobPeerProtocolflags	int	用于确定计算机是否向对等体提供内容以及是否可以从对等体下载内容的配置标志
BitsjobPeerBytestransferred	int	通过p2p传输的字节数
BitsjobProxy	string	用于传输数据的代理服务器
BitsjobBandwidthLimit	int	BITS作业可用于下载或上传数据的最大速度
BitsjobBandwidthIgnoreonlan	uint	该参数确定如果来源或目标位置位于本地网络上是否忽略速度限制
BitsjobOwnerUserName	string	作业所有者的用户名

Service Create

Windows和Linux操作系统均支持此事件类型。

Service Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值

字段	类型	描述
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileAttr	int	文件系统属性
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
ServiceTitle	string	服务名称，服务的唯一标识符
ServiceType	string	服务类型
ServiceStarttype	string	服务启动类型
ServiceCmdline	string	已启动服务的命令行
ServiceLoadordergroup	string	此服务的加载顺序群组名称
ServiceTagid	uint	ServiceLoadOrderGroup中此服务的唯一标签值
ServiceDependencies	string	必须在此服务之前启动的加载顺序群组名称或服务名称
ServiceStartname	string	启动服务的帐户名称
ServiceDisplayname	string	服务的显示名称
ServiceDeletedelayed	uint	延迟删除标志。1 - 服务将在停止时删除；0 - 服务将立即删除。对于“服务创建”事件，此字段为可选字段。
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessProperties	string	运行该进程的帐户属性列表
ProcessIntegritylevel	int	进程完整性级别
ProcessUserName	string	执行进程的域和用户名
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ParentProcessUniqueid	int	父进程唯一ID

字段	类型	描述
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessUserName	string	执行父进程的域和用户名
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessProperties	string	运行父进程的帐户属性列表
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表

Service Modify

Windows和Linux操作系统均支持此事件类型。

Service Modify 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间

字段	类型	描述
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileAttr	int	文件系统属性
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
ServiceTitle	string	服务名称，服务的唯一标识符
ServiceType	string	服务类型
ServiceStarttype	string	服务启动类型
ServiceCmdline	string	已启动服务的命令行
ServiceLoadordergroup	string	此服务的加载顺序群组名称
ServiceTagid	uint	ServiceLoadOrderGroup中此服务的唯一标签值
ServiceDependencies	string	必须在此服务之前启动的加载顺序群组名称或服务名称
ServiceStartname	string	启动服务的帐户名称
ServiceDisplayname	string	服务的显示名称
ServiceOldType	string	修改前服务类型
ServiceOldStarttype	string	修改前服务的启动类型
ServiceOldCmdline	string	服务修改前可执行文件的路径
ServiceOldLoadordergroup	string	修改前此服务的加载顺序群组名称
ServiceOldTagid	uint	修改前此服务在ServiceLoadOrderGroup中的唯一标签值
ServiceOldDependencies	string	必须在此服务之前启动的加载顺序群组名称或服务名称（服务修改前）
ServiceOldStartname	string	服务修改前启动此服务的帐户名称
ServiceOldDisplayname	string	服务修改前显示的服务名称
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessProperties	string	运行该进程的帐户属性列表
ProcessIntegritylevel	int	进程完整性级别
ProcessUserName	string	执行进程的域和用户名
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称

字段	类型	描述
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessUserName	string	执行父进程的域和用户名
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessProperties	string	运行父进程的帐户属性列表
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表

Service Delete

Windows和Linux操作系统均支持此事件类型。

Service Delete 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
FileName	string	文件的名称（不含文件路径）
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值

字段	类型	描述
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileType	string	文件的类型
FileAttr	int	文件系统属性
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
ServiceTitle	string	服务名称，服务的唯一标识符
ServiceType	string	服务类型
ServiceStarttype	string	服务启动类型
ServiceCmdline	string	已启动服务的命令行
ServiceLoadordergroup	string	此服务的加载顺序群组名称
ServiceTagid	uint	ServiceLoadOrderGroup中此服务的唯一标签值
ServiceDependencies	string	必须在此服务之前启动的加载顺序群组名称或服务名称
ServiceStartname	string	启动服务的帐户名称
ServiceDisplayname	string	服务的显示名称
ServiceDeletedelayed	uint	延迟删除标志。1 - 服务将在停止时删除；0 - 服务将立即删除。对于“服务创建”事件，此字段为可选字段。
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessProperties	string	运行该进程的帐户属性列表
ProcessIntegritylevel	int	进程完整性级别
ProcessUserName	string	执行进程的域和用户名
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ParentProcessUniqueid	int	父进程唯一ID

字段	类型	描述
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessUserName	string	执行父进程的域和用户名
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessProperties	string	运行父进程的帐户属性列表
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表

Scheduled Task Create

Windows和Linux操作系统均支持此事件类型。

Scheduled Task Create 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
TaskName	string	任务名称，服务唯一标识符

字段	类型	描述
TaskAuthorName	string	任务作者的用户名
TaskUserName	string	启动服务的用户名
TaskUserId	int	启动服务的用户标识符仅适用于Linux/Mac OS
TaskUserSid	string	启动服务的用户SID仅适用于Windows
TaskRunlevel	string	任务运行的权限级别
TaskCreationtime	int	创建任务的日期和时间
TaskCmdline	string	任务中执行的操作
TaskEnabled	string	标记任务是否已启用
TaskHidden	string	标记任务是否隐藏
TaskLocation	string	操作系统中任务对象的路径
TaskSchedule	string	任务运行计划
TaskSource	string	任务来源
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间

字段	类型	描述
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别

字段	类型	描述
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志

字段	类型	描述
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称

字段	类型	描述
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称

字段	类型	描述
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Scheduled Task Modify

此事件类型支持 Windows（Windows Vista、Windows Server 2008 及更高版本）和 Linux 操作系统。

Scheduled Task Modify 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
TaskName	string	任务名称，服务唯一标识符

字段	类型	描述
TaskAuthorName	string	任务作者的用户名
TaskUserName	string	启动服务的用户名
TaskUserSid	string	启动服务的用户SID仅适用于Windows
TaskRunlevel	string	任务运行的权限级别
TaskCreationtime	int	创建任务的日期和时间
TaskCmdline	string	任务中执行的操作
TaskEnabled	string	标记任务是否已启用
TaskHidden	string	标记任务是否隐藏
TaskLocation	string	操作系统中任务对象的路径
TaskSchedule	string	任务运行计划
TaskSource	string	任务来源
TaskOldUserName	string	启动服务的先前用户名称
TaskOldUserSid	string	运行任务的先前用户SID
TaskOldEnabled	string	指示任务是否已启用的标记的先前值
TaskOldHidden	string	指示任务是否隐藏的标记的先前值
TaskOldRunlevel	string	任务运行权限的先前级别
TaskOldCmdline	string	任务中执行的先前操作
TaskOldSchedule	string	先前的任务执行计划
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值

字段	类型	描述
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段

字段	类型	描述
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值

字段	类型	描述
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值

字段	类型	描述
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Scheduled Task Delete

Windows和Linux操作系统均支持此事件类型。

Scheduled Task Delete 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
TaskName	string	任务名称，服务唯一标识符

字段	类型	描述
TaskAuthorName	string	任务作者的用户名
TaskUserName	string	启动服务的用户名
TaskUserId	int	启动服务的用户标识符仅适用于Linux/Mac OS
TaskUserSid	string	启动服务的用户SID仅适用于Windows
TaskRunlevel	string	任务运行的权限级别
TaskCreationtime	int	创建任务的日期和时间
TaskCmdline	string	任务中执行的操作
TaskEnabled	string	标记任务是否已启用
TaskHidden	string	标记任务是否隐藏
TaskLocation	string	操作系统中任务对象的路径
TaskSchedule	string	任务运行计划
TaskSource	string	任务来源
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间

字段	类型	描述
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值

字段	类型	描述
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行

字段	类型	描述
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间

字段	类型	描述
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名

字段	类型	描述
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Owner Change

此事件类型支持 Windows 和 Linux 操作系统，但 Windows XP x64、Windows Server 2003 x64 以及内核版本早于 4.19.* 的 Linux 除外。

File Owner Change 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳

字段	类型	描述
FileOldOwnerUserName	string	先前文件所有者的域用户名
FileOldOwnerGroupName	string	先前文件所有者的域群组名称
FileName	string	文件的名称（不含文件路径）
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群组名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群组ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径

字段	类型	描述
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false

字段	类型	描述
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址

字段	类型	描述
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间

字段	类型	描述
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS

字段	类型	描述
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

File ACL Change

此事件类型支持 Windows 和 Linux 操作系统，但 Windows XP x64、Windows Server 2003 x64 以及内核版本早于 4.19.* 的 Linux 除外。

File ACL Change 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳

字段	类型	描述
FileDacl	string	文件的DACL中定义的访问控制条目列表
FileOldDacl	string	文件的DACL中定义的访问控制条目的先前列表
FileModifiedDacl	string	文件的DACL中已修改条目的列表
FileSacl	string	文件的SACL中定义的访问控制条目列表
FileOldSacl	string	文件的SACL中定义的访问控制条目的先前列表
FileModifiedSacl	string	文件的SACL中已修改条目的列表
FileName	string	文件的名称（不含文件路径）
FilePath	string	文件的完整路径（不含文件名）
FileFullname	string	文件的完整路径
FileMd5	string	文件内容的MD5哈希值
FileSha256	string	文件内容的SHA256哈希值
FileSize	int	文件的大小（以字节为单位）
FileCreationtime	int	文件的创建时间
FileModificationtime	int	文件上次修改时间
FileOwnerUserId	int	文件所有者用户ID。适用于Linux和macOS
FileOwnerUserName	string	文件所有者用户名。适用于Linux和macOS
FileOwnerGroupName	string	文件所有者群组名称。适用于Linux和macOS
FileOwnerGroupId	int	文件所有者群组ID。适用于Linux和macOS
FileType	string	文件的类型
FileCapPermitted	string	文件的允许权限
FileCapInheritable	string	文件的可继承权限
FileCapEffective	string	文件的有效权限
FileOpenflags	string	指定的打开标志（例如 O_RDWR | O_APPEND），用于创建/修改/读取操作。
FileAttrModificationtime	int	上次修改文件属性时
FileAttr	int	文件系统属性
FileZoneidentifier	int	从文件的备用流Zone.Identifier获取的区域ID
FileProductname	string	文件的VERSIONINFO资源的产品名称值
FileProductvendor	string	文件的VERSIONINFO资源的公司名称值
FileDescription	string	文件的VERSIONINFO资源中的描述
FileOriginalname	string	文件的VERSIONINFO资源的原始文件名
FileSignSubjectname	string	关于签署文件的组织的信息
FileSignResult	string	签名验证结果：通过 - true，不通过 - false
FileSignTimestamp	int	文件签署的日期和时间
FileUrl	string	下载文件的URL
FileEmailSrcAddress	string	文件作为附件接收的发件人地址
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量

字段	类型	描述
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名

字段	类型	描述
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。

字段	类型	描述
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。

字段	类型	描述
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型

字段	类型	描述
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Owner Change

此事件类型支持 Windows 操作系统，但 Windows XP x64 和 Windows Server 2003 x64 除外。

Registry Owner Change 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称
RegOwnerUserName	string	密钥注册表所有者的域用户名

字段	类型	描述
RegOldOwnerUserName	string	先前密钥注册所有者的域名用户名
RegOwnerGroupName	string	密钥注册表所有者的域群组名称
RegOldOwnerGroupName	string	先前密钥注册所有者的域群组名称
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本

字段	类型	描述
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID

字段	类型	描述
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID

字段	类型	描述
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID

字段	类型	描述
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

字段	类型	描述
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry ACL Change

此事件类型支持 Windows 操作系统，但 Windows XP x64 和 Windows Server 2003 x64 除外。

Registry ACL Change 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
RegKeyName	string	受此操作影响的注册表项的完整路径和名称

字段	类型	描述
RegDacl	string	注册表项的DACL中定义的访问控制条目列表
RegOldDacl	string	注册表项的DACL中定义的访问控制条目的先前列表
RegModifiedDacl	string	注册表项的DACL中已修改条目的列表
RegSacl	string	SACL注册表项中的访问控制条目列表
RegOldSacl	string	注册表项的SACL中定义的访问控制条目的先前列表
RegModifiedSacl	string	注册表项的SACL中已修改条目的列表
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限

字段	类型	描述
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型

字段	类型	描述
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型

字段	类型	描述
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型

字段	类型	描述
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Executable Memory Mapped

Linux操作系统支持此事件类型。

Executable Memory Mapped 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
SyscallArgs	string	系统调用参数仅适用于Linux

字段	类型	描述
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	LNK文件的命令行
ProcessFileLnkMd5	string	已执行的LNK文件的MD5哈希值
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	已执行进程的文件名（不含路径）
ProcessFilePath	string	可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	已执行进程的文件大小（以字节为单位）
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	当前进程的可执行文件的上次修改时间
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	执行文件的MD5哈希值
ProcessFileSha256	string	父进程可执行文件的SHA256哈希值
ProcessFileAttr	int	启动进程的可执行文件的文件系统属性列表
ProcessFileType	string	已执行进程的文件类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	进程可执行文件作为附件接收的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限

字段	类型	描述
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	签发证书的实体（个人或组织）名称
ProcessLogonType	string	执行进程的用户的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	string	启动进程的用户的帐户类型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	启动进程的用户登录的远程主机的完全限定域名（FQDN）
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）

字段	类型	描述
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	string	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS

字段	类型	描述
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	string	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）

字段	类型	描述
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	string	运行下载器进程的帐户属性列表

字段	类型	描述
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

Agent Start

Windows、 Linux和macOS操作系统均支持此事件类型。

Agent Start 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
InitiatorId	string	事件发起程序标识符
InitiatorName	string	事件发起程序名称
InitiatorType	string	事件发起程序类型
AgentInstanceid	string	唯一代理程序运行标识符
ProcessId	int	进程ID
ProcessUniqueid	int	进程唯一ID

Agent Stop

Windows、 Linux和macOS操作系统均支持此事件类型。

Agent Stop 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
InitiatorId	string	事件发起程序标识符
InitiatorName	string	事件发起程序名称
InitiatorType	string	事件发起程序类型
AgentInstanceid	string	唯一代理程序运行标识符
ProcessId	int	代理程序进程ID
ProcessUniqueid	int	代理程序进程唯一ID

字段	类型	描述
AgentStopreason	string	代理程序终止原因
AgentExitcode	int	代理程序进程退出代码

Agent Install

Windows、 Linux和macOS操作系统均支持此事件类型。

Agent Install 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
InitiatorId	string	事件发起程序标识符
InitiatorName	string	事件发起程序名称
InitiatorType	string	事件发起程序类型

Agent Uninstall

Windows、 Linux和macOS操作系统均支持此事件类型。

Agent Uninstall 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
InitiatorId	string	事件发起程序标识符
InitiatorName	string	事件发起程序名称
InitiatorType	string	事件发起程序类型

Agent Action

Windows、 Linux和macOS操作系统均支持此事件类型。

Agent Action 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
InitiatorId	string	事件发起程序标识符

字段	类型	描述
InitiatorName	string	事件发起程序名称
InitiatorType	string	事件发起程序类型
AgentInstanceid	string	唯一代理程序运行标识符
ProcessId	int	代理程序进程ID
ProcessUniqueid	int	代理程序进程唯一ID
AgentActionType	string	代理程序中执行的操作类型：0 → SelfProtectionDisabled,1 → SelfProtectionEnabled,2 → SelfProtectionTriggered,3 → PasswordProtectionOn,4 → PasswordProtectionOff,5 → CheckedPermission,Otherwise → Unknown
AgentActionDescription	string	执行操作的描述
AgentResultcode	int	执行操作的结果代码

System Startup

Windows、 Linux和macOS操作系统均支持此事件类型。

System Startup 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳

System Shutdown

Windows、 Linux和macOS操作系统均支持此事件类型。

System Shutdown 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows、 Linux、 macOS）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	事件生成的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装程序的产品版本
AgentKdbTimestamp	int	组件更新KDB的时间戳
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳

Connection Close

启用 `Connection Close` 事件可能会显著增加受保护设备的资源使用。

Windows和Linux操作系统均支持此事件类型。

Connection Close 事件字段

字段	类型	描述
IoAId	string array	攻击指标唯一ID
IoAName	string array	攻击指标的名称
IoAVersion	integer array	攻击版本指标
IoAAlert	string array	提高警觉性的属性
IoAConfidence	string array	攻击指标检测置信度等级（高、中、低）
IoASeverity	string array	攻击指标严重程度等级（高、中、低）
IoATactics	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix政策
IoATechniques	string array	当前攻击指标所映射的MITRE ATT&CK® Matrix技术
IoAEventIds	string array	与当前攻击指标相关的事件ID列表
IoAEventCount	integer array	与当前攻击指标相关的事件计数
IoASB	string array	根据攻击逻辑指标，发送到沙盒的文件的完整路径
EventType	string	通知类型
EventId	string	唯一事件ID
EventTimestamp	int	客户端上的日期和时间（原为UTC时间）
EventReceivedtimestamp	int	服务器收到通知的日期和时间
EventSequenceid	int	已发送事件的序列号
HostId	string	主机唯一标识符
HostKscId	string	通过KSC进行管理的主机ID
HostMdrId	string	MDR解决方案中的受保护主机ID
HostOsmpId	string	与受保护主机关联的基于 OSMP 的 XDR 解决方案服务器的标识符列表
HostOsFamily	string	操作系统系列（Windows和Linux）
HostOsName	string	操作系统名称
HostOsVersion	string	操作系统版本
HostName	string	生成事件的主机名
HostIp	string	主机的IP地址
AgentVersion	string	计算机上安装的产品
AgentKdbTimestamp	int	组件更新KDB的时间戳

字段	类型	描述
AgentSw2Timestamp	int	组件更新sw2基础版的时间戳
AgentIndexTimestamp	int	所有组件上次基础更新的时间戳
NetSrcIp	string	来源的IPv4/IPv6地址
NetSrcPort	int	源端口号
NetDstIp	string	目标位置的IPv4/IPv6地址
NetDstPort	int	目标位置的端口号
NetProtocol	string	IP协议
NetDirection	string	网络连接方向（入站、出站）
NetCreationtime	int	连接的创建时间
NetBytessent	int	连接期间发送的字节数
NetBytesreceived	int	连接期间接收的字节数
NetDuration	int	连接持续时间（秒）
ProcessUniqueid	int	进程唯一ID
ProcessId	int	进程ID
ProcessCmdline	string	进程的命令行
ProcessCreationflags	string	进程创建标志列表
ProcessDirectory	string	进程初始目录
ProcessEnvironment	string	环境变量
ProcessProperties	string	运行该进程的帐户属性列表
ProcessFileLnkName	string	已执行的LNK文件名（不含路径）
ProcessFileLnkPath	string	已执行的LNK文件的完整路径（不含文件名）
ProcessFileLnkFullname	string	已执行的LNK文件的完整路径
ProcessFileLnkCmdline	string	可执行LNK文件的命令行
ProcessFileLnkMd5	string	执行的LNK文件的MD5哈希值。
ProcessFileLnkSha256	string	已执行的LNK文件的SHA256哈希值。
ProcessIntegritylevel	int	进程完整性级别
ProcessType	string	进程的类型
ProcessUserRealid	int	真实用户ID适用于Linux和macOS
ProcessGroupRealid	int	真实用户群组ID。适用于Linux和macOS
ProcessUserRealname	string	真实用户名。适用于Linux和macOS
ProcessGroupRealname	string	真实群组名称。适用于Linux和macOS
ProcessUserEffectiveid	int	有效的用户ID。适用于Linux和macOS
ProcessGroupEffectiveid	int	有效的用户群组ID。适用于Linux和macOS
ProcessUserEffectivename	string	有效的用户名映射。适用于Linux和macOS
ProcessGroupEffectivename	string	有效的群组名映射。适用于Linux和macOS
ProcessFileName	string	进程可执行文件名（不含路径）
ProcessFilePath	string	进程可执行文件的完整路径（不含文件名）
ProcessFileFullname	string	进程可执行文件的完整路径
ProcessFileSize	int	进程可执行文件的大小（以字节为单位）。
ProcessFileCreationtime	int	进程可执行文件的创建时间
ProcessFileModificationtime	int	进程可执行文件的上次修改时间

字段	类型	描述
ProcessFileAttrModificationtime	int	进程可执行文件的上次修改时间
ProcessFileMd5	string	进程可执行文件的MD5哈希值。
ProcessFileSha256	string	进程可执行文件的SHA256哈希值。
ProcessFileAttr	int	进程可执行文件的文件系统属性列表
ProcessFileType	string	进程可执行文件的类型
ProcessFileUrl	string	进程可执行文件的下载URL
ProcessFileEmailSrcAddress	string	作为附件接收进程可执行文件的发件人地址
ProcessFileOwnerUserId	int	文件所有者用户ID
ProcessFileOwnerGroupId	int	文件所有者群组ID
ProcessFileOwnerUserName	string	文件所有者用户名
ProcessFileOwnerGroupName	string	文件所有者组名称
ProcessFileCapPermitted	string	进程可执行文件的允许权限
ProcessFileCapInheritable	string	进程可执行文件的可继承权限
ProcessFileCapEffective	string	进程可执行文件的有效权限
ProcessFileZoneidentifier	int	由与文件连接的备用流Zone.Identifier提供的区域ID
ProcessFileProductname	string	VERSIONINFO资源中的应用程序名称
ProcessFileProductversion	string	VERSIONINFO资源中的应用程序版本
ProcessFileOriginalname	string	VERSIONINFO资源中的原始文件名
ProcessFileProductvendor	string	VERSIONINFO资源中的公司名称
ProcessFileDescription	string	VERSIONINFO资源中的描述
ProcessFileVersion	string	VERSIONINFO资源中的文件版本
ProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ProcessFileSignTimestamp	int	文件签署的日期和时间
ProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ProcessLogonType	string	进程的登录会话类型
ProcessLogonSessionId	int	进程访问令牌中的登录会话ID
ProcessUserType	int	运行进程的帐户属性列表
ProcessUserName	string	执行进程的域和用户名
ProcessLogonUserId	int	登录用户ID。适用于Linux和macOS
ProcessLogonHostName	string	登录远程主机/IP。适用于Linux和macOS
ParentProcessUniqueid	int	父进程唯一ID
ParentProcessId	int	父进程ID
ParentProcessCmdline	string	父进程的命令行
ParentProcessCreationflags	string	父进程的创建标志
ParentProcessDirectory	string	父进程的当前工作目录。适用于Linux和macOS
ParentProcessFileLnkName	string	启动父进程的LNK文件名称（不含路径）
ParentProcessFileLnkPath	string	启动父进程的LNK文件的完整路径（不含名称）
ParentProcessFileLnkFullname	string	启动父进程的LNK文件的完整路径
ParentProcessFileLnkCmdline	string	启动父进程的LNK文件的命令行
ParentProcessFileLnkMd5	string	启动父进程的LNK文件的MD5哈希值
ParentProcessFileLnkSha256	string	启动父进程的LNK文件的SHA256哈希值

字段	类型	描述
ParentProcessIntegritylevel	int	父进程的完整性级别
ParentProcessType	string	父进程的类型
ParentProcessUserRealid	int	启动父进程的用户的真实用户ID。适用于Linux和macOS
ParentProcessGroupRealid	int	启动父进程的用户的真实用户群组ID。适用于Linux和macOS
ParentProcessUserRealname	string	启动父进程的用户的真实用户名。适用于Linux和macOS
ParentProcessGroupRealname	string	启动父进程的用户的真实群组名称。适用于Linux和macOS
ParentProcessUserEffectiveid	int	启动父进程的用户的有效用户ID。Auditd引用字段
ParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
ParentProcessUserEffectivename	string	启动父进程的用户的有效用户名。Auditd引用字段
ParentProcessGroupEffectivename	string	启动父进程的用户的有效群组名称。Auditd引用字段
ParentProcessFileName	string	父进程可执行文件的名称（不含路径）
ParentProcessFilePath	string	父进程可执行文件的完整路径（不含文件名）
ParentProcessFileFullname	string	父进程可执行文件的完整路径
ParentProcessFileCreationtime	int	父进程可执行文件的创建时间
ParentProcessFileModificationtime	int	父进程可执行文件的上次修改时间
ParentProcessFileAttrModificationtime	int	父进程可执行文件属性的上次修改时间
ParentProcessFileMd5	string	父进程可执行文件的MD5哈希值。
ParentProcessFileSha256	string	父进程可执行文件的SHA256哈希值。
ParentProcessFileAttr	int	父进程可执行文件的文件系统属性列表
ParentProcessFileType	string	父进程可执行文件的类型
ParentProcessFileUrl	string	父进程可执行文件的下载URL
ParentProcessFileEmailSrcAddress	string	作为附件接收父进程可执行文件的发件人地址
ParentProcessFileOwnerUserId	int	父进程可执行文件所有者的用户ID
ParentProcessFileOwnerGroupId	int	父进程可执行文件所有者的群组ID
ParentProcessFileOwnerUserName	string	父进程可执行文件的所有者的用户名
ParentProcessFileOwnerGroupName	string	父进程可执行文件的所有者的群组名称
ParentProcessFileCapEffective	string	父进程可执行文件的有效权限
ParentProcessFileProductname	string	父进程可执行文件的VERSIONINFO资源中的产品名称值
ParentProcessFileOriginalname	string	父进程可执行文件的VERSIONINFO资源中的原始文件名
ParentProcessFileProductvendor	string	父进程可执行文件的VERSIONINFO资源中的公司名称值
ParentProcessFileDescription	string	父进程可执行文件的VERSIONINFO资源中的描述
ParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
ParentProcessFileSignTimestamp	int	文件签署的日期和时间
ParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
ParentProcessLogonType	string	父进程的登录会话类型
ParentProcessLogonSessionId	int	父进程的访问令牌中的登录会话ID
ParentProcessProperties	int	运行父进程的帐户属性列表
ParentProcessUserName	string	执行父进程的域和用户名
GrandParentProcessUniqueid	int	祖父进程的唯一进程ID
GrandParentProcessId	int	祖父进程ID
GrandParentProcessCmdline	string	祖父进程的命令行

字段	类型	描述
GrandParentProcessCreationflags	string	祖父进程的创建标志
GrandParentProcessDirectory	string	祖父进程的当前工作目录。Linux或macOS特定字段
GrandParentProcessFileLnkName	string	启动祖父进程的LNK文件名（不含路径）
GrandParentProcessFileLnkPath	string	启动祖父进程的LNK文件的完整路径（不含文件名）
GrandParentProcessFileLnkFullname	string	启动祖父进程的LNK文件的完整路径
GrandParentProcessFileLnkCmdline	string	启动祖父进程的LNK文件命令行
GrandParentProcessFileLnkMd5	string	启动祖父进程的LNK文件的MD5哈希值
GrandParentProcessFileLnkSha256	string	启动祖父进程的LNK文件的SHA256哈希值
GrandParentProcessIntegritylevel	int	祖父进程的完整性级别
GrandParentProcessType	string	祖父进程的类型
GrandParentProcessUserRealid	int	发起祖父进程的用户的真实用户ID。适用于Linux和macOS
GrandParentProcessGroupRealid	int	发起祖父进程的用户的真实用户群组ID。适用于Linux和macOS
GrandParentProcessUserRealname	string	发起祖父进程的用户的真实用户名。适用于Linux和macOS
GrandParentProcessGroupRealname	string	发起祖父进程的用户的真实群组名称。适用于Linux和macOS
GrandParentProcessUserEffectiveid	int	发起祖父进程的用户的有效用户ID。Auditd引用字段
GrandParentProcessGroupEffectiveid	int	启动父进程的用户的有效群组ID。Auditd引用字段
GrandParentProcessUserEffectivename	string	发起祖父进程的用户的有效用户名。Auditd引用字段
GrandParentProcessGroupEffectivename	string	发起祖父流程的用户的有效群组名称。Auditd引用字段
GrandParentProcessFileName	string	祖父进程可执行文件的名称（不含路径）
GrandParentProcessFilePath	string	祖父进程可执行文件的完整路径（不含文件名）
GrandParentProcessFileFullname	string	祖父进程可执行文件的完整路径
GrandParentProcessFileCreationtime	int	祖父进程可执行文件的创建时间
GrandParentProcessFileModificationtime	int	祖父进程可执行文件的上次修改时间
GrandParentProcessFileAttrModificationtime	int	祖父进程可执行文件属性的上次修改时间
GrandParentProcessFileMd5	string	祖父进程可执行文件的MD5哈希值
GrandParentProcessFileSha256	string	祖父进程可执行文件的SHA256哈希值
GrandParentProcessFileAttr	int	祖父进程可执行文件的文件系统属性列表
GrandParentProcessFileType	string	祖父进程可执行文件的类型
GrandParentProcessFileUrl	string	祖父进程可执行文件的下载URL
GrandParentProcessFileEmailSrcAddress	string	作为附件接收祖父进程可执行文件的发件人地址
GrandParentProcessFileOwnerUserId	int	祖父进程可执行文件所有者的用户ID
GrandParentProcessFileOwnerGroupId	int	祖父进程可执行文件所有者的群组ID
GrandParentProcessFileOwnerUserName	string	祖父进程可执行文件所有者的用户名
GrandParentProcessFileOwnerGroupName	string	祖父进程可执行文件所有者的群组名称
GrandParentProcessFileCapEffective	string	祖父进程可执行文件的有效权限
GrandParentProcessFileProductname	string	祖父进程可执行文件的VERSIONINFO资源中的产品名称值
GrandParentProcessFileOriginalname	string	祖父进程可执行文件的VERSIONINFO资源中的原始文件名
GrandParentProcessFileProductvendor	string	祖父进程可执行文件的VERSIONINFO资源中的公司名称值
GrandParentProcessFileDescription	string	祖父进程可执行文件的VERSIONINFO资源中的描述
GrandParentProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
GrandParentProcessFileSignTimestamp	int	文件签署的日期和时间

字段	类型	描述
GrandParentProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
GrandParentProcessLogonType	string	祖父进程的登录会话类型
GrandParentProcessLogonSessionId	int	祖父进程的访问令牌的登录会话ID
GrandParentProcessProperties	int	运行祖父进程的帐户属性列表
GrandParentProcessUserName	string	执行祖父进程的域名和用户名
DownloaderProcessUniqueid	int	下载器进程唯一ID
DownloaderProcessId	int	下载器进程ID
DownloaderProcessCmdline	string	下载器进程的命令行
DownloaderProcessCreationflags	string	下载器进程的创建标志
DownloaderProcessDirectory	string	下载器进程的当前工作目录。Linux或macOS特定字段
DownloaderProcessFileLnkName	string	启动下载器进程的LNK文件名（不含路径）
DownloaderProcessFileLnkPath	string	启动下载器进程的LNK文件的完整路径（不含文件名）
DownloaderProcessFileLnkFullname	string	启动下载器程序的LNK文件的完整路径
DownloaderProcessFileLnkCmdline	string	启动下载器进程的LNK文件命令行
DownloaderProcessFileLnkMd5	string	启动下载器进程的LNK文件的MD5哈希值
DownloaderProcessFileLnkSha256	string	启动下载器进程的LNK文件的SHA256哈希值
DownloaderProcessIntegritylevel	int	下载器进程的完整性级别
DownloaderProcessType	string	下载器进程的类型
DownloaderProcessUserRealid	int	启动下载器进程的用户的真实用户ID。适用于Linux和macOS
DownloaderProcessGroupRealid	int	启动下载器进程的用户的真实用户群组ID。适用于Linux和macOS
DownloaderProcessUserRealname	string	启动下载器进程的用户的真实用户名。适用于Linux和macOS
DownloaderProcessGroupRealname	string	启动下载器进程的用户的真实群组名称。适用于Linux和macOS
DownloaderProcessUserEffectiveid	int	启动下载器进程的用户的有效用户ID。Auditd引用字段
DownloaderProcessGroupEffectiveid	int	启动下载器进程的用户的有效群组ID。Auditd引用字段
DownloaderProcessUserEffectivename	string	启动下载器进程的用户的有效用户名。Auditd引用字段
DownloaderProcessGroupEffectivename	string	启动下载器进程的用户的有效群组名称。Auditd引用字段
DownloaderProcessFileName	string	下载器进程可执行文件的名称（不含路径）
DownloaderProcessFilePath	string	下载器进程可执行文件的完整路径（不含文件名）
DownloaderProcessFileFullname	string	下载器进程可执行文件的完整路径
DownloaderProcessFileCreationtime	int	下载器进程可执行文件的创建时间
DownloaderProcessFileModificationtime	int	下载器进程可执行文件的上次修改时间
DownloaderProcessFileAttrModificationtime	int	下载器进程可执行文件属性的上次修改时间
DownloaderProcessFileMd5	string	下载器进程可执行文件的MD5哈希值。
DownloaderProcessFileSha256	string	下载器进程可执行文件的SHA256哈希值。
DownloaderProcessFileAttr	int	下载器进程可执行文件的文件系统属性列表
DownloaderProcessFileType	string	下载器进程可执行文件的类型
DownloaderProcessFileUrl	string	下载器进程可执行文件的下载URL
DownloaderProcessFileEmailSrcAddress	string	作为附件接收下载器进程可执行文件的发件人地址
DownloaderProcessFileOwnerUserId	int	下载器进程可执行文件所有者的用户ID
DownloaderProcessFileOwnerGroupId	int	下载器进程可执行文件所有者的群组ID
DownloaderProcessFileOwnerUserName	string	下载器进程可执行文件所有者的用户名

字段	类型	描述
DownloaderProcessFileOwnerGroupName	string	下载器进程可执行文件所有者的群组名称
DownloaderProcessFileCapEffective	string	下载器进程可执行文件的有效权限
DownloaderProcessFileProductname	string	下载器进程可执行文件的VERSIONINFO资源中的产品名称值
DownloaderProcessFileOriginalname	string	下载器进程可执行文件的VERSIONINFO资源中的原始文件名
DownloaderProcessFileProductvendor	string	下载器进程可执行文件的VERSIONINFO资源中的公司名称值
DownloaderProcessFileDescription	string	下载器进程可执行文件的VERSIONINFO资源中的描述
DownloaderProcessFileSignResult	string	签名验证结果：通过 - true，不通过 - false
DownloaderProcessFileSignTimestamp	int	文件签署的日期和时间
DownloaderProcessFileSignSubjectname	string	用于签署文件的证书的主题名称
DownloaderProcessLogonType	string	下载器进程的登录会话类型
DownloaderProcessLogonSessionId	int	下载器进程的访问令牌中的登录会话ID
DownloaderProcessProperties	int	运行下载器进程的帐户属性列表
DownloaderProcessUserName	string	执行下载器进程的域名和用户名
CreatorProcessUniqueid	int	当前进程的实际发起进程的唯一ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessId	int	当前进程的实际发起进程的ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCmdline	string	当前进程的实际发起进程的命令行。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessCreationflags	string	当前进程的实际发起进程的创建标志。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessDirectory	string	ParentProcess*字段表示当前进程的实际发起进程的当前工作目录。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkName	string	当前进程的实际发起进程的LNK文件的名称（不包含路径）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkPath	string	当前进程的实际发起进程的LNK文件的完整路径（不包含名称）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkFullname	string	当前进程的实际发起进程的LNK文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkCmdline	string	当前进程的实际发起进程的LNK文件的命令行参数。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkMd5	string	当前进程的实际发起进程的LNK文件的MD5哈希值通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileLnkSha256	string	当前进程的实际发起进程的LNK文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessIntegritylevel	int	当前进程的实际发起进程的完整性级别。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessType	string	当前进程的实际发起进程的进程的类型。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealid	int	当前进程的实际发起者的真实用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessGroupRealid	int	当前进程的实际发起者（即启动该进程的用户）的实际群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserRealname	string	当前进程的实际发起者（即启动该进程的用户）的实际用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessGroupRealname	string	当前进程的实际发起者的实际群组。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效用户ID。适用于Linux和macOS通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	当前进程的实际发起者（即启动该进程的用户）的有效群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserEffectivename	string	当前进程的实际发起者的有效用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	当前进程的实际发起者的有效群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileName	string	当前进程的实际发起进程的可执行文件的名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	当前进程的实际发起进程的可执行文件的完整路径（不包含文件名）。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileFullname	string	当前进程的实际发起进程的可执行文件的完整路径。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	当前进程的实际发起进程的可执行文件的创建时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	当前进程的实际发起进程的可执行文件的修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	当前进程的实际发起进程的可执行文件的属性修改时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	当前进程的实际发起进程的可执行文件的MD5哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	当前进程的实际发起进程的可执行文件的SHA256哈希值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	当前进程的实际发起进程的文件系统属性列表。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	当前进程的实际发起进程的类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileUrl	string	当前进程的实际发起进程的URL。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作为附件接收可执行文件的发件人地址，即当前进程的实际发起者。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserId	int	当前进程的实际发起进程文件的所有者用户ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段

字段	类型	描述
CreatorProcessFileOwnerGroupId	int	当前进程的实际发起进程文件的所有者群组ID。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerUserName	string	当前进程的实际发起者进程文件的所有者用户名。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	当前进程的实际发起者进程文件的所有者群组名称。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileCapEffective	string	当前进程的实际发起者进程的有效性能。适用于Linux和macOS通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的产品名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileOriginalname	string	当前进程的实际发起进程文件的VERSIONINFO资源中的原始文件名。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileProductvendor	string	当前进程的实际发起进程文件的VERSIONINFO资源中的公司名称值。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileDescription	string	当前进程的实际发起进程的VERSIONINFO资源中的描述通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignResult	string	对当前进程的实际发起者进程的可执行文件进行签名验证的结果：通过 - true，否则 - false。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignTimestamp	int	文件（当前进程的实际发起者）签署的日期和时间。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用于签署当前进程实际发起者进程的文件的证书的主题名称。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonType	string	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessLogonSessionId	int	当前进程的实际发起进程的访问令牌中的登录会话ID。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessProperties	int	当前进程的实际发起者的登录会话类型。通常，“ParentProcess”与“CreatorProcess”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看 ParentProcess*字段
CreatorProcessUserName	string	当前进程的实际发起者的域名和用户名。通常情况下，“父进程”与“创建者进程”相同。此时，遥测数据中将缺少CreatorProcess*字段，需要查看ParentProcess*字段

事件的细粒度访问

在 KUMA 中，具有不同权限的用户可以对事件进行细粒度的访问。对事件的访问权限在存储空间级别进行控制。

您可以在“**空间权限**”部分将空间分配给用户。升级到最新版本后，“所有空间”空间集将分配给所有现有用户，即，对所有空间的访问不受限制。事件包含租户 ID 和空间 ID，因此用户需要相应租户和空间的访问权限才能访问该事件。

请注意以下存储显示功能：

- 如果存储未在“**活动服务**”部分中列出，则存储及其空间不会显示在该集合的空间列表中。
- 如果使用 `systemctl stop kuma-<storage ID>` 命令停止了存储服务，则该存储及其空间不会显示在集合的空间列表中。
- 如果存储已启动，然后使用 `uninstall` 命令将其删除，则该存储及其空间保留在集合的空间列表中。

在事件列表中，您可以将“**SpaceID**”字段添加到表中，该表将显示空间的名称。审计事件的空间显示为 KUMA 审计。KUMA Default 是每个存储内的空间，如果存储没有配置空间或事件与现有空间的条件不匹配，则所有事件都会进入该空间。

将事件列表导出为 TSV 文件时，会显示空间的 ID 和名称。

要区分访问权限：

1. 配置空间集。

   您可以创建、编辑或删除空间集。这些操作会生成审计事件。

2. 配置空间集的访问权限。您可以授予或撤销选定用户的访问权限。

创建空间集

要创建空间集：

1. 在 KUMA Web 控制台中，转到“**设置**” → “**访问**” → “**空间访问权限**”部分。
2. 在打开的窗口中，单击“**添加**”按钮。
3. 在“**创建空间集合**”窗口中，配置以下内容：

   a. 在“**名称**”字段中，指定空间集名称。最多可以使用 128 个 Unicode 字符。

   b. 在“**空间**”下拉列表中，通过选中空间名称旁边的复选框来选择要包含在集合中的空间。要从集合中删除空间，请取消选中复选框。

   c. 如果希望所有未分配任何集合的用户都可以使用默认空间集，请选中“**设为默认**”复选框。

   这会使创建的集合成为默认集合。在空间集列表中，它被标记为默认集合：在“**默认**”列中，其对应的值为“**是**”。

   只能有一个默认集合。如果在不同集合的设置中选中“**设为默认**”复选框并保存设置，则会重新分配默认集合。

4. 单击“**创建**”。

空间集被创建并显示在空间列表中。创建空间集后，会在 KUMA 中生成审计事件。

然后，您需要授予用户对创建的空间集的访问权限。

编辑空间集

要编辑空间集：

1. 在 KUMA Web 控制台中，转到“**设置**” → “**访问**” → “**空间访问权限**”部分。
2. 在打开的窗口中，单击一个空间集。
3. 在“**编辑空间集合**”窗口中，配置以下内容：
   a. 在“**名称**”字段中，指定空间集名称。最多可以使用 128 个 Unicode 字符。
   b. 在“**空间**”下拉列表中，通过选中空间名称旁边的复选框来选择要包含在集合中的空间。要从集合中删除空间，请取消选中复选框。
   c. 如果希望所有未分配任何集合的用户都可以使用默认空间集，请选中“**设为默认**”复选框。
      这会使该集合在您保存更改时成为默认集合。在空间集列表中，它被标记为默认集合：在“**默认**”列中，其对应的值为“**是**”。
      只能有一个默认集合。如果在不同集合的设置中选中“**设为默认**”复选框并保存设置，则会重新分配默认集合。
4. 单击“**保存**”。

空间集将保存并显示在空间列表中。

所有有权访问原始空间集的用户都可以访问编辑后的空间集。您可以控制对已编辑空间集的访问，并使用“**访问控制**”按钮授予或撤销访问权限。

删除空间集

要删除空间集：

1. 在 KUMA Web 控制台中，转到“**设置**” → “**访问**” → “**空间访问权限**”部分。
2. 在“**空间访问权限**”窗口中，选中相关空间集旁边的复选框。
   如果要删除所有空间集，请选中列表左上角的“**全选**”复选框，然后单击“**删除**”。

   > 您无法删除默认空间集和“所有空间”空间集。

3. 单击“**删除**”。

空间集被删除并从空间列表中移除。空间集删除后，KUMA 中会生成审计事件。

如果用户只能访问已删除的空间集而不能访问其他任何空间集，则该用户将自动获得默认空间集的访问权限。

授予空间集访问权限

要授予空间集访问权限：

1. 在 KUMA Web 控制台中，转到“**设置**” → “**访问**” → “**空间访问权限**”部分。
2. 通过选中旁边的复选框来选择列表中的一组空间，然后单击工具栏上的“**访问控制**”按钮。
3. 这将打开“**用户**”窗口；在该窗口中，单击“**添加用户**”。

4. 在“**添加用户**”窗口的列表中，选择要授予其空间集访问权限的用户，然后单击“**添加**”。

   如果要向所有用户授予所选空间集的访问权限，请选中左上角的复选框，然后选择以下选项之一：“**选中当前页所有项**”或“**全选**”，然后单击“**添加**”。

   这将打开一个确认窗口。

5. 如果要向列出的用户授予访问权限，请在确认窗口中点击“**确认**”。

用户现在可以访问空间集。

撤销对空间集的访问权限

撤销对空间集的访问权限

1. 在 KUMA Web 控制台中，转到“**设置**” → “**空间访问权限**”部分。
2. 通过选中旁边的复选框来选择列表中的一组空间，然后单击工具栏上的“**访问控制**”按钮。
3. 这将打开“**用户**”窗口；在该窗口中，通过选中相应的复选框来选择用户，然后单击“**删除**”。

   如果要撤销所有用户对所选空间集的访问权限，请选中左上角的复选框，然后选择以下选项之一：“**选中当前页所有项**”或“**全选**”，然后单击“**删除**”。

   这将打开一个确认窗口。

4. 如果要撤销列出的用户的访问权限，请在确认窗口中单击“**确认**”。

用户将不再拥有对该空间集的访问权限。

如果用户无权访问任何其他空间集，则该用户将自动获得默认空间集的访问权限。

用例

迁移至 KUMA 最新版本（含事件差异化访问权限配置）

目标：更新产品。

操作：管理员将 KUMA 更新到版本 4.0。

结果：用户的事件访问权限不会发生变化，所有用户仅能访问其被授权查看事件列表的租户内的事件。添加新用户、租户或空间时，所有用户都可以看到租户的事件，具体取决于他们是否被授权查看事件列表，无其他额外限制。

限制所有用户对空间的访问权限

目标：安装环境中的某些空间必须禁止部分用户访问。现有用户和新用户不得拥有此类空间的访问权限。

操作：管理员创建一组新的空间，其中包含所有用户必须有权访问的空间。每个空间都以元组的形式指定：集群 ID、租户 ID、空间 ID。通过这种方式，您可以从有限数量的空间中组合出一个空间集。创建空间集后，管理员将此集合设为默认集合。

结果：对于所有未明确指定此空间集的用户（包括新用户），其事件访问权限将根据默认空间集受到额外限制。也就是说，此类用户可以访问他们有权查看事件列表的租户中的事件，以及默认集合中包含的空间中的事件。

允许部分用户查看所有事件

目标：KUMA 有一个默认集合，其中仅明确指定了有限数量的空间。此外，KUMA 中的某些用户必须对所有事件具有不受限制的访问权限。您希望允许这些用户查看默认集合中未指定的空间中的事件。

操作：管理员进入 **空间访问权限** 部分并选择“所有空间”集，该集允许无限制地访问所有空间，并向选定的用户授予对该集的访问权限。

结果：已被明确授予“所有空间”集访问权限的用户现在可以不受限制地访问空间中的事件。用户对事件的访问权限，仅取决于其依据所分配角色获得的事件列表查看权限。添加新空间或租户时，这些用户将有权访问这些新空间和租户中的事件，前提是他们有权查看相应租户的事件列表。未被明确授予“所有空间”集访问权限的用户，其事件访问权限将根据默认空间集受到限制。

允许某些用户查看有限空间集中的事件

目标：KUMA 有一个默认集合，其中仅明确指定了有限数量的空间。某些用户需要查看不同的空间集，但不需要查看所有可用空间。

操作：管理员创建一个包含相关空间的空间集，并将此集的访问权限授予部分用户。

结果：根据可用的空间集，限制用户对事件的访问权限。未被明确授予该集合访问权限的用户，其事件访问权限将根据默认空间集受到限制。

为用户补充明确指定的空间集

目标：用户 u1、u2、u3、u4 已被明确授予空间集“set1”的访问权限，该集合包括 Windows 和 Linux 事件所在的空间。用户 u1 和 u2 除了 Windows 和 Linux 事件之外，还需要查看位于相应空间的 Cisco 和 VMware 事件。

操作：管理员创建空间集“set2”，其中包括 Cisco 和 VMware 事件的空间。除了 set1 之外，管理员还将 set2 分配给 u1 和 u2。

结果：用户 u1 和 u2 现在可以访问他们可以使用的所有集合空间中的事件，即来自 set1 和 set2 的事件：Windows、Linux、Cisco 和 VMware 事件。用户 u3 和 u4 对事件的访问权限保持不变。

编辑空间集

目标：部分用户可以访问某个空间集（明确授予访问权限或该集合是默认集合）。对于所有这些用户，您需要添加对不在集合中的某个空间的访问权限，或撤销对集合中某个空间的访问权限。

操作：管理员通过添加或删除相关空间来编辑现有的空间集。

结果：所有有权访问该集合的用户现在都可以根据更新后的空间集查看事件。

删除空间集

目标：该空间集不再相关，需要从 KUMA 中删除。

操作：管理员删除现有的空间集。无法删除“所有空间”集。默认空间集无法删除。

结果：已删除的空间集从 KUMA 中移除。所有被明确授予此空间集访问权限的用户现在将根据其仍可使用的空间集来访问事件。如果用户没有任何被明确授予访问权限的空间集，其事件访问权限将由默认空间集控制。

查看事件表

事件表为您提供了 KUMA Core 从数据源接收的所有事件的概览。该表显示根据执行的 SQL 查询过滤的事件列表。

要查看事件表：

1. 在主菜单中，转到“**监控**” → “**威胁搜索**”。
2. 如有必要，过滤租户。默认情况下，租户过滤器是禁用的，事件表显示与您拥有**读取**访问权限的所有租户相关的事件。要应用租户过滤器：
   a. 点击“**租户过滤器**”设置旁边的链接。
      租户过滤器将打开。
   b. 选中相应租户旁边的复选框。
      事件表仅显示与所选租户相关的事件。

事件表已显示。有关表中各列的详细信息，请参阅规范化事件数据模型。

搜索和筛选事件

执行事件搜索时，会为手动运行的查询生成一个审计事件。

由控制板、报告或数据收集和分析规则发起的查询不会生成审计事件。用于接收事件的REST API请求也不会生成审计事件。

使用GROUP BY选项时，展开组会触发审计事件的创建，因为此时会执行额外的查询。

选中**后台运行**选项后，会生成两个审计事件：事件读取尝试和搜索查询已取消。

要搜索和筛选事件，请在搜索字段中修改 SQL 查询，然后单击“**运行查询**”按钮。您可以手动输入 SQL 查询，也可以使用查询构建器生成。

SQL 查询支持数据聚合和分组。

您可以在用于查看统计信息的窗口、事件表和事件详情区域向已生成的 SQL 查询添加筛选条件。

要在统计信息窗口中更改筛选设置

1. 按照以下步骤打开事件表。
2. 使用以下方法之一打开“**威胁统计信息**”详细信息区域：
   - 单击事件表右上角的 ⋯ 按钮，然后单击“**威胁统计信息**”。
   - 在事件表中，单击任意值，然后在打开的上下文菜单中选择“**威胁统计信息**”。

   “**威胁统计信息**”详细信息区域将出现在 Web 界面窗口的右侧。
3. 打开相关参数的下拉列表，然后将鼠标光标悬停在所需数值上。

4. 通过执行以下操作之一更改筛选器设置：

   - 要仅包含具有选定值的事件，请单击 ＋ 按钮。
   - 要排除具有选定值的所有事件，请单击 − 按钮。

要更改事件表中的筛选设置

1. 按照以下步骤打开事件表。
2. 单击事件表中的事件参数值。
3. 在上下文菜单中，选择以下选项之一：

   - 要仅显示具有选定值的事件，请选择“**按此值筛选**”。
   - 要从表中排除具有选定值的所有事件，请选择“**从筛选器中排除**”。

要在事件详情区域中更改筛选器设置

1. 按照以下步骤打开事件表。
2. 单击相关事件，以调用事件详情面板。
3. 通过执行以下操作之一更改筛选器设置：

   - 要仅包含具有选定值的事件，请单击 ＋ 按钮。
   - 要排除具有选定值的所有事件，请单击 − 按钮。

通过该操作，筛选器设置和事件表将更新，新的搜索查询会显示在屏幕上方。

> 切换到查询生成器时，在搜索字段中手动输入的查询参数不会传输到生成器，因此您需要重新创建查询。在生成器中创建的查询不会覆盖在搜索字符串中输入的查询，直到您单击生成器窗口中的“**应用**”按钮。

单击 按钮以保存当前筛选器。

手动创建 SQL 查询

您可以通过搜索字符串手动创建任何复杂程度的 SQL 查询以筛选事件。

执行 SQL 查询会影响表格中显示的列。

若 SQL 查询包含 * 值，则查询中指定的列（如果原本不存在）会添加至表格中。所显示的列，即使在后续查询中被移除，也不会在表格中隐藏。

若 SQL 查询不包含 * 值，则表格仅显示符合规范化事件数据模型的指定字段对应的列。即使这些列中没有数据，仍旧会显示。

要手动生成 SQL 查询：

1. 按照以下步骤打开事件表。
2. 在输入字段中输入您的 SQL 查询。

   在 SQL 查询字段中输入函数名称时，会显示可用函数列表。选择某个函数后，右侧会显示用法示例。例如，`concatWithSeparator` 函数附带以下示例：

   ```
   concatWithSeparator('a', '1', '2', '3')
   ```

3. 单击“**运行查询**”按钮。

   查询最长可能需要几分钟才能完成。

   您还可以在后台运行查询。为此，请单击“**运行查询**”按钮旁边的箭头图标，然后选择“**在后台运行**”。在这种情况下，将发生以下情况：

   - 查询将排队等待在后台执行，同时会在“**检测和响应**”部分创建一个任务来运行此查询。
   - 后台查询以低优先级并行运行。
   - 包含超过 10,000 个事件的查询无法排队在后台执行。

   表格将根据生成的 SQL 查询显示搜索结果。您可以在**“检测和响应”**部分查看后台查询的运行结果。

   如有必要，您可以单击**“运行查询”**按钮旁边的箭头图标，然后选择**“取消查询”**来取消后台查询的执行。取消查询后，系统会自动生成一个审计事件。

   如有必要，您可以按时间段筛选表格中的事件。

要在 SQL 查询字段中显示不可打印字符，请按下以下任一组合键：

- **Ctrl** + ***/Command** + *****
- **Ctrl** + **Shift** + **8/Command** + **Shift** + **8**

如果在 XDR 组件中启用不可打印字符的显示，则其他组件（例如 KUMA）不会自动显示不可打印字符，直到您重新加载组件的浏览器标签页。

支持的函数和运算符

SELECT

应返回的事件字段。

对于 **SELECT** 字段，程序支持以下函数和运算符：

聚合函数：**count**、**avg**、**max**、**min**、**sum**。

算术运算符：**+**、**-**、*****、**/**、**<**、**>**、**=**、**!=**、**>=**、**<=**。

您可以组合使用这些函数和运算符。

如果在查询中使用聚合函数，则无法自定义事件表显示、按升序或降序对事件进行排序或接收统计信息。

FROM

数据源。

WHERE：

筛选事件的条件。

- **AND**、**OR**、**NOT**、**=**、**!=**、**>**、**>=**、**<**、**<=**
- **IN**
- **BETWEEN**
- **LIKE**
- **ILIKE**
- **inSubnet**
- **match**（在查询时使用 re2 语法 的正则表达式；特殊字符必须用“\”进行转义）

GROUP BY

用于对返回数据进行分组的事件字段或别名。

如果您在查询中使用数据分组，则无法自定义事件表显示、按升序或降序对事件进行排序、接收统计信息或执行回顾性扫描。

ORDER BY

用于对返回数据进行排序的列。

可能值：

- **DESC**—降序。
- **ASC**—升序。

OFFSET

在打印查询结果输出之前跳过指定的行数。

LIMIT

表格中可以显示的行数。

默认值是 250。

切换到查询构建器时，手动输入搜索字符串的查询参数不会传递到构建器，因此您需要重新创建查询。此外，在构建器中创建的查询不会覆盖输入到搜索字符串中的查询，直到您单击构建器窗口中的“应用”按钮。

别名不能包含空格。

查询示例：

- **SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有类型为“**Base**”和“**Audit**”的事件，均按照“**Timestamp**”列降序排列。表格可以显示的字符串数量为 250。

- **SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250**

  在事件表中，所有“**BytesIn**”字段的值（即接收流量）在 1,000 到 2,000 字节范围内的事件，均按照“**Timestamp**”列升序排列。表格可以显示的字符串数量为 250。

- **SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有“**Message**”字段包含与定义的 %ssh:% 小写模板对应数据的事件，均按照“**Timestamp**”列降序排列。表格可以显示的字符串数量为 250。

- **SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有位于 00.0.0.0/00 子网中的主机的事件，均按照“**Timestamp**”列降序排列。表格可以显示的字符串数量为 250。

- **SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有“**Message**”字段包含与 ssh.* 模板对应文本的事件，均按照“**Timestamp**”列降序排列。表格可以显示的字符串数量为 250。

- **SELECT max(BytesOut) / 1024 FROM `events`**

  指定时间段内的最大出站流量 (KB)。

- **SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250**

  事件数量和端口号。事件按端口号分组，并按“**Port**”列升序排列。表格可以显示的字符串数量为 250。

  在事件表中，“**ID**”列被命名为 Count，“**SourcePort**”列被命名为 Port。

- **SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250**

  如果要在查询中使用特殊字符，则需要在特殊字符前面添加反斜杠 (\) 字符进行转义。

  在事件表中，所有“**Message**”字段包含与 ssh: 'connection' 模板对应文本的事件，均按照“**Timestamp**”列降序排列。表格可以显示的字符串数量为 250。

使用构建器生成 SQL 查询

您可以使用查询构建器生成用于筛选事件的 SQL 查询。

执行 SQL 查询会影响表格中显示的列。

若 SQL 查询包含 * 值，则查询中指定的列（如果原本不存在）会添加至表格中。所显示的列，即使在后续查询中被移除，也不会在表格中隐藏。

若 SQL 查询不包含 * 值，则表格仅显示符合规范化事件数据模型的指定字段对应的列。即使这些列中没有数据，仍旧会显示。

要使用构建器生成 SQL 查询：

1. 按照以下步骤打开事件表。
2. 单击 按钮打开查询构建器。

   通过在以下参数块中提供数据来生成搜索查询：

   - **SELECT**

     应返回的事件字段。默认情况下选择 * 值，这意味着必须返回所有可用的事件字段。要调整显示的字段，请在下拉列表中选择所需字段。请注意，选择 * 会增加请求执行的持续时间，但无需在请求中指定字段。

     选择事件字段时，可以使用下拉列表右侧的字段为显示的数据列指定别名，也可以使用最右边的下拉列表选择要对数据执行的操作：**count**、**max**、**min**、**avg**、**sum**。

   - **FROM**

     数据源。选择**事件**值。

   - **WHERE：**

     筛选事件的条件。

     要添加条件和组，请单击“**添加条件**”和“**添加组**”按钮。条件组中的“**AND**”运算符值默认被选中。单击运算符值，即可进行更改。可用值：**AND**、**OR**、**NOT**。

     要更改条件和条件组的结构，请使用 图标拖放表达式。

     要添加筛选条件：

     a. 在左侧下拉列表中，选择要用于过滤的事件字段。

     b. 从中间下拉列表中选择必要的运算符。可用的运算符取决于所选事件字段的值的类型。

     c. 输入条件的值。根据所选字段类型，您可能需要手动输入、从下拉列表中选择或在日历上选择该值。

     要删除筛选条件，请单击“**X**”按钮。要删除分组条件，请单击“**删除组**”按钮。

   - **GROUP BY**

     用于对返回数据进行分组的事件字段或别名。

     如果您在查询中使用数据分组，则无法自定义事件表显示、按升序或降序对事件进行排序、接收统计信息或执行回顾性扫描。

- **ORDER BY**

  用于对返回数据进行排序的列。在右侧的下拉列表中，您可以选择所需的排序方式：**DESC**—降序，**ASC**—升序。

- **LIMIT**

  表格中可以显示的行数。

  默认值是 250。

  若按用户定义的时间段筛选事件，且搜索结果中的字符串数量超出了定义值，可以单击“**显示后续记录**”按钮以在表格中显示更多字符串。按标准时间段筛选事件时，不会显示此按钮。

3. 单击“**应用**”。

   当前的 SQL 查询将被覆盖。生成的 SQL 查询将显示在搜索字段中。

   要重置构建器设置，请单击“**默认查询**”按钮。

   要关闭构建器而不覆盖现有查询，请单击 按钮。

4. 单击“**运行查询**”按钮以显示表格中的数据。

   查询最长可能需要几分钟才能完成。

   您还可以在后台运行查询。为此，请单击“**运行查询**”按钮旁边的箭头图标，然后选择“**在后台运行**”。在这种情况下，将发生以下情况：

   - 查询将排队等待在后台执行，同时会在“**检测和响应**”部分创建一个任务来运行此查询。
   - 后台查询以低优先级并行运行。
   - 包含超过 10,000 个事件的查询无法排队在后台执行。

   表格将根据生成的 SQL 查询显示搜索结果。您可以在**“检测和响应”**部分查看后台查询的运行结果。

   如有必要，您可以单击**“运行查询”**按钮旁边的箭头图标，然后选择**“取消查询”**来取消后台查询的执行。取消查询后，系统会自动生成一个审计事件。

切换到 Web 界面的另一个部分时，构建器中生成的查询不会保留。如果从另一个部分返回到事件部分，构建器将显示默认查询。

使用 KUMA SQL 函数生成 SQL 查询

KUMA 的 SQL 函数允许在搜索查询中使用资产和账户的属性来筛选事件，以及生成报告和小部件（图表类型：**表**）。您可以使用以下函数集，利用字典、表、资产和账户中的数据来丰富事件：

- enrich 函数组。可使用资产或账户的字段、**字典**类型的字典中的值或**表**类型的字典中的值来丰富查询结果。`enrich` 函数组包括以下函数：
  - `enrich_assets`；
  - `enrich_accounts`；

- `enrich_table`;
- `enrich_dictionary`。

- lookup 函数组。可在搜索查询中添加资产和账户的条件。`lookup` 函数组包括以下函数：
  - `lookup_assets`;
  - `lookup_accounts`;
  - `lookup_assets_category`。

> 每次查询最多可包含 10,000 个事件。

在 SQL 查询中使用“enrich”函数集

`enrich` 函数集（见下表）用于 SQL 查询的 `SELECT` 子句，以扩充查询结果。

使用此函数集时，无法按扩充字段对事件进行分组。

使用这些函数扩充的小部件和报告最多只能属于一个租户。

> SQL 查询中指定的资产字段值区分大小写。

"enrich"函数集的描述

函数	事件字段	资产字段	描述
enrich_assets	DeviceAssetID DestinationAssetID SourceAssetID	name os osBuild ipAddress macAddress fqdn source software cii ramSize kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart kscStatusMask kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus lastVisible aistatus aiscore	根据传递给函数的指定 ID，使用资产字段丰富查询结果。 示例 `enrich_assets(DeviceAssetID, name)`
enrich_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name uac	根据传递给函数的指定 ID，使用账户字段扩充查询结果。 示例 `enrich_account(SourceAccountID, name)` 此功能仅适用于已启用 LDAP 信息扩充的租户。

函数	事件字段	资产字段	描述

enrich_table	任何	–	根据 ClickHouse 集群响应中的事件字段，使用**表**类型字典中的值扩充查询结果。
			
			示例
			`enrich_table('Main/some-table', [DeviceProduct], 'value')`
			
			表中只能有一列作为密钥，但记录密钥可以是复合密钥。
			
			示例
			`enrich_table('Main/Dictionary', [BytesOut|BytesIn], 'value2')`
			
			`enrich_table` 函数仅返回表中的一列。如果需要调用更多列，请指定相关字段并再次调用该函数。

enrich_dictionary	任何	–	根据 ClickHouse 集群响应中的事件字段，使用**字典**类型的字典中的值扩充查询结果。
			
			示例 1
			`enrich_dictionary('Main/some-dict', [SourceAddress]`
			
			示例 2
			`enrich_dictionary('Main/some-dict', [SourceAddress, DeviceAddress])`
			
			您可以在**资源 → 字典**部分查看字典的路径。

手动创建 SQL 查询时，可以指定 `enrich` 函数。

使用 `enrich` 函数的查询示例

`events` 表中包含 `Name` 和 `Message` 字段的所有事件，以及用于通过资产数据扩充结果的 `macAddress` 和 `osBuild` 资产字段。表中最多可显示 250 行。

```
SELECT Name,
Message,
   enrich_assets(DeviceAssetID, macAddress),
   enrich_assets(DeviceAssetID, osBuild)
FROM `events`
WHERE DeviceAssetID != ''
LIMIT 250
```

`events` 表中的所有事件，包括事件字段 `SourceUserName` 和 `SourceAddress`，以及用于通过帐户数据丰富结果的 `mobile` 字段值。表中最多可显示 10 行。

```
SELECT SourceUserName,
SourceAddress,
   enrich_accounts(SourceAccountID, mobile) as mobile
FROM `events`
WHERE SourceAccountID != ''
LIMIT 10
```

`events` 表中 `DeviceProduct` 事件字段值来自 **Main/[OOTB] Linux 的所有事件。Auditd 记录类型**。按 **时间戳**降序排序。表中最多可显示 1000 行。

```
SELECT DeviceProduct,
   enrich_table('Main/[OOTB] Linux&period; Auditd record types', [DeviceProduct], 'Description') as HTTP
FROM `events` WHERE Type!=4
LIMIT 1000
```

`events` 表中的所有事件，其中 `DeviceAction` 事件字段的值来自 **Main/[OOTB] KEDR** 字典。表中可显示的行数为 250。

```
SELECT DeviceAction,
   enrich_dictionary('Main/[OOTB] KEDR&period; AccountType', [BytesOut]) as accountType
FROM `events` WHERE Type!=4
LIMIT 255
```

在 SQL 查询中使用“lookup”函数集

`lookup` 函数集（见下表）用于 SQL 查询的 `WHERE` 子句，以便向搜索查询添加资产和帐户条件。

对于包含 `lookup` 函数的查询，KUMA 会自动将在查询的 `lookup` 函数中使用的 `*ID` 字段添加到 `SELECT` 子句中。例如，对于包含 `lookup_assets(DeviceAssetID, osBuild, '=', '19045.000000')` 函数的查询，系统会将 `DeviceAssetID` 字段添加到 `SELECT` 子句中。

对于包含 `lookup` 函数的查询，建议在 `SELECT` 子句中指定要返回的字段列表。不建议在 `SELECT` 子句中使用 *。这会返回所有可用字段，从而可能会显著延长查询处理时间。

"lookup"函数集的描述

函数类型	事件字段	资产字段	运算符	描述
lookup_assets	DeviceAssetID SourceAssetID DestinationAssetID	name os osBuild source cii ramSize kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus aistatus aiscore	=	允许您向查询结果添加条件，查询中指定的值匹配的资产。 对于数值，必须指定一个包含串。 例如： lookup_assets(DeviceAss '=', '19045.000000') lookup_assets(DeviceAss '=', '3241234234')
		kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart lastVisible ramSize aiscore	< > <= >=	允许您为字段值符合以下条件件： • 小于查询中指定的值 • 大于查询中指定的值 • 小于或等于查询中指定的 • 大于或等于查询中指定的对于数值，必须指定一个包含串。 例如： lookup_assets(DeviceAss '>', '50') 日期值可以采用以下格式指定 • 秒数：lookup_assets(Device lastVisible, '>', '1 • 毫秒数：lookup_assets(Device lastVisible, '<', '1725971837834') • 天数：lookup_assets(Device lastVisible, '<', 'n
		name os osBuild fqdn software	like	允许您为查询结果添加条件，查询中指定的"like"表达式匹配 有关 like 操作员的更多信息，表达式 参考文档。 lookup_assets(Destinati name, 'like','test.compa
		ipAddress macAddress fqdn software kscStatusMask	in	允许您将值与查询中指定的值件添加到结果中。 例如： lookup_assets(DeviceAss 'in', ['test_fqdn1.compa 'test_fqdn2.company.ru'
		ipAddress	insubnet	允许您为 IP 地址位于指定子网件。IP 地址以 CIDR 格式指定。 例如： lookup_assets(DeviceAss ipAddress, 'insubnet',

函数类型	事件字段	资产字段	运算符	描述

		ipAddress	inrange	允许您为 IP 地址位于指定范围
				件。
				查询中指定的第一个 IP 地址是
				第二个 IP 地址是结束 IP 地址。
				例如：
				`lookup_assets(DeviceAss`
				`ipAddress, 'inrange', [`
				`'192.168.1.184'])`
				该查询会筛选出 IP 地址在 192
				192.168.1.184 范围内的资产。

函数类型	事件字段	资产字段	运算符	描述
lookup_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn title division department manager location company street_address physical_delivery_office_name uac	=	允许您向查询结果添加条件，查询中指定值匹配的帐户。 对于数值，必须指定一个包含串。 例如： lookup_accounts(SourceA employee_id, '=', '1545
		name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name	like	允许您向查询结果添加条件，查询中指定的"like"表达式匹配 有关 like 操作员的更多信息，表达式 参考文档。 lookup_accounts(Destina name, 'like', '_ccount1
lookup_assets_category	DeviceAssetID SourceAssetID DestinationAssetID	–	–	查找具有指定文件夹中关联资 例如： lookup_assets_category(['Main/Business Impact'] 其中 Main 是租户名称， Bus 是文件夹名称。

带有查找函数的 SQL 查询示例
手动创建 SQL 查询时，可以指定 lookup 函数。带有 lookup 函数的查询示例

- "events"表中的所有事件，包含 TenantID 和 DeviceProduct 事件字段以及 fqdn 资产字段，且该资产字段的值包含 win10 子字符串。 表中可显示的行数为 250。
  ```
  SELECT TenantID, DeviceProduct
  FROM `events`
  WHERE DeviceAssetID != ''
  AND lookup_assets(DeviceAssetID, fqdn, 'match', 'win10')
  LIMIT 250
  ```
- "events"表中的所有事件，包含 TenantID 和 DeviceProduct 事件字段，其中 the EmployeeID 字段的值为 15452. 。表中可显示的行数为 10。
  ```
  SELECT TenantID, DeviceProduct
  FROM `events`
  WHERE SourceAccountID != ''
  AND lookup_accounts(SourceAccountID, employee_id, '=', '15452')
  LIMIT 10
  ```
- "events"表中的所有事件，包含 TenantID 和 DeviceProduct 事件字段以及资产所在的文件夹。表中可显示的行数为 100。
  ```
  SELECT TenantID, DeviceProduct
  FROM `events`
  WHERE DeviceAssetID != ''
  AND lookup_assets_category(DeviceAssetID, ['Main/Business Impact'])
  LIMIT 100
  ```

查看事件详情

要打开事件详情面板，请在"**威胁搜索**"部分的事件表中或警报详情页面中选择一个事件。

事件详情面板显示在 Web 界面窗口的右侧，包含事件参数及其值的列表。在此区域中，您可以：

- 通过单击参数值旁边的 + 或者 −，可将所选字段纳入搜索范围或从搜索范围中排除。
- 单击"**FileHash**"和"**DeviceCustomString**"值，查找相似事件并添加或删除防护规则。
- 当与 Kaspersky CyberTrace 和卡巴斯基威胁情报门户集成时，您可以通过单击"**FileHash**"和"**DeviceCustomString**"值来添加到 CyberTrace 的内部 TI 并显示来自威胁查找的信息。
- 通过单击"**服务**"值来查看注册事件的服务设置。
- 通过单击"**DeviceAssetID**"值并选择"**资产详情**"，查看与设备相关的警报或事故列表。在打开的"**设备详情**"窗口中，单击"**显示相关**"按钮，然后选择要查看的"**警报**"或"**事故**"。
- 查看事件创建时触发的IOA规则列表；单击规则名称即可查看这些IOA规则的详细信息。

  打开的"IOA 规则"窗格会显示详细信息。

  在打开的IOA规则详细信息中，您可以执行以下操作：

  - 查看IOA规则名称、ID、严重等级和置信度级别。
  - 将IOA规则添加到排除项。
  - 单击**在 Kaspersky TIP 中查找**按钮查看狩猎信息；
  - 单击**参看于**按钮，查看触发IOA规则时创建的警报和事件。
  - 单击**在威胁搜索中查找**按钮查看相关事件。

    事件的默认显示时间间隔为24小时。

您还可以在Kaspersky TIP中查看IOA规则的详细信息。为此，请在IOA规则详细信息窗口中，单击**在 Kaspersky TIP 中查找**按钮。

- 单击 图标并将拨动开关移至所需位置，以启用或禁用 `*Label` 字段的紧凑显示模式。默认情况下，切换开关设置为 **完整视图** 位置。当为 `DeviceCustom*` 和 `Flex*` 字段选择 **紧凑视图** 模式时，相应 `*Label` 字段的值将显示为字段名称，而 `*Label` 字段本身会从事件字段列表中隐藏。如果缺少 `*Label` 字段值，则显示原始字段名称。在刷新页面以及离开 **威胁搜索** 区域后，所选显示模式仍会保留。

在“**事件详情**”面板中，以下设置的值显示的是所描述对象的名称，而不是其 ID。如果您从“**事件详情**”面板更改过滤器设置，则会将对象的 ID（而不是其名称）添加到 SQL 查询中：

- TenantID
- SeriviceID
- 设备资产 ID
- SourceAssetID
- DestinationAssetID
- SourceAccountID
- DestinationAccountID

保存和选择事件过滤器配置

您可以保存当前的过滤器配置以供将来使用，这些配置包括基于时间的过滤器、查询构建器和事件表设置。已保存的过滤器配置可供您和其他具有相应访问权限的用户使用。

要保存过滤器、查询和时间段的当前设置

1. 按照以下步骤打开事件表格。
2. 单击 图标，然后选择“**保存当前过滤器**”。
3. 在打开的“**新过滤器**”窗口中，在“**名称**”字段中输入过滤器配置的名称。名称包含的 Unicode 字符数量不得超过 128 个。
4. 在“**租户**”下拉列表中，选择要为其保存所创建过滤器的租户。
5. 单击“**保存**”按钮。
   过滤器配置现已保存。

要选择之前保存的过滤器配置

1. 按照以下步骤打开事件表。
2. 单击搜索查询旁边的 图标，然后选择所需的过滤器。

要保存过滤器、查询和事件表设置的当前设置

1. 按照以下步骤打开事件表。
2. 单击事件表上方面板中的齿轮图标。
3. 单击“**保存当前预设**”。
4. 在打开的“**新建预设**”窗口中，在“**名称**”字段中输入预设的名称。名称包含的 Unicode 字符数量不得超过 128 个。
5. 在“**租户**”下拉列表中，选择要为其保存所创建预设的租户。
6. 单击“**保存**”按钮。
   预设配置现已保存。

要选择以前保存的预设

1. 按照以下步骤打开事件表。
2. 单击事件表上方面板中的齿轮图标。选择“**预设**”选项卡。
3. 选择所需的预设。

要删除所有用户之前保存的过滤器配置

1. 按照以下步骤打开事件表。
2. 单击搜索查询旁边的 图标。
3. 单击需要删除的配置旁边的 图标。
4. 单击“**确定**”。

按时间段筛选事件

您可以指定显示事件的时间段。

按时间段筛选事件：

1. 按照以下步骤打开事件表。
2. 打开窗口上部的第二个下拉列表。
3. 指定时间范围。您可以选择相对于当前日期和时间的预定义范围，或使用“**范围起始**”和“**范围结束**”字段，或者在日历中选择日期来指定自定义时间范围。
4. 单击**应用**。

导出事件

您可以将事件信息导出为 TSV 文件。选择将哪些事件导出为 TSV 文件取决于过滤器设置。信息将从已显示在事件表中的列导出。即使某些列由于 SQL 查询的特性未在“**威胁搜索**”部分的事件表中显示，导出文件中的这些列仍会填充可用数据。

要导出事件信息：

1. 按照以下步骤打开事件表。
2. 单击事件表右上角的 ••• 按钮并选择“**导出 TSV**”。
   新的 TSV 文件导出任务已在 KUMA 的**任务管理器**部分中创建。
3. 在“KUMA”部分，找到您在**任务管理器**部分中创建的任务。
4. 单击任务类型名称，然后从下拉列表中选择“**上传**”。
   TSV 文件将根据您的浏览器设置进行下载。默认情况下，文件名为 event-export-<date>_<time>.tsv。

该文件根据 Web 浏览器设置进行保存。

查看审计事件和配置通知

审计是一个监控、注册和分析用户操作和系统操作的过程，旨在确保更改的安全性和可追溯性。

Kaspersky Next XDR Expert会自动从解决方案组件中收集审计事件，无需额外配置。在解决方案部署期间，Kaspersky Next XDR Expert会在根租户中创建一个预定义的收集器**[OOTB] Kaspersky OSMP**。此收集器关联了一个预定义的连接器**[OOTB] Kaspersky OSMP**和关联的预定义规范化器**[OOTB] Kaspersky OSMP审计**。收集器会将审计事件发送到**KUMA审计**存储空间。此存储空间会自动创建。

仅当您在单节点部署、多节点部署期间，或在解决方案界面中，在`license`参数中为SIEM组件指定了有效的授权许可密钥时，Kaspersky Next XDR Expert才会收集审计事件。

如有必要，您可以在创建存储资源集时配置审计事件的存储设置。

有关审计事件的参数和操作类型的详细信息，请参阅文章：审计事件。

如何查看审计事件并将其导出到文件

审计事件可在**监控→威胁搜索**中进行。

如果您希望事件表仅显示审计事件，请执行以下操作之一：

- 在事件表中，在**EventType**字段中，设置`Audit`值。
- 通过审计事件区分对空间的访问权限。

  为此，请前往**设置→KUMA→打开KUMA设置→空间访问权限**，然后配置KUMA审计空间的访问权限。只有被授予空间访问权限的用户才能在**威胁搜索**部分查看审计事件。

在事件表中筛选审计事件后，您可以将审计事件导出到文件。

如何配置审计事件的电子邮件通知

一旦发生事件（例如，用户尝试登录OSMP控制台超过五次均失败），系统将触发预定义的关联规则并生成警报。

如果您希望接收有关警报的电子邮件通知，则必须创建通知模板。在**创建电子邮件模板**窗格中，指定以下参数：

- 在**事件类型**下拉列表中，选择**创建新警报**通知模板类型。
- 在**相关规则**下拉列表中，选择预定义的关联规则。

审计事件

审计事件显示在**威胁搜索**部分，可能包括下表列出的操作类型。

操作类型	操作名称	参数和描述
组件操作	`Service start`	

	Service stop	reason 服务中断原因（如有）。
警报操作	Alert assigning	• alert_id 执行操作的警报ID。 • group_name 被分配警报的群组名称。 • group_id 被分配警报的群组ID。
	Changing alert status	• alert_id 执行操作的警报ID。 • alert_status 警报的之前状态。 • new_alert_status 警报的新状态。
	Alert auto assigning	• alert_id 执行操作的警报ID。 • account_name 被分配警报的用户ID。 • account_id 分配警报的用户的 ID。
事故操作	Creating incident	incident_id 执行操作的事件ID。
	Incident assigning	• incident_id 执行操作的事件ID。 • group_name 被分配事故的群组名称。 • group_id 被分配事故的群组ID。
	Changing incident status	• incident_id 执行操作的事件ID。 • incident_status 事故的之前状态。 • new_incident_status 事故的新状态。
	Merge incidents	incident_id 合并后的目标事故ID。
	Incident auto assigning	• incident_id 执行操作的事件ID。 • account_name 被分配事故的用户名称。 • account_id 被分配事故的用户ID。
分段规则操作	Creating segmentation rule	rule_name 分段规则的名称。
	Changing segmentation rule	
	Enabling segmentation rule	
	Disabling segmentation rule	
	Deleting segmentation rule	
分段规则操作	Creating aggregation rule	rule_name 聚合规则的名称。
	Changing aggregation rule	
	Enabling aggregation rule	
	Disabling aggregation rule	
	Deleting aggregation rule	

电子邮件通知	Creating e-mail templates	subject 执行操作的电子邮件通知模板的主题。
	Enabling e-mail templates	
	Disabling e-mail template	
	Changing e-mail templates	
	Deleting e-mail templates	
设置	Enabling auto send to SB by IOA trigger	tenant_name 执行操作的租户名称。
	Disabling auto send to SB by IOA trigger	
	Turning on the Assign "Untrusted" status to alerts toggle switch	
	Turning off the Assign "Untrusted" status to alerts toggle switch	
	Enabling the use of KSN	
	Disabling the use of KSN	
	Enabling the use of KPSN	
	Disabling the use of KPSN	
	Enabling the use of MDR	
	Disabling the use of MDR	
	Configuring the connection of OSMP to a local reputation database of KPSN	
	Enabling auto send to SB	
	Disabling auto send to SB	
	Enabling manual send to SB	
	Disabling manual send to SB	
	Selecting a database update source	
	Updating database manually	version_of_updated_databases 病毒数据库的版本。
	Auto updating database	
	Changing passwords for archives	
	Enabling the required password change	
	Disabling the required password change	
	Enabling user password change	period 密码必须在多少天后更改。
租户管理	Creating tenant	tenant_name 租户名称。
	Changing tenant	
	Bind Administration Server	
	Changing integration KATA/KEDR	integration_parameters 集成设置。
	Changing integration TIP	
	Changing custom integration	

	Changing integration	
存储库	Uploading file to storage	• file_name 文件名称。 • alert_id 执行操作的事件ID。 • incident_id 执行操作的事件ID。
	Downloading file from storage	
	Deleting file from storage	
	Auto deleting file from storage	
设置	Configuring an IOC scan schedule	
防御规则	Uploading prevention rules from file	• file_name 文件名称。 • count 导入文件后建立的阻止规则的数量。
	Creating a prevention rule	file_name 文件名称。
	Modifying a prevention rule	
	Enabling the use of a prevention rule	
	Disabling the use of a prevention rule	
	Removing a prevention rule	
行动手册	Creating a playbook	playbook_name 行动手册名称。
	Removing a playbook	
	Changing the operation mode	
YARA	Uploading a YARA file	file_name 文件名称。
	Downloading a YARA rule	rule_name YARA规则名称。
	Changing YARA rule	
	Enabling the automatic use of YARA rules	
	Disabling the automatic use of YARA rules	
	Deleting a YARA rule	
IOC	Uploading an IOC file	file_name 文件名称。
	Downloading an IOC rule	rule_name IOC规则的名称。
	Changing IOC rule	
	Enabling the automatic use of IOC rules	
	Disabling the automatic use of IOC rules	
	Deleting an IOC rule	
TLS证书操作	Generating a TLS certificate for the Endpoint Agent component	
	Uploading a TLS certificate for the Endpoint Agent component	
	Deleting a TLS certificate for the Endpoint Agent component	
	Downloading the TLS certificate of the server	

Sandbox 设置	OS set of virtual machines changed	sb_name 沙盒名称。
	Creating a request for connection to the server with the Sandbox component	
	Enabling a connection with the Sandbox component	
	Disabling a connection with the Sandbox component	
	Deleting a connection with the Sandbox component	
	Renaming the Sandbox server	• new_sb_name 新沙盒名称。 • sb_ip 沙盒的IP地址。
沙盒规则	Creating a file scanning rule in custom images	virtual_machine_name 虚拟机的名称。
	Enabling a file scanning rule in custom images	
	Disabling a file scanning rule in custom images	
	Deleting a file scanning rule in custom images	
	Editing a file scanning rule in custom images	• virtual_machine_name 虚拟机的名称。 • new_virtual_machine_name 虚拟机的新名称，如果它被更改了。
	Export a file scanning rule in custom images	file_name 文件名称。
	Import a file scanning rule in custom images	file_name 文件名称。
分布式解决方案	Assigning the PCN OSMP role	tenant_name 租户名称。
	Assigning the SCN OSMP role	
	Creating a request for connection of the SCN OSMP to the PCN OSMP	
	Accepting a request for connection of the SCN OSMP to the PCN OSMP	
	Rejecting a request for connection of the SCN OSMP to the PCN OSMP	
	Confirming the assign PCN role to CN	
	Disconnecting an SCN from PCN	
账户操作	Creating a user account	• account_name 用户名。 • account_id 用户 ID。 • account_authorization 执行操作的帐户的上次登录日期和时间。 • password_verification 执行操作的账户的密码验证状态。 • account_expiration_date 执行操作的帐户的到期日。该值始终为 01.01.2222。 • account_status 执行操作的帐户状态。 • account_type 执行操作的账户类型。
	Changing access rights of user account	
	Change the password	
	Enabling account	
	Disabling account	
	Deleting an account	

用户身份验证和授权	登录成功	`administrator_rights` 指示用户是否具有管理员权限。
	登录被拒绝，因为用户没有注册	
	登录被拒绝，因为用户被屏蔽了	
	登录被拒绝，因为密码不正确	
	登录被拒绝，因为超过了密码尝试限制	
	登录被拒绝，因为密码已过期	
	登出	

回溯扫描

您可以使用追溯扫描来优化关联规则资源或分析历史数据。

您也可以选择基于追溯扫描创建警报。

要使用追溯扫描：

1. 在主菜单中，转到**"监控"**→**"威胁搜索"**。
2. 单击事件表右上角的 ••• 按钮，然后选择"**追溯扫描**"。
   将打开"**追溯扫描**"面板。
3. 在"**关联器**"下拉列表中，选择要将选定事件发送到的关联器。
4. 在"**相关规则**"下拉列表中，选择处理事件时必须使用的关联规则。
5. 要在事件处理期间执行响应，请打开"**执行响应**"切换开关。
6. 要在事件处理期间生成警报，请打开"**创建警报**"切换开关。
7. 单击"**创建任务**"按钮。
   追溯扫描任务在 KUMA 的"**任务管理器**"部分中创建。

获取事件表统计信息

您可以获取事件表中显示的当前事件分类统计信息。事件分类取决于过滤器设置。

要获取统计信息：

1. 按照以下步骤打开事件表格。
2. 执行以下操作之一：
   - 在事件表的右上角，从 ••• 下拉列表中选择"**统计信息**"。
   - 在事件表中，单击任意值，然后从打开的上下文菜单中选择"**统计信息**"。

“**统计信息**”详细信息区域将显示当前事件分类的参数列表。每个参数附近的数字表示事件分类中包含该参数的事件数。如果展开某个参数，则会显示五个最常出现的值。在**搜索字段**中输入参数名称以过滤显示的数据。

“**统计信息**”窗口允许您修改事件过滤器。

> 当使用带有数据分组和聚合的 SQL 查询来过滤事件时，统计信息不可用。

威胁响应

若要执行响应操作、查看通过行动手册执行的数据增强结果，或手动启动行动手册，必须转到“**警报**”或“**事故**”部分。

如果满足以下条件，则“**警报**”和“**事故**”部分将显示在主菜单中：

- 拥有 Kaspersky Next XDR Expert 的授权许可密钥。
- 已连接到 OSMP 控制台中的根管理服务器。
- 您拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师、SOC 经理、审批人、审计员。

执行响应操作后，即可查看响应历史记录。

响应操作

可以通过以下任一方式启动响应操作：

- 手动启动（详见本部分说明）。

  对于未安装带有内置代理的Kaspersky Endpoint Security的设备，您无法执行以下响应操作：管理服务、删除文件、YARA扫描、IOC扫描、从隔离区获取文件，以及获取文件以供进一步分析部分中描述的响应操作。

  从警报或事故详情或从资产表进行响应时，无法选择已归档的设备。

- 在行动手册中启动。

  在这种情况下，在创建或编辑行动手册时，您可以将响应操作配置为自动运行，或在行动手册中启动响应操作之前请求用户手动审批。默认情况下，响应操作的手动审批处于禁用状态。

  如果在执行响应操作期间设备被归档，则行动手册结果将显示“**错误**”消息。如果为包含已归档设备的警报触发行动手册，则行动手册结果将显示“警告”消息以及设备已归档的说明。

终止进程

“*终止进程*”响应操作允许您远程终止设备上的进程。您可以对可观察对象或资产运行终止进程响应操作。

您可以通过以下任一方式执行终止进程响应操作：

- 从警报或事故详情操作
- 从设备详情操作
- 从遥测事件

  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。

- 从调查图操作

  > 如果已构建调查图，则该选项可用。

- 从资产表
- 从**响应历史**部分

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

> 要运行终止进程响应操作，您必须拥有以下 XDR 角色之一：主管理员、1 级分析师、2 级分析师、租户管理员。

> 由于受管理设备和管理服务器之间存在同步间隔，响应操作启动可能需要长达 15 分钟。

从警报或事故详细信息中响应

要从警报或事故详情中终止进程：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**资产**”选项卡。

   > 您也可以转到“**可观察对象**”选项卡，选择要终止进程的一个或多个观察点。可观测对象可能包括 MD5 或 SHA256 哈希值。

3. 在资产列表中，选择一个或多个设备。
4. 在“**选择响应操作**”下拉列表中，选择“**终止进程**”。
5. 在打开的右侧窗格中，执行以下操作：
   a. 在 **完整路径** 字段中，指定进程文件的完整路径。
   b. 在“**资产**”下拉列表中，选择要终止进程的设备。

      如果在步骤 2 中选择了“**资产**”选项卡，则默认情况下，您选中的复选框对应的设备名称会显示在“**资产**”字段中。您可以更改它们或在**范围**下拉列表中选择**所有资产**选项，以终止属于警报或事件租户及其子租户的所有设备上的进程。

只有您可以对其执行响应操作的资产才可供选择。
设备显示方式如下：属于警报或事故的设备位于下拉列表开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

c. 如有必要，请在相应字段中配置以下设置：

- 指定进程文件的SHA256或MD5哈希值。

  如果在步骤 2 中选择了“**可观察对象**”选项卡，则默认情况下会显示您选择的哈希值。您可以更改这些哈希值。

- 为响应操作编写描述或注释。

6. 单击“**终止**”按钮。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从设备详情中响应

要从设备详情中终止进程：

1. 执行以下操作之一：

- 在主菜单中，前往**监控**→**警报**部分。在“ID”列中，单击包含要移动至隔离区的文件所在设备的警报 ID。
- 在主菜单中，前往**监控**→**事故**部分。在“ID”列中，单击包含要移动至隔离区的文件所在设备的事故 ID。

2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
4. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从遥测事件响应

要从通过警报或事故详情打开的遥测事件中终止进程：

1. 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含要移动至隔离区的文件所在设备的警报 ID。
2. 在打开的窗口中，转到“**详细信息**”选项卡，然后执行以下操作之一：
   - 单击目标事件名称并选择设备。
   - 单击“**在威胁搜索中查找**”按钮，以转到“**威胁搜索**”部分，然后选择所需设备。

   > 您也可以转到“**可观察对象**”选项卡，选择要终止进程的一个或多个观察点。可观测对象可能包括 MD5 或 SHA256 哈希值。
3. 在“**选择响应操作**”下拉列表中，选择“**终止进程**”。
4. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

要从通过“威胁搜索”部分打开的遥测事件中进行响应：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。
2. 单击您要打开其详情的事件名称。
3. 在打开的事件详情窗口中，单击设备名称，然后从打开的下拉列表中选择“**终止进程**”。
4. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从调查图响应

> 如果已构建调查图，则该选项可用。

要从调查图终止进程：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的“**事故详情**”窗口中，单击“**在图表上查看**”按钮。
   “**调查图**”窗口将打开。

3. 单击所需设备的名称，然后在下拉列表中选择“**查看详情**”。
4. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从资产表响应

要从资产表中进行响应：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   这将打开资产表。
2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   > 已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择“**终止进程**”。
4. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从响应历史部分响应

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。
2. 在“**响应**”下拉列表中，选择“**终止进程**”。
3. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

进程终止。操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示错误消息以及有关错误原因的信息。

如果您想查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

将设备移动至其他管理组

作为响应操作，您可以将设备移动至 Open Single Management Platform 的其他管理组。若警报或事故分析显示设备的保护级别较低，则可能需要执行此操作。将设备移动至其他管理组时，组策略和任务将自动应用于该设备。

目标管理组必须与设备同属于同一租户。

您可以通过以下方式之一将设备移动至其他管理组：

- 从警报或事故详情操作
- 从设备详情操作
- 从调查图表操作

您也可以配置在创建或编辑行动手册时自动运行的响应操作。

要将设备移动至其他管理组，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

由于受管理设备和管理服务器之间存在同步间隔，响应操作启动可能需要长达 15 分钟。

将设备从警报或事故详情移动至其他管理组

要将设备从警报或事故详情移动至其他管理组：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含待移动设备的警报的 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待移动设备的事故的 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 选中要移动至其他管理组的设备旁边的复选框。

   如果设备由同一管理服务器管理，则可以选择多个设备：主管理服务器、从属管理服务器或虚拟服务器。

4. 在“**选择响应操作**”下拉列表中，选择“**移动到组**”。
“**移动到组**”窗口将在屏幕右侧打开，其中显示了管理选定设备的管理服务器所在的管理组。
5. 选择要将设备移动到的目标管理组，然后单击“**移动**”按钮。

选定设备将被移动到选定管理组。屏幕上会显示相应消息。

将设备从设备详情移动到其他管理组

要将设备从设备详情移动到其他管理组：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含待移动设备的警报的 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待移动设备的事故的 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
4. 在“**选择响应操作**”下拉列表中，选择“**移动到组**”。
“**移动到组**”窗口将在屏幕右侧打开，其中显示了管理选定设备的管理服务器所在的管理组。
5. 选择要将设备移动到的目标管理组，然后单击“**移动**”按钮。

选定设备将被移动到选定管理组。屏幕上会显示相应消息。

将设备从调查图移动到其他管理组

> 如果构建了调查图，则此选项可用。

要将设备从调查图移动到其他管理组：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待移动设备的事故的 ID。
2. 单击“**在图表上查看**按钮。
3. 在打开的调查图中，单击设备名称以打开设备详情。
4. 在“**选择响应操作**”下拉列表中，选择“**移动到组**”。
“**移动到组**”窗口将在屏幕右侧打开，其中显示了管理选定设备的管理服务器所在的管理组。
5. 选择要将设备移动到的目标管理组，然后单击“**移动**”按钮。

选定设备将被移动到选定管理组。屏幕上会显示相应消息。

更新数据库

为了快速检测威胁并确保客户端设备的保护级别保持最新，您必须定期更新设备上的数据库和应用程序模块。

您可以通过以下任一方式更新设备上的数据库：

- 从警报或事故详细信息操作
- 从设备详情操作
- 从调查图表操作

您也可以配置在创建或编辑行动手册时自动运行的响应操作。

> 要更新设备上的数据库，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

> 由于受管理设备和管理服务器之间存在同步间隔，响应操作启动可能需要长达 15 分钟。

从警报或事故详情更新数据库

要从警报或事故详情更新设备上的数据库：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含待更新数据库的设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待更新数据库的设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 选中待更新数据库的设备旁边的复选框。
   如有必要，您可以选择多个设备。
4. 在“**选择响应操作**”下拉列表中，选择“**更新数据库**”。

操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从设备详情更新数据库

要从设备详情更新设备上的数据库：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含待更新数据库的设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待更新数据库的设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
4. 在“**选择响应操作**”下拉列表中，选择“**更新数据库**”。

   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从调查图更新数据库

> 如果构建了调查图，则此选项可用。

要从调查图更新设备上的数据库：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待更新数据库的设备的事故 ID。
2. 单击“**在图表上查看**按钮。
3. 在打开的调查图中，单击设备名称以打开设备详情。
4. 在“**选择响应操作**”下拉列表中，选择“**更新数据库**”。

   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

更改设备的授权状态

当警报或事故分析显示设备的保护级别较低或设备会损害您的基础设施时，您可以更改设备的授权状态。

> 此响应操作可在安装了 KICS for Networks 的设备上执行。

您可以通过以下任一方式更改设备的授权状态：

- 从警报或事故详情操作
- 从设备详情操作

- 从遥测事件
- 从调查图表

您也可以配置在创建或编辑行动手册时自动运行的响应操作。

> 要更改设备的授权状态，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

从警报或事故详情中更改设备的授权状态

要从警报或事故详情中更改设备的授权状态：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含要更改授权状态的设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含要更改授权状态的设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 选中要更改授权状态的设备旁边的复选框。
   如有必要，您可以选择多个设备。
4. 在“**选择响应操作**”下拉列表中，选择“**更改授权状态**”。
5. 在屏幕右侧打开的窗口中，选择设备的新状态（*授权*或*未授权*），然后单击“**更改**”按钮。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从设备详情更改设备的授权状态

要从设备详情更改设备的授权状态：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含要更改授权状态的设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含要更改授权状态的设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
4. 在“**选择响应操作**”下拉列表中，选择“**更改授权状态**”。
5. 在屏幕右侧打开的窗口中，选择设备的新状态（*授权*或*未授权*），然后单击“**更改**”按钮。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从遥测事件更改设备的授权状态

要从遥测事件更改设备的授权状态：

1. 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含要更改授权状态的设备的警报 ID。
2. 在打开的窗口中，转到“**详细信息**”选项卡，然后执行以下操作之一：
   - 单击目标事件名称并选择设备。
   - 单击“**在威胁搜索中查找**”按钮，以转到“**威胁搜索**”部分，然后选择所需设备。
3. 在“**选择响应操作**”下拉列表中，选择“**更改授权状态**”。
4. 在屏幕右侧打开的窗口中，选择设备的新状态（*授权*或*未授权*），然后单击“**更改**”按钮。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

从调查图更改设备的授权状态

> 如果构建了调查图，则此选项可用。

要从调查图更改设备的授权状态：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含要更改授权状态的设备的事故 ID。
2. 在打开的窗口中，单击“**在图表上查看**”按钮。
   将打开调查图。
3. 单击设备名称以打开设备详情。
4. 在“**选择响应操作**”下拉列表中，选择“**更改授权状态**”。
5. 在屏幕右侧打开的窗口中，选择设备的新状态（*授权*或*未授权*），然后单击“**更改**”按钮。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

设备选定的授权状态显示在警报或事故卡片中，具体位置为“**资产**”选项卡 → “**授权状态**”列。

将文件移动至隔离区

为防止威胁传播，您可以通过以下任一方式将受感染的文件移至隔离区：

- 从警报或事故详情操作
- 从设备详情操作

- 从遥测事件
  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。
- 从调查图表操作
- 从资产表
- 从**响应历史**部分

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

> 要将文件移动至隔离区，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

> 由于受管理设备和管理服务器之间存在同步间隔，响应操作启动可能需要长达 15 分钟。

从警报或事故详细信息中响应

要从警报或事故详情将文件移动到隔离区：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含要移动至隔离区的文件所在设备的警报 ID。
   - 在主菜单中，前往**监控→事故**部分。在“**ID**”列中，单击包含要移动至隔离区的文件所在设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。

   > 您也可以转到“**可观察对象**”选项卡，选中要移动到隔离区的文件旁边的复选框，然后单击“**移动到隔离区**”按钮。

3. 选中要移动至隔离区的文件所在设备旁边的复选框。
   如有必要，您可以选择多个设备。
4. 在“**选择响应操作**”下拉列表中，选择“**移动到隔离区**”。
5. 在打开的右侧窗格中，执行以下操作：
   a. 在“**完整路径**”字段中，指定要移动到隔离区的文件的完整路径。
   b. 在“**资产**”字段中，选择要移动到隔离区的文件所在的设备。
      如果在步骤 2 中选择了“**资产**”选项卡，则默认情况下，您选中的复选框对应的设备名称会显示在“**资产**”字段中。您可以更改这些名称，并指定与警报或事故无关但属于警报或事故租户（及其子租户）的设备。

只有您可以对其执行响应操作的资产才可供选择。
设备显示方式如下：属于警报或事故的设备位于下拉列表开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

c. 如有必要，请在相应字段中配置以下设置：

- 指定文件的 SHA256 或 MD5 哈希值。

  如果在步骤 2 中选择了**可观察对象**选项卡，则会自动指定哈希值。您可以更改值。

- 为响应操作编写描述或注释。

6. 单击“**移动**”按钮。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

从设备详情中响应

要从设备详情中将文件移动至隔离区：

1. 执行以下操作之一：

- 在主菜单中，前往**监控→警报**部分。在“ID”列中，单击包含要移动至隔离区的文件所在设备的警报 ID。
- 在主菜单中，前往**监控→事故**部分。在“ID”列中，单击包含要移动至隔离区的文件所在设备的事故 ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。

4. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

从遥测事件响应

要从通过警报或事故详情打开的遥测事件中将文件移动到隔离区：

1. 在主菜单中，前往**监控→警报**部分。在“ID”列中，单击包含要移动至隔离区的文件所在设备的警报 ID。
2. 在打开的窗口中，转到“**详细信息**”选项卡，然后执行以下操作之一：
   - 单击目标事件名称并选择设备。
   - 单击“**在威胁搜索中查找**”按钮，以转到“**威胁搜索**”部分，然后选择所需设备。

     > 您也可以转到“**可观察对象**”选项卡，选中要移动到隔离区的文件旁边的复选框，然后单击“**移动到隔离区**”按钮。
3. 在“**选择响应操作**”下拉列表中，选择“**移动到隔离区**”。
4. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

要从通过“威胁搜索”部分打开的遥测事件中进行响应：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。
2. 单击您要打开其详情的事件名称。
3. 在打开的事件详细信息窗口中，单击设备名称，然后从打开的下拉列表中选择“**移动到隔离区**”。
4. 执行与“*从警报或事故详情中响应*”流程中步骤 5-6 相同的操作。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

从调查图响应

> 如果构建了调查图，则此选项可用。

要从调查图将文件移动至隔离区：

1. 在主菜单中，前往**监控→事故**部分。在“ID”列中，单击包含要移动至隔离区的文件所在设备的事故 ID。
2. 在打开的窗口中，单击“**在图表上查看**”按钮。
   将打开调查图。

3. 单击设备名称以打开设备详情。

4. 在“**选择响应操作**”下拉列表中，选择“**移动到隔离区**”。

5. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

从资产表响应

要从资产表中进行响应：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   这将打开资产表。

2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   > 已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择“**移动到隔离区**”。

4. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

从响应历史部分响应

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。

2. 在“**响应**”下拉列表中，选择“**移动到隔离区**”。

3. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

操作成功完成后，屏幕上将显示相应消息。文件将从其所在设备的目录中删除，并移动到同一设备上的隔离区目录中。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示**错误**消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

从隔离区恢复文件

如果您有理由相信已移动到隔离区的文件是安全的，则可以通过以下方式之一将文件恢复到设备上：

- 从主菜单的“**隔离**”部分。
- 根据**移动到隔离区**响应操作的结果。

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从“隔离”部分响应

要从“隔离”部分进行响应：

1. 在主菜单中，转到**存储库** → **隔离**。
2. 执行以下操作之一：
   - 选择要从隔离区恢复的文件。
     您可以选择多个文件。
   - 单击要从隔离区恢复的文件的名称。

   文件详情已打开。
3. 单击“**恢复**” 按钮，然后确认操作。
   如有必要，请在“**描述**”字段中输入注释，然后再确认操作。

如果操作成功完成，屏幕上将显示相应的消息。文件已恢复到您之前将其移动到隔离区的设备上，并且位于原始路径（您在“将文件移动到隔离区”场景的步骤 5 中指定的路径）。否则，将显示错误消息。

根据“**移动到隔离区**”响应操作的结果作出响应

要根据“移动到隔离区”响应操作的结果进行响应：

1. 您可以通过以下方式之一打开“**移动到隔离区**”响应操作的结果：

   - 在主菜单中，转到“**监控**” → “**响应历史**”。
   - 在主菜单中，转到“**监控**”，然后选择“**警报**”或“**事故**”部分。在“ID”列中，单击包含您已执行“**移动到隔离区**”响应操作的资产或观察点的警报或事故的 ID。在打开的警报或事故详情中，转到“**历史记录**”选项卡。

2. 要查看“**移动到隔离区**”响应操作的结果，请在“**操作状态**”列中单击“**成功**”链接。

3. 在打开的详情窗口中，单击“**恢复**”按钮，然后确认操作。

4. 如有必要，请在“**描述**”字段中输入注释，然后再确认操作。

操作成功完成后，屏幕上将显示相应消息。文件已恢复到您之前将其移动到隔离区的设备上，并且位于原始路径（您在“将文件移动到隔离区”场景的步骤 5 中指定的路径）。否则，将显示错误消息。

查看响应操作结果

如果带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上，则响应操作的结果将显示在“**响应历史**”部分。

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示**错误**消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

从隔离区获取文件

要执行响应操作，您必须具备以下条件：

- 以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。
- 带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上

可以从隔离区目录中获取设备上的隔离文件，以便进行进一步分析。获得的文件将显示在OSMP控制台的**文件**部分。

您可以通过以下方式之一执行此响应操作：

- 从主菜单的**隔离**部分。
- 根据**移动到隔离区**响应操作的结果。

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从“隔离”部分响应

要从“隔离”部分进行响应：

1. 在主菜单中，转到**存储库 → 隔离**。
2. 执行以下操作之一：
   - 选择要从隔离区获取的文件。
   - 单击要从隔离区获取的文件的名称。

   文件详情已打开。
3. 单击**获取文件**按钮，然后确认操作。

   如果您希望在文件获得后检查是否有威胁，请单击**获取和扫描**按钮。

如果操作成功完成，屏幕上将显示相应的消息，并从设备中获取隔离的文件。否则，将显示错误消息。

根据“移动到隔离区”响应操作的结果作出响应

要根据“移动到隔离区”响应操作的结果进行响应：

1. 您可以通过以下方式之一打开“**移动到隔离区**”响应操作的结果：
   - 在主菜单中，转到“**监控**” → “**响应历史**”。
   - 在主菜单中，转到“**监控**”，然后选择“**警报**”或“**事故**”部分。在“ID”列中，单击包含您对其执行了“**移动到隔离区**”响应操作的资产或可观测对象所属警报或事故的 ID。在打开的警报或事故详情中，转到“**历史记录**”选项卡。
2. 要查看“**移动到隔离区**”响应操作的结果，请在“**操作状态**”列中单击“**成功**”链接。
3. 在打开的详情窗口中，单击**获取文件**按钮，然后确认操作。

   如果您希望在文件获得后检查是否有威胁，请单击**获取和扫描**按钮。

查看响应操作结果

响应操作的结果将显示在以下位置：

- 在主菜单的**文件**部分
- 在主菜单的**响应历史**部分

  在点击**操作状态**列中的链接后，文件详情打开时会默认选中**结果**选项卡，您可以在其中查看并根据需要将受密码保护的ZIP压缩包下载到您的计算机中。密码已*感染*。

  如果响应操作未成功完成，屏幕上将显示**错误**消息和有关错误原因的信息。

  如果要查看启动 ID 和包含响应操作结果的 JSON，请转到"**调试数据**"选项卡。

从隔离区删除文件

要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1级分析师、2 级分析师。

您可以通过以下方式之一从设备上的隔离区目录中删除受感染的文件：

- 从 OSMP 控制台菜单的"**隔离**"部分操作
- 根据"**移动到隔离区**"响应操作的结果。

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从"隔离"部分响应

要从"隔离"部分进行响应：

1. 在主菜单中，转到**存储库 → 隔离**。
2. 执行以下操作之一：
   - 选择要从隔离区删除的文件。

     您可以选择多个文件。
   - 单击要从隔离区删除的文件的名称。

     文件详情已打开。
3. 单击"**删除**"按钮，然后确认操作。

操作成功完成后，屏幕上将显示相应消息。该文件已从其所在设备的隔离区目录中永久删除。否则，将显示错误消息。

根据“**移动到隔离区**”响应操作的结果作出响应

要根据“移动到隔离区”响应操作的结果进行响应：

1. 您可以通过以下方式之一打开“**移动到隔离区**”响应操作的结果：

   - 在主菜单中，转到“**监控**” → “**响应历史**”。
   - 在主菜单中，转到“**监控**”，然后选择“**警报**”或“**事故**”部分。在“ID”列中，单击包含您已执行“**移动到隔离区**”响应操作的资产或观察点的警报或事故的 ID。在打开的警报或事故详情中，转到“**历史记录**”选项卡。

2. 要查看“**移动到隔离区**”响应操作的结果，请在“**操作状态**”列中单击“**成功**”链接。

3. 在打开的详情窗口中，单击“**删除**”按钮，然后确认操作。

   操作成功完成后，屏幕上将显示相应消息。该文件已从其所在设备的隔离区目录中永久删除。否则，将显示错误消息。

查看响应操作结果

如果带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上，则响应操作的结果将显示在“**响应历史**”部分。

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示**错误**消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

查看有关 KASAP 用户的信息并更改学习组

完成 KASAP 和 KUMA 之间的集成配置后，在查看与警报或事故关联的用户数据时，OSMP Console 将提供来自 KASAP 的以下信息：

- 用户所属的学习组。
- 用户完成的学习课程。
- 计划的学习课程及其当前进度。

您可以查看有关 KASAP 用户的数据。为此，您必须通过以下方式之一打开用户详细信息：

- 从警报或事故详情操作
- 从遥测事件中（如果从警报详情中打开的话）。

- 从调查图中打开。

  如果构建了调查图，则此选项可用。

要打开用户详细信息：

1. 在主菜单中，转到“**监控**”，然后选择“**警报**”或“**事故**”部分。
   如果要从遥测事件中打开用户详细信息，请选择“**警报**”部分。
   如果要从调查图中打开用户详细信息，请选择“**事故**”部分。
2. 单击所需警报或事故的 ID。
3. 在打开的窗口中，执行以下操作之一：
   - 如果要从遥测事件中打开用户详细信息，请转到“**详细信息**”选项卡，然后单击所需事件的名称并选择用户；或者单击“**威胁搜索中查找**”按钮以转到“**威胁搜索**”部分，然后选择所需用户。
   - 如果要从警报或事故详情中打开用户详情，请转到“**资产**”选项卡，然后单击所需用户的名称。
   - 如果要从调查图中打开用户详细信息，请单击“**在图表上查看**按钮。在打开的调查图中，单击所需用户的名称。

   “**账户详情**”窗口将在屏幕右侧打开。
4. 选择“**网络安全课程**”选项卡。
   该窗口将显示有关 KASAP 用户的信息。

您可以通过以下方式之一更改 KASAP 用户的学习组：

- 从警报或事故详细信息中更改
- 从遥测事件中（如果从警报详情中打开的话）。
- 从调查图

  如果构建了调查图，则此选项可用。

您还可以配置在创建或编辑行动手册时自动运行的响应操作。在这种情况下，如果将用户移动到未开始学习的分组，则用户将无法开始学习。

要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

要更改 KASAP 用户学习组：

1. 在主菜单中，转到“**监控**”，然后选择“**警报**”或“**事故**”部分。
   如果您想从遥测事件更改 KASAP 用户学习组，请选择“**警报**”部分。
   如果您想从调查图更改 KASAP 用户学习组，请选择“**事故**”部分。
2. 单击所需警报或事故的 ID。

3. 在打开的窗口中，执行以下操作之一：

   - 如果要通过遥测事件响应，请转到“**详细信息**”选项卡，单击所需事件名称，然后选择用户；或者，单击“**在威胁搜索中查找**”按钮以转到“**威胁搜索**”部分，然后选择所需用户。
   - 如果您想通过用户详细信息响应，请转到“**资产**”选项卡，然后单击用户名称。
   - 如果您想通过调查图响应，请单击“**在图表上查看**按钮。在打开的调查图中，单击用户名称。

   “**账户详情**”窗口将在屏幕右侧打开。

4. 在“**分配 KASAP 组**”下拉列表中，选择要分配给该用户的 KASAP 学习组。

   重新计算 KASAP 用户培训计划可能需要长达 30 分钟。在此期间不建议更改 KASAP 学习组。

   该用户被移动到所选 KASAP 分组。KASAP 公司管理员将收到有关学习组更改的通知，并将为选定的学习组重新计算学习计划。

有关学习小组以及如何开始的详细信息，请参阅 KASAP 文档。

启用和禁用网络隔离

您可以通过以下方式之一启用和禁用设备上的网络隔离：

- 从警报或事故详情操作
- 从设备详情操作
- 从调查图表操作
- 从资产表
- 从事件详情

  此选项仅在启用网络隔离时可用。

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

如果带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上，则网络隔离状态将显示在“设备详情”中。

设备可能具有以下状态之一：*已隔离*、*正在隔离*、*应用隔离时出错*、*未隔离*。

此外，当您从警报或事故详情的“**资产**”选项卡或通过“**资产管理**” → “**资产(设备)**”**打开资产表时，也会在资产表中看到网络隔离状态。**您可以过滤资产表中**隔离状态**列的值，以显示具有所需网络隔离状态的设备。

从警报或事故详情中执行响应操作

要从警报或事故详情中进行响应：

1. 执行以下操作之一：

   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

3. 选择所需设备旁边的复选框。
   如有必要，您可以选择多个设备。

4. 在**选择响应操作**下拉列表中，选择**“网络隔离”**，然后在上下文菜单中，选择要执行的响应操作：

   - **启用**
     如果您为已启用网络隔离的设备选择此响应操作，则参数将被新值覆盖。

     > 启用网络隔离之前，请确保已从 Kaspersky Security Center 导入资产：在**任务** → **检测和响应**中，KSC **资产导入**任务显示为已完成状态。

   - **禁用**
     选择此响应操作后，在确认对话框中，单击**禁用**。
     您可以为启用了网络隔离的设备选择此响应操作。

5. 如果选择了“**启用**”，则可以在打开的右侧窗格中配置以下设置：

   a. 在**资产**下拉列表中，指定要隔离的设备。
      默认情况下，会显示您之前选择的复选框的设备。如果需要的话，您可以更改设备。您无法选择具有以下状态的设备：**已隔离**、**正在隔离**、**应用隔离错误**。

      > 只有可对其执行响应操作的设备才可供选择。
      > 设备显示方式如下：属于警报或事故的设备位于下拉列表开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

   b. 指定设备隔离的时间段和单位。

   c. 在**描述**字段中，编写对响应操作的描述或注释。

d. 如果需要添加网络隔离规则的例外项，请单击**添加排除项**按钮，然后在**网络流量方向**下拉列表中选择以下值之一：

- **入站**，然后在相应的字段中指定要从网络流量阻止中排除的设备的 IP 地址和本地端口范围。
- **出站**，然后在相应的字段中指定要从网络流量阻止中排除的设备的 IP 地址和远程端口范围。
- **入站/出站**，然后指定要从网络隔离中排除的设备的 IP 地址。

6. 单击“**启用**”按钮。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从设备详情执行响应操作

要从设备详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
4. 执行与*从设备详情执行响应操作*中步骤4-6相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从调查图执行响应操作

> 如果构建了调查图，则此选项可用。

要从调查图中进行响应：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，单击“**在图表上查看**”按钮。
   将打开调查图。
3. 单击设备名称以打开设备详情。
4. 执行与*从设备详情执行响应操作*中步骤4-6相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从资产表执行响应操作

要从资产表中进行响应：

1. 在主菜单中，转到 **资产管理 → 资产(设备)。**
   这将打开资产表。
2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择下列选项之一：
   - **启用网络隔离**，然后在打开的右侧窗格中配置响应操作设置。
   - **禁用网络隔离**，然后在确认对话框中单击“**禁用**”。

从事件详情启用网络隔离

要从事件详情启用网络隔离：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。
2. 单击您要打开其详情的事件名称。
3. 在打开的事件详情窗口中，单击设备名称，然后从打开的下拉列表中选择“**启用网络隔离**”。
4. 在打开的右侧窗格中，配置响应操作设置。

如果您的设备尚未安装具有内置代理的 Kaspersky Endpoint Security 应用程序，并且在执行响应操作时出现错误，请确保 Kaspersky Next XDR Expert 中的设备名称与版本低于 8.0 的 Kaspersky Anti Targeted Attack Platform 中的设备名称一致。

执行“添加防护规则”和“删除防护规则”响应操作

预防规则允许您阻止您认为不安全的文件或进程在设备上运行。Kaspersky Next XDR Expert使用MD5和SHA256哈希值算法根据其哈希值识别文件。

您可以通过以下方式之一配置**添加防护规则**和**删除防护规则**响应操作，以添加和删除设备或文件哈希值的阻止规则：

- 从警报或事故详情操作
- 从设备详情操作
- 从调查图表操作
- 从资产表
- 从**响应历史**部分
- 从事件详情
  此选项适用于 **添加防护规则** 响应操作。您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。
- 从文件详情

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

> 要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

从警报或事故详情中执行响应操作

要从警报或事故详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**警报 ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**事故 ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 选择所需设备旁边的复选框。
   如有必要，您可以选择多个设备。
4. 在**选择响应操作**下拉列表中，选择**管理防护规则**，然后在上下文菜单中，选择要执行的响应操作：
   - **添加防护规则**
   - **删除防护规则**

5. 在打开的窗口中，设置您在步骤 4 中选择的响应操作的必要参数：

- **对于添加阻止规则**

  在打开的右侧窗格中，配置以下设置：

  1. 在“**MD5 或 SHA256**”字段中，指定要阻止的文件的哈希值。

     如果要指定多个哈希值，请单击**添加哈希值**按钮。

  2. 如果必要，配置以下设置：

     - 更改响应操作的范围。

       默认情况下，在**范围**设置中，**特定资产**选项处于选中状态，并且**资产**下拉列表中包含您之前选中了复选框的设备名称。

       您可以更改要添加防御规则的设备，或选择“**范围**”设置组中的“**所有资产**”选项，为属于警报或事故租户及其子租户的所有设备添加防御规则。

       > 只有您可以对其执行响应操作的资产才可供选择。
       > 设备显示方式如下：属于警报或事故的设备位于下拉列表的开头，然后按字母顺序显示属于警报或事故租户和子租户的设备。

     - 启用“**通知用户有关阻止文件执行的信息**”拨动开关。

     - 在**描述**字段中，编写对响应操作的描述或注释。

  3. 然后单击“**添加**”按钮。

  窗口将被关闭。

- **对于删除阻止规则**

  在打开的右侧窗格中，配置以下设置：

  1. 选择要删除的对象。

     默认情况下，在“**规则**”设置组中，“**特定规则**”选项已选中。如果要通过文件哈希删除防御规则，请在“**MD5 或 SHA256**”字段中指定要删除的文件的哈希值。如果要指定多个哈希值，请单击**添加哈希值**按钮。

     如果要删除所有防御规则，请选择“**所有规则**”选项。

  2. 如果必要，配置以下设置：

     - 更改响应操作的范围。

       默认情况下，在**范围**设置中，**特定资产**选项处于选中状态，并且**资产**下拉列表中包含您之前选中了复选框的设备名称。

       您可以更改要删除防御规则的设备，或选择“**范围**”设置组中的“**所有资产**”选项，以删除属于警报或事故租户及其子租户的所有设备的防御规则。

只有您可以对其执行响应操作的资产才可供选择。
设备显示方式如下：属于警报或事故的设备位于下拉列表开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

- 在**描述**字段中，编写对响应操作的描述或注释。

3. 下一步，单击“**删除**”按钮。

窗口将被关闭。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从设备详情执行响应操作

要从设备详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**警报 ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**事故 ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
4. 执行与“*从设备详情执行响应操作*”中步骤 4-5 相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从调查图执行响应操作

如果构建了调查图，则此选项可用。

要从调查图中进行响应：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**事故 ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，单击“**在图表上查看**”按钮。
   将打开调查图。
3. 单击设备名称以打开设备详情。
4. 执行与“*从设备详情执行响应操作*”中步骤 4-5 相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从资产表执行响应操作

要从资产表中进行响应：

1. 在主菜单中，转到 **资产管理 → 资产(设备)。**
   这将打开资产表。
2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   > 已存档的设备无法选择。

3. 在 **响应** 下拉列表中，选择 **管理防护规则**，然后在上下文菜单中选择要执行的响应操作。
4. 在打开的右侧窗格中，按照“*从警报或事故详情执行响应操作*”中的步骤 5 所述配置响应操作设置。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从响应历史执行响应操作

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。
2. 在**响应**下拉列表中，选择**添加防护规则**或**删除防护规则**。
3. 在打开的右侧窗格中，按照“*从警报或事故详情执行响应操作*”中的步骤 5 所述配置响应操作设置。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从事件详情中执行响应操作

> 此选项适用于 **添加防护规则** 响应操作。

要从事件详情中执行响应操作：

1. 在主菜单中，前往**监控→警报**部分。在“ID”列中，单击包含所需设备的警报 ID。
2. 在打开的窗口中，转到“**详细信息**”选项卡，然后选择所需的文件哈希值。

3. 单击**添加阻止规则**按钮，然后选择要为其添加阻止规则的设备。

> 您还可以转到“**可观察对象**”选项卡，然后选中要阻止的文件哈希旁边的复选框。在“**选择响应操作**”下拉列表中，单击“**管理防御规则**”，然后选择“**添加防护规则**”或“**删除防护规则**”。

4. 执行与“*从设备详情执行响应操作*”中步骤 4-5 相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

在打开的事件详情窗口中，在“主机名”字段中单击设备名称，然后从打开的下拉列表中选择“添加防御规则”。

执行与“从设备详情执行响应操作”中步骤 5 所述相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则会显示“**成功**”消息和“**查看资产**”按钮。您可以单击该按钮，然后在打开的窗口中转到“**防护规则**”选项卡，查看设备上防御规则的状态。

否则，将显示错误消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

> 如果您的设备尚未安装带有内置代理的 Kaspersky Endpoint Security 应用程序，并且在执行响应操作时出现错误，请确保 Kaspersky Next XDR Expert 中的设备名称与版本低于 8.0 的 Kaspersky Anti Targeted Attack Platform 中的设备名称相匹配。

运行程序

您可以通过以下方式之一执行响应操作：

- 从警报或事故详情操作
- 从设备详情操作
- 从调查图表操作
- 从资产表

- 从**响应历史**部分
- 从事件详情

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

> 要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

从警报或事故详情中执行响应操作

要从警报或事故详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 选择所需设备旁边的复选框。
   如有必要，您可以选择多个设备。
4. 在**选择响应操作**下拉列表中，选择**运行**，然后在上下文菜单中，单击**程序**。
5. 在打开的右侧窗格中，执行以下操作：
   a. 在“**完整路径**”字段中，指定要运行的可执行文件的完整路径。
   b. 如果必要，配置以下设置：
      - 更改响应操作的范围。
        默认情况下，在**范围**下拉列表中，**特定资产**选项已选中，并且**资产**下拉列表包含您之前选择的复选框的设备名称。这意味着，该可执行文件将在这些设备上运行。
        您可以更改设备或选择“**范围**”下拉列表中的“**所有资产**”选项，以在属于警报或事故租户（及其子租户）的所有设备上运行可执行文件。

只有可对其执行响应操作的资产才可供选择。
设备将按如下方式显示：属于警报或事故的设备将显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

- 在"**命令行参数**"字段中，指定运行可执行文件的其他选项，例如：`/all argument`。
- 在"**工作目录**"字段中，指定工作目录。
- 在**描述**字段中，编写对响应操作的描述或注释。

6. 单击"**运行**"按钮。

窗格关闭。窗口将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从设备详情执行响应操作

要从设备详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在"ID"列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到"**监控**" → "**事故**"部分。在"ID"列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，转到"**资产**"选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择"**查看属性**"。
4. 执行与"*从设备详情执行响应操作*"流程中步骤 4-6 相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从调查图执行响应操作

如果构建了调查图，则此选项可用。

要从调查图中进行响应：

1. 在主菜单中，转到"**监控**" → "**事故**"部分。在"ID"列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，单击"**在图表上查看**"按钮。
   将打开调查图。

3. 单击设备名称以打开设备详情。

4. 执行与“*从设备详情执行响应操作*”流程中步骤 4-6 相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

如果您的设备尚未安装带有内置代理的 Kaspersky Endpoint Security 应用程序，并且在执行响应操作时出现错误，请确保 Kaspersky Next XDR Expert 中的设备名称与版本低于 8.0 的 Kaspersky Anti Targeted Attack Platform 中的设备名称相匹配。

从资产表执行响应操作

要从资产表中进行响应：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   这将打开资产表。

2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择“**程序**”。

4. 在打开的右侧窗格中，按照“*从设备详情执行响应操作*”流程中的步骤 4-6 所述配置响应操作设置。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从响应历史执行响应操作

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。

2. 在“**Response**”下拉列表中，选择“**程序**”。

3. 在打开的右侧窗格中，按照“*从设备详情执行响应操作*”流程中的步骤 4-6 所述配置响应操作设置。 程序。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从事件详情执行响应操作

要从事件详情执行响应操作：

1. 在主菜单中，转到**“监控”** → **“威胁搜索”。**
   事件表随即打开。
2. 单击您要打开其详情的事件名称。
3. 在打开的事件详情窗口中，单击设备名称，然后从打开的下拉列表中选择“**程序**”。
4. 在打开的右侧窗格中，按照“*从设备详情执行响应操作*”流程中的步骤 4-6 所述配置响应操作设置。

   如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示错误消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

管理服务

您可以远程启动、停止、暂停、恢复或删除设备上的服务。

要执行“**管理服务**”响应操作，您必须具备以下条件：

- 以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。
- 带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上

您可以通过以下方式之一执行响应操作：

- 从警报或事故详情操作
- 从设备详情操作
- 从遥测事件
  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。

- 从调查图

  > 如果构建了调查图，则此选项可用。

- 从资产表
- 从**响应历史**部分

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从警报或事故详情中响应

要从警报或事故详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。
2. 在打开的窗口中，转到“**资产**”选项卡。

   > 您也可以转到**可观察对象**选项卡，选中要执行响应操作的警报旁边的复选框，然后点击**管理服务**。

3. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。
4. 在“**选择响应操作**”下拉列表中，选择“**管理服务**”。
5. 在打开的右侧窗格中，在相应的字段中配置以下设置：
   a. 您希望在其上管理该服务的设备。
      默认情况下，在**范围**设置组中，**特定资产**选项处于选中状态，**资产**下拉列表中包含您在步骤 3 中选中复选框的设备名称。
      您可以更改设备或选择设置的**范围**组中的**所有资产**选项，以在属于警报或事故租户（及其子租户）的所有设备上管理服务。

      > 只有可对其执行响应操作的资产才可供选择。
      > 设备将按如下方式显示：属于警报或事故的设备将显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

   b. 服务名称。
   c. 要对服务执行的操作：**修改启动类型**、**开始**、**停止**、**暂停**、**恢复**或**删除**。
      如果选择**修改启动类型**操作，则必须在**新的启动类型**字段中选择对应值。

强烈不建议停止、暂停、删除服务，或更改会影响主机运行的服务的启动类型。
不建议管理的服务列表

- AVP*
- BFE
- CertPropSvc
- CoreMessagingRegistrar
- CryptSvc
- DcomLaunch
- Dhcp
- DispBrokerDesktopSvc
- EventLog
- EventSystem
- LanmanServer
- LanmanWorkstation
- LSM
- mpssvc
- Netlogon
- Netman
- PlugPlay
- PolicyAgent
- Power
- ProfSvc
- RasMan
- RpcEptMapper
- RpcSs
- SamSs
- SCardSvr
- SecurityHealthService

- SessionEnv
- Spooler
- SstpSvc
- TermService
- UmRdpService
- UserManager
- UsoSvc
- VaultSvc
- W32Time
- WebClient
- Winmgmt
- WlanSvc
- wscsvc

d. 如果必要，配置以下设置：

- 指定文件的 SHA256 或 MD5 哈希值。
  如果在步骤 2 中选择了**可观察对象**选项卡，则会自动指定哈希值。您可以更改值。
- 为响应操作编写描述或注释。

6. 单击“**启动**”按钮。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从设备详情中响应

要从设备详情中进行响应：

1. 执行以下操作之一：

- 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含所需设备的警报 ID。
- 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
   “设备详情”面板随即打开。

4. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从遥测事件响应

要从通过警报或事故详情打开的遥测事件中进行响应：

1. 执行以下操作之一：

   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含所需设备的警报 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。

2. 在打开的窗口中，转到“**详细信息** ”选项卡，然后执行以下操作之一：

   - 单击目标事件名称并选择设备。
   - 单击**在威胁搜索中查找**按钮，转到**威胁搜索**部分，然后选择所需设备。

3. 执行与“*从警报或事故详情中响应*”流程中步骤 4-6 相同的操作。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

要从通过“威胁搜索”部分打开的遥测事件中进行响应：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。

2. 单击您要打开其详情的事件名称。

3. 在打开的事件详情面板中，单击设备名称，然后从下拉列表中选择**管理服务**。

4. 在打开的右侧面板中，按照*从警报或事件详情中响应*第5步中所述配置响应操作设置，然后启动响应操作。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从调查图响应

要从调查图中进行响应：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含所需设备的事故 ID。

2. 单击“**在图表上查看**按钮。

3. 在打开的调查图中，单击设备名称，然后在下拉列表中选择“**查看属性**”。

4. 在打开的“设备详情”面板中，执行*从警告或事故详情中响应*第4-6步中所述的相同操作。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从资产表响应

要从资产表中进行响应：

1. 在主菜单中，转到 **资产管理 → 资产(设备)。**
这将打开资产表。

2. 选中要执行响应操作的设备旁边的复选框。
您可以选择多个设备。

> 已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择“**管理服务**”。

4. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”流程中的步骤 5-6 所述来配置响应操作设置。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从响应历史部分响应

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
将打开包含所有警报和事故的响应历史记录的表格。

2. 在“**响应**”下拉列表中，选择“**管理服务**”。

3. 在打开的右侧面板中，按照*从警报或事件详情中响应*第5步中所述配置响应操作设置，然后启动响应操作。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示**错误**消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

通过 Kaspersky NGFW 阻止 IP 地址

您可以通过将 IP 地址添加到阻止列表，从而阻止潜在威胁的传播以及联网设备上的恶意活动。

如果 Open Single Management Platform 分发包中包含 Kaspersky NGFW Web 插件，则可以执行响应操作。要通过 Kaspersky NGFW 执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

您可以通过以下方式之一执行响应操作：

- 从警报或事故详情操作
- 从遥测事件
  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从警报或事故详情中响应

要从警报或事故详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**可观察对象**”选项卡。
3. 勾选要阻止其 IP 地址的设备旁边的复选框。
4. 在“**选择响应操作**”下拉列表中，选择“**将 IP 添加到网络设备上的阻止列表**”响应操作。

   窗口将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从遥测事件响应

要从通过警报或事故详情打开的遥测事件中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**详细信息** ”选项卡，然后执行以下操作之一：
   - 单击所需事件的名称。
3. 单击“**在威胁搜索中查找**”按钮，以转到“**威胁搜索**”部分，然后单击所需事件的名称。
4. 在打开的事件详细信息窗口中，单击包含要阻止的设备的 IP 地址的链接，然后从下拉列表中选择“**将 IP 添加到网络设备上的阻止列表**”。

   窗口将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

要从通过“威胁搜索”部分打开的遥测事件中进行响应：

1. 在主菜单中，转到“**监控**”→“**威胁搜索**”。
   事件表随即打开。
2. 单击您要打开其详细信息的事件名称。
3. 在打开的事件详细信息窗口中，单击包含要阻止的设备的 IP 地址的链接，然后从下拉列表中选择“**将 IP 添加到网络设备上的阻止列表**”。

   窗口将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

获取文件以供进一步分析

本部分包含旨在获取安全漏洞证据的响应操作，以便进一步调查。您可以获取：

- 文件
- 注册表键
- NTFS 元文件
- 取证
- 磁盘镜像
- 内存转储
- 进程内存转储

要执行响应操作，您必须具备以下条件：

- 以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。
- 带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上

您可以通过以下方式之一执行响应操作：

- 从警报或事故详情操作
- 从设备详情操作
- 从遥测事件
  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。
- 从调查图

  > 如果构建了调查图，则此选项可用。

- 从资产表
- 从**响应历史**部分

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从警报或事故详情中响应

要从警报或事故详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“ID”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“ID”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 选中要执行响应操作的设备旁边的复选框。
   如果要执行“**注册表键**”或“**取证**”响应操作，您可以选择多个设备。
4. 在“**选择响应操作**”下拉列表中，单击“**获取**”。
5. 在打开的上下文菜单中，选择所需的响应操作。

从设备详情中响应

要从设备详情中进行响应：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**资产**”选项卡。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
   “设备详情”窗口打开。
4. 在“**选择响应操作**”下拉列表中，单击“**获取**”。
5. 在打开的上下文菜单中，选择所需的响应操作。

从遥测事件响应

要从通过警报或事故详情打开的遥测事件中执行响应操作：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**详细信息** ”选项卡，然后执行以下操作之一：
   - 单击目标事件名称并选择设备。
   - 单击**在威胁搜索中查找**按钮，转到**威胁搜索**部分，然后选择所需设备。
3. 在“**选择响应操作**”下拉列表中，单击“**获取**”。
4. 在打开的上下文菜单中，选择所需的响应操作。

要从通过“威胁搜索”部分打开的遥测事件中进行响应：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。
2. 单击您要打开其详情的事件名称。
3. 在打开的事件详情窗口中，单击设备名称，然后从打开的下拉列表中选择所需的响应操作。

从调查图响应

要从调查图中进行响应：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“ID”列中，单击包含要执行响应操作的设备的事故 ID。
2. 在打开的窗口中，单击“**在图表上查看**”按钮。
   将打开调查图。
3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。
   “设备详情”窗口打开。
4. 在“**选择响应操作**”下拉列表中，单击“**获取**”。
5. 在打开的上下文菜单中，选择所需的响应操作。

从资产表响应

要从资产表中进行响应：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   这将打开资产表。
2. 选中要执行响应操作的设备旁边的复选框。
   如果要执行“ 取证”或“注册表键”响应操作，您可以选择多个设备。

   > 已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择所需的响应操作。

从响应历史部分响应

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。
2. 在“**响应**”下拉列表中，选择所需的响应操作。

获取文件

要获取文件：

1. 选择文件响应操作。
   “**获取文件**”窗格随即打开。
2. 在“**完整路径**”字段中，指定要获取的文件的路径。
3. 如果必要，配置以下设置：
   - 在**资产**下拉列表中，更改要获取文件的设备。
   - 默认情况下，此字段包含您之前选中的复选框对应的设备名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

     只有可对其执行响应操作的资产才可供选择。
     设备将按如下方式显示：属于警报或事故的设备将显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。
   - 在“**MD5 或 SHA256**”字段中，指定要获取的文件的哈希值。
   - 如果您不想扫描文件，请禁用“**扫描文件**”选项。
     默认情况下已启用该选项。这意味着在获取文件后，会对文件进行威胁检查。

     在行动手册中启动响应操作时，如果要扫描获取的文件，则必须手动添加此选项。
   - 在**描述**字段中，编写对响应操作的描述或注释。
4. 单击“**获取**”按钮。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，文件将保存到 ZIP 压缩包中。密码已*感染*。

查看响应操作结果

您可以通过以下方式之一查看和下载该存档：

- 从主菜单的响应历史部分，或从警报或事故详情中的历史记录选项卡
- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。

如果在步骤 2 中您没有禁用“**扫描文件**”选项，则文件扫描结果会同步显示。单击**操作状态**列中的链接后，将打开文件详情页面并选中**结果**选项卡，您可以在其中查看扫描结果，并根据需要将文件下载到计算机。

获取注册表键

若要获取注册表键：

1. 选择注册表键响应操作。

   “**获取注册表键**”窗格随即打开。

2. 在“**注册表键的相对路径**”字段中，采用以下格式之一指定要获取的注册表键的路径：

   - 相对于根键的路径，例如：

     \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

   - 使用根键完整名称的相对路径，例如：

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

   - 使用根键缩写（而非完整名称）的相对路径，例如：

     HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

3. 如果必要，配置以下设置：

   - 在**资产**下拉列表中，更改要从中获取注册表项的设备。

     默认情况下，该字段包含您之前选中其复选框的设备的名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

     > 只有可对其执行响应操作的资产才可供选择。
     > 设备按如下方式显示：属于警报或事故的设备显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

4. 在**描述**字段中，编写对响应操作的描述或注释。

5. 单击“**获取**”按钮。

   窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，系统会生成一个REG文件。该文件包含您指定路径下的注册表键及其值的列表。

查看响应行动结果

您可以通过以下方式之一查看和下载该文件：

- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。
- 从主菜单的响应历史部分，或从警报或事故详细信息中的历史记录选项卡

  点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，屏幕上会显示**成功**消息和生成的文件。否则，将显示**错误**消息以及有关错误原因的信息。

  如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

获取 NTFS 元文件

获取 NTFS 元文件任务仅检索文件的默认数据流。不支持备用（命名）数据流。

要获取 NTFS 元文件：

1. 选择NTFS 元文件响应操作。
   “**获取 NTFS 元文件**”窗格随即打开。
2. 在“**元文件**”字段中，选中要获取的元文件旁边的复选框：
   - $MFT
   - $LogFile
   - $Boot
   - $Secure
   - $Extend/$UsnJrnl
3. 在“**卷**”字段中，指定要从中获取元文件的磁盘名称。
   默认情况下，“*%SystemDrive%*”值已指定。
4. 如果必要，配置以下设置：
   - 在**资产**下拉列表中，选择要从中获取元文件的设备。
     默认情况下，此字段包含您之前选中的复选框对应的设备名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

     只有可对其执行响应操作的资产才可供选择。
     设备显示如下：属于警报或事故的设备显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及子租户的设备。
   - 在“**描述**”字段中，您可以为响应操作编写描述或注释。
5. 单击“**获取**”按钮。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，NTFS 元文件将保存到 ZIP 存档中。

查看响应操作结果

您可以通过以下方式之一查看和下载该存档：

- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。
- 从主菜单的响应历史部分，或从警报或事故详细信息中的历史记录选项卡

  点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”消息和获取的文件。否则，将显示**错误**消息以及有关错误原因的信息。

  如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

获取取证信息

要获取取证信息：

1. 选择取证响应操作。

   “**获取取证**”窗格随即打开。

2. 在**信息类型**部分中，选中要获取的数据类型旁边的复选框：

   - **进程列表**。用于查看设备上正在运行的进程列表。
   - **自动运行点列表**。用于查看自动运行点列表。

     该列表包含有关已添加到启动文件夹或在“Run”注册表键中注册的应用程序的信息，以及在指定设备被启动和用户登录到设备上的操作系统时自动运行的应用程序的信息。

     支持的自动运行点列表

     支持以下类型的自动运行点：

     - 登录
     - Shell
     - Office
     - 浏览器
     - 计划器
     - 服务
     - 驱动程序
     - 加密
     - 调试器
     - COM
     - SessionManager

- 网络
- LSA
- 应用程序
- WMI
- GroupPolicy
- DriverLog
- BootLog
- 过程
- OsUpdate
- 打印机
- 未指定
- OsLoader
- EfiLoader

- **文件列表**。用于查看磁盘上存储的文件和文件夹列表。

> 列表中最多可显示20,000个文件。

3. 如果您选中了"**文件列表**"复选框，请执行以下操作：

   a. 通过选择以下设置组之一来指定文件搜索范围：

   - **所有本地磁盘**。该列表将包含存储在本地磁盘所有文件夹中的文件。
   - **文件夹**，然后在"**初始文件夹**"字段中，指定文件搜索的起始文件夹路径。
     列表将包含存储在指定文件夹及其子文件夹中的文件。

   b. 如有必要，请指定以下文件夹内文件的搜索条件：

   - 要包含在文件列表中的文件掩码。
   - "**备用数据流**"选项，用于在文件列表中记录有关备用数据流的信息。
     默认情况下，切换开关处于打开状态。
   - 应用程序搜索文件时文件夹的最大嵌套级别。
   - 在**排除项**字段中，指定要禁止搜索文件信息的文件夹路径。

4. 如果必要，配置以下设置：

- 在**资产**下拉列表中，选择要从中获取取证信息的设备。

默认情况下，该字段包含您之前选中其复选框的设备的名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

只有可对其执行响应操作的资产可供选择。
设备显示如下：属于警报或事故的设备显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及子租户的设备。

- 在**描述**字段中，编写对响应操作的描述或注释。

5. 单击“**获取**”按钮。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，所选数据将保存到受密码保护的 ZIP 存档中。密码已*感染*。

查看响应操作结果

您可以通过以下方式之一查看和下载该存档：

- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。
- 从主菜单的响应历史部分，或从警报或事故详情中的历史记录选项卡

  点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则会显示“**成功**”消息和获取的文件。否则，将显示**错误**消息以及有关错误原因的信息。

  如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

获取磁盘映像

要获取磁盘映像：

1. 选择磁盘镜像响应操作。

   “**获取磁盘镜像**”窗格随即打开。

2. 在**共享网络资源的路径**字段中，以UNC格式指定共享网络资源的路径。

3. 在“**用户名**”字段中，选择用于访问共享网络资源的账户的用户名。

   您必须预先在租户设置中配置访问共享网络资源的凭证。

4. 在“**磁盘类型**”设置组中，选择以下选项之一：

   - **逻辑**，然后在“**卷**”字段中，指定驱动器号，不带冒号和斜杠，例如 E 或 C。

     默认值是“%SystemDrive%”。

- **物理**，然后在“**物理驱动器**”字段中，按以下格式指定磁盘路径：
  - 对于安装了 Kaspersky Endpoint Security for Windows 的设备：\\.\PHYSICALDRIVE0、\\.\PHYSICALDRIVE1、\\.\PHYSICALDRIVE2
  - 对于安装了 Kaspersky Endpoint Security for Linux 的设备：/dev/sda

5. 如果要将磁盘映像文件分割成多个部分，请启用“**将文件拆分成几部分**”选项，然后指定保存文件单个部分的最小大小（以 GB 为单位）。
6. 如果必要，配置以下设置：
   - 在**资产**下拉列表中，更改要获取磁盘映像的设备。

     默认情况下，此字段包含您之前选中的复选框对应的设备名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

     > 只有可对其执行响应操作的资产可供选择。
     > 设备显示如下：属于警报或事故的设备显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及子租户的设备。

   - 在**描述**字段中，编写对响应操作的描述或注释。
7. 单击“**获取**”按钮。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，磁盘映像将保存到 EWF 文件中。

> 这些文件无法被覆盖：如果目标文件夹中已存在同名文件，则 EWF 文件的名称将包含一个后缀，例如 Filename-1。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则会显示“**成功**”消息以及位于共享网络资源中的内存磁盘映像文件的路径。您可以复制该路径。

否则，将显示**错误**消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

> 您无法直接从响应操作结果跳转到共享网络资源。

获取内存转储

若要获取内存转储：

1. 选择选定的内存转储响应操作。
   获取内存转储窗格随即打开。
2. 在**共享网络资源的路径**字段中，以UNC格式指定共享网络资源的路径。
3. 在"**用户名**"字段中，选择用于访问共享网络资源的账户的用户名。

   > 您必须预先在租户设置中配置访问共享网络资源的凭证。

4. 如果必要，配置以下设置：
   - 在**资产**下拉列表中，选择要从中获取内存转储的设备。
     默认情况下，此字段包含您之前选中的复选框对应的设备名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

     > 只有可对其执行响应操作的资产可供选择。
     > 设备显示如下：属于警报或事故的设备显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及子租户的设备。

   - 在**描述**字段中，编写对响应操作的描述或注释。
5. 单击"**获取**"按钮。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，磁盘映像将保存到 RAW 文件中。

> 这些文件无法被覆盖：如果目标文件夹中已存在同名文件，则 RAW 文件的名称将包含一个后缀，例如 Filename-1。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，屏幕上讲显示**成功**消息以及位于共享网络资源中的内存转储文件的路径。您可以复制该路径。

否则，将显示**错误**消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

> 您无法直接从响应操作结果跳转到共享网络资源。

获取进程内存转储

若要获取进程内存转储：

1. 选择进程内存转储响应操作。
   “**获取进程内存转储**”窗格随即打开。
2. 在“**进程 ID**”字段中，指定您想获取内存转储的进程的 ID。
3. 如果必要，配置以下设置：
   - 在**资产**下拉列表中，更改要获取进程内存转储的设备。
     默认情况下，此字段包含您之前选中的复选框对应的设备名称。您可以选择与警报或事故无关，但属于警报或事故租户（及其子租户）的设备。

     > 只有可对其执行响应操作的资产可供选择。
     > 设备将按以下方式显示：属于警报或事故的设备置于**资产**下拉列表开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。
   - 在**MD5 或 SHA256**字段中，指定要获取其进程内存转储的文件的哈希值。
   - 在**描述**字段中，编写对响应操作的描述或注释。
4. 单击“**获取**”按钮。

窗格将被关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

响应操作完成后，进程的内存转储将保存到 ZIP 存档中。

查看响应操作结果

您可以通过以下方式之一查看和下载该存档：

- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。
- 从主菜单的响应历史部分，或从警报或事故详细信息中的历史记录选项卡
  点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则会显示**成功**消息和一个受密码保护的包含扫描结果的ZIP压缩包。您可以将该压缩包下载到您的计算机中。密码为：infected。
  否则，将显示错误消息以及有关错误原因的信息。

如果要查看启动 ID 和包含响应操作结果的 JSON，请转到“**调试数据**”选项卡。

扫描设备以检测威胁

要防止在受感染的设备上传播威胁，您可以通过执行以下响应操作之一来扫描设备中的威胁：

- 恶意软件扫描
- YARA 扫描
- IOC 扫描

> 要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

您可以通过以下方式之一执行响应操作：

- 从警报或事故详情操作
- 从设备详情操作
- 从遥测事件
  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。
- 从调查图

  > 如果构建了调查图，则此选项可用。

- 从资产表
- 从**响应历史**部分
- 从 YARA 规则或 IOC 规则列表中

  > 此选项适用于“YARA 扫描”和“IOC 扫描”响应操作。

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从警报或事故详情中运行扫描

要从警报或事故详情中对设备执行扫描：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控→警报**部分。在“**ID**”列中，单击包含待扫描设备的警报的 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待扫描设备的事故的 ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

3. 选中待扫描的设备旁边的复选框。
   如有必要，您可以选择多个设备。

4. 在“**选择响应操作**”下拉列表中，单击“**扫描**”。

5. 在打开的上下文菜单中，选择所需的响应操作。

从设备详情中运行扫描

要从设备详情对设备执行扫描：

1. 执行以下操作之一：

   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击包含待扫描设备的警报的 ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待扫描设备的事故的 ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。

4. 在“**选择响应操作**”下拉列表中，单击“**扫描**”。

5. 在打开的上下文菜单中，选择所需的响应操作。

从调查图中运行扫描

要从调查图对设备执行扫描：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击包含待扫描设备的事故的 ID。

2. 单击“**在图表上查看**按钮。

3. 在打开的调查图中，单击设备名称以打开设备详情。

4. 在“**选择响应操作**”下拉列表中，单击“**扫描**”。

5. 在打开的上下文菜单中，选择所需的响应操作。

从遥测事件中运行扫描

从通过警报或事故详情打开的遥测事件中扫描设备：

1. 执行以下操作之一：
   - 在主菜单中，前往**监控**→**警报**部分。在“**ID**”列中，单击所需警报 ID 的链接。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在“**ID**”列中，单击所需事故 ID 的链接。
2. 在打开的窗口中，转到“**详细信息** ”选项卡，然后执行以下操作之一：
   - 单击目标事件名称并选择设备。
   - 单击“在威胁搜索中查找”按钮，转到**威胁搜索**部分，然后选择所需设备。
3. 在“**选择响应操作**”下拉列表中，单击“**扫描**”。
4. 在打开的上下文菜单中，选择所需的响应操作。

若要从通过威胁搜索部分打开的遥测事件中扫描设备：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。
2. 单击您要打开其详情的事件名称。
3. 在打开的事件详情窗口中，单击设备名称，然后从打开的下拉列表中选择所需的响应操作。

从资产表中运行扫描

要从资产表中运行扫描：

1. 在主菜单中，转到 **资产管理 → 资产(设备)。**
   这将打开资产表。
2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   > 已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择所需的响应操作。

从响应历史中运行扫描

若要从响应历史中运行扫描：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。
2. 在“**响应**”下拉列表中，选择所需的响应操作。

从 YARA 规则或 IOC 规则列表中运行扫描

要从 YARA 规则或 IOC 规则列表中扫描：

1. 在主菜单中，前往**规则和服务**，然后选择以下选项之一：**YARA 规则**或**IOC 规则**。
   规则列表随即显示。
2. 选中要扫描的一个或多个设备旁边的复选框。
3. 在工具栏上，单击以下按钮：
   - “**运行 YARA 扫描**”，前提是已在步骤 1 中选择了“**YARA 规则**”。
   - “**运行 IOC 扫描**”，前提是已在步骤 1 中选择了“**IOC 规则**”。
4. 在打开的右侧窗格中，配置扫描设置。

运行恶意软件扫描

由于受管理设备和管理服务器之间存在同步间隔，响应操作启动可能需要长达 15 分钟。

如有必要，您可以单击**在 KUMA 中编辑**按钮，以便在 KUMA 控制台中编辑设备参数。

如果您选择了“恶意软件扫描”响应操作，请在“**运行恶意软件扫描**”窗格中执行以下操作：

1. 选择恶意软件扫描类型：
   - **全盘扫描**
     您可以切换**扫描网络驱动器**切换按钮，从而将网络设备包含在扫描中。默认情况下已禁用该选项。

     全盘扫描会增加操作系统的负载，可能导致设备运行速度变慢。
     对于安装了Kaspersky Endpoint Security for Linux 12.4版本的设备，不支持完整扫描。
   - **关键区域扫描**
     如果选择此类型，将扫描内核内存、正在运行的进程和磁盘引导扇区。

- **自定义扫描**

  在“**指定路径**”字段中，指定待扫描文件的路径。如果要设置多个路径，请单击“**添加路径**”按钮，然后指定路径。

2. 单击“**扫描**”按钮。

所选类型的恶意软件扫描将启动。

恶意软件扫描成功完成后，屏幕上将显示相应消息，警报或事故将显示在警报表或事故表中，且操作状态为“**成功**”。否则，将显示错误消息，且警报或事故的操作状态显示为“**错误**”。

恶意软件扫描操作完成后，您可以查看结果。

YARA 扫描

YARA扫描是使用通过OSMP控制台手动下载的YARA文件，在设备上搜索恶意活动的签名。

若要执行YARA扫描，您必须满足以下条件：

- 带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上
- YARA 规则列表中至少包含一条规则

若要执行YARA扫描：

1. 选择YARA 扫描响应操作。

   “**运行 YARA 扫描**”窗格随即打开。

2. 在**规则**下拉列表中，选择一条或多条YARA规则。

   您可以输入规则名称或规则名称中的某个字符序列。

   > 最多可指定 200 条规则。

3. 在“**扫描范围**”中，执行以下操作：

   a. 选择该选项并指定其必填参数：

   - **RAM**，用于扫描在执行响应操作时正在运行的进程。

     此选项默认选中，并且在“**扫描**”设置组中，“**所有进程**”选项已默认选中。

     如果您想扫描特定进程，请在**扫描**设置组中选择**具体进程**选项，然后输入要扫描的一个或多个进程的名称。否则，将扫描所有进程。

     > 应用程序不会扫描低优先级的进程。

   - **自动运行点**扫描从**取证**响应操作中获取的自动运行点。

然后指定扫描类型：

- **快速扫描**。扫描所有自动运行点，但不包括 COM 对象。
- **全盘扫描**。扫描所有自动运行点及其相关文件。

支持的自动运行点列表

支持以下类型的自动运行点：

- 登录
- Shell
- Office
- 浏览器
- 计划器
- 服务
- 驱动程序
- 加密
- 调试器
- COM
- SessionManager
- 网络
- LSA
- 应用程序
- WMI
- GroupPolicy
- DriverLog
- BootLog
- 过程
- OsUpdate
- 打印机
- 未指定

- OsLoader
- EfiLoader

- **所有本地磁盘**，用于扫描本地磁盘上所有文件夹中存储的文件。

  > 扫描所有本地磁盘可能会导致设备负载过高。

- **指定的目录**，用于扫描指定目录及其所有嵌套文件夹中的文件。
  您必须在相应字段中指定目录的完整路径，并在末尾附加掩码 * 以包含子目录，例如 `C:\Users\Administrator\Desktop\*`。

b. 如有必要，请在相应的字段中为所选选项指定以下参数：

- **最大扫描时长(小时)**
  默认值是 23。指定时间过后，即使某些规则未应用于扫描设备，扫描也会停止。响应操作结果包含扫描停止时的最新数据。

- **排除项**
  指定要从扫描中排除的进程的简称或文件掩码。如果设备上运行着多个同名进程，应用程序会将所有此类进程从扫描中排除。

4. 如果必要，配置以下设置：

- 指定租户。
  如果您从YARA规则列表中运行响应操作，并选择了属于不同租户的规则，则**租户**字段为空。您必须手动指定要对其设备执行YARA扫描的租户。

- 更改响应操作的范围。
  默认情况下，在**范围**设置中，**特定资产**选项处于选中状态，并且**资产**下拉列表中包含您之前选中了复选框的设备名称。YARA扫描将在这些设备上执行。
  您可以更改要扫描的设备，或选择**范围**设置组中的**所有资产**选项，以扫描属于警报或事故租户（及其子租户）的所有设备。

  > 只有可对其执行响应操作的资产才可供选择。
  > 设备显示如下：属于警报或事故的设备显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及子租户的设备。

- 在**描述**字段中，编写对响应操作的描述或注释。

5. 单击“**运行**”按钮。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

在“**资产**”列中，您必须单击已启动 YARA 扫描的资产数量对应的链接。在打开的窗口中会选中“**结果**”选项卡，您可以查看每条 YARA 规则的扫描状态。如果扫描检测到威胁，则会创建相应的警报。您可以从响应操作结果跳转到警报。

如果响应操作未成功完成，屏幕上将显示**错误**消息和有关错误原因的信息。

IOC 扫描

IOC扫描是通过使用可通过OSMP控制台手动下载的IOC文件（入侵指标文件）来搜索设备上是否存在针对性攻击迹象以及已感染或可能已感染的对象。

若要执行IOC扫描，您必须满足以下条件：

- 带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上
- IOC 规则列表中至少包含一条规则

若要执行IOC扫描：

1. 选择IOC 扫描响应操作。
   “**运行 IOC 扫描**”窗格随即打开。
2. 在**规则**下拉列表中，选择一个或多个IOC规则。
3. 如果必要，配置以下设置：
   - 指定租户。
     如果您是从IOC规则列表中运行响应操作，并选择了属于不同租户的规则，则**租户**字段为空。您必须手动指定要对其设备执行IOC扫描的租户。
   - 更改响应操作的范围。
     默认情况下，在**范围**设置中，**特定资产**选项处于选中状态，并且**资产**下拉列表中包含您之前选中了复选框的设备名称。这意味着将对这些设备执行IOC扫描。
     您可以更改要扫描的设备，或选择**范围**设置组中的**所有资产**选项，以扫描属于警报或事故租户（及其子租户）的所有设备。

     只有可对其执行响应操作的资产才可供选择。
     设备将按如下方式显示：属于警报或事故的设备将显示在**资产**下拉列表的开头，然后按字母顺序显示属于警报或事故租户及其子租户的设备。

- 在“**最大扫描时长(小时)**”字段中，指定最大扫描持续时间。

  默认值是 23。指定时间过后，即使某些规则未应用于扫描设备，扫描也会停止。响应操作结果包含扫描停止时的最新数据。

- 在**描述**字段中，编写对响应操作的描述或注释。

4. 单击“**运行**”按钮。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

在“**资产**”列中，您必须单击已启动 IOC 扫描的资产数量对应的链接。在打开的窗口中会选中**结果**选项卡，您可以查看每条IOC规则的扫描状态。如果扫描检测到威胁，则会创建相应的警报。您可以从响应操作结果跳转到警报。

如果响应操作失败，则会显示错误消息和错误原因信息。

扫描从设备中获取的文件

从设备或隔离区目录中获取文件后，您可以扫描该文件是否存在威胁。

要执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1级分析师、2 级分析师。

您可以通过以下方式之一运行文件扫描：

- 在执行“文件”响应操作时。

  默认情况下启用了**扫描文件**选项。有关详情，请参阅“获取文件”一文。

- 在主菜单的**存储库** → **隔离**部分，点击**获取和扫描**按钮。

  如果带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上，则可以使用此选项。

- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。

  此选项适用于因文件或获取文件响应操作而放置到**文件**部分的文件以及您手动上传的文件。

- 根据以下响应操作的结果：
  - 文件
  - 获取文件
  - 移动到隔离区

从文件部分或选项卡运行扫描

弱要从文件部分或选项卡运行扫描：

1. 在主菜单中，执行以下操作之一：
   - 转到**存储库** → **文件**。
   - 转到“**监控**”，然后选择“**警报**”或“**事故**”部分。在ID列中，单击包含通过获取文件和从隔离区获取文件响应操作而获得的文件的警报或事故的ID。在打开的警报或事故详情中，转到**文件**选项卡。
2. 在文件表中，执行以下操作之一：
   - 选中所需文件旁边的复选框，然后在工具栏中单击“**Scan**”按钮。
   - 单击文件名，然后在打开的文件详情面板中，单击**扫描**按钮。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

根据其他响应操作的结果运行扫描

要根据其他响应操作的结果运行扫描：

1. 在主菜单中，执行以下操作之一：
   - 转到“**监控**” → “**响应历史**”。
   - 转到“**监控**”，然后选择“**警报**”或“**事故**”部分。在ID列中，点击您执行获取文件、从隔离区获取文件或将文件移动到隔离区响应操作所对应的警报或事故的 ID。在打开的警报或事故详情窗口中，前往**历史记录**选项卡，然后选择**响应历史**选项卡以显示事件列表。
2. 在“**操作状态**”列中，单击您要查看所需响应操作结果对应的事件的“**成功**”状态。
3. 在打开的右侧窗格中，单击包含文件名的链接。
   文件详情面板随即打开。
4. 在工具栏上，单击“**扫描**”按钮。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看文件扫描结果

您可以通过以下方式之一查看文件扫描结果：

- 从主菜单的“**文件**”部分，或从警报或事故详情中的“**文件**”选项卡。
- 从主菜单的 **响应历史** 部分，或从警报或事故详情中的 **历史记录**选项卡

  点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则会显示**成功**消息和一个受密码保护的包含扫描结果的ZIP压缩包。您可以将该压缩包下载到您的计算机中。密码为：infected。

  否则，将显示错误消息以及有关错误原因的信息。

  如果您想查看**启动 ID**和包含响应操作结果的JSON，请前往**调试数据**选项卡。

删除文件

要执行“**删除文件**”响应操作，您必须具备以下条件：

- 以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。
- 带有内置代理的 Kaspersky Endpoint Security 已安装在您的设备上

您可以通过以下方式之一执行响应操作：

- 从警报或事故详情操作
- 从设备详情操作
- 从遥测事件

  您可以从警报或事故详情中，或从**威胁搜索**部分打开事件详情。
- 从调查图

  > 如果构建了调查图，则此选项可用。
- 从资产表
- 从**响应历史**部分

您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

从警报或事故详情中响应

要从警报或事故详情中进行响应：

1. 执行以下操作之一：

   - 在主菜单中，前往**监控**→**警报**部分。在**ID**列中，点击包含要删除文件的设备的警报ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在**ID**列中，点击其中包含要删除文件的设备的事故ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

   > 您也可以转到“**观察点**”选项卡，选中要删除的文件旁边的复选框，然后单击“**删除文件**”。

3. 选中要删除的文件所在设备旁边的复选框。
   您可以选择多个设备。

4. 在“**选择响应操作**”下拉列表中，选择“**删除文件**”。

5. 在打开的右侧窗格中，执行以下操作：

   - 在“**完整路径**”字段中，指定要删除的文件的完整路径。
   - 在**资产**下拉列表中，选择文件所在的设备。
     如果在步骤2中选择了**资产**选项卡，则默认情况下，您选中的复选框对应的设备名称会显示在**资产**字段中。
     您可以更改设备或选择设置的**范围**组中的**所有资产**选项，以对属于警报或事故租户（及其子租户）的所有设备执行响应操作。

     > 只有可对其执行响应操作的资产才可供选择。
     > 设备显示如下：属于警报或事故的设备位于**资产**下拉列表的开头，随后按字母顺序显示属于警报或事故租户及其子租户的设备。

   - 如有必要，请在相应字段中配置以下设置：
     - 指定文件的 SHA256 或 MD5 哈希值。

       > 如果在步骤 2 中选择了“**观察点**”选项卡，则会自动指定哈希值。您可以更改值。

     - 为响应操作编写描述或注释。

6. 单击“**删除**”按钮。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从设备详情中响应

要从设备详情中进行响应：

1. 执行以下操作之一：

   - 在主菜单中，前往**监控**→**警报**部分。在**ID**列中，点击包含要删除文件的设备的警报ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在**ID**列中，点击其中包含要删除文件的设备的事故ID。

2. 在打开的窗口中，转到“**资产**”选项卡。

3. 单击所需设备的名称，然后在下拉列表中选择“**查看属性**”。

4. 执行与“*从警报或事故详情中响应*”中步骤 4-6 相同的操作。

   窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从遥测事件响应

要从通过警报或事故详情打开的遥测事件中进行响应：

1. 执行以下操作之一：

   - 在主菜单中，前往**监控**→**警报**部分。在**ID**列中，点击包含要删除文件的设备的警报ID。
   - 在主菜单中，转到“**监控**” → “**事故**”部分。在**ID**列中，点击其中包含要删除文件的设备的事故ID。

2. 在打开的窗口中，转到“**详细信息** ”选项卡，然后执行以下操作之一：

   - 单击目标事件名称并选择设备。
   - 单击**在威胁搜索中查找**按钮，转到**威胁搜索**部分，然后选择所需设备。

3. 执行与“*从警报或事故详情中响应*”中步骤 4-6 相同的操作。

   窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

要从通过“威胁搜索”部分打开的遥测事件中进行响应：

1. 在主菜单中，转到**“监控” → “威胁搜索”。**
   事件表随即打开。

2. 单击您要打开其详情的事件名称。

3. 在打开的事件详情窗口中，点击设备名称，然后从下拉列表中，选择**删除文件**。
4. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从调查图响应

要从调查图对设备执行扫描：

1. 在主菜单中，转到“**监控**” → “**事故**”部分。在ID列中，点击其中包含要删除文件的设备的事故ID。
2. 单击“**在图表上查看**按钮。
3. 在打开的调查图中，单击设备名称以打开设备详情。
4. 在“**选择响应操作**”下拉列表中，选择“**删除文件**”。
5. 执行与“*从警报或事故详情中响应*”中步骤 5-6 相同的操作。

如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从资产表响应

要从资产表中进行响应：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   这将打开资产表。
2. 选中要执行响应操作的设备旁边的复选框。
   您可以选择多个设备。

   > 已存档的设备无法选择。

3. 在“**选择响应操作**”下拉列表中，选择“**删除文件**”。
4. 在打开的右侧窗格中，按照“*从警报或事故详细信息中响应*”中的步骤 5-6 所述来配置响应操作设置。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

从响应历史部分响应

若要从响应历史执行响应操作：

1. 在主菜单中，转到“**监控**” → “**响应历史**”。
   将打开包含所有警报和事故的响应历史记录的表格。
2. 在“**响应**”下拉列表中，选择“**删除文件**”。
3. 在打开的右侧窗格中，按照“*从警报或事故详情中响应*”中的步骤 5-6 所述来配置响应操作设置。

窗格关闭。如果响应操作成功完成，屏幕上会显示相应的消息。否则，将显示错误消息。

查看响应操作结果

您可以通过下列方式之一查看响应操作结果：

- 从主菜单的响应历史部分
- 从警报或事故详细信息的历史记录选项卡

点击**操作状态**列中的链接后，窗口打开时会默认选中**结果**选项卡。如果响应操作成功完成，则显示“**成功**”字样。否则，将显示错误消息以及有关错误原因的信息。

如果您想查看启动 ID和包含响应操作结果的 JSON，请转到**调试数据**选项卡。

如果文件已被其他进程占用，则操作结果会显示为“**成功**”状态，但该文件只有在设备重启后才会删除。建议重启设备后检查文件是否已成功删除。

通过 Active Directory 响应

您可以将 Kaspersky Next XDR Expert 与您组织中使用的 Active Directory 服务集成。配置 Active Directory 与 KUMA 的集成后，Active Directory 即视为已与 Kaspersky Next XDR Expert 集成。

配置 Kaspersky Next XDR Expert 和 Active Directory 之间的集成的过程包括配置与 LDAP 的连接。您必须为每个租户单独配置与 LDAP 的连接。

如此，发生警报或事故时，您便能针对该租户的关联用户执行响应操作。

您可以通过以下方式之一使用 Active Directory 执行响应操作：

- 从警报或事故详细信息中
- 从遥测事件中（如果从警报详情中打开的话）。

- 从调查图

  如果构建了调查图，则此选项可用。

您还可以配置在创建或编辑行动手册时自动运行的响应操作。

要通过 Active Directory 执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

要通过 Active Directory 执行响应操作：

1. 在主菜单中，转到“**监控**”，然后选择“**警报**”或“**事故**”部分。

   如果要从遥测事件中进行响应，请选择“**警报**”部分。

   如果要从调查图中进行响应，请选择“**事故**”部分。

2. 单击所需警报或事故的 ID。

3. 在打开的窗口中，执行以下操作之一：

   - 如果要通过警报或事故详情响应，请转到“**资产**”选项卡，然后单击用户名称。
   - 如果要通过遥测事件响应，请转到“**详细信息**”选项卡，单击所需事件名称，然后选择用户；或者单击“**在威胁搜索中查找**”按钮以转到“**威胁搜索**”部分，然后选择所需用户。
   - 如果您想通过调查图响应，请单击“**在图表上查看**按钮。在打开的调查图中，单击用户名称。

   “**账户详情**”窗口将在屏幕右侧打开。

4. 在“**通过 Active Directory 进行响应**”下拉列表中，选择要执行的操作：

   - **锁定账户**

     如果用户账户因相关警报或事故而被锁定，屏幕上会显示相应消息。否则，会显示错误消息。

   - **重置密码**

     如果用户账户密码因相关警报或事故而重置，屏幕上会显示相应消息。否则，将显示错误消息。

   - **将用户添加到安全组**

     在打开的窗口中，在必填字段“**安全组 DN**”中，指定要添加用户的安全组的完整路径。CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。然后单击“**添加**”按钮。一次操作中只能指定一个组。

     如果用户因相关警报或事故而被添加到安全组，屏幕上会显示相应消息。否则，将显示错误消息。

   - **从安全组中删除用户**

     在打开的窗口中，在必填字段“**安全组 DN**”中，指定要从中删除用户的安全组的完整路径。例如，CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。单击“**删除**”按钮。一次操作中只能指定一个组。

     如果用户因相关警报或事故而从安全组中被删除，屏幕上会显示相应消息。否则，将显示错误消息。

使用第三方脚本进行响应

本节包含您可以通过在远程客户端设备上启动第三方脚本通过外部系统执行的响应操作。

为此，您必须：

- 配置Kaspersky Next XDR Expert和脚本启动服务之间的集成。
- 创建一个行动手册，该行动手册将启动用于响应脚本。
- 下载，然后使用本节提供的说明中描述的脚本。

通过 UserGate 响应

UserGate 包含统一威胁管理解决方案的功能，并为您的本地网络提供以下保护措施：

- 防火墙
- 入侵和攻击防护
- 反病毒流量扫描
- 应用程序控制

支持 UserGate UTM API 7 版本。

如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务之间的集成，并创建了将启动脚本进行响应的行动手册，则您可以通过 UserGate 响应警报和事故。您可以单击此链接下载脚本。

下载脚本

访问 UserGate 的登录名和密码存储在 ug.py 脚本中。您可以在此脚本中更改*端点*、*登录名*和*密码*的值。

运行脚本需要 Python 3.10 及更高版本。

要通过 UserGate 执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师、2 级分析师。

您可以创建将通过 UserGate 执行以下响应操作的行动手册：

- 阻止 IP 地址、URL 和域名。
  UserGate 将在行动手册启动后阻止 IP 地址、URL 和域名。
- 注销用户。
  所有登录到 UserGate 的用户都将在行动手册启动后注销。

要启动通过 UserGate 进行响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中单击目标警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中选择所创建的用于通过 UserGate 进行响应的行动手册。
3. 单击“**启动**”按钮。
   所选行动手册将启动通过 UserGate 进行响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 Ideco NGFW 响应

Ideco NGFW 是一种解决方案，可充当企业和私人网络中互联网流量的过滤器。如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务的集成，它允许您阻止 Kaspersky Next XDR Expert 检测到的 IP 地址和 URL。

> 支持 Ideco NGFW 16.0 或更高版本。

访问 Ideco NGFW 的登录名和密码存储在脚本中，以便与 Ideco NGFW 集成。您可以通过单击以下链接来下载脚本：

下载脚本

要使用脚本：

1. 通过下列其中一种方式安装脚本：
   - 例如，通过 pip：
     ```
     pip install -r requirements.txt
     ```
   - 例如，从 WHL 文件：
     ```
     pip install ./dist/kaspersky_xdr_ideco_integration-<version>-py3-none-any.whl
     ```
   - 离线安装。
     如果您无法访问互联网，则必须离线安装脚本。在这种情况下，请执行以下操作：
     a. 通过运行以下命令在可以访问互联网的计算机上下载依赖项：
        ```
        pip download -r requirements.txt
        ```
     b. 将下载的依赖项移动到您将运行脚本的设备上。
     c. 使用以下命令安装依赖项：
        ```
        pip install --no-index --find-links <folder_path_to_downloaded_dependencies> -r
        requirements.txt
        ```
2. 通过下列其中一种方式配置脚本：
   - 例如，通过 ENV 文件：

```
cp .env.sample .env
nano .env
```

- 在脚本 (ideco.py) 的主体中，编辑以下字符串中的参数：

```
BASE_URL: str = getenv("BASE_URL", "https://your-ip:your-port")
LOGIN: str = getenv("LOGIN", "your-login")
PASSWORD: str = getenv("PASSWORD", "your-password")
IP_DENY_LIMIT: int = int(getenv("IP_DENY_LIMIT", 1000))
```

3. 为 Kaspersky Next XDR Expert 检测到的 IP 地址及恶意 URL 添加拒绝规则。

要添加将阻止 IP 地址的防火墙规则：

1. **使用 add_firewall_rule 命令运行脚本**。

   该命令具有以下逻辑：

   1. 检查 Ideco NGFW 对象列表中是否存在 IP 地址。
      如果存在，则不添加当前 IP 地址。
      如果不存在，则添加当前 IP 地址。

   2. 检查名为 XDR 的 IP 地址列表是否存在。
      如果该列表存在，则重复使用该列表，并将 IP 地址添加到其中。
      如果列表不存在，则创建一个新列表，并将 IP 地址添加到其中。

   3. 检查名为 XDR 的防火墙规则是否存在。
      如果防火墙规则存在，则重复使用该规则，并将步骤 2 中的 IP 地址列表添加到其中。
      如果防火墙规则不存在，则创建一个新的防火墙规则，并将步骤 2 中的 IP 地址列表添加到其中。

2. 请指定要阻止的 IP 地址。

   > 默认情况下，IP 地址的最大数量为 1000。您可以编辑此值，如步骤 2“*配置脚本*”中所述。

   您必须添加有效的 IPv4 地址，用逗号分隔且不带空格，例如：

   ```
   python ideco.py add_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
   ```

   针对所选 IPv4 地址的拒绝规则将被添加。

要添加将阻止恶意 URL 的过滤规则：

1. **使用 add_content_filter_file 命令运行脚本**。

   该命令具有以下逻辑：

   1. 检查名为 XDR 的类别是否存在。
      如果存在，则将 URL 添加到此类别。
      如果不存在，则创建一个新类别，然后将 URL 添加到其中。

   2. 检查名为 XDR 的内容过滤规则是否存在。

如果内容过滤规则已存在，则将步骤 1 中的类别添加到其中。

如果不存在，则创建一个新的内容过滤规则，然后将步骤 1 中的类别添加到其中。

2. 指定要阻止的 URL。

URL 必须以逗号分隔，且需带有 http:// 或 https:// 前缀，例如：

```
python ideco.py add_content_filter_rule --url "https://url_1.com, http://url_2.com.uk,
http://qwerty.nl, http://zxc.xc"
```

针对指定URL的拒绝规则随即添加。

通过 Ideco UTM 响应

Ideco UTM 是一款为企业网络提供以下保护措施的解决方案：

- 防火墙 — 过滤网络流量，保护网络免受未经授权的访问。
- 入侵和攻击防护 — 识别和阻止可疑操作，确保系统完整性。
- 反病毒流量扫描 — 抵御恶意软件和恶意的活动。
- 应用程序控制 — 阻止或限制未经授权的应用程序的执行。
- Web 过滤 — 限制用户访问您认为不需要的网站。

支持 Ideco UTM 15.7.35 版本。

如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务之间的集成，并创建了将启动脚本进行响应的行动手册，则您可以使用 Ideco UTM 对警报和事故作出响应。行动手册启动后，Ideco UTM 将阻止 IP 地址、IP 范围或 URL，具体取决于您在创建行动手册时指定的操作。

要解除对已被阻止的 IP 地址、IP 范围或 URL 的阻止，您必须创建并启动另一个行动手册。

您可以单击此链接来下载脚本：

下载脚本

访问 Ideco UTM 所需的登录名和密码存储在 env.sample 配置文件中。您必须将此文件中的信息复制到您创建的新 ENV 文件中，然后在新文件中指定必要的参数。

运行该脚本需要使用 Python 3.10。

要通过 Ideco UTM 执行响应操作，您必须具有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

要启动通过 Ideco UTM 响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 Ideco UTM 响应而创建的行动手册。
3. 单击“**启动**”按钮。
   所选的行动手册将启动通过 Ideco UTM 响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 Redmine 响应

Redmine 是一个用于项目管理和问题跟踪的 Web 应用程序。如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务之间的集成，则可以通过脚本实现 Redmine 项目中问题处理场景的自动化。

单击此链接以下载脚本：

下载脚本

要使用脚本：

1. 通过下列其中一种方式安装脚本：
   - 例如，通过 pip：
     ```
     pip install -r requirements.txt
     ```
   - 例如，从 WHL 文件：
     ```
     pip install ./dist/kaspersky_xdr_redmine_integration-1.0-py3-none-any.whl
     ```
   - 离线安装。
     如果您无法访问互联网，则必须离线安装脚本。在这种情况下，请执行以下操作：
     a. 使用以下命令在可以访问互联网的计算机上下载依赖项：
        ```
        pip download -r requirements.txt
        ```
     b. 将下载的依赖项移动到您将运行脚本的设备上。
     c. 使用以下命令安装依赖项：
        ```
        pip install --no-index --find-links <folder_path_to_downloaded_dependencies> -r
        requirements.txt
        ```
2. 通过下列其中一种方式配置脚本：
   - 例如，通过 ENV 文件：
     ```
     cp .env.sample .env
     nano .env
     ```
   - 在脚本 (redmine.py) 的主体中，编辑以下字符串中的参数：

```
REDMINE_URL: str = getenv("REDMINE_URL", "http://<ip_or_hostname>")
REDMINE_PORT: str = getenv("REDMINE_PORT", "8080")
REDMINE_API_KEY: str = str(getenv("REDMINE_API_KEY", "<redmine_api_key>"))
```

您可以使用脚本处理 Redmine 中存在的问题。

- 如果要创建新问题，请运行以下命令：

  ```
  python redmine.py create_issue "project-identifier" "Issue subject" --description "Issue description text" --priority_id <id: int>
  ```

  结果：

  ```
  {"issue_id": 57}
  ```

- 如果要更新问题，请运行以下命令：

  ```
  python redmine.py update_issue <issue_id: int> --subject "Subject text to be updated" --description "Description text to be updated" --priority_id <id: int>
  ```

  结果：

  ```
  {"status": "issue_updated"}
  ```

- 如果要获取问题，请运行以下命令：

  ```
  python redmine.py get_issue <issue id: int>
  ```

  结果：

  ```
  {
  "subject": "86",
  "description": "18",
  "project_name": "Test project",
  "author_name": "Redmine Admin",
  "status_name": "backlog",
  "priority_name": "high",
  "start_date": "24.07.2023",
  "due_date": null,
  "created_on": "24.07.2023 10:56:15",
  "updated_on": "24.07.2023 17:18:38"
  }
  ```

通过 Check Point NGFW 响应

Check Point NGFW 是一款在企业网络中用作互联网流量过滤器的解决方案。与 Check Point NGFW 集成可以阻止 Kaspersky Next XDR Expert 检测到的 IP 地址和 URL。

Check Point NGFW 集成了统一威胁管理解决方案的功能，并为企业网络提供以下保护措施：

- 防火墙 — 过滤网络流量，保护网络免受未经授权的访问。
- 入侵和攻击防护 — 识别和阻止可疑操作，确保系统完整性。
- 反病毒流量扫描 — 抵御恶意软件和恶意的活动。

- 应用程序控制 — 阻止或限制未经授权的应用程序的执行。
- Web 过滤 — 限制用户访问您认为不需要的网站。

支持 Check Point NGFW 版本 R81.20 或更高版本。

如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务之间的集成，并创建了将启动响应脚本的行动手册，则您可以通过 Check Point NGFW 响应警报和事故。要解除对已被阻止的 IP 地址或 URL 的阻止，您必须创建并启动另一个行动手册。

运行脚本需要使用 Python 3.10。

要通过 Check Point NGFW 执行响应操作，您必须具有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

您可以通过单击以下链接来下载响应脚本：

下载脚本

用于访问 Check Point NGFW 的登录名和密码存储在 `.envSample` 文件中。

要使用脚本：

1. 通过下列其中一种方式安装脚本：
   - 例如，通过 pip：
     ```
     pip install -r requirements.txt
     ```
   - 离线安装。
     如果您无法访问互联网，则必须离线安装脚本。在这种情况下，请执行以下操作：
     a. 通过运行以下命令在可以访问互联网的计算机上下载依赖项：
        ```
        pip download -r requirements.txt
        ```
     b. 将下载的依赖项移动到您将运行脚本的设备上。
     c. 使用以下命令安装依赖项：
        ```
        pip install --no-index --find-links <folder_path_to_downloaded_dependencies> -r requirements.txt
        ```
2. 通过下列其中一种方式配置脚本：
   - 例如，通过 ENV 文件：
     ```
     cp .env.sample .env
     nano .env
     ```
   - 在脚本主体 (main.py) 中，编辑以下字符串中的参数：
     ```
     BASE_IP: str = getenv("BASE_IP", "your-ip")
     ```

```
BASE_PORT: str = getenv("BASE_PORT", "your-port")
LOGIN: str = getenv("LOGIN", "your-login")
PASSWORD: str = getenv("PASSWORD", "your-password")
```

3. 为 Kaspersky Next XDR Expert 检测到的 IP 地址及恶意 URL 添加拒绝规则。

要添加将阻止 IP 地址的防火墙规则：

1. **使用 add_firewall_rule 命令运行脚本**。

   该命令具有以下逻辑：

   1. 检查 IP 地址是否存在于 Check Point NGFW 对象列表中。
      如果存在，则不添加当前 IP 地址。
      如果不存在，则添加当前 IP 地址。
   2. 检查名为 XDR 的 IP 地址列表是否存在。
      如果该列表存在，则重复使用该列表，并将 IP 地址添加到其中。
      如果列表不存在，则创建一个新列表，并将 IP 地址添加到其中。
   3. 检查名为 XDR 的防火墙规则是否存在。
      如果防火墙规则存在，则重复使用该规则，并将步骤 2 中的 IP 地址列表添加到其中。
      如果防火墙规则不存在，则创建一个新的防火墙规则，并将步骤 2 中的 IP 地址列表添加到其中。

2. 请指定要阻止的 IP 地址。

   > 默认情况下，IP 地址的最大数量为 1000。您可以按照先前步骤 2“*配置脚本*”中所述的方法编辑此值。

   您必须添加有效的 IPv4 地址，用逗号分隔且不带空格，例如：

   ```
   python main.py add_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
   ```

针对所选 IPv4 地址的拒绝规则将被添加。

要删除阻止 IP 地址的防火墙规则：

1. **使用 delete_firewall_rule 命令运行脚本**。

   该命令具有以下逻辑：

   1. 检查 IP 地址是否存在于 Check Point NGFW 对象列表中。
      如果存在，则不添加当前 IP 地址。
      如果不存在，则添加当前 IP 地址。
   2. 检查名为 XDR 的 IP 地址列表是否存在。
      如果该列表存在，则重复使用该列表，并将 IP 地址添加到其中。
      如果列表不存在，则创建一个新列表，并将 IP 地址添加到其中。
   3. 检查名为 XDR 的防火墙规则是否存在。
      如果防火墙规则存在，则重复使用该规则，并将步骤 2 中的 IP 地址列表添加到其中。

如果防火墙规则不存在，则创建一个新的防火墙规则，并将步骤 2 中的 IP 地址列表添加到其中。

2. 请指定要阻止的 IP 地址。

> 默认情况下，IP 地址的最大数量为 1000。您可以按照先前步骤 2“*配置脚本*”中所述的方法编辑此值。

您必须添加有效的 IPv4 地址，用逗号分隔且不带空格，例如：

```
python main.py delete_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
```

针对所选 IPv4 地址的拒绝规则将被删除。

要添加将阻止恶意 URL 的过滤规则：

1. **使用 add_content_filter_file 命令运行脚本**。

   该命令具有以下逻辑：

   1. 检查名为 XDR 的类别是否存在。
      如果存在，则将 URL 添加到此类别。
      如果不存在，则创建一个新类别，然后将 URL 添加到其中。

   2. 检查名为 XDR 的内容过滤规则是否存在。
      如果内容过滤规则已存在，则将步骤 1 中的类别添加到其中。
      如果不存在，则创建一个新的内容过滤规则，然后将步骤 1 中的类别添加到其中。

2. 指定要阻止的 URL。
   URL 必须以逗号分隔，且需带有 http:// 或 https:// 前缀，例如：

```
python main.py add_content_filter_rule --url "https://url_1.com, http://url_2.com.uk,
http://qwerty.nl, http://zxc.xc"
```

针对指定URL的拒绝规则随即添加。

要删除阻止恶意 URL 的过滤规则：

1. **使用 delete_content_filter_file 命令运行脚本**。

   该命令具有以下逻辑：

   1. 检查名为 XDR 的类别是否存在。
      如果存在，则将 URL 添加到此类别。
      如果不存在，则创建一个新类别，然后将 URL 添加到其中。

   2. 检查名为 XDR 的内容过滤规则是否存在。
      如果内容过滤规则已存在，则将步骤 1 中的类别添加到其中。
      如果不存在，则创建一个新的内容过滤规则，然后将步骤 1 中的类别添加到其中。

2. 指定要阻止的 URL。
   URL 必须以逗号分隔，且需带有 http:// 或 https:// 前缀，例如：

```
python main.py delete_content_filter_rule --url "https://url_1.com,
http://url_2.com.uk, http://qwerty.nl, http://zxc.xc"
```

针对指定 URL 的拒绝规则已删除。

要启动通过 Check Point NGFW 进行响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**Incidents**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 Check Point NGFW 响应而创建的行动手册。
3. 单击“**启动**”按钮。
   所选的行动手册将启动通过 Check Point NGFW 响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 Sophos Firewall 响应

Sophos Firewall 是一款为企业网络提供以下防护措施的解决方案：

- 防火墙 — 过滤网络流量，保护网络免受未经授权的访问。
- 入侵和攻击防护 — 识别和阻止可疑操作，确保系统完整性。
- 反病毒流量扫描 — 抵御恶意软件和恶意的活动。
- 应用程序控制 — 阻止或限制未经授权的应用程序的执行。
- Web 过滤 — 限制用户访问您认为不需要的网站。

支持 Sophos Firewall 19.5 版本。

如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务的集成，并创建了将启动脚本进行响应的行动手册，则可以使用 Sophos Firewall 对警报和事故进行响应。行动手册启动后，Sophos Firewall 将阻止 IP 地址、IP 范围或 URL，具体取决于您在创建行动手册时指定的操作。

要解除对已被阻止的 IP 地址、IP 范围或 URL 的阻止，您必须创建并启动另一个行动手册。

您可以单击此链接来下载脚本：

下载脚本

访问 Sophos Firewall 所需的登录名和密码存储在 env.sample 配置文件中。您必须将此文件中的信息复制到您创建的新 ENV 文件中，然后在新文件中指定必要的参数。

运行该脚本需要使用 Python 3.10。

要通过 Sophos Firewall 执行响应操作，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

要启动通过 Sophos Firewall 响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 Sophos Firewall 响应而创建的行动手册。
3. 单击“**启动**”按钮。
   所选的行动手册将启动通过 Sophos Firewall 响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 Continent 4 响应

Continent 4 是一款为企业网络提供以下保护措施的解决方案：

- 防火墙 — 过滤网络流量，保护网络免受未经授权的访问。
- 入侵和攻击防护 — 识别和阻止可疑操作，确保系统完整性。
- VPN 网关 — 为您组织的网络之间的数据传输创建安全隧道。
- 访问控制 — 根据安全规则和策略管理用户对内部和外部网络资源的访问。
- 数据加密 — 使用加密算法来保护传输的数据。

支持 Continent 4 版本 4.1.7。

如果您之前配置了 Kaspersky Next XDR Expert 和脚本启动服务之间的集成，并创建了将启动脚本进行响应的行动手册，则您可以通过 Continent 4 对警报和事故作出响应。

您可以创建通过 Continent 4 执行以下响应操作的行动手册：

- 阻止 IP 地址和 URL。
  Continent 4 将阻止 IP 地址和 URL。要解除对已被阻止的 IP 地址或 URL 的阻止，您必须创建并启动另一个行动手册。
- 阻止入侵指标（下称“IoC”）。
  Continent 4 将阻止您在行动手册触发器中指定的可观察对象。

您可以单击此链接来下载脚本：

下载脚本

访问 Continent 4 所需的登录名和密码存储在 env.sample 配置文件中。您必须将此文件中的信息复制到您创建的新 ENV 文件中，然后在新文件中指定必要的参数。

运行该脚本需要使用 Python 3.10。

要通过 Continent 4 执行响应操作，您必须具有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

要启动通过 Continent 4 响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 Continent 4 响应而创建的行动手册。
3. 单击“**启动**”按钮。

   所选的行动手册将启动通过 Continent 4 响应的脚本。

   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 SKDPU NT 响应

SKDPU NT 是一款特权账户管理解决方案。

支持 SKDPU NT 7.0.4 版本。

如果您之前已配置 Kaspersky Next XDR Expert 与脚本启动服务的集成，并创建了会启动响应脚本的行动手册，则可以通过 SKDPU NT 对警报和事故作出响应。

您可以创建行动手册，通过 SKDPU NT 执行以下响应操作：

- 终止用户会话。当检测到可疑活动或违反安全规则时，行动手册将终止用户的所有会话。
- 阻止用户账户。行动手册将阻止用户账户并限制用户对系统的访问。
- 撤销用户权限。该用户将被移出特权用户组，其权限也将被撤销。

您可以单击此链接来下载脚本：

下载脚本

访问 SKDPU NT 所需的登录名和密码存储在 env.sample 配置文件中。您必须将此文件中的信息复制到您创建的新 ENV 文件中，然后在新文件中指定必要的参数。

运行该脚本需要使用 Python 3.10。

要通过 SKDPU NT 执行响应操作，您必须具有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

要启动通过 SKDPU NT 响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 SKDPU NT 响应而创建的行动手册。
3. 单击“**启动**”按钮。
   所选的行动手册将启动通过 SKDPU NT 响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 FortiGate 响应

FortiGate 解决方案可为企业网络提供以下保护措施：

- 防火墙 — 过滤网络流量并防止未经授权的访问。
- 入侵和攻击防护 — 识别并阻止可疑操作。
- Web 过滤 — 限制用户访问您认为不需要的网站。
- 恶意软件防护 — 防止恶意软件感染。
- 电子邮件过滤 — 阻止垃圾邮件和可疑电子邮件。

支持 FortiGate 7.6.0 版本。

如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务之间的集成，并创建了会启动响应脚本的行动手册，则可以使用 FortiGate 对警报和事故作出响应。行动手册启动后，FortiGate 将阻止 IP 地址、URL 或域名，具体取决于您在创建行动手册时指定的操作。

要解除对已被阻止的 IP 地址、URL 或域名的阻止，您必须创建并启动另一个行动手册。

您可以通过单击以下链接来下载脚本：

下载脚本

访问 FortiGate 所需的登录名、密码和 API 密钥存储在 env.sample 配置文件中。您必须将此文件中的信息复制到您创建的新 ENV 文件中，然后在新文件中指定必要的参数。

运行该脚本需要使用 Python 3.10。

要通过 FortiGate 执行响应操作，您必须具有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

要启动通过 FortiGate 响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 FortiGate 响应而创建的行动手册。
3. 单击“**启动**”按钮。
   所选的行动手册将启动通过 FortiGate 响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 Palo Alto NGFW 进行响应

Palo Alto NGFW 是一款为企业网络提供以下防护措施的解决方案：

- 防火墙 — 过滤网络流量，保护网络免受未经授权的访问。
- 入侵和攻击防护 — 识别和阻止可疑操作，确保系统完整性。
- 恶意软件防护 — 防止恶意软件感染。
- Web 过滤 — 限制用户访问您认为不需要的网站。

支持 PAN-OS（运行 Palo Alto NGFW 的操作系统）版本 11.1.6-h7。

如果您之前配置了 Kaspersky Next XDR Expert 和脚本启动服务之间的集成，并创建了将启动脚本进行响应的行动手册，则您可以通过 Palo Alto NGFW 对警报和事故作出响应。如果您想查看行动手册示例，请点击此链接。

行动手册启动后，Palo Alto NGFW 将阻止 IP 地址或 URL，具体取决于您在创建行动手册时指定的操作。要解除对已被阻止的 IP 地址或 URL 的阻止，您必须创建并启动另一个行动手册。

您可以单击此链接来下载脚本：

下载脚本

您必须按照 README 文件中的说明配置脚本：

a. 将 config.ini 文件中的 config.ini.example 文件重命名。

b. 在该文件中，指定部署了 Palo Alto NGFW 的设备的地址，以及您之前在 Palo Alto NGFW 界面中生成的 API 密钥。或者，您也可以在脚本所在的目录中运行以下命令来获取：

```
python main.py --get-api-key
```

如有必要，您还可以更改要添加 IP 地址或 URL 的默认组和政策。

要通过 Palo Alto NGFW 执行响应操作，您必须具有以下 XDR 角色之一：主管理员、租户管理员、1 级分析师或 2 级分析师。

要启动通过 Palo Alto NGFW 进行响应的脚本：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击所需警报或事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中，选择您为通过 Palo Alto NGFW 进行响应而创建的行动手册。
3. 单击“**启动**”按钮。

   所选的行动手册将启动通过 Palo Alto NGFW 进行响应的脚本。

   如果操作成功，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可以在“**历史记录**”选项卡上的警报或事故详情中找到。

通过 Jira 响应

Kaspersky Next XDR Expert 允许您将 Kaspersky XDR 事故与 Atlassian Jira 问题同步。

通过 Jira 集成响应可让您：

- 根据 XDR 事故创建具有全面上下文的 Jira 问题。
- 在事故数据发生变化时更新现有 Jira 问题。
- 检索 Jira 问题以便进行诊断。
- 将证据文件附加到 Jira 问题。
- 在不进行 API 调用的情况下，以试运行模式测试集成。
- 向 Jira 问题添加评论。

如果您之前配置了 Kaspersky Next XDR Expert 与脚本启动服务之间的集成，并创建了将启动脚本进行响应的行动手册，则可以通过 Jira 响应。

运行脚本需要 Python 3.12 及更高版本。

支持 Jira Software Cloud 或 Jira Data Center 8.4 或更高版本。

您可以通过单击以下链接来下载响应脚本：

下载脚本

要使用脚本：

1. 通过下列其中一种方式安装脚本：
   - 例如，通过 pip：

     ```
     pip install -r requirements.txt
     ```

   - 例如，通过 uv：

     ```
     uv sync
     ```

2. 根据您的 Jira 部署情况，执行以下操作之一：
   - 对于 Jira Cloud，生成 API 令牌。
   - 对于 Jira Data Center，请在您的 Jira Data Center 实例中生成个人访问令牌 (PAT)。
3. 运行以下命令，从 `.env.sample` 文件创建 `.env` 文件：

   ```
   cp .env.sample .env
   ```

4. 编辑 `.env` 文件并指定您的 Jira 凭据，例如：

   ```
   JIRA_BASE_URL="https://your-company.atlassian.net"
   JIRA_USER_EMAIL="bot@your-company.com"
   JIRA_API_TOKEN="your-api-token-here"
   JIRA_PROJECT_KEY="SEC"
   JIRA_ISSUE_TYPE="Incident"
   JIRA_ATTACHMENT_MAX_MB=10
   JIRA_INSECURE=false
   JIRA_AUTH_TYPE="basic"
   ```

   设置 `JIRA_INSECURE=true` 会禁用 SSL 证书验证。我们建议仅在使用自签名证书的测试环境中启用此选项。我们不建议在生产环境中启用此选项。

   `JIRA_AUTH_TYPE` 的值取决于您的 Jira 部署：Jira Cloud 为 `basic`，Jira 数据中心/服务器为 `bearer`。

脚本已配置并安装。

处理 Jira 问题

配置脚本后，您可以使用它执行以下操作：

- 创建问题。

  为此，请执行以下操作：

  ```
  uv run python -m src.jira --create \
    --incident-id 12345 \
    --name "Suspicious Lateral Movement Detected" \
    --severity high \
    --description "Detected unusual network activity" \
    --deep-link "https://xdr-console/incidents/12345" \
    --asset "host01|10.0.0.5|Windows" \
    --asset "host02|10.0.0.6|Linux" \
    --observable "md5:abcd1234" \
    --observable "url:https://malicious.com" \
    --mitre-technique "T1021" \
    --mitre-technique "T1003"
  ```

  如果命令执行成功，输出类似于以下内容：

  ```
  {
    "status": "created",
    "issue_key": "SEC-123",
    "issue_id": "10001",
    "self": "https://company.atlassian.net/rest/api/2/issue/10001"
  }
  ```

- 更新问题。

  为此，请执行以下操作：

  ```
  uv run python -m src.jira --update \
    --issue-key SEC-123 \
    --incident-id 12345 \
    --severity critical \
    --observable "ip:192.168.1.100" \
    --hash "new-hash-value" \
    --previous-hash "old-hash-value"
  ```

  如果命令执行成功，输出类似于以下内容：

  ```
  {
    "status": "updated",
    "issue_key": "SEC-123"
  }
  ```

- 检索 Jira 问题以便进行诊断。

  为此，请执行以下操作：

  ```
  uv run python -m src.jira --get --issue-key SEC-123
  ```

  如果命令执行成功，输出类似于以下内容：

  ```
  {
    "status": "success",
    "issue_key": "SEC-123",
    "fields": {
      "summary": "[XDR] Suspicious Activity - host01",
      "status": "Open",
      "priority": "High",
      "created": "2025-11-28T10:00:00.000+0000",
      "updated": "2025-11-28T10:30:00.000+0000",
      "labels": ["XDR_12345", "TECHNIQUE_T1021"]
    }
  }
  ```

- 在试运行模式下测试集成。

  为此，请执行以下操作：

  ```
  uv run python -m src.jira --create \
    --incident-id 12345 \
    --name "Test Incident" \
    --severity high \
    --dry-run
  ```

- 将文件附加到该问题。

  为此，请执行以下操作：

  ```
  uv run python -m src.jira --create \
    --incident-id 12345 \
    --name "Malware Detected" \
    --severity critical \
    --attachment "/path/to/evidence.json" \
    --attachment "/path/to/screenshot.png"
  ```

- 向该问题添加评论。

  为此，请执行以下操作：

  ```
  uv run python -m src.jira --comment \
    --issue-key SEC-123 \
    --comment-text "Investigation in progress, escalating to L2"
  ```

  如果命令执行成功，输出类似于以下内容：

  ```
  {"status":"commented","issue_key":"SEC-123"}
  ```

使用行动手册进行响应

要使用行动手册对 Jira 问题执行操作：

1. 在主菜单中，转到“**监控**”部分，然后在“**事故**”部分中，单击所需事故的 ID。
2. 单击“**选择行动手册**”按钮，然后在打开的窗口中选择您创建的用于通过 Jira 进行响应的行动手册。
3. 单击“**启动**”按钮。
   所选行动手册将启动通过 Jira 进行响应的脚本。
   操作成功完成后，屏幕上将显示相应消息。否则，将显示错误消息。

行动手册启动的结果可在事故详情的“**历史记录**”选项卡上查看。

查看警报或事故详情中的响应历史记录

执行响应操作后，您可以通过以下方式之一查看响应历史记录：

- 从警报或事故详细信息中查看。
- 从“响应历史记录”部分查看。
- 从行动手册详细信息中查看。
- 从“隔离”部分。
  当您选中所需文件旁边的复选框，然后单击**“在响应历史记录中查看文件”**按钮时，您将进入“**响应历史**”部分。您可以查看将文件移动到“**隔离**”的响应操作。

要从警报或事故详情中查看响应操作历史记录：

1. 在主菜单中，转到“**监控**”部分。
2. 打开“**警报**”或“**事故**”部分，然后单击执行响应操作的警报或事故的 ID。
3. 在打开的窗口中，转到“**历史记录**”选项卡，然后选择“**响应历史**”选项卡。
   将显示事件表并包含以下列：
   - **时间**。事件发生的时间。
   - **启动者**。启动响应操作的用户名称。
   - **事件**。事件描述。
   - **响应参数**。响应操作中指定的响应操作参数。
   - **资产**。启动响应操作的资产数量。您可以单击包含资产数量的链接来查看资产详情。

- **操作状态**。响应操作的执行状态。此列可显示以下值：
  - **等待批准** – 响应操作正在等待启动审批。
  - **已推出** – 响应操作正在执行中。
  - **成功** – 响应操作执行完成，无错误或警告。
  - **警告** – 响应操作已完成，但存在警告。
  - **错误** – 响应操作已完成，但存在错误。
  - **已终止** – 由于用户中断了执行，响应操作停止执行。
  - **批准时间已过** – 由于审批等待超时，响应操作停止执行。
  - **被拒绝**– 由于用户拒绝了启动，响应操作停止执行。
- **行动手册**。在其中启动响应操作的行动手册的名称。您可以单击链接以查看行动手册详情。
- **响应操作**。已执行的响应操作的名称。
- **资产类型** 为其启动响应操作的资产类型。可能值：**设备**或**用户**。
- **资产租户**。租户是为其启动响应操作的资产的所有者。

4. 如有必要，单击设置图标 (⚙)，然后选择要在表中显示的列。
5. 如有必要，单击过滤器图标 (▽)，然后在打开的窗口中指定并应用过滤条件：
   - 单击“**添加过滤器**”按钮，添加新过滤器。
   - 通过在以下字段中选择必要的值来编辑过滤器：
     - **属性**
     - **条件**
     - **值**
   - 删除过滤器。
   - 单击“**全部重置**”按钮，删除所有过滤器。

查看恶意软件扫描结果

恶意软件扫描完成后，您可以通过以下任一方式查看其结果：

- 从警报或事故详细信息
- 从响应历史记录
- 从行动手册详细信息

要查看恶意软件扫描的结果：

1. 在主菜单中，转到“**监控**”，然后执行以下操作之一：

   - 如果要从警报或事故详情中查看该结果，请转到“**警报**或**事故**”部分，然后单击执行了恶意软件扫描的警报或事故的 ID。在打开的窗口中，转到“**历史记录**”选项卡，然后选择“**响应历史**”选项卡以显示事件列表。
   - 如果要查看响应历史记录的结果，请转到“**响应历史**”部分。
   - 如果要从行动手册表中查看恶意软件扫描的结果，请转到“**行动手册**”部分，然后执行以下操作之一：
     - 选择执行了恶意软件扫描的行动手册。在工具栏中，单击“**查看历史**”按钮，然后选择“**查看响应历史**”。
     - 单击执行了恶意软件扫描的行动手册的名称。在打开的窗口中，单击“**查看历史**”按钮，然后选择“**查看响应历史**”。

2. 在“**操作状态**”列中，单击您要查看其恶意软件扫描结果的事件的状态。
   在打开的窗口中，将显示一个检测结果表。在“**管理服务器**”字段中，您可以选择显示检测表的管理服务器。
   资源表包含以下各列：

   - “**设备**”。设备名称或 ID。
   - **路径**。文件路径。
   - **哈希**。SHA-256哈希值
   - **检测名称**。设备上发生的检测的名称。
   - **操作状态**。威胁处理结果。
   - **用户**。与检测关联的用户账户。

处理因响应操作而获得的文件

要查看**文件**部分，您必须具有以下XDR角色之一：主要管理员、租户管理员、SOC管理员、SOC经理、一级分析师、二级分析师、初级分析师、批准人、审计员。

文件部分显示您手动下载并执行以下响应操作后获得的文件：文件、取证、注册表键、NTFS 元文件、进程内存转储、从隔离区获取文件。

我们建议您启用文件自动轮换功能，以便从**文件**中删除最旧的文件，然后您可以上传新文件。检测到威胁的文件不会被删除。此类文件与因威胁检测而创建的警报相关联。
您不会收到有关删除最旧文件的通知。

查看文件表格

要打开文件表格，请在主菜单中转到**存储库 → 文件**。该表显示存储在您拥有访问权限的租户中的文件。

在工具栏的右上角，您可以按如下方式对表格中的数据进行分组、过滤和搜索：

- 单击设置图标 ( )，然后选择要在表中显示的列。
- 单击筛选图标 ( )，然后在调用的菜单中指定并应用筛选条件。
- 在显示的**搜索**字段中单击搜索图标 ( )，写下您想要查找的内容，然后按**回车键**。

资源表包含以下各列：

- **名称或完整路径**。如果您手动下载了文件，文件名将显示在列中。如果文件是通过响应操作获得的，则会显示文件的完整路径。
- **大小**。文件大小。
- **MD5**。文件的MD5哈希值（如有）。
- **SHA256**。文件的SHA256哈希值（如有）。
- **上传于**。将文件添加到**文件**存储库的日期。
- **更新于**。文件在**文件**存储库中更新的日期。
- **租户**。文件所属的租户。

  在OSMP 实例层次结构中，如果租户是在子实例上创建的，则**租户**字段中的值将与子实例图标（ ）一起显示。
- **源**。将文件添加到**文件**存储库的用户名或响应操作结果获取文件的设备名称。
- **添加方法**。用于将文件添加到**文件**存储库的方法。

  如果文件是由用户上传的，则该列中会显示**由用户上传**值。如果文件是响应操作的结果，则会显示响应操作名称。
- **扫描状态**。上次执行文件扫描的结果。以下值会显示在此列：
  - **未扫描**
  - **正在扫描**
  - **未检测到**
  - **检测日期**
  - **错误**
- **描述**。该列包含您在配置响应操作参数或手动上传文件时在**描述**字段中编写的信息（如果有）。

您可以通过单击列标题并从下拉列表中选择所需的方法或状态来过滤**添加方法**列和**扫描状态**列中的数据。

在文件表中执行操作

在工具栏的左上角，您可以执行以下操作：

- 点按**刷新**按钮以更新表格中的数据。
- 通过单击**上传**按钮将文件从计算机上传到**文件**存储库。

  此时将在右侧打开一个侧边栏。在**租户**字段中，指定您希望拥有该文件的租户。然后单击**上传文件**链接，并选择计算机上的文件。如有必要，您还可以在**描述**字段中添加备注或描述，如果您想扫描文件以检测威胁，则开启**上传后扫描文件**切换开关。

  点按**上传**按钮后，面板会关闭，上传的文件会显示在表格中。上传大文件或多个文件时，您需要刷新表格以显示新文件。如果文件正在上传，则**名称或完整路径**列会显示加载指示器， **大小**列会显示已上传的文件大小占总文件大小的比例。
- 将文件保存到您的计算机。要做到这一点，请选中表格中一个或多个文件旁边的复选框，然后单击**下载**按钮。
- 使用以下技术扫描所选文件以检测威胁：YARA、沙盒和反恶意软件引擎。要做到这一点，请选中表格中一个或多个文件旁边的复选框，然后单击**扫描**按钮。
- 删除文件。为此，请选中表格中一个或多个文件旁边的复选框，然后单击**删除**按钮。
- 前往与文件相关的警报列表。为此，请选中表格中一个或多个文件旁边的复选框，然后单击**查找警报**按钮。显示因威胁检测而创建的警报以及您运行响应操作的详细信息的警报（如果响应操作导致文件被放置到**文件**存储库）。

> 如果以下响应操作：取证、注册表键、NTFS 元文件、进程内存转储，则**扫描**选项不可用，并且不会为获得的文件计算文件哈希值。

查看文件详细信息

您可以通过单击表格中**名称或完整路径**列中的链接来打开文件详细信息。

在打开的右侧面板中，显示文件元数据（例如，文件名或路径、大小、哈希值）、扫描状态和扫描结果：

- 如果发送了存档进行扫描，文件详细信息将显示存档中检测到威胁的文件的信息，以及此类文件的哈希值和每种技术的状态：反恶意软件、沙盒、YARA。
- 如果没有扫描文件，将显示相应的信息。
- 如果文件的扫描不可用，文件详细信息仅显示元数据。

> 如果文件是手动上传的并进行了扫描来检测威胁，在文件详细信息中，您还可以通过单击**扫描状态**字段中的**下载报告**链接来查看扫描报告。

在文件详细信息中，您可以进行以下操作：

- 通过单击工具栏中的相应按钮执行以下操作：扫描、下载、删除文件、查找关联的警报、编辑文件描述、移至响应历史记录。

  在响应历史中显示显示选项不适用于手动上传的文件。对于响应操作后获得的文件，单击**在响应历史中显示**后，您将转到**响应历史**部分，其中事件表将按文件过滤。

- 单击带有MD5或SHA256哈希值的链接，然后在下拉列表中选择要执行的操作：

  - 为检测到威胁的文件**创建防护规则**。选择该选项后，将打开**添加防护规则**面板，您可以在其中使用防御规则表。
  - **在 Kaspersky TIP 上查找**，用于在Kaspersky Threat Intelligence Portal上查看文件的哈希值。
  - **查看沙盒报告**。该选项适用于手动上传到**文件**存储库并使用沙盒技术扫描的文件。
  - **查找关联的警报**。关联的警报是由于威胁检测而创建的警报，以及您从其详细信息中运行响应操作的警报（如果响应操作导致文件被放入**文件**存储库）。
  - **查找关联的事件**，用于前往**威胁搜索**部分，其中事件表按文件的哈希值进行过滤。

在OSMP 实例层次结构中，在子实例上执行响应操作后下载和获取的文件会显示在父实例上的文件表中，并且在**租户** 字段中带有以下图标：(⛓)。

使用防护规则表

预防规则允许您阻止您认为不安全的文件或进程在设备上运行。Kaspersky Next XDR Expert使用MD5和SHA256哈希值算法根据其哈希值识别文件。

您可以通过以下方式管理预防规则：

- 如本文所述，从阻止规则表中手动创建、导入、编辑和删除阻止规则
- 通过执行相应的响应操作来创建和删除阻止规则
- 您也可以在创建或编辑行动手册时，配置自动运行的响应操作。

要打开防御规则表，您必须具有以下XDR角色之一：主管理员、租户管理员、SOC管理员、SOC经理、一级分析师、二级分析师、初级分析师、批准人、审计员。
要创建或导入防御规则，您必须具有以下XDR角色之一：主管理员、租户管理员、一级分析师、二级分析师。

要打开阻止规则表，请在主菜单中前往**监控→资源和服务→防护规则**。

资源表包含以下各列：

- **名称**。对于手动创建的阻止规则，该列会显示您在**创建防护规则**面板中指定的名称。对于导入的阻止规则，文件哈希值显示在列中。
- **哈希**。要阻止的文件的MD5或SHA256哈希值。

- **租户所有者**。阻止规则所属的租户。

  在分布式解决方案模式下，如果在次要节点上创建了租户，则**租户**字段中的值将与次要节点图标（⛓）一起显示。

- **资产**。应用了阻止规则的设备。该列显示设备数量或**租户的所有资产**的值。

- **创建日期**。阻止规则创建或导入的日期和时间。

- **创建者**。创建或导入阻止规则的用户。

- **更新于**。最后一次编辑阻止规则设置的日期和时间。

- **更新者**。上次编辑阻止规则设置的用户。

- **规则状态**。如果启用了阻止规则，该列将显示该规则的**启用**值。否则，会显示**禁用**值。

- **文件阻止时通知**。如果在创建或编辑阻止规则时禁用了有关阻止文件的通知，该列将显示**否**值。否则，会显示**是**值。

在表格中，您可以执行以下操作：

- 创建或导入阻止规则。

- 通过选中所需规则名称旁边的复选框，然后单击工具栏中的**删除**按钮来删除阻止规则。您还可以一次性删除所有规则。

- 通过选中所需规则名称旁边的复选框，单击工具栏中的**更改状态**按钮，然后选择**启用**或**停用**，启用和禁用防御规则。您还可以一次性启用和禁用所有规则。

- 通过单击列表中的规则名称来查看和编辑阻止规则的详细信息。

  打开**编辑防护规则**面板，并选中了**详细信息**选项卡。您可以编辑阻止规则设置。设置与从规则列表中创建阻止规则时相同。此外，您可以单击**前往威胁搜索**按钮，以查看触发阻止规则时获得的事件。

  在**更改日志**选项卡上，您可以查看应用于预防规则的所有更改：从预防规则表中手动查看、通过执行响应操作或通过启动行动手册。

要一次性对所有规则应用操作：

1. 选中**名称**列旁边的复选框。
2. 在下拉列表中，单击以下项之一：
   - 如果您要对表中的所有规则执行操作，请选择**全部选择**。
   - 如果您要对当前页面上的所有规则执行操作，请选择**在当前页面上全选**。
3. 如有必要，您可以通过清除规则名称旁边的复选框，将一条或多条规则排除在作用范围之外。
4. 在工具栏中，根据要执行的操作，单击相应的按钮：**删除**或**更改状态**（启用或禁用规则）。

   该操作将应用于您选择的所有规则。

创建防止规则

要创建防御规则：

1. 在主菜单中，前往**监控→资源和服务→防护规则**。
   阻止规则表随即显示。
2. 在工具栏中，单击**新建**按钮。
3. 在打开的**创建防护规则**面板中，配置设置：
   a. 在**租户所有者**字段中，指定阻止规则所属的租户。

   > 保存阻止规则设置后，您将无法编辑**租户所有者**字段中的值。如果要更改租户，则必须删除阻止规则，创建一个新规则，并在**租户所有者**字段中指定所需的值。

   b. 在“**MD5 或 SHA256**”字段中，指定要阻止的文件的哈希值。
   如果要指定多个哈希值，请单击**添加哈希值**按钮。

   > 应用程序检查哈希值是否存在于要阻止的文件哈希列表中的租户中。在创建新的阻止规则时，您无法指定此类哈希值。

   c. 如果必要，配置以下设置：
   - 改变阻止规则的范围。
     默认情况下，在**应用规则到**设置组中，**所有资产**选项已选择。这意味着阻止规则适用于所有设备。您可以选择**特定资产**选项，然后在显示的**资产**字段中，指定要应用阻止规则的一个或多个设备。

     > 如果您设置了要应用阻止规则的设备，然后删除了设备，则此类设备也会从阻止规则中删除，相应的信息将显示在阻止规则详细信息的**更改日志**选项卡中。

   - 在**规则名称**字段中，指定阻止规则的名称。如果未指定名称，则该字段将显示为空。
   - 在**通知用户有关阻止文件执行的信息**字段中，如果您不想在文件被阻止时接收通知，请禁用切换开关。
     默认情况下已启用该选项。
   - 如果您不想应用预防规则，请在**状态**字段中禁用切换开关。
     如果您要创建状态为**已禁用**的预防规则，则必须先配置其他设置。否则，您将无法保存该规则。

   d. 单击“**创建**”按钮。

面板将关闭，阻止规则将显示在规则列表中。

导入阻止规则

若要导入阻止规则：

1. 在主菜单中，前往**监控→资源和服务→防护规则**。
   阻止规则表随即显示。
2. 在工具栏上，单击**导入**按钮。

   从文件导入的阻止规则将适用于属于租户的资产，包括子租户。

3. 在打开的**导入防护规则**面板中，配置必要的设置：
   a. 从您的计算机上选择一个CSV文件。
      您只能添加一个包含哈希值的CSV文件。哈希值的数量等于要创建的阻止规则数量。文件大小不得超过15MB
   b. 在下拉列表中，选择要应用防御规则的租户。
      默认情况下，系统会选中您拥有访问权限的租户。如果需要的话，您可以更改其值。
      如果您拥有对多个租户的访问权限，则该值为空，您必须指定所需的租户。
   c. 单击**导入**按钮。

面板随即关闭，导入的阻止规则将显示在规则列表中。

使用IOC规则表

Kaspersky Next XDR Expert可以扫描设备以查找入侵指标（IOC）。多个IOC可以合并成一个结构化描述的IOC文件。导入 IOC 规则时，Kaspersky Next XDR Expert 会从 IOC 文件中提取结构化描述，并根据该描述创建规则。触发IOC规则后，会生成IOC警报。

查看IOC文件表

要查看IOC规则表，您必须具有以下XDR角色之一：主管理员、租户管理员、SOC管理员、SOC经理、一级分析师、二级分析师、初级分析师、批准人、审计员。

要打开IOC规则表，在主菜单中，前往**监控→资源和服务→IOC 规则**。该表显示存储在您拥有访问权限的租户中的IOC规则。

您可以按如下方式对表中的数据进行分组、筛选和搜索：

- 单击设置图标 (⚙)，然后选择要在表中显示的列。
- 单击筛选图标 (▽)，然后在调用的菜单中指定并应用筛选条件。
- 在显示的**搜索**字段中单击搜索图标 (🔍)，写下您想要查找的内容，然后按**回车键**。

资源表包含以下各列：

- **名称**。IOC规则名称。
- **创建日期**。IOC规则的创建日期和时间。
- **创建者**。创建IOC规则的用户。
- **更新于**。IOC文件的更新日期。
- **更新者**。上次编辑IOC规则设置的用户。
- **重要性**。IOC规则的重要性级别：**低**、**中**或**高**。
- **租户所有者**。IOC规则所属的租户。
  在分布式解决方案模式下，如果在子实例上创建了租户，则**租户**字段中的值将与子实例图标（🔗）一起显示。
- **计划扫描**。计划扫描的状态：**已启用**或**已禁用**。您可以通过将切换开关移动到**已启用**或**已禁用**位置来更改状态。

在IOC规则表中执行操作

在工具栏的左上角，您可以执行以下操作：

- 点按**刷新**按钮以更新表格中的数据。
- 通过单击**导入**按钮，从包含IOC规则的文件中导入IOC规则。
  要导入IOC规则，您必须具有以下XDR角色之一：主管理员、租户管理员、SOC管理员、一级分析师、二级分析师。
- 将IOC规则保存到您的电脑。为此，请选中表格中一个或多个规则旁边的复选框，然后单击**导出**按钮。
- 删除IOC规则。为此，请选中表格中一个或多个文件旁边的复选框，然后单击**删除**按钮。您还可以一次性删除所有规则。
- 执行IOC扫描响应操作。为此，请选中表格中一个或多个文件旁边的复选框，然后单击**运行 IOC 扫描**按钮。您还可以一次性对所有规则执行响应操作。
  要执行扫描，您必须拥有以下 XDR角色之一：主管理员、租户管理员、一级分析师、二级分析师。
- 打开或关闭所选IOC规则的计划扫描。为此，请选中表格中一个或多个规则旁边的复选框，单击**计划扫描**按钮，然后在下拉菜单中选择**启用**或**禁用**选项之一。您还可以一次性为所有规则启用或禁用扫描。
  必须配置计划扫描。

要一次性对所有规则应用操作：

1. 选中**名称**列旁边的复选框。
2. 在下拉列表中，单击以下项之一：
   - 如果您要对表中的所有规则执行操作，请选择**全部选择**。
   - 如果您要对当前页面上的所有规则执行操作，请选择**在当前页面上全选**。
3. 如有必要，您可以通过清除规则名称旁边的复选框，将一条或多条规则排除在作用范围之外。
4. 在工具栏中，根据要执行的操作，单击所需按钮：**删除**、启用或禁用**计划扫描**。

   该操作将应用于您选择的所有规则。

在OSMP 实例层次结构中，如果您在子实例中一次性启用、禁用或删除所有规则，并且所选规则中包含父实例的某些规则，则该操作不会应用于这些规则。
如果您单击**全部选择 → 计划扫描**或**全部选择 → 删除**，该操作仅应用于子实例的规则。
如果您单击**在当前页面上全选**，则**计划扫描**和**删除**按钮将被禁用。

查看IOC规则详细信息

您可以通过单击表格中**名称**列中的链接来打开IOC规则详细信息。

在打开的右侧窗格中，有关IOC规则的信息显示在相应的字段中：规则名称、规则所属的租户、规则的重要性、计划扫描状态（启用或禁用）以及触发规则的条件。

在详细信息面板中，您可以完成以下操作：

- 单击**导出**按钮，将IOC规则保存到您的电脑。
- 单击**运行 IOC 扫描**按钮，执行IOC扫描响应操作。
- 单击**查找警报**按钮，转到与IOC规则相关的警报列表。
  列表中将显示触发了该IOC规则的警报。如果没有此类警报，则会显示所有IOC警报。

使用YARA规则表

YARA规则是针对组织 IT 基础设施的针对性攻击和入侵的特征描述。Kaspersky Next XDR Expert 根据这些规则扫描对象。

查看YARA规则表

> 要查看YARA规则表，您必须具有以下XDR角色之一：主管理员、租户管理员、SOC管理员、SOC经理、一级分析师、二级分析师、初级分析师、批准人、审计员。

要打开YARA规则表，请在主菜单中前往**监控→资源和服务→YARA 规则。**

该表显示存储在您拥有访问权限的租户中的YARA规则。

您可以按如下方式对表中的数据进行分组、筛选和搜索：

- 单击设置图标 (⚙)，然后选择要在表中显示的列。
- 单击筛选图标 (▽)，然后在调用的菜单中指定并应用筛选条件。
- 在显示的**搜索**字段中单击搜索图标 (🔍)，写下您想要查找的内容，然后按**回车键**。

资源表包含以下各列：

- **名称**。YARA规则名称。
- **创建日期**。YARA规则的创建日期和时间。
- **创建者**。创建YARA规则的用户。
- **更新于**。YARA规则的更新日期。
- **更新者**。上次编辑YARA规则设置的用户
- **重要性**。YARA规则的重要性级别：**低**、**中**或**高**。
- **租户所有者**。YARA规则所属的租户。
  在分布式解决方案模式下，如果在子实例上创建了租户，则**租户**字段中的值将与子实例图标（🔗）一起显示。
- **文件扫描**。YARA扫描的状态：**已启用**或**已禁用**。您可以通过将切换开关移动到**已启用**或**已禁用**位置来更改状态。
- **描述**。YARA规则的描述或注释。

在YARA规则表中执行操作

在工具栏的左上角，您可以执行以下操作：

- 点按**刷新**按钮以更新表格中的数据。
- 单击**导入**按钮，从包含YARA规则的文件中导入YARA规则。
  要导入YARA规则，您必须具有以下XDR角色之一：主管理员、租户管理员、SOC管理员、一级分析师、二级分析师。

- 将YARA规则保存到您的电脑。为此，请选中表格中一个或多个规则旁边的复选框，然后单击**导出**按钮。
- 删除YARA规则。为此，请选中表格中一个或多个文件旁边的复选框，然后单击**删除**按钮。您还可以一次性删除所有规则。
- 执行YARA扫描响应操作。为此，请选中表格中一个或多个规则旁边的复选框，然后单击**运行 YARA 扫描**按钮。您还可以一次性对所有规则执行响应操作。

  要执行扫描，您必须拥有以下 XDR角色之一：主管理员、租户管理员、一级分析师、二级分析师。
- 打开或关闭所选YARA规则的计划扫描。为此，请选中表格中一个或多个规则旁边的复选框，单击**文件扫描**按钮，然后在下拉菜单中选择以下选项之一：**启用**或**禁用**。您还可以一次性为所有规则启用或禁用扫描。

要一次性对所有规则应用操作：

1. 选中**名称**列旁边的复选框。
2. 在下拉列表中，单击以下项之一：
   - 如果您要对表中的所有规则执行操作，请选择**全部选择**。
   - 如果您要对当前页面上的所有规则执行操作，请选择**在当前页面上全选**。
3. 如有必要，您可以通过清除规则名称旁边的复选框，将一条或多条规则排除在作用范围之外。
4. 在工具栏中，根据您要执行的操作，单击所需按钮：**删除**，或者启用或禁用**文件扫描**。

   该操作将应用于您选择的所有规则。

如果您要一次性启用或禁用所有规则，并且所选内容包含属于子租户的规则：

- 单击**全部选择**时，仅属于根租户的规则会更改其状态。
- 单击**在当前页面上全选**时，**文件扫描**按钮将灰显。

在OSMP 实例层次结构中，一次性对所有规则应用操作需要注意一些特定事项。

点击此处查看

一次性启用和禁用所有规则

在父实例中

- 如果您单击**全部选择**，并且所选内容包含属于父实例或子实例的子租户的规则，则该操作不会应用于这些规则。

  对于这两个实例，仅会启用或禁用属于根租户的规则。
- 如果您单击**在当前页面上全选**，并且所选内容包含属于父实例或子实例的子租户的规则，则**文件扫描**按钮将灰显。

在子实例中

- 如果您单击**全部选择**，并且所选内容包含属于子租户的规则或父实例的任何规则，则该操作将仅应用于属于根租户的子实例规则。
- 如果您单击**在当前页面上全选**，并且所选内容包含属于子租户的规则或父实例的任何规则，则**文件扫描**按钮将灰显。

一次性删除所有规则

在父实例中，

您可以删除属于父实例和子实例的任何租户的任何规则。

在子实例中：

- 如果您单击**全部选择**，并且所选内容包含父实例规则，则这些规则不会被删除。
- 如果您**在当前页面上全选**，并且所选内容包含父实例规则，则**删除** 按钮将灰显。

查看YARA规则详细信息

您可以通过单击表格中**名称**列内的链接，打开YARA规则详细信息。

在打开的右侧窗格中，有关YARA规则的信息显示在相应的字段中：规则名称、规则所属的租户、规则的重要性、扫描状态（启用或禁用）、规则描述以及触发规则的条件。

在详细信息面板中，您可以完成以下操作：

- 单击**导出**按钮，将YARA规则保存到您的电脑。
- 单击**运行 YARA 扫描**按钮，执行YARA扫描响应操作。
- 单击**查找警报**按钮，转到与YARA规则相关的警报列表。
  列表中将显示触发了该YARA规则的警报。如果没有此类警报，则会显示所有YARA警报。

行动手册

Kaspersky Next XDR Expert 使用行动手册来自动执行工作流，并缩短处理警报和事故所需的时间。

*行动手册*会根据预设*算法*对警报或事故做出响应。行动手册将启动包含一系列响应操作的算法，帮助分析和处理警报或事故。您可以手动启动行动手册，也可以为所需行动手册配置自动启动。

行动手册的自动启动是根据您在*创建行动手册*时配置的触发规则执行的。触发规则定义了警报或事故触发行动手册自动启动必须满足的条件。

一个行动手册的适用范围仅限于警报或事故中的一种。

子事故无法触发行动手册自动启动。对于子事故，您只能手动启动行动手册。启动之前，您需要选择要启动行动手册的资产和可观察对象。请注意，只能为属于警报或事故租户的对象启动行动手册。

请注意，行动手册仅归属于一个租户，并且会被父租户的所有子租户自动继承，包括在行动手册创建后新增的子租户。创建或编辑行动手册时，您可以禁用子租户对行动手册的继承。

Kaspersky Next XDR Expert 中有两种类型的行动手册：

- 预定义行动手册

  预定义行动手册由卡巴斯基专家创建。这些行动手册的名称带有 [KL] 前缀，无法编辑或删除。

  默认情况下，预定义行动手册在“**培训**”模式下运行。有关详情，请参阅预定义行动手册部分。

- 自定义行动手册

  您可以自行创建和配置行动手册。创建自定义行动手册时，需要指定行动手册适用范围（警报或事故）、自动启动行动手册的触发规则以及威胁响应算法。有关创建行动手册的详细信息，请参阅创建行动手册。

您可以使用XDR REST API为特定租户导入和导出行动手册。

操作模式

您可以同时配置自动和手动启动行动手册。行动手册的启动方式取决于所选的操作模式。

操作模式包括以下类型：

- **自动**。在该操作模式下，行动手册会在检测到相应警报或事故时自动启动。
- **培训**。在该操作模式下，当检测到相应警报或事故时，行动手册将在启动前请求用户确认。
- **手动**。在该操作模式下，仅支持手动启动行动手册。

用户角色

通过分配用户角色，您可以向用户授予管理行动手册的权限。

下表列出了管理行动手册和执行用户操作的访问权限。

用户角色	用户角色权限				
	读取	写入	删除	执行	响应确认
常规管理员	✓	✓	✓	✓	✓
SOC 管理员	✓	✓	✓	–	–
初级分析师	✓	–	–	–	–
1级分析师	✓	–	–	✓	–
2 级分析师	✓	✓	✓	✓	–
SOC 经理	✓	–	–	–	–
审批人	✓	–	–	–	✓
审计员	✓	–	–	–	–
租户管理员	✓	✓	✓	✓	✓

查看行动手册列表

行动手册表显示在“**监控**” → “**行动手册**”部分。默认情况下，该表格显示与您有访问权限的所有租户相关的行动手册。

> 行动手册表显示所有现有行动手册，“**已删除**”状态的行动手册除外。

要配置行动手册表，请执行以下操作之一：

- 应用租户过滤器：
  a. 单击“**租户过滤器**”设置旁边的链接。
  b. 租户过滤器将打开。
  c. 选中相应租户旁边的复选框。
- 筛选行动手册表的数据：
  a. 单击筛选 ( ) 图标。
  b. 单击“**过滤器**”选项卡，然后在调用的菜单中指定并应用筛选条件。
- 如果要隐藏或显示某一列，请单击设置 ( ) 图标，然后选择必要的列。

行动手册表已配置并显示您需要的数据。

行动手册表包含以下信息：

- **名称**。自定义或预定义行动手册的名称。

  > 预定义行动手册的名称以 [KL] 前缀标记，无法编辑或删除。

- **状态**。行动手册状态。可能值：
  - **活动**。行动手册已创建并可供使用（所有必要的 Web 插件均已安装）。
  - **草稿**。行动手册已创建并保存为草稿。该行动手册无法启动，但可以在其所属的租户中进行查看、编辑、自定义和删除操作。
  - **已删除**。行动手册已删除。默认情况下，处于此状态的行动手册不会显示在表格中。如果要查看这些行动手册，请单击“**状态**”列，然后在下拉列表中选择“**已删除**”。

    只有处于活动状态和不可用的行动手册在删除后才具有“**已删除**”状态。处于“**草稿**”状态的行动手册将被永久删除，不会显示在行动手册表中。

  - **不可用**。行动手册算法使用不可用的 Web 插件或包含授权许可不允许的响应操作。
- **操作模式**。定义如何启动行动手册的行动手册操作模式。有关操作模式的更多详细信息，请参阅“行动手册”部分。
- **标签**。分配给行动手册的标签。您可以使用所分配的标签筛选行动手册。
- **操作**。在行动手册内启动的操作。
- **启动**。行动手册启动的总次数。
- **已修改**。上次编辑行动手册的日期和时间。
- **创建日期**。行动手册创建的日期和时间。
- **父租户**。行动手册所属租户名称。
- **描述。**行动手册的描述或注释。默认情况下，此列处于隐藏状态。
- **范围**。行动手册适用范围。可能值：**警报**或**事故**。
- **创建者**。创建行动手册的用户名称。默认情况下，此列处于隐藏状态。
- **更新者**。编辑行动手册的用户名称。默认情况下，此列处于隐藏状态。

创建行动手册

您可以通过创建行动手册来实现威胁分析和威胁响应自动化。

要创建行动手册，您必须拥有以下任一用户角色：主管理员、SOC 管理员、1级分析师、2 级分析师、租户管理员。

Kaspersky Next XDR Expert 还支持基于现有行动手册创建满足您需求的新行动手册。有关详细信息，请参阅自定义行动手册。

要创建新的行动手册：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。

2. 单击“**创建**”按钮。

   将打开“**创建行动手册**”窗口，窗口左侧为可视化编辑器工作区，右侧为“**行动手册设置**”窗格。在可视化编辑器中，您可以构建行动手册执行流程及各流程步骤之间的关系，并实现可视化。

   > 根据您在可视化编辑器中执行的操作，系统会生成行动手册算法的 DSL 模式。您在可视化编辑器工作区中所做的更改将显示为代码，反之亦然。如有必要，您可以单击工具栏中的“**显示代码**”按钮，以打开代码编辑器。

3. 在“**行动手册设置**”窗格中，指定以下设置：

   - 在“**租户和继承**”字段中，选择要为其启动行动手册的父租户和子租户。

     > 所选父租户的所有子租户将自动继承该行动手册。要禁用行动手册继承，请清除所需子租户旁边的复选框。将针对该租户及其子租户（如有）禁用行动手册继承。
     > 如果您选择一个子租户，则会自动选择其子租户。

   - 在“**名称**”字段中，输入行动手册的名称。

     请注意，行动手册名称在所属租户中必须是唯一的，且长度不能超过 255 个字符。

   - 在“**范围**”列表中，选择以下选项之一：

     - **警报**。行动手册将仅在出现警报时启动。默认情况下已选中该选项。
     - **事故**。行动手册将仅在出现事故时启动。

   - 在“**操作模式**”列表中，选择以下选项之一：

     - **自动**。在该操作模式下，行动手册会在检测到相应警报或事故时自动启动。
     - **培训**。在该操作模式下，当检测到相应警报或事故时，行动手册将在启动前请求用户确认。
     - **手动**。在该操作模式下，仅支持手动启动行动手册。

   - 如有必要，在“**标签**”字段中指定最多 30 个标签。您可以使用所分配的标签筛选行动手册。

     请注意，标签的最大长度为 50 个字符。

   - 如有必要，在“**描述**”字段中输入行动手册描述或注释。

   - 在“**同时启动多个行动手册实例时**”下拉列表中，选择两个或多个行动手册实例同时启动时要执行的操作：

     - **将新的行动手册实例添加到队列**。新的行动手册实例将在当前实例完成执行后启动。默认情况下已选定该操作。
     - **终止当前执行并启动新实例**。当前行动手册实例的执行将被终止。之后，将启动一个新的行动手册实例。
     - **不启动新的行动手册实例**。不会启动新的行动手册实例。当前行动手册实例继续执行。

只有选择“**自动**”操作模式时，才会显示“**同时启动多个行动手册实例时**”列表。

- 默认情况下，只有出现与触发规则匹配的新警报或事故时才会启动行动手册。

  如果要针对与触发规则匹配的现有警报或事故启动新的行动手册，请选中“**针对所有匹配的警报或事故启动行动手册。请注意，系统可能会超载**”复选框。

- 如有必要，在**附加设置**部分中，指定以下行动手册参数：

  - **行动手册超时** – 行动手册的最长执行时间。默认情况下，该值为 24h。最大值为 48h。

    若要创建策略以便后续将其应用于响应操作，请启用“**对响应操作使用超时策略**”切换开关，然后添加策略。

    禁用切换开关后，已添加的策略将被删除。

  - **输入** – 用于在执行前修改行动手册传入数据的 jq 表达式。
  - **输出** – 用于在执行后修改行动手册输出数据的 jq 表达式。
  - **更改方法** – 如何更改输出数据。选择“**合并**”或“**覆盖**”选项，以决定合并当前数据与新数据，或使用新数据覆盖当前数据。

  其他附加设置是预定义的，无法更改：

  - **行动手册版本** – 行动手册的版本。可用于在遥测数据中精准标识行动手册。
  - **DSL 版本** – DSL 架构版本。
  - **操作版本** – 响应操作模式版本，其中包含响应函数输入参数的描述。

4. 在可视化编辑器工作区中，配置行动手册触发规则和算法。单击“**触发器**”步骤，然后在打开的触发规则设置窗格中，指定自动启动行动手册的条件。

   如果选择“**手动**”操作模式，则触发规则设置不可用。

   要描述触发条件，请使用 jq 表达式。有关 jq 表达式的更多信息，请参阅 jq 手册。

   根据您在创建或编辑行动手册时在“**范围**”列表中选择的选项，将使用警报数据模型或事故数据模型。

   例如，要按严重级别筛选警报或事故，请指定以下表达式：

   ```
   .Severity == "critical"
   ```

   您也可以指定复杂的表达式来筛选警报或事故。

   例如，要按规则名称筛选严重警报或事故，请指定以下表达式：

   ```
   (.Severity == "critical") and (.Rules[] |.Name | contains("Rule_1"))
   ```

   其中 `Rules[] |.Name` 定义触发规则的名称。

   jq 表达式的验证已配置。如果在配置行动手册触发规则时指定了不正确的表达式，则错误将以红色标记。如果要查看详细信息，请将鼠标光标悬停在错误上。

5. 如果要查看与行动手册触发规则匹配的警报或事故，请在“**触发器匹配**”部分中单击“**查找**”按钮。默认情况下，将显示最近修改的 10 个警报和事故。如果要更改该值，请打开下拉列表，然后选择所需的值。

   您还可以请求完整的警报或事故列表。为此，请在“**触发器**”部分中输入 `true`，然后单击“**查找**”按钮。

   将显示完整的警报或事故列表。

6. 指定行动手册算法步骤。

   您可以从另一个行动手册复制算法。要执行此操作，请在工具栏中单击“**复制算法**”按钮，然后在打开的窗口中选择要复制算法的行动手册，并单击“**确定**”。

   > jq 表达式和 JSON 语法的验证已配置。如果在配置行动手册算法时指定了错误的表达式，则错误将以红色标记。如果要查看详细信息，请将鼠标光标悬停在错误上。

   要添加算法步骤，请执行以下操作：

   a. 将鼠标光标悬停在要与新步骤建立关联的步骤上。

      如果您是第一次添加步骤，则只能将鼠标光标悬停在“**触发器**”步骤上。

   b. 单击并按住显示的白点符号 ( )，然后开始绘制箭头。

   c. 松开鼠标光标，然后在打开的菜单中选择步骤。

      所选步骤将显示在可视化编辑器中。

   d. 单击该步骤，即可配置其设置。有关详细信息，请参阅“在可视化编辑器中配置行动手册执行步骤”。

   或者，您可以右键单击可视化编辑器工作区的任何部分以调用菜单，然后选择要添加的步骤。在这种情况下，添加步骤后，您必须通过在所需步骤之间绘制箭头来建立关系。如果没有建立任何关系，您只能将行动手册保存为草稿。

   > 如果没有添加算法步骤，您只能将行动手册保存为草稿。

7. 通过以下任一方式保存行动手册：

   - 单击“**发布**”按钮。所保存的行动手册可以使用，并将以“**活动**”状态显示在行动手册表中。
   - 单击“**创建为草稿**”按钮。只需指定名称和所属租户，即可创建行动手册。该行动手册将显示在行动手册列表中，状态为“**草稿**”。您可以打开该手册并继续编辑。

     > 将行动手册保存为草稿时，系统会对其进行检查；错误会突出显示，但会被忽略。
     > 仅当执行步骤与触发器之间未建立任何链接、未配置必需参数或指定了无效参数时，才能将行动手册保存为草稿。

   新的行动手册已创建，并显示在行动手册列表中。

在可视化编辑器中配置行动手册执行步骤

在创建或编辑行动手册时添加行动手册执行步骤后，您必须配置其设置。为此，请单击包含该步骤的区块，然后在右侧窗格中使用 jq 表达式指定所需的参数。

在可视化编辑器中，您可以添加和配置以下类型的行动手册执行步骤：

- **操作**

  - 在“**操作类型**”列表中，选择响应操作的类型。其他设置根据所选类型而有所不同。
    响应操作的类型通常可分为**若干组**。

    KATA/KEDR 响应操作：

    - **添加防护规则**
      指定必须应用该操作的资产，以及要阻止的文件的 SHA256 或 MD5 哈希。
    - **删除防护规则**
      指定应用了防护规则的资产，以及要删除的文件哈希。
    - **重置防护规则**
      指定要重置防护规则的资产。
    - **运行程序**
      指定资产和可执行文件参数：“**完整路径**”字段中文件的完整路径，以及在“**命令行参数**”字段中启动文件所需的参数。在“**工作目录**”文件中，您可以指定要保存命令或文件执行结果的目录的路径。
    - **启用网络隔离**
      指定要启用隔离的资产以及隔离期。如果要添加网络隔离规则的例外项，请单击“**添加排除项**”按钮，然后指定所需的参数。
    - **禁用网络隔离**
      指定应用网络隔离的资产。

    Active Directory 响应操作：

    - **锁定账户**
      指定要阻止其账户的用户。
    - **重置密码**
      指定要重置其密码的用户。
    - **将用户添加到安全组**
      指定用户和要将用户添加到哪个组。
    - **从安全组中删除用户**
      指定用户和要从中删除用户的组。

    Kaspersky NGFW 响应操作：

    - **将 IP 添加到网络设备上的阻止列表**
      请指定要阻止的 IP 地址。

    KES for Windows 响应操作：

    - **运行恶意软件扫描**

指定资产和扫描类型：

- **关键区域扫描**。
- **自定义扫描**。然后，指定要扫描的文件的路径。
- **全盘扫描**。如有必要，请启用 **扫描网络驱动器** 切换开关，将网络设备纳入扫描范围。

如果您希望仅在恶意软件扫描后启动下一个响应操作，请启用“**等待响应操作完成**”切换开关。

- **更新数据库**

  指定要进行数据库更新的设备。如果您希望仅在数据库更新后启动下一个响应操作，请启用“**等待响应操作完成**”切换开关。

- **终止进程**

  指定要终止进程的设备。然后，选择其中一个参数，并指定包含所需信息的 jq 表达式：进程文件的**哈希和路径**、文件的**完整路径**或 **PID**（进程 ID）。

  > 当带有内置代理的 Kaspersky Endpoint Security 以 EDR Expert 模式运行时，不支持通过系统 PID 终止进程。

- **移动到隔离区**

  指定要移动的文件所在的设备。然后，选择其中一个参数并指定包含所需信息的 jq 表达式：要隔离的文件的**完整路径**或文件的**哈希和路径**。

KASAP 响应操作：

- **分配 KASAP 组**

  指定要移动到 KASAP 学习组的用户，然后指定组 ID。

Kaspersky Security Center 响应操作：

- **移动到组**

  指定设备和要将设备移动到其中的组的路径。

KICS for Networks 响应操作：

- **更改授权状态**

  指定设备及其状态：*已授权*或*未授权*。

自定义第三方响应操作：

- **运行自定义脚本**

  在相应的字段中，指定要运行的命令、要应用于命令的带有命令行参数的 jq 表达式以及工作目录的路径。如果脚本需要来自标准输入的附加数据，请在“**标准输入**”字段中指定此数据。

卡巴斯基威胁情报门户响应操作：

- **丰富数据**

  选择要进行数据增强的对象数：所有对象或来自源的前 100 个对象。指定 jq 表达式，其中包含要进行数据增强的可观察对象数组。您可以对以下类型的可观察对象进行数据增强：MD5、SHA256、URL、域或 IP 地址。

使用行动手册编辑警报或事故：

- **分配给用户或用户组**

  选择要向其分配警报或事故的用户或用户组。

- **更改外部引用属性**

  使用警报或事故外部参考属性指定 jq 表达式，然后选择是覆盖当前输出数据，还是合并当前数据和新数据。

- **更改附加数据**

  选择是覆盖当前输出数据，还是合并当前数据和新数据。

- **更改状态**

  选择警报或事故的状态：**新建**、**进行中**或**已关闭**。如果行动手册的适用范围是事故，则还必须选择事故类型。

- **更改类型**

  选择事故的类型。

  仅当您在创建或编辑行动手册时在“**范围**”下拉列表中选择了“**事故**”时，此操作类型才可用。

- **更改描述**

  指定包含事故描述的 jq 表达式，然后选择是覆盖当前输出数据，还是合并新数据和当前数据。

  仅当您在创建或编辑行动手册时在“**范围**”下拉列表中选择了“**事故**”时，此操作类型才可用。

- **更改优先级**

  选择事故的优先级：**严重**、**高**、**中**或**低**。

  仅当您在创建或编辑行动手册时在“**范围**”下拉列表中选择了“**事故**”时，此操作类型才可用。

- **添加注释**

  指定带有警报或事故注释的 jq 表达式。

- 如有必要，请在“**附加设置**”部分中单击 V 形图标 (⌄)，然后**指定其他设置**

  - 单击“**终止**”或“**继续**”按钮，选择在发生错误时终止还是继续执行行动手册。

  - 配置响应操作超时。您可以选择“**策略**”选项，然后指定所需的超时策略；或者选择“**自定义**”选项，然后指定以小时为单位的超时时间。

  - 通过启用“**输出数据**”切换开关来修改行动手册的传出数据。在“**输出**”字段中，指定用于替换响应操作返回数据的 jq 表达式，然后选择“**合并**”或“**覆盖**”替换方法。

  - 通过启用“**手动批准**”切换开关来手动审批响应函数调用，然后指定以分钟为单位的审批超时时间。默认值是 60 分钟。

    如果要启用电子邮件通知，请选中“**通过邮件通知**”复选框，然后指定发送电子邮件通知之前的延迟时间。最小值为 5 分钟，最大值为 30 分钟。此外，请确保已配置 SMTP 服务器连接，并在用户属性中指定了电子邮件地址。

- **循环**

选择此类型的步骤后，“**循环**”和“**结束循环**”区块将添加到可视化编辑器中。

- 单击“**循环**”区块，指定一个 jq 表达式以生成传入数据的数组，然后选择用于处理元素的“**并行**”或“**顺序**”模式。
- 如有必要，请在“**附加设置**”部分中单击 V 形图标 (⌄)，然后**指定其他设置**
  - 单击“**终止**”或“**继续**”按钮，选择在发生错误时终止还是继续执行行动手册。
  - 在“**最大批次大小**”字段，指定行动手册可以作为输入的元素数量。
  - 设置用于将行动手册执行结果聚合到传入数组元素的规则。启用“**聚合结果**”切换开关后，在“**表达式**”字段中指定 jq 表达式，以将传出数据用作后续执行步骤的输入数据。
  - 通过在**输出**字段中指定jq表达式来修改传出数据。
  - 单击“**合并**”或“**覆盖**”按钮，选择是覆盖当前输出数据，还是合并新数据和当前数据。

- **并行**

  选择此类型的步骤后，“**并行**”和“**并行结束**”区块将添加到可视化编辑器中。

  - 单击“**并行**”区块，指定一个 jq 表达式来生成传入数据的数组，然后输入分支的名称。

    您可以通过单击“**添加分支**”按钮来添加新的分支。
  - 如有必要，请在“**附加设置**”部分中单击 V 形图标 (⌄)，然后**指定其他设置**
    - 单击“**终止**”或“**继续**”按钮，选择在发生错误时终止还是继续执行行动手册。
    - 设置用于将行动手册执行结果聚合到传入数组元素的规则。启用“**聚合结果**”切换开关后，在“**表达式**”字段中指定 jq 表达式，以便将传出数据用于后续执行步骤。
    - 通过在**输出**字段中指定jq表达式来修改传出数据。
    - 单击“**合并**”或“**覆盖**”按钮，选择是覆盖当前输出数据，还是合并新数据和当前数据。

- **决定**

  选择此类型的步骤后，“**决定**”和“**决定结束**”区块将添加到可视化编辑器中。单击“**决定**”区块，指定一个包含条件的 jq 表达式以及条件名称。

  如有必要，请单击“**添加条件**”按钮来添加新条件。

- **更新数据**

  在“**输出**”字段中指定 jq 表达式，然后选择是覆盖当前输出数据，还是合并新数据和当前数据。

您可以按照行动手册执行步骤来执行以下操作：

- 通过单击执行步骤区块进行编辑，然后在打开的属性窗口中更改所需的参数。

  > 对于暗示输入 jq 表达式的参数，语法会突出显示，并且在您开始输入时会显示建议。

- 通过单击并拖动执行步骤区块，在可视化编辑器工作区中移动。
- 通过单击执行步骤区块，然后按 `Backspace` 键或 `Delete` 键进行删除。

在工具栏中，您可以执行以下操作：

- 单击“**设置**”按钮以打开“**行动手册设置**”窗格。
- 单击“**显示代码**”按钮以打开包含 DSL 架构的代码编辑器。
  单击 (⌓) 图标可以展开代码面板，单击 (⨯) 图标可以关闭面板。
- 单击“**复制算法**”按钮，从另一个行动手册复制算法。
- 单击“**查看响应历史**”按钮，打开行动手册响应历史记录。
- 单击“在测试模式下启动**以测试模式启动模拟行动手册启动**，而无需实际执行响应操作。
- 单击“**撤销**”按钮，即可撤消可视化编辑器中的任何操作。
- 单击“**重做**”按钮可恢复之前撤消的操作。
- 单击“**Arrange**”按钮可自动对齐各元素。

编辑行动手册

要编辑行动手册，您必须拥有以下任一用户角色：主管理员、SOC 管理员、1级分析师、2 级分析师、租户管理员。

对于预定义的行动手册，您只能更改行动手册模式和启动规则。您也可以查看与预定义行动手册匹配的警报或事故。

仅当您有权限更改行动手册所属的租户时，才可以编辑行动手册。

要编辑行动手册：

1. 在主菜单中，转到**监控 → 行动手册**。
2. 单击您需要编辑的行动手册名称。
3. 在打开的窗口中，编辑行动手册的属性。有关您可以编辑的行动手册属性的更多详细信息，请参阅“创建行动手册”。
4. 如果您已将操作模式更改为“**自动**”，请在“**同时启动多个行动手册实例时**”下拉列表中选择以下任一操作：
   - **将新的行动手册实例添加到队列**。新的行动手册实例将在当前实例完成执行后启动。默认情况下已选定该操作。
   - **终止当前执行并启动新实例**。当前行动手册实例的执行将被终止。之后，将启动一个新的行动手册实例。
   - **不启动新的行动手册实例**。不会启动新的行动手册实例。当前行动手册实例继续执行。

5. 如果您已将操作模式更改为“**手动**”，请在“**对已启动的行动手册实例的操作**”下拉列表中，选择要应用于启动行动手册实例的操作：

   - **终止正在执行或待审批的实例**。
   - **仅终止待审批的实例**。
   - **执行所有正在进行或待审批的实例**。

6. 单击“**保存**”按钮保存更改。
   如果您想在保存之前向行动手册添加注释，也可以单击“**保存并注释**”按钮。

行动手册的属性已被修改并保存。

自定义行动手册

您可以根据需要自定义任何行动手册。

要自定义行动手册：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 从列表中选择行动手册，然后单击“**复制和编辑**”按钮，即可打开行动手册进行编辑。
3. 在打开的窗口中，根据您的需要配置行动手册的属性。
   有关您可以编辑的行动手册属性的更多详细信息，请参阅“创建行动手册”。
   如果要自定义行动手册算法参数，请参阅“行动手册算法”。

   > 自定义行动手册的名称必须是唯一的。

4. 单击“**保存**”按钮。

自定义行动手册已修改并保存。

查看行动手册属性

行动手册可用于工作流自动化并减少处理警报和事故所需的时间。

> 要查看行动手册，您必须拥有以下任一用户角色：主管理员、SOC 管理员、1级分析师、2 级分析师、SOC 经理、审批人、审计者、租户管理员。

要查看行动手册的属性：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 在行动手册列表中，单击需要查看的行动手册的名称。
   包含该行动手册相关信息的窗口将打开。

在右侧的“**行动手册设置**”窗格中，显示以下基本信息：

- **租户和继承**。行动手册所属租户名称。
- **名称**。行动手册名称。
- **范围**。行动手册适用范围。可能值：**警报**或**事故**。
- **操作模式**。行动手册操作模式。可能值：**自动**、**培训**、**手动**。
  如果行动手册的操作模式设置为“**自动**”，将显示“**同时启动多个行动手册实例时**”字段。可能值： **不启动新的行动手册实例**、**终止当前执行并启动新实例**、**将新的行动手册实例添加到队列**。
- **标签**。分配给行动手册的标签。
- **描述**。行动手册描述。
- **附加设置**。创建行动手册时指定的可选设置。

在左侧可视化编辑器工作区中，显示了行动手册触发规则和算法（行动手册执行步骤）。

> 如果您拥有以下任一角色，则可以编辑行动手册的属性：主管理员、SOC 管理员、1级分析师、2 级分析师、租户管理员。

单击工具栏中的**查看响应历史**按钮，即可查看行动手册响应历史记录。行动手册及其中所有已启动响应操作的列表将打开。您可以通过单击**终止**按钮来终止任何已启动的行动手册或响应操作。

如有必要，您可以按如下方式对表格中的数据进行分组和筛选：

- 单击设置图标 (⚙)，然后选择要在表中显示的列。
- 单击筛选图标 (⛛)，然后在调用的菜单中指定并应用筛选条件。

  > 当您为“**状态**”列应用筛选条件后，表格将显示状态包含所选值的手动启动响应操作，以及状态包含所选值的响应操作所属行动手册。这意味着只会显示符合筛选条件的行动手册的响应操作。

  将显示筛选后的行动手册表。

资源表包含以下各列：

- **操作**。响应操作名称。
- **响应参数**。在行动手册算法中指定的响应操作参数。
- **开始**。启动行动手册或响应操作的日期和时间。
- **结束**。行动手册或响应操作执行完成的日期和时间。
- **警报或事故 ID**。包含指向警报或事故详情的链接的 ID。
- **启动者**。启动行动手册或响应操作的用户的名称。

- **批准者**。批准启动行动手册或响应操作的用户的名称。
  默认情况下，此列处于隐藏状态。要显示此列，请单击设置图标 (⚙)，然后选择“**批准者**”列。
- **审批时间**。用户确认或拒绝启动行动手册或响应操作的日期和时间。
  默认情况下，此列处于隐藏状态。要显示此列，请单击设置图标 (⚙)，然后选择“**审批时间**”列。
- **状态**。行动手册的执行状态。此列可显示以下值：
  - **等待批准** – 行动手册正在等待启动审批。
  - **进行中** – 行动手册正在执行中。
  - **成功** – 行动手册执行完成，无错误或警告。
  - **警告** – 行动手册执行完成，但存在警告。
  - **错误** – 行动手册执行完成，但存在错误。
  - **已终止** – 由于用户中断了执行，行动手册停止执行。
  - **批准时间已过** – 由于审批等待超时，行动手册停止执行。
  - **被拒绝** – 由于用户拒绝了启动，行动手册停止执行。

  单击**状态**，可打开包含行动手册启动结果的窗口。技术支持人员可以使用启动 ID 下载所需分析数据，来排查执行错误。默认情况下，数据会存储 72 小时。
  如果状态为**进行中**，您可以将鼠标光标悬停在状态旁边的图标上查看启动 ID。
- **资产**。行动手册或响应操作所作用的资产数量。您可以单击包含资产数量的链接来查看资产详细信息。如果行动手册或响应操作不涉及资产，则该字段为空。

您也可以从**响应历史**部分，或从警报或事故详情，查看响应历史记录。

终止行动手册

您可以强制终止已启动的行动手册。在这种情况下，未完成的响应操作将被终止。行动手册终止后，已完成的响应操作不会被取消。

要终止行动手册，您必须拥有以下角色之一：主管理员、1 级分析师、2 级分析师、租户管理员。

要终止行动手册：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 在行动手册列表中，执行以下操作之一：
   - 选择所需的行动手册，然后在工具栏中单击“**查看历史**”按钮。
   - 单击所需行动手册的名称，然后在打开的窗口中单击“**查看历史**”按钮。

3. 选择“**查看响应历史**”。

   将打开包含已启动的行动手册实例列表的窗格。

4. 选择要终止的一个或多个实例，然后单击“**终止**”按钮并确认选择。

   行动手册将被终止。

删除行动手册

无法删除预定义行动手册。

要删除自定义行动手册，您必须拥有以下任一角色：主管理员、SOC 管理员、1 级分析师、2 级分析师、租户管理员。

要删除自定义行动手册：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 从列表中选择行动手册，然后单击“**删除**”按钮。
3. 在确认对话框中，单击**删除**。

   如果存在已启动的行动手册实例，则无法删除行动手册。在这种情况下，请终止所有已启动实例，然后再删除行动手册。

如果您删除了处于“**活动**”或“**不可用**”状态的行动手册，则该行动手册将在行动手册表中显示为“**已删除**”状态，且仅支持查看和复制操作。

状态为“**已删除**”的行动手册将被永久删除。

管理行动手册版本

Kaspersky Next XDR Expert会存储行动手册的版本历史记录。创建行动手册或保存对现有行动手册的更改时，会自动创建一个新版本。您只能在行动手册发布后管理其版本。版本管理不适用于行动手册草稿。

新发布的行动手册会被分配一个版本号`1`。每次保存更改时，版本号都会增加1。最新保存的版本会在版本列表中标记为`Current`。

如果您是从Kaspersky Next XDR Expert 2.0版本升级，首次编辑现有行动手册后，系统会自动为其分配一个版本号。现有行动手册的先前版本也会被保存，以便与最新版本进行比较。

比较行动手册版本

Kaspersky Next XDR Expert允许您比较行动手册的不同版本，以跟踪更改并恢复以前的版本。

为此，您必须拥有以下XDR角色之一：主管理员、租户管理员、SOC管理员、一级分析师、二级分析师、SOC经理、审批人、审计员。

若要比较行动手册版本：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 在行动手册列表中，选择要比较版本的行动手册。
3. 单击**查看历史**按钮，然后选择**查看版本历史**。
   此时将打开**行动手册版本历史**窗口。
4. 在行动手册版本列表中，选择两个版本进行比较，然后单击**比较**按钮。
   屏幕上会弹出一个窗口，显示不同行动手册版本之间的差异。请注意，您无法在此窗口中编辑行动手册。
   如有必要，在打开的窗口中，您可以选择不同的行动手册版本进行比较。

对不同版本的行动手册进行比较。

恢复行动手册版本

您可以随时恢复到行动手册的先前版本。

为此，您必须拥有以下XDR角色之一：主管理员、租户管理员、SOC管理员、一级分析师、二级分析师。

若要恢复行动手册版本：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 在行动手册列表中，选择要恢复先前版本的行动手册。
   或者，您可以点击行动手册名称。
3. 单击**查看历史**按钮，然后选择**查看版本历史**。
   此时将打开**行动手册版本历史**窗口。
4. 在行动手册版本列表中，找到要恢复的版本。
   如果要查看所选行动手册版本的详细信息，请单击版本名称。
5. 在**操作**列中，单击**恢复**按钮。

6. 在打开的确认对话框中，单击**恢复**。

   如有必要，您可以添加备注。如果您没有添加注释，则会自动添加，指示恢复行动手册的版本。

先前版本的行动手册随即恢复。

在测试模式下启动行动手册

您可以以测试模式启动行动手册来进行调试或验证结果。在测试运行期间，行动手册会处理选定的警报和事故，但不会对资产执行任何操作。

任何状态的行动手册都可以以测试模式启动。

要在测试模式下启动行动手册，您必须具有以下角色之一：主管理员、一级分析师、二级分析师、租户管理员。

要以测试模式启动行动手册：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 执行以下操作之一：
   - 单击您需要编辑的行动手册名称。在打开的**行动手册详细信息**窗口中，单击“**以测试模式启动**”按钮。
   - 从列表中选择行动手册，然后单击“**以测试模式启动**按钮。

     根据行动手册的范围，将弹出**选择事故**或**选择警报**面板。
3. 在弹出的面板中选择事故或警报。

   如果行动手册需要选择可观察对象和资产，请启用“**在启动行动手册之前选择目标对象**”选项。
4. 点击“**启动**”。

   如果您启用了“**在启动行动手册之前选择目标对象**”选项，则会弹出**目标对象**面板。从“**可观察对象**”和“**资产**”选项卡中选择您要为其启动行动手册的对象，然后单击“**应用并启动**”按钮。
5. 将弹出**“行动手册已在测试模式下启动”**提示。测试运行结束后，将弹出**“行动手册已在测试模式下完成”**提示。点击此弹出窗口中的**“查看结果”**链接，即可显示显示结果的面板。如果测试运行成功，则会弹出“**行动手册成功**”面板。如果测试运行失败，则会弹出**“行动手册错误”**面板。

   运行结果保存在行动手册的“**响应历史**”部分。测试运行结果不会显示在常规响应历史部分中。

启动行动手册和响应操作

启动行动手册

您可以根据需要配置行动手册的启动方式。您可以在创建行动手册时选择以下操作模式之一：

- **自动**。若需自动启动行动手册和响应操作，请选择此操作模式。

  此模式下的行动手册可实现威胁响应自动化，并减少分析警报和事故所需时间。

- **培训**。若需检查行动手册配置是否正确，请选择此操作模式。
  在检测到相应警报或事故时，此模式下的行动手册不会自动启动。相反，行动手册将请求用户批准启动。
- **手动**。若仅需手动启动行动手册，请选择此操作模式。
  此模式下的行动手册无触发条件，您可根据所选行动手册适用范围针对任何警报或事故启动此类行动手册。有关详细信息，请参阅手动启动行动手册。

您也可以更改现有行动手册的操作模式。有关详细信息，请参阅编辑行动手册。

启动响应操作

响应操作可以手动启动、在行动手册中自动启动，或者配置为在行动手册内启动前请求用户批准。默认情况下，响应操作的手动审批处于禁用状态。

有关如何配置行动手册内所启动响应操作的手动审批，请参阅配置响应操作的手动审批。

手动启动行动手册

Kaspersky Next XDR Expert 支持手动启动与您希望响应的警报或事故匹配的任何行动手册。

> 要手动启动行动手册，您必须拥有以下任一角色：主管理员、1 级分析师、2 级分析师、租户管理员。

如果在创建和启动行动手册时指定了可观察对象和资产，您也可以针对可观察对象和资产启动行动手册。

为警报启动行动手册

要为警报设置手动启动行动手册：

1. 在主菜单中，前往**监控→警报**部分。
2. 在警报表中，单击包含希望为其启动行动手册的警报 ID 的链接。
3. 在打开的“**警报详情**”窗口中，单击“**选择行动手册**”按钮。
   将打开**选择行动手册**窗口。
4. 在与该警报匹配的行动手册列表中，选择要启动的行动手册，然后单击“**启动**”按钮。
   如果所选行动手册已针对该警报运行，请在弹出的“**监控**”窗口中执行以下操作之一：
   - 如果希望等待当前行动手册实例完成执行，请单击“**等待并启动**”按钮。
     新的行动手册实例将在当前实例完成执行后启动。
   - 如果希望立即启动新的行动手册实例，请单击“**终止并启动新的**”按钮。
     当前行动手册实例将被终止，新的行动手册实例将启动。
   - 如果希望取消启动新的行动手册，请单击“**关闭**”按钮 (×)。

如果选定的行动手册处于“**等待批准**”状态，手动启动后，该行动手册的状态将变更为“**已推出**”。

行动手册针对所选警报进行启动。行动手册执行完成后，您将收到一条通知。

为事故启动行动手册

要为事故手动启动行动手册：

1. 在主菜单中，转到“**监控**” → “**事故**”，然后选择“**XDR 事故**”选项卡。
2. 在事故表中，单击希望为其启动行动手册的事故 ID 的链接。
3. 在打开的“**事故详情**”窗口中，单击“**选择行动手册**”按钮。
   “**选择行动手册**”窗口将打开。
4. 在与该事故匹配的行动手册列表中，选择要启动的行动手册，然后单击“**启动**”按钮。
   如果选定的行动手册已针对此事故运行，请在弹出的“**监控**”窗口中执行以下操作之一：
   - 如果希望等待当前行动手册实例完成执行，请单击“**等待并启动**”按钮。
     新的行动手册实例将在当前实例完成执行后启动。
   - 如果希望立即启动新的行动手册实例，请单击“**终止并启动新的**”按钮。
     当前行动手册实例将被终止，新的行动手册实例将启动。
   - 如果希望取消启动新的行动手册，请单击“**关闭**”按钮 (✕)。

如果选定的行动手册处于“**等待批准**”状态，手动启动后，该行动手册的状态将变更为“**已推出**”。

行动手册将针对所选事故进行启动。行动手册执行完成后，您将收到一条通知。

为用户指定的对象启动行动手册

您可以指定必须为其运行行动手册的可观察对象和资产。您必须使用以下设置创建行动手册：

- 在“**范围**”列表中，选择“**警报**”或“**事故**”。
- 在“**操作模式**”列表中，选择“**手动**”。
- 在可视化编辑器的工作区中，在可视化编辑器中配置行动手册执行步骤时，使用 jq 表达式指定要为其启动行动手册的对象（可观察对象或资产）。这些对象将作为行动手册启动时的输入。

如果您未在行动手册算法中指定对象，而仅在启动行动手册之前选择了对象，则这些对象会被忽略。

创建行动手册后，您可以为选定的对象启动行动手册。

为此，您必须拥有以下 XDR 角色之一：主管理员、1 级分析师、2 级分析师或租户管理员。

要为选定的对象启动行动手册：

1. 在主菜单中，转到“**监控**”部分，然后在“**警报**”或“**事故**”部分中，单击要从中启动行动手册的警报或事故的 ID。
2. 在打开的详情窗口中，单击“**选择行动手册**”按钮。
   “**选择行动手册**”窗口将打开。
3. 选择“**启动行动手册前选择目标对象**”选项，然后单击“**启动**”按钮。
4. 在打开的“**目标对象**”窗口中，从“**可观察对象**”和“**资产**”选项卡中选择您要为其启动行动手册的对象，然后单击“**应用并启动**”按钮。
   将针对您选择的对象启动该行动手册。

您可以通过以下途径查看行动手册执行结果：进入警报或事故详情中的“**历史记录**”选项卡；通过单击“**查看历史**”按钮进入“行动手册详情”或“行动手册表”；进入“响应历史记录”部分。

例如，您编写了一个在 executeCustomScript 响应操作期间调用的脚本。创建行动手册时，您可以在可视化编辑器工作区中，添加“**运行自定义脚本**”执行步骤，并传入行动手册输入数据。然后，您必须针对启动行动手册时选择的 IP 类型的可观察对象运行该脚本。该脚本使用您选择的 IP 地址作为参数：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "executeCustomScript",
                    "params": {
                        "commandLine": "./script.py",
                        "commandLineParameters": "${ \"-ip \" + ([.input.observables[] | select(.type == \"ip\")]
| map(.value) | join(\",\")) }",
                        "workingDirectory": "/folder/with/script"
                    }
                },
                "onError": "stop"
            }
        },
      {
        "action": {
          "function": {
            "type": "updateBases",
            "params": {
              "wait": false
            },
            "assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
          }
        }
      }
    ]
}
```

多个对象将作为行动手册的输入，且以逗号分隔的 IP 地址列表必须作为脚本的输入：

```
{
    "input": {
        "observables": [
            {
```

```
                "type": "ip",
                "value": "127.0.0.1"
            },
            {
                "type": "ip",
                "value": "127.0.0.2"
            },
            {
                "type": "md5",
                "value": "29f975b01f762f1a6d2fe1b33b8e3e6e"
            }
        ],
        "assets":[
    {
        "AttackerOrVictim": "unknown",
        "ID": "c13a6983-0c40-4986-ab30-e85e49f98114",
        "InternalID": "6d831b04-00c2-44f4-b9e3-f7a720643fb7",
        "KSCServer": "E5DE6B73D962B18E849DC0BF5A2BA72D",
        "Name": "VIM-W10-64-01",
        "Type": "host"
    }
  ]
}
```


jq 表达式对行动手册操作数据进行计算后，以下信息将作为命令行参数传递：

```
-ip 127.0.0.1,127.0.0.2
```

对于需要输入数据的行动手册，如果您在创建行动手册和启动行动手册时指定了不同类型的对象，或者如果您没有选择“**在启动行动手册之前选择目标对象**”选项，行动手册的执行将以下列其中一种结果结束：

- 由于行动手册未收到输入数据，因此将发生错误。
- 操作将不会执行，因为行动手册包含基于输入数据的条件或循环。
- 结果将取决于执行操作的应用程序、服务或脚本的响应。

以“训练”操作模式启动行动手册

“**培训**”操作模式允许您检查行动手册是否配置正确。如果您打算将行动手册操作模式更改为“**自动**”，这将非常有用。

“**培训**”操作模式下的所有行动手册都需要用户批准才能启动。

要在“**培训**”操作模式下启动行动手册，您必须具有以下角色之一：主管理员、1 级分析师、2 级分析师、租户管理员。

在“**培训**”操作模式下，行动手册由警报或事故触发，但在启动前需要手动审批。您可以通过以下方式之一在“**培训**”操作模式下测试行动手册的启动：

- 创建与行动手册触发器匹配的警报或事故。
- 编辑与行动手册触发器匹配的警报或事故。警报或事故必须处于除“**已关闭**”之外的状态。

仅当触发器设置为响应手动更改时，编辑警报或事故才会触发行动手册。默认情况下，手动更改警报或事故将被忽略。为了使行动手册能够响应手动更改，触发器必须使用`event.manual`函数。有关详细信息，请参阅行动手册触发器。

完成上述操作之一后，行动手册将请求用户批准启动。有关如何批准行动手册的更多信息，请参阅“批准行动手册或响应操作”。

启动行动手册的手动审批时间限制为 60 分钟。

配置响应操作的手动审批

Kaspersky Next XDR Expert 支持为自定义行动手册中启动的响应操作配置手动审批。默认情况下，响应操作的手动审批处于禁用状态。

在配置手动审批之前，请确保已配置租户的电子邮件通知并指定了审批人的电子邮件地址。

建议为以下响应操作配置手动审批：将设备移动到另一个管理组、将文件移动到隔离区、启用和禁用网络隔离、通过 Active Directory 对账户执行响应操作，以及数据增强。

要配置响应操作的手动审批：

1. 在主菜单中，转到“**监控**” → “**行动手册**”。
2. 通过执行以下操作之一，打开行动手册进行编辑：
   - 单击您需要编辑的行动手册名称。在打开的**行动手册详情**窗口中，单击“**编辑**”按钮。
   - 从列表中选择行动手册，然后单击“**编辑**”按钮。
     如果您选择了多个行动手册，“**编辑**”按钮将被禁用。

   将打开“**编辑行动手册**”窗口。
3. 在“**算法**”部分，为需要启用手动审批的响应操作指定以下参数之一：
   - 要为响应操作启用带有默认审批时间的手动审批，请指定以下参数：

     ```
     "manualApprove": true
     ```

     默认情况下，审批时间为 60 分钟。

- 要为响应操作启用带有可调整审批时间的手动审批，请指定以下参数：

```
"manualApprove": {"timeout": "period"}
```

其中“周期”是可调整的审批时间。

支持以小时 (h) 和/或分钟 (m) 为单位配置审批时间，例如：

```
"manualApprove": {"timeout": "20h"}
"manualApprove": {"timeout": "2h30m"}
```

- 要启用响应操作的手动审批，并将通知发送到审批人的电子邮件地址，请指定以下参数：

```
"emailNotifications": {
 "enabled":true
}
```

- 要启用响应操作的手动审批，并在一定时间后向审批人的电子邮件地址发送通知，请指定以下参数：

```
"manualApprove": {
  "emailNotifications": {
    "enabled": true,
    "delay": "period"
  }
```

其中“周期”是可调整的发送时间。

您可以配置发送时间（以分钟 (m) 为单位），例如：

```
"delay": "20m"
```

4. 单击“**保存**”按钮。

已配置响应操作的手动审批。包含审批响应操作请求的电子邮件通知将被发送到用户账户属性中所指定的电子邮件地址。

您可以在“审批请求**批准请求查看响应操作的审批请求**。

审批行动手册或响应操作

“**培训**”操作模式下的所有行动手册都需要用户批准。您也可以配置手动审批行动手册内启动的响应操作。

要批准或拒绝行动手册启动，您必须拥有以下角色之一：主管理员、1级分析师、2 级分析师、租户管理员。

要批准或拒绝响应操作启动，您必须拥有以下角色之一：主管理员、批准人、租户管理员。

如果有任何行动手册或响应操作正在等待用户批准，OSMP 控制台上部会显示通知。此外，如果响应操作启动需要用户批准，则会在行动手册算法指定的时间段内向电子邮件地址发送电子邮件通知。

查看行动手册和响应操作的列表

要查看等待批准的行动手册和响应操作列表，请执行以下操作之一：

- 单击 OSMP 控制台上部的**查看批准请求**链接。
- 按照发送至您电子邮件地址的通知中的链接操作。

包含完整批准请求列表表格的“**批准请求**”窗格将打开。

批准请求表包含以下列：

- **时间**。行动手册或响应操作请求用户批准的日期和时间。
- **批准截止日期**。用户必须批准或拒绝行动手册或响应操作的截止日期和时间。如果用户在截止时间之前未批准行动手册或响应操作，则启动将被取消。
- **行动手册**。请求用户批准的自定义或预定义行动手册的名称。
- **响应操作**。在行动手册内启动的操作。
- **资产**。行动手册或响应操作所作用的资产数量。您可以通过单击包含资产数量的链接来查看请求用户批准的资产列表。
- **响应参数**。在响应操作或行动手册算法中指定的响应操作参数。
- **警报或事故 ID**。包含指向警报或事故详细信息的链接的 ID。

批准和拒绝行动手册

要批准或拒绝行动手册：

1. 在 OSMP 控制台顶部的通知中，单击“**查看批准请求**”链接。

   > 仅当存在等待用户批准的行动手册时，才会显示带有“**查看批准请求**”链接的通知。

2. 在打开的“**批准请求**”窗格中，选择一个或多个行动手册，然后执行以下操作之一：
   - 要批准行动手册启动，请单击“**批准**”按钮。
     之后，行动手册将被启动。“**响应历史**”部分中的操作状态将变更为“**进行中**”。
   - 要拒绝行动手册启动，请单击“**拒绝**”按钮。
     完成操作后，行动手册的启动将被取消。“**响应历史**”部分中的操作状态将变更为“**被拒绝**”。
3. 单击“**关闭**”按钮（✕）以关闭“**批准请求**”窗格。

批准或拒绝行动手册后，您可以在“**响应历史**”部分查看其状态。

批准和拒绝响应操作

要批准或拒绝响应操作：

1. 在 OSMP 控制台顶部的通知中，单击“**查看批准请求**”链接。

   仅当有响应操作等待用户批准时，才会显示带有“**查看批准请求**”链接的通知。

   将打开“**批准请求**”窗格。

2. 在打开的“**批准请求**”窗格中，在“**资产**”列中单击带有资产数量的链接。
   将打开包含完整资产列表的“**要批准的资产**”窗格。

3. 检查需要手动审批的资产列表，然后执行以下操作之一：

   - 要批准启动资产的响应操作，请选择您需要的一个或多个资产，然后单击“**批准**”按钮。完成操作后，将为选定资产启动响应操作。
   - 要拒绝启动资产的响应操作，请选择一个或多个目标资产，然后单击“**拒绝**”按钮。完成操作后，将取消选定资产的响应操作启动。

4. 单击“**关闭**”按钮（×）以关闭“**要批准的资产**”窗格。

5. 单击“**关闭**”按钮（×）以关闭“**批准请求**”窗格。

批准或拒绝响应操作后，您可以在“**响应历史**”部分查看其状态。

通过行动手册进行数据增强

配置 Kaspersky Next XDR Expert 与 Kaspersky TIP 之间的集成后，您可以从 Kaspersky TIP 或 Kaspersky OpenTIP 获取与警报或事故相关的可观察对象的信誉信息，然后增强所获取的数据。

您只能获取具有以下类型的可观察对象的信息：域、URL、IP、MD5、SHA256。

您可以将数据增强功能配置为自动运行。为此，在创建或编辑行动手册时，您必须在可视化编辑器工作区中添加“在可视化编辑器中配置行动手册执行步骤”，并指定以下内容：

1. 如有必要，可以指定 Kaspersky TIP 或 Kaspersky OpenTIP 返回数据的限制条件。
   您可以指定下列值之一：

   - 所有记录
   - Top100

     默认设置此值。

2. 行动手册从 Kaspersky TIP 或 Kaspersky OpenTIP 请求数据的可观察对象。

> 数据增强通过使用与卡巴斯基威胁情报门户集成中指定的服务来执行。

在行动手册算法中，您可以使用 Kaspersky TIP 返回的字段中显示的输出数据增强参数。

您可以通过以下方式之一查看与警报或事故相关的所有可观察对象的数据增强结果：

- 从警报或事故详情操作
- 从响应历史记录
- 从行动手册中

要查看数据增强结果：

1. 在主菜单中，转到“**监控**”，然后执行以下操作之一：
   - 如果要查看警报或事故详情的结果，请转到“**警报**”或“**事故**”部分，然后单击已执行数据增强的警报或事故的 ID。在打开的窗口中，转到“**历史记录**”选项卡，然后选择“**响应历史记录**”选项卡。
   - 如果要查看响应历史记录的结果，请转到“**响应历史**”部分。
   - 如果要查看行动手册表的结果，请转到“**行动手册**”部分，然后执行以下操作之一：
     - 选择执行了数据增强的行动手册。在工具栏中，单击“**查看历史**”按钮，然后选择“**查看响应历史**”。
     - 单击执行了数据增强的行动手册名称。在打开的窗口中，单击“**查看历史**”按钮，然后选择“**查看响应历史**”。
2. 在“**操作状态**”列中，单击要查看数据增强结果的行动手册的状态。

您还可以从 Kaspersky TIP 获取信息，然后在警报或事故详情的“**可观察对象**”选项卡上手动增强数据。

查看响应历史记录

您可以在**响应历史**部分中查看有关所有检测到的警报和事故的详细响应历史记录。请注意，如果警报或事故已被删除，则该警报或事故的响应历史记录将不会显示。

> 要查看响应历史记录，您必须拥有以下任一角色：主管理员、1 级分析师、2 级分析师、SOC 经理、初级分析师、审批人、审计员、租户管理员。

要查看响应历史记录，请在主菜单中，转到**监控 → 响应历史**。将打开包含所有警报和事故的响应历史记录的表格。

默认情况下，表格将根据启动行动手册或响应操作的时间排序。行动手册中的响应操作将根据其在行动手册算法中的顺序排序。

您可以按照下述方法，使用表格上部的工具栏对表格中的数据进行分组和筛选：

- 单击设置图标 (⚙)，然后选择要在表中显示的列。
- 单击筛选图标 (⛛)，然后在调用的菜单中指定并应用筛选条件。

> 为“**操作状态**”列应用筛选条件后，表格将显示状态包含所选值的手动启动响应操作，以及状态包含所选值的响应操作所属行动手册。这意味着只会显示符合筛选条件的行动手册的响应操作。

表格搜索适用于除“**操作状态**”和“**行动手册状态**”之外的所有列。要对这些列中的数据进行筛选，请单击列标题并从下拉列表中选择所需状态。

资源表包含以下各列：

- **操作**。响应操作或行动手册名称。
- **响应参数**。在响应操作或行动手册算法中指定的响应操作参数。
- **开始**。启动行动手册或响应操作的日期和时间。
- **结束**。行动手册或响应操作执行完成的日期和时间。
- **警报或事故 ID**。包含指向警报或事故详细信息的链接的 ID。
- **启动者**。启动行动手册或响应操作的用户的名称。
- **操作状态**。响应操作的执行状态。此列可显示以下值：
  - **等待批准** – 响应操作正在等待启动审批。
  - **进行中** – 响应操作正在执行中。
  - **成功** – 响应操作执行完成，无错误或警告。
  - **警告** – 响应操作已完成，但存在警告。
  - **错误** – 响应操作已完成，但存在错误。
  - **已终止** – 由于用户中断了执行，响应操作停止执行。
  - **批准时间已过** – 由于审批等待超时，响应操作停止执行。
  - **被拒绝**– 由于用户拒绝了启动，响应操作停止执行。

> 已启用网络隔离的设备可能会在隔离过程完成之前收到**成功**状态。

- **行动手册状态**。行动手册的执行状态。此列可显示以下值：
  - **等待批准** – 行动手册正在等待启动审批。
  - **进行中** – 行动手册正在执行中。

- **成功** – 行动手册执行完成，无错误或警告。
- **警告** – 行动手册执行完成，但存在警告。
- **错误** – 行动手册执行完成，但存在错误。
- **已终止** – 由于用户中断了执行，行动手册停止执行。
- **批准时间已过** – 由于审批等待超时，行动手册停止执行。
- **被拒绝** – 由于用户拒绝了启动，行动手册停止执行。

单击“**行动手册状态**”值或“**操作状态**”值，即可打开包含行动手册或响应操作启动结果的窗口。若执行过程中出现错误，技术支持人员可借助“**调试数据**”选项卡中显示的启动 ID，下载分析所需的相关数据。默认情况下，数据保存 72 小时。
如果状态为**进行中**，您可以将鼠标光标悬停在状态旁边的图标上查看启动 ID。

- **资产**。行动手册或响应操作所作用的资产数量。您可以单击包含资产数量的链接来查看资产详细信息。如果行动手册或响应操作不涉及资产，则该字段为空。
- **租户**。行动手册所属租户名称。
- **批准者**。批准或拒绝启动行动手册或响应操作的用户名称。
  默认情况下，此列处于隐藏状态。要显示此列，请单击设置图标 (⚙)，然后选择“**批准者**”列。
- **审批时间**。批准或拒绝启动行动手册或响应操作的日期和时间。默认情况下，此列不显示。
  默认情况下，此列处于隐藏状态。要显示此列，请单击设置图标 (⚙)，然后选择“**审批时间**”列。

预定义行动手册

Kaspersky Next XDR Expert 提供由卡巴斯基专家创建的现成的预定义行动手册。预定义行动手册基于 KUMA 关联规则。有关分发包中包含的 KUMA 关联规则的更多信息，请参阅“关联规则”。

您可以在“**行动手册**”部分找到预定义行动手册。此类行动手册标有“**预定义**”标签，名称中带有 [KL] 前缀。

请注意，除了“**操作模式**”和“**对已启动的行动手册实例的操作**”字段外，您无法编辑预定义行动手册的参数。如果要编辑预定义行动手册的其他参数，则需要复制该行动手册，然后将其用作模板来创建自定义行动手册。有关详细信息，请参阅“自定义行动手册”。

在使用预定义行动手册之前，您必须在 KUMA 中执行以下操作：

- 当“**源类型**”设置选择为“**事件**”类型时，需配置用于事件数据增强的规则设置。在**目标字段**中指定“**VictimUserID**”和“**AttackerUserID**”的值。
- 在 KUMA 中配置数据增强功能以获取 Windows 事件日志。

无法删除预定义行动手册。

预定义行动手册属于父租户，并由所有子租户继承。

[KL] P001"办公应用程序创建可执行文件"

此行动手册包含"通过 KASAP 响应"这一响应操作，并且只能用作模板。如果要启动行动手册，请单击"**复制和编辑**"按钮。在打开的窗口中，在"**分配 KASAP 组**"操作中，指定 KASAP 组 ID。

在使用行动手册之前，您必须在 KUMA 中配置数据增强功能以获取 Windows 事件日志。

默认情况下，行动手册会为警报中的所有用户启动响应操作。如果您希望行动手册仅针对受影响用户的账户启动响应操作，您可以执行以下操作：

1. 在 KUMA 中，配置数据增强规则设置。针对已将"**事件**"类型选为"**源类型**"设置的事件数据增强功能，请在"**目标字段**"中指定"**受影响用户 ID**"的值。

2. 在"**分配 KASAP 组**"操作中，在"**资产**"字段中指定 `and .IsVictim`，如下所示：

   ```
   [ alert.Assets[] | select(.Type == \"user\" and .IsVictim) | .ID]
   ```

借助 **[KL] P001"办公应用程序创建可执行文件"**预定义行动手册，您可以阻止攻击者使用办公应用程序实施攻击，例如，当用户打开受感染的文档时发起网络钓鱼攻击，随后该文档会创建并执行可执行文件。

触发该行动手册的警报是根据"*办公应用程序创建可执行文件*"关联规则创建的。此规则有助于检测以办公应用程序名义创建带有可疑扩展名的文件（例如脚本和可执行文件）。

行动手册触发器包含以下表达式：

```
[.OriginalEvents[] | .ExternalID == "R350"] | any
```

在执行期间，此行动手册将启动以下响应操作：

1. 通过 Active Directory 响应，然后重置攻击者和受影响用户账户的密码。

   如果在执行响应操作期间发生错误，行动手册会终止运行。

2. 通过 KASAP 响应，然后为账户分配信息安全课程。

   如果在执行响应操作期间发生错误，行动手册将继续运行。

行动手册算法包含以下一系列响应操作：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "resetLDAPPassword",
```

```
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}"
                },
                "onError": "stop"
            }
        },
        {
            "action": {
                "function": {
                    "type": "assignKasapGroup",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}",
                    "params": {
                        "groupId": "SET KASAP GROUP ID"
                    }
                },
                "onError": "continue"
            }
        }
    ]
}
```

[KL] P002"Windows 事件日志已被清除"

默认情况下，此行动手册在"**手动**"操作模式下运行。不建议将此行动手册切换到"**自动**"或"**培训**"操作模式。

在使用行动手册之前，您必须在 KUMA 中执行以下操作：

- 配置事件增强的增强规则设置，其中"源种类"设置选择了"事件类型"。在"**目标字段**"中指定"**攻击者用户** ID"值。
- 在 KUMA 中配置数据增强功能以获取 Windows 事件日志。

[KL] P002"Windows 事件日志已清除"预定义行动手册可用于阻止攻击者清除 Windows 事件日志，因为该日志包含足够的遥测数据，有助于调查攻击者的恶意活动。

触发行动手册的事故包含根据"*Windows 事件日志已清除*"关联规则创建的一个或多个警报。此规则有助于检测 Windows 日志何时通过 wevutil 实用程序、用户界面或 PowerShell 命令被清除或删除。要启用事故的创建，您必须配置分段规则。

行动手册触发器包含以下表达式：

```
[.Alerts[] | .OriginalEvents[] | .ExternalID  == "R050"] | any
```

在执行期间，此行动手册启动"通过 Active Directory 响应"这一响应操作，然后阻止攻击者的账户。

如果在执行响应操作期间发生错误，行动手册会终止运行。

如果事故中的一个或多个警报由另一个关联规则生成，则行动手册不适用于这些警报。

行动手册算法包含以下一系列响应操作：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "blockLDAPAccount",
                    "assets": "${{ incident.Alerts[] | select(.OriginalEvents[] | .ExternalID == \"R050\") |
.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
                },
                "onError": "stop"
            }
        }
    ]
}
```

[KL] P003“来自 wmiprvse.exe 的可疑子进程”

在使用行动手册之前，您必须在 KUMA 中执行以下操作：

- 配置事件增强的增强规则设置，其中“源种类”设置选择了“事件类型”。在“**目标字段**”中指定“**攻击者用户** ID”值。
- 在 KUMA 中配置数据增强功能以获取 Windows 事件日志。

[KL] P003“来自 wmiprvse.exe 的可疑子进程”预定义行动手册可用于检测异常且必须视为可疑的父进程和子进程对。

触发行动手册的警报是根据“*R297_来自 wmiprvse.exe 的可疑子进程*”关联规则创建的。此规则有助于检测以 wmiprvse.exe 名义启动的可疑进程。

行动手册触发器包含以下表达式：

```
[.OriginalEvents[] | .ExternalID  == "R297"] | any
```

在执行期间，此行动手册将启动以下响应操作：

1. 通过 Active Directory 响应，然后阻止攻击者的账户。
2. 终止在警报中注册的设备上的进程。
3. 运行恶意软件扫描，然后对检测到警报的设备执行全盘扫描。

> 默认情况下，不会扫描网络驱动器，以避免系统过载。若要扫描网络驱动器，则必须复制此行动手册，然后在**运行恶意软件扫描**操作中，开启**扫描网络驱动器**切换开关，或在代码编辑器中将`allowScanNetworkDrives`参数设置为`true`。

行动手册算法包含以下一系列响应操作：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
```

```
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "blockLDAPAccount",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
                },
                "onError": "stop"
            }
        },
        {
            "loop": {
                "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and
.DestinationProcessName != \"\")][] | .DestinationProcessName] }",
                "onError": "stop",
                "steps": [
                    {
                        "action": {
                            "function": {
                                "type": "killProcess",
                                "params": {
                                    "path": "${ .[0] }"
                                },
                                "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
                            }
                        }
                    }
                ]
            }
        },
        {
            "action": {
                "function": {
                    "type": "avScan",
                    "params": {
                        "scope": {
                            "area": "full",
                            "allowScanNetworkDrives": false
                        },
                        "wait": false
                    },
                    "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
                },
                "onError": "stop"
            }
        }
    ]
}
```

如果在执行任何响应操作期间发生错误，则行动手册将终止。

[KL] P004 “沙盒中等检测”

[KL] P004 “沙盒中等检测”预定义行动手册创建一条规则，以阻止在分析期间由沙盒组件分配的警报**中**严重等级的文件的执行。

行动手册触发器包含以下表达式：

```
"event.new and .Severity == \"medium\" and any(.DetectionTechnologies[] == \"SB\"; .)"
```

行动手册使用的 ResponseFunction： `addFilePreventionRules`。

在执行期间，此行动手册使用添加阻止规则响应操作。

行动手册算法包含以下一系列响应操作：


```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "addFilePreventionRules",
          "assets":[
            "selector": "execution-tenant"
          },
          "params": {
            "files": "${[alert.ScannedFiles[] | select(any(.DetectionTechnologies[] == \"SB\"; .)) | .Hashes |
map(.Value)] | flatten}",
            "notify": true
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```


[KL] P005 “沙盒高等检测”

[KL] P005 “沙箱高等检测”预定义行动手册会创建一个规则，以阻止在分析期间由沙箱组件分配的警报**高**严重等级的文件的执行。

行动手册触发器包含以下表达式：

```
"event.new and .Severity == \"high\" and any(.DetectionTechnologies[] == \"SB\"; .)"
```

行动手册使用的 ResponseFunction： `addFilePreventionRules`。

在执行期间，此行动手册使用添加阻止规则响应操作。

行动手册算法包含以下一系列响应操作：


```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "addFilePreventionRules",
          "assets":[
            "selector": "execution-tenant"
          },
          "params": {
            "files": "${[alert.ScannedFiles[] | select(any(.DetectionTechnologies[] == \"SB\"; .)) | .Hashes |
map(.Value)] | flatten}",
            "notify": true
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

[KL] “检查外部IP地址的行动手册”

[KL] 检查外部IP地址的行动手册的预定义行动手册在检测到与外部IP地址的连接时被触发，并启动TIP增强进程。如果增强结果显示威胁评分高于80，则会请求“主机”类型资产的取证数据（进程列表），并启用网络隔离。

关于行动手册的其他信息：

- 要使行动手册正常运行，必须配置Kaspersky TIP集成；
- 要执行帐户锁定操作，需要与Active Directory集成；
- 如果增强结果表明威胁得分低于80，则终止执行行动手册；
- 如果在执行过程中任何步骤发生错误，将停止执行行动手册；
- “启用网络隔离”操作需要在行动手册执行期间进行手动批准。

行动手册触发器包含以下表达式：

```
"event.new and ([ .Alerts[] | .Observables[] | select(.Value | test("^(10\\.|172\\.(1[6-9]|2[0-9]|3[01])\\.|192\\.168\\.|127\\.)") | not) | .Value ] | length > 0)"
```

行动手册使用的 ResponseFunction：`iocsEnrichment, getForensics, netIsolateOn`。

行动手册算法包含以下一系列响应操作：


```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "iocsEnrichment",
          "params": {
            "fullEnrichment": true,
            "observables": "${[ incident.Alerts[] | .Observables[] | {\"type\": .Type, \"value\": .Value } | select(.type==\"ip\" and (.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.)\") | not)) ] | unique_by(.value)}"
          }
        },
        "onError": "stop",
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        },
        "output": {
          "filter": "${.}",
          "action": "overwrite"
        }
      }
    },
    {
      "decision": {
        "conditions": [
          {
            "condition": "${\"${([.details.observableData[] | select(.status == \\\"ok\\\" and .ipObservableData.ipGeneralInfo.threatScore > 80)] | length > 0)}\"}",
            "name": "Condition 1",
            "steps": [
              {
                "decision": {
                  "conditions": [
                    {
```

```
                    "condition": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type == \"host\")) |
length > 0}",
                    "name": "alert has host(s)",
                    "steps": [
                      {
                        "action": {
                          "function": {
                            "type": "getForensics",
                            "assets": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type ==
\"host\")) | map(.ID)}",
                            "params": {
                              "processes": {
                                "collect": true
                              },
                              "autoruns": {
                                "collect": false
                              }
                            }
                          },
                          "onError": "stop",
                          "timeout": {
                            "scheduleToCloseTimeout": "24h"
                          }
                        }
                      },
                      {
                        "action": {
                          "function": {
                            "type": "netIsolateOn",
                            "assets": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type ==
\"host\")) | map(.ID)}",
                            "params": {
                              "exclusions": [],
                              "exclusionsConflictBehavior": "replace",
                              "isolationTimeoutSec": 28800
                            }
                          },
                          "onError": "stop",
                          "timeout": {
                            "scheduleToCloseTimeout": "24h"
                          },
                          "manualApprove": {
                            "timeout": "60m",
                            "emailNotifications": {
                              "enabled": true,
                              "delay": "10m"
                            }
                          }
                        }
                      }
                    ]
                  }
                ]
              }
            }
          ]
        }
      ]
    }
  ]
}
```


[KL] “检测到受感染文件时隔离设备的行动手册”

[KL] 用于隔离检测到受感染文件的设备的行动手册的预定义行动手册会在检测到受感染文件后隔离设备。

该行动手册不包含触发器。必须手动启动该行动手册，并且需要用户选择上下文。要执行此行动手册，您必须选中**在启动行动手册之前选择目标对象**复选框，并选择要执行行动手册的事故资产和可观察对象。

对每个选定哈希值类型的可观察对象执行以下操作：

1. 从选定的资产中检索文件。
2. 发送检索到的文件进行扫描。
    - 如果在扫描过程中发生错误，则终止执行行动手册；
    - 如果扫描完成且未检测到威胁，则终止执行行动手册；
    - 如果扫描完成并检测到威胁：
        - 所有选定设备随即启用网络隔离；
        - 租户内的所有设备随即添加基于哈希值的阻止规则。

关于行动手册的其他信息：

- 如果在添加启用网络隔离的阻止规则的步骤中出现错误，将停止执行行动手册；在所有其他情况下，它将继续执行。
- “启用网络隔离”和“添加阻止规则”操作需要在行动手册执行期间进行手动批准。

行动手册使用的 ResponseFunction：`getFile`、`serverScan`、`addCommentToIncident`、`addFilePreventionRules`、`netIsolateOn`。

行动手册算法包含以下一系列响应操作：


```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "decision": {
        "conditions": [
          {
            "condition": "${((.input.assets // []) | length) > 0 and ([.input.observables[] | select(.type ==
\"md5\" or .type == \"sha256\" and .value != null and .value != \"\")] | length) > 0}",
            "name": "has input data",
            "steps": [
              {
                "loop": {
                  "input": "${[(.input.observables | map(select(.type == \"md5\" or .type == \"sha256\") |
select(.value != null and .value != \"\") | .value))[] as $hash | [incident.Alerts[] | .Observables[]? |
select((.Type == \"md5\" or .Type == \"sha256\") and .Value == $hash and .Details != \"\")][0] | {\"path\":
.Details,\"hash\":.Value}]}",
                  "steps": [
                    {
                      "decision": {
                        "conditions": [
                          {
                            "condition": "${.[0].path? | length > 0}",
                            "name": "hash with path",
                            "steps": [
                              {
                                "updateData": {
                                  "action": "merge",
                                  "filter": "${.[0]}"
                                }
                              },
                              {
                                "action": {
                                  "function": {
                                    "type": "getFile",
                                    "asset": "${([incident.Alerts[] | .Assets[]? | select(.Type == \"host\")]
[0].ID // (.assets[0] // \"\"))}",
```

```
                                    "params": {
                                      "path": "${.path}"
                                    }
                                  },
                                  "onError": "continue",
                                  "timeout": {
                                    "scheduleToCloseTimeout": "24h"
                                  },
                                  "output": {
                                    "action": "merge",
                                    "filter": "${{\"fileID\": (.details[0].details.file.id // null),
\"scanResult\": null}}"
                                  }
                                }
                              },
                              {
                                "decision": {
                                  "conditions": [
                                    {
                                      "condition": "${.fileID != null and .fileID != \"\"}",
                                      "name": "fileID exists",
                                      "steps": [
                                        {
                                          "action": {
                                            "function": {
                                              "type": "serverScan",
                                              "params": {
                                                "file": {
                                                  "id": "${.fileID}"
                                                }
                                              }
                                            },
                                            "onError": "continue",
                                            "timeout": {
                                              "scheduleToCloseTimeout": "24h"
                                            },
                                            "output": {
                                              "action": "merge",
                                              "filter": "${{\"scanResult\": .}}"
                                            }
                                          }
                                        },
                                        {
                                          "decision": {
                                            "conditions": [
                                              {
                                                "condition": "${.scanResult != null and (.scanResult.resultCode ==
\"error\" or .scanResult.resultCode == null)}",
                                                "name": "scan error",
                                                "steps": [
                                                  {
                                                    "action": {
                                                      "function": {
                                                        "type": "addCommentToIncident",
                                                        "params": {
                                                          "text": "${\"[DEBUG scan ERROR] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \" | errorCode: \" +
(.scanResult.result.errorCode // \"null\") + \" | internalCode: \" + (.scanResult.result.internalCode // \"null\")
+ \"\\noriginalError: \" + (.scanResult.result.originalError // \"null\")}"
                                                        }
                                                      },
                                                      "onError": "continue",
                                                      "timeout": {
                                                        "scheduleToCloseTimeout": "24h"
                                                      }
                                                    }
                                                  }
                                                ]
                                              },
                                              {
                                                "condition": "${.scanResult != null and .scanResult.resultCode ==
\"success\"}",
                                                "name": "scan success",
                                                "steps": [
                                                  {
                                                    "action": {
                                                      "function": {
                                                        "type": "addCommentToIncident",
                                                        "params": {
                                                          "text": "${\"[DEBUG scan] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \"\\nresult: \" + ({\"fileID\": .fileID,
\"resultCode\": .scanResult.resultCode, \"technologies\": .scanResult.details.scanResult.technologies} |
```

```
tostring)}"
                                                    }
                                                  },
                                                  "onError": "continue",
                                                  "timeout": {
                                                    "scheduleToCloseTimeout": "24h"
                                                  }
                                                }
                                              },
                                              {
                                                "decision": {
                                                  "conditions": [
                                                    {
                                                      "condition":
"${[.scanResult.details.scanResult.technologies[] | .result] | contains([\"Infected\"])}",
                                                      "name": "infected",
                                                      "steps": [
                                                        {
                                                            "action": {
                                                                "function": {
                                                                  "type": "addFilePreventionRules",
                                                                  "assets":[
                                                                    "selector": "execution-tenant"
                                                                  },
                                                                  "params": {
                                                                    "files": "${[.hash]}"
                                                                  }
                                                                },
                                                                "onError": "stop",
                                                                "timeout": {
                                                                  "scheduleToCloseTimeout": "24h"
                                                                },
                                                                "manualApprove": true
                                                            }
                                                        },
                                                        {
                                                          "updateData": {
                                                            "action": "overwrite",
                                                            "filter": "${{\"isInfected\": true}}"
                                                          }
                                                        }
                                                      ]
                                                    }
                                                  ]
                                                }
                                              }
                                            ]
                                          }
                                        ]
                                      }
                                    ]
                                  }
                                ]
                              }
                            ]
                          }
                        ]
                      }
                    ]
                  }
                ],
                "onError": "continue",
                "batchSize": 1,
                "aggregate": "${.}",
                "output": {
                  "filter": "${{\"scanResult\": .}}"
                }
              }
            },
            {
              "decision": {
                "conditions": [
                  {
                    "condition": "${.scanResult | map(.isInfected) | any}",
                    "name": "isInfected",
                    "steps": [
                      {
                        "action": {
                          "function": {
                            "type": "netIsolateOn",
                            "assets": "${.input.assets | map(select(.Type == \"host\") | .ID)}",
```

```
                        "params": {
                          "exclusions": [],
                          "exclusionsConflictBehavior": "replace",
                          "isolationTimeoutSec": 28800
                        }
                      },
                      "onError": "stop",
                      "timeout": {
                        "scheduleToCloseTimeout": "24h"
                      }
                    }
                  }
                ]
              }
            ]
          }
        ]
      }
    }
  ]
}
```

[KL][EDR]“删除从告警传输到主机的恶意文件”

[KL][EDR] 删除通过告警传输到主机的恶意文件预定义行动手册旨在自动响应检测到用于向设备投放其他恶意软件的恶意文件这一情况。当检测到与技术 T1105（入口工具传输）相关的活动时，行动手册会从设备中删除此类文件，以防止后续使用。

行动手册的作用域为告警。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any(.S.KL_EventType == "File Modify" and (.FileFullname // "") != "" and ([.SA.KL_IoAAlert,
.SA.KL_IoATechniques] | transpose | any(.[0] and .[1] == "t1105"))))] | any)"
```

行动手册 `deleteFile` 使用的 ResponseFunction。

运行时，行动手册使用**删除文件**响应。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select(.S.KL_EventType == \"File Modify\" and (.FileFullname //
\"\") != \"\" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0] and .[1] == \"t1105\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].FileFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
```

```
              "scheduleToCloseTimeout": "24h"
            }
          }
        }
      ],
      "onError": "continue",
      "batchSize": 1
    }
  }
 ]
}
```

[KL][EDR]“删除从事故传输到主机的恶意文件”

[KL][EDR] 删除从事故传输到主机的恶意文件预定义行动手册旨在自动响应对用于向设备投放其他恶意软件的恶意文件的检测。该行动手册会处理与事故关联的警报；当检测到与技术 T1105（入站工具传输）相关的活动时，行动手册会从设备中删除此类文件，以防止其被进一步使用。

该行动手册的作用域为事故。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .OriginalEvents // [] | select(any(.S.KL_EventType ==
"File Modify" and (.FileFullname // "") != "" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0]
and .[1] == "t1105")))) ] | any)"
```

行动手册 `deleteFile` 使用的 ResponseFunction。

运行时，行动手册使用**删除文件**响应。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select(.S.KL_EventType == \"File Modify\" and
(.FileFullname // \"\") != \"\" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0] and .[1] ==
\"t1105\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].FileFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
```

```
  ]
}
```

[KL][EDR]“当从告警中检测到发现活动时隔离主机”

[KL][EDR] 检测到警报中的发现活动时隔离主机预定义行动手册旨在自动响应涉及收集设备及其环境相关信息的活动。如果检测到此类活动，行动手册会为设备启用网络隔离，以防止攻击者在调查期间继续进行活动。

行动手册的作用域为告警。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.Rules // [] |
select(any(.Name == "Discovery_activity_on_the_host"))] | any)"
```

行动手册 `netIsolateOn` 使用的 ResponseFunction。

运行时，行动手册使用**启用网络隔离**响应。此响应会将设备与网络隔离 8 小时。启用网络隔离需要用户确认。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ alert.Assets[] | select(.Type == \"host\") | .ID] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]“当从事故中检测到发现活动时隔离主机”

[KL][EDR] 从事故中检测到发现活动时隔离主机预定义行动手册旨在自动响应涉及收集设备及其环境信息的活动。该行动手册会处理与事故关联的警报，如果检测到此类活动，则会对设备启用网络隔离，以防止攻击者在调查期间继续活动。

该行动手册的作用域为事故。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .Rules // [] | select(any(.Name ==
"Discovery_activity_on_the_host")) ] | any)"
```

行动手册 `netIsolateOn` 使用的 ResponseFunction。

运行时，行动手册使用**启用网络隔离**响应。此响应会将设备与网络隔离 8 小时。启用网络隔离需要用户确认。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | select(.Rules | any(.Name == \"Discovery_activity_on_the_host\")) |
.Assets[] | select(.Type == \"host\") | .ID] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]“检测到外泄活动时隔离主机”

[KL][EDR] 检测到数据渗出活动时隔离主机预定义行动手册旨在自动响应从设备进行未经授权的数据传输以及连接到攻击者的命令与控制 (C2) 基础设施的尝试。该行动手册会处理与事故关联的警报。如果检测到此类活动，它会对设备启用网络隔离，以防止进一步传输数据和开展恶意活动。

该行动手册的作用域为事故。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert,
.SA.KL_IoAName] | transpose | map(select(.[0]) | .[1]) | any(. as $v | ["not_standard_directory_archive",
"compress_data_for_exfiltration_via_archive"] | index($v)) and any(. as $v | ["lolc2_connection_activity_network",
"lolc2_connection_activity_dns", "network_connection_to_cloud_storage_win"] | index($v)))) ] | any)"
```

行动手册 `netIsolateOn` 使用的 ResponseFunction。

运行时，行动手册使用**启用网络隔离**响应。此响应会将设备与网络隔离 8 小时。启用网络隔离需要用户确认。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | map(select(.[0]) | .[1]) | any(. as $v | [\"not_standard_directory_archive\",
\"compress_data_for_exfiltration_via_archive\"] | index($v)) and any(. as $v |
[\"lolc2_connection_activity_network\", \"lolc2_connection_activity_dns\",
\"network_connection_to_cloud_storage_win\"] | index($v))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]“当从告警中检测到反向 Shell 活动时隔离主机”

[KL][EDR] 从警报中检测到反向 shell 活动时隔离主机预定义行动手册旨在自动响应设备上出现的反向 shell 使用迹象。检测到此类活动时，行动手册会为设备启用网络隔离，以防止攻击者远程控制该设备。

行动手册的作用域为告警。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and
(["invoke_golang_reverse_shell", "invoke_lua_reverse_shell", "invoke_netcat_reverse_or_bind_shell",
"invoke_perl_reverse_shell", "invoke_php_reverse_shell", "invoke_reverse_shell_via_curl"] | index($ioaname))))) ]
| any)"
```

行动手册 `netIsolateOn` 使用的 ResponseFunction。

运行时，行动手册使用**启用网络隔离**响应。此响应会将设备与网络隔离 8 小时。启用网络隔离需要用户确认。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ alert.OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1]
as $ioaname | .[0] and ([\"invoke_golang_reverse_shell\", \"invoke_lua_reverse_shell\",
```

```
\"invoke_netcat_reverse_or_bind_shell\", \"invoke_perl_reverse_shell\", \"invoke_php_reverse_shell\",
\"invoke_reverse_shell_via_curl\"] | index($ioaname)))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]“当从事故中检测到反向 Shell 活动时隔离主机”

[KL][EDR] 当检测到事故中的反向 Shell 活动时隔离主机预定义行动手册旨在自动响应设备上出现的反向 Shell 使用迹象。行动手册会处理与事故关联的警报；如果检测到此类活动，行动手册将为设备启用网络隔离，以防止攻击者远程控制设备。

该行动手册的作用域为事故。

行动手册触发器包含以下表达式：

"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . == "incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and (["invoke_golang_reverse_shell", "invoke_lua_reverse_shell", "invoke_netcat_reverse_or_bind_shell", "invoke_perl_reverse_shell", "invoke_php_reverse_shell", "invoke_reverse_shell_via_curl"] | index($ioaname)))))] | any)"

行动手册 `netIsolateOn` 使用的 ResponseFunction。

运行时，行动手册使用**启用网络隔离**响应。此响应会将设备与网络隔离 8 小时。启用网络隔离需要用户确认。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | any(.[1] as $ioaname | .[0] and ([\"invoke_golang_reverse_shell\", \"invoke_lua_reverse_shell\",
\"invoke_netcat_reverse_or_bind_shell\", \"invoke_perl_reverse_shell\", \"invoke_php_reverse_shell\",
\"invoke_reverse_shell_via_curl\"] | index($ioaname)))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
```

```
  ]
}
```

[KL][EDR]“从告警中缓解电子邮件附件引发的恶意活动”

[KL][EDR] 根据警报缓解电子邮件附件中的恶意活动预定义行动手册旨在自动响应与通过电子邮件接收的文件相关的恶意活动。如果在设备上检测到此类活动，行动手册将终止与恶意文件关联的进程，并从设备中删除该文件。

行动手册的作用域为告警。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([ .OriginalEvents // [] | select(any(. as $event | $event.SA.KL_IoAName | index("mail_utility_threatdetect") as $idx | if $idx != null then $event.SA.KL_IoAAlert[$idx] else false end)) ] | any)"
```

行动手册使用的 ResponseFunction：`killProcess`、`deleteFile`。

执行期间，行动手册使用以下响应：

- 终止进程

  > 如果无法终止进程，行动手册将继续执行。

- 删除文件

警报中的事件可能涉及不同的设备和恶意文件。行动手册会针对每个匹配事件分别触发响应。如果警报中没有匹配事件，行动手册将停止执行。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select((.FileName == \"OUTLOOK.exe\" or .ParentFileName == \"OUTLOOK.exe\") and .ThreatObjectType == \"file\" and (.ThreatObjectFullname | test(\"\\\\w\\\\:\\\\\\\\\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
```

```
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        }
      ],
      "onError": "continue",
      "batchSize": 1
    }
  }
 ]
}
```

[KL][EDR]"从事故中缓解电子邮件附件引发的恶意活动"

[KL][EDR] 缓解事故中电子邮件附件引发的恶意活动预定义行动手册旨在自动响应与通过电子邮件接收的文件相关的恶意活动。该行动手册会处理与事故相关的警报，如果检测到设备上存在恶意活动，则会终止与恶意文件关联的进程，并从设备中删除该文件。

该行动手册的作用域为事故。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .OriginalEvents // [] | select(any(. as $event |
$event.SA.KL_IoAName | index("mail_utility_threatdetect") as $idx | if $idx != null then
$event.SA.KL_IoAAlert[$idx] else false end)) ] | any)"
```

行动手册使用的 ResponseFunction： `killProcess`、`deleteFile`。

执行期间，行动手册使用以下响应：

- 终止进程

  > 如果无法终止进程，行动手册将继续执行。

- 删除文件

警报中的事件可能涉及不同的设备和恶意文件。行动手册会针对每个匹配事件分别触发响应。如果警报中没有匹配事件，行动手册将停止执行。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select((.FileName == \"OUTLOOK.exe\" or
.ParentFileName == \"OUTLOOK.exe\") and .ThreatObjectType == \"file\" and (.ThreatObjectFullname |
```

```
test(\"\\\\w\\\\:\\\\\\\\\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
  }
```

[KL][EDR]“从告警中缓解内存转储活动”

[KL][EDR] 缓解告警中的内存转储活动预定义行动手册旨在自动响应可用于获取凭据和其他敏感信息的内存转储创建活动。如果在设备上检测到此类活动，该行动手册将终止创建内存转储的进程，并删除该进程创建的文件。

行动手册的作用域为告警。

行动手册触发器包含以下表达式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and
(["createdump_lolbin_execution_process", "credentials_dumping_tools_epp",
"credentials_dumping_tools_file_artifacts_creation"] | index($ioaname))))) ] | any)"
```

行动手册使用的 ResponseFunction： `killProcess`、`deleteFile`。

执行期间，行动手册使用以下响应：

- 终止进程

  > 如果无法终止进程，行动手册将继续执行。

- 删除文件

警报中的事件可能涉及不同的设备和恶意文件。行动手册会针对每个匹配事件分别触发响应。如果警报中没有匹配事件，行动手册将停止执行。

行动手册算法包含以下一系列响应操作：


```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any( .[1]
as $ioaname | .[0] and ([\"createdump_lolbin_execution_process\", \"credentials_dumping_tools_epp\",
\"credentials_dumping_tools_file_artifacts_creation\"] | index($ioaname)))) ] }",
        "batchSize": 1,
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue"
      }
    }
  ]
}
```


[KL][EDR]“缓解事故中的内存转储活动”

[KL][EDR] 缓解事故中的内存转储活动预定义行动手册旨在自动响应内存转储的创建，这些内存转储可用于获取凭据和其他敏感信息。该行动手册会处理与事故关联的警报。如果在设备上检测到此类活动，行动手册将终止创建内存转储的进程，并删除该进程创建的文件。

该行动手册的作用域为事故。

行动手册触发器包含以下表达式：


```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert,
.SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and (["createdump_lolbin_execution_process",
```

```
"credentials_dumping_tools_epp", "credentials_dumping_tools_file_artifacts_creation"] | index($ioaname))))) ] |
any)"
```

行动手册使用的 ResponseFunction： `killProcess`、`deleteFile`。

执行期间，行动手册使用以下响应：

- 终止进程

  > 如果无法终止进程，行动手册将继续执行。

- 删除文件

警报中的事件可能涉及不同的设备和恶意文件。行动手册会针对每个匹配事件分别触发响应。如果警报中没有匹配事件，行动手册将停止执行。

行动手册算法包含以下一系列响应操作：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | any(.[1] as $ioaname | .[0] and ([\"createdump_lolbin_execution_process\",
\"credentials_dumping_tools_epp\", \"credentials_dumping_tools_file_artifacts_creation\"] | index($ioaname)))) ]
}",
        "batchSize": 1,
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue"
      }
    }
  ]
}
```

行动手册触发规则

行动手册触发器是一个过滤器，允许您选择必须启动行动手册的警报或事故。过滤器（触发器）会单独应用于每个对象（警报或事故），并采用单个值：`true` 或 `false`。触发器由 jq 语言的表达式组成，用于处理 JSON 格式的结构化数据。有关 jq 表达式的更多信息，请参阅 jq 手册。

在 Kaspersky Next XDR Expert 中，将使用 gojq。它是用 go 语言编写的 jq 的实现，与 jq 有以下区别：

- 以更方便的方式实现数学函数。
- 错误消息清楚地地指示了需要修复查询的位置。
- 整数计算更加精确。
- jq 中运行错误的函数在 gojq 中得到了改进。

有关 gojq 和 jq 之间差异的更多信息，请参阅 GitHub。

如何编写触发器

在创建或编辑行动手册时，您可以在可视化编辑器的“**触发器**”区块中编写触发器。

根据您在创建或编辑行动手册时在“**范围**”列表中选择的选项，将使用警报数据模型或事故数据模型。

> 行动手册触发器中的参数名称必须与数据模型中的相同。请注意，jq 表达式的元素区分大小写。

> 为避免系统过载，不建议在触发器中指定 `OriginalEvents`, `Observables`, `Extra`, 和 `Alerts` 数据。

当您开始编写触发器时，可能会显示以下建议：

- 函数名称。
- 特殊值。
- 根据数据模型指定为对象标识符的字段。

当您开始输入时，会过滤出合适的值并显示在建议列表中。为方便操作，某些建议包含搜索字符串。例如，如果要指定事故类型 ID 或事故状态 ID，则可以通过名称搜索相应的记录，并且该 ID 将在触发器中指定。

> 请注意，标准状态（*新建*和*关闭*）在不同的工作流中具有相同的 ID。这意味着，所有具有指定状态 ID 的事故都会触发该行动手册。要限制行动手册将运行的事故范围，您必须在触发器中指定事故状态 ID 和事故类型。

jq 语言还提供语法高亮和 jq 表达式验证功能。如果触发器包含无效表达式，则无法保存行动手册。

编写触发器时，将使用基本语法规则。

要引用结构属性，必须使用点号“.”并指定属性，例如：

- `.MITRETactics[]`—查看与警报中所有触发的 IOA 规则关联的 MITRE 策略数组。
- `.MITRETactics[0]`—查看 MITRE 策略数组中的第一个元素。

要引用子属性，可以使用竖线（|）或不带竖线的相同组合，例如：

- `.Assignee.Name`—该表达式输出该警报被分配给的用户的名称。
- `.MITRETactics[0].ID` 或 `.MITRETactics[0] | .ID`—该表达式输出第一个 MITRE 策略的 ID。

要获取值，您必须使用以下运算符：==、>、<、>=、<=、!=，例如：

- `.Assignee.Name == "user"`—如果警报已分配给该用户，则该表达式返回 `true`。
- `(.Severity == "high") and (.DetectSource == "KES")`—如果警报严重级别为高且数据源为 Kaspersky Endpoint Security，则该表达式返回 `true`。
- `[ .DetectionTechnologies[] | . == "IOC" ] | any`—如果触发 IOC 检测技术，则该表达式返回 `true`。
- `.DetectionTechnologies | length > 1`—如果触发多个检测技术，则该表达式返回 `true`。

要枚举对象数组中的值，可以使用`any`方法，例如：

- `[.Assets[] | .Name == "W21H2-X64-3160"] | any`—该表达式筛选满足以下条件的警报：`Assets` 数组的任意元素在 `Name` 字段中具有 `W21H2-X64-3160` 值。
- `[.Observables[] | .Value == "127.0.0.1"] | any`—该表达式筛选满足以下条件的警报：`Observables` 数组的任意元素在 `Value` 字段中具有 `127.0.0.1` 值。
- `[.Assets[].ID]`—输出 ID 数组。
- `[.Assets[] | select(.AttackerOrVictim=="attacker") | .ID]`—显示按 `AttackerOrVictim` 字段筛选的资产的 ID 数组。

如果要重用计算结果，可以使用`$`来定义一个变量。例如，表达式 `event.manual != true as $not_manual | [ .DetectionTechnologies[] | . == "IOC" ] | any and $not_manual` 定义并使用 `$not_manual` 变量，该变量包含一个标志，用于指示更改是否为手动更改。

要处理日期，您可以使用以下函数：

- `now`—获取当前 Unix 时间（以秒为单位），例如 `now == 1690541520.537496`。
- `todate`—将当前 Unix 时间转换为日期字符串，例如 `now | todate == "2023-07-28T10:47:36Z".`
- `fromdate`—将日期转换为秒数，例如：
  - `.CreatedAt | split(".")[0] + "Z"`—此命令移除毫秒，并将字符串转换为 2023-07-15T07:49:51Z 格式。
  - `(.CreatedAt | split(".")[0] + "Z") | fromdate == 1689407391`—秒数转换完成。

jq 使用迭代器 – 这是一种接口，可访问集合（例如数组）元素并允许您遍历这些元素。迭代器始终是计算的结果。区别在于迭代器包含的元素数量。在 Kaspersky Next XDR Expert 中，迭代器必须只有一个元素。所有其他情况均视为错误。

要编写正确的触发器，您必须将迭代器括在方括号中（`[ ... ]`）。例如，`.DetectionTechnologies[] == "IOC"` 触发器会导致错误，因为它返回包含两个元素的迭代器。正确的触发器必须具有以下形式：`[ .DetectionTechnologies == "IOC" ] | any`，其中，您首先必须使用 `[]` 将比较结果包装到数组中，然后使用 `any` 方法进行处理；如果数组中至少有一个元素为 `true`，该方法就会返回 `true`。否则，返回`false`。

触发器运行时

当发生以下触发事件之一时，将开始搜索合适的行动手册：

- 创建新的警报/事故。
- 活动警报/事故的任何字段发生更改。
- 创建或修改行动手册时，用户选择了**针对所有匹配的警报或事故启动行动手册。请注意，系统可能会超载**。

支持以下类型的警报更改事件：

- 分配或移除分析师。
- 更改警报状态。
- 更改基本事件。
- 将警报与事故关联或解除关联。
- 更改 `ExternalReference` 字段中的值。

支持以下类型的事故更改事件：

- 分配或移除分析师。
- 更改事故状态。
- 更改基本事件。
- 将警报与事故关联或解除关联。
- 更改事故名称。
- 编辑事故描述
- 更改事故优先级
- 更改 `ExternalReference` 字段中的值。
- 合并事故。

警报/事故结构不包含有关警报/事故变更的任何数据。此数据以附加信息的形式转移。如果您想在行动手册触发器中引用变更，请使用不带参数的事件函数。

默认情况下，对警报或事故详情的手动更改将被忽略。如果您希望行动手册在手动更改时启动，则必须在触发器中使用 `event.manual` 函数，例如：

- `event.manual and ([ event.updateOperations[] | . == "alertReopened" ] | any)`—仅当手动重新打开警报时，触发器才会生效。
- `[ event.updateOperations[] | . == "alertLinkedWithIncidentBySystem" ] | any`—仅当警报自动关联到事故时，触发器才会生效。
- `event.manual != null and (([ event.updateOperations[] | . == "alertChangedToNew" ] | any) | not)`—无论是手动还是自动，只要警报状态更改为 *新建* 以外的任何状态，触发器就会生效。
- `event == null and .Status == "inIncident"`—此触发器适用于所有处于 *事故中* 状态的警报，但仅在行动手册发生更改时生效，而不是警报发生更改时。

如有必要，您可以测试 jq 表达式的示例，应用过滤器，然后在 jq playground 服务中查看结果。

行动手册算法

Kaspersky Next XDR Expert 允许您使用行动手册手动或自动响应警报和事故。对警报或事故做出响应可能不止涉及一项操作，而是包含一整套步骤和参数。这些步骤取决于指定的条件、警报或事故数据以及先前响应操作的结果。

行动手册算法允许您以 JSON 格式指定响应操作的顺序、必要条件以及对目标对象产生的必要影响。行动手册算法步骤按顺序执行。您可以在创建或编辑行动手册时指定行动手册算法。

启动后，行动手册会获取所有警报或事故数据，并将它们放置在全局数据中。行动手册使用以下数据：

- 全局数据

  全局数据在行动手册的任何步骤均可读取。全局数据包含有关触发行动手册启动的警报或事故的信息。

  > 您无法通过使用行动手册或更改警报或事故数据来编辑全局数据。全局数据在行动手册实例的整个生命周期内保持不变。

- 操作数据

  操作数据在行动手册的各步骤之间传输。您可以使用 jq 表达式来管理操作数据，这些表达式在`input`和`output`参数中指定。

- 局部数据

  局部数据仅限于特定步骤内使用。您可以使用`input`（局部数据生成）和`output`（从局部数据生成操作数据）参数来管理局部数据。

如何编写算法

行动手册算法以 JSON 格式编写，主要包含两个部分：

- 行动手册的一般信息：
  - 名称（`name`）
  - 描述（`description`）
  - 范围（`inputType`）
  - 行动手册输入数据的转换（`input`）
  - 行动手册输出数据的转换（`output`）
  - 行动手册执行超时（`playbookRunTimeout`）
  - 可在特定步骤应用的超时策略（`timeouts`）
  - 行动手册版本（`version`）
  - DSL 架构版本（`dslSpecVersion`）
  - 响应操作架构版本（`actionsSpecVersion`）
- 行动手册执行步骤（`executionFlow`）。

编写算法时需提供以下参数：

- `dslSpecVersion`。所需值：1.1.0。
- `actionsSpecVersion`
- `version`
- `executionFlow`（至少一个执行步骤）

> 每个执行步骤都有特定的必填字段。

如果未填写必填字段就尝试保存行动手册，系统会报错。

行动手册算法区分大小写。要使用警报的资产数据，您需要将`Assets`参数大写。例如：`alert.Assets[]`。但是，当手动为目标对象启动行动手册时，若要在输入数据中使用资产数据，请勿将`assets`参数大写。例如：`.input.assets[]`。

根据在创建或编辑行动手册时选择的范围，您可以在以 jq 语言编写的表达式中使用警报数据模型或事故数据模型。为此，请编写带有`alert`或`incident`值的表达式（不要在值的开头使用点号“`.`”）。例如：

```
"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
```

您可以在任何执行步骤的 jq 表达式中使用警报或事故数据。警报或事故数据仅在读取模式下可用。这些数据在行动手册运行期间不会更改。如果在启动行动手册后，警报或事故数据发生变化，则不会影响行动手册的执行。

在算法中使用行动手册数据时，还可以使用 jq 表达式。有关 jq 表达式的更多信息，请参阅 jq 手册。

如果在 jq 表达式中使用引号，则需要使用反斜杠转义这些引号。例如：`"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"`。

并非用于转义引号的反斜杠也必须用其他反斜杠进行转义。例如：`${\"add_firewall_rule --ip_address=\" + ([.input.observables[] | select(.type == \"ip\") | select(.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.).*\") | not) | .value] | join(\",\"))}`。

如果要为特定对象（可观察对象或资产）启动行动手册，请使用算法中的`.input`参数。这些对象将作为行动手册启动时的输入。例如：

```
"assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
```

有关详情，请参阅“为用户指定的对象启动行动手册”。

如何调用提示

如果在编写算法时需要有关可用字段的提示，请使用引号（""）。可用字段列表随即显示。

要在警报或事故数据上显示提示：

在 jq 表达式中，写入`alert`或`incident`，并在末尾加上点号“`.`”。

如果上述表达式中没有错误，则会显示正确的提示。否则，可用字段列表可能不正确。

如何调用提示

您可以在编写行动手册算法时调用建议。建议中包含搜索字符串并帮助您快速指定字段值。要查看建议，请使用引号（""）。更新列表随即显示。

建议还允许您按名称搜索。但是，当您选择所需的值时，名称将自动更改为算法中的 ID。有关详细信息，请参阅使用行动手册编辑事故和使用行动手册编辑警报。

如果您在选择后删除了引号之间指定的参数名称，则即使您在引号之间指定了新参数，也不会出现该参数的建议。

要返回参数的建议模式，请执行以下操作之一：

- 删除引号，然后添加一个左双引号。右双引号将自动添加，并显示建议。
- 在引号之间输入任意字符，然后按“**Backspace**”键。这将返回到建议模式。

> 如果逐个字符地删除参数名称，即使完全删除了参数名称，也不会退出建议模式。

行动手册算法示例

```
{
  "actionsSpecVersion": "1",
  "dslSpecVersion": "1.1.0",
  "version": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "blockLDAPAccount"
          "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
        },
        "onError": "stop"
      }
    },
    {
      "loop": {
        "batchSize": 1,
        "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and .DestinationProcessName
!= \"\")][] | .DestinationProcessName] }",
        "mode": "parallel",
        "onError": "stop",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
                "params": {
                  "path": "${ .[0] }"
                }
              }
            }
          }
        ]
      }
    },
    {
      "action": {
        "function": {
          "type": "avScan",
          "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
          "params": {
            "scope": {
              "allowScanNetworkDrives": false,
              "area": "full"
            },
            "wait": false
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

行动手册参数

参数 ID	Description
`name`	行动手册名称。由系统在创建或更新行动手册时指定。如果算法中设置了该值，则会被系统替换。
`description`	行动手册描述。由系统在创建或更新行动手册时指定。如果算法中设置了该值，则会被系统替换。
`version`	行动手册版本。最小长度是 1。 此参数是必需的。
`dslSpecVersion`	DSL 架构版本。最小长度是 1。 此参数是必需的。
`actionSpecVersion`	响应操作架构版本。最小长度是 1。 此参数是必需的。
`playbookRunTimeout`	行动手册的最长执行时间，包括在队列中等待的时间。最大值为 48 小时（`48h`）。支持以小时 (h) 和/或分钟 (m) 为单位配置最长执行时间。 默认情况下，该值为 `24h`。
`inputType`	入站对象类型。可能的值：`alert` 或 `incident`。入站对象类型由系统在创建或更新行动手册时指定。如果算法中设置了该值，则会被系统替换。
`input`	可用于在执行行动手册之前转换或过滤传入数据的 jq 表达式。
`output`	可用于在执行之前修改行动手册输出的 jq 表达式。
`timeouts`	超时定义。
`executionFlow`	执行行动手册的步骤。 此参数是必需的。

执行步骤参数

执行步骤元素数组描述了行动手册的逻辑。执行步骤按照行动手册中描述的顺序执行。执行步骤有以下几种类型：

- 操作
- Loop
- 并行
- 决定
- 更新数据

操作参数

`Action` 参数调用响应函数。

参数 ID	Description
`function`	定义响应操作的对象。更多信息，请参阅 ResponseFunction 参数。

filterProduct	此参数允许您过滤执行响应操作的组件。请求时，组件插件将按允许和限制的组件进行过滤。 例如，该参数可按以下方式指定： `"filterProduct": { "allowed": ["PRODUCT_NAME"] }`
output	此参数允许您编辑响应操作返回的值，方法是使用 JQ 表达式并将其放入行动手册数据（本地或操作）中。
timeout	此参数允许您设置调用响应函数的超时时间。您可以指定行动手册中设置的超时策略名称，也可以手动设置超时值。 如果未指定该值，则应用默认超时时间。
manualApprove	此参数允许您配置手动审批响应操作。可能值： • 布尔值： • true—使用默认参数启用手动审批。 • false—手动审批已禁用。 • 对象 ManualApprove。
onError	此参数定义在执行响应操作期间发生错误时的行为。可能值： • stop—定义在执行响应操作期间发生错误时终止行动手册。 • continue—定义即使某个响应操作出现错误，行动手册仍继续执行。在这种情况下，行动手册将启动算法中指定的下一个响应操作。 默认情况下，该值为 stop。 请注意，如果发生系统错误，则无论指定的 onError 参数值是什么，行动手册执行都会以出错结束。

超时策略

执行步骤的超时策略。系统会自动确定默认超时策略。

您可以使用默认策略名称重新配置默认超时策略。在这种情况下，新策略将自动应用于所有执行步骤。

参数 ID	Description
name	超时策略名称。
scheduleToCloseTimeout	最大执行时间，包括在队列中等待和重试。该参数以 Go 字符串格式 指定。 如果未指定值或值为 0，则使用 playbookRunTimeout 字段中的值。

输出

output 参数在步骤结束时生成操作数据，然后将其传输到下一个步骤。如果要在下一个步骤中使用行动手册当前步骤的结果，请指定 output 参数。

为避免系统过载，建议对放置在行动手册数据（本地或操作）中的数据施加限制。

参数 ID	Description
action	此参数定义行动手册数据（本地或操作）是否将被覆盖或合并。可能值： • merge—新数据与当前数据合并。 • overwrite—当前数据被新数据覆盖。
filter	此参数定义用于处理输出数据的 jq 表达式。

手动审批

参数 ID	Description
`timeout`	手动审批的超时时间（分钟）。最小值为10分钟（`10m`），最大值为180分钟（`180m`）。 默认情况下，该值为60分钟（`60m`）。
`emailNotifications`	此参数允许您配置电子邮件通知的发送方式。

邮件通知设置

参数 ID	Description
`enabled`	用于启用电子邮件通知的标志。
`delay`	此参数定义发送电子邮件通知之前的延迟。该值以分钟为单位。 最小值为5分钟（`5m`），最大值为30分钟（`30m`）。 默认情况下，该值为10分钟（`10m)`。

循环

在指定Loop参数之前，请确保行动手册算法中也指定了aggregate参数。

Loop参数用于按元素拆分传入数据的数组并对元素执行各种操作。

参数 ID	Description
`input`	用于组成数组或引用数组的 jq 表达式。
`aggregate`	此参数允许您使用 jq 表达式来配置聚合规则。
`output`	配置如何将输出数据应用于当前行动手册数据。可能值： • 字符串常量：`merge` 或 `overwrite`。 • 对象 `Output`。
`mode`	循环操作模式。可能值： • `parallel`—定义所有元素并行处理。线程的数量由解释器控制。 • `sequence`—定义所有元素按顺序处理。 默认情况下，该值为 `parallel`。
`batchSize`	此参数允许您指定在一个循环或一个并行线程中处理的数组元素数量。如果插件功能限制了输入元素的数量，则可以使用此参数。 例如，如果插件函数在一次循环中最多只能处理10个元素，则可以指定以下参数值：`batchSize=10`。 默认情况下，该值为 `1`。
`onError`	此参数定义当其中一个分支发生错误时的行为。可能值： • `stop`—定义发生错误时终止所有分支。其余分支将继续运行。 • 如果为 `mode=sequence`，在一个分支发生错误后，所有后续分支都将停止运行。 • 如果为 `mode=parallel`，在一个分支发生错误后，所有分支仍会继续独立运行。 • `continue`—定义发生错误的某个分支停止运行。其余分支将继续运行。 默认情况下，该值为`stop`。
`steps`	执行步骤数组。

并行

在指定Parallel参数之前，请确保行动手册算法中也指定了aggregate参数。

`Parallel`参数用于同时对数据执行多项操作。与"循环"不同， `Parallel`会将相同的输入数据传输到不同的执行分支。

参数 ID	Description
`input`	用于组成数组的 jq 表达式。
`aggregate`	此参数允许您使用 jq 表达式来配置聚合规则。
`output`	配置如何将输出数据应用于当前行动手册数据。可能值： • 字符串常量： `merge` 或 `overwrite`。 • 对象 `Output`。
`onError`	此参数定义当其中一个分支发生错误时的行为。可能值： • `stop`—定义发生错误时终止所有分支。其余分支将继续运行。 • `continue`—定义发生错误的某个分支停止运行。其余分支将继续运行。 默认情况下，该值为`stop`。
`branches`	执行分支。

分支

参数 ID	Description
`name`	在`Parallel`中唯一的分支名称。
`steps`	执行步骤数组。

决定

`Decision`执行步骤允许您根据条件执行一个步骤或一组步骤。请注意，仅执行第一个经过验证的条件。

参数 ID	Description
`conditions`	条件数组。

条件

参数 ID	Description
`condition`	包含执行条件的 jq 表达式。
`steps`	当前分支的执行步骤。

更新数据

UpdateData 参数可描述为具有状态更改逻辑的 jq 脚本，也可描述为 `Output` 对象。

响应函数参数

参数 ID	Description
`action`	响应操作名称。
`params`	该参数用于描述要启动的响应操作的参数。您可以将参数指定为 jq 表达式或对象。下表描述了响应操作的参数。
`assets`	该参数允许您使用 jq 表达式或字符串数组来指定要启动响应操作的资产列表。 `assets` 参数是涉及资产的响应操作所必需的参数，而不适用于不涉及资产的响应操作。

响应操作参数

响应操作名称	设置
`updateBases`	更新数据库响应操作。可能的参数： • `wait`。可能值： • `true` • `false` 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`avScan`	运行恶意软件扫描响应操作。可能的参数： • `wait`。可能值： • `true` • `false` • `scope`。可能值： • `full`—对检测到警报的设备执行全盘扫描。 • `critical`—对内核内存、正在运行的进程和磁盘引导扇区执行扫描。 • `selective`—对指定文件执行扫描。要指定文件的路径，请使用`path`参数。 • `allowScanNetworkDrives`。可能值： • `true` • `false` 默认情况下，该值为`false`。 仅当您要执行全盘扫描时，此参数才可用。 请注意，扫描网络驱动器可能会使系统过载。 • `path`—jq 表达式或包含要扫描的文件路径的字符串。您还可以指定多个文件路径。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`moveHostsToAdministrationGroup`	移至组响应操作。可能的参数： • `group`—Open Single Management Platform 管理组路径。例如，`HQ/OrgUnit1`。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`quarantineFile`	移至隔离区响应操作。可能的参数： • `path`—要隔离的文件的路径。 • `md5`—文件的 MD5 哈希。 • `sha256`—文件的 SHA256 哈希。 您可以通过以下方式之一指定响应操作参数： • 指定要隔离的文件的完整路径。在这种情况下，无需指定 MD5 哈希或 SHA256 哈希。 • 指定文件路径和文件哈希（MD5 或 SHA256）。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`restoreQuarantinedFile`	从隔离响应操作中恢复文件。可能的参数： • `path`—要恢复的文件的路径。 • `md5`—文件的 MD5 哈希。 • `sha256`—文件的 SHA256 哈希。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`killProcess`	终止进程响应操作。可能的参数： • `pid`—进程标识符。 • `path`—要隔离的文件的路径。 • `md5`—文件的 MD5 哈希。 • `sha256`—文件的 SHA256 哈希。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。

changeAuthorizationStatus	更改授权状态响应操作。可能的参数： • authorized。可能值： • true • false 要启动此响应操作，您需要指定响应函数的 asset 参数。
netIsolateOn	启用网络隔离响应操作。可能的参数： • isolationTimeoutSec—网络隔离期。您可以按小时数或天数来指定此参数。以小时为单位的最小值为1小时，最大值为 9999 小时。 网络隔离时长以秒为单位指定。 • exclusions—排除规则。您可以指定一个或多个排除规则。 • remoteIPV4Address—来自指定 IPv4 地址的网络流量将被排除在阻止范围之外。例如，192.168.2.15。 • remoteIPV6Address—来自指定 IPv6 地址的网络流量将被排除在阻止范围之外。例如，2001:0db8:0000:0000:0000:ff00:0042。 • remotePortRange—远程端口范围。 • localPortRange—本地端口范围。 如果未指定 remotePortRange 和 localPortRange，则排除规则适用于所有端口。 • exclusionsConflictBehavior—定义不同排除规则之间出现冲突时的行为。可能的参数： • replace • skip • fail
netIsolateOff	禁用网络隔离响应操作。 要启动此响应操作，您需要指定响应函数的 asset 参数。
executeCommand	运行可执行文件响应操作。可能的参数： • commandLine—要运行的命令或可执行文件的完整路径。 • workingDirectory—工作目录的路径。 • commandLineParameters—要应用于命令的命令行参数。 要启动此响应操作，您需要指定响应函数的 asset 参数。
addFilePreventionRules	添加预防规则响应操作。可能的参数： • md5—MD5哈希数组。 • sha256—SHA256哈希数组。 要启动此响应操作，您需要指定响应函数的 asset 参数。
deleteFilePreventionRules	删除预防规则响应操作。可能的参数： • md5—MD5哈希数组。 • sha256—SHA256哈希数组。 要启动此响应操作，您需要指定响应函数的 asset 参数。
resetFilePreventionRules	删除所有预防规则。 要启动此响应操作，您需要指定响应函数的 asset 参数。
assignKasapGroup	分配 KASAP 组响应操作。可能的参数： groupId—KASAP组标识符。 要启动此响应操作，您需要指定响应函数的 asset 参数。
addToLDAPGroup	将用户添加到安全组响应操作。可能的参数： groupDN—LDAP组的可分辨名称 (DN)。 要启动此响应操作，您需要指定响应函数的 asset 参数。
removeFromLDAPGroup	从安全组中删除用户响应操作。可能的参数： groupDN—LDAP组的可分辨名称 (DN)。 要启动此响应操作，您需要指定响应函数的 asset 参数。

`blockLDAPAccount`	锁定账户响应操作。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`resetLDAPPassword`	重置密码响应操作。 要启动此响应操作，您需要指定响应函数的 `asset` 参数。
`executeCustomScript`	执行自定义脚本。可能的参数： • `commandLine`—要运行的命令。 • `commandLineParameters`—要应用于命令的命令行参数。 • `stdIn`—标准输入流。如果脚本需要来自标准输入的一些附加数据，请使用此参数。 • `workingDirectory`—工作目录的路径。
`iocsEnrichment`	数据增强。可能的参数： • `observables`—包含要增强的可观察对象数组的 jq 表达式。 • `fullEnrichment`—定义要请求的记录数。可能值： • `true`—从来源请求所有记录。 • `false`—从来源请求前 100 条记录。

使用行动手册编辑事故

可通过 Kaspersky Next XDR Expert 来手动或使用行动手册编辑事故。创建行动手册时，您可以配置行动手册算法来编辑事故属性。

要使用行动手册编辑事故，您必须具有以下角色之一：主管理员、SOC 管理员、1 级分析师、2 级分析师或租户管理员。

您无法编辑状态为“**已关闭**”的事故。

您可以使用行动手册编辑以下事故属性：

- 负责人
- 事故工作流状态
- 事故类型
- 注释
- 描述
- 优先级
- ExternalReference 属性
- 附加数据属性

以下是您可以在行动手册中用来编辑事故属性的示例表达式。您可以在可视化编辑器的“**显示代码**”部分指定这些表达式。

- **将事故分配给用户**

```
{
  "action": {
    "function": {
       "type": "assignIncident",
       "params": {
     "assignee": {
        "id": "user_ID"
       }
        }
        }
    }
       }
```

在行动手册算法中编辑负责人时，会显示建议。为方便操作，建议中包含一个搜索字符串，您可通过名称进行搜索。如果您想指定事故负责人，可以按用户的名称搜索相应的记录，算法中会指定 ID。

- **将事故分配给用户组**

```
{
    "action": {
      "function": {
         "type": "assignIncident",
         "params": {
           "group": {
              "id": "GROUP_ID"
                           }
                      }
                 }
              }
         }
```

在行动手册算法中编辑负责人时，会显示建议。为方便操作，建议中包含一个搜索字符串，您可通过名称进行搜索。如果您想指定事故负责人，可以按用户组的名称搜索相应的记录，算法中会指定 ID。

- **取消向用户分配事故**

```
{
  "action": {
    "function": {
       "type": "assignIncident",
       "params": {
     "assignee": {
        "id": "nobody"
       }
        }
        }
    }
       }
```

- **取消向用户组分配事故**

```
{
    "action": {
      "function": {
         "type": "assignIncident",
         "params": {
           "group": {
```

```
            "id": "nobody"
                        }
                    }
                }
            }
        }
```

- **更改事故工作流的状态**

  要将事故工作流状态更改为“**已打开**”：

```
{
    "action": {
      "function": {
         "type": "setIncidentStatus",
         "params": {
           "typeId": "af9dd279-fc30-4596-963b-942f79920375",
           "statusId": "4db36105-5223-4078-b72c-e9e9983b0987"
                    }
                }
            }
        }
```

  要将事故工作流状态更改为“**已关闭**”：

```
{
  "action": {
    "function": {
       "type": "setIncidentStatus",
       "params": {
        "statusId": "INCIDENT_STATUS_ID",
                  "statusResolution": "truePositive"
         }
         }
    }
       }
```

  您还可以为 `statusResolution` 参数指定以下值：`falsePositive` 和 `lowPriority`。

  要将事故工作流状态更改为自定义状态：

```
{
  "action": {
    "function": {
       "type": "setIncidentStatus",
       "params": {
                  "typeId": "22222222-2222-2222-2222-222222222222",
                  "statusId": "11111111-1111-1111-1111-111111111111"
         }
         }
    }
       }
```

  在行动手册算法中编辑事故工作流状态时，会显示建议。为方便操作，建议中包含一个搜索字符串，您可通过名称进行搜索。如果您想指定事故工作流状态，可以按名称搜索相应的记录，算法中会指定 ID。

- **更改事故类型**

```
{
  "action": {
    "function": {
       "type": "setIncidentType",
```

```
      "params": {
       "id": "INCIDENT_TYPE_UUID"
        }
        }
    }
       }
```

在行动手册算法中编辑事故类型时，会显示建议。为方便操作，建议中包含一个搜索字符串，您可通过名称进行搜索。如果您想指定事故类型，您可以按名称搜索相应的记录，算法中会指定 ID。

- **为事故添加注释**

```
{
  "action": {
    "function": {
       "type": "addCommentToIncident",
       "params": {
     "text": "${ \"针对指定 ID 事故的新注释: \\(incident.ID)\" }"
        }
        }
    }
       }
```

- **编辑事故描述**

```
{
   "action": {
     "function": {
        "type": "setIncidentDescription",
        "params": {
              "description": "${ incident.ID | tostring | \"事故的新评论，ID 为: \" + . }",
              "mode": "replace"
                    }
                }
              }
        }
```

要在现有描述后追加内容，请为 `mode` 参数指定 `append` 值。

- **更改事故优先级**

```
{
  "action": {
    "function": {
       "type": "setIncidentPriority",
       "params": {
        "priority": "critical"
        }
        }
    }
       }
```

您还可以为 `priority` 参数指定以下值：`high`、`medium`、`low`。

- **编辑 ExternalReference 属性**

```
{
    "action": {
      "function": {
```

```
        "type": "setIncidentExternalRef",
        "params": {
              "externalRef": "${ \"新的值 extReference\" }",
              "mode": "replace"
                        }
                   }
              }
         }
```

要在 ExternalReference 属性后追加内容，请为 mode 参数指定 append 值。

- **编辑附加数据属性**

```
{
  "action": {
    "function": {
       "type": "addIncidentAdditionalData",
       "params": {
     "data": "${ {\"customKey\": \"customValue\"} }",
                "mode": "replace"
          }
          }
    }
       }
```

要向附加数据属性追加内容，请为 mode 参数指定 append 值。

使用行动手册编辑警报

Kaspersky Next XDR Expert可让您手动或使用行动手册编辑警报。创建行动手册时，您可以配置行动手册算法来编辑警报属性。

要使用行动手册编辑警报，您必须具有以下 XDR 角色之一：主管理员、SOC 管理员、1 级分析师、2 级分析师或租户管理员。

您无法编辑状态为 **已关闭** 的警报。

您可以使用行动手册编辑以下警报属性：

- 负责人
- 警报状态。
- 注释
- ExternalReference 属性
- 附加数据属性

以下是您可以在可视化行动手册编辑器的“**显示代码**”部分输入的示例表达式，用于更改警报属性。

- **向用户分配警报**

```
{
       "action": {
           "function": {
               "type": "assignAlert",
                   "params": {
                      "assignee": {
                         "id": "user_ID"
                       }
                   }
               }
           }
       }
```

在行动手册算法中编辑负责人时，会显示建议。为方便操作，建议中包含一个搜索字符串，您可通过名称进行搜索。如果要指定警报负责人，您可以按用户名搜索相应记录，并且 ID 将在算法中指定。

- **将警报分配给用户组**

```
{
    "action": {
      "function": {
         "type": "assignAlert",
          "params": {
            "group": {
               "id": "GROUP_ID"
                           }
                     }
                }
             }
          }
```

在行动手册算法中编辑负责人时，会显示建议。为方便操作，建议包含搜索字符串，您可以在其中按用户组名称搜索。如果要指定警报负责人，您可以按用户名搜索相应记录，并且 ID 将在算法中指定。

- **取消向用户分配警报**

```
{
            "action": {
                "function": {
                    "type": "assignAlert",
                    "params": {
                        "assignee": {
                            "id": "nobody"
                        }
                    }
                }
            }
        }
```

- **取消向用户组分配警报**

```
{
    "action": {
      "function": {
         "type": "assignAlert",
          "params": {
            "group": {
               "id": "nobody"
```

```
                    }
                }
            }
        }
    }
```

- **更改警报状态**

  要将警报状态更改为“**进行中**”：

```
{
            "action": {
                "function": {
                    "type": "setAlertStatus",
                        "params": {
                            "status": "inProgress"
                     }
                }
            }
        }
```

  要将警报状态更改为“**已关闭**”：

```
{
            "action": {
                "function": {
                    "type": "setAlertStatus",
                        "params": {
                            "status": "closed",
                            "statusResolution": "truePositive"
                     }
                }
            }
        }
```

  您还可以为 statusResolution 参数指定以下值：`falsePositive` 和 `lowPriority`。

  当您在行动手册算法中编辑警报状态时，可能会显示以下建议：`new`、`inProgress` 和 `closed`。

- **向警报添加注释**

```
{
            "action": {
                "function": {
                    "type": "addCommentToAlert",
                    "params": {
                        "text": "${ \"New comment for alert with ID: \" + alert.InternalID }"
                    }
                }
            }
        }
```

- **编辑 ExternalReference 属性**

```
{
      "action": {
          "function": {
                "type": "setAlertExternalRef",
                   "params": {
                     "externalRef": "${ \"Appended externalRef for alert with ID: \" + alert.InternalID }",
                       "mode": "append"
                    }
                }
```

```
            }
        }
```

要用行动手册中的值替换警报中 ExternalReference 属性的当前值，请为 `mode` 参数指定 `replace` 值。

- **编辑附加数据属性**

```
{
      "action": {
           "function": {
              "type": "addAlertAdditionalData",
                 "params": {
                    "data": "${ {\"customKey_1 (alert.InternalID)\": (\"customValue_1 (\" + alert.InternalID +
\")\" )} }",
                    "mode": "append"
                    }
                }
            }
        }
```

要用行动手册中的值替换警报中 AdditionalData 属性的当前值，请为 `mode` 参数指定 `replace` 值。

管理 Sandbox

Sandbox 是一款安全组件，它利用带有操作系统映像的虚拟机 (VM) 来分析对象（例如文件、程序或脚本）的行为，以发现潜在的恶意活动和针对企业 IT 基础设施的针对性攻击迹象。

要让 Sandbox 处理对象，需要对其进行配置，然后在 Sandbox 中安装虚拟机。

初始 Sandbox 设置

在安装虚拟机之前，您需要配置 Sandbox：

- 配置数据库更新。
- 确保在 Sandbox 安装期间正确配置了互联网访问。如有必要，调整设置。

您还可以选择更改管理员密码和配置身份验证政策。

为 Sandbox 配置数据库更新

在授权许可有效期内，Sandbox 每小时自动获取一次更新包。

要为 Sandbox 配置数据库更新：

1. 在 Sandbox Web 界面中，转到“**数据库更新**”。
2. 在“**更新源**”设置组中，选择要从中接收更新的源：
   - **卡巴斯基更新服务器**

     Sandbox 通过 HTTP 连接到卡巴斯基更新服务器并下载最新的数据库。
   - **卡巴斯基更新服务器(安全连接)**

     Sandbox 通过 HTTPS 连接到卡巴斯基更新服务器，以下载最新的数据库。推荐使用 HTTPS 进行安全更新。
   - **自定义服务器**

     Sandbox 连接到您的 FTP 或 HTTP 服务器或计算机上包含程序数据库的文件夹以下载最新的数据库。
3. 如果您选择了**自定义服务器**：
   - 如果要指定 FTP 或 HTTP 服务器作为更新源，请在此设置下方的字段中指定应用程序数据库更新包目录的完整路径，以下载最新的数据库。
   - 如果要将托管 Sandbox 组件的 Kaspersky Next XDR Expert 服务器指定为更新源，请在此设置下方的字段中指定以下更新源地址，以下载最新的数据库：

     ```
     http://updater.<smp_domain>:8083/retranslation
     ```

4. 决定在下载更新时是否使用代理服务器：

   - 要启用代理服务器，请打开“**代理服务器**”设置组名称旁边的切换开关，然后指定连接到代理服务器的设置：

     - 代理服务器地址和端口号。
     - 代理服务器用户名和密码。

   - 要禁用代理服务器，请关闭“**代理服务器**”设置组名称旁边的切换开关。

5. 单击“**应用**”以保存设置。

Sandbox 网络接口

配置 Sandbox 网络接口包括设置 DNS 服务器、配置管理网络接口、管理已处理对象的互联网访问以及添加静态网络路由。

配置 DNS 设置

要配置 DNS：

1. 在 Sandbox Web 界面中，转到**“网络接口”**。
2. 在**“主机名”**字段中，指定要安装 Sandbox 的服务器名称。服务器名称必须采用 FQDN 格式。
3. 单击**“DNS 服务器”**右侧的**“添加”**按钮。
4. 在出现的空白字段中，以 IPv4 格式指定主要 DNS 服务器的 IP 地址。
5. 点击指定IP地址右侧的✓按钮。

DNS 服务器已添加。

要添加更多 DNS 服务器，请重复步骤 2 至 5。

要删除先前添加的 DNS 服务器，请在指定的 DNS 服务器 IP 地址右侧单击 🗑。请注意，您只能移除其他 DNS 服务器，而不能移除主要 DNS 服务器。如果您添加了两个或更多 DNS 服务器，则可以移除其中任何一个。剩余的 DNS 服务器将成为主要服务器。

配置管理网络接口

管理网络接口旨在通过 SSH 协议提供对 Sandbox 服务器的访问。Sandbox 也通过此接口接收对象。

管理网络接口在 Sandbox 安装期间进行初始配置。Sandbox 安装完成后，您可以按照以下说明从 Sandbox Web 界面更改管理网络接口设置。

要配置管理网络接口：

1. 在 Sandbox Web 界面中，转到**"网络接口"**。
2. 在"**接口**"下拉列表中的"**管理接口**"设置组中，选择要用作管理接口的网络接口。
3. 配置管理接口参数：
   - **IP**：如果未分配 IP 地址，则要分配给此网络接口的 IP 地址。
   - **掩码**：您要使用此网络接口的网络的掩码。
4. 单击"**应用**"。

管理网络接口被配置。

配置已处理对象的互联网访问

Sandbox 处理的对象可能会尝试通过为访问互联网配置的网络接口在互联网上执行操作。在这种情况下，Sandbox 可以分析这些对象在互联网上的行为。如果阻止互联网访问，Sandbox 会分析对象的行为，但不包括它们在互联网上的操作。

安全风险及注意事项

如果贵组织的安全政策阻止本地网络计算机访问互联网，且用于访问互联网的 Sandbox 网络接口是打开的，则可能会出现以下情况：

1. 黑客将恶意应用程序添加到随机文件中，然后从本地网络计算机将其发送到 Sandbox 进行扫描。
2. 扫描过程中，文件会被传输到本地网络之外。

如果阻止对已处理对象的互联网访问，则可以消除这种风险。然而，这也意味着警报质量降低，因为已处理的对象无法得到正确的分析。

要配置用于对已处理对象进行互联网访问的网络接口：

1. 在 Sandbox Web 界面中，转到**"网络接口"**。
2. 在"**互联网界面** "设置组的**"接口"**列表中，选择要用于对已处理对象进行互联网访问的网络接口。
3. 配置接口参数：
   - **IP**：如果未分配 IP 地址，则要分配给此网络接口的 IP 地址。
   - **掩码**：您要使用此网络接口的网络的掩码。
   - **默认网关**：您希望使用此网络接口的网络的网关地址。
4. 单击"**应用**"。

已配置用于对已处理对象进行互联网访问的网络接口。

添加静态网络路由

要添加静态网络路由：

1. 在 Sandbox Web 界面中，转到**"网络接口"**。
2. 在"**静态路由**"设置组中，单击**"添加"**按钮。
   静态网络路由列表中出现了一组空字段。
3. 配置路由参数：
   - **IP**：要为其配置静态网络路由的服务器的 IP 地址。
   - **掩码**：子网掩码。
   - **网关**：网关的 IP 地址。
4. 从**接口**列表中，选择一个想要为其添加静态网络路由的网络接口。
5. 单击指定路由右侧的✓按钮。
6. 单击"**应用**"。

已添加静态网络路由。

添加静态网络路由后，您可以进一步管理他。通过单击 按钮删除它或单击 按钮修改它。修改时，您需要指定与创建新路由时相同的参数，如上所述。

更改 Sandbox 管理员账户密码

要更改 Sandbox 管理员账户密码：

1. 在 Sandbox Web 界面中，转到"**管理** → **更改密码**"。
2. 在"**当前密码**"字段中，输入您用于登录 Sandbox 的密码。
3. 在"**新密码**"和"**确认密码**"字段中，输入新密码。
4. 单击"**更改密码**"。

沙盒身份验证政策

您可以在 Sandbox 中为 Kaspersky Next XDR Expert 用户配置身份验证策略。

终止非活动会话

如果用户没有执行任何操作（会话处于空闲状态），我们建议终止此类会话。这样可以降低用户实际完成应用程序操作但未结束会话时，未经授权访问 Sandbox 的风险。

关于身份验证尝试失败的通知

频繁尝试登录 Web 界面失败可能表明网络犯罪分子正试图通过暴力破解密码来获取 Sandbox 的访问权限。为了防止此类未经授权的访问，我们建议启用有关超出身份验证尝试失败次数限制的通知。

终止不活动的 Sandbox 会话

如果用户没有执行任何操作（会话处于空闲状态），我们建议终止此类会话。这样可以降低用户实际完成应用程序操作但未结束会话时，未经授权访问 Sandbox 的风险。

要启用并配置非活动会话的终止：

1. 在沙盒网页界面中，转到**身份验证政策**。
2. 在“**终止不活动会话**”部分，指定当用户未执行任何操作时终止用户会话的时间。在“**终止不活动会话**”字段输入时间（分钟）。
3. 单击“**应用**”。

Sandbox 会在指定时间后终止不活动的用户会话。

关于 Sandbox 身份验证尝试失败的通知

频繁尝试登录 Web 界面失败可能表明网络犯罪分子正试图通过暴力破解密码来获取 Sandbox 的访问权限。为了防止此类未经授权的访问，我们建议启用有关超出身份验证尝试失败次数限制的通知。

要启用并配置有关失败的身份验证尝试的通知：

1. 在 Sandbox Web 界面中，转到**“身份验证策略”**。
2. 在**“统计身份验证尝试次数”**部分，将**“计数尝试”**切换开关设置为**“启用”**。
3. 在“**计数周期**”字段中，输入您想要计算失败的身份验证尝试次数的时间段。时间以分钟为单位指定。如果用户尝试登录 Web 界面或管理控制台并连续失败两次以上，则会发生以下情况：
   - 有关用户身份验证尝试失败的记录将写入用户活动日志。
   - 如果已创建用于发送失败身份验证尝试次数过多的通知的规则，则会向通知规则中指定的地址发送电子邮件。该邮件包含有关失败的用户身份验证尝试的信息。

在**计数周期**字段中，您可以指定`0`，在这种情况下，所有失败的身份验证尝试都会被计算在内，无论它们之间经过了多少时间。

4. 单击**应用**。

设置将已检测到的对象发送到KPSN拒绝列表

该应用程序允许具有一级分析师和二级分析师角色的用户启用或禁用将沙盒扫描到的恶意的文件哈希值自动发送到KPSN拒绝列表。此参数的配置因租户而异。只能在OSMP安装程序的根租户中更改：在子租户中，无法更改此选项。

在启用将检测到的对象自动发送到KPSN拒绝列表之前，请确保已启用KPSN使用，并且已配置与KPSN本地信誉数据库的连接。

若要启用将检测到的对象自动发送到KPSN拒绝列表的功能：

1. 在应用程序主窗口中，转到**设置→租户**部分。
2. 点击**根租户**，然后转到**设置 → KPSN信誉数据库**子部分。
3. 打开**“将对象状态设置为‘不受信任’”**切换按钮。
4. 单击“**保存**”按钮。

准备虚拟机以供使用

Sandbox 使用虚拟机在各种操作系统上运行对象，以便分析对象的行为并检测其恶意活动。

您可以安装两种类型的虚拟机：

- *预配置*虚拟机和*默认虚拟机*。预配置虚拟机基于分发包中的操作系统镜像（ISO 文件）。您无法修改这些镜像或其中安装的应用程序。

  > 默认操作系统和应用程序可能需要激活。激活是使用您的授权许可进行的。

- *自定义*。默认虚拟机基于您选择的操作系统。您可以在这些操作系统上安装任何应用程序。

您可以同时使用自定义和默认操作系统镜像。

安装虚拟机涉及以下步骤：

1. *可选*。将镜像上传到存储。创建模板时，您可以跳过此步骤，直接从计算机上传镜像。
2. 创建模板，可以通过导入预配置模板或创建自定义虚拟机模板来实现。
3. *对于自定义模板*，需要配置操作系统和软件。

4. 创建虚拟机。
5. 安装虚拟机。

将镜像上传到存储

要将镜像上传到存储：

1. 在 Sandbox Web 界面中，转到**“模板和存储”**→**“存储”**。
2. 单击“**上传**”。
3. 选择要上传到存储的 .ISO 文件，然后单击“**打开”**。

导入模板

如果要安装预配置的虚拟机，导入模板是第一步。

如果您之前已经创建并导出了自定义虚拟机模板，也可以导入该模板。

要导入虚拟机模板：

1. 在 Sandbox Web 界面中，转到**“模板和存储”**→**“模板”**。
2. 从“**添加**”下拉列表中，选择“**导入模板**”。
3. 选择要导入的文件，然后单击“**打开**”。

创建自定义虚拟机模板

要创建自定义虚拟机模板：

1. 在 Sandbox Web 界面中，转到**“模板和存储”**→**“模板”**。
2. 从**“添加”**下拉列表中，选择**“创建模板”**。
   此时将打开模板创建窗口。

3. 在**"准备镜像"**步骤中：

   a. 指定镜像**名称**和可选的**描述**。

   b. 要为模板指定操作系统，请执行以下操作之一：

   - 从**"操作系统镜像"**下拉列表中选择一个镜像。
   - 上传操作系统镜像：单击**"上传"**，选择一个 ISO 文件，然后单击**"打开"**。

   c. 单击**"继续"**。

4. 在**"自定义模板"**步骤中：

   a. 在**"挂载 ISO"**下拉列表中，选择要安装在操作系统中的应用程序镜像。
   要使镜像显示在列表中，请执行以下操作之一：

   - 将镜像上传到存储。
   - 上传应用程序镜像文件：单击**"上传"**，选择一个 ISO 文件，然后单击**"打开"**。

   b. 安装应用程序后，卸载已安装的镜像：在"**挂载 ISO**"下拉列表中，单击镜像旁边的 ⏏ 图标。

   c. 配置操作系统和已安装的软件。

配置操作系统和软件

准备操作系统以供使用

安装 Windows 7、8.1 或 10 操作系统时，必须满足以下要求：

- 禁用屏幕保护程序。
- 选择"始终开启"电源计划。
- 禁用自动更新。
- 禁用 Windows 防火墙。

如果您使用的是 Windows 7，则需要支持 SHA-2 哈希算法。要确保此哈希算法受支持，请安装适用于 x64 系统的 Windows 7 安全更新 (KB3033929)。对于 32 位 Windows 7 操作系统，还必须安装更新 KB3033929。

> 不要安装更新 KB4474419。此更新可能会导致虚拟机部署期间崩溃。

要使用 Windows 7，您必须在操作系统设置中启用 TLS 1.1 和 TLS 1.2。为此，在 Windows 7 中的"**控制面板**" → "**Internet 选项**" → "**高级**"部分中，选中"**使用 TLS 1.1**"和"**使用 TLS 1.2**"复选框。

使用 Windows 8.1 或 10 时，必须禁用快速启动并启用自动登录。

操作系统的本地化

您可以在安装系统时选择本地化语言，也可以安装带有英语本地化的系统，并在该系统中额外安装本地化包。您可以选择以下语言之一：俄语、英语、中文（简体）、阿拉伯语、西班牙语（墨西哥）。如果选择不同的本地化，对象扫描的质量会降低。

对于 Windows XP 操作系统，仅支持俄语和英语。

配置操作系统

安装操作系统时：

- 确保配置了默认命令 shell。
- 激活操作系统和其他许可软件。

您可以使用已安装的操作系统执行以下操作：

- 为计算机分配静态名称。
- 创建用户账户。

  此时，您需要配置自动登录。

- 安装软件。
  软件安装限制：
  - 一次只能将一张镜像连接到一个模板。保存模板后，您可以断开一个镜像并安装另一个镜像。
  - 不支持 2016 年之后的 Microsoft Office 版本。
  - 强烈建议不要安装以下类型的软件：
    - 将自身代码注入到另一个正在运行的进程中的软件
    - 保护驱动程序
    - 防病毒应用程序，包括 Windows Defender
  - 对于依赖高度专业化软件运行的文件，无法保证能够检测到恶意活动。

Kaspersky Next XDR Expert 不会就操作系统上安装的软件的问题发出通知。

创建虚拟机

要创建具有自定义操作系统镜像的虚拟机，需要连接互联网。

要创建虚拟机：

1. *对于自定义模板*，请确保用于创建虚拟机的模板已关闭：
   a. 在 Sandbox Web 界面中，转到**“模板和存储”**→**“模板”**。
   b. 选择模板。
   c. 如果模板已启用，请从**“关机”**下拉列表中选择其中一个选项：
      - **关机**，如果您想关闭系统同时保存正在运行的应用程序的结果。
      - **断电**，如果您想关闭系统而不保存结果。
2. 在 Sandbox Web 界面中，转到**“虚拟机”**。
3. 单击“**创建 VM**”。
4. 在**“模板”**下拉列表中，选择一个模板。
5. *对于自定义操作系统*：指定虚拟机**名称**和可选的**描述**。
6. 单击“**保存**”按钮。
7. *对于预配置的操作系统*：分发包中的某些操作系统需要接受最终用户授权许可协议的条款。请阅读最终用户授权许可协议的文本，然后单击**“接受”**。
8. *对于自定义操作系统*：如果您要创建虚拟机的服务器未配置互联网访问，则*“模板”*窗口中将显示**“无互联网访问”**错误消息。要完成虚拟机创建过程，您必须下载调试符号。

安装虚拟机

要安装运行预配置操作系统的虚拟机：

1. 在 Sandbox Web 界面中，转到**虚拟机 → 预配置**。
2. 在“**未安装的虚拟机**”部分，单击“**安装就绪的虚拟机**”。

要安装运行自定义操作系统的虚拟机：

1. 在 Sandbox Web 界面中，转到**虚拟机 → 自定义**。
2. 在列表中找到虚拟机，然后在“**操作**”列中单击“**安装**”。
3. 安装虚拟机后，在“**操作**”列中单击“**启用**”。

下载调试符号

如果安装了自定义映像的虚拟机的服务器未配置互联网访问，则必须下载 Microsoft 调试符号才能正确完成虚拟机安装。

> 为了正确下载调试符号，用于虚拟机模板的操作系统必须安装 Windows 调试工具，并且连接到网络的主机名必须仅包含拉丁字母、数字和特殊字符。

下载调试符号：

1. 在 Sandbox Web 界面中，转到**“模板和存储”**→**“模板”**。
2. 选择模板。
3. 在显示“**无网络连接**”错误的窗口中，单击“**下载清单文件**”。

   > 只有当虚拟机状态变为“**失败**”时，才能**下载清单文件**。

4. 解压下载的压缩包。
5. 使用 Windows PowerShell 运行 sbsymtool.ps1。
   此脚本会下载一个包含调试符号的压缩包。
6. 在 Sandbox Web 界面中，转到**“模板和存储”**→**“模板”**。
7. 选择已下载调试符号的模板。
8. 在“**操作**”下拉列表中，选择“**上传符号**”。
9. 在打开的窗口中，选择包含调试符号的压缩包，然后单击“**打开**”。

调试符号已下载。

配置 OSMP 以使用检测技术

Kaspersky Next XDR Expert 使用不同的检测技术（例如反恶意软件引擎或 Sandbox）来检测威胁。您需要配置 OSMP 才能使用这些检测技术。

反恶意软件引擎

对于反恶意软件引擎，请执行以下操作：

- 配置反病毒数据库的更新获取。
- 创建受密码保护的存档的密码列表。

沙盒

安装并配置 Sandbox，并在其中安装虚拟机后，您需要执行以下操作：

- 配置反病毒数据库的更新获取。
- 选择要扫描对象的操作系统。
- 如果您要使用自定义操作系统，请创建自定义 Sandbox 规则。
- 配置从 Endpoint Agent 发送文件。

YARA

对于YARA扫描，请执行以下操作：

导入 YARA 规则

IOC

对于IOC扫描，请执行以下操作：

- 配置定期IOC扫描
- 导入 IOC 规则

更新沙盒和反恶意软件引擎的反病毒数据库

扫描对象时，沙箱和反恶意软件引擎需要最新的反病毒数据库，因此应定期更新反病毒数据库。作为更新源，您可以使用卡巴斯基服务器或您自己的更新源，该更新源可以是 HTTP 服务器、FTP 服务器或文件夹。

Kaspersky Next XDR Expert 每隔 30 分钟自动从指定来源查找新的更新包。您也可以随时手动更新防病毒数据库。

要配置沙箱和反恶意软件引擎获取更新，您必须具有以下XDR 角色之一：主管理员、SOC 管理员、租户管理员、审计员。
具有审计员角色的用户只能查看当前更新源。具有其他角色的用户可以查看和更改更新源。

要配置沙盒和反恶意软件引擎的更新获取：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击**根**租户（无法在其他租户中更改更新设置）。
   这将打开“租户属性”窗口。
3. 选择“**设置**”选项卡。
4. 在“**正在扫描**”部分，选择“**更新数据库**”选项卡。
5. 在“**更新源**”下拉列表中，选择以下更新源之一：
   - **卡巴斯基更新服务器(安全连接)**
     Kaspersky Next XDR Expert 通过 HTTPS 连接到卡巴斯基更新服务器并下载最新的数据库。建议使用 HTTPS 来下载数据库更新。
   - **卡巴斯基更新服务器**
     Kaspersky Next XDR Expert 通过 HTTP 连接到卡巴斯基更新服务器并下载最新的数据库。
   - **自定义服务器**
     Kaspersky Next XDR Expert 会连接到您的更新源以下载最新的数据库。在**URL 或文件夹路径**中指定更新来源的路径。它可以是 HTTP 或 FTP 服务器的 URL，也可以是包含更新包的文件夹的完整路径。
6. 如果要立即更新反病毒数据库，请单击“**更新**”。
7. 单击“**保存**”按钮。

已配置沙盒和反恶意软件引擎的更新获取。Kaspersky Next XDR Expert在**更新于**字段中显示有关最新更新的信息。

您可以随时单击**更新**按钮以手动更新病毒数据库。

创建受密码保护的存档的密码列表

默认情况下，Kaspersky Next XDR Expert无法扫描受密码保护的存档中的对象。此类存档必须先解压缩。您可以创建一个组织内常用存档密码列表。Kaspersky Next XDR Expert 在扫描存档时会尝试列表中的密码。如果其中一个密码匹配，Kaspersky Next XDR Expert 将解压缩存档并扫描其中的对象。

要使用受密码保护的压缩文件的密码列表，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、一级分析师、二级分析师、审计员。
具有审计员角色的用户只能查看密码列表。具有其他角色的用户可以查看和编辑该列表。

要创建用于解压缩受密码保护的存档的密码列表，请执行以下操作：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击**根**租户（其他租户中的密码列表无法更改）。
   这将打开“租户属性”窗口。
3. 选择“**设置**”选项卡。
4. 在**正在扫描**部分，选择**存档**选项卡。
5. 在**存档密码**字段中，添加用于解压缩受密码保护的存档的密码，每个密码占一行。
6. 如果您想限制对密码列表的访问，请打开**需要密码才能访问密码列表**切换开关，然后**设置访问密码**面板中指定密码。您可以将此密码共享给需要访问受密码保护的存档的密码列表的 OSMP 用户。
   单击**保存**保存访问密码。
   如有必要，您可以稍后通过单击**存档**选项卡上的**更改密码**来更改此密码。
7. 单击**保存**或**保存并关闭**，以保存受密码保护的压缩文件的密码列表。

在 Sandbox 中选择用于扫描对象的操作系统

Sandbox 组件在多个操作系统中运行对象，并分析这些对象的行为以检测恶意活动以及针对性攻击和入侵企业 IT 基础构架的指标。

您可以选择用于扫描对象的操作系统。它可以是预定义集合之一、自定义集合或它们的组合。

要选择一组操作系统：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   这将打开“租户属性”窗口。

3. 选择“**设置**”选项卡。
4. 在Sandbox **服务器**部分，单击**要检查的操作系统**进行检查。
5. 在打开的**编辑操作系统集**面板中，在**操作系统集**下，选择预定义的操作系统集或**自定义**。
   如果要将预设操作系统与自定义操作系统结合使用，请选择“**自定义**”。
6. 如果您选择了**自定义**，则**集内容**下会显示可用操作系统的列表。
   此列表始终包含预设的操作系统。如果在 Sandbox 中没有运行预设操作系统的虚拟机，则该操作系统的状态为**“未知”**。
   如果 Sandbox 服务器上存在运行此操作系统的虚拟机，则该列表包括自定义操作系统。
   选中要包含在集合中的操作系统旁边的复选框。
7. 单击“**保存**”按钮。

用于扫描对象的操作系统集已准备就绪。

对于自定义操作系统集，您还需要创建自定义规则。

创建自定义 Sandbox 规则

如果您已选择自定义操作系统来扫描对象，则还需要创建自定义规则来定义应扫描哪种类型的对象以及在哪个操作系统上进行扫描。

您无需创建规则将要扫描的对象发送到预设的操作系统，Kaspersky Next XDR Expert 会自动将对象发送到那里。

> 自定义规则仅适用于在沙箱网页界面中创建的自定义虚拟机。

要添加自定义 Sandbox 规则：

1. 在主菜单中，前往**监控→资源和服务→Sandbox 规则**。
2. 单击**添加**。
   规则创建窗口打开。
3. 配置以下设置：
   - 如果您希望在规则创建后立即启用它，请打开**规则状态**切换开关。
   - 选择租户所有者。
   - 选择要扫描文件的虚拟机。
     您只能从运行您选择的自定义操作系统的虚拟机中进行选择。
   - 在**匹配条件**下，选择要使用**掩码**、**文件类别**还是**两者都**作为匹配条件。
   - 如果您已选择**掩码**或**两者都**作为匹配条件：
     - 根据规则，指定要发送到沙盒的文件名**掩码**。

您可以指定多个值，每个值占一行。

您可以使用 * 和 ? 通配符。不支持其他通配符。

- 即使其文件扩展名与之前指定的掩码匹配，仍需为必须排除在扫描之外的文件指定可选的**掩码排除项**。

  您可以指定多个值，每个值占一行。

  您可以使用 * 和 ? 通配符。不支持其他通配符。

> 如果在**掩码排除项**设置的**自定义**列表中仅选择了标记为**自定义集**的虚拟机，则可以使用**Sandbox 服务器**字段。如果同时选择了自定义虚拟机和预配置虚拟机，则**掩码排除项**字段将被忽略。

- 如果您已选择**文件类别**或**两者都**作为匹配条件：

  在**文件类别**下拉列表中，选择根据规则要发送到沙盒的文件类别。

- 要限制发送到沙盒的文件大小，请单击**添加文件大小**，然后指定文件的**最小值**和**最大**大小。这样就可以设置多个大小范围。

4. 单击“**保存**”按钮。

该规则出现在自定义 Sandbox 规则列表中。

扫描存档的具体细节

存档扫描方式如下：

1. Kaspersky Next XDR Expert 解压缩该存档。
2. 如果存档中的某些文件符合规则，Kaspersky Next XDR Expert 会发送它们以进行扫描。

带有 MSI 扩展名的文件与存档处理方式类似。

配置从 Endpoint Agent 向 Sandbox 发送文件

Endpoint Agent 可以通过多种方式将文件发送到 Sandbox 进行扫描：

- Endpoint Agent **自动**检测对象并将其提交到 Sandbox 进行扫描。
- Endpoint Agent 用户**手动**提交文件进行扫描。
- Endpoint Agent 发送一个触发了 **IOA 规则**的文件。当设备上触发 IOA规则，并且此IOA规则包含将已检测到的对象发送到沙盒的条件时，Kaspersky Next XDR Expert会自动启动 **获取文件**响应，并启用 **扫描文件**选项。

> 自动向沙箱发送文件可能会显著增加OSMP的负载。

要配置发送文件到 Sandbox 以进行扫描，请执行以下操作：

1. 确保沙盒已与OSMP集成。
2. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
3. 点击目标租户的名称。
   这将打开“租户属性”窗口。
4. 选择“**设置**”选项卡。
5. 在**正在扫描**部分，选择**沙盒**选项卡。
6. 配置设置：
   - 要启用**自动**发送 Endpoint Agent 检测到的文件功能：
     在**将文件从设备发送到 Sandbox 进行分析**下，打开**自动发送文件**切换开关。
     默认情况下已禁用该选项。
   - 要启用用户**手动**发送文件功能：
     在**将文件从设备发送到 Sandbox 进行分析**下，打开**手动发送文件**切换开关。
     默认情况下已禁用该功能。
   - 若要启用在触发IOA**规则**时发送文件的功能：
     在**自动将文件发送到 Sandbox**下，打开**发生文件**切换开关。
     默认情况下已禁用该选项。
7. 单击**保存并关闭**。

已配置向 Sandbox 发送文件。根据扫描结果，Kaspersky Next XDR Expert可能会创建警报。

关于入侵指标、IOC 文件和 IOC 规则

Kaspersky Next XDR Expert 可以扫描设备以查找入侵指标。入侵指标 (IOC) 是数字对象，例如文件哈希值或 IP 地址，它们可能表明存在网络攻击。您可以在 Kaspersky IT encyclopedia 以及 Securelist 中了解有关 IOC 的更多信息。

IOC 文件

多个 IOC 可以合并成一个结构化描述的 *IOC 文件*。此类文件有标准的 *OpenIOC 格式*。

下面是一个简单 IOC 文件的示例。

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="unique
ID in the UUID format" last-modified="date of the last modification of the rule in the YYYY-MM-DDThh:mm:ss format"
xmlns="http://schemas.mandiant.com/2010/ioc">
```

```
  <short_description>Rule name</short_description>
  <authored_by>Rule name</authored_by>
  <authored_date>file creation date in the YYYY-MM-DDThh:mm:ss format</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="Unique ID in the UUID format">
      <IndicatorItem id="Unique ID in the UUID format" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">MD5 hash of the file</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```

您可以使用文本编辑器创建自己的 IOC 文件，并将其保存为 .ioc 扩展名。根据您的 Endpoint Agent 应用程序，您可以使用以下文件中列出的 OpenIOC 术语：

适用于 Kaspersky Endpoint Security for Windows 的 OpenIOC 术语

适用于 Kaspersky Endpoint Security for Linux 的 OpenIOC 术语

由于 Kaspersky Next XDR Expert 不会向 Kaspersky Endpoint Security for Mac 发送 IOC 扫描任务，因此没有适用于 Kaspersky Endpoint Security for Mac 的 OpenIOC 术语列表。

IOC 规则

导入 IOC 规则时，Kaspersky Next XDR Expert 会从 IOC 文件中提取结构化描述，并根据该描述创建规则。

IOC规则可在OSMP控制台界面的IOC规则列表中找到：**监控 → 资源和服务 → IOC 规则**。

导入 IOC 规则

Kaspersky Next XDR Expert从包含IOC规则的文件中导入IOC规则。一个文件只能包含一条IOC规则，因此IOC规则列表也是创建这些规则的IOC文件列表。

IOC 规则列表可在OSMP控制台界面 → **监控** → **资源和服务** → **IOC 规则** 中找到。

要导入 IOC 规则：

1. 在主菜单中，转到 **监控 → 资源和服务 → IOC 规则**。
   IOC 规则列表随即打开。
2. 单击“**导入**”。
3. 在打开的“**导入 IOC 规则**”窗格中，配置以下设置：
   - 在“**租户**”下拉列表中，选择租户。
   - 在“**重要性**”下拉列表中，选择规则的重要性。Kaspersky Next XDR Expert 会将此值分配给因触发 IOC 规则而创建的警报。

- 如果您希望 Kaspersky Next XDR Expert 定期扫描设备中规则所描述的受感染迹象，请开启“**计划扫描**”切换开关（必须先配置定期扫描）。

  您还可以稍后通过开启 IOC 规则列表的“**计划扫描**”列中的切换开关来启用定期扫描。

4. 上传包含 IOC 规则的文件。
5. 单击“**导入**”。

导入的规则出现在 IOC 规则列表中。

导入 YARA 规则

Kaspersky Next XDR Expert使用YARA规则扫描发送到OSMP的文件并扫描设备。

Kaspersky Next XDR Expert 会从包含YARA规则的文件中导入YARA规则。一个文件可以包含多个YARA规则。Kaspersky Next XDR Expert会解析该文件，提取规则并将其添加到规则列表中。无法保证成功导入包含超过 65,535 条规则的文件。

YARA 规则列表可在“OSMP 控制台界面 → **监控** → **资源和服务** → **YARA 规则**”中找到。

导入 YARA 规则：

1. 在主菜单中，转到“**监控** → **资源和服务** → **YARA 规则**”。

   YARA 规则列表随即打开。
2. 单击“**导入**”。
3. 在打开的“**导入 YARA 规则**”窗格中，配置以下设置：

   - 在“**租户**”下拉列表中，选择租户。
   - 默认情况下，任何YARA规则的重要性均为**高度**，且无法更改。Kaspersky Next XDR Expert 会将此值分配给因触发 YARA 规则而创建的警报。
   - 如果您希望Kaspersky Next XDR Expert使用所有导入的规则扫描发送到OSMP的文件，请启用**文件扫描**开关。

     您还可以稍后通过打开YARA规则列表的**文件扫描**列中的开关，将任意规则添加到文件扫描的规则集中。

     > 此功能仅适用于根租户。

   - 指定描述（可选）
4. 上传包含YARA规则的文件。

   文件上传后，Kaspersky Next XDR Expert 会从文件中提取规则，并显示有关提取的规则的信息。
5. 单击“**导入**”。

导入的规则会出现在 YARA 规则列表中。

Kaspersky Next XDR Expert API

Kaspersky Next XDR Expert允许您使用REST API和OpenAPI。

使用REST API

通过使用该 API，您可以从第三方解决方案访问 Kaspersky Next XDR Expert。REST API基于HTTP协议运行，包含一系列请求/响应方法。

REST API Help Swagger: XDR

REST API Help Swagger: KUMA

在 Swagger 页面上，使用"**选择定义**"下拉列表在 KUMA 和 XDR (OSMP) API 集之间切换。

REST API 请求必须发送至以下地址：

https://<api_host>.<smp_domain>/xdr/api/v1/<request>

https://<api_host>.<smp_domain>/xdr/api/v3/kuma/<request>（用于 KUMA 特定 API）

其中，<smp_domain>参数是在Kaspersky Next XDR Expert部署期间配置文件中指定的服务域名。

例如：

https://api.example.com/xdr/api/v1/

https://api.example.com/xdr/api/v3/kuma/（适用于 KUMA 专用 API）

由于REST API请求必须经过授权，因此您需要创建一个令牌。

使用OpenAPI

OpenAPI允许您使用脚本自动执行和自定义管理服务器的管理。OpenAPI还可用于开发自定义客户端应用程序，通过使用基于JSON的同步请求和响应，通过HTTP与Kaspersky Next XDR Expert交互。

OpenAPI请求必须发送到以下地址：

https://api.<smp_domain>:13299

其中，<smp_domain>参数是在Kaspersky Next XDR Expert部署期间配置文件中指定的服务域名。

例如：

https://api.example.com:13299

创建令牌

要生成用户 API 令牌：

1. 在主菜单中，转到“**设置** → **备份**”。
2. 单击“**添加令牌**”按钮。
3. 在“**添加令牌**”面板中，配置令牌选项：
   a. 单击“**到期日期**”并使用日历指定到期日期。如果要禁用令牌的自动到期，请选中“**无到期日期**”复选框。
   最长到期日期范围为 365 天。

   > 建议您为可以访问 POST 方法的令牌启用自动到期。

   b. 选中要允许访问的API 方法旁边的复选框。
   除了 API 方法之外，您还可以选择创建令牌的用途：
   - POST:DynamicClientRegistration，用于动态注册 OAuth 客户端。
   - POST:KSCOpenAPI，用于使用 API 令牌进行 OpenAPI 身份验证。
4. 点击**生成**按钮。
5. 单击“**复制并关闭**”。

> 您以后将无法复制令牌。

令牌已创建并复制到剪贴板。以任何便捷的方式保存令牌。

授权 API 请求

每个 API 请求必须包含基于令牌的授权。使用令牌发出 API 请求的用户必须具有执行此类请求的权限。

每个请求必须附带以下标头：

```
Authorization: Bearer <token>
```

可能的错误

HTTP 代码	Description	message字段值
400	无效标头	无效授权标头
403	令牌不存在或所属用户被禁用	访问被拒绝

使用 Open Single Management Platform

Open Single Management Platform（以下简称 OSMP）是一个开放式技术平台，支持将卡巴斯基应用程序和第三方应用程序集成到单一安全系统中，并提供跨应用程序的场景。Kaspersky Next XDR Expert 基于 OSMP 构建。OSMP Web 界面（以下简称 OSMP 控制台）用于管理 Kaspersky Next XDR Expert。

通过 OSMP 控制台可执行以下操作：

- 管理组织的安全系统状态。
- 查看有关组织网络的安全信息。
- 配置威胁检测、搜索和响应。
- 管理为您网络中的资产所创建的策略。
- 管理网络设备上已安装应用程序的任务。
- 管理用户和角色。
- 对向 Kaspersky Next XDR Expert 的数据迁移进行配置。
- 在网络设备上安装卡巴斯基应用程序，并管理已安装的应用程序。
- 轮询网络以发现客户端设备，并将设备手动或自动分发到管理组。
- 管理 Kaspersky Next XDR Expert 与其他应用程序的集成。

OSMP 控制台是一个多语言 Web 界面。您可以随时更改界面语言，无需重新打开应用程序。

OSMP 控制台中的默认身份验证方法是输入用户名、密码和用于双重身份验证的附加一次性安全代码。从 Kaspersky Next XDR Expert 2.0开始，双重身份验证默认自动启用，并默认禁用登录时配置双重身份验证的选项。

您可以通过Kerberos协议配置域身份验证。域身份验证可让您在 OSMP Console 中启用安全身份验证，而无需在公司网络上重新输入密码（单点登录）。

配置管理服务器

本部分介绍管理服务器的配置过程和属性。

配置管理服务器连接地址

管理服务器连接地址是用于以下用途的网络地址：

- 作为创建网络代理安装包时的默认地址

  安装网络代理后，受管理设备通过此地址连接到管理服务器。

- 作为 KSN 代理服务器地址
  受管理设备通过此地址连接到 KSN 代理服务器。

配置管理服务器连接地址：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**常规**”区域。
3. 在打开的窗口中，在**管理服务器连接地址** 字段中，指定新的管理服务器连接地址。
   连接地址的最大长度为 255 个字符。
   您可以将管理服务器连接地址指定为 NetBIOS 名称、FQDN 或管理服务器的 IP 地址。
4. 单击“**保存**”按钮。

指定的地址用作管理服务器地址和 KSN 代理服务器地址。

配置 OSMP 控制台与管理服务器的连接

您可以通过管理服务器属性或使用管理服务器策略设置来配置 OSMP 控制台与管理服务器的连接。

要通过管理服务器属性设置连接端口：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**连接端口**”区域。
3. 如有必要，请指定**Web Console 的 SSL 端口**设置或指定其他管理服务器连接端口。

所选服务器的主要连接设置已指定。

要通过管理服务器策略设置来设置连接端口：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 单击管理服务器策略的名称，然后转到**应用程序设置**选项卡。
3. 如有必要，请指定**Web Console 的 SSL 端口**设置或指定其他管理服务器连接端口。

> 如果您禁用“**打开 Web Console 的端口**”选项，并且此策略设置将被应用于设备，您将无法使用 OSMP 控制台连接到管理服务器。在这种情况下，连接将被终止。如果您拥有未应用此策略的管理服务器，则可以通过 OSMP 控制台重新连接到该管理服务器。

所选服务器的主要连接设置已指定。

配置互联网访问设置

Kaspersky Next XDR Expert 组件的正常运行需要互联网连接，并且可以用于特定的集成，包括 Kaspersky 和第三方。例如，您必须为管理服务器配置互联网访问，以便使用卡巴斯基安全网络，以及下载 Kaspersky Next XDR Expert 和受管理的卡巴斯基应用程序的反病毒数据库更新。

某些卡巴斯基应用程序的集成设置包含启用或禁用代理服务器使用的选项。例如，当您配置与 Kaspersky 威胁情报门户的集成时，可以使用这样的选项。

指定互联网访问设置：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**配置互联网访问**”区域。

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

   - **地址**

     Kaspersky Next XDR Expert 连接到互联网时使用的代理服务器地址。

   - **端口号**

     用于建立 Kaspersky Next XDR Expert 代理连接的端口号。

   - **对本地地址不使用代理服务器**

     将不会使用代理服务器连接本地网络的设备。

   - **代理服务器身份验证**

     如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

     如果选中“**使用代理服务器**”复选框，则该输入字段可用。

   - **用户名**

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

   - **密码**

     建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

     要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

用于在 Open Single Management Platform 操作的证书

本部分包含有关 Open Single Management Platform 证书的信息，并描述了如何颁发和替换 OSMP Console 证书，以及如何在服务器与 OSMP Console 交互时续订管理服务器证书。

关于 Open Single Management Platform 证书

Open Single Management Platform 使用以下类型的证书来启用应用程序组件之间的安全交互：

- 管理服务器证书
- OSMP 控制台服务器证书
- OSMP 控制台证书

默认情况下，Open Single Management Platform 使用自签名证书（即由 Open Single Management Platform 自行颁发的证书）。如有必要，您可以根据贵组织的安全标准，将自签名证书替换为用户证书。在管理服务器验证自定义证书是否满足所有适用要求之后，该证书将承担与自签名证书相同的功能范围。唯一的区别是自定义证书不会在到期后自动重新颁发。您可以通过 klsetsrvcert 实用程序或通过 OSMP 控制台中的管理服务器属性部分将证书替换为自定义证书，具体取决于证书类型。使用 klsetsrvcert 实用程序时，需要使用以下值之一指定证书类型：

- C—端口 13000 和 13291 的通用证书。
- CR—端口 13000 和 13291 的通用备用证书。

管理服务器证书的最长有效期不得超过 397 天。

管理服务器证书

出于以下目的需要管理服务器证书：

- 连接到 OSMP 控制台时对管理服务器进行身份验证
- 受管理设备上管理服务器和网络代理之间的安全交互
- 主管理服务器连接到从属管理服务器时的身份验证。

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

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

> 管理服务器证书的最长有效期不得超过 397 天。

如果必要，您可以为管理服务器分配自定义证书。例如，为了更好的整合您企业的现有 PKI 或为了证书字段的自定义配置，这可能是必要的。在替换证书时，所有先前通过 SSL 连接到管理服务器的网络代理将丢失连接，并返回“*管理服务器身份验证错误*”消息。要消除该错误，您将必须在证书替换后恢复连接。

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

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

移动证书

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

此外，还存在移动备用（“MR”）证书：它用于无缝替换移动证书。Open Single Management Platform 会在通用证书到期前 90 天自动生成此证书。当移动证书即将到期时，移动备用证书用于保持与受管理移动设备上安装的网络代理实例的连接。为此，移动备用证书会在旧的移动证书到期前 24 小时自动成为新的移动证书。

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

Web 服务器证书

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

Web Server 按优先顺序使用以下证书之一：

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

OSMP 控制台证书

OSMP 控制台服务器拥有自己的证书。当您打开网站时，浏览器会验证您的连接是否可信。Web Console 证书允许您对 Web Console 进行身份验证，并用于加密浏览器和 Web Console 之间的流量。

打开 Web Console 时，浏览器可能会通知您与 OSMP Console 的连接不是私密连接，并且 OSMP Console 证书无效。出现此警告是因为 OSMP Console 证书是自签名的，并且由 Open Single Management Platform 自动生成。要移除此警告，可以执行以下操作之一：

- 将 Web Console 证书替换为自定义证书（推荐选项）。创建在您的基础架构中受信任且满足自定义证书要求的证书。
- 将 Web Console 证书添加到受信任浏览器证书列表中。我们建议您仅在无法创建自定义证书时才使用此选项。

Open Single Management Platform 中使用的自定义证书的要求

下表显示了为不同的 Open Single Management Platform 组件指定的自定义证书的要求。

证书类别	要求	注释
通用证书，通用备用证书（“C”，“CR”）	最小密钥长度：2048 基本限制： • 路径长度限制：无 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法（可选）：服务器身份验证，客户端身份验证。 证书必须包含有效的“主题备用名称（SAN）”，其中包含管理服务器的回环地址： • 对于 IPv4：127.0.0.1 • 对于 IPv6：0:0:0:0:0:0:0:1	扩展密钥用法参数是可选的。 路径长度约束值可以是不同于“无”的整数，但不能小于 1。
移动证书，移动备用证书（“M”，“MR”）	最小密钥长度：2048 基本限制： • CA：true • 路径长度限制：无 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法（可选）：服务器身份验证。	扩展密钥用法参数是可选的。 如果通用证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。
自动生成的用户证书的证书 CA（“MCA”）	最小密钥长度：2048 基本限制： • CA：true • 路径长度限制：无 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法（可选）：服务器身份验证，客户端身份验证。	扩展密钥用法参数是可选的。 如果通用证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。
Web 服务器证书	扩展密钥用法：服务器身份验证。 从中指定证书的 PKCS #12/PEM 容器包括整个公钥链。 证书的主题备用名称 (SAN) 存在；即 `subjectAltName` 字段值有效。 证书符合浏览器对服务器证书施加的有效要求，以及 CA/浏览器论坛 的当前基线要求。	—
OSMP 控制台证书	从中指定证书的 PEM 容器包括整个公钥链。 证书的主题备用名称 (SAN) 存在；即 `subjectAltName` 字段值有效。 证书符合浏览器对服务器证书的有效要求，以及 CA/浏览器论坛 的当前基线要求。	OSMP 控制台不支持加密证书。
Kaspersky Next XDR Expert 公共服务中级证书	PEM 容器包含完整的证书链（或单个证书）以及未加密的私钥。 中间证书必须由您组织的私钥基础架构 (PKI) 颁发。自定义中间证书的有效期必须为 399 天或更长。	—

重新颁发 OSMP 控制台证书

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

不支持自动重新颁发 OSMP Console 证书。您必须手动重新颁发过期的证书。

当您打开 OSMP Console 时，浏览器可能会通知您与 OSMP Console 的连接不是私密连接，并且 OSMP Console 证书无效。出现此警告是因为 OSMP Console 证书是自签名的，并且由 Open Single Management Platform 自动生成。要移除或防止此警告，可以执行以下操作之一：

- 重新颁发证书时指定自定义证书（推荐选项）。创建在您的基础架构中受信任且满足自定义证书要求的证书。
- 重新颁发 OSMP Console 证书后，将该证书添加到受信任浏览器证书列表中。我们建议您仅在无法创建自定义证书时才使用此选项。

要重新颁发过期的 OSMP Console 证书：

通过执行以下操作之一重新安装 OSMP Console：

- 如果要使用相同的 OSMP 控制台安装文件，请卸载 OSMP 控制台，然后安装相同版本的 OSMP 控制台。
- 如果要使用升级版本的安装文件，请运行升级命令。

重新颁发的 OSMP Console 证书的有效期为 397 天。

替换 OSMP 控制台的证书

默认情况下，当您安装 OSMP 控制台服务器（又称“OSMP 控制台”）时，应用程序的浏览器证书会自动生成。您可以使用自定义证书替换自动生成的证书。

要用自定义证书替换 OSMP 控制台的证书：

1. 打开安装 OSMP 控制台时创建的响应文件。
   您可以根据需要创建新的响应文件。
2. 在该文件中，指定以下路径：
   - 使用“`certPath`”参数指定 OSMP 控制台自定义证书文件的路径
   - 使用“`keyPath`”参数指定与 OSMP 控制台自定义证书关联的私钥的路径。

     您必须指定这两条路径。否则，Web 浏览器会不断通知您您的连接不是私密的。

3. 通过指定新的响应文件，重新安装 OSMP 控制台。执行以下操作之一：

   - 如果要使用相同的 OSMP 控制台安装文件，请卸载 OSMP 控制台，然后安装相同版本的 OSMP 控制台。
   - 如果要使用升级版本的安装文件，请运行升级命令。

   OSMP 控制台使用指定的证书。

将 PFX 证书转换为 PEM 格式

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

要在 Linux 操作系统中将 PFX 证书转换为 PEM 格式：

1. 在基于 OpenSSL 的跨平台实用程序中，执行以下命令：

   ```
   openssl pkcs12 -in <文件名.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

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

2. 确保证书文件和私钥生成到存储 .pfx 文件的同一目录中。

3. OSMP Console 不支持受密码保护的证书。因此，在基于 OpenSSL 的跨平台实用程序中运行以下命令，从 .pem 文件中删除密码：

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

   > 输入和输出 .pem 文件不要使用相同名称。

   结果，新的 .pem 文件未加密。无需输入密码即可使用。

.crt 和 .pem 文件已可以使用，因此您可以在 OSMP Console 安装程序中对其进行指定。

场景：指定自定义管理服务器证书

例如，您可以分配自定义管理服务器证书，以便更好地与贵司的现有公钥基础结构 (PKI) 集成，或自定义配置证书字段。建议在安装管理服务器后立即替换证书。

> 管理服务器证书的最长有效期不得超过 397 天。

先决条件

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

证书类型：通用证书，通用备用证书（“C”，“CR”）

要求：

- 最小密钥长度：2048
- 基本限制：
  - CA：true
  - 路径长度限制：无
    路径长度约束值可以是不同于“无”的整数，但不能小于 1。
- 密钥用法：
  - 数字签名
  - 证书签名
  - 密钥加密
  - CRL 签名
- 扩展密钥用法 (EKU)：服务器身份验证，客户端身份验证。EKU 可选，但如果您的证书包含它，则必须在 EKU 中指定服务器和客户端身份验证数据。
- 证书必须包含有效的“主题备用名称（SAN）”。
- `subjectAltName`字段必须包含管理服务器回环地址：
  - 对于 IPv4：127.0.0.1
  - IPv6：0:0:0:0:0:0:0:1

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

阶段

指定管理服务器证书分阶段进行：

1. **替换管理服务器证书**

   为此目的使用命令行 klsetsrvcert utility。

2. **指定新证书并恢复网络代理与管理服务器的连接**

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

结果

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

使用 klsetsrvcert 实用程序替换管理服务器证书

要替换管理服务器证书，

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke ksc --action klsetsrvcert \
  --param ksc_server_certificate="<新证书路径>" \
  --param ksc_server_cert_pass="<密码>"
```

其中：

- < 新证书路径 > 是包含 PKCS #12 格式证书和私钥的容器的路径（扩展名为 .P12 或 .PFX 的文件）。
- < 密码 > 是用于保护 PKCS #12 容器的密码。证书和私钥存储在容器中，因此需要密码才能解密容器文件。如果密码包含双引号，请使用反斜杠 (\") 将其转义。

默认情况下，未指定证书验证参数，使用没有签名权限的自定义证书。您可以替换端口 13000 的通用证书。

> 您无需下载 klsetsrvcert 实用程序。该证书包含在 Kubernetes 集群中，不能直接运行。您只能使用管理员主机上的 KDT 运行 klsetsrvcert 实用程序。

使用 klmover 实用程序将网络代理连接到管理服务器

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

要指定新的管理服务器证书并恢复连接：

从命令提示符运行以下实用程序：

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

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

klmover 实用程序参数的描述如下表所示。

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

管理服务器层级

一些客户公司，例如 MSP，可能运行多个管理服务器。可能不方便管理几个不同的管理服务器，因此可以应用层次结构。在该层级结构的不同嵌套级别上，每个管理服务器都可以拥有多个从属管理服务器。根管理服务器只能充当主服务器。

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

两个管理服务器的“主/从”配置提供了以下选项：

- 一个从属管理服务器从主管理服务器继承策略、任务、用户角色和安装包，从而防止了重复设置。
- 主管理服务器上的设备分类可以包含从属管理服务器的设备。
- 主管理服务器的报告和事件分类可以包含从属管理服务器的数据（包括详细信息）。
- 主管理服务器可以用作从属管理服务器的更新源。

主管理服务器仅接收来自上面列出的选项范围内的非虚拟从属管理服务器的数据。此限制不适用于虚拟管理服务器，虚拟管理服务器与其主管理服务器共享数据库。

创建管理服务器层级：添加从属管理服务器

在层次结构中，基于 Linux 的管理服务器既可以作为主服务器也可以作为辅助服务器。基于 Linux 的主服务器可以管理基于 Linux 和基于 Windows 的从属服务器。基于 Windows 的主服务器可以管理基于 Linux 的从属服务器。根管理服务器只能充当主服务器。

您可以添加管理服务器作为从属管理服务器，从而建立“主/从属”层级。

要添加可以通过 OSMP 控制台连接的从属管理服务器：

1. 确保未来主管理服务器的端口 13000 可用于从从属管理服务器接收连接。
2. 转到未来主管理服务器的属性：
   a. 在主菜单中，选择一个区域（**市场**、**控制台导航**和**设置**除外），然后在页面顶部单击**显示层级**按钮。
   b. 在打开的导航窗格中，将鼠标光标悬停在所需管理服务器的名称上，然后单击设置图标 (⚙)。
   或者，您可以单击管理服务器名称，然后在主菜单中显示该名称后，在主菜单中单击该名称以打开服务器属性窗口。
3. 在打开的属性窗口中，单击“**管理服务器**”选项卡。
4. 选择您要向其添加管理服务器的管理组名称旁边的复选框。
5. 在菜单行中，单击“**连接从属管理服务器**”。
   “添加从属管理服务器向导”启动。使用“**NEXT**”按钮继续完成向导。
6. 填充以下字段：
   - **从属管理服务器显示名称**

     从属管理服务器将显示在层级的名称。如果需要，您可以输入 IP 地址作为名称，也可以使用名称，例如“组 1 的从属服务器”。
   - **从属管理服务器地址(可选)**

     指定从属管理服务器的 IP 地址或域名。
     如果启用了“**连接主管理服务器到 DMZ 中的从属管理服务器**”选项，则需要此参数。
   - **管理服务器 SSL 端口**

     指定主管理服务器上的 SSL 端口号。默认端口号是 13000。
     端口 13000 用于根管理服务器；此端口号无法更改。
   - **管理服务器 API 端口**

     Web Console 将用于通过 OpenAPI 接收来自从属管理服务器的连接的端口号。默认端口号是 13299。

     构建层级结构时，Web Console 会连接到未来的从属服务器，请求凭证，检索公共证书并执行初始设置。

     管理服务器层级结构构建完成后，将不再使用端口 13299。管理服务器将通过端口 13000 进行交互。
   - **连接主管理服务器到 DMZ 中的从属管理服务器**

     如果从属管理服务器位于隔离区 (DMZ)，选择该选项。
     如果选择此选项，主管理服务器将发起与从属管理服务器的连接。否则，从属管理服务器将发起与主管理服务器的连接。
7. 指定未来从属服务器的证书。
   向导已完成。

8. 将未来主管理服务器的证书文件发送给未来从属管理服务器所在办公室的系统管理员。（例如，您可以将文件写入闪存驱动器等外部设备，或通过电子邮件发送它。）

   证书文件位于未来的主管理服务器上的 /var/opt/kaspersky/klnagent_srv/1093/cert/ 中。

9. 提示未来从属管理服务器的责任系统管理员做以下事情：

   a. 单击管理服务器名称。

   b. 在打开的属性页面上，转到“**常规**”选项卡的“**管理服务器层级**”区域。

   c. 选择**该管理服务器是服务器层级中的从属**选项。

   > 根管理服务器只能充当主服务器。

   d. 在“**主管理服务器地址**”字段中，输入将来的主管理服务器的网络名称。

   e. 通过单击“**浏览**”选择先前保存的带有未来主管理服务器证书的文件。

   f. 如有必要，选中“**连接主管理服务器到 DMZ 中的从属管理服务器**”复选框。

   g. 如果通过代理服务器连接到未来主管理服务器，请选中 **使用代理服务器** 复选框并指定连接设置。

   h. 单击“**保存**”按钮。

“主/从属”层级被创建。主管理服务器开始使用端口 13000 从从属管理服务器接收连接。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

查看从属管理服务器列表

要查看从属（包括虚拟）管理服务器列表：

1. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外）。

2. 在页面顶部，单击“**显示层级**”按钮。

   在打开的导航窗格中，显示辅助（包括虚拟）管理服务器的列表。您可以通过单击名称转到任一管理服务器。

> 如果您从“**IP 范围**”和“**已删除对象**”区域打开了导航窗格，则无法转到虚拟管理服务器。
> 此外，还会显示管理组。如果您从以下区域打开导航窗格，则可以管理这些组：“**资产(设备)**”、“**策略**”、“**任务**”和“**分发点**”。否则，这些组将显示为灰色。

如果您在 OSMP 控制台中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，则可以使用以下方法之一：

- **修改现有的 OSMP 控制台安装，以将从属服务器添加到受信任的管理服务器列表中**。然后您将能够在 OSMP 控制台中连接到该虚拟管理服务器。

  1. 在安装了 OSMP 控制台的设备上，使用具有管理权限的账户运行与您设备上安装的 Linux 分发包相对应的 OSMP 控制台安装文件。

     安装向导将启动。使用**下一步**按钮继续向导操作。

2. 选择**升级**选项。

3. 在“**修改类型**”步骤中，选择“**编辑连接设置**”选项。

4. 在“**受信任的管理服务器**”步骤中，添加所需的从属管理服务器。

5. 在最后一步中，单击**修改**以应用新设置。

6. 在应用程序重新配置成功完成后，单击“**完成**”按钮。

- 使用 OSMP 控制台直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 OSMP 控制台中切换到该虚拟管理服务器。

管理虚拟管理服务器

本部分介绍管理虚拟管理服务器的以下操作：

- 创建虚拟管理服务器
- 启用和禁用虚拟管理服务器
- 为虚拟管理服务器分配管理员
- 更改客户端设备的管理服务器
- 删除虚拟管理服务器

创建虚拟管理服务器

您可以创建虚拟管理服务器并添加它们到管理组。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。

要创建和添加虚拟管理服务器：

1. 在主菜单中，单击管理服务器名称。

2. 在打开的页面上，转到“**管理服务器**”选项卡。

3. 选择您要添加虚拟管理服务器到的管理组。
虚拟管理服务器将管理选定组（包括子组）中的设备。

4. 在菜单行中，单击“**新虚拟管理服务器**”。

5. 在打开的页面上，定义新虚拟管理服务器的属性：

   - **虚拟管理服务器名称**。
   - **管理服务器连接地址**

     您可以指定管理服务器的名称或 IP 地址。

6. 从用户列表中，选择虚拟管理服务器管理员。如果您想，您可以编辑现有账户之一，然后分配其管理员角色，或创建一个新用户账户。

   如有必要，您可以使用 kladduser 实用程序创建一个将充当虚拟管理服务器管理员的新账户。为此，请使用以下命令：

   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```

   其中`virtual_server_name`是虚拟管理服务器的名称。

7. 单击“**保存**”按钮。

新的虚拟管理服务器将创建，添加到管理组并显示在“**管理服务器**”选项卡上。

如果您已在 OSMP 控制台中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，则可以使用以下方法之一：

- **修改现有的 OSMP 控制台安装，以将从属服务器添加到受信任的管理服务器列表中**。然后您将能够在 OSMP 控制台中连接到该虚拟管理服务器。

  1. 在安装了 OSMP 控制台的设备上，使用具有管理权限的账户运行与您设备上安装的 Linux 分发包相对应的 OSMP 控制台安装文件。

     安装向导将启动。使用**下一步**按钮继续向导操作。

  2. 选择**升级**选项。
  3. 在“**修改类型**”步骤中，选择“**编辑连接设置**”选项。
  4. 在“**受信任的管理服务器**”步骤中，添加所需的从属管理服务器。
  5. 在最后一步中，单击**修改**以应用新设置。
  6. 在应用程序重新配置成功完成后，单击“**完成**”按钮。

- 使用 OSMP 控制台直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 OSMP 控制台中切换到该虚拟管理服务器。

启用或禁用虚拟管理服务器

当您创建新的虚拟管理服务器时，默认情况下会启用它。您可以随时禁用或再次启用它。禁用或启用虚拟管理服务器等同于关闭或打开物理管理服务器。

要启用或禁用虚拟管理服务器：

1. 在主菜单中，单击管理服务器名称。
2. 在打开的页面上，转到“**管理服务器**”选项卡。

3. 选择要启用或禁用的虚拟管理服务器。

4. 在菜单行上，单击“**启用/禁用虚拟管理服务器**”按钮。

虚拟管理服务器状态被更改为已启用或禁用，具体取决于其先前的状态。更新的状态将显示在管理服务器名称旁边。

为虚拟管理服务器分配管理员

当您在组织中使用虚拟管理服务器时，可能希望为每个虚拟管理服务器分配一名专门的管理员。例如，当您创建虚拟管理服务器来管理组织的独立办公室或部门时，或者如果您是 MSP 提供商并通过虚拟管理服务器来管理您的租户时，这可能很有用。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。如果您想要仅为虚拟管理服务器分配管理员，请确保该管理员没有主管理服务器的访问权限。

您可以通过向管理员授予虚拟管理服务器的访问权限来为虚拟管理服务器分配管理员。您可以通过以下方式之一授予所需的访问权限：

- 手动配置管理员的访问权限
- 为管理员分配一个或多个用户角色

要登录 OSMP Console，虚拟管理服务器的管理员要指定虚拟管理服务器名称、用户名和密码。OSMP Console 会对管理员进行身份验证并打开管理员有权访问的虚拟管理服务器。管理员不能在管理服务器之间切换。

先决条件

在开始之前，请确保满足以下条件：

- 虚拟管理服务器已创建。
- 在主管理服务器上，您已为希望为其分配虚拟管理服务器的管理员创建一个账户。
- 您在“**修改对象 ACL** right in the **常规功能** → **用户权限**“修改对象 ACL”权限。

手动配置访问权限

要为虚拟管理服务器分配管理员：

1. 切换到所需的虚拟管理服务器：

   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。

   b. 在打开的导航窗格中，单击所需虚拟管理服务器的名称。

> 您无法从“**IP 范围**”和“**已删除对象**”区域切换到虚拟管理服务器。

在主菜单中，管理服务器将更改为您选择的服务器。

2. 在主菜单中单击管理服务器的名称，移动到其属性。
   或者，在导航窗格中，将鼠标光标悬停在所需虚拟管理服务器的名称上，然后单击设置图标 (⚙)。
   管理服务器属性窗口将打开。

3. 在“**访问权限**”选项卡上，单击“**添加**”按钮。
   系统会打开主管理服务器和当前虚拟管理服务器的用户的统一列表。

4. 从用户列表中，选择要为虚拟管理服务器分配的管理员帐户，然后单击**确定**按钮。
   应用程序将选定的用户添加到**访问权限**选项卡上的用户列表中。

5. 选中已添加帐户旁边的复选框，然后点按**访问权限**按钮。

6. 配置管理员将拥有的虚拟管理服务器的权限。
   要成功进行身份验证，管理员至少必须具有以下权限：

   - 在**常规功能→基本功能**区域中**读取**权限
   - 在**常规功能→虚拟管理服务器**功能区域中**读取**权限

应用程序将修改后的用户权限保存到管理员账户中。

要为多个虚拟管理服务器分配管理员：

1. 在主菜单中，单击主管理服务器名称。

2. 在打开的页面上，转到**访问权限**选项卡，然后单击**分配**。
   在打开的**添加用户或组**窗口中，选中要指定为管理员的用户旁边的复选框。

3. 您可以切换到**组**选项卡来选择用户群组。

4. 单击“**下一步**”。

5. 选择要为其分配管理员的服务器，然后单击**下一步**。

6. 如有必要，选择要为用户设置的管理员角色。
   如果要为用户设置当前管理服务器的自定义角色，请转到所需管理服务器的属性，单击**设置角色**，然后选择自定义角色。

7. 单击**完成**以应用更改。

具有所选角色的管理员随即分配给多个虚拟管理服务器。

要撤销管理员访问权限：

1. 切换到所需的管理服务器。

2. 在主菜单中，单击管理服务器名称。

3. 在打开的页面上，前往**访问权限**选项卡。

4. 选中要撤销其访问权限的用户旁边的复选框。

5. 单击**撤销**并确认您的操作。

所选用户的访问权限已被撤销。

通过分配用户角色配置访问权限

或者，您可以通过用户角色向虚拟管理服务器管理员授予访问权限。例如，如果您想在同一个虚拟管理服务器上分配多个管理员，这可能很有用。如果是这种情况，您可以为管理员账户分配相同的一个或多个用户角色，而不是为多个管理员配置相同的用户权限。

通过分配用户角色为虚拟管理服务器分配管理员：

1. 在主管理服务器上，创建一个新的用户角色，然后指定管理员在虚拟管理服务器上必须拥有的所有所需访问权限。您可以创建多个角色，例如，如果您想要单独访问不同的功能区域。

2. 切换到所需的虚拟管理服务器：

   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。

   b. 在打开的导航窗格中，单击所需虚拟管理服务器的名称。

   > 您无法从“**IP 范围**”和“**已删除对象**”区域切换到虚拟管理服务器。

   在主菜单中，管理服务器将更改为您选择的服务器。

3. 向管理员账户分配新角色或多个角色。

应用程序向管理员账户分配角色。

配置对象级别的访问权限

除了分配功能区域级别的访问权限，您还可以在虚拟管理服务器上配置对特定对象的访问，例如对特定管理组或任务的访问。为此，请切换到虚拟管理服务器，然后在对象的属性中配置访问权限。

更改客户端设备的管理服务器

您可以使用“*更改管理服务器*”任务来更改管理客户端设备的管理服务器。任务执行完毕后，选定的客户端设备将由指定的管理服务器管理。

> 您不能对通过连接网关连接到管理服务器的客户端设备使用*更改管理服务器*任务。对于此类设备，您必须重新配置网络代理或重新安装网络代理并指定连接网关。

要更改管理客户端设备的管理服务器：

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在向导的“**新任务设置**”步骤中，指定以下设置：
   a. 在“**应用程序**”下拉列表中，选择“**Open Single Management Platform**”。
   b. 在**任务类型**字段中，选择**更改管理服务器**。
   c. 在**任务名称**字段中，指定您正在创建的任务的名称。
      任务名称不能超过 100 个字符并且不能包括任何特殊字符 ("*<>?\:|)。
   d. 选择要将任务分配到的设备：
      - **分配任务到管理组**

        任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
        例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。
        如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。
      - **手动指定设备地址或从列表导入地址**

        您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。
        您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。
      - **分配任务到设备分类**

        该任务被分配到设备分类中的设备。您可以指定现有分类之一。
        例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。
4. 在向导的**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。
5. 在向导的该步骤，确认您同意更改客户端设备的管理服务器的条款。
6. 在向导的该步骤，选择要用于管理选定设备的管理服务器：
   - **更改到另一个主管理服务器**

     要将客户端设备移动至另一台主管理服务器，请指定以下管理服务器连接设置：
     1. 在**管理服务器地址**字段中，指定新的主管理服务器的地址。
     2. 在**端口号**字段中，指定要连接到管理服务器的端口号。
        默认端口号是 14000。
     3. 在**SSL 端口**字段中，指定主管理服务器上的 SSL 端口号。
        默认端口号是 13000。

4. 如有必要，请启用**使用代理服务器**选项。

   如果此选项被禁用，则使用直接连接将设备连接到管理服务器。

   如果此选项被启用，请指定代理服务器参数：

   - **代理服务器地址**
   - **代理服务器端口**

   如果您的代理服务器需要身份验证，请在**用户名** 和 **密码**字段中指定与代理服务器建立连接的账户的凭据。我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

5. 如有必要，请上传新的管理服务器证书。

- **在该主服务器上更改到另一个虚拟服务器**

  选择此选项可以将客户端设备移动到当前主管理服务器上的虚拟管理服务器。为此，在**虚拟管理服务器名称**下拉列表中，选择必要的虚拟管理服务器。

7. 在向导的**选择账户以运行任务**步骤中，指定账户设置：

   - **默认账户**

     在与执行该任务的应用程序相同的账户下运行该任务。

     默认情况下已选定该选项。

   - **指定账户**

     填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

     - **账户**

       运行该任务的账户。

     - **密码**

       任务运行时使用的账户的密码。

8. 如果要更改默认任务设置，请在向导的**完成任务创建**步骤中启用**创建完成时打开任务详情**选项。

   如果您不启用该选项，任务使用默认设置创建。您可以稍后随时更改默认设置。

9. 单击“**完成**”按钮。

   任务被创建并显示在任务列表。

10. 单击创建的任务的名称以打开任务属性窗口。

11. 如果要更改默认任务设置，请在任务属性窗口中根据需要指定常规任务设置。

12. 单击“**保存**”按钮。

    任务被创建和配置。

13. 运行创建的任务。

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

删除虚拟管理服务器

如果删除虚拟管理服务器，在管理服务器上创建的所有对象（包括策略和任务）也将被删除。由虚拟管理服务器管理的管理组中的受管理设备将被从管理组中删除。要返回 Kaspersky Next XDR Expert 管理的设备，请运行网络轮询，然后将找到的设备从未分配的设备组移动到管理组。

要删除虚拟管理服务器：

1. 切换到要删除的虚拟管理服务器所属的主物理管理服务器：
   a. 在主菜单中，选择一个区域（**市场**、**控制台导航**和**设置**除外），然后在页面顶部单击**显示层级**按钮。
   b. 在打开的导航面板中，点击主物理管理服务器的名称。
   在主菜单中，管理服务器将更改为您选择的服务器。
2. 通过以下方式之一移动到主物理管理服务器的属性：
   - 在导航面板中，将鼠标光标悬停在所需管理服务器的名称上，然后点击设置图标（⚙）。
   - 在主菜单中，单击管理服务器名称。
3. 在打开的属性窗口上，转到“**管理服务器**”选项卡。
4. 选择要删除的虚拟管理服务器。
5. 在菜单项目上，单击“**删除**”按钮。

虚拟管理服务器被删除。

配置管理服务器连接事件记录

操作期间的连接历史和到管理服务器的连接尝试可以被保存到文件。文件中的信息允许您跟踪不仅您的网络基础设施中的连接，还有非授权的到服务器的访问尝试。

要记录连接管理服务器事件：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**连接端口**”区域。
3. 启用“**记录管理服务器连接事件**”设置。

后续所有入站连接到管理服务器的事件、身份验证结果和 SSL 错误将被保存至 /var/opt/kaspersky/klnagent_srv/logs/SC.syslog 文件。

设置事件存储库中的最大事件数量

在管理服务器属性窗口的“**事件存储库**”部分，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入操作系统日志。新事件被列队，然后在删除操作后被保存到数据库。默认情况下，事件队列限制为 20,000 个事件。您可以通过编辑 KLEVP_MAX_POSTPONED_CNT 标记值来自定义队列限制。

要限制存储在管理服务器事件存储库中的事件的数量：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**事件存储库**”区域。指定存储在数据库中的最大事件数量。
3. 单击“**保存**”按钮。

此外，您可以执行以下操作：

- 更改任何任务的设置以保存与任务进度相关的事件，或者仅保存任务执行结果。
- 减少或禁用安装在受管理设备上的管理服务器、网络代理和卡巴斯基应用程序的事件的存储期限。

为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

更改 DBMS 凭据

有时，您可能需要更改 DBMS 凭据，例如，出于安全目的执行凭据循环。

更改管理服务器数据库凭证

在 Linux 环境中更改管理服务器和 IAM 数据库凭证：

1. 停止管理服务器。根据 Kaspersky Security Center Linux 的部署类型，使用根账户运行以下命令之一：
   - 对于 Kaspersky Security Center Linux 故障转移集群：
     在活动节点上，运行以下命令：

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

- 对于地理分布式 Kaspersky Security Center Linux 故障转移集群：
  在两个节点上，运行以下命令：

  ```
  crm node standby
  ```

- 对于非集群管理服务器部署：
  运行以下命令：

  ```
  systemctl stop kladminserver_srv.service
  systemctl stop kliam_srv.service
  ```

2. 使用 DBMS 超级用户权限连接到管理服务器数据库，并运行以下命令：

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   其中，`<old_kscdbadmin>` 是管理服务器之前用于连接其数据库的 DBMS 帐户，`<new_kscdbadmin>` 是新的 DBMS 帐户。

3. 使用 DBMS 超级用户权限连接到 IAM 数据库，并运行以下命令：

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   其中，`<old_iamdbadmin>` 是管理服务器之前用于连接其数据库的 DBMS 帐户，`<new_iamdbadmin>` 是新的 DBMS 帐户。

4. IAM配置文件位于：/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. 在 `dbms_iam` 部分，在用户和密码字段中指定新帐户凭据。确保该账户存在于 DBMS 中，并被指定为 IAM 数据库所有者。

6. 运行管理服务器。根据 Kaspersky Security Center Linux 的部署类型，使用根账户运行以下命令之一：

   - 对于 Kaspersky Security Center Linux 故障转移集群：
     在活动节点上，运行以下命令：

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - 对于地理分布式 Kaspersky Security Center Linux 故障转移集群：
     在两个节点上，运行以下命令：

     ```
     crm node online
     ```

   - 对于非集群管理服务器部署：
     运行以下命令：

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. 运行klsrvconfig实用程序。

```
sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
```

8. 指定一个新的账户名。您应该指定 DBMS 中存在的账户的凭据。

9. 输入新密码。

10. 指定新密码以确认。

11. 等待管理服务器恢复运行，并等待活动节点上出现一条 syslog 条目，指出管理服务器已准备好执行 GUI 操作。

管理服务器数据库凭据已更改。

管理服务器数据的备份复制与恢复

通过数据备份，您可以将管理服务器数据保存在特定状态，并在需要时（例如，如果管理服务器数据损坏）恢复数据。

备份管理服务器数据之前，请检查虚拟管理服务器是否已添加到管理组。如果添加了虚拟管理服务器，请确保在备份之前为该虚拟管理服务器分配了管理员。备份后，您将无法授予管理员对虚拟管理服务器的访问权限。请注意，如果管理员账户凭据丢失，您将无法向虚拟管理员服务器分配新管理员。

您只能通过运行管理服务器备份任务来创建*管理服务器数据的备份副本*。在部署 Kaspersky Next XDR Expert 时会自动创建此任务。

在主管理服务器上，无法创建和删除"*备份管理服务器数据*"任务。

备份副本保存在 `/var/spool/ksc/backup` 目录中。当您部署 Kaspersky Next XDR Expert 时，会在安装管理服务器的工作节点上自动创建备份目录。在主管理服务器上，您无法更改备份目录路径。

以下数据保存在管理服务器的备份副本中：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）
- 有关管理组和客户端设备结构的配置详情
- 远程安装的应用程序分发包的存储库
- 管理服务器证书

只有使用 KDT 实用程序才能恢复管理服务器数据。

您可以创建 KUMA Core 的备份副本，并在需要时从备份中进行恢复。如果您使用安装在 Kubernetes 集群之外的单独服务器上的 DBMS，则还可以使用第三方工具备份其他 Kaspersky Next XDR Expert 组件。您不能使用第三方工具创建管理服务器数据库备份。

配置管理服务器备份任务

部署 Kaspersky Next XDR Expert 时会自动创建*管理服务器备份*任务，并且无法删除。您只能通过运行*管理服务器备份*任务来创建管理服务器数据的备份副本。

要配置管理服务器数据备份任务：

1. 在主菜单中，转到“**任务**”，然后选择“**管理服务器备份**”任务。
2. 单击“**管理服务器备份**”任务。
   任务属性窗口打开。
3. 如有必要，请根据需要指定常规任务设置。
4. 在“**应用程序设置**”部分，您可以根据需要设置备份保护密码和备份副本数量。
   我们建议限制备份管理服务器数据备份的数量，以避免分配给存储备份的磁盘空间溢出。
5. 单击**保存**以应用更改。

*管理服务器数据备份*任务已配置。

使用 KDT 实用程序来恢复管理服务器数据

“*管理服务器数据备份*”任务允许您复制管理服务器数据以进行备份。要恢复管理服务器数据，您必须使用 KDT 实用程序。

要恢复管理服务器数据：

1. 在 KDT 实用程序所在的管理员主机上，运行以下命令：
   `./kdt invoke ksc --action listBackup`
   显示位于 `/var/spool/ksc/backup` 目录中的备份列表。
2. 执行以下命令：

   ```
   ./kdt invoke ksc --action restoreBackup \
     --param ksc_file_backup="<文件名>" \
     --param ksc_backup_password="<密码>"
   ```

   其中：

   - `ksc_file_backup` 是所需备份压缩文件的路径和压缩文件名称。
   - 如果备份是使用密码保存的，则 `ksc_backup_password` 是压缩文件密码。如果未使用密码，请将 `ksc_backup_password` 变量设置为 `""`。
     如果密码包含双引号，请使用反斜杠 (`\"`) 将其转义。

从所选的备份存档文件中恢复管理服务器数据。

删除管理服务器层级

如果不再想拥有管理服务器层级结构，您可以从该层级将其断开连接。

要删除管理服务器层级：

1. 在主菜单中，单击管理服务器名称。
2. 在打开的页面上，转到“**管理服务器**选项卡。
3. 在要从其中删除从属管理服务器的管理组中，选择从属管理服务器。
4. 在菜单项目上，单击“**删除**”按钮。
5. 在打开的窗口中，单击“**确定**”以确认您要删除该从属管理服务器。

先前的主管理服务器和从属管理服务器现在彼此独立。层级不再存在。

访问公共 DNS 服务器

如果无法使用系统 DNS 访问卡巴斯基服务器，Open Single Management Platform 可以按以下顺序使用这些公共 DNS 服务器：

1. Google Public DNS™ (8.8.8.8)
2. Cloudflare® DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

对这些 DNS 服务器的请求可能包含域地址和管理服务器的公共 IP 地址，因为应用程序建立了到 DNS 服务器的 TCP/UDP 连接。如果 Open Single Management Platform 使用公共 DNS 服务器，则数据处理受相关服务的隐私策略约束。

要通过使用 klscflag 实用程序配置公共 DNS 的使用：

1. 在 KDT 实用程序所在的管理员主机上，运行以下命令以禁用公共 DNS：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1'
```

2. 要启用公共 DNS 的使用，请运行以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0'
```

配置界面

您可以配置 OSMP Console 界面以显示和隐藏不同的区域和界面元素，具体取决于所使用的功能。

要根据当前使用的功能集配置 OSMP Console 界面：

1. 在主菜单中，转到“**设置**” → “**界面选项**”。
2. 启用或禁用所需的选项：
   - **显示数据加密和保护**
   - **显示 MDR 功能**
   - **显示 EDR 警告**
3. 单击“**保存**”按钮。

启用所需选项后，控制台会在主菜单中显示相应的部分。例如，如果您启用**显示 EDR 警告**，则**监控** → **警报**区域会出现在主菜单中。

使用 TLS 的加密通信

要修复您组织企业网络中的漏洞，您可以使用 TLS 协议启用流量加密。您可以在管理服务器上启用 TLS 加密协议和支持的密码套件。Open Single Management Platform 支持 TLS 协议版本 1.0、1.1、1.2 和 1.3。您可以选择所需的加密协议和加密套件。

Open Single Management Platform 使用自签名证书。您也可以使用您自己的证书。建议使用由受信任证书机构颁发的证书。

要在管理服务器上配置允许的加密协议和加密套件：

1. 在 KDT 实用程序所在的管理员主机上，运行以下命令：

   ```
   ./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
   ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <值> -t d'
   ```

   使用 SrvUseStrictSslSettings 标志在管理服务器上配置允许的加密协议和加密套件。

   指定 SrvUseStrictSslSettings 标志的<value>参数：

   - 4 — 仅启用 TLS 1.2 和 TLS 1.3 协议。此外，还启用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密码套件（向后兼容 Kaspersky Security Center 11 需要这些密码套件）。这是默认值。

     TLS 1.2 协议支持的密码套件：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384（具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密码套件）

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

TLS 1.3 协议支持的密码套件：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 — 仅启用 TLS 1.2 和 TLS 1.3 协议。对于 TLS 1.2 和 TLS 1.3 协议，支持下面列出的特定密码套件。

TLS 1.2 协议支持的密码套件：

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

TLS 1.3 协议支持的密码套件：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

我们不建议使用 0、1、2 或 3 作为 SrvUseStrictSslSettings 标志的参数值。这些参数值对应于不安全的 TLS 协议版本（TLS 1.0 和 TLS 1.1 协议）和不安全的密码套件，仅用于向后兼容早期 Kaspersky Security Center 版本。

2. 重启以下 Open Single Management Platform 服务：

- 管理服务器
- Web 服务器
- 激活代理

使用 TLS 协议进行流量加密被启用。

您可以使用 KLTR_TLS12_ENABLED 和 KLTR_TLS13_ENABLED 标志分别启用对 TLS 1.2 和 TLS 1.3 协议的支持。这些标志默认启用。

要启用或禁用对 TLS 1.2 和 TLS 1.3 协议的支持，

在 KDT 实用程序所在的管理员主机上，运行以下命令之一：

- 要启用或禁用对 TLS 1.2 协议的支持：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <value> -t d'
```

- 要启用或禁用对 TLS 1.3 协议的支持：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <value> -t d'
```

指定标志的 < 值 > 参数：

- `1` — 启用对 TLS 协议的支持。
- `0` — 禁用对 TLS 协议的支持。

发现网络设备

该部分描述网络设备的搜索和发现。

Open Single Management Platform 允许您按照指定条件来查找设备。您可以保存搜索结果到文本文件。

搜索和发现功能允许您查找以下设备：

- Open Single Management Platform 管理服务器及其从属管理服务器的管理组中的受管理设备。
- 由管理服务器及其从属管理服务器管理的未分配设备。

情景：发现网络设备

您必须在安装安全应用程序之前执行设备发现。当所有网络设备被发现时，您可以接收它们的信息并通过策略管理。常规网络轮询用于发现是否有新设备以及先前发现的设备是否仍在网络中。

网络设备发现分步骤进行：

1. **初始设备发现**

   手动执行设备发现。

2. **配置未来轮询**

   确保 IP 范围轮询已启用且轮询计划满足您组织的需要。当配置轮询计划时，使用建议的网络轮询频率。

   如果您的网络包括 IPv6 设备，还可以启用 Zeroconf 轮询。

   如果域中包含联网设备，建议使用域控制器轮询。

   使用基于 Windows 的分发点来轮询 Windows 网络。

您只能使用分发点执行 IP 范围轮询和 Zeroconf 轮询。

3. **设置规则以添加发现的设备到管理组（可选）**

   新设备在网络轮询过程中被检测到后，会显示在网络中。这些设备会自动归入 **未分配的设备** 组。如果需要，可以设置自动将这些设备移至“**受管理设备**”组的规则。您也可以建立保留规则。

   如果您跳过该规则设置步骤，所有新发现的设备都将转到“**未分配的设备**”组并保留在那里。如果需要，可以手动将这些设备移动到“**受管理设备**”组。如果您手动将这些设备移动到“**受管理设备**”组，您可以分析每台设备的信息并决定您是否要将它移动到管理组以及移动到哪个组。

结果

完成方案可以导致如下：

- Kaspersky Security Center 管理服务器发现网络中的设备并提供您它们的信息。
- 未来轮询被设置并根据指定的计划工作。

新发现的设备将按照指定的规则进行分配。如果未配置任何规则，设备将保留在“**未分配的设备**”组中。

Windows 网络轮询

关于 Windows 网络轮询

Kaspersky Next XDR Expert 管理服务器不支持 Windows 网络轮询。使用基于 Windows 的分发点来轮询 Windows 网络。

在快速轮询过程中，分发点只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。在完整轮询中，以下信息被从每个客户端设备请求：

- 操作系统名称
- IP 地址
- DNS 名称
- NetBIOS 名称

快速轮询和完整轮询都需要以下：

- 端口 UDP 137/138、TCP 139、UDP 445、TCP 445、必须在网络中可用。
- SMB 协议已启用。
- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在管理服务器上启用。

- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在客户端设备上启用：
  - 至少一台设备上，如果网络设备数量不超过 32。
  - 对每 32 台网络设备至少一台设备上。

完整轮询仅在快速轮询至少运行了一次时可以运行。

IP 范围轮询

Kaspersky Next XDR Expert 允许您仅使用分发点来轮询 IP 范围。分发点会尝试通过标准 DNS 请求，将指定范围内的每个 IPv4 地址反向解析为对应的 DNS 名称。如果此操作成功，分发点会向接收到的名称发送一个 `ICMP ECHO REQUEST`（与 `ping` 命令功能相同）。如果设备做出响应，有关该设备的信息会被添加到 Kaspersky Next XDR Expert 数据库中。反向名称解析的作用是排除那些可能拥有 IP 地址但并非计算机的网络设备，例如网络打印机或路由器。

该轮询方法依赖正确配置的本地 DNS 服务。它必须具有反向查询域。如果该域未被配置，IP 子网轮询将没有结果。

最初，分发点从分配为分发点的设备的网络设置中获取用于轮询的 IP 范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，则网络 192.168.0.0/24 会自动纳入轮询地址列表。分发点会对 192.168.0.1 至 192.168.0.254 网段内的所有地址进行轮询。

如果仅启用 IP 范围轮询，分发点只能发现具有 IPv4 地址的设备。如果您的网络包括 IPv6 设备，请开启设备的 Zeroconf 轮询。

对于 Microsoft Active Directory 或 Samba 域控制器内所有基于 Linux 的主机，在 `/etc/samba/smb.conf` 文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

使用分发点进行 IP 范围轮询

要使用分发点配置 IP 范围轮询：

1. 打开分发点属性。
2. 转到“**IP 范围轮询**”部分，然后选择“**启用范围轮询**”选项。
   “**IP 范围**”窗口将开启。
3. 指定新 IP 范围的名称。
4. 单击“**添加**”，然后使用地址和子网掩码或起始和结束 IP 地址指定 IP 范围。您还可以单击“**浏览**”按钮来添加一个现有子网。
5. 如果需要，单击“**设置轮询计划**”按钮以指定轮询计划选项。
   轮询仅根据指定的时间表开始。无法手动启动轮询。
   轮询计划选项：
   - **每 N 天**
     轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。

默认下，轮询每天运行一次，从当前系统日期和时间开始。

- **每 N 分钟**

  轮询定期运行，按照指定分钟间隔，从指定的时间开始。

- **按星期中的天数**

  轮询定期运行，在指定星期的指定时间。

- **每月在所选工作日**

  轮询定期运行，在指定月日的指定时间。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已禁用该选项。

6. 启用“**使用 Zeroconf 轮询 IPv6 网络**”选项，使用零配置网络（又称为 *Zeroconf*）自动轮询 IPv6 网络。

   在这种情况下，指定的 IP 范围将被忽略，因为分发点会轮询整个网络。如果分发点运行 Linux，则**使用 Zeroconf 轮询 IPv6 网络**选项可用。要使用 Zeroconf IPv6 轮询，您必须在分发点上安装 avahi-browse 实用程序。

轮询完成后，如果您设置并启用了设备移动规则，新发现的设备将自动纳入“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

域控制器轮询

Open Single Management Platform 支持轮询以下类型的域控制器：

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

对于 Samba 域控制器，Samba 4 用作 Active Directory 域控制器。

当您轮询域控制器时，管理服务器或分发点会检索有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。

如果所有联网设备都是域的成员，我们建议使用域控制器轮询。如果某些联网设备未包含在域中，则域控制器轮询无法发现这些设备。

先决条件

在轮询域控制器之前，请确保启用以下协议：

- 简单身份验证和安全层 (SASL)
- 轻量级目录访问协议 (LDAP)

确保域控制器设备上的以下端口可用：

- 389 用于 SASL
- 636 用于 TLS

对于 Microsoft Active Directory、Samba、FreeIPA 或 ALD Pro 域控制器内的所有基于 Linux 的主机，您需要在`/etc/samba/smb.conf`文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

如果 Microsoft Active Directory 域包含多个域控制器，则不支持在域轮询期间选择特定控制器。将与检测到的第一个域控制器建立连接。为确保与 Microsoft Active Directory 域进行正确的身份验证，证书的“使用者备用名称 (SAN)”字段必须包含此域中包含的所有域控制器的地址，以及 Microsoft Active Directory 域的 NetBIOS 名称。

使用管理服务器进行域控制器轮询

要使用管理服务器轮询域控制器：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**域控制器**”。
2. 单击**配置轮询设置**。
   域控制器轮询设置窗口将打开。
3. 在**轮询**字段中，将切换按钮切换到**已启用**位置。
4. 在**轮询指定域**中，单击**添加**，然后指定域控制器的地址和用户凭据，然后单击**确定**。
5. 在**域控制器轮询设置**窗口中，执行以下操作：
   - 选择要轮询的域控制器的类型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。
   - 如果必要，设置轮询计划。默认间隔是一小时。下次轮询接收的数据会完全替换旧数据。
     有以下轮询计划选项可用：
     - **每 N 天**

       轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
       默认下，轮询每天运行一次，从当前系统日期和时间开始。

- **每 N 分钟**

  轮询定期运行，按照指定分钟间隔，从指定的时间开始。

- **按星期中的天数**

  轮询定期运行，在指定星期的指定时间。

- **每月在所选工作日**

  轮询定期运行，在指定月日的指定时间。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已禁用该选项。

如果您更改域安全组中的用户账户，这些更改将在您轮询域控制器一小时后显示在 Open Single Management Platform 中。

6. 如有必要，请更改要分配给已发现用户帐户的租户。为此，请从**租户**下拉列表中选择所需的租户。
   默认情况下，指定“管理服务器”租户。您可以选择多个租户。
7. 单击**保存**以应用更改。
8. 如果您要立即执行轮询，请单击“**开始轮询**”按钮。

使用分发点进行域控制器轮询

您还可以使用分发点轮询域控制器。基于 Windows 或 Linux 的受管理设备可以充当分发点。

对于 Linux 分发点，支持轮询所有类型的域控制器。
对于 Windows 分发点，仅支持轮询 Microsoft Active Directory 域控制器。
不支持使用 Mac 分发点进行轮询。

要使用分发点配置域控制器轮询：

1. 打开分发点属性。
2. 选择**域控制器轮询**部分。
3. 在**轮询**字段中，将切换按钮切换到**已启用**位置。
4. 如果使用 Linux 分发点，请选择要轮询的域控制器的类型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。
   使用分发点和使用管理服务器配置轮询时，不必指定相同的域控制器类型。

5. 选择要轮询的域控制器。

   如果您使用 Linux 分发点，请在“**轮询指定域**”部分中单击“**添加**”，然后指定域控制器的地址和用户凭据。

   如果您使用 Windows 分发点，则可以选择以下选项之一：

   - **轮询当前域**
   - **轮询整个域森林**
   - **轮询指定域**

6. 如果需要，单击“**设置轮询计划**”按钮以指定轮询计划选项。

   轮询仅根据指定的时间表开始。无法手动启动轮询。

轮询完成后，域结构将显示在**域控制器**部分。

如果设置并启用了设备移动规则，则新发现的设备将自动包含在“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

发现的用户账户可通过 Kerberos 协议在 OSMP 控制台中用于域身份验证。

身份验证和连接到域控制器

与域控制器初始连接时，管理服务器会识别连接协议。该协议用于将来与域控制器的所有连接。

与域控制器的初始连接过程如下：

1. 管理服务器尝试通过 TLS 连接到域控制器。

   默认情况下不需要证书验证。将 KLNAG_LDAP_TLS_REQCERT 标志设置为 1 以强制执行证书验证。

   默认情况下，使用与操作系统相关的证书颁发机构 (CA) 路径来访问证书链。使用 KLNAG_LDAP_SSL_CACERT 标志指定自定义路径。

2. 如果 TLS 连接失败，管理服务器将尝试通过 SASL (DIGEST-MD5) 连接到域控制器。

3. 如果 SASL (DIGEST-MD5) 连接失败，管理服务器将使用通过非加密 TCP 连接的简单身份验证来连接到域控制器。

您可以使用 KDT 命令来配置标志。例如，您可以强制进行证书验证。为此，在 KDT 实用程序所在的管理员主机上运行以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
KLNAG_LDAP_TLS_REQCERT -t d -v 1'
```

配置 Samba 域控制器

Open Single Management Platform 支持仅在 Samba 4 上运行的 Linux 域控制器。

Samba 域控制器支持与 Microsoft Active Directory 域控制器相同的架构扩展。您可以使用 Samba 4 架构扩展启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这是一个可选操作。

我们建议启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这将确保 Open Single Management Platform 和 Samba 域控制器之间的正确交互。

要启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容：

1. 执行以下命令以使用 RFC2307 架构扩展：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 域控制器中启用架构更新。为此，请将以下行添加到 `/etc/samba/smb.conf` 文件：

   ```
   dsdb:schema update allowed = true
   ```

   如果架构更新完成时出现错误，则需要对充当架构主机的域控制器执行完整还原。

对于 Samba 域控制器中的所有基于 Linux 的主机，请在 `/etc/samba/smb.conf` 文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

在客户端设备上使用 VDI 动态模式

虚拟基础架构可以使用临时虚拟机部署企业网络。Kaspersky Next XDR Expert 可检测临时虚拟机，并将其相关信息添加到管理服务器数据库中。用户使用完临时虚拟机后，这些虚拟机将从虚拟架构中移除。然而，以后虚拟机的记录可以保存在管理服务器数据库中。此外，OSMP 控制台中可能会显示不存在的虚拟机。

为防止保存不存在的虚拟机的相关信息，Kaspersky Next XDR Expert 支持虚拟桌面基础架构 (VDI) 动态模式。管理员可以在被安装到临时虚拟机的网络代理安装包的属性中启用支持动态 VDI。

当临时虚拟机被禁用，网络代理通知管理服务器该虚拟机已被禁用。如果虚拟机被成功禁用，它将从连接到管理服务器的设备列表中被移除。如果虚拟机被禁用错误，网络代理没有发送禁用虚拟机的通知到管理服务器，使用备份方案。使用这个方案，和管理服务器尝试同步三次未成功后，虚拟机从连接管理服务器的设备列表移除。

在网络代理安装包属性中启用 VDI 动态模式

要启用 VDI 动态模式，请执行以下操作：

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。
2. 在网络代理安装包的上下文菜单中，选择“**属性**”。

   属性窗口将打开。
3. 在**属性**窗口中，选择“**高级**”部分。
4. 在“**高级**”部分中，选择“**启用 VDI 动态模式**”选项。

   要安装网络代理的设备成为 VDI 的一部分。

将组成 VDI 的设备移至管理组

要将组成 VDI 的设备移至管理组，请执行以下操作：

1. 转到 **资产管理** → **移动规则**。
2. 单击**添加**。
3. 在“**规则条件**”选项卡上，选择“**虚拟机**”选项卡。
4. 将“**这是一台虚拟机**”规则设置为“**是**”，将“**虚拟桌面基础架构的一部分**”设置为“**是**”。
5. 单击“**保存**”。

管理客户端设备

Kaspersky Next XDR Expert 支持您管理客户端设备：

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

您可以使用管理组将客户端设备合并成一组，并作为一个单元进行管理。一个客户端设备只能包含在一个管理组中。**规则条件**可以根据规则条件自动将设备分配到某个组：

- 创建设备移动规则。
- 复制设备移动规则。
- 设备移动规则的条件。

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

受管理设备设置

要查看受管理设备设置：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击带有所需设备名称的链接。

   将显示所选设备的属性窗口。

以下选项卡显示在代表主要设置组的属性窗口的上部：

- **常规**

  此选项卡包括以下区域：

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

    - **名称**

      在该字段中，您可以查看和修改管理组中的客户端设备名称。

    - **描述**

      在该字段中，您可以输入客户端设备的附加描述。

    - **设备状态**

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

    - **设备所有者**

      设备所有者的名称。您可以作为设备所有者，通过单击**管理设备所有者**链接分配或删除用户。

    - **完整组名称**

      包括了客户端设备的管理组。

    - **反病毒数据库上次更新**

      设备上病毒数据库或应用程序最后更新日期。

    - **连接到管理服务器**

      客户端设备上安装的网络代理上一次连接到管理服务器的日期和时间。

    - **上一次可见**

      设备在网络中最后可见的日期和时间。

    - **网络代理版本**

      安装的网络代理的版本。

    - **创建日期**

      在 Open Single Management Platform 中设备创建的日期。

    - **强制同步**

      尽管 Open Single Management Platform 会自动同步受管理设备的状态、设置、任务和策略，但在某些情况下，管理员需要确切了解当前是否已对指定设备执行同步。

      如果您单击**强制同步**按钮，应用程序会将所选设备与管理服务器同步。

- **不断开与管理服务器的连接**

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

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

  选中“**不断开与管理服务器的连接**”选项时的最大设备总数为 300。

  默认情况下已在受管理设备上禁用该选项。此选项在安装了管理服务器的设备上默认启用，即使您尝试禁用它也保持启用状态。

- **会话**

  本部分包含一个表格，其中含有有关当前登录到设备的用户的信息。该表在相应的列中显示以下数据：

  - 用户名。
  - SAM 账户名
  - 用户主体名称
  - 电子邮件地址。

  要正确显示有关域用户会话的信息，必须使用域控制器轮询。

- “**网络**”区域显示有关客户端设备的网络属性的以下信息：

  - **IP 地址**

    设备 IP 地址。

  - **Windows 域**

    包含设备的工作组。

  - **DNS 名称**

    客户端设备的 DNS 域名。

  - **NetBIOS 名称**

    客户端设备名称。

  - **IPv6 地址**

    客户端设备的 IPv6 地址。

- “**系统**”区域提供有关安装在客户端设备上的操作系统的信息。

  - **操作系统**
  - **CPU 架构**
  - **设备名称**
  - **虚拟机类型**

    虚拟机制造商。

- **作为 VDI 一部分的动态虚拟机**

  此行显示客户端设备是否是作为 VDI 一部分的动态虚拟机。

- **OS 内部版本**

- "**保护**"区域提供有关客户端设备上反病毒保护当前状态的以下信息：

  - **可见**

    客户端设备的可见状态。

  - **设备状态**

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

  - **状态描述**

    客户端设备保护和与管理服务器连接的状态。

  - **保护状态**

    该字段显示当前的客户端设备实时保护状态。

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

  - **上一次全盘扫描**

    客户端设备上次执行恶意软件扫描的日期和时间。

  - **检测到的病毒**

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

  - **清除失败的对象**

    客户端设备上的未处理文件数量。

    该字段移动设备上的未处理文件数量。

  - **磁盘加密状态**

    设备本地驱动器上的当前文件加密状态。有关状态的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

    只能在安装了 Kaspersky Endpoint Security for Windows 的受管理设备上加密文件。

  - **查看数据加密错误**

    有关设备上数据加密错误的信息。加密由卡巴斯基应用程序的加密数据功能执行。受管理应用程序通过网络代理将数据从设备传输到管理服务器。

- "**应用程序定义的设备状态**"区域提供有关由安装在设备上的受管理应用程序定义的设备状态的信息。此设备状态可能与 Kaspersky Next XDR Expert 定义的状态不同。

- **应用程序**

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

- **活动策略和策略配置文件**

  此选项卡列出了当前分配给受管理设备上的策略和策略配置文件。

- **任务**

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

  如果未建立连接，则不显示状态，按钮被禁用。

- **事件**

  “**事件**”选项卡将显示选定客户端设备在管理服务器上所记录的事件。

  您可以导出、复制和删除设备事件。

- **安全问题**

  在**安全问题**选项卡上，可以为客户端设备查看、编辑和创建安全问题。安全问题可以通过安装在客户端设备上的受管 Kaspersky 应用程序自动创建，也可以由管理员手动创建。例如，如果用户定期将恶意软件从其可移动驱动器移至设备，则管理员可以创建安全问题。管理员可以在安全问题文本中提供情况的简要说明和建议的操作（例如对于一个用户的纪律性操作），还可以添加链接到用户。

  对其采用了所有必要操作的安全问题被称为*已处理安全问题*。存在的未处理安全问题可被选为将设备的状态更改为*严重*或*警告*的条件。

  此部分包含已为设备创建的安全问题的列表。安全问题按严重级别和类型分类。安全问题类型由创建安全问题的卡巴斯基应用程序定义。选中**已处理**列中的复选框即可突出显示列表上的已处理安全问题。

- **标签**

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

- **高级**

  此选项卡包括以下区域：

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

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

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

  - **可执行文件**。此区域显示在客户端设备上发现的可执行文件。

- **分发点**。该区域提供设备与之交互的分发点列表。

  - **导出到文件**

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

  - **属性**

    单击“**属性**”按钮查看和配置设备与之交互的分发点。

- **硬件注册表**。在此区域，您可以查看客户端设备上安装的硬件的信息。

  如果网络代理安装在运行 Windows 的设备上，它会向管理服务器发送有关设备硬件的以下信息：

  - RAM
  - 大容量存储设备
  - 主板
  - CPU
  - 网络适配器
  - 监控器
  - 视频适配器
  - 声卡

  如果网络代理安装在运行 Linux 或 macOS 的设备上，它会向管理服务器发送有关设备硬件的以下信息（如果该信息由操作系统提供）：

  - 总 RAM 容量
  - 大容量存储设备总容量
  - 主板
  - CPU
  - 网络适配器

- **可用更新**。该区域显示在该设备上发现的未安装的软件更新列表。

- **软件漏洞**。此区域提供有关客户端设备上安装的第三方应用程序中的漏洞信息。

  要将漏洞保存到文件中，请选择要保存的漏洞旁边的复选框，然后单击“**导出到 CSV**”按钮或“**导出到 TXT**”按钮。

  此部分包含以下设置：

  - **仅显示可以被修复的漏洞**

    如果启用此选项，该区域会显示可通过使用补丁修复的漏洞。

    如果禁用此选项，该区域会同时显示可通过使用补丁修复的漏洞，以及未发布补丁的漏洞。

    默认情况下已启用该选项。

- **漏洞属性**

  单击列表中的软件漏洞名称，以在单独的窗口中查看所选软件漏洞的属性。在窗口中，您可以执行以下操作：

  - 忽略此受管理设备上的软件漏洞（在 OSMP Console 中）。
  - 查看该漏洞的建议修复程序列表。
  - 手动指定软件更新以修复漏洞（在 OSMP Console 中）。
  - 查看漏洞实例。
  - 查看现有任务列表以修复漏洞，并创建新任务以修复漏洞。

- **远程诊断**。在此区域，您可以执行远程诊断客户端设备。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，则**事件**选项卡可能会显示所选客户端设备的不完整事件列表。当 DBMS 存储大量事件时就会发生这种情况。您可以通过执行以下操作之一来增加显示的事件数量：

- 删除不必要的事件。
- 减少不必要事件的存储期限。

要查看设备管理服务器上记录的完整事件列表，请使用报告。

检查客户端设备与管理服务器之间的连接。klnagchk 实用程序

您可以通过使用 klnagchk 实用程序手动检查连接和获取客户端设备与管理服务器之间的连接设置信息。klnagchk 实用程序位于网络代理安装文件夹。

从命令行启动时，klnagchk 实用程序能够执行以下操作（根据使用的键值）：

- 显示或记录用以连接设备上网络代理到管理服务器的设置值。
- 将网络代理统计数据（自上次启动以来）和实用程序运行结果记录在事件日志文件中或者显示在屏幕上。
- 尝试在网络代理和管理服务器之间建立连接。

  如果连接尝试失败，实用程序将发送一个 ICMP 包检查装有管理服务器的设备状态。

要使用 klnagchk 实用程序检查客户端设备和管理服务器之间的连接，请执行以下操作：

在安装了网络代理的设备上，以本地管理员账户从命令行启动 klnagchk 实用程序。

实用程序命令行语法：

```
klnagchk [-logfile <文件名>] [-sp] [-savecert <证书文件路径>] [-restart][-sendhb]
```

参数描述：

- `-logfile <文件名>`—将网络代理和管理服务器之间连接设置的值和实用程序操作结果记录到日志文件中。

  默认情况下，信息保存在标准输出流（stdout）中。如果未使用该键值，设置、运行结果和错误信息将显示在屏幕上。

- `-sp`—显示用于在代理服务器上对用户进行身份验证的密码。

  如果是通过代理服务器与管理服务器建立的连接，则使用本密钥。

- `-savecert <文件名>`—将用于访问管理服务器的证书保存到指定文件中。

- `-restart`—实用程序操作完成后启动网络代理。

- `-sendhb`—启动网络代理与管理服务器的同步。

启动后，klnagchk 实用程序将访问网络代理的配置文件并显示连接参数。这些参数在网络代理安装期间和网络代理策略设置中指定：

- `Current device`—客户端设备的 Windows 网络名。

- `Network Agent version`—设备上安装的网络代理版本（带补丁）的完整编号。

- `Server address`—管理服务器地址。

- `Use SSL`—指示连接到管理服务器时是否使用安全连接的参数。

  可能值：

  - 0—不使用安全连接。

  - 1—使用安全连接。

- `Compress traffic`—指示客户端设备和管理服务器之间的流量是否被压缩的参数。

- `Server SSL ports`—使用安全连接与管理服务器通信的有效端口数。

- `Server ports`—使用普通连接与管理服务器通信的有效端口数。

- `Use proxy server`—指示是否使用代理服务器的参数。

  可能值：

  - 0—不使用代理服务器。

  - 1—使用代理服务器。

- `Address`—代理服务器的地址和端口，以冒号分隔。仅当使用代理服务器时才会显示此参数。

- `User name`—用于访问代理服务器的用户名。仅当使用代理服务器时才会显示此参数。

- `Password`—用于访问代理服务器的密码。仅当使用代理服务器时才会显示此参数。要显示代理服务器密码，需要在命令中使用`sp`密钥。

- `Certificate`—指示客户端设备是否具有管理服务器证书的参数。例如，如果网络代理从未成功连接到管理服务器，则证书可能不存在。

  可能值：

  - `not installed`—客户端设备没有管理服务器证书。

  - `present`—客户端设备具有管理服务器证书。

- `Open UDP port`—指示网络代理是否使用 UDP 端口接收来自管理服务器的同步请求的参数。

可能值：

- 0—UDP 端口已关闭，无法接收来自管理服务器的同步请求。
- 1—UDP 端口已打开，可用于接收来自管理服务器的同步请求。

- `UDP ports`—网络代理可以使用的 UDP 端口号。
- `Location name`—设备的网络位置。
- `State of network location`—指示客户端设备是否可以从一个管理服务器连接配置文件切换到另一个管理服务器连接配置文件的参数。

  可能值：

  - `Enabled`—可以为客户端设备切换管理服务器连接配置文件。
  - `Disabled`—无法为客户端设备切换管理服务器连接配置文件。
- `Profile to use`—管理服务器的连接配置文件。
- `Condition`—客户端设备所连接网络的 IP 地址和子网掩码。
- `Ping period, minutes`—同步之间的标准间隔。
- `Conn timeout, s`—连接超时。
- `RW timeout, s`—读写操作的连接超时。
- `Host ID`—网络中的设备标识符。`Device ID`在特定管理服务器管理的客户端设备中是唯一的。
- `Locations of connection gateways`—通过连接网关将客户端设备连接到管理服务器的参数。
- `Location of distribution points`—通过分发点将客户端设备连接到管理服务器的参数。
- `Connection with server`—指示连接网关是否与管理服务器保持持续连接的参数。仅当客户端设备充当连接网关时才显示该参数。

  可能值：

  - `active`—连接网关与管理服务器保持持续连接。
  - `inactive`—连接网关与管理服务器没有持续连接。
- `Connection with server through connection gateway`—指示是否已通过连接网关正确建立与管理服务器的连接的参数。仅当客户端设备充当连接网关时才显示该参数。

  可能值：

  - `active`—已通过连接网关正确建立与管理服务器的连接。
  - `inactive`—未通过连接网关正确建立与管理服务器的连接。

此外，klnagchk 实用程序输出可能包含以下行之一：

- `Administration Server is installed on this device`—klnagchk 实用程序在管理服务器设备上运行。
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`—klnagchk 实用程序在安装了网络代理的设备上以连接网关模式运行。配置的连接网关正在等待来自管理服务器的连接，但管理服务器未将该设备列在管理设备中。您需要确保管理服务器发起与连接网关的连接。
- `This device is a connection gateway`—klnagchk 实用程序在充当连接网关的设备上运行。
- `Acts as a distribution point`—klnagchk 实用程序在充当分发点的设备上运行。

klnagchk 实用程序可检查网络代理服务的状态。如果该服务未运行，实用程序将停止。如果服务正在运行，实用程序将显示以下连接统计信息：

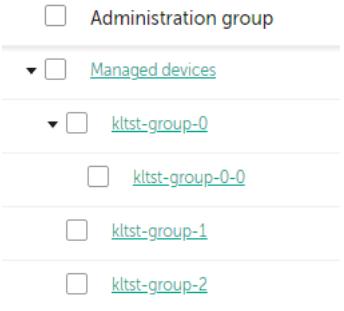
- `Ping count`—客户端设备连接到管理服务器的尝试次数。
- `Succ. pings`—客户端设备成功连接到管理服务器的尝试次数。
- `Sync count`— 尝试将客户端设备设置与管理服务器设置同步的次数。
- `Succ. syncs`—客户端设备设置与管理服务器成功同步的尝试次数。
- `Last ping`—上次连接的日期和时间。

分析管理服务器与网络代理之间的连接时，您需要使用 `Ping count` 和 `Succ. pings` 参数。仅当管理服务器设置发生更改时（例如，添加了新任务或修改了策略设置），客户端设备设置才会与管理服务器设置同步。否则，`Ping count` 和 `Succ. pings` 参数的值保持不变。

有关如何解决网络代理程序连接到管理服务器问题的更多信息，请参阅Open Single Management Platform常见问题解答。

创建管理组

Kaspersky Next XDR Expert 安装后，管理组层次结构仅包含一个名为 **受管理设备** 的管理组。当创建管理组层次结构时，您可以将设备和虚拟机添加到"**受管理设备**"组，并添加嵌套组（请参见下图）。



查看管理组层次结构

要创建管理组，请执行以下操作：

1. 在主菜单中，转到“**资产管理**” → “**组层级**”。
2. 在管理组结构中，选择要包括新管理组的管理组。
3. 单击**添加**。
4. 在打开的“**新管理组名称**”窗口中，输入组的名称，然后单击“**添加**”按钮。

一个具有指定名称的新管理组将出现在管理组层次结构中。

要创建管理组结构：

1. 在主菜单中，转到“**资产管理**” → “**组层级**”。
2. 单击“**导入**”。

新管理组结构向导启动。遵照向导的说明操作。

设备移动规则

建议通过*设备移动规则*自动分配设备到管理组。设备移动规则由三个主要部分组成：名称、执行条件（带设备属性的逻辑表达式）和目标管理组。如果设备属性满足规则执行条件，则规则移动设备到目标管理组。

所有设备移动规则都有优先级。管理服务器检查设备属性以查看它们是否满足每条规则的执行条件（升序优先级）。如果设备属性满足某条规则的执行条件，设备被移动到目标组，至此规则处理在该设备上完成。如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

设备移动规则可以被间接创建。例如，在安装包或远程安装任务的属性中，您可以指定安装网络代理后设备必须被移动到的管理组。此外，Kaspersky Next XDR Expert 管理员还可以在**资产管理 → 移动规则**部分中显式创建设备移动规则。

默认下，设备移动规则用于设备到管理组的一次性初始分配。该规则仅将设备从未分配的设备组中移动一次。如果某个设备曾经被此规则移动，则此规则永远不会再次移动该设备，即使您手动将该设备放回未分配的设备组也是如此。这是应用移动规则的推荐方法。

您可以移动已经被分配的设备到一些管理组。为此，在规则的属性中，请清空“**仅移动不属于任何管理组的设备**”复选框。

应用移动规则到已经分配到一些管理组中的设备会显著增加管理服务器负载。

仅移动不属于任何管理组的设备复选框在自动创建的移动规则的属性中被锁定。当您添加*远程安装应用程序*任务或创建独立安装包时，会创建此类规则。

您可以创建重复影响单一设备的移动规则。

我们强烈建议您避免从一个组重复移动单一设备到另一个组（例如，为了应用特别策略到该设备，运行特别组任务，或者通过特别分发点更新设备）。

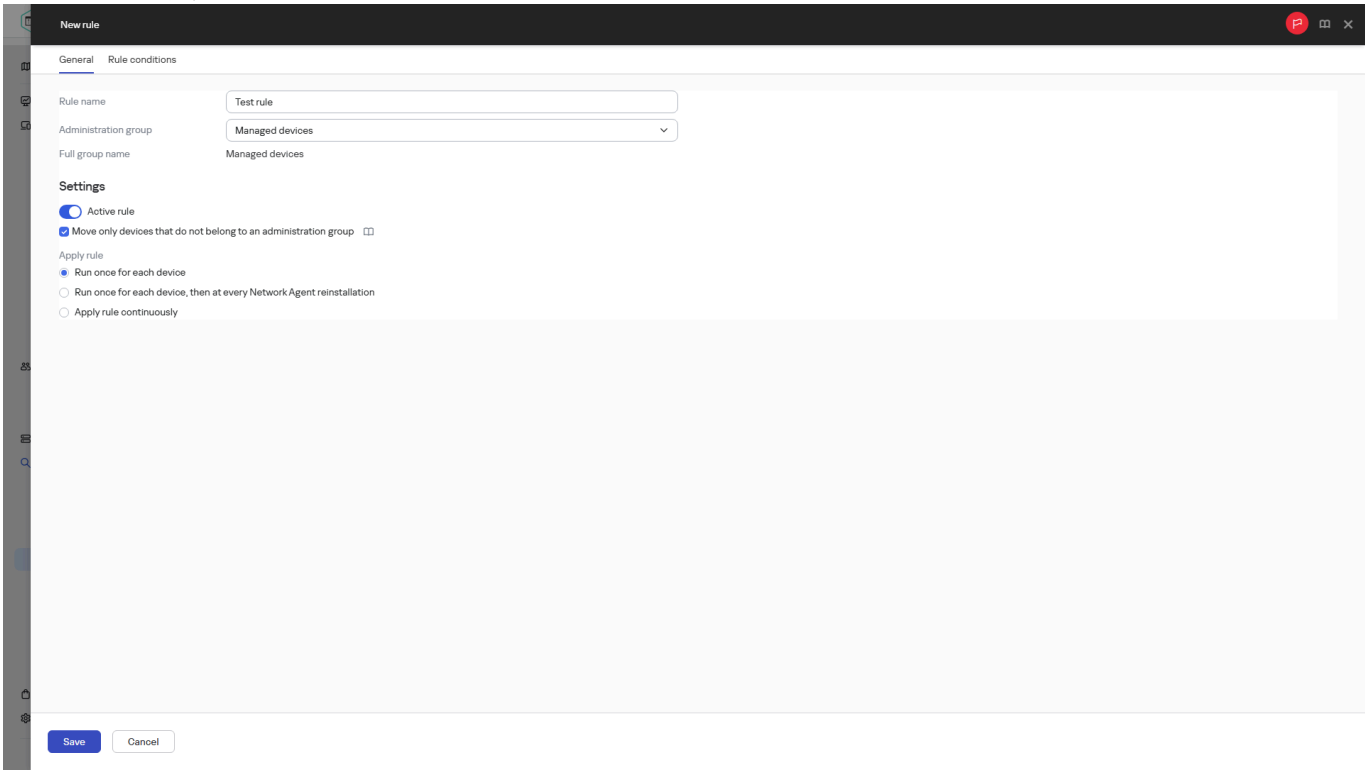
此类方案不被支持，因为它们显著增加了管理服务器负载和网络流量。这些场景也与 Kaspersky Next XDR Expert 的运行原则相冲突（尤其是在访问权限、事件和报告方面）。必须找到其他解决方案，例如，通过使用策略配置文件、设备分类的任务、根据标准方案分配网络代理。

创建设备移动规则

您可以设置设备移动规则，即自动分配设备到管理组的规则。

要创建移动规则：

1. 在主菜单中，转到“**资产管理**”→“**移动规则**”。
2. 单击**添加**。“**新规则**”窗口将开启。



创建新的移动规则

3. 在打开的窗口中，在“**常规**”选项卡上指定以下信息：

- **规则名称**

  输入新规则名称。

  如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。

- **管理组**

  选择要自动移动设备的管理组。

- **激活的规则**

  如果启用该选项，规则被启用并在被保存后开始工作。

  如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

- **优先级**

  您可以指定移动规则的优先等级。最高优先级为1。**优先级**值越大，规则的优先等级越低，在列表中的位置也越靠后。

  如果未指定优先等级，则规则的优先等级为最低。

  复制规则时，副本的优先等级与原规则相同。原规则的优先等级则加1。

- **仅移动不属于任何管理组的设备**

  如果启用该选项，仅未分配的设备将被移动到所选组。
  如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

- **应用规则**

  您可以选择以下选项之一：

  - **对每台设备运行一次**
    规则对匹配标准的每台设备应用一次。

  - **对每台设备运行一次，然后在每次网络代理重新安装时**
    规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。

  - **持续应用规则**
    规则根据管理服务器自动设置的计划被应用（通常每几个小时）。

4. 在“**规则条件**”选项卡上，指定至少一个标准，设备将依据该标准移至管理组。
5. 单击“**保存**”。

移动规则被创建。它显示在移动规则列表。

列表上的位置越高，规则的优先级越高。

若要更改移动规则的优先等级：

1. 在主菜单中，转到“**资产管理**”→“**移动规则**”。
2. 在移动规则列表中，选中要更改优先等级的移动规则旁边的复选框。
3. 执行以下操作之一：

   - 单击**更改优先级**按钮，然后在打开的窗口中指定新的优先等级。
   - 单击**上移**或**下移**按钮，即可在列表中向上或向下移动规则。

4. 单击“**保存**”按钮。

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

如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

复制设备移动规则

您可以复制移动规则，例如，如果您要对不同目标管理组拥有几个相同规则。

要复制现有移动规则：

1. 执行以下操作之一：

   - 在主菜单中，转到“**资产管理**”→“**移动规则**”。
   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**移动规则**”。

   移动规则列表被显示。

2. 选择您要复制的规则旁边的复选框。
3. 单击**复制**。
4. 在打开的窗口中的“**常规**”选项卡上更改以下信息或不进行任何更改（如果您仅想复制规则而不更改其设置）：

   - **规则名称**

     输入新规则名称。
     如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。

   - **管理组**

     选择要自动移动设备的管理组。

   - **激活的规则**

     如果启用该选项，规则被启用并在被保存后开始工作。
     如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

   - **优先级**

     您可以指定移动规则的优先等级。最高优先级为1。**优先级**值越大，规则的优先等级越低，在列表中的位置也越靠后。

     如果未指定优先等级，则规则的优先等级为最低。

     复制规则时，副本的优先等级与原规则相同。原规则的优先等级则加1。

   - **仅移动不属于任何管理组的设备**

     如果启用该选项，仅未分配的设备将被移动到所选组。
     如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

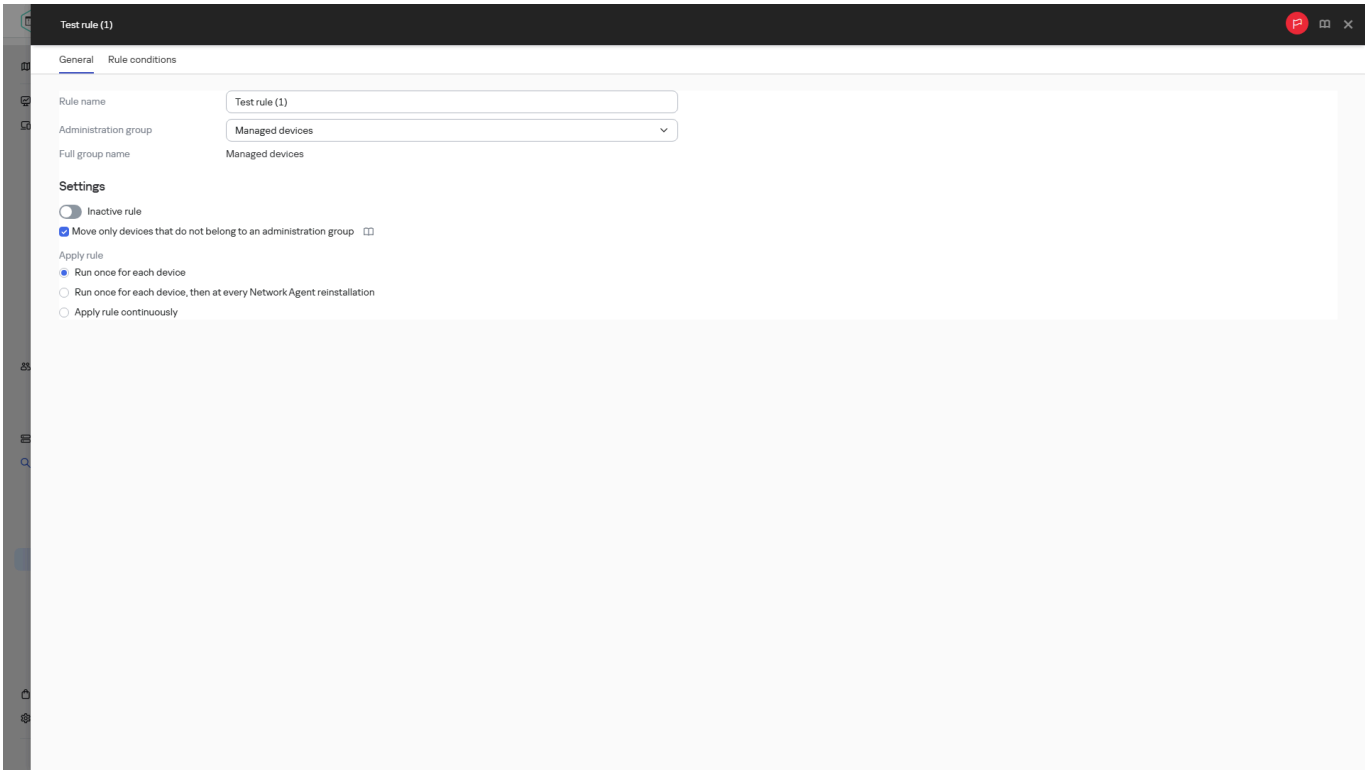
   - **应用规则**

     您可以选择以下选项之一：

     - **对每台设备运行一次**

       规则对匹配标准的每台设备应用一次。

- **对每台设备运行一次，然后在每次网络代理重新安装时**
  规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。
- **持续应用规则**
  规则根据管理服务器自动设置的计划被应用（通常每几个小时）。



设备移动规则的属性

5. 在“**规则条件**”选项卡上，为您希望自动移动的设备指定至少一个标准。
6. 单击“**保存**”。

新移动规则被创建。它显示在移动规则列表。

设备移动规则的条件

当创建或复制将客户端设备移动到管理组的规则时，在“**规则条件**”选项卡上设置移动设备的条件。要确定移动哪些设备，可以使用以下标准：

- 分配给客户端设备的标签。
- 网络参数。例如，您可以移动具有指定范围内 IP 地址的设备。
- 设备所有者、其角色以及安全组成员身份。
- 安装在客户端设备上的受管理应用程序，例如网络代理或管理服务器。
- 虚拟机，即客户端设备。
- 域控制器组织单位。
- 云段。

您可以在下面找到有关如何在设备移动规则中指定此信息的说明。

如果在规则中指定多个条件，AND 逻辑运算符将生效并且所有条件同时适用。如果不选择任何选项或将某些字段留空，则此类条件不适用。

标签选项卡

在该选项卡上，可以基于先前添加到客户端设备描述的设备标签配置设备移动规则。为此，请选择所需标签。此外，还可以启用以下选项：

- **应用到没有指定标签的设备**

  如果启用此选项，则具有指定标签的所有设备都将从设备移动规则中排除。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

- **如果至少一个指定的标签匹配则应用**

  如果启用此选项，则设备移动规则将应用于具有至少一个选定标签的客户端设备。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

网络选项卡

在此选项卡上，可以指定设备移动规则考虑的设备的网络数据：

- **Windows 网络中的设备名**

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

- **Windows 域**

  设备移动规则应用于指定 Windows 域中包含的所有设备。

- **设备的 DNS 名称**

  要移动的客户端设备的 DNS 域名。如果网络包含 DNS 服务器，请填写此字段。

  > 如果您用于 Open Single Management Platform 的数据库设置了区分大小写的排序规则，则在指定设备的 DNS 名称时需保留大小写格式。否则，设备移动规则将不起作用。

- **DNS 域**

  设备移动规则应用于指定主 DNS 后缀中包含的所有设备。如果网络包含 DNS 服务器，请填写此字段。

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。

  默认情况下已禁用该选项。

- **用于连接管理服务器的 IP 地址**

  如果启用此选项，则可以设置客户端设备用于连接到管理服务器的 IP 地址。为此，请指定包含所有必要 IP 地址的 IP 范围。

  默认情况下已禁用该选项。

- **设备在域组的子组中**

  如果启用此选项，您可以选择“域”组的子组。相关设备必须位于所选子组中。

  默认情况下已禁用该选项。

- **设备在 IP 范围中**

  如果启用此选项，您可以选择之前在“**IP 范围**”部分添加的 IP 范围。相关设备必须包含在所选的 IP 范围内。

  默认情况下已禁用该选项。

- **连接配置文件已更改**

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于连接配置文件已更改的客户端设备。
  - **否**。设备移动规则仅应用于连接配置文件未更改的客户端设备。
  - **未选择值**。条件不适用。

- **由不同管理服务器管理**

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于由其他管理服务器管理的客户端设备。这些服务器与配置了设备移动规则的服务器不同。
  - **否**。设备移动规则仅应用于当前管理服务器管理的客户端设备。
  - **未选择值**。条件不适用。

“设备所有者”选项卡

在此选项卡上，您可以根据设备所有者、安全组成员身份和角色配置设备移动规则：

- **设备所有者**

  从内部安全组中选择设备所有者的用户名。在本部分中了解有关用户和用户角色的更多信息。

  > 最多只能有一名用户注册为设备所有者。

- **在活动目录安全组中的设备所有者成员关系**

  选择设备所有者所属的外部活动目录安全组。

  > 用户可以是活动目录安全组的一部分，也可以是此活动目录安全组中包含的组的一部分。

- **设备所有者角色**

  选择设备所有者的指定角色。在本文中了解有关用户角色的更多信息。

- **设备所有者在内部安全组中的成员身份**

  选择设备所有者所属的内部安全组。

应用程序选项卡

在此选项卡上，可以根据客户端设备上安装的受管理应用程序和操作系统来配置设备移动规则：

- **网络代理已安装**

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于安装了网络代理的客户端设备。
  - **否**。设备移动规则仅应用于未安装网络代理的客户端设备。
  - **未选择值**。条件不适用。

- **应用程序**

  指定应在客户端设备上安装哪些受管理应用程序，以便设备移动规则应用于这些设备。例如，您可以选择 **Kaspersky Security Center 16.3 网络代理** 或 **Kaspersky Security Center 16.3 管理服务器**。

  如果不选择任何受管理应用程序，则条件不适用。

- **操作系统版本**

  您可以根据操作系统版本剔除客户端设备。为此，请指定应在客户端设备上安装的操作系统。结果是，设备移动规则应用于具有选定操作系统的客户端设备。

  如果不启用此选项，则条件不适用。默认情况下已禁用该选项。

- **OS 架构**

  您可以按操作系统位数来剔除客户端设备。在“**操作系统架构**”字段中，您可以选择以下值之一：

  - **未知**
  - **x86**
  - **AMD64**
  - **IA64**

要检查客户端设备的操作系统位数：

1. 在主菜单中，转到**资产管理** → **资产(设备)**区域。
2. 单击右侧的设置图标 (⚙)。
3. 选择**OS 架构**选项，然后单击**保存**按钮。
   之后，将显示每个受管理设备的操作系统位数。

- **OS 包管理器**

  您可以按操作系统包管理器来筛选客户端设备。在“**OS 包管理器**”字段中，您可以选择以下值之一：

  - rpm — 适用于运行 Red Hat Enterprise Linux、CentOS、Fedora、SUSE、Oracle Linux 操作系统的设备
  - apt (dpkg) — 适用于运行 Debian、Ubuntu、Kali 操作系统的设备
  - pkg — 适用于运行 FreeBSD、OpenBSD 操作系统的设备

  要检查客户端设备的操作系统包管理器：

  1. 在主菜单中，转到**资产管理** → **资产(设备)**区域。
  2. 单击右侧的“**列设置**”按钮 (⚙)。
  3. 选择“**OS 包管理器**”选项，然后单击“**保存**”按钮。

     每个受管理设备都会显示操作系统软件包管理器。

- **OS 服务包版本**

  在该字段中，可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- **用户证书**

  您可以选择以下值之一：
  - **已安装**。设备移动规则仅应用于具有移动证书的移动设备。
  - **未安装**。设备移动规则仅应用于没有移动证书的移动设备。
  - **未选择值**。条件不适用。

- **OS 内部版本**

  > 该设置仅应用到 Windows 操作系统。

  您可以指定所选操作系统必须具有相同、更早还是更晚的版本号。您也可以为除指定内部版本号外的所有内部版本号配置设备移动规则。

- **OS 发布号**

  > 该设置仅应用到 Windows 操作系统。

您可以指定所选操作系统必须具有相同、更早还是更晚的版本号。您也可以为除指定内部版本号外的所有内部版本号配置设备移动规则。

虚拟机选项卡

在该选项卡上，可以根据客户端设备是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来配置设备移动规则：

- **这是一台虚拟机**

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动非虚拟机设备。
  - **是**。移动虚拟机设备。

- **虚拟机类型**

- **虚拟桌面基础架构的一部分**

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动不属于 VDI 的设备。
  - **是**。移动属于 VDI 的设备。

域控制器选项卡

在此选项卡上，您可以指定需要移动域组织单元中包含的设备。您还可以从指定域组织单元的所有子组织单元移动设备：

- **设备包含在以下组织单元中**

  如果启用此选项，则设备移动规则将应用于该选项下的列表中指定的域控制器组织单元中的设备。
  默认情况下已禁用该选项。

- **包括子组织单元**

  如果启用此选项，选择范围将包括指定域控制器组织单元的所有子组织单元中的设备。
  默认情况下已禁用该选项。

- **将设备从子单元移动到对应子组**

- **创建对应于新检测到设备的容器的子组**

- **删除域中不存在的子组**

- **设备包含在以下域安全组中**

  如果启用此选项，设备移动规则将应用于该选项下的列表中指定的域安全组中的设备。

  默认情况下已禁用该选项。

云段选项卡

在此选项卡上，您可以指定需要移动云段中包含的设备。您还可以从指定域组织单元的所有子组织单元移动设备：

- **设备在云段中**

  如果选择此选项，则设备移动规则将应用于属于云段的客户端设备。您可以在该选项下的列表中选择需要添加至子网的云段。

  默认情况下已禁用该选项。

- **包含子对象**

  如果启用此选项，选择范围将包括指定云段的所有子组织单元中的设备。

  默认情况下已禁用该选项。

- **从嵌套对象移动设备到对应子组**
- **创建对应于新检测到设备的容器的子组**
- **删除在云段中未找到匹配的子组**
- **使用 API 发现的设备**

  在该下拉列表中，可以选择以下选项之一：

  - 未选择值。条件不适用。
  - **否**。移动不是使用 API 发现的设备。
  - **AWS**。移动使用 AWS API 发现的设备。
  - **Azure**。移动使用 Azure API 发现的设备。
  - **Google Cloud**。移动使用 Google Cloud API 发现的设备。

  之后，根据所选值，可以填写以下字段：

  - **云设备子网**。
  - **云设备可用区域**。
  - **云设备放置组**。

手动将设备添加到管理组

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

要手动将一台或多台设备添加到选定的管理组：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
2. 选择您要向其添加设备的管理组：
   - 对于根组：
     在这种情况下，您可以继续下一步。
   - 对于子组：
     a. 单击页面顶部的“**显示层级**”按钮。
     按钮名称将更改为“**隐藏层级**”。
     b. 在打开的窗口中，单击子组的名称。

   所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。
3. 单击“**添加设备**”按钮。
   移动设备向导启动。
4. 生成要添加到管理组的设备列表。

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

   选择要将设备添加到列表的方式：
   - 单击“**添加设备**”按钮，然后通过以下方式之一指定设备：
     - 从管理服务器检测到的设备列表中选择设备。
     - 指定设备 IP 地址或 IP 范围。

       > IP地址范围不得包含超过1,048,576个地址。

     - 指定设备 DNS 名称。

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

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

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

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

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

手动将设备或者集群移动至管理组

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

您还可以将集群或服务器阵列从一个管理组移动到另一个管理组。当您将集群或服务器阵列移动到另一个组时，其所有节点都会随之移动，因为集群及其任何节点始终属于同一管理组。当您在“**设备**”选项卡上选择单个集群节点时，“**移动到组**”按钮将变得不可用。

要将一台或多台设备或者集群移动到选定的管理组：

1. 打开要从中移动设备的管理组。为此，请执行以下步骤之一：
   - 要打开管理组，请在主菜单中转到**资产管理→资产(设备)**，然后选择所需的管理组。
     - 对于根组，您可以继续进行下一步。
     - 对于子组，单击页面顶部的“**显示层级**”按钮，然后在打开的窗口中选择所需的管理组。
   - 要打开**未分配的设备**群组，请在主菜单中，前往**资产管理→未分配的设备**。
2. 如果管理组包含集群或服务器阵列，则“**资产(设备)**”区域将被分为两个选项卡：“**设备**”选项卡和“**集群和服务器阵列**”选项卡。打开要移动的对象的选项卡。
3. 选中要移动到其他组的设备或者集群旁边的复选框。
4. 单击**移动到组**按钮。
5. 在管理组的层级中，选中要将选定设备或者集群移动到的管理组旁边的复选框。
6. 单击“**移动**”按钮。

选定设备或者集群将被移动到选定管理组。

关于集群和服务器阵列

Kaspersky Next XDR Expert 支持集群技术。如果网络代理向管理服务器发送信息确认组成服务器阵列的客户端设备上已安装该应用程序，则该客户端设备就成为一个集群节点。

如果管理组包含集群或服务器阵列，则“**资产(设备)**”页面将显示两个选项卡：一个用于单个设备，另一个用于集群和服务器阵列。受管理设备被检测为集群节点后，集群将被作为单独对象添加到“**集群和服务器阵列**”选项卡。

集群或服务器阵列节点与其他受管理设备一起列在**设备**选项卡上。您可以将节点作为单个设备查看属性并执行其他操作，但不能删除集群节点或将其从集群中单独移动到另一个管理组。您只能删除或移动整个集群。

您可以对集群或服务器阵列执行以下操作：

- 查看属性
- 将集群或服务器阵列移至另一个管理组

  当您将集群或服务器阵列移动到另一个组时，其所有节点都会随之移动，因为集群及其任何节点始终属于同一管理组。
- 删除

  仅当集群或服务器阵列不在组织网络中存在时，删除该集群或服务器阵列才合理。如果集群在您的网络上仍然可见，并且网络代理和卡巴斯基安全应用程序仍然安装在集群节点上，Open Single Management Platform 会自动将已删除的集群及其节点返回到受管理设备列表。

集群或服务器阵列的属性

要查看集群或服务器阵列的设置：

1. 在主菜单中，转到“**资产管理**”→“**资产(设备)**”→“**集群和服务器阵列**”。

   集群和服务器阵列的列表将显示。
2. 单击所需集群或服务器阵列的名称。

所选集群或服务器阵列的属性窗口将显示。

常规

常规部分显示有关集群或服务器阵列的常规信息。信息基于上一次集群节点与管理服务器之间的同步接收的数据来提供：

- **名称**
- **描述**
- **Windows 域**

  Windows 域或工作组，包含集群或服务器阵列。
- **NetBIOS 名称**

  集群或服务器阵列的 Windows 网络名称。
- **DNS 名称**

  集群或服务器阵列的 DNS 域名称。

任务

在“**任务**”选项卡中，您可以管理分配给集群或者服务器阵列的任务：查看现有任务列表；创建新任务；删除、启动和停止任务；修改任务设置；查看执行结果。列出的任务与安装在集群节点上的卡巴斯基安全应用程序相关。Open Single Management Platform 从集群节点接收任务列表和任务状态详情。如果未建立连接，则不显示状态。

节点

此选项卡显示集群或服务器阵列中包含的节点列表。您可以单击节点名称来查看设备属性窗口。

卡巴斯基应用程序

属性窗口还可能包含其他选项卡，其中包含与集群节点上安装的卡巴斯基安全应用程序相关的信息和设置。

分发点和连接网关的调整

Kaspersky Next XDR Expert 中的管理组结构具有以下功能：

- 设置策略范围
  将相关设置应用到设备还有一种方式：使用*策略配置文件*。
- 设置组任务范围
  还有一个不基于管理组层级定义组任务范围的方法：使用设备分类的任务和特定设备的任务。
- 设置设备、虚拟管理服务器和从属管理服务器的访问权限。
- 分配分发点

当建立管理组结构时，您必须考虑到组织网络的拓扑以便最优分配分发点。分发点的最优分发允许您在企业网络中保存流量。

根据组织图表和网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个小远程分办公室

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

分发点的标准配置：单一办公室

在标准“单一办公室”配置中，所有设备都在组织网络中，因此它们能看见彼此。组织网络可能包含几部分(网络或网段)，由窄通道连接。

有以下构建管理组结构的方法：

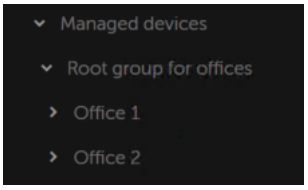
- 构建管理组结构涉及到网络拓扑。管理组结构可能不精确反映网络拓扑。网络各部分之间以及特定管理组相互匹配。您可以使用分发点自动分配或手动分配它们。

- 不考虑网络拓扑而构建管理组结构。此种情况下，您必须禁用分发点自动分配，然后为网络中每个部分的根管理组分配一个或几个设备作为分发点，例如为“**受管理设备**”组。所有分发点将处于相同级别，并将掌控组织网络中所有设备的相同范围。此种情况下，每个网络代理都将连接到具有最短路由的分发点。分发点的路由可以使用 tracert 使用工具跟踪。

分发点的标准配置：多个小远程办公室

该标准配置可用于多个小型远程办公室，它们可能通过互联网与总部联络。每个远程办公室都位于 NAT 之外，就是说，从一个远程办公室到另一个远程办公室的连接是不可能的，因为办公室是彼此隔离的。

配置必须在管理组中体现：必须为每个远程办公室创建各自的管理组（下图中的组**办公室 1**和**办公室 2**）。



远程办公室包含在管理组结构

必须指定一个或多个分发点给每个办公室的对应管理组。分发点必须是远程办公室中具有足够剩余磁盘空间的设备。部署在**办公室 1**组的设备，例如，将访问分配到**办公室 1**管理组的分发点。

如果一些用户在办公室之间移动他们的便携电脑，您必须在远程办公室选择两个或更多设备(除了现有的分发点)并分配它们作为等级管理组的分发点(上图中**办公室根组**)。

例如：便携式电脑部署在**办公室 1**管理组，然后被移动到对应于**办公室 2** 管理组的办公室。在移动便携式电脑后，网络代理试图访问分配到**办公室 1**组的分发点，但是那些分发点不可用。然后，网络代理开始尝试访问分配到**办公室根组**的分发点。因为远程办公室是彼此隔离的，尝试访问分配到**办公室根组**管理组的分发点仅在网络代理尝试访问**办公室 2** 组中的分发点时才会成功。就是说，便携式电脑将保持在原始办公室对应的管理组，但是将使用它当时所在办公室的分发点。

计算分发点的数量和配置

网络包含越多的客户端设备，就需要越多的分发点。我们建议您禁用分发点的自动分配。当分发点的自动分配被启用时，如果客户端设备数量很大，管理服务器就分配分发点并定义其配置。

使用单独分配的分发点

如果您计划使用特定设备作为分发点(就是，单独分配的服务器)，您可以不使用分发点的自动分配。此种情况下，确保您要分配为分发点的设备具有足够的剩余磁盘空间卷，不定期关闭，且禁用了睡眠模式。

包含一个网段的网络中的专用分发点数量（取决于网络中的设备数量）

每个网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	可接受：(N/10,000 + 1)，建议：(N/5000 + 2)，N 是网络设备数量

包含多个网段的网络中的专用分发点数量（取决于网络中的设备数量）

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–100	1
大于 100	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–30	1
31–300	2
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

自动分配分发点

我们建议您自动分配分发点。在这种情况下，Kaspersky Next XDR Expert 将自行选择应指定为分发点的设备。

运行基于Arm架构的Microsoft Windows的设备不能充当分发点。

要自动分配分发点：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 选择“**自动分配分发点**”选项。

   如果自动指派设备做为分发点被启用，您无法手动配置分发点，也不能编辑分发点列表。

4. 单击“**保存**”按钮。

管理服务器便自动指派和配置分发点。

手动分配分发点

Kaspersky Next XDR Expert 允许您手动指定设备充当分发点。

我们建议您自动分配分发点。在这种情况下，Kaspersky Next XDR Expert 将自行选择应指定为分发点的设备。但是，如果您出于任何原因必须选择不自动分配分发点（例如，如果您想使用专门分配的服务器），您可以在计算分发点的数量和配置后手动分配分发点。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

运行基于 Arm 架构的 Microsoft Windows 的设备不能充当分发点。

要手动指派设备做为分发点：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 选择“**手动分配分发点**”选项。
4. 单击“**分配**”按钮。
5. 选择您要制作分发点的设备。
   选择设备时，请牢记分发点的操作功能以及设备做为分发点的需求。
6. 选择您要包含在所选分发点范围的管理组。
7. 单击“**确定**”。
   您添加的分发点将显示在“**分发点**”区域的分发点列表中。
8. 在列表中单击新添加的分发点以打开其属性窗口。

9. 在属性窗口中配置分发点：

- **常规**区域中包含用于设定分发点与客户端设备进行交互的设置。
  - **SSL 端口**

    客户端设备与分发点之间，使用 SSL 进行安全连接的 SSL 端口号。

    默认端口号是 13000。

  - **已启用**

    如果启用此选项，将使用 IP 多点传送自动向组内的客户端设备上分发安装包。

    IP 多点传送减少了将应用程序从安装包安装到一组客户端设备所需的时间，但是增加了在将应用程序安装到单个客户端设备时的安装时间。

  - **IP 多点传送地址**

    用于多点传送的 IP 地址。您可以定义范围是 224.0.0.0 – 239.255.255.255 的 IP 地址

    默认情况下，Kaspersky Next XDR Expert 会自动分配给定范围内的唯一 IP 多点传送地址。

  - **IP 多点传送端口号**

    IP 多点传送的端口号。

    默认情况下，端口号指定为 15001。如果运行管理服务器的设备指定为分发点，端口 13001 默认用于 SSL 连接。

  - **远程设备的分发点地址**

    远程设备连接到分法点的网络地址。

  - **部署更新**

    更新被从以下来源分发到受管理设备：

    - 此分发点（如果启用此选项）。
    - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

    如果您使用分发点来部署更新，则可以节省流量，因为您减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。您可以通过计算分发点的数量和配置来确定网络所需的分发点数量，以优化流量和负载。

    如果禁用此选项，管理服务器上的更新下载和加载次数可能会增加。默认情况下已启用该选项。

  - **部署安装包**

    安装包被从以下来源分发到受管理设备：

    - 此分发点（如果启用此选项）。
    - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

    如果使用分发点部署安装包，您可以节省流量，因为减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。您可以通过计算分发点的数量和配置来确定网络所需的分发点数量，以优化流量和负载。

    如果禁用此选项，管理服务器上的安装包下载和加载次数可能会增加。默认情况下已启用该选项。

- **运行推送服务器**

  在 Open Single Management Platform 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

- **推送服务器端口**

  推送服务器的端口号。您可以指定任何未占用的端口号。

- 在“**范围**”区域中，指定分发点将向其分发更新的管理组。
- 在“**更新源**”区域中，可以选择分发点的更新源：
  - **更新源**

    为分发点选择更新源：
    - 要允许分发点从管理服务器接收更新，请选择“**从管理服务器检索**”。
    - 要允许分发点使用任务接收更新，请选择“**使用更新下载任务**”，然后指定“*将更新下载至分发点存储库*”任务：
      - 如果设备上已存在此类任务，请在列表中选择该任务。
      - 如果设备上尚不存在此类任务，请单击“**创建任务**”链接创建任务。“新任务向导”启动。遵照向导的说明操作。
  - **下载差异文件**

    该选项启用下载 diff 文件功能。

    默认情况下已启用该选项。

- 如果您的分发点在连接到互联网时使用代理服务器，则可以在**互联网连接设置**子部分中指定以下设置：
  - **使用代理服务器**

    如果选中此复选框，则使用互联网代理服务器将分发点连接到卡巴斯基更新服务器。您可以在输入字段中配置代理服务器连接。

    默认情况下，此复选框未被选中。

  - **代理服务器地址**

    代理服务器地址。

  - **端口号**

    用于连接的端口号。

  - **对本地地址不使用代理服务器**

    如果启用此选项，将不使用代理服务器连接本地网络的设备。

    默认情况下已禁用该选项。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  默认情况下，此复选框未被选中。

- **用户名**

  建立连接代理服务器的用户账户。

- **密码**

  任务运行时使用的账户的密码。

- 在“**KSN 代理**”区域，您可以配置应用程序使用分发点从受管理设备转发 KSN 请求：

  - **在分发点端启用 KSN 代理**

    KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

    分发点发送列在Kaspersky Security Network声明中的KSN统计信息到卡巴斯基。

    默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器** 和 **我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。

    您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

  - **转发 KSN 请求到管理服务器**

    分发点从受管理设备转发 KSN 请求到管理服务器。

    默认情况下已启用该选项。

  - **通过互联网直接访问 KSN 云/KPSN**

    分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

  - **当连接到 KPSN 时忽略代理服务器设置**

    如果您在分发点属性或网络代理策略中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，则启用此选项。否则，从受管理应用程序的请求无法到达 KPSN。

    如果您选择“**通过互联网直接访问 KSN 云/KPSN**”选项，则此选项可用。

  - **端口**

    受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

  - **使用 UDP 端口**

    如果需要受管理设备通过 UDP 端口连接到 KSN 代理，则启用“**使用 UDP 端口**”选项并指定 UDP 端口号。默认情况下已启用该选项。

  - **UDP 端口**

    受管理设备将用于连接到 KSN 代理服务器的 UDP 端口号。连接到 KSN 代理的默认 UDP 端口是 15111。

  - **使用 HTTPS**

    如果需要受管理设备通过 HTTPS 端口连接到 KSN 代理服务器，启用“**使用 HTTPS 端口**”选项，并指定 **HTTPS 端口**号。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

- **HTTPS 端口**

  受管理设备用于连接到 KSN 代理服务器的 HTTPS 端口号。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

- 在“**连接网关**”区域中，可以配置分发点，充当网络代理实例和管理服务器之间连接的网关：

  - **连接网关**

    如果由于您的网络组织而无法在管理服务器和网络代理之间建立直接连接，您可以使用分发点作为管理服务器和网络代理之间的连接网关。

    如果您需要分发点充当网络代理和管理服务器之间的连接网关，请启用此选项。默认情况下已禁用该选项。

  - **从管理服务器建立连接到网关(如果网关位于 DMZ 中)**

    如果管理服务器位于隔离区域 (DMZ) 之外，在局域网中，安装在远程设备上的网络代理无法连接到管理服务器。您可以使用分发点作为具有反向连接的连接网关（管理服务器建立到分发点的连接）。

    如果您需要将管理服务器连接到 DMZ 中的连接网关，请启用此选项。

  - **为 Kaspersky Security Center Web Console 打开本地端口**

    如果您需要 DMZ 中的连接网关为位于 DMZ 中或互联网上的 Web Console 打开一个端口，请启用此选项。指定将用于从 Web Console 连接到分发点的端口号。默认端口号是 13299。

    如果启用“**从管理服务器建立连接到网关(如果网关位于 DMZ 中)**”选项，则此选项可用。

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

  - **为移动设备打开端口(仅管理服务器 SSL 身份验证)**

    如果您需要连接网关为移动设备打开一个端口并指定移动设备将用于连接到分发点的端口号，请启用此选项。默认端口号是 13292。移动设备将检查管理服务器证书。建立连接时，仅对管理服务器进行身份验证。

  - **为移动设备打开端口(双向 SSL 身份验证)**

    如果您需要连接网关打开一个端口，该端口将用于管理服务器和移动设备的双向身份验证，请启用此选项。移动设备将检查管理服务器证书，管理服务器也将检查移动设备证书。指定下列设置：

    - 移动设备将用于连接到分发点的端口号。默认端口号是 13293。
    - 移动设备将使用的连接网关的 DNS 域名。用逗号分隔域名。指定的域名将包含在分发点证书中。如果移动设备使用的域名与分发点证书中的通用名称不匹配，则移动设备不会连接到分发点。

      默认 DNS 域名是连接网关的 FQDN 名称。

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

- 通过基于 Windows 的分发点配置 Windows 网络轮询。

  - **Windows 域**

    您可以启用 Windows 域设备发现并为发现设置计划。

- 配置分发点的域控制器轮询。
  - **域控制器轮询**

    您可以对域控制器启用设备发现。

    在**轮询**字段中，将切换按钮切换到**已启用**位置后，您可以选择要轮询的域控制器，还可以为它们指定轮询计划。

    如果使用 Linux 分发点，请在“**轮询指定域**”区域中单击“**添加**”，然后指定域控制器的地址和用户凭据。另外，您可以指定要轮询的域的类型：Active Directory 或 Samba、FreeIPA、ALD Pro。

    如果您使用 Windows 分发点，则可以选择以下选项之一：

    - **轮询当前域**
    - **轮询整个域森林**
    - **轮询指定域**
- 按分发点配置 IP 范围轮询。
  - **IP 范围轮询**

    您可以针对 IPv4 范围和 IPv6 网络启用设备发现。

    如果启用“**启用范围轮询**”选项，则可以添加扫描范围并为其设置计划。您可以添加 IP 范围到已扫描范围列表。

    如果启用“**使用 Zeroconf 轮询 IPv6 网络**”选项，分发点将使用零配置网络（也称为 *Zeroconf*）自动轮询 IPv6 网络。在这种情况下，指定的 IP 范围将被忽略，因为分发点会轮询整个网络。如果分发点运行 Linux，则**使用 Zeroconf 轮询 IPv6 网络**选项可用。要使用 Zeroconf IPv6 轮询，您必须在分发点上安装 avahi-browse 实用程序。
- 在**高级**区域，指定分发点必须使用以存储发布数据的文件夹。
  - **使用默认的文件夹**

    如果您选择此选项，应用程序使用分发点上的网络代理安装文件夹。
  - **使用指定的文件夹**

    如果您选择该选项，则可以在下面的字段中指定该文件夹的路径。它可以是分发点上的本地文件夹，也可以是企业网络中任何设备上的目录。

    分发点上用于运行网络代理的用户账户必须具有对指定文件夹的访问权限以进行读写操作。

10. 单击“**确定**”。

所选设备作为分发点运行。

修改管理组的分发点列表

您可以查看为特定管理组分配的分发点列表并通过添加或删除分发点来修改列表。

要查看和修改分配给管理组的分发点列表：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
2. 通过单击页面顶部的“**显示层级**”按钮，选择要查看所分配的分发点的管理组，然后在打开的窗口中单击所需组的名称。

   这将启用**分发点**菜单项。

   所选组的路径显示在页面顶部。如果需要，您可以在此路径中单击带有管理组名称的链接转到该组。默认情况下，路径中的最后一个链接不活动。
3. 在主菜单中，转到“**资产管理**”→“**分发点**”。
4. 要为管理组添加新的分发点，请单击**分配**按钮。
5. 要删除分配的分发点，请从列表中选择设备并单击**取消分配**按钮。

根据于您的修改，新分发点被添加到列表或现有分发点被从列表删除。

启用推送服务器

在 Open Single Management Platform 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

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

推送服务器支持最多 50,000 个同时连接的负载。

要在分发点上启用推送服务器：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 单击要在其上启用推送服务器的分发点的名称。

   分发点属性窗口将打开。
4. 在“**常规**”区域中，启用“**已启用**”选项。
5. 在“**推送服务器端口**”字段中，键入端口号。您可以指定任何未占用的端口号。
6. 在“**远程主机地址**”字段中，指定分发点设备的 IP 地址或名称。
7. 单击“**确定**”。

在所选分发点上已启用推送服务器。

关于设备状态

Kaspersky Next XDR Expert 会为每台受管理设备分配一个状态。具体状态取决于是否满足用户定义的条件。在某些情况下，为设备分配状态时，Kaspersky Next XDR Expert 会考虑该设备在网络上的可见性标志（见下表）。如果 Kaspersky Next XDR Expert 在两小时内未在网络上发现某台设备，则该设备的可见性标志将设置为“*不可见*”。

状态如下：

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

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

分配状态到设备的条件

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

条件	条件描述	可用值
需要重启后的时间	设备在网络上可见，但应用程序要求重启的时间已超过指定时间间隔。	超过 0 分钟。
重启原因	设备在网络上可见，但由于所选原因之一，应用程序需要重新启动设备。	• 未知原因 • 应用程序在重启前不会运行 • 需要重启以完成更新；应用程序正在运行 • 需要重启以启动更新 • 需要重启以完成扫描或清除 • 需要重启以完成远程安装/卸载 • 即将完成磁盘的数据加密
安装了不兼容的应用程序	设备在网络中可见，但通过网络代理执行的软件清查在设备上检测到了不兼容的应用程序。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到软件漏洞	设备在网络中可见且网络代理已安装到设备，但“*查找漏洞和所需更新*”任务在设备应用程序中检测到指定严重级别的漏洞。	• 严重 • 高。 • 中。 • 如果漏洞无法被修复则忽略。 • 如果为安装分配了更新则忽略。
授权许可已过期	设备在网络中可见，但授权许可已过期。	• 开关按钮被关闭。 • 开关按钮被开启。
授权许可即将过期	设备在网络中可见，但设备上的授权许可即将在指定天数内过期。	少于 0 天。
Windows Update 更新检查已长时间未执行	设备在网络中可见，但“*寻找漏洞和所需更新*”任务在指定时间段内未运行。	超过 1 天。
无效的加密状态	网络代理已安装到设备，但设备加密结果等于指定值。	• 由于用户拒绝未遵从策略(仅对外部设备)。 • 由于错误未遵从策略。 • 应用策略时需要重启。 • 未指定加密策略。 • 不支持。 • 当应用策略时。
移动设备设置不遵从策略	移动设备设置不同于 Kaspersky Endpoint Security for Android 策略中指定的设置。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到未处理的安全问题	设备上发现了一些未处理的安全问题。安全问题可以通过安装在客户端设备上的受管卡巴斯基应用程序自动创建，也可以由管理员手动创建。	• 开关按钮被关闭。 • 开关按钮被开启。
应用程序定义的设备状态	设备状态由受管理应用程序定义。	• 开关按钮被关闭。 • 开关按钮被开启。
设备磁盘空间不足	设备剩余磁盘空间少于指定值或设备无法与管理服务器同步。当设备已与管理服务器成功同步且设备上的剩余空间大于或等于指定值时，*严重*或*警告*状态被更改为*正常*状态。	大于 0 MB。
设备已失去管理	在设备发现过程中，设备在网络中可见，但是超过三次尝试与管理服务器同步都失败了。	• 开关按钮被关闭。 • 开关按钮被开启。
保护已禁用	设备在网络中可见，但设备上的安全应用程序已被禁用长于指定的时间段。 在这种情况下，安全应用程序的状态为*stopped*或*failure*，不同于以下状态：*starting*、*running*或*suspended*。	超过 0 分钟。
安全应用程序没有运行	设备在网络中可见且安全应用程序已安装到设备，但其未在运行。	• 开关按钮被关闭。 • 开关按钮被开启。

Kaspersky Next XDR Expert 允许您设置在满足指定条件时自动切换管理组中设备的状态。当指定条件满足时，客户端设备被分配以下状态之一：*严重*或*警告*。未满足指定条件时，客户端设备被分配“*正常*”状态。

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

当 Kaspersky Next XDR Expert 为设备分配状态时，对于某些条件（请参阅上表中的“条件描述”列），会将可见性标志考虑在内。例如，如果某个受管理设备由于满足“数据库已过期”条件而被分配“*严重*”状态，稍后为设备设置了可见性标志，则该设备被分配“*正常*”状态。

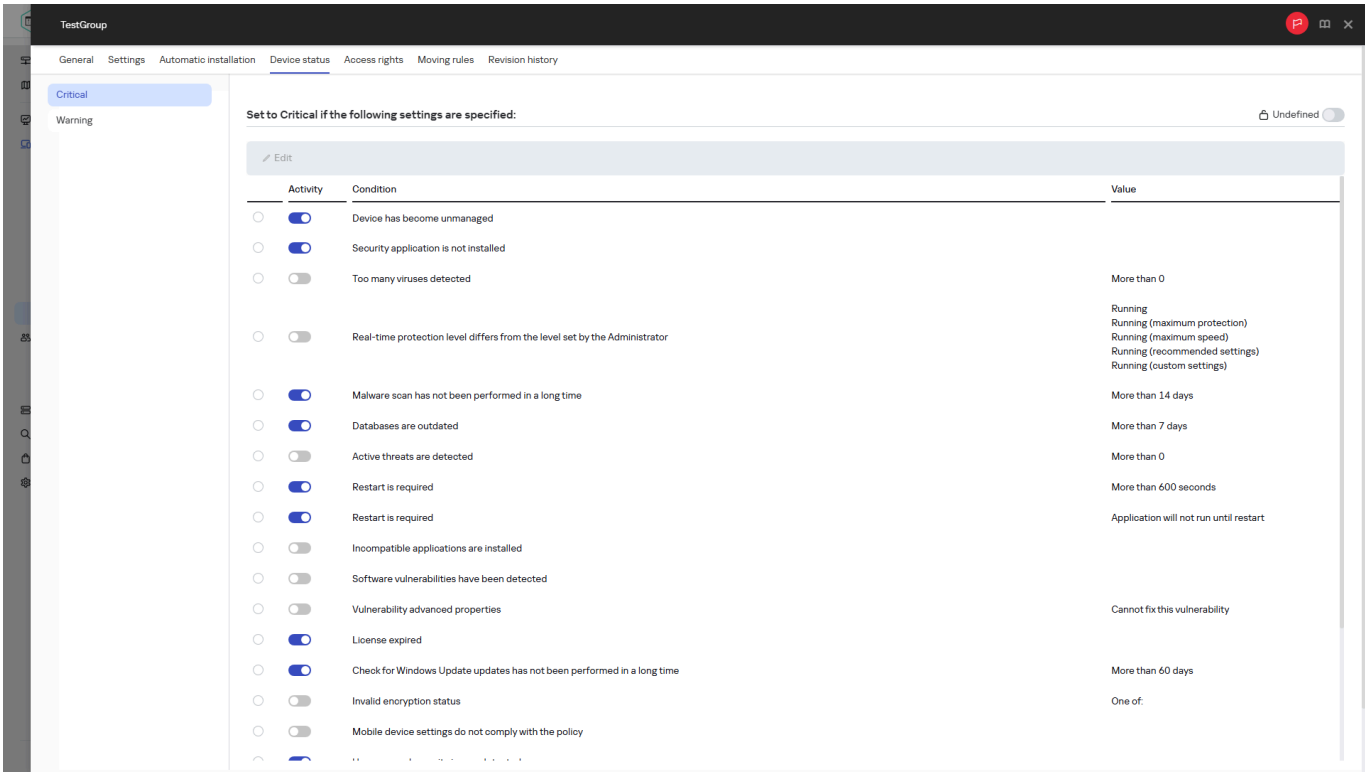
配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 在主菜单中，转到“**资产管理**”→ “**组层级**”。
2. 通过以下方式之一，转到要更改设备状态的管理组的属性：
   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标 (⚙)。

   管理组属性窗口将开启。
3. 在属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**严重**”。
5. 在右侧窗格的“**如果指定了以下设置，则设置为“严重”**”区域中，启用将设备切换为“*严重*”状态的条件。



> 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。
10. 单击“**保存**”保存更改。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 在主菜单中，转到“**资产管理**” → “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**警告**”。
5. 在右侧窗格的“**如果指定了以下设置，则设置为“警告”**”区域中，启用将设备切换为“*警告*”状态的条件。

> 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。
10. 单击“**保存**”保存更改。

满足指定条件时，受管理设备被分配*警告*状态。

设备分类

*设备分类*是根据特定条件筛选设备的工具。您可以使用设备分类管理几个设备：例如，查看仅查看这些设备的报告或移动所有这些设备到其他组。

Open Single Management Platform 提供多种*预定义分类*（例如，**处于“严重”状态的设备**、**保护已禁用**、**检测到活动威胁**）。预定义分类无法被删除。您也可以创建和配置附加*用户定义分类*。

在用户定义分类中，您可以设置搜索范围并选择所有设备、受管理设备、或者未分配的设备。搜索参数在条件中指定。在设备分类中，您可以创建带有不同搜索参数的多个条件。例如，您可以创建两个条件并指定不同的 IP 范围。如果多个条件被指定，分类显示满足任意条件的设备。相比之下，条件中的搜索参数是附加的。如果 IP 范围和已安装应用程序名称都被指定在一个条件，仅安装了应用程序且 IP 地址处于指定范围的设备被显示。

从设备分类中查看设备列表

Open Single Management Platform 允许您从设备选择中查看设备列表。

若要从设备分类中查看设备列表：

1. 在主菜单中，转到“**资产管理 → 设备分类**或者**发现和部署 → 设备分类**”区域。
2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。
3. 您可以按如下方式对设备表中的数据进行分组和筛选：
   - 单击设置图标 (⚙)，然后选择要在表中显示的列。
   - 单击筛选图标 (▽)，然后在调用的菜单中指定并应用筛选条件。
     筛选出的设备表将显示。

您可以在设备分类中选择一个或多个设备，然后单击**新任务**按钮以创建将被应用于这些设备的任务。

要将设备分类中的选定设备移动到另一个管理组，请单击**移动到组**按钮，然后选择目标管理组。

创建设备分类

要创建设备分类，请执行以下操作：

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

   您可以启用**包含来自从属管理服务器的数据**复选框以启用搜索满足选择条件并由从属管理服务器管理的设备。
5. 单击**添加**。

6. 在打开的窗口中，指定将设备包括在此分类中必须满足的条件，然后单击“**保存**”按钮。
7. 单击“**保存**”按钮。

设备分类即被创建并添加到设备分类列表中。

配置设备分类

要配置设备分类：

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

设备被应用并保存。

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

常规

在“**常规**”区域，您可以更改分类条件的名称，指定条件是否必须被倒转：

反转分类条件

默认情况下已禁用该选项。

如果启用此选项，指定的分类条件将倒转。此分类将包含所有不符合该条件的设备。

以下示例展示了反转工作的逻辑：

- **条件**：您的设备上存在操作系统类型为 Linux 且内部版本号为 00.0.000 的设备。
- **反转条件**：您的设备上存在操作系统类型为非 Linux 且内部版本号为非 00.0.000 的设备，这等价于：
  存在操作系统类型为非 Linux 或内部版本号为非 00.0.000 的设备。

因此，选择范围将包括操作系统类型为 Windows 且内部版本号为 00.0.000 的设备，或者 Linux 且内部版本号不为 00.0.000 的设备。

网络基础架构

在“**网络**”子区域，您可以指定根据网络数据包含设备到分类的标准：

- **设备名称**

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

- **域**

  显示指定工作组中包括的所有设备。

- **管理组**

  显示指定的管理组中包括的设备。

- **描述**

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

  - 在单词中：

    - *****。用任意数量的字符替换任何字符串。

    例如：
    要描述单词 **Server** 或 **Server's**，您可以输入 **Server***。

    - **?。**替换任意单个字符。

    例如：
    要描述 **SUSE Linux Enterprise Server 12** 或 **SUSE Linux Enterprise Server 15** 等短语，可以输入 **SUSE Linux Enterprise Server 1?**。
    星号(*****)或问号(**?**)不能用于查询中的第一个字符。

  - 要查找多个单词：

    - 空格。显示所有在其描述中包含列出的任何单词的设备。

    例如：
    要查找包含“**从属**”或“**虚拟**”单词的短语，可以在查询中包含“**从属 虚拟**”行。

    - **+**。当单词带有加号前缀时，所有搜索结果都将包含该单词。

    例如：
    要查找同时包含“**从属**”和“**虚拟**”的短语，请输入“**+从属+虚拟**”查询。

    - **-**。当单词带有减号前缀时，所有搜索结果都不包含该单词。

    例如：
    要查找包含“**从属**”但不包含“**虚拟**”的短语，请输入“**+从属-虚拟**”查询。

    - **“<某些文本>”**。引号中围绕的文本必须存在于文本中。

例如:

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

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。

  默认情况下已禁用该选项。

- **由不同管理服务器管理**

  您可以选择以下值之一:

  - **是**。设备移动规则仅应用于由其他管理服务器管理的客户端设备。这些服务器与配置了设备移动规则的服务器不同。
  - **否**。设备移动规则仅应用于当前管理服务器管理的客户端设备。
  - **未选择值**。条件不适用。

在“**域控制器**”子区域，您可以配置基于域成员包含设备到分类的标准:

- **设备在域组织单元中**

  如果启用此选项，选择范围将包括输入字段中指定的域组织单元中的设备。

  默认情况下已禁用该选项。

- **该设备是域安全组成员**

  如果启用此选项，选择范围将包括输入字段中指定的域安全组中的设备。

  默认情况下已禁用该选项。

在“**网络活动**”子区域，您可以指定根据网络活动包含设备到分类的标准:

- **作为分发点**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准:

  - **是**。选择范围将包括充当分发点的设备。
  - **否**。选择范围将不包括充当分发点的设备。
  - **未选择值**。将不应用标准。

- **不断开与管理服务器的连接**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准:

  - **已启用**。分类将包含选中了“**不断开与管理服务器的连接**”复选框的设备。
  - **已禁用**。分类将包含清空了“**不断开与管理服务器的连接**”复选框的设备。
  - **未选择值**。将不应用标准。

- **连接配置文件已切换**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

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

- **上一次连接到管理服务器**

  您可使用此选框设置按上一次连接到管理服务器的时间搜索设备的标准。

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

  如果清除此选框，则将不会应用标准。

  默认情况下，此复选框未被选中。

- **网络轮询时检测到新设备**

  搜索最近几天通过网络轮询检测到的新设备。

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

  如果禁用此选项，分类将包括通过设备发现检测到的所有设备。

  默认情况下已禁用该选项。

- **设备可见**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

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

设备状态

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

- **设备状态**

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

- **实时保护状态**

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

- **设备状态描述**

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

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

- **数据泄漏防护状态**

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

- **协作服务器保护状态**

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

- **邮件服务器的反病毒保护状态**

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

- **端点传感器状态**

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

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

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

系统详情

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

- **平台类型**

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

- **OS 服务包版本**

  在该字段中，可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- **OS 架构**

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

- **OS 内部版本**

  > 该设置仅应用到 Windows 操作系统。

  操作系统版本号。您可以指定所选操作系统必须具有相同、更早还是更晚的版本号。您也可以配置对所有版本号的搜索，除了指定版本号。

- **OS 发布号**

  > 该设置仅应用到 Windows 操作系统。

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

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

- **这是一台虚拟机**

  在该下拉列表中，您可以选择以下选项：

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

- **虚拟机类型**

  在该下拉列表中，您可以选择虚拟机生产商。

  如果在“**这是一台虚拟机**”下拉列表中选择了“**是**”或“**不重要**”值，则该下拉列表可用。

- **虚拟桌面基础架构的一部分**

  在该下拉列表中，您可以选择以下选项：

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

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

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

- **设备**

  在该下拉列表中，您可以选择单元类型。所有带有该单元的设备被包含在搜索结果。

  该字段支持完整文本搜索。

- **供应商**

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

  该字段支持完整文本搜索。

- **设备名称**

  具有指定名称的设备将包括在该分类中。

- **描述**

  设备或硬件单元的描述。带有该字段中指定的描述的设备将包括在分类范围内。

  可在设备的属性窗口输入任何格式的设备描述。该字段支持完整文本搜索。

- **设备制造商**

  设备制造商的名称。被指定生产商制造的设备将包括在分类范围内。

  您可以在设备的属性窗口中输入制造商的名称。

- **序列号**

  带该字段中指定序列号的所有硬件设备将包括在该分类中。

- **清单号**

  带有该字段中指定的清单编号的设备将包括在选择范围内。

- **用户**

  该字段中指定用户的所有硬件设备都将包括在该分类中。

- **位置**

  设备或硬件单元的位置（例如，在总部或分公司）。在该字段中指定的位置部署的计算机或其他设备将包括在该分类中。

  您可以在该设备的属性窗口中以任何格式描述设备的位置。

- **CPU 时钟频率 (MHz)，从**

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

- **CPU 时钟频率 (MHz)，到**

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

- **虚拟 CPU 内核数量，从**

  虚拟 CPU 内核的最小数量。CPU 与输入字段中指定的虚拟核心数范围（含）匹配的设备将包含在分类中。

- **虚拟 CPU 内核数量，到**

  虚拟 CPU 内核的最大数量。CPU 与输入字段中指定的虚拟核心数范围（含）匹配的设备将包含在分类中。

- **硬盘卷(GB)，从**

  设备上硬盘的最小容量。硬盘与输入字段中指定的容量范围（含）匹配的设备将被包括在分类内。

- **硬盘卷(GB)，到**

  设备上硬盘的最大容量。硬盘与输入字段中指定的容量范围（含）匹配的设备将被包括在分类内。

- **内存大小(MB)，从**

  设备 RAM 的最小容量。RAM 容量与输入字段中的数值范围（含）匹配的设备将被包括在分类内。

- **内存大小(MB)**

  设备 RAM 的最大容量。RAM 容量与输入字段中的数值范围（含）匹配的设备将被包括在分类内。

第三方软件详情

在“**应用程序注册表**”子区域，您可以设置基于已安装的应用程序搜索设备的标准：

- **应用程序名称**

  在该下拉列表中，您可以选择应用程序。安装有指定应用程序的设备将包括在选择范围中。

- **应用程序版本**

  在该输入字段中，您可以指定选定应用程序的版本。

- **供应商**

  在该下拉列表中，您可以选择已安装应用程序的生产商。

- **应用程序状态**

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- **根据更新查找**

  如果启用此选项，则搜索操作将使用相关设备内应用程序更新的有关信息来执行。选中复选框后，“**应用程序名称**”、“**应用程序版本**”和“**应用程序状态**”字段将分别更改为“**更新名称**”、“**更新版本**”和“**状态**”。

  默认情况下已禁用该选项。

- **不兼容安全应用程序名称**

  在该下拉列表中，您可以选择第三方安全应用程序。在搜索过程中，安装有指定程序的设备将包括在选择范围中。

- **应用程序标签**

  在该下拉列表中，您可以选择应用程序标签。所有安装了描述中带有所选标签的应用程序的设备都被包含在设备分类。

- **应用到没有指定标签的设备**

  如果启用此选项，分类将包含未带有所选标签的描述的设备。

  如果禁用此选项，则不应用该标准。

  默认情况下已禁用该选项。

在“**漏洞和更新**”子区域，您可以指定根据 Windows 更新源包含设备到分类的标准：

WUA 已切换到管理服务器

您可以在下拉列表中选择以下搜索选项之一：

- **是**。如果选中该选项，搜索结果会包含从管理服务器收到 Windows Update 更新的设备。
- **否**。如果选中该选项，搜索结果将包含从其它源收到 Windows Update 更新的设备。

卡巴斯基应用程序详情

在“**卡巴斯基应用程序**”子区域，您可以配置基于所选的受管理应用程序包含设备到分类的标准：

- **应用程序名称**

  在下拉列表中，可设置按卡巴斯基应用程序名称执行搜索时在分类中包括设备的标准。

  列表仅提供管理员工作站上已安装管理插件的应用程序的名称。

  如果未选择任何应用程序，则将不会应用该标准。

- **应用程序版本**

  在输入字段，可设置按卡巴斯基应用程序版本号执行搜索时在分类中包括设备的标准。

  如果未指定版本号，则将不会应用该标准。

- **关键更新名称**

  在输入字段中，可设置按应用程序名称或更新包编号执行搜索时在分类中包括设备的标准。

  如果字段留空，则将不会应用该标准。

- **应用程序状态**

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- **选择模块上次更新的时间段**

  您可以使用此选项来设置按这些设备上安装的程序模块上次更新的时间搜索设备的标准。

  如果选中此选框，则您可以在输入字段中指定执行这些设备上安装的程序模块的上一次更新的时间间隔（日期和时间）。

  如果清除此选框，则将不会应用标准。

  默认情况下，此复选框未被选中。

- **设备通过管理服务器管理**

  在下拉列表中，您可以将通过 Kaspersky Next XDR Expert 管理的设备包含在分类中：

  - **是**。应用程序将通过 Kaspersky Next XDR Expert 管理的设备包含在分类中。
  - **否**。如果设备未通过 Kaspersky Next XDR Expert 管理，应用程序会将其包含在分类中。
  - **未选择值**。将不应用标准。

- **安全应用程序已安装**

  在该下拉列表，您可以包含已安装安全应用程序的设备到分类：

  - **是**。应用程序包含安装了安全应用程序的设备到分类。
  - **否**。应用程序在分类中包含未安装安全应用程序的设备。
  - **未选择值**。将不应用标准。

在“**反病毒保护**”子区域，您可以设置基于保护状态包含设备到分类的标准：

- **数据库发布日期**

  如果选择此选项，您可以按反病毒数据库发布日期搜索客户端设备。在该输入字段中，您可以设置执行搜索的时间间隔。

  默认情况下已禁用该选项。

- **数据库记录数**

  如果启用此选项，可以按数据库记录数量搜索客户端设备。在输入字段中，您可以设置反病毒数据库记录数的上限值和下限值。

  默认情况下已禁用该选项。

- **上一次扫描**

  如果启用此选项，您可以按上次恶意软件扫描时间来搜索客户端设备。在该输入字段中，您可以指定执行上一次恶意软件扫描的时段。

  默认情况下已禁用该选项。

- **检测到的威胁**

  如果启用此选项，您可以根据发现的病毒数量来搜索客户端设备。在输入字段中，您可以设置发现病毒总数的上限值和下限值。

  默认情况下已禁用该选项。

在“**加密**”子区域中，您可以配置基于所选的加密算法包含设备到分类的标准：

加密算法

高级加密标准(AES)对称分组密码算法。在下拉列表中，您可以选择加密密钥大小(56 位、128 位、192 位或 256 位)。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

“**应用程序组件**”子部分包含在 OSMP Console 中已安装相应管理插件的应用程序的组件列表。

在“**应用程序组件**”子区域，您可以指定根据所选应用程序组件的状态和版本号包含设备到分类的标准：

- **状态**

  根据应用程序发送到管理服务器的组件状态搜索设备。您可以选择以下状态之一：*N/A*、*已停止*、*已暂停*、*正在开始*、*正在运行*、*已失败*、*未安装*、*不受授权许可支持*。如果安装在受管理设备上的应用程序的所选组件具有指定状态，设备被包含到设备分类。

  由应用程序发送的状态：

  - *已停止* - 组件被禁用且不在工作。
  - *已暂停* - 组件被暂停，例如，在用户在受管理应用程序上停止了保护后。
  - *正在启动* - 组件处于初始化进程中。
  - *运行中* - 组件被启用且在正常工作。

- *已失败* - 组件操作中发生错误。
- *未安装* - 当配置应用程序自定义安装时，用户未选择该组件以安装。
- *不受授权许可支持* – 授权许可不涵盖所选组件。

不同于其他状态，*N/A* 状态不由应用程序发送。该选项显示应用程序没有所选组件状态的信息。例如，这可能发生在所选组件不属于任何在设备上安装的应用程序时，或设备关闭时。

- **版本**

  根据您在列表中选择的版本号搜索设备。您可以输入版本号，例如 `3.4.1.0`，然后指定所选组件是否必须具有相同、更早或更新版本。您也可以配置对所有版本的搜索，除了指定的值。

标签

在“**标签**”区域，您可以基于先前添加到受管理设备的描述的关键字（标签）配置包含设备到分类的标准：

如果至少一个指定的标签匹配则应用

如果启用此选项，搜索结果将显示包含带有所选标签的描述的设备。

如果禁用此选项，搜索结果将仅显示包含带有所有标签的描述的设备。

默认情况下已禁用该选项。

要将标签添加到条件，请单击**添加**按钮，然后通过单击**标签**输入字段来选择标签。指定是否在设备分类中包括或排除具有所选标签的设备。

- **所有带有此标签的设备**

  如果选择了该选项，搜索结果将显示带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

  默认情况下已选定该选项。

- **所有没有此标签的设备**

  如果选择了该选项，搜索结果将显示不带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

用户

在“**用户**”区域，您可以设置根据登录到操作系统的用户账户包含设备到分类的标准。

- **最后一次登录系统的用户**

  如果启用此选项，您可以选择用于配置标准的用户账户。搜索结果包含所选用户上一次登录系统的设备。

- **登录系统至少一次的用户**

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含指定用户至少登录一次的设备。

设备所有者

在“**设备所有者**”部分，您可以根据设备的注册所有者、他们的角色以及他们在安全组中的成员资格来设置将设备纳入选择范围的条件：

- **设备所有者**

  从内部安全组中选择设备所有者的用户名。在本部分中了解有关用户和用户角色的更多信息。

  > 最多只能有一名用户注册为设备所有者。

- **在活动目录安全组中的设备所有者成员关系**

  选择设备所有者所属的外部活动目录安全组。

  > 用户可以是活动目录安全组的一部分，也可以是此活动目录安全组中包含的组的一部分。

- **设备所有者角色**

  选择设备所有者的指定角色。在本文中了解有关用户角色的更多信息。

- **设备所有者在内部安全组中的成员身份**

  选择设备所有者所属的内部安全组。

从设备分类中导出设备列表

Open Single Management Platform 允许您将设备分类中的设备信息保存并导出为 CSV 或 TXT 文件。

若要从设备分类中导出设备列表：

1. 从设备分类中打开包含设备的表格。
2. 使用以下方法之一选择要导出的设备：
   - 要选择特定设备，请选中它们旁边的复选框。
   - 要从当前表格页面选择所有设备，请选中设备表格表头中的复选框，然后选中**全选当前页面**复选框。
   - 要从表中选择所有设备，请选中设备表格表头中的复选框，然后选择**全选**复选框。
3. 单击**导出到 CSV**或**导出到 TXT**按钮。表中包含的有关所选设备的所有信息都将被导出。

> 请注意，如果您将筛选条件应用于设备表，则只有来自显示列的筛选数据将被导出。

在分类中从管理组中删除设备

在使用设备分类时，你可以直接从管理组中删除设备，而不是切换到包含这些设备的管理组。

要从管理组删除设备，请执行以下操作：

1. 在主菜单中，转到“**资产管理**” → “**设备分类**”或者“**发现和部署**” → “**设备分类**”。
2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。
3. 选择要删除的设备，然后单击“**删除**”。
   所选设备即从相应管理组中删除。

设备标签

该部分描述了设备标签，提供了创建和修改它们以及手动或自动标记设备的说明。

设备标签

Open Single Management Platform 支持您*标记*设备。标签是字符串值，可以用于分组、描述或查找设备。分配到设备的标签可以用于创建分类、查找设备以及分发设备到管理组。

您可以手动或自动标记设备。如果您想标记单个设备，则可以使用手动标记。Open Single Management Platform 通过以下方式之一执行自动标记：

- 按照指定的标记规则。
- 通过应用程序。

> 我们不建议您使用不同的标记方式来分配相同的标签。例如，如果标签是由规则分配的，则不建议手动将此标签分配给设备。

如果标签是通过规则分配的，则当满足指定的规则时，设备会自动被标记。每个标签对应一条单独的规则。规则会应用到设备网络属性、操作系统、设备上安装的应用程序以及其他设备属性。例如，您可以设置规则以分配 `[CentOS]` 标签到运行 CentOS 操作系统的所有设备。然后，您可以在创建设备分类时使用此标签；这将帮助您整理所有 CentOS 设备，并向其分配任务。

> 每个标签只能添加一条自动标记规则。如果为同一标签创建新规则，则之前的规则将被替换。

在以下情况下标签从设备上被自动删除：

- 当设备停止满足分配标签的规则的条件时。
- 当分配标签的规则被禁用或删除时。

每个管理服务器的标签列表和规则列表是独立的，包括主管理服务器和从属虚拟管理服务器。规则仅被应用到来自创建规则的相同管理服务器的设备。

创建设备标签

要创建设备标签：

1. 在主菜单中，转到“**资产管理**”→“**标签**”→“**设备标签**”。
2. 单击**添加**。
   新标签窗口打开。
3. 在“**标签**”字段中，输入标签名称。
4. 单击“**保存**”保存更改。

新标签出现在设备标签列表。

重命名设备标签

要重命名设备标签：

1. 在主菜单中，转到“**资产管理**”→“**标签**”→“**设备标签**”。
2. 单击您要重命名的标签名称。
   标签属性窗口打开。
3. 在“**标签**”字段中，更改标签名称。
4. 单击“**保存**”保存设置。

更新的标签出现在设备标签列表。

删除设备标签

您只能删除手动分配的标签。

要删除手动分配的设备标签：

1. 在主菜单中，转到“**资产管理 → 标签 → 设备标签**“。
   显示标签列表。
2. 选择要删除的设备标签。

3. 下一步，单击“**删除**”按钮。

4. 在打开的窗口中，单击“**是**”。

设备标签被删除。删除的标签被从其分配的所有设备上自动删除。

当您删除通过自动标记规则分配给设备的标签时，不会删除该规则，而且当新设备首次满足规则条件时，该标签将被分配给该设备。如果删除自动标记规则，规则条件中指定的标签将从分配了该标签的所有设备中删除，但不会从标签列表中删除。如有必要，您可以手动从列表中删除该标签。

如果此标记由应用程序或网络代理分配给设备，则已删除的标记不会自动从设备中删除。若要管理此类标签，请使用klscflag实用程序。

查看分配了标签的设备

要查看分配了标签的设备：

1. 在主菜单中，转到“**资产管理 → 标签 → 设备标签**“。

2. 单击您要查看所分配设备的标签旁边的“**查看设备**”链接。

   您将被重定向到主菜单的“**资产(设备)**”部分，其中的设备将按您单击“**查看设备**”链接的标签进行过滤。

3. 如果您想返回设备标签列表，单击您浏览器的“**后退**”按钮。

查看已分配标签的设备后，您可以创建并分配新标签，也可以将现有标签分配给其他设备。在这种情况下，您必须按标签删除过滤器，选择设备，然后分配标签。

查看分配到设备的标签

要查看分配到设备的标签：

1. 在主菜单中，转到 “**资产管理**” → “**资产(设备)**”。

2. 单击您要查看其标签的设备名称。

3. 在打开的设备属性窗口中，选择“**标签**”选项卡。

分配给所选设备的标签列表被显示。在“**分配的标签**”列中，您可以看到标签是如何分配的。

在工具栏中，您可以进行以下操作：

- 为设备分配另一个标签。
- 移除已分配的标签。
- 查看管理服务器上存在的所有设备标签。

> 您无法在设备上本地查看分配的标签。

手动标记设备

要手动分配标签到设备：

1. 查看分配到您要分配其他标签的设备的标签。
2. 单击**添加**。
3. 在打开的窗口中，执行以下操作之一：
   - 要创建和分配新标签，请选择“**创建新标签**”，然后指定新标签的名称。
   - 要选择现有标签，请选择“**分配现有标签**”，然后在下拉列表中选择所需标签。
4. 单击“**确定**”应用更改。
5. 单击“**保存**”保存更改。

所选的标签被分配到设备。

从设备上删除分配的标签

要从设备上删除标签：

1. 在主菜单中，转到 “**资产管理**” → “**资产(设备)**”。
2. 单击您要查看其标签的设备名称。
3. 在打开的设备属性窗口中，选择“**标签**”选项卡。
4. 选择您要删除的条目旁边的复选框。

5. 在列表顶部，单击**取消分配标签**按钮。

6. 在打开的窗口中，单击“**确定**”。

标签从设备上删除。

未分配的设备标签不被删除。如果您想，您可以手动删除它。

您不能手动删除应用程序或网络代理分配给设备的标签。若要管理此类标签，请使用klscflag实用程序。

查看自动标记设备规则

要查看自动标记设备规则，

执行以下操作之一：

- 在主菜单中，转到“**资产管理**”→“**标签**”→“**自动标记规则**”。
- 在主菜单中，转到“**资产管理**”→“**标签**”→“**设备标签**”，然后单击“**设置自动标记规则**”链接。
- 查看分配给设备的标签，然后单击“**设置自动标记规则**”按钮。

自动标记设备规则列表出现。

编辑自动标记设备规则

要编辑自动标记设备规则：

1. 查看自动标记设备规则。
2. 单击您要编辑的规则名称。
   规则设置窗口打开。
3. 编辑规则的常规属性：
   a. 在“**规则名称**”字段中，更改规则名称。
      名称不能包括 256 个以上字符。
   b. 执行以下操作之一：
      - 通过将切换按钮切换到“**规则已启用**”来启用规则。
      - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

4. 执行以下操作之一：

   - 如果要添加新条件，请单击“**添加**”按钮，然后在打开的窗口中指定新条件的设置。
   - 如果要编辑现有条件，请单击要编辑的条件名称，然后编辑条件设置。
   - 如果要删除条件，请选中要删除的条件名称旁边的复选框，然后单击“**删除**”。

5. 在条件设置窗口中单击“**确定**”。

6. 单击“**保存**”保存更改。

编辑的规则显示在列表。

创建自动标记设备规则

要创建自动标记设备规则：

1. 查看自动标记设备规则。

2. 单击**添加**。
   新规则设置窗口打开。

3. 配置规则的常规属性：

   a. 在“**规则名称**”字段中，输入规则名称。
   名称不能包括 256 个以上字符。

   b. 执行以下操作之一：

      - 通过将切换按钮切换到“**规则已启用**”来启用规则。
      - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

   c. 在“**标签**”字段中，输入新设备标签名称或从列表中选择现有设备标签之一。
   名称不能包括 256 个以上字符。

4. 在条件区域中，单击“**添加**”按钮以添加新条件。
   新条件设置窗口打开。

5. 输入条件名称。
   名称不能包括 256 个以上字符。名称必须在规则内唯一。

6. 配置规则，使其在满足以下条件时触发（可选择多个条件）：

   - **网络**—设备的网络属性，例如设备的 DNS 名称，或设备是否属于某个 IP 子网。

     如果您用于 Open Single Management Platform 的数据库设置了区分大小写的排序规则，则在指定设备的 DNS 名称时需保留大小写格式。否则，自动标记规则将不起作用。

   - **应用程序** — 设备上是否存在网络代理，操作系统类型、版本、架构和包管理器。

- **虚拟机**—设备属于特定类型的虚拟机。
- **应用程序注册表**—设备上是否存在不同供应商的应用程序。

7. 单击“**确定**”保存更改。

   如果必要，您可以为一个规则设置多个条件。此种情况下，在满足至少一个条件时，标签将被分配到设备。

8. 单击“**保存**”保存更改。

所创建的规则被强加到被所选管理服务器管理的设备。如果设备的设置满足规则条件，标签被分配到设备。

然后，规则被应用到以下情况：

- 自动和间歇性，取决于服务器负载
- 在您编辑规则之后
- 当您手动运行规则时
- 在管理服务器检测到满足规则条件的设备设置的更改或包含此设备的组设置的更改后

您可以创建多个标记规则。如果您创建了多个标记规则且规则对应的条件同时被满足，单个设备可以被分配多个标签。您可以在设备属性中查看所有分配的标签列表。

为自动标记设备运行规则

当规则运行时，规则属性中指定的标签被分配到满足相同规则中指定条件的设备。您仅可以运行活动规则。

要为自动标记设备运行规则：

1. 查看自动标记设备规则。
2. 选择您要运行的活动规则旁边的复选框。
3. 单击**运行规则**按钮。

所选规则被运行。

删除自动标记设备规则

要删除自动标记设备规则：

1. 查看自动标记设备规则。
2. 选择您要删除的规则旁边的复选框。

3. 单击“**删除**”按钮。

4. 在打开的窗口中，单击“**确定**”。

所选规则被删除。规则属性中指定的标签从所有所分配的设备上取消分配。

未分配的设备标签不被删除。如果您想，您可以手动删除它。

数据加密和保护

如果您的笔记本电脑或硬盘驱动器被盗或丢失，数据加密可降低敏感数据和公司数据意外泄露的风险。此外，数据加密还可让您防止未经授权的用户和应用程序进行访问。

如果您的网络包括安装了 Kaspersky Endpoint Security for Windows 的基于 Windows 的受管理设备，您可以使用数据加密功能。在这种情况下，在运行 Windows 操作系统的设备上，您可以管理以下类型的加密：

- BitLocker 驱动器加密®
- 卡巴斯基磁盘加密

我们不建议在 VDI 中启用加密。

通过使用 Kaspersky Endpoint Security for Windows 的这些组件，您可以（例如）启用或禁用加密、查看加密驱动器列表或生成和查看有关加密的报告等活动。

若要配置加密，请在 Open Single Management Platform 中定义 Kaspersky Endpoint Security for Windows 策略。Kaspersky Endpoint Security for Windows 会根据活动策略执行加密和解密。有关如何配置加密功能的规则和描述的详细说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

目前，Web Console 中不提供管理服务器层次结构的加密管理。使用主管理服务器来管理加密的设备。

您可以使用用户界面设置来显示或隐藏与加密管理功能相关的某些界面元素。

查看加密驱动器列表

在 Open Single Management Platform 中，您可以查看有关加密驱动器以及在驱动器级别加密的设备的详细信息。驱动器上的信息解密后，该驱动器将自动从列表中移除。

要查看加密驱动器列表，

在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密驱动器**”。

如果该区域不在菜单上，则表示它已隐藏。在“用户界面设置”中启用“**显示数据加密和保护**”选项来显示该区域。

您可以将加密驱动器列表导出到 CSV 文件或 TXT 文件。为此，请单击**导出到 CSV**或**导出到 TXT**按钮。

查看加密事件列表

在设备上运行数据加密或解密任务时，Kaspersky Endpoint Security for Windows 会将以下类型的事件信息发送给 Open Single Management Platform：

- 无法加密或解密文件，或者由于磁盘空间不足无法创建加密的压缩包。
- 无法加密或解密文件，或者由于授权许可问题无法创建加密的压缩包。
- 无法加密或解密文件，或者由于缺少访问权限无法创建加密的压缩包。
- 应用程序被禁止访问加密文件。
- 未知错误。

要查看在设备上加密数据时发生的事件的列表：

在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密事件**”。

如果该区域不在菜单上，则表示它已隐藏。在“用户界面设置”中启用“**显示数据加密和保护**”选项来显示该区域。

您可以将加密驱动器列表导出到 CSV 文件或 TXT 文件。为此，请单击**导出到 CSV**或**导出到 TXT**按钮。

或者，您可以检查每个受管理设备的加密事件列表。

要查看受管理设备的加密事件：

1. 在主菜单中，转到**资产管理 → 资产(设备)**区域。
2. 单击受管理设备的名称。
3. 在**常规**选项卡上，转到**保护**部分。
4. 单击**查看数据加密错误**链接。

创建和查看加密报告

您可以生成以下报告：

- “受管理设备加密状态报告”。此报告提供有关各种受管理设备的数据加密的详细信息。例如，该报告显示应用已配置加密规则的策略的设备数量。此外，您还可以了解需要重启的设备数量。该报告还包含有关每个设备的加密技术和算法的信息。
- 大容量存储设备加密状态报告。此报告包含与受管理设备加密状态报告类似的信息，但它仅提供大容量存储设备和可移动驱动器的数据。
- 加密驱动器访问权限报告。此报告显示哪些用户账户可以访问加密驱动器。

- “文件加密错误报告”。该报告包含在设备上运行数据加密或解密任务时相关的错误信息。
- “加密文件访问被阻止报告”。该报告包含了阻止应用程序访问加密文件的信息。如果未经授权的用户或应用程序试图访问加密文件或驱动器，此报告会很有帮助。

您可以在“**监控 → 报告**”区域中生成任何报告。或者，在**操作→数据加密和保护**区域中，您可以生成以下加密报告：

- 大容量存储设备加密状态报告
- 加密驱动器访问权限报告
- 文件加密错误报告

*要在**数据加密和保护**区域中生成加密报告：*

1. 确保您启用了界面选项中的“**显示数据加密和保护**”选项。
2. 在主菜单中，转到**操作→数据加密和保护**。
3. 打开以下区域之一：
   - **加密驱动器**可生成大容量存储设备加密状态报告或加密驱动器访问权限报告。
   - **加密事件**可生成文件加密错误报告。
4. 单击您要生成的报告的名称。

报告生成将开始。

授予对处于离线模式的加密驱动器的访问权限

用户可能请求访问加密设备，例如，当受管理设备上未安装 Kaspersky Endpoint Security时。在您收到请求后，您可以创建访问密钥文件并将其发送给用户。Kaspersky Endpoint Security帮助文档中提供了所有使用案例和详细说明。

若要在Kaspersky Endpoint Security for Windows中以离线模式访问加密驱动器：

1. 从用户那里获取请求访问文件（具有 FDERTC 扩展名的文件）。按照 Kaspersky Endpoint Security for Windows 帮助 中的说明在 Kaspersky Endpoint Security for Windows 中生成文件。
2. 在主菜单中，转到“**操作**” → “**数据加密和保护**” → “**加密驱动器**”。

   将显示加密驱动器列表。
3. 选择用户请求访问权限的驱动器。
4. 单击**授予移动模式设备访问权限**按钮。
5. 在打开的窗口中，选择 Kaspersky Endpoint Security for Windows 插件。
6. 按照 Kaspersky Endpoint Security for Windows 帮助 中提供的说明进行操作（请参阅本节末尾的 OSMP Console 操作说明）。

之后用户可以使用收到的文件来访问加密驱动器和读取驱动器上存储的数据。

在管理服务器之间传输加密密钥

如果在受管理设备上启用数据加密功能，加密密钥存储在管理服务器上。加密密钥用于访问加密数据和管理加密策略。

在以下情况下，必须将加密密钥传输到其他管理服务器：

- 重新配置受管理设备上的网络代理，以将该设备分配给其他管理服务器。如果此设备包含加密数据，则必须将加密密钥传输到目标管理服务器。否则，数据将无法解密。
- 对连接到由管理服务器 S1 管理的设备 D1 的可移动驱动器进行加密，然后将该可移动驱动器连接到由管理服务器 S2 管理的设备 D2。要访问该可移动驱动器上的数据，必须将加密密钥从管理服务器 S1 传输到管理服务器 S2。
- 对由管理服务器 S1 管理的设备 D1 上的文件进行加密，然后在由管理服务器 S2 管理的设备 D2 上尝试访问该文件。要访问该文件，必须将加密密钥从管理服务器 S1 传输到管理服务器 S2。

您可以通过以下方式传输加密密钥：

- 自动传输，通过在必须互相传输加密密钥的两个管理服务器的属性中启用“**使用管理服务器层级获取加密密钥**”选项。如果对其中一个管理服务器禁用此选项，则无法自动传输加密密钥。

  在管理服务器属性中启用“**使用管理服务器层级获取加密密钥**”选项后，管理服务器会将其存储库中存储的所有加密密钥发送到层级中上一级的主管理服务器（如果有）。

  当您尝试访问加密数据时，管理服务器首先在其自己的存储库中搜索加密密钥。如果启用了“**使用管理服务器层级获取加密密钥**”选项，并且在存储库中找不到所需的加密密钥，则管理服务器还会向主管理服务器（如果有）发送请求，以提供所需的加密密钥。该请求将发送到所有主管理服务器，直到最高层级的服务器。
- 通过导出和导入包含加密密钥的文件，手动将密钥从一个管理服务器传递到另一个。

  加密密钥的导出和导入是加密密钥管理功能中包含的操作。要执行这些操作，需要通过以下方式为 Open Single Management Platform 用户配置对功能的访问权限：

  - 向自从属管理服务器导出加密密钥的用户授予对加密密钥管理功能的“**读取**”访问权限。
  - 向对目标管理服务器导入加密密钥的用户授予对加密密钥管理功能的“**写入**”访问权限。

要启用在层级内的管理服务器之间自动传输加密密钥：

1. 转到所需管理服务器的属性：
   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。
   b. 在打开的导航窗格中，将鼠标光标悬停在所需管理服务器的名称上，然后单击设置图标 (⚙)。

      或者，您可以单击管理服务器名称，然后在主菜单中显示该名称后，在主菜单中单击该名称以打开服务器属性窗口。
2. 在打开的属性窗口中，选择“**加密算法**”区域。

3. 启用**使用管理服务器层级获取加密密钥**选项。

4. 单击**保存**以应用更改。

下次同步（心跳）时，加密密钥将传输到主管理服务器（如果有）。该管理服务器还将根据请求将其存储库中的加密密钥提供给从属管理服务器。

要在管理服务器之间手动传输加密密钥：

1. 转到要从中导出加密密钥的管理服务器的属性：

   a. 在主菜单中，选择一个区域（“**市场**”、“**控制台导航**”和“**设置**”除外），然后在页面顶部单击“**显示层级**”按钮。

   b. 在打开的导航窗格中，将鼠标光标悬停在所需管理服务器的名称上，然后单击设置图标 (⚙)。

   或者，您可以单击管理服务器名称，然后在主菜单中显示该名称后，在主菜单中单击该名称以打开服务器属性窗口。

2. 在打开的属性窗口中，选择“**加密算法**”区域。

3. 单击**导出加密密钥**。

   确保向从服务器导出加密密钥的用户授予对加密密钥管理功能的“**读取**”访问权限。

4. 在“**从管理服务器导出加密密钥吗?**”窗口中，执行以下操作：

   a. 指定密码以防止文件被未经授权访问。

   b. 指定文件的保存位置。

   记住密码。丢失的密码无法恢复。如果密码丢失，则必须重复导出程序。因此，请记下密码并使其随时可用。

5. 例如，通过共享文件夹或可移动驱动器将文件传输到另一个管理服务器。

6. 转到要向其导入加密密钥的管理服务器的属性。

7. 在属性窗口中，选择“**加密算法**”区域。

8. 单击**导入加密密钥**。

   确保向对服务器导入加密密钥的用户授予对加密密钥管理功能的“**写入**”访问权限。

9. 选择包含加密密钥的文件。

10. 输入密码并单击 **确定**。

加密密钥将传输到目标管理服务器。

更改客户端设备的管理服务器

对于特定客户端设备，您可以将管理服务器更改为不同的管理服务器。为此，请使用“*更改管理服务器*”任务。

要更改管理客户端设备的管理服务器：

1. 连接至管理设备的管理服务器。
2. 创建管理服务器更改任务。

   “新任务向导”启动。遵照向导的说明操作。在新任务向导的“**新任务**”窗口中，选择“**Kaspersky Security Center 16.3**”应用程序和“**更改管理服务器**”任务类型。之后，指定要更改管理服务器的设备：

   - **分配任务到管理组**

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

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

   - **手动指定设备地址或从列表导入地址**

     您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **分配任务到设备分类**

     该任务被分配到设备分类中的设备。您可以指定现有分类之一。

     例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

3. 运行创建的任务。

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

如果管理服务器支持加密和数据保护，并且您正在创建*更改管理服务器*任务，将显示警告。警告声明如果有加密数据存储在设备，在新服务器开始管理设备之后，用户将仅可以访问他之前使用过的加密数据。除此之外，将不会提供对加密数据的访问权限。有关不提供加密数据访问权限的情况的详细说明，请参见 Kaspersky Endpoint Security for Windows 帮助。

当设备显示不活动时查看和配置操作

如果组中的客户端设备不活动，您可以获取关于它的通知。您也可以自动删除此类设备。

要在组中设备显示不活动时查看或配置操作：

1. 在主菜单中，转到“**资产管理**”→“**组层级**”。
2. 通过以下方式之一转到所需管理组的属性：

   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标（⚙）。

管理组属性窗口将开启。

3. 在属性窗口中，转到“**设置**”选项卡。

4. 在“**继承**”区域中，启用或禁用以下选项：

- **从父组继承**

  该区域的设置将从包含客户端设备的父组继承。如果启用该选项，“**网络中的设备活动**”下的设置将被锁定以阻止更改。

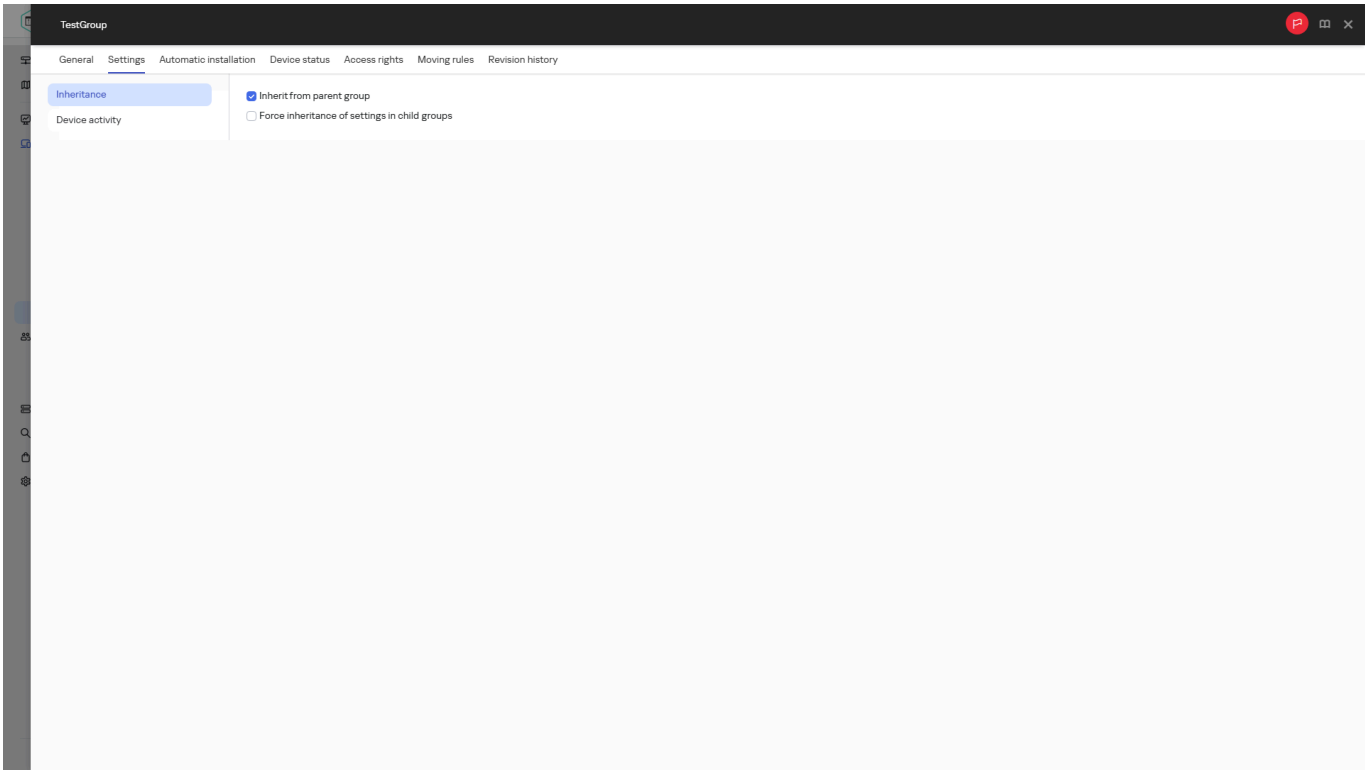
  该选项仅在管理组拥有父组时可用。

  默认情况下已启用该选项。

- **在子组中强制继承设置**

  该设置值将被分发到子组，但在子组的属性中这些设置被锁定。

  默认情况下已禁用该选项。



管理组属性

5. 在“**设备活动**”区域中，启用或禁用以下选项：

- **当设备处于非活动状态超过指定天数时，通知管理员**

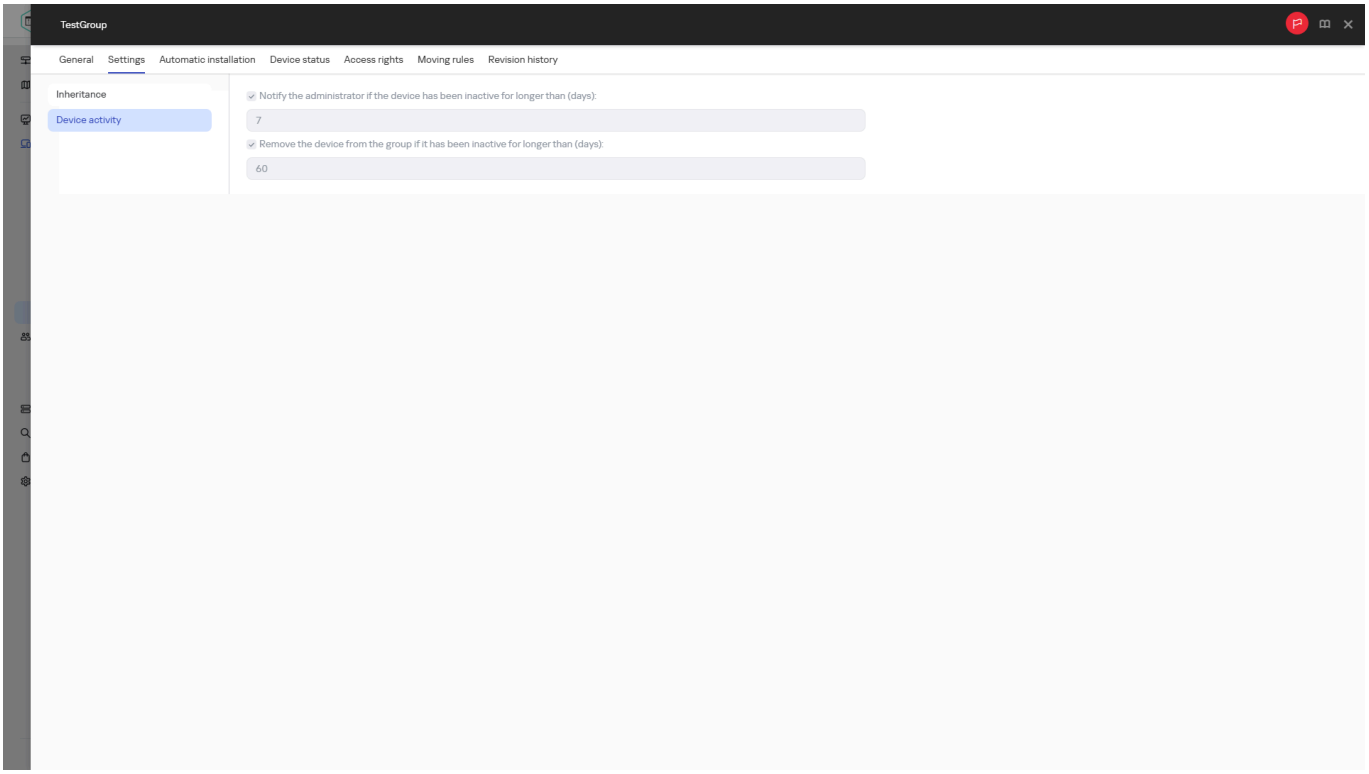
  如果启用该选项，管理员接收不活动设备的通知。您可以指定**设备在网络上已长时间没有活动**事件被创建的时间间隔。默认时间间隔是 7 天。

  默认情况下已启用该选项。

- **当设备处于非活动状态超过指定天数时，从组中删除设备**

  如果启用该选项，您可以指定设备被从组中自动移除的时间间隔。默认时间间隔是 60 天。

默认情况下已启用该选项。



管理组属性

6. 单击“**保存**”按钮。

您的更改已保存并应用。

远程访问受管理设备

您可通过 Open Single Management Platform 建立与受管理设备之间的远程连接。管理员可以通过设备上安装的网络代理获取对受管理设备的远程访问权限。即使客户端设备的 TCP 和 UDP 端口关闭，也可以通过网络代理远程连接至设备。在与设备建立连接后，管理员会获取对此设备上存储的信息的完全访问权限，以便他或她可以管理其上安装的应用程序。

建立远程连接的方法取决于安装有 OSMP 控制台的设备上使用的平台。OSMP 控制台可以安装在除管理服务器设备以外的设备上，即基于 Windows 或 Linux 的设备上。

通过安装在 Linux 设备上的 OSMP 控制台，您可以建立以下连接：

- 使用以下方式到基于 Linux 的受管理设备：
  - 远程桌面连接 (RDP)
  - 虚拟网络计算 (VNC)
- 通过使用以下方式到基于 Windows 的受管理设备：
  - 远程桌面连接 (RDP)
  - 虚拟网络计算 (VNC)

通过安装在 Windows 设备上的 OSMP 控制台，您可以建立以下连接：

- 使用以下方式到基于 Linux 的受管理设备：
  - 远程桌面连接 (RDP)
  - 虚拟网络计算 (VNC)
- 通过使用以下方式到基于 Windows 的受管理设备：
  - 远程桌面连接 (RDP)
  - Windows 桌面共享 (WDS)

从运行Microsoft Windows on Arm的设备访问OSMP控制台时，不支持与托管设备的远程连接。

要建立与设备的远程连接，您必须有：

- klsctunnel 实用程序

  卡巴斯基实用程序用于在受管理设备和管理服务器之间建立隧道连接。

  Open Single Management Platform 支持将 OSMP 控制台的 TCP 连接，经管理服务器和网络代理隧道传输至受管理设备的端口。隧道技术用于在 OSMP 控制台与目标设备无法直接建立连接时，将安装有 OSMP 控制台的设备上的客户端应用程序连接至受管理设备的 TCP 端口。

  如果用于连接到管理服务器的端口在设备上不可用，则需要客户端设备和管理服务器之间的连接隧道。在以下情况下设备端口可能不可用：

  - 远程设备连接到使用 NAT 装置的本地网络。
  - 远程设备是本地网络管理服务器的一部分，但是它的端口被防火墙关闭。

  通过 OSMP 控制台建立远程连接或手动建立远程连接时，可下载该实用程序。klsctunnel 实用程序安装在管理服务器设备上。

  klsctunnel 实用程序用于所有类型的远程连接 (RDP、 VNC、 WDS)。

- RDP 或 VNC 客户端

  RDP 或 VNC 客户端安装在管理服务器设备上。此客户端允许您使用 klsctunnel 实用程序提供的本地连接的地址和端口来获取对受管理设备的远程访问。

  RDP 到用户的当前远程桌面会话的连接是在用户不知道的情况下建立的。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

- Windows 桌面共享（仅适用于基于 Windows 的受管理设备）

  此功能可让您连接至客户端设备上的现有会话而不会断开此会话中的用户。在这种情况下，设备上的管理员和会话用户将共享桌面访问权限。

  当连接到远程桌面的现有会话时，设备上的会话用户会收到来自管理员的连接请求。Kaspersky Next XDR Expert 创建的报告中不会保存有关设备上的远程活动及其结果的任何信息。

  管理员可以在远程客户端设备上配置用户活动的审核。审核期间，应用程序会保存有关客户端设备上管理员打开和/或修改过的文件的信息。

使用 OSMP 控制台从基于 Linux 的设备远程访问基于 Linux 的受管理设备

先决条件

在您开始之前，确保您已做了如下：

- 在运行 Linux 的受管理设备上，安装了网络代理 15.3 或更高版本的安装程序。
- 在运行 Linux 的受管理设备上，安装了 RDP 服务器（如果您使用远程桌面连接连接到受管理设备）。
- 在运行 Linux 的受管理设备上，安装了 VNC 服务器（如果您使用虚拟网络计算连接到受管理设备）。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接（如果您使用远程桌面连接连接到受管理设备）。
- 管理员拥有"**创建通道**"的权限，可建立用于 VNC 的隧道连接（前提是通过虚拟网络计算连接受管理设备）。

要通过在基于 Linux 的设备上打开的 OSMP 控制台，使用 RDP 或 VNC 连接到基于 Linux 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。
   "**连接到远程桌面**窗口将打开。
   如果您选择多个设备、一个移动设备或一个运行macOS 的设备，则"**连接到远程桌面**按钮将被禁用。
3. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。
   下载该实用程序时，请考虑以下事项：
   - 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。
     您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。
   - 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent_srv 目录中。
4. 在**连接到远程桌面**窗口中，指定连接端口。默认端口号是 3389。
5. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。
   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
6. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。
   klsctunnel 实用程序显示远程访问客户端的本地连接的地址和端口。

该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

7. 运行远程访问客户端（RDP 或 VNC），并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立。桌面显示在远程访问客户端窗口中。

使用 OSMP 控制台从基于 Linux 的设备远程访问基于 Windows 的受管理设备

远程桌面连接 (RDP)

先决条件

在您开始之前，确保您已做了如下：

- 受管理设备的操作系统设置中允许远程连接。
- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接。

要通过在基于 Linux 的设备上打开的 OSMP 控制台，使用 RDP 连接到基于 Windows 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。
   “**连接到远程桌面**窗口将打开。
   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择**RDP**连接类型。
4. 如果受管理设备的操作系统设置不允许远程连接，请单击**更改设置**按钮集中允许远程连接。
   如果设置正确，则会显示通知。另外，在受管理设备上，在**设置→系统→远程桌面**部分，**启用远程桌面**选项已启用。
   如果受管理设备的操作系统设置中允许远程连接，则不会显示**更改设置**按钮。
5. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。
   如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序。
6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。
   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。
   klsctunnel 实用程序显示与远程设备的连接的地址和端口。

该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

8. 运行 RDP 客户端并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立。桌面显示在 RDP 客户端窗口中。

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

虚拟网络计算系统 (VNC)

先决条件

在您开始之前，确保您已做了如下：

- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 在运行 Windows 操作系统的受管理设备上，安装了 VNC 服务器。
- 管理员具有**创建通道**权限，可以为 VNC 建立隧道连接。

要通过在基于 Linux 的设备上打开的 OSMP 控制台，使用 VNC 连接到基于 Windows 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。
   "**连接到远程桌面**窗口将打开。
   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则"**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择连接类型**VNC**。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。
   下载该实用程序时，请考虑以下事项：
   - 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。
     您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。
   - 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent 目录中。
5. 在**连接到远程桌面**窗口中，指定 VNC 连接端口。默认端口号是 5900。
6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。
   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。
   klsctunnel 实用程序显示 VNC 客户端本地连接的地址和端口。

该实用程序允许远程用户关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

8. 运行 VNC 客户端并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立。桌面显示在 VNC 客户端窗口中。

使用 OSMP 控制台从基于 Windows 的设备远程访问基于 Linux 的受管理设备

远程桌面连接 (RDP)

先决条件

在您开始之前，确保您已做了如下：

- 在运行 Linux 的受管理设备上，安装了 RDP 服务器。
- 在运行 Linux的受管理设备上，安装了网络代理15.3 或更高版本的安装程序。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接。

要通过在基于 Windows 的设备上打开的 OSMP 控制台，使用 RDP 连接到基于 Linux 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。
   “**连接到远程桌面**窗口将打开。
   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择**RDP**连接类型。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。
   如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序。
5. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。
   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
6. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。
   为此，请选中**使用代理服务器**复选框，然后指定连接设置。
7. 单击“**打开端口**”按钮。
   将打开远程桌面连接登录窗口。
8. 指定您当前用来登录 OSMP 控制台的账户的凭证，然后连接到受管理设备。
   klsctunnel 实用程序显示与远程设备的连接的地址和端口。

该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

在与设备建立连接后，可以在 Microsoft Windows 的远程连接窗口使用桌面。

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

虚拟网络计算系统 (VNC)

先决条件

在您开始之前，确保您已做了如下：

- 在运行 Linux 的受管理设备上，安装了网络代理 15.3 或更高版本的安装程序。
- 在运行 Linux 的受管理设备上，安装了 VNC 服务器。
- 管理员具有**创建通道**权限，可以为 VNC 建立隧道连接。

要通过在基于 Windows 的设备上打开的 OSMP 控制台，使用 VNC 连接到基于 Linux 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。
3. 在**连接到远程桌面**窗口中，选择连接类型**VNC**。
4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

   下载该实用程序时，请考虑以下事项：

   - 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。

     您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。
   - 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent 目录中。
5. 在**连接到远程桌面**窗口中，指定 VNC 连接端口。默认端口号是 5900。
6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。
7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   为此，请选中**使用代理服务器**复选框，然后指定连接设置。
8. 单击“**打开端口**”按钮。

klsctunnel 实用程序显示 VNC 客户端本地连接的地址和端口。

该实用程序允许远程用户关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

9. 运行 VNC 客户端并使用 klsctunnel 实用程序提供的地址和端口将其连接到受管理设备。

与受管理设备的连接已建立。桌面显示在 VNC 客户端窗口中。

使用 OSMP 控制台从基于 Windows 的设备远程访问基于 Windows 的受管理设备

远程桌面连接 (RDP)

先决条件

在您开始之前，确保您已做了如下：

- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 管理员具有**启动 RDP 会话**权限来建立 RDP 连接。
- 受管理设备的操作系统设置中允许远程连接。

要通过在基于 Windows 的设备上打开的 OSMP 控制台，使用 RDP 连接到基于 Windows 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

“**连接到远程桌面**窗口将打开。

如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。

3. 在**连接到远程桌面**窗口中，选择**远程桌面连接**连接类型。
4. 如果受管理设备的操作系统设置不允许远程连接，请单击**更改设置**按钮集中允许远程连接。

如果设置正确，则会显示通知。另外，在受管理设备上，在**设置→系统→远程桌面**部分，**启用远程桌面**选项已启用。

如果受管理设备的操作系统设置中允许远程连接，则不会显示**更改设置**按钮。

5. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序。

6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。

7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

为此，请选中**使用代理服务器**复选框，然后指定连接设置。

8. 单击“**打开端口**”按钮。

   将打开远程桌面连接登录窗口。

9. 指定您当前用来登录 OSMP 控制台的账户的凭证，然后连接到受管理设备。

   klsctunnel 实用程序显示与远程设备的连接的地址和端口。

   该实用程序允许管理员关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

在与设备建立连接后，可以在 Microsoft Windows 的远程连接窗口使用桌面。

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有通知的情况下从会话断开连接。

Windows 桌面共享 (WDS)

先决条件

在您开始之前，确保您已做了如下：

- 在运行 Windows 的受管理设备上，安装了网络代理 13.0 或更高版本。
- 管理员具有**连接到现有 RDP 会话**权限来建立 WDS 连接。
- 漏洞和补丁管理的授权许可处于可用状态。
- 管理员工作站上安装了 Microsoft Windows Vista® 或更高版本。管理服务器设备操作系统的类型对通过 Windows 桌面共享进行连接没有限制。

  检查您的 Windows 版本是否包含 Windows 桌面共享功能，确保 Windows 注册表中存在 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 密钥。

- 客户端设备上安装了 Microsoft Windows Vista 或更高版本。

要通过在基于 Windows 的设备上打开的 OSMP 控制台，使用 VNC 连接到基于 Windows 的受管理设备：

1. 在主菜单中，转到**资产管理→资产(设备)**部分或打开设备分类。
2. 选中要远程连接的受管理设备旁边的复选框，然后单击**连接到远程桌面**按钮。

   “**连接到远程桌面**窗口将打开。

   如果您选择多个设备、一个移动设备或一个运行 macOS 的设备，则“**连接到远程桌面**按钮将被禁用。

3. 在**连接到远程桌面**窗口中，选择连接类型**Windows 桌面共享**。

   如果漏洞和补丁管理授权许可不可用，则会显示错误消息。

4. 单击**下载**按钮下载 klsctunnel 实用程序，然后运行它。

下载该实用程序时，请考虑以下事项：

- 要获取 klsctunnel 实用程序的最新版本，请确保管理服务器可以访问卡巴斯基更新服务器。

  您可以运行*下载更新到管理服务器存储库*任务并选择卡巴斯基更新服务器作为更新源。如果任务成功完成，管理服务器就可以访问卡巴斯基更新服务器。

- 如果实用程序文件无法下载，则会显示一条错误消息。在这种情况下，手动下载实用程序，然后将其放在管理服务器设备的 /var/opt/kaspersky/klnagent 目录中。

5. 在选定设备上活动的可用用户会话列表中，选择要连接的会话。

   远程用户必须允许连接。如果远程用户拒绝连接或者远程用户在超时期限内不允许连接，则会显示错误消息。

6. 单击**生成 Blob**按钮生成具有编码连接参数的文本 blob，然后将文本复制并粘贴到 klsctunnel 实用程序中的相应字段中。

   Blob 包含在管理服务器和受管理设备之间建立连接所需的设置。Blob 有效期为 3 分钟。如果已过期，请生成一个新的 Blob。

7. 在 klsctunnel 实用程序中，如果使用代理服务器，请指定代理服务器连接设置。

   为此，请选中**使用代理服务器**复选框，然后指定连接设置。

8. 单击“**打开端口**”按钮。

   klsctunnel 实用程序显示 VNC 客户端本地连接的地址和端口。

   该实用程序允许远程用户关闭隧道连接。如果隧道连接关闭，则当前与远程桌面的连接将终止。

桌面共享在新窗口中启动。如果要与设备互动，请单击窗口左上角的“菜单”图标 ( )，然后选择**交互模式**。

管理资产

资产代表组织的计算机。您可以将资产添加到 OSMP；在这种情况下，OSMP 在增强事件时会自动添加资产 ID，并且当您分析事件时，您可以获得有关组织中计算机的其他信息。

您可以通过以下方式将资产添加到 OSMP：

- 导入资产：

  - 从 MaxPatrol VM 导入。

  - 按照计划从 **Kaspersky Security Center** 和 KICS for Networks 导入。

    受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

    KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

    - 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本

    - 资产属性信息：漏洞；软件，包括操作系统；资产所有者

若要导入卡巴斯基安全管理中心资产信息：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 点击**导入**，然后选择以下操作之一：
   - 如要导入资产基本属性信息，请点击**导入KSC资产**。
     这将打开**导入KSC资产**窗口。
   - 若要导入资产其他属性信息，请点击**导入KSC资产属性**。
     这将打开**导入KSC资产属性**窗口。
3. 在下拉列表中，选择要为其执行导入操作的租户。
   在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。
   如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。
4. 单击“**导入**”按钮。

将导入资产信息。

此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

默认情况下，资产每 12 小时导入一次，此频率可以配置。也可以按需导入资产；这种按需导入不会影响计划的导入时间。OSMP 从 Kaspersky Security Center 数据库导入已安装 Kaspersky Security Center 网络代理且该代理已连接到 Kaspersky Security Center（即 SQL 数据库中“连接时间”字段非空）的设备的信息。OSMP 导入有关计算机的以下信息：名称、地址、连接到 Kaspersky Security Center 的时间、有关硬件和软件的信息，包括操作系统以及漏洞，即从 Kaspersky Security Center 网络代理接收的信息。

- 通过网页界面或API手动创建资产。
  您可以手动添加资产。在这种情况下，您必须手动指定以下信息：地址、FQDN、操作系统名称和版本、硬件信息。无法通过 Web 界面添加资产的漏洞相关信息。如果您使用 API 添加资产，则可以提供有关漏洞的信息。

您可以管理 OSMP 资产：查看资产信息、搜索资产、添加、编辑或删除资产，以及将资产数据导出为 CSV 文件。

从将资产添加到 OSMP 时起，大约需要 2 分钟，解决方案才能开始使用该资产丰富事件信息。例如，如果在添加资产后的两分钟内发生关联事件，则生成的警报中不会显示该资产。

资产类别

您可以对资产进行分类，然后在过滤条件或关联规则中使用这些类别。例如，您可以为来自较高严重级别类别的资产创建更高严重级别的警报。默认情况下，所有资产都属于“**未分类资产**”类别。一个设备可以添加到多个类别。

默认情况下，OSMP 为资产类别分配以下严重级别：低、中、高、严重。您可以创建自定义类别，类别可以嵌套。

类别可以通过以下方式填充：

- **手动**
- **活动**：如果资产**满足指定条件，**则为动态状态。例如，当资产升级到指定的操作系统版本或放置在指定的子网中时，资产将移动到指定的类别。

  1. 在“**重复分类间隔**”下拉列表中，指定资产关联到类别的频率。您可以选择从每小时一次到每 24 小时一次不等的值。

     您可以通过在类别上下文菜单中选择“**开始分类**”来强制启动分类操作。

  2. 在“**条件**”下，指定用于匹配要添加到资产类别的资产的筛选条件。

     您可以通过单击“**添加条件**”按钮来添加条件。可以通过点击“**添加组**”按钮来添加条件组。组运算符可以在 **AND**、**OR** 和 **NOT** 值之间切换。

     分类过滤器操作数和运算符

操作数	运算符	注释
内部版本号	>、>=、=、<=、<	
操作系统	=, like	“like”运算符确保搜索不区分大小写。
IP 地址	inSubnet、inRange	IP 地址以 CIDR 表示法表示（例如：192.168.0.0/24）。 选择 inRange 运算符时，仅可指示来自私有 IP 地址范围的地址（例如：10.0.0.0–10.255.255.255）。两个地址必须在同一范围内。
FQDN	=, like	“like”运算符确保搜索不区分大小写。
CVE	=, in	“in”运算符允许您指定一个值数组。
软件	=, like	
CII	in	可以选择多个值。
反病毒数据库上次更新	>=、<=	
信息的最后更新时间	>=、<=	
保护上次更新	>=、<=	
系统上次启动	>=、<=	
KSC 扩展状态	in	设备的扩展状态。 可以选择多个值。
实时保护状态	=	在受管理设备上安装的卡巴斯基应用程序的状态。
加密状态	=	
网络保护状态	=	
邮件服务器的反病毒保护状态	=	
数据泄漏防护状态	=	
KSC 扩展状态 ID	=	
端点传感器状态	=	
最后可见日期	>=、<=	

  3. 使用“**测试条件**”按钮，确保指定的过滤器正确无误。单击该按钮后，您应该会看到“**给定条件的资产**”窗口，其中包含满足搜索条件的资产列表。

- **响应式** – 当触发关联规则时，资产将移动到指定的组。

在 OSMP 中，资产按租户和类别进行分类。资产按树形结构排列，其中租户位于根节点，资产类别从根节点分支延伸。您可以在**"资产"→"所有资产"**部分查看租户和类别的树形结构。选择一个树节点后，分配给它的资产将显示在窗口的右侧。如果您指定要递归显示资产，则会显示所选类别的子类别中的资产。您可以选中要查看其资产的租户旁边的复选框。

要打开某个类别的上下文菜单，请将鼠标光标悬停在该类别上，然后单击类别名称右侧显示的省略号图标。上下文菜单中提供以下操作：

类别上下文菜单项

操作	描述
显示资产	在窗口右侧显示所选类别的资产。
递归显示资产	查看所选类别的子类别中的资产。如果要退出递归查看模式，请选择其他类别进行查看。
显示信息	在 Web 界面窗口右侧显示的**类别信息**详情区域中查看有关所选类别的信息。
开始分类	开始将资产自动绑定到所选类别。此选项适用于已启用活动分类的类别。
添加子类别	为所选类别添加子类别。
编辑类别	编辑所选类别。
删除类别	删除所选类别。您只能删除没有资产或子类别的类别。否则，**删除类别**选项处于非活动状态。
固定为选项卡	在单独的选项卡上显示所选类别。您可以通过在相关类别的上下文菜单中选择"**取消固定为选项卡**"来撤消此操作。

添加资产类别

要添加资产类别：

1. 在主菜单中，转到"**资产管理**" → "**资产(设备)**" → "**检测和响应**"。
2. 打开类别创建窗口：
   - 单击"**添加类别**"按钮。
   - 如果要创建子类别，请在父类别的上下文菜单中选择"**添加子类别**"。

   控制台窗口右侧将显示"**添加类别**"详情区域。
3. 添加类别信息：
   - 在"**名称**"字段中，输入类别的名称。该名称必须包含 1 到 128 个 Unicode 字符。
   - 在"**父级**"字段中，指明类别在类别树层次结构中的位置：
     a. 单击 按钮。
     这将打开"**选择类别**"窗口，其中显示类别树。如果您要创建新类别而非子类别，则该窗口可能会显示多个资产类别树，每个可访问的租户对应一个。您在此窗口中选择租户的操作无法撤消。
     b. 选择您正在创建的类别的父类别。
     c. 单击"**保存**"按钮。

     所选类别将显示在"**父级**"字段中。
   - "**租户**"字段显示您在其结构中选择了父类别的租户。租户类别无法更改。

- 在**优先级**下拉列表中为类别分配严重级别。
- 如有必要，您可以在“**描述**”字段中添加最多包含 256 个 Unicode 字符的注释。

4. 在“**分类类型**”下拉列表中，选择如何用资产填充类别。根据您的选择，您可能需要指定其他设置：
   - **手动** — 资产只能手动关联到类别。
   - **活动** — 如果资产满足定义的过滤条件，系统将定期为其分配类别。

     活动资产类别

     1. 在“**重复分类间隔**”下拉列表中，指定资产关联到类别的频率。您可以选择从每小时一次到每 24 小时一次不等的值。

        您可以通过在类别上下文菜单中选择“**开始分类**”来强制启动分类操作。

     2. 在“**条件**”下，指定用于匹配要添加到资产类别的资产的筛选条件。

        您可以通过单击“**添加条件**”按钮来添加条件。可以通过点击“**添加组**”按钮来添加条件组。组运算符可以在 **AND**、**OR** 和 **NOT** 值之间切换。

        分类过滤器操作数和运算符

操作数	运算符	注释
内部版本号	>、>=、=、<=、<	
操作系统	=, like	“like”运算符确保搜索不区分大小写。
IP 地址	inSubnet、inRange	IP 地址以 CIDR 表示法表示（例如：192.168.0.0/24）。 选择 inRange 运算符时，仅可指示来自私有 IP 地址范围的地址（例如：10.0.0.0–10.255.255.255）。两个地址必须在同一范围内。
FQDN	=, like	“like”运算符确保搜索不区分大小写。
CVE	=, in	“in”运算符允许您指定一个值数组。
软件	=, like	
CII	in	可以选择多个值。
反病毒数据库上次更新	>=、<=	
信息的最后更新时间	>=、<=	
保护上次更新	>=、<=	
系统上次启动	>=、<=	
KSC 扩展状态	in	设备的扩展状态。 可以选择多个值。
实时保护状态	=	在受管理设备上安装的卡巴斯基应用程序的状态。
加密状态	=	
网络保护状态	=	
邮件服务器的反病毒保护状态	=	
数据泄漏防护状态	=	
KSC 扩展状态 ID	=	

端点传感器状态	=	
最后可见日期	>=、<=	

3. 使用“**测试条件**”按钮，确保指定的过滤器正确无误。单击该按钮后，您应该会看到“**给定条件的资产**”窗口，其中包含满足搜索条件的资产列表。

- **响应式**– 该类别将使用关联规则来填充资产。

5. 单击“**保存**”按钮。

新类别将添加到资产类别树中。

配置资产表

在 OSMP 中，您可以配置资产表中显示的列的内容和顺序。这些设置存储在您的本地计算机上。

要配置显示资产表的设置：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**” → “**检测和响应**”。
2. 单击资产表右上角的“**设置**”图标 (⚙)。
3. 在下拉列表中，选中要在表中查看的参数旁边的复选框：
   - **名称**
   - FQDN
   - **IP 地址**
   - **类别**
   - MAC **地址**
   - **资产来源**
   - **操作系统**
   - **创建者**
   - **更新日期**
   - **最后可见日期**
   - **租户**–选中此复选框并将该列显示在资产表中后，**租户**列的下拉列表中将提供以下资产筛选选项：
     - **仅显示子实例**– 仅显示所选租户层级结构中子实例的资产。
     - **仅显示父实例**– 仅显示所选租户层级结构中父实例的资产。

       这些选项允许您根据资产所属层级结构的位置筛选资产，从而帮助您专注于更高层级（父实例）或更低层级（子实例）的实例。所选筛选条件将立即应用于资产表。
   - CII **类别**

- **已存档**–选中此复选框并将该列显示在资产表中后，**已存档**的下拉列表中将提供以下资产筛选选项：
  - **是**– 仅显示已归档的资产。
  - **否** –仅显示活动资产。
- **权重**
- KSC **组**
- **遥测数据接收日期**
- **遥测数据状态**
- **EDR状态**
- **上一次连接KSC时间**
- **上一次连接EDR时间**
- **EDR授权许可**
- **EDR代理程序版本**
- **EDR隔离度**
- **AI分数**

选中复选框后，资产表将更新并添加新列。取消选中复选框后，该列将消失。可以根据多列对表进行排序。

4. 如果需要更改列的顺序，请在列名称上单击鼠标左键，然后将其拖动到表中的所需位置。

资产表的显示设置配置完成。

搜索资产

OSMP有两种资产搜索模式。您可以使用窗口左上角的按钮在搜索模式之间切换：

- – 通过以下资产设置进行简单搜索：**名称**、FQDN、IP **地址**、MAC **地址**和**所有者**。
- – 使用条件和条件组过滤器对资产进行高级搜索。

您可以选中找到的资产旁边的复选框，将其数据导出为 CSV 文件。

简单搜索

要使用简单搜索查找资产，

请在 **资产管理** → **资产(设备)** → **检测和响应**部分的 **搜索** 字段中输入搜索查询。

表格将显示“**名称**”、“FQDN”、“IP **地址**”、“MAC **地址**”和“**所有者**”设置与搜索条件匹配的资产。

高级搜索

要使用高级搜索查找资产：

1. 在 **资产管理 → 资产(设备) → 检测和响应**部分中，单击漏斗图标（ ）。
   资产过滤设置显示在窗口的上方区域。

2. 指定资产过滤设置并单击“**搜索**”按钮。
   有关资产过滤设置的详细信息，请参见下表。

该表显示满足搜索条件的资产。

高级资产搜索通过可在窗口上部指定的过滤条件来执行：

- 您可以点击**添加条件**按钮来添加包含用于识别条件的字段的字符串。
- 您可以点击**添加群组**按钮来添加过滤器群组。组运算符可以在 **AND**、**OR** 和 **NOT** 之间切换。
- 可以使用鼠标拖动条件和条件组。
- 可以通过点击 按钮来删除条件、条件群组和过滤器。
- 您可以单击“**折叠**”按钮来折叠过滤选项。在这种情况下，将显示生成的搜索表达式。单击该按钮将再次显示完整的搜索条件。
- 您可以单击“**清除**”按钮来重置过滤选项。
- 右操作数的条件运算符和可用值取决于所选的左操作数：

左操作数	可用运算符	右操作数
内部版本号	=, ilike	任意值。
操作系统	=, ilike	任意值。
IP 地址	inSubnet、inRange	任意值或值的范围。 如果左操作数中的 IP 地址包含在右操作数中指定的子网内，则满足 inSubnet 运算符的筛选条件。例如，IP 地址 10.80.16.206 的子网应在右操作数中使用斜杠表示法指定，如下所示：`10.80.16.206/25`。
FQDN	=, ilike	任意值。
CVE	=, in	任意值。 **in** 运算符用于指定 CVE（通用漏洞披露）ID 数组，例如 `CVE-2017-0143`。
CVSS	>、>=、=、<=、<	0到10之间的数字（资产CVE漏洞的可能严重级别）。 不适用于来自Open Single Management Platform的漏洞。

CVE 计数	>、>=、=、<=、<	数字。该资产中具有 CVE 属性的唯一漏洞数量。没有 CVE 的漏洞不计入此数字。
		如果将`0`指定为右操作数，并选择`=`或`<=`运算符，搜索结果将包含没有CVE漏洞的资产。
		要按特定严重级别的CVE数量进行分类，可以使用组合条件。例如：
		`CVE count >= 1`
		`CVSS >= 6.5`

软件	=, ilike	任意值。

软件版本	=, ilike, in	任意值。资产上安装的软件的版本（内部版本）编号。
资产来源	in	• Open Single Management Platform。 • KICS/KATA。 • 手动创建。
CII	in	• 信息资源不是CII对象。 • 没有重要性类别的CII对象。 • 属于第三类重要性的CII对象。 • 属于第二类重要性的CII对象。 • 属于第一类重要性的CII对象。
RAM（字节）	=、>、>=、<、<=	数字。
磁盘数量	=、>、>=、<、<=	数字。
网卡数量	=、>、>=、<、<=	数字。
磁盘可用空间（字节数）	=、>、>=、<、<=	数字。
KSC 组	=, ilike	任意值。资产所属的Open Single Management Platform管理群组的名称。
反病毒数据库上次更新	>=、<=	对于搜索，时间被指定为UTC时间，然后在KUMA界面中转换为浏览器中设置的本地时区。 您可以通过以下方式之一指定此操作数的日期和时间： • 在日历中选择确切的日期。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动输入一个值：确切的日期和时间、相对时间段，或两者的组合。 有关详细信息，请参阅下面的*使用时间值子*部分。
信息的最后更新时间	>=、<=	对于搜索，时间被指定为UTC时间，然后在KUMA界面中转换为浏览器中设置的本地时区。 您可以通过以下方式之一指定此操作数的日期和时间： • 在日历中选择确切的日期。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动输入一个值：确切的日期和时间、相对时间段，或两者的组合。 有关详细信息，请参阅下面的"*使用时间值*"小节。
保护上次更新	>=、<=	对于搜索，时间被指定为UTC时间，然后在KUMA界面中转换为浏览器中设置的本地时区。 您可以通过以下方式之一指定此操作数的日期和时间： • 在日历中选择确切的日期。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动输入一个值：确切的日期和时间、相对时间段，或两者的组合。 有关详细信息，请参阅下面的*使用时间值子*部分。

系统上次启动	>=、<=	对于搜索，时间被指定为UTC时间，然后在KUMA界面中转换为浏览器中设置的本地时区。 您可以通过以下方式之一指定此操作数的日期和时间： • 在日历中选择确切的日期。 • 在“**相对时间段**”列表中选择相对于当前时间的时间段。 • 手动输入一个值：确切的日期和时间、相对时间段，或两者的组合。 有关详细信息，请参阅下面的“*使用时间值*”小节。
KSC 扩展状态	in	• 安装了网络代理的主机已连接网络，但网络代理未处于活动状态。 • 反病毒应用程序已安装，但实时保护未运行。 • 反病毒应用程序已安装，但未运行。 • 检测到的病毒数量过多。 • 反病毒应用程序已安装，但实时保护状态与安全管理员设置的状态不同。 • 未安装反病毒应用程序。 • 太久未进行病毒全盘扫描。 • 太久未更新反病毒数据库。 • 网络代理程序处于非活动状态太久。 • 旧授权许可。 • 未修复对象数量过多。 • 需要重新启动。 • 主机上安装了不兼容的应用程序 • 主机存在一个或多个漏洞。 • 主机的操作系统已过久未执行更新扫描 • 主机的加密状态无效 • 移动设备设置不符合安全政策的要求。 • 存在尚未处理的事故。 • 主机状态由受管理的应用程序建议。 • 主机上的磁盘空间不足。发生同步错误或磁盘空间不足
实时保护状态	=	• 未知。 • 已停止。 • 已暂停。 • 启动中。 • 运行中（如果反病毒应用程序不支持“运行中”状态类别）。 • 以最大保护级别运行。 • 以最快速度运行。 • 按推荐设置运行。 • 按自定义设置运行。 • 错误。
加密状态	=	• 主机上未配置加密规则。 • 加密正在进行中。 • 用户已取消加密。 • 发生加密错误。 • 所有主机加密规则均已满足。 • 加密正在进行中，必须重启主机。 • 在主机上检测到未指定加密规则的加密文件。
网络保护状态	=	• 未知。 • 已停止。 • 已暂停。 • 启动中。 • 正在运行。 • 错误。 • 未安装。 • 没有授权许可。
邮件服务器的反病毒保护状态	=	• 未知。 • 已停止。 • 已暂停。 • 启动中。 • 正在运行。 • 错误。 • 未安装。 • 没有授权许可。
数据泄漏防护状态	=	• 未知。 • 已停止。 • 已暂停。 • 启动中。 • 正在运行。 • 错误。 • 未安装。 • 没有授权许可。
KSC 扩展状态 ID	=	• 确定。 • 严重。 • 警告。

端点传感器状态	=	• 未知。 • 已停止。 • 已暂停。 • 启动中。 • 正在运行。 • 错误。 • 未安装。 • 没有授权许可。
上一次可见	>=、<=	对于搜索，时间被指定为UTC时间，然后在KUMA界面中转换为浏览器中设置的本地时区。 您可以通过以下方式之一指定此操作数的日期和时间： • 在日历中选择确切的日期。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动输入一个值：确切的日期和时间、相对时间段，或两者的组合。 有关详细信息，请参阅下面的*使用时间值*子部分。
分数 ML	=、>、>=、<、<=	数字。AI服务分配的资产分数。
状态	=, in	AI服务分配的资产状态： • 低。 • 中。 • 高。 • 严重。
自定义资产字段	=, ilike	任意值。搜索资产的自定义字段。

使用时间值

某些条件（例如**反病毒数据库上次更新时间**或**系统上次启动时间**）使用日期和时间作为操作数值。对于这些条件，您可以使用确切日期和时间或相对时间段。

要指定日期和时间值：

1. 选择一个操作数、一个运算符，然后单击日期字段。
2. 执行以下操作之一：

- 在日历中选择确切的日期。

  默认情况下，当前时间会自动添加到所选日期，精度为毫秒。更改日历中的日期不会更改指定的时间。日期和时间会显示在浏览器的时区中。如有必要，您可以在字段中编辑日期和时间。

- 在"**相对时间段**"列表中，选择一个相对时间段。

  该时间段是相对于当前分类的开始时间计算的，并考虑了当时最新的资产信息。例如，对于**反病毒数据库上次更新时间**条件，您可以选择**1 小时**和**>=**运算符，以找到那些反病毒数据库没有更新超过1小时的资产。

- 在日期和时间字段中，手动输入一个值。

  您可以按 **DD.MM.YYYY HH:mm:ss.SSS** 格式（俄语本地化版本）和 **YYYY-MM-DD HH:mm:ss.SSS**（英语本地化版本）输入确切的日期和时间，或者通过公式输入相对时间段。如果需要，您还可以结合使用这些方法。

  如果在输入确切日期时未指定毫秒，系统会自动补填 000。

  在相对时间段公式中，您可以使用 **now** 参数表示当前日期和时间以及间隔参数化语言：**+**、**-**、**/**（四舍五入到最接近的数），以及时间单位：**y**（年）、**M**（月）、**w**（周）、**d**（天）、**h**（小时）、**m**（分钟）、**s**（秒）。

  例如，对于**信息上次更新时间**条件，您可以指定带有**>=**操作员的**now-2d**以及带有**>=**操作员的**now-1d**，以查找信息上次更新时间为搜索开始前一天的资产；或者，您可以指定带有**<=**操作员的**now/w**，以查找信息上次更新时间介于本周第一天的开始时间（UTC 00:00:00:000）和当前时间 **now** 之间的资产。

KUMA 以 UTC 格式存储时间值，但在用户界面中，时间会转换为浏览器所在的时区。这与相对时间段相关：**今天**、**昨天**、**本周**和**本月**。例如，如果浏览器所在的时区是 UTC+3，并且您选择“**今天**”作为时间段，则类别将涵盖从 03:00:00.000 到现在的资产，而不是从 00:00:00.000 到现在的资产。

如果在选择相对时间段（例如**今天**、**昨天**、**本周**或**本月**）时要考虑时区，则需要在日期和时间字段中手动添加时间偏移量，即加上或减去正确的小时数。例如，如果浏览器所在的时区是 UTC+3，并且您希望分类涵盖“**昨天**”这个时间段，则需要将值更改为“**now-1d/d-3h**”。如果您希望分类涵盖“**今天**”这个时间段，请需要将值更改为“**now/d-3h**”。

导出资产数据

您可以将资产表中显示的资产数据导出为 CSV 文件。

要导出资产数据：

1. 配置资产表。

   仅表中指定的数据会写入文件。资产表中各列的显示顺序将保留在导出的文件中。

2. 找到所需的资产并选中它们旁边的复选框。

   通过选中资产表标题左侧的复选框，可以同时选择表中的所有资产。

3. 单击“**导出 CSV**”按钮。

资产数据将写入 assets_<export date>_<export time>.csv 文件。该文件根据您的浏览器设置进行下载。

查看资产详情

要查看有关资产的信息，请使用以下方式之一打开资产信息窗口：

- 在主菜单中，选择**资产管理**部分→选择包含相关资产的类别→选择资产。
- 在主菜单中，选择**警报**→单击带有相关警报的链接→在**相关端点**部分选择资产。
- 在主菜单中，选择**事件**部分→搜索和过滤事件→选择相关事件→单击以下字段之一的链接：SourceAssetID、DestinationAssetID或DeviceAssetID。

资产详情窗口中可能会显示以下信息：

- **名称、IDS** — 资产名称和ID。

  导入OSMP的资产会保留其在源中分配的名称。您可以在 OSMP Web 界面中更改这些资产名称。
- **租户** — 拥有资产的租户的名称。
- **已存档**— 资产的归档状态。可能的值：是、否。
- **KSC群组**— 资产所属的KSC服务器群组。
- **资产源** — 资产信息源。可能存在多个来源。例如，可以在OSMP网页界面中或使用API添加信息，也可以从Open Single Management Platform和KICS/KATA导入信息。

  当使用多个源将有关同一资产的信息添加到OSMP时，您应该考虑合并资产数据的规则。

- **创建时间** — 资产添加到OSMP的日期和时间。
- **更新时间** — 资产信息的最近修改日期和时间。
- **所有者** — 资产的所有者（如有）。
- **IP 地址** — 资产的 IP 地址（如有）。

  如果OSMP中有多个具有相同IP地址的资产，则在按IP地址搜索资产时，始终返回最新添加的资产。如果具有相同 IP 地址的资产可以在您组织的网络中共存，请进行相应规划并使用额外属性来标识这些资产。例如，这在关联过程中可能非常重要。

- **FQDN** — 资产的完全限定域名（如有）。
- **MAC 地址** — 资产的 MAC 地址（如有）。
- **操作系统** — 资产的操作系统。
- **评分** AI是一个数值，用于量化资产活动的非典型程度，以及是否值得关注。**AI状态**字段的可能值为：**低**、**中**、**高**、**严重**。AI评分的取值范围为0到1。
- **隔离状态**是指资产的网络隔离状态。您可以通过点击状态旁边的**设置**链接来查看和更改设备的网络隔离状态。如果资产（设备）上安装了带有内置代理程序的Kaspersky Endpoint Security安全应用程序，则会显示此字段。
- **CII 类别**—有关资产是否为关键信息基础设施 (CII) 对象的信息。
- **相关警报** — 与资产相关的警报（如有）。

  要查看与资产相关的警报列表，请单击“**在警报中查找**”链接。这将打开**警报**选项卡，其中设置了搜索表达式，以过滤具有相应资产ID的所有资产。

- **软件信息**和**硬件信息** — 如果提供了资产软件和硬件参数，则它们将显示在此部分中。
- 资产漏洞信息：
  - **卡巴斯基安全管理中心漏洞** — 资产的漏洞（如有）。此信息适用于从Open Single Management Platform导入的资产。

    单击 图标即可打开卡巴斯基威胁门户，您可以在此了解有关漏洞的更多信息。您还可以通过点击**更新**链接并从Open Single Management Platform请求更新信息来更新漏洞列表。

  - **KICS/KATA漏洞** — 资产的漏洞（如有）。此信息适用于从KICS/KATA导入的资产。
- 资产源信息：
  - **上次出现时间** — 上次从Open Single Management Platform收到有关资产的信息的时间。此信息适用于从Open Single Management Platform导入的资产。
  - **主机 ID** — 从中接收资产信息的开Open Single Management Platform*网络代理程序*的ID。此信息适用于从Open Single Management Platform导入的资产。此ID用于确定资产在Open Single Management Platform中的唯一性。
  - **KICS/KATA 服务器 IP 地址**和**KICS/KATA 连接器 ID** — 从中导入该资产的KICS/KATA实例相关数据。
- **自定义字段**—写入资产自定义字段的数据。

- 有关安装了 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的资产保护设置的其他信息：
  - **KSC 扩展状态 ID** — 资产状态。它可以具有以下值：
    - 确定
    - 严重
    - 警告
  - **KSC 扩展状态**— 有关资产状态的信息。例如，**反病毒数据库太久未更新**。
  - **实时保护状态** — 安装在资产上的卡巴斯基应用程序的状态。例如：**运行中（如果反病毒应用程序不支持“运行中”状态类别）** 。
  - **加密状态** — 有关资产加密的信息。例如：**主机没有任何加密规则**。
  - **垃圾邮件保护状态** — 反垃圾邮件保护的状态。例如，**启动中**。
  - **邮件服务器的反病毒保护状态** — 邮件服务器的病毒防护状态。例如，**启动中**。
  - **数据泄露防护状态** — 数据泄漏防护的状态。例如，**启动中**。
  - **端点传感器状态** — 数据泄漏保护的状态。例如，**启动中**。
  - **反病毒数据库上次更新时间** — 已下载反病毒数据库的版本。
  - **防护上次更新时间** — 反病毒数据库上次更新的时间。
  - **系统上次启动时间** — 系统上次启动的时间。
  - **信息上次更新时间**是指资产上次出现在网络上的时间。对于搜索，时间指定为UTC时间，然后在界面中转换为浏览器中设置的本地时区。

  如果资产是从Open Single Management Platform导入的，则会显示此信息。
- **类别** — 与资产关联的类别（如有）。

点击**移至 KSC 群组**按钮，您可以在Open Single Management Platform管理组之间移动当前查看的资产。您还可以点击**启动任务**下拉列表来运行资产上可用的任务：

- 通过单击KSC **响应**按钮，您可以在资产上启动Open Single Management Platform任务。
- 点击KEDR **响应**按钮，即可对资产运行Kaspersky Endpoint Detection and Response任务。
- 点击**刷新 KSC 资产**按钮，即可运行一项任务，从Open Single Management Platform刷新有关该资产的信息。

当与Open Single Management Platform集成以及与Kaspersky Endpoint Detection and Response集成时，这些任务可用。

添加资产

您可以通过以下方式添加资产信息：

- 手动。
  您可以使用 OSMP 控制台或 API 添加资产。
- 导入资产。
  您可以**从 Kaspersky Security Center**、KICS for Networks 和 MaxPatrol VM 导入资产。

  受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

  KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

  - 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
  - 资产属性信息：漏洞；软件，包括操作系统；资产所有者

  若要导入卡巴斯基安全管理中心资产信息：

  1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
  2. 点击**导入**，然后选择以下操作之一：
     - 如要导入资产基本属性信息，请点击**导入KSC资产**。
       这将打开**导入KSC资产**窗口。
     - 若要导入资产其他属性信息，请点击**导入KSC资产属性**。
       这将打开**导入KSC资产属性**窗口。
  3. 在下拉列表中，选择要为其执行导入操作的租户。
     在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。
     如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。
  4. 单击“**导入**”按钮。

  将导入资产信息。

  此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

添加资产时，OSMP 中已经存在的资产可以与正在添加的资产合并。

资产合并算法：

1. 检查 Kaspersky Security Center 或 KICS for Networks 资产的唯一性。

   - 从 Kaspersky Security Center 导入的资产的唯一性由“**主机 ID**”参数确定，该参数包含 Kaspersky Security Center *网络代理*标识符。如果两个资产的 ID 不同，则它们将被视为单独的资产，不会合并。
   - 从 KICS for Networks 导入的资产的唯一性由“**IP 地址**”、“**KICS for Networks 服务器 IP 地址**”和“**KICS for Networks 连接器 ID**”参数的组合决定。如果两个资产的任意参数不同，则它们将被视为单独的资产，不会合并。

   如果比较的资产匹配，则进一步执行算法。

2. 确保“**IP**”、“**MAC**”和“**FQDN**”字段中的值匹配。

   如果至少两个指定字段匹配，则资产可以合并，前提是其他字段为空。

   可能的匹配情况：

   - 资产的 FQDN 和 IP 地址匹配。**MAC** 字段为空。

     针对整个 IP 地址值数组执行检查。如果 FQDN 中包含资产的 IP 地址，则认为值匹配。

   - 资产的 FQDN 和 MAC 地址匹配。“**IP**”字段为空。

     针对整个 MAC 地址值数组执行检查。如果数组中至少有一个值与 FQDN 完全匹配，则认为值匹配。

   - 资产的 IP 地址和 MAC 地址匹配。“**FQDN**”字段为空。

     针对整个 IP 和 MAC 地址值数组执行检查。如果数组中至少有一个值完全匹配，则认为值匹配。

3. 确保“**IP**”、“**MAC**”或“**FQDN**”字段中至少有一个值匹配，前提是其中一个资产或两个资产的其他两个字段未填写。

   如果字段中的值匹配，则资产会合并。例如，如果 KUMA 资产指定了 FQDN 和 IP 地址，而导入的资产仅指定了相同值的 IP 地址，则字段匹配。在这种情况下，资产会合并。

   对于每个字段，验证将单独执行，并在首次匹配时结束。

资产字段比较示例显示在此处。

有关资产的信息可以从各种来源生成。如果添加的资产和 OSMP 资产包含从同一来源接收的数据，则此数据会被覆盖。例如，Kaspersky Security Center 资产在导入 OSMP 时会收到完全限定域名、软件信息和主机 ID。从 Kaspersky Security Center 导入具有相同完全限定域名时，所有这些数据都将被覆盖（如果已为添加的资产配置了这些数据）。可更新数据表中列出了所有可以刷新数据的字段。

可更新数据

字段名称	更新程序
名称	根据以下优先级选择： • 手动定义。 • 从 Kaspersky Security Center 接收。 • 由 KICS for Networks 接收。
所有者	根据以下优先级选择来自源的第一个值： • 从 Kaspersky Security Center 接收。 • 手动定义。

字段名称	更新程序
IP 地址	数据将进行合并。如果地址数组包含相同的地址，则会删除重复地址的副本。
FQDN	根据以下优先级选择来自源的第一个值： • 从 Kaspersky Security Center 接收。 • 由 KICS for Networks 接收。 • 手动定义。
MAC 地址	数据将进行合并。如果地址数组包含相同的地址，则会删除其中一个重复的地址。
操作系统	根据以下优先级选择来自源的第一个值： • 从 Kaspersky Security Center 接收。 • 由 KICS for Networks 接收。 • 手动定义。
漏洞	KUMA 资产数据通过所添加资产的信息进行补充。在资产详情中，数据按源名称进行分组。 针对每个来源单独消除漏洞。
软件信息	始终记录来自 KICS for Networks 的数据（如果可用）。 对于其他源，将根据以下优先级选择第一个值： • 从 Kaspersky Security Center 接收。 • 手动定义。
硬件信息	根据以下优先级选择来自源的第一个值： • 从 Kaspersky Security Center 接收。 • 通过 API 定义。

更新后的数据将显示在资产详情中。您可以在 OSMP 控制台中查看资产详情。

添加新资产时，此数据可能会被覆盖。如果用于生成资产信息的数据超过 30 天未从源更新，则该资产将被删除。下次从相同源添加资产时，将创建新资产。

如果您使用 OSMP 控制台编辑从 Kaspersky Security Center 或 KICS for Networks 收到的资产信息，则可以编辑以下资产数据：

- Name。
- 类别。

如果资产信息是手动添加的，则在 OSMP 控制台中编辑这些资产时可以编辑以下资产数据：

- Name。
- 拥有资产的租户的名称。
- IP 地址。
- 完全限定域名。
- MAC 地址。
- 所有者。
- 类别。
- 操作系统。
- 硬件信息。

无法通过 REST API 编辑资产数据。从 REST API 导入时，数据将根据上述合并资产详情规则进行更新。

在OSMP中添加资产信息

若要在OSMP中添加资产：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**” → “**检测和响应**”，然后单击“**添加**”。
   “**添加资产**”详情区域在窗口右侧打开。
2. 输入资产参数：
   - **资产名称**（必填）
   - **租户**（必填）
   - **IP 地址**和/或**FQDN**（必填）。您可以通过单击“**添加 FQDN**”指定多个 FQDN。
   - **MAC 地址。**
   - **所有者。**
3. 如有必要，请管理以下选项卡中的设置：
   - **附加** 选项卡包含有关资产所有者、类别和操作系统的信息。
   - **硬件**选项卡包含有关资产硬件的信息。
4. 单击“**添加**”。

   资产会在分配给它的类别或“**未分类资产**”类别的资产表中创建和显示。

从 Kaspersky Security Center 导入资产信息

受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

- 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
- 资产属性信息：漏洞；软件，包括操作系统；资产所有者

若要导入卡巴斯基安全管理中心资产信息：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 点击**导入**，然后选择以下操作之一：
   - 如要导入资产基本属性信息，请点击**导入KSC资产**。
     这将打开**导入KSC资产**窗口。

- 若要导入资产其他属性信息，请点击**导入KSC资产属性**。

  这将打开**导入KSC资产属性**窗口。

3. 在下拉列表中，选择要为其执行导入操作的租户。

   在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。

   如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。

4. 单击“**导入**”按钮。

将导入资产信息。

此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

从 MaxPatrol 导入资产信息

您可以将资产信息从 MaxPatrol VM 导入 XDR。导入的资产显示在“**资产**”组中。如有必要，您可以编辑资产的设置。

从 MaxPatrol VM 导入资产信息

OSMP 分发包中包括 kuma-ptvm 实用程序，该实用程序由可执行文件和配置文件组成。该实用程序在 Windows 和 Linux 操作系统上受支持。该实用程序允许您连接到 MaxPatrol VM API 以获取有关设备及其属性（包括漏洞）的数据，还允许您编辑资产数据并使用 XDR API 导入数据。MaxPatrol VM 版本 1.1 至 2.7（含）支持导入数据。

配置将资产信息从 MaxPatrol VM 导入 KUMA Core 的操作包含以下步骤：

1. 准备 XDR 和 MaxPatrol VM。

   您必须为 API 操作创建用户账户和 XDR 令牌。

2. 创建包含数据导出和导入设置的配置文件。

3. 使用 kuma-ptvm 实用程序将资产数据导入 KUMA Core：

   a. 数据从 MaxPatrol VM 导出并保存在实用程序的目录中。每个租户的信息以 JSON 格式保存到单独的文件中。

      如有必要，您可以编辑收到的文件。

   b. 文件中的信息会被导入 KUMA Core。

重新导入现有资产时，KUMA Core 中已存在的资产将被覆盖。这样一来，已修复的漏洞将被移除。

已知限制：

- 如果两个具有不同 FQDN 的资产指定了相同的 IP 地址，KUMA Core 会将其作为两个不同的资产导入。这些资产不会被合并。

- 如果一项资产包含两个软件，且其名称、版本和供应商字段中的数据相同，则 KUMA Core 会将此数据作为一个软件导入，即使该资产中的软件安装路径不同。

- 如果资产的 FQDN 包含空格或下划线 (_)，则此类资产的数据不会被导入 KUMA Core。事件日志会显示导入时跳过了这些资产。
- 如果导入过程中发生错误，则错误详情会被记录且导入会停止。

准备操作：

1. 在 XDR 和 MaxPatrol VM 中创建一个单独的用户账户，并赋予其使用 API 请求所需的最低权限。
2. 创建稍后将为其生成 API 令牌的用户账户。
   对生成 API令牌的账户的要求：
   - 主管理员、租户管理员、2 级分析师或 1 级分析师角色。
   - 访问将导入资产的租户。
   - 在用户账户的 API 访问权限下，选中 POST /xdr/api/v2.1/kuma/assets/import 的复选框。
3. 生成用于访问 XDR REST API 的令牌。
4. 将 kuma-ptvm 实用程序复制到托管 KUMA Core 的服务器，并通过运行以下命令将该实用程序的文件设置为可执行：

   ```
   chmod +x <path to the kuma-ptvm file on the server hosting the KUMA Core>
   ```

要创建配置文件：

1. 转到 KUMA 实用程序文件夹：

   ```
   cd /opt/kaspersky/kuma/utils/
   ```

2. 复制 kuma-ptvm-config-template.yaml 模板以创建名为 kuma-ptvm-config.yaml 的配置文件：

   ```
   cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
   ```

3. 编辑 KUMA-ptvm-config.yaml 配置文件中的设置。
4. 将更改保存到文件。

配置文件将被创建。

要导入资产信息：

1. 如果要将资产信息从 MaxPatrol VM 导入 KUMA Core，而不对导出的数据进行中间验证，请使用以下选项运行 kuma-ptvm 实用程序：

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download --upload`

2. 如果要在将从 MaxPatrol VM 导出的数据导入 KUMA Core 之前检查其正确性：

   a. 请使用以下选项运行 kuma-ptvm 实用程序：

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download`

对于配置文件中指定的每个租户，将创建一个单独的文件，其名称格式为 <租户 ID>.JSON。此外，在导出期间，将创建一个“租户”文件，其中包含要上传到 KUMA Core 的 JSON 文件列表。所有文件都保存在该实用程序的目录中。

b. 检查导出的资产文件，如有必要，请进行以下编辑：

- 将资产分配给相应的租户。
- 手动将资产数据从“默认”租户文件传输到相关租户的文件。
- 在“租户”文件中，编辑要将其资产导入 KUMA Core 的租户列表。

c. 将资产信息导入 KUMA Core：

```
kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --upload
```

要查看该实用程序可用命令的信息，请运行 --help 命令。

资产信息将从 MaxPatrol VM 导入 KUMA Core。控制台显示新增和已更新资产数量的信息。

可能的错误：

运行 kuma-ptvm 实用程序时，可能会返回 `tls: failed to verify certificate: x509: certificate is valid for localhost` 错误。

解决问题的办法：

- 根据 MaxPatrol 文档颁发证书。建议通过这种方式解决错误。
- 禁用证书验证。
  要禁用证书验证，请在配置文件的“MaxPatrol 设置”部分中添加以下行：
  `ignore_server_cert: true`

这样一来，实用程序启动时不会出现错误。

从 MaxPatrol VM 导入资产信息

OSMP 分发包中包括 kuma-ptvm 实用程序，该实用程序由可执行文件和配置文件组成。该实用程序在 Windows 和 Linux 操作系统上受支持。该实用程序允许您连接到 MaxPatrol VM API，以获取设备及其属性（包括漏洞）的相关数据，还可编辑资产数据并使用 KUMA API 导入数据。MaxPatrol VM 版本 1.1 至 2.7（含）支持导入数据。

配置将资产信息从 MaxPatrol VM 导入 OSMP 涉及以下步骤：

1. 准备 KUMA 和 MaxPatrol VM。
   您必须创建用户账户和 OSMP 令牌以执行 API 操作。
2. 创建包含数据导出和导入设置的配置文件。
3. 使用 kuma-ptvm 实用程序将资产数据导入 OSMP：

   a. 数据从 MaxPatrol VM 导出并保存在实用程序的目录中。每个租户的信息以 JSON 格式保存到单独的文件中。
   如有必要，您可以编辑收到的文件。

   b. 将文件中的信息导入 OSMP。

重新导入现有资产时，OSMP 中已存在的资产将被覆盖。这样一来，已修复的漏洞将被移除。

已知限制

如果为两个具有不同 FQDN 的资产指定了相同的 IP 地址，OSMP 会将其作为两个不同的资产导入，而不会将它们合并。

如果一个资产中的两个软件在名称、版本和供应商字段中具有相同的数据，则即使它们在该资产中的安装路径不同，OSMP 也会将这些数据作为一个软件导入。

如果在 kuma-ptvm-config.yaml 配置文件中将 `strict_import` 设置为 false，则会从 MaxPatrol 导入所有资产的数据，包括缺少 OSMP 所要求字段的资产，以及字段值不符合 OSMP 要求的资产。如果资产的 FQDN 包含空格或下划线（"_"），则不会将此类资产的数据导入 OSMP，并且日志会显示导入过程中跳过了这些资产。

如果导入过程中发生错误，则错误详情会被记录且导入会停止。

准备工作

1. 在 OSMP 和 MaxPatrol VM 中分别创建一个用户账户，并为其授予使用 API 请求所需的最低权限集。
2. 创建稍后要为其生成 API 令牌的用户账户。
   对生成 API令牌的账户的要求：
   - 主管理员、租户管理员、二级分析师或一级分析师角色。
   - 访问将导入资产的租户。
   - 在用户账户的 **API 访问权限** 下，选中 POST/api/v1/assets/import 对应的复选框。
3. 生成用于访问 OSMP REST API 的令牌。

创建配置文件

要创建配置文件：

1. 运行以下命令，转到 OSMP 清单文件的 utils 部分中指定的主机目录：

   ```
   cd /opt/kaspersky/kuma/utils/
   ```

2. 运行以下命令解压 kuma-ptvm.tar.gz 压缩文件：
   `tar -xvf kuma-ptvm.tar.gz`

3. 根据所需的资产导入方式创建配置文件：

   - 要导入所有资产，请复制 `kuma-ptvm-config-template.yaml` 模板，创建名为 `kuma-ptvm-config.yaml` 的配置文件：

     ```
     cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
     ```

   - 要仅导入符合筛选条件的资产，请复制 `kuma-ptvm-vulnerable-assets-config-template.yaml` 模板，并创建名为 `kuma-ptvm-vulnerable-assets-config.yaml` 的配置文件：

     ```
     cp kuma-ptvm-vulnerable-assets-config-template.yaml kuma-ptvm-vulnerable-assets-config.yaml
     ```

4. 根据所选的资产导入方式，编辑 kuma-ptvm-config.yaml 配置文件中的设置或 kuma-ptvm-vulnerable-assets-config-template.yaml 配置文件中的设置。

5. 将更改保存到文件。

配置文件将被创建。转到“导入资产数据”步骤。

导入资产数据

要将资产信息从 MaxPatrol VM 导入 OSMP，请使用 kuma-ptvm 实用程序以及在上一步中创建的配置文件。

要导入资产信息：

1. 如果要在不对导出的数据进行中间验证的情况下将资产信息从 MaxPatrol VM 导入 OSMP，请根据所选的资产导入方式，使用以下选项运行 kuma-ptvm 实用程序：

   - 要导入所有资产：

     ```
     ./kuma-ptvm --config <path> --download --upload
     ```

     其中：

     <path> 是 `kuma-ptvm-config.yaml` 配置文件的完整路径。

   - 要导入根据配置文件中指定的参数筛选的资产：

     ```
     kuma-ptvm vulnerable-assets-api --config <path> --download --upload
     ```

     其中：

     <path> 是 `kuma-ptvm-vulnerable-assets-config.yaml` 配置文件的完整路径。

2. 如果要在将 MaxPatrol VM 导出的数据导入 OSMP 之前对其进行验证，请根据所选的资产导入方式运行以下命令之一：

   - 要导入所有资产，请使用以下选项运行 kuma-ptvm 实用程序：

     ```
     ./kuma-ptvm --config <path> --download
     ```

- 要导入根据配置文件中指定的参数筛选的资产：

```
kuma-ptvm vulnerable-assets-api --config <path> --download
```

其中：

<path> 是相应配置文件的完整路径：`kuma-ptvm-config.yaml` 或 `kuma-ptvm-vulnerable-assets-config.yaml`。

如有必要，可以使用 `--cvss-version <CVSS version number>` 选项指定要加载其资产漏洞值的 CVSS 版本。可用值：

- `2` 仅加载 CVSS 版本 2 的值。
- `3` 仅加载 CVSS 版本 3 的值。如果漏洞仅有版本 2 的描述，则 CVSS 字段为空。
- `latest`（默认）加载最新可用 CVSS 版本的值。如果漏洞没有 CVSS 版本 3 的值，则使用版本 2 的值。

示例：

```
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 2 --download
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 3 --download
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version latest --download
```

其中：

<path> 是相应配置文件的完整路径：`kuma-ptvm-config.yaml` 或 `kuma-ptvm-vulnerable-assets-config.yaml`。

对于配置文件中指定的每个租户，都会创建一个名为 <OSMP_tenant_ID>.json 的单独文件。此外，还会创建一个“tenants”文件，其中包含要上传到 OSMP 的 JSON 文件列表。所有文件都保存在该实用程序的目录中。

a. 检查导出的资产文件，如有必要，请进行以下编辑：

- 将资产分配给相应的租户。
- 手动将资产数据从“默认”租户文件传输到相关租户的文件。
- 在“tenants”文件中，编辑要将其资产导入 OSMP 的租户列表。

b. 运行以下命令之一，将资产信息导入 OSMP：

- 要导入所有资产：

```
./kuma-ptvm --config <path> --upload
```

- 要导入根据配置文件中指定的参数筛选的资产：

```
kuma-ptvm vulnerable-assets-api --config <path> --upload
```

其中：

<path> 是相应配置文件的完整路径：`kuma-ptvm-config.yaml` 或 `kuma-ptvm-vulnerable-assets-config.yaml`。

要查看该实用程序的可用命令信息，请运行 `--help` 命令。

资产信息从 MaxPatrol VM 导入 OSMP。控制台显示新增和已更新资产数量的信息。

可能的错误

运行 kuma-ptvm 实用程序时，可能会返回 `tls: failed to verify certificate: x509: certificate is valid for localhost` 错误。

解决方案：

- 根据 MaxPatrol 文档颁发证书。建议通过这种方式解决错误。
- 禁用证书验证。
  要禁用证书验证，请在配置文件的 `MaxPatrol settings` 部分中添加以下行：
  `ignore_server_cert: true`

这样一来，实用程序启动时不会出现错误。

kuma–ptvm–config.yaml 配置文件设置

该表列出了您可以在 `kuma-ptvm-vulnerable-assets-config-template.yaml` 文件中指定的设置。

kuma-ptvm-vulnerable-assets-config-template.yaml 配置文件设置说明

设置	描述	值
`General settings` 部分		
`log_level`	可选设置。 日志记录级别。	可用值： • `trace` • `info` • `warning` • `error` 默认设置：`info`。
`period`	可选设置。 从 MaxPatrol 导出在指定时间段内发生变化的资产数据。	无限制。 默认设置：`30d`。
`strict_import`	可选设置。 从 MaxPatrol 导出资产时，请检查是否填写了 KUMA 的必填字段。请勿从 MaxPatrol 导出未经验证的资产。	可用值： • `true` 用于检查是否存在 KUMA 所需字段。 • `false` 用于跳过对是否存在 KUMA 所需字段的检查。 默认值为 `false`。 从 MaxPatrol 导出资产时，我们建议指定 `true`，这样便可在将资产导入 KUMA 之前检测并修复 JSON 文件中可能存在的错误。
`parallel_downloading`	可选设置。 设置从 MaxPatrol 导入数据时的下载模式。	可用值： • `true` 并行下载 CSV 文件。 • `false` 按顺序下载 CSV 文件，以减轻 MaxPatrol 的负载。 默认设置为 `true`。 如果需要在数据导入期间减轻 MaxPatrol 的负载，我们建议指定 `false`。
`KUMA settings` 部分		
`endpoint`	必需设置。 KUMA API 服务器的 URL。例如，kuma.example.com:7223	–
`token`	必需设置。 KUMA API 令牌。	–

设置	描述	值
`ignore_server_cert`	可选设置。 KUMA 证书验证。	可用值： • `true` 可禁用 KUMA 证书验证。 • `false` 可启用 KUMA 证书验证。 此设置未包含在配置文件模板中。您可以手动添加此设置并将其设置为“true”，这将阻止 kuma-ptvm 实用程序在启动时验证证书。
`MaxPatrol settings` 部分		
`endpoint`	必需设置。 MaxPatrol API 服务器的 URL。	–
`user`	可选设置。 MaxPatrol API 用户名。	–
`password`	可选设置。 MaxPatrol API 用户密码。	–
`secret`	可选设置。 MaxPatrol API 密钥。	–
`token`	可选设置。 MaxPatrol API 令牌。	要通过 API 访问 MaxPatrol 服务器，请指定 `user`、`password` 和 `secret` 参数的值，或 `token` 参数的值。
`ignore_server_cert`	可选设置。 MaxPatrol 证书的验证。	可用值： • `true` 用于禁用 MaxPatrol 证书验证。 • `true` 用于启用 MaxPatrol 证书验证。 此设置未包含在配置文件模板中。如果发生 `tls: failed to verify certificate: x509: certificate is valid for localhost` 错误，您可以手动添加此设置并将其值设为 true。在这种情况下，kuma-ptvm 实用程序在启动时不会验证证书。 建议优先按照 MaxPatrol 文档中的说明颁发证书，以此解决该错误。
`Vulnerable Assets API Parameters` 部分 存在一项限制：当前 Swagger 合约中提供了 `from` 和 `to` 参数，但是否支持这些参数取决于已部署的 PTVM 版本。		
`groups`	可选设置。 用于筛选的资产组 ID 列表。导入操作仅包含属于指定组的资产。	例如： 4b7d711f-ae35-4c94-8625-4cfabf5fb99e
`statuses`	可选设置。 待筛选资产的漏洞状态。	可用值： • `new` 表示漏洞是新发现的。 • `inProgress` 表示漏洞正在修复。 • `awaitingFix` 表示漏洞正在等待修复。 • `excluded` 表示漏洞已被排除在处理范围之外。 • `fixed` 表示漏洞已修复。 • `overdue` 表示漏洞已超过修复期限。 • `stale` 表示漏洞已过时。
`severities`	可选设置。 待筛选资产的漏洞严重级别。	可用值： • `none` 表示未设置严重级别。 • `low` • `medium` • `high` • `critical`
`from`	可选设置。 按资产上次审计日期进行筛选的起始日期和时间（含）。UTC。	例如： [待定]
`to`	可选设置。 按资产上次审计日期进行筛选的截止日期和时间（含）。UTC。	例如： [待定]
`Vulnerability filter` 部分		
`only_exploitable`	可选设置。 仅从 MaxPatrol 中导出存在漏洞且已知漏洞利用手段的资产。	可用值： • `true` 用于仅导出存在已知漏洞利用方式的漏洞的资产。 • `false` 用于导出所有资产。 默认设置：`false`。

设置	描述	值
`min_severity`	可选设置。 仅导入指定级别或更高级别的漏洞。	可用值： • `low` • `medium` • `high` • `critical` 默认值：`low`。
`Tenant map` 部分		
`id`	必需设置。 KUMA 中的租户 ID。 资产按照配置文件中指定租户的顺序分配给租户：租户在列表中的位置越高，其优先级越高。这意味着您可以指定重叠的子网。	–
`fqdn`	可选设置。 用于搜索资产 FQDN 的正则表达式。	–
`networks`	可选设置。 一个或多个子网。	–
`default_tenant`	可选设置。 用于存储无法分配给"租户"部分中指定租户的资产相关数据的默认 KUMA 租户。	–

从 KICS for Networks 导入资产信息

受卡巴斯基安全管理中心保护的资产的相关信息可以导入KUMA。为此，您需要提前配置应用程序之间的集成。

配置 KICS for Networks 集成后，会自动创建获取有关 KICS for Networks 资产数据的任务。发生的情况包括：

- 创建新集成后立即执行。
- 更改现有集成的设置后立即执行。
- 每隔几个小时按照定期计划执行。默认每 12 小时执行一次。可以更改计划。

可以手动创建账户数据更新任务。

若要启动更新租户的KICS for Networks资产数据的任务：

1. 在应用程序主窗口中，转到**设置→租户**部分。
2. 选择要导入KICS/KATA资产的租户。
   该租户的属性窗口将打开。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产设置**。
4. 在**KICS/KATA导入**选项卡上，确保**状态**切换开关已打开。
5. 配置资产数据导入：
   - 要安排定期导入，请在**导入间隔（小时）**字段中指定OSMP更新KICS/KATA资产数据的时间间隔。
   - 若要手动运行导入，请点击**导入**按钮。

OSMP 控制台的"任务管理器"部分添加了一个从所选租户接收账户数据的**任务**。

导入过程中的资产字段比对示例

每个导入的资产都会与匹配的 OSMP 资产进行比较。

检查 IP、MAC 和 FQDN 字段中的双字段值匹配情况

比较的资产	比较的字段		
	FQDN	IP	MAC
KUMA 资产	是	是	空
导入的资产 1	是，匹配	是，匹配	是
导入的资产 2	是，匹配	是，匹配	空
导入的资产 3	是，匹配	空	是
导入的资产 4	空	是，匹配	是
导入的资产 5	是，匹配	空	空
导入的资产 6	空	空	是

比对结果：

- 导入的资产 1 与 OSMP 资产：FQDN 和 IP 字段已填写且匹配，两个资产的 MAC 字段没有冲突。资产将合并。
- 导入的资产 2 与 OSMP 资产：FQDN 和 IP 字段已填写且匹配。资产将合并。
- 导入的资产 3 与 OSMP 资产：FQDN 和 MAC 字段已填写且匹配，两个资产的 IP 字段不冲突。资产将合并。
- 导入的资产 4 与 OSMP 资产：IP 字段已填写且匹配，两个资产的 FQDN 和 MAC 字段不冲突。资产将合并。
- 导入的资产 5 与 OSMP 资产：FQDN 字段已填写且匹配，两个资产的 IP 和 MAC 字段不冲突。资产将合并。
- 导入的资产 6 和 OSMP 资产：无匹配字段。资产不会合并。

检查 IP、MAC 和 FQDN 字段中的单字段值是否匹配

比较的资产	比较的字段		
	FQDN	IP	MAC
OSMP资产	空	是	空
导入的资产 1	是	是，匹配	是
导入的资产 2	是	是，匹配	空
导入的资产 3	是	空	是
导入的资产 4	空	空	是

比对结果：

- 导入的资产 1 与 OSMP 资产：IP 字段已填写且匹配，两个资产的 FQDN 和 MAC 字段不冲突。资产将合并。
- 导入的资产 2 与 OSMP 资产：IP 字段已填写且匹配，两个资产的 FQDN 和 MAC 字段不冲突。资产将合并。
- 导入的资产 3 和 OSMP 资产：无匹配字段。资产不会合并。
- 导入的资产 4 和 OSMP 资产：无匹配字段。资产不会合并。

kuma-ptvm-config.yaml 配置文件的设置

下表列出了您可以在 kuma-ptvm-config.yaml 文件中指定的设置。

设置	描述	值
`General settings` 组		
`log_level`	可选设置。 日志记录级别。	可用值： • `trace` • `info` • `warning` • `error` 默认设置：`info`。
`period`	可选设置。 从 MaxPatrol 导出在指定时间段内发生变化的资产数据。	无限制。 默认设置：30d。
`strict_import`	可选设置。 从 MaxPatrol 导出资产时，请检查是否填写了 KUMA 的必填字段。请勿从 MaxPatrol 导出未经验证的资产。	可用值： • `true` 用于检查是否存在 KUMA 所需字段。 • `false` 用于跳过对是否存在 KUMA 所需字段的检查。 默认设置：`false`。 我们建议在从 MaxPatrol 导出资产时将其设置为 true。这样可以在将资产导入 XDR 之前检测并修复 JSON 文件中可能存在的错误。
`KUMA settings` 组		
`endpoint`	必需设置。 XDR API 服务器的 URL。例如，`api.<XDR FQDN>/xdr/`	-
`token`	必需设置。 XDR API 令牌。	-
`ignore_server_cert`	可选设置。 XDR 证书的验证。	可用值： `true` 用于禁用证书验证。 `false` 用于启用证书验证。 此设置未包含在配置文件模板中。您可以手动添加此设置，并将其值设置为 true。kuma-ptvm 实用程序在启动时不会验证证书。
`MaxPatrol settings` 组		
`endpoint`	必需设置。 MaxPatrol API 服务器的 URL。	-
`user`	可选设置。 MaxPatrol API 用户名。	-
`password`	可选设置。 MaxPatrol API 用户密码。	-
`secret`	可选设置。 MaxPatrol API 密钥。	-

`token`	可选设置。 MaxPatrol API 令牌。	要通过 API 访问 MaxPatrol 服务器，请指定 `user`、`password` 和 `secret` 设置的值，或指定 `token` 设置的值。
`ignore_server_cert`	可选设置。 MaxPatrol 证书的验证。	可用值： • `true` 用于禁用 MaxPatrol 证书验证。 • `false` 用于启用 MaxPatrol 证书验证。 此设置未包含在配置文件模板中。如果出现 `tls: failed to verify certificate: x509: certificate is valid for localhost` 错误，您可以手动添加此设置并将其值设为 `true`。在这种情况下，kuma-ptvm 实用程序在启动时不会验证证书。 建议优先按照 MaxPatrol 文档中的说明颁发证书，以此解决该错误。
`Vulnerability filter` 组		
`only_exploitable`	可选设置。 仅从 MaxPatrol 中导出存在漏洞且已知漏洞利用手段的资产。	可用值： `true` 用于仅导出存在已知漏洞利用方式的漏洞的资产。 `false` 用于导出所有资产。 默认设置：`false`。
`min_severity`	可选设置。 仅导入指定级别或更高级别的漏洞。	可用值： • `low` • `medium` • `high` • `critical` 默认值：`low`。
`Tenant map` 组		
`id`	必需设置。 XDR 中的租户 ID。 资产按照配置文件中指定租户的顺序分配给租户：租户在列表中的位置越高，其优先级越高。这意味着您可以指定重叠的子网。	-
`fqdn`	可选设置。 用于搜索资产 FQDN 的正则表达式。	-
`networks`	可选设置。 一个或多个子网。	-
`default_tenant`	可选设置。 默认 XDR 租户，用于接收无法分配给“租户”设置组中指定租户的资产数据。	-

将类别分配给资产

在资产属性中为单个资产分配类别

此方法不适用于为KSC或KICS资产分配类别。按照说明为一个或多个资产分配类别。

要为一个资产分配类别：

1. 在主菜单中，转到**资产管理 → 资产(设备) → 检测和响应**。
2. 点击**显示导航**按钮，然后选择租户以及包含所需资产的类别。
   将显示资产表。
3. 选择一个资产，然后在菜单中选择**显示更多**。

4. 在打开的窗口中，单击“**编辑**”按钮。
5. 在**附加**选项卡的**类别**字段中，选择一个类别。

> 如果要将资产移动到“**未分类资产**”部分，则必须通过单击 × 按钮来删除该资产的现有类别。

6. 单击“**保存**”按钮。

类别将被分配。

为一个或多个资产分配类别

要为一个或多个资产分配类别：

1. 在主菜单中，转到**资产管理 → 资产(设备) → 检测和响应**。
2. 点击**显示导航**按钮，然后选择租户以及包含所需资产的类别。
   将显示资产表。
3. 选中要更改类别的资产旁边的复选框。
4. 单击“**关联到类别**”按钮。
5. 在打开的窗口中，选择一个类别。
6. 单击“**绑定**”按钮。

类别将被分配。

请勿将 `Categorized assets` 类别分配给资产。

将一组资产关联到一个类别

若要将一组资产关联到一个类别：

1. 在**资产管理**部分，选中资产表标题中的复选框。
2. 选择页面上所有可见的资产，或选择符合选择条件的所有资产。
   关联到类别按钮变为活动，并打开可用的类别。
3. 点击**关联到类别**按钮，然后选择一个或多个要关联到的类别。
4. 单击“**确定**”。
   资产随即关联到选定的类别或文件夹。

将一组资产与某个类别取消关联

若要将一组资产与某个类别取消关联：

1. 在导航面板中选择一个类别（租户）。
   该类别中的资产列表随即显示。
   文件夹属性中已添加**清理类别**按钮。
2. 从任务的上下文菜单中，选择**清理类别**。
   屏幕上会显示一个对话框，其中包含确认提示以及将要取消关联的资产数量。
   此选项允许您取消关联所选类别中的所有资产，而不仅仅是页面上可见的资产。子类别中的资产并不取消关联。
3. 在对话框中，点击**确定**。
   所有选定的资产均已从选定的类别中取消关联。

编辑资产参数

在 OSMP 中，您可以编辑资产参数。手动添加的资产的所有参数均可编辑。对于从 Kaspersky Security Center 导入的资产，您只能更改资产的名称及其类别。

要更改资产的参数：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 选择具有相关资产的类别。
   将显示资产表。
3. 选择一个资产，然后单击“**详情**”。
4. 在打开的窗口中，单击“**编辑**”按钮。
   “**编辑资产**”窗口打开。
5. 在可用字段中进行所需的更改：
   - **资产名称**（必填）如果资产是从 Kaspersky Security Center 或 KICS for Networks 导入的，则只有此字段可编辑。
   - **IP 地址**和/或 **FQDN**（必填）。您可以指定多个 FQDN，并以逗号分隔。
   - **MAC 地址。**
   - **所有者。**
   - **软件信息**：
     - **操作系统名称**
     - **操作系统版本**

- **硬件信息**：
  硬件参数

  您可以将有关资产硬件的信息添加到“**硬件信息**”部分：

  可用于描述资产 CPU 的字段：

  - **CPU 名称**
  - **CPU 频率**
  - **CPU 核心数**

    您可以使用“**添加 CPU**”按钮将 CPU 添加到资产。

  可用于描述资产磁盘的字段：

  - **磁盘可用空间（字节数）**
  - **磁盘空间**

    您可以使用“**添加磁盘**”按钮将磁盘添加到资产。

  可用于描述资产 RAM 的字段：

  - **RAM 频率**
  - **RAM 总字节数**

  可用于描述资产网卡的字段：

  - **网卡名称**
  - **网卡制造商**
  - **网卡驱动程序版本**

    您可以使用“**添加网卡**”按钮将网卡添加到资产。

- **自定义字段**。
- **CII 类别**。

6. 在**附加**选项卡的**类别**字段中，选择一个类别。

> 您也可以选择资产，然后将其拖放到相关类别中。此类别将添加到资产类别列表中。

> 请勿将 `Categorized assets` 类别分配给资产。

7. 单击“**保存**”按钮。

资产参数已更改。

归档资产

在 OSMP 中，存档功能适用于以下类型的资产：

- 从 Kaspersky Security Center 和 KICS 导入的资产。

  如果 OSMP 尝试导入十次后仍无法获取有关资产的信息，该资产将自动归档，并在数据库中保存。您可以通过 **已存档资产的 TTL（天）** 设置指定保存时长。默认设置是 0 天。这意味着已存档资产将无限期保留。如果 OSMP 在存档资产的保留期到期之前从源收到有关资产的信息，则存档资产将变为活动状态。

- 合并后的资产

  导入时，OSMP 会检查从 Kaspersky Security Center 和 KICS 导入的资产以及手动添加的资产的唯一性。如果导入的资产和手动添加的资产的字段匹配，则这些资产将合并为一个资产，该资产被视为已导入并可存档。

- 在控制台中手动添加或使用API添加的资产将被归档并存储在数据库中，存储时间由**已归档资产的TTL（天数）**设置指定。默认设置是 0 天。这意味着已存档资产将无限期保留。如果您希望在已归档资产的保留期限到期前活动该资产，可以使用**取消归档资产**选项。

在以下情况下，资产将被存档：

- 对于在控制台中手动创建或使用API创建的资产，请使用**归档资产**选项。
- OSMP 尝试导入十次后，仍无法从 Kaspersky Security Center 或 KICS for Networks 获取有关资产的信息。
- 已禁用与 Kaspersky Security Center 的集成。

  如果您禁用与 Kaspersky Security Center 的集成，则资产将被视为在 30 天内保持活动状态。30天后，资产将自动存档，并存储在数据库中，存储期限为**已存档资产的TTL（以天为单位）**中指定的时间。

以下情况下不会更新资产：

- Kaspersky Security Center 资产相关信息未更新的时长已超过存档资产的保留期。
- 有关该资产的信息在 Kaspersky Security Center 或 KICS for Networks 中不存在。
- 与 Kaspersky Security Center 服务器的连接已超过 30 天未建立。

要更改手动创建的资产或资产组的归档状态：

1. 在主菜单中，前往**资产管理→资产（设备）→分析和响应**。

   这将打开资产表。

2. 在资产表中，选中手动创建的资产旁边的复选框，即可更改其归档状态。
3. 在资产表上方的工具栏中，单击以下按钮之一：

   - 归档**资产**将选定的资产归档。
   - **取消归档资产**以恢复选定的已归档资产。

   资产的归档状态已更改。您可以在资产表中**已存档**列的下拉列表中按归档状态筛选资产，方法是选择**是**以仅显示已归档资产，或选择**否**以仅显示活动资产。

要配置已存档资产的保留期：

1. 在应用程序主窗口中，转到**设置→租户**部分。
2. 选择您要更改存档资产保留期的租户。
   这将打开“租户属性”窗口。
3. 在“**设置**”选项卡上，点击“**资产设置**”。
4. 在**常规**选项卡上，在**已存档资产的TTL（以天为单位）**字段中输入新值。
   默认设置是 30 天。输入 0 可无限期保留已存档资产。
5. 单击“**保存**”按钮。

已存档资产的保留期配置完成。

有关已存档资产的信息仍然可在警报和事故卡中查看。

要查看已存档资产卡：

1. 在主菜单的“**监控**”下，选择“**警报**”或“**事故**”部分。
   将显示警报或事故列表。
2. 打开关联到已存档资产的警报或事故卡。
   您可以在已存档资产卡中查看信息。

删除资产

您可以在**管理和保护**选项卡中删除资产。在**检测和响应**选项卡上，OSMP 仅自动删除已存档资产。您无法手动删除资产。如果资产信息的未更新时间超过已存档资产的保留期，OSMP会删除该资产。

删除资产类别

类别删除分两个阶段进行：归档文件和永久删除。归档允许您在从系统中永久删除之前验证该类别是否仍然被任何资源引用。

当OSMP父实例上的某个类别被归档时，所有OSMP子实例上的对应类别也会被归档。系统随后会检查是否还有资源引用已归档的类别。如果没有引用，则该类别将被永久删除。

要删除资产类别：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 在类别树状图中，点击要删除的类别旁边的（⋮）图标。
3. 在上下文菜单中，选择**归档**。
4. 在**删除类别？**对话框中，单击**确定**进行确认。

如果资源仍然关联到该类别，则该类别将保持归档状态，直到所有链接都被删除。

已归档的类别不会出现在类别列表中，但可能仍然会在引用该类别的筛选器中可用。类别属性仍然可供查看，资源关联可以被移除。除类别名称外，禁止修改类别属性。

包含子类别的类别还需遵守其他限制：

- 如果一个父类别至少包含一个未归档的子类别，则该父类别不能被归档或删除。
- 在删除父类别之前，必须先将所有子类别存档或永久删除。
- 所有子类别都归档后，父类别将按照标准的归档和删除流程进行处理。

只有当所有对某个类别的引用都被删除，并且所有层次结构约束都得到满足时，该类别才会被永久删除。

批量删除资产

在KUMA网页界面中，您可以使用筛选器选择多个资产，然后删除所有选定的资产。

若要删除资产，您必须拥有删除资产的权限。

批量删除资产

若删除所有选定资产：

1. 在应用程序的主窗口中，转到**资产管理**部分，然后选择一个资产类别。
   资产表随即显示。
2. 选中资产表标题中的复选框。
   您可以删除所有资产，或删除页面上当前显示的所有资产。
3. 点击**页面中全选**或**全选**。
   删除按钮随即变为活动。
4. 单击“**删除**”按钮。
   这将打开一个窗口，提示您确认删除，并告知您已删除的资产将不会在警报、事件和小部件中可用。
   页面下方会显示已选择删除的资产数量。
5. 单击“**确定**”。
   如果您点击了**全选**，则必须将显示的生成字符串输入到窗口中的文本框中以确认删除。

所有选定的资产随即被删除。

删除资产文件夹

若要删除文件夹，您可以先取消所有资源与该文件夹的关联（这会取消资源的关联，但不会删除它们），然后再删除该文件夹本身；或者，您可以先删除所有资源，然后再删除该文件夹。

更新 Kaspersky Security Center 资产中的第三方应用程序并修复漏洞

您可以更新安装在 Kaspersky Security Center 资产上的第三方应用程序（包括 Microsoft 应用程序）并修复这些应用程序的漏洞。

首先，您需要在所选的 Kaspersky Security Center 管理服务器上创建“*安装所需更新并修复漏洞*”任务，设置如下：

- 应用程序 — Kaspersky Security Center。
- 任务类型 — *安装所需更新并修复漏洞*。
- 将任务分配给的设备 — 您需要将任务分配给根管理组。
- 安装更新的规则：
  - 仅安装已批准的更新。
  - 修复严重级别等于或高于（可选设置）的漏洞。

    如果已启用该设置，更新仅修复卡巴斯基设置的严重级别等于或高于在列表中所选的值（*中*、*高*或*严重*）的漏洞。严重级别低于选定值的漏洞不被修复。
- 计划启动 — 任务运行计划。

有关如何创建任务的详细信息，请参阅 *Kaspersky Security Center 帮助指南*。

“*安装所需更新并修复漏洞*”任务在“漏洞和补丁管理”授权许可下可用。

接下来，您需要安装第三方应用程序的更新并修复 OSMP 中资产的漏洞。

要在 OSMP 中为资产安装第三方应用程序更新并修复其漏洞：

1. 按下列方式之一打开资产详情窗口：
   - 在主菜单中，转到“**资产管理**” → “**资产(设备)**” → “**检测和响应**”，选择相关资产的类别，然后选择一个资产，并单击“**详情**”。
   - 在主菜单中，转到**“监控”→“威胁搜索”**。搜索并筛选事件。然后选择所需的事件，并单击以下字段之一中的链接：SourceAssetID、DestinationAssetID 或 DeviceAssetID。
2. 在资产详情窗口中，展开**“Kaspersky Security Center 漏洞”**列表。
3. 选中要更新的应用程序旁边的复选框。
4. 单击“**上传更新**”链接。
5. 在打开的窗口中，选中要修复的漏洞 ID 旁边的复选框。
6. 如果所选 ID 的“**已接受 EULA**”列中显示“**否**”，请单击“**批准更新**”按钮。

7. 单击“**EULA URL**”列中的链接，仔细阅读最终用户授权许可协议的文本。

8. 如果您接受，请点击**“接受所选的EULA”**。
   已接受 EULA 的漏洞 ID 会在“**已成功接受 EULA**”列中显示“**是**”。

9. 对每个所需的漏洞 ID 重复步骤 7-10。

10. 单击“**确定**”。

更新将上传并安装到启动任务的管理服务器所管理的资产上以及所有从属管理服务器的资产上。

> 每台从属管理服务器必须分别接受最终用户授权许可协议中关于更新和漏洞补丁的条款。

更新将安装在检测到漏洞的资产上。

您可以在资产详情窗口中单击“**更新**”链接来更新资产的漏洞列表。

将资产移动到所选管理组

您可以将资产移动到 Kaspersky Security Center 的所选管理组。在这种情况下，组策略和任务将应用于资产。有关 Kaspersky Security Center 任务和策略的更多详细信息，请参阅 *Kaspersky Security Center 帮助指南*。

在**从 Kaspersky Security Center 导入资产**期间加载层次结构时，管理组将添加到 OSMP。首先，您需要配置 OSMP 与 Kaspersky Security Center 的集成。

受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

- 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
- 资产属性信息：漏洞；软件，包括操作系统；资产所有者

若要导入卡巴斯基安全管理中心资产信息：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。

2. 点击**导入**，然后选择以下操作之一：

   - 如要导入资产基本属性信息，请点击**导入KSC资产**。
     这将打开**导入KSC资产**窗口。
   - 若要导入资产其他属性信息，请点击**导入KSC资产属性**。
     这将打开**导入KSC资产属性**窗口。

3. 在下拉列表中，选择要为其执行导入操作的租户。
   在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。

如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。

4. 单击“**导入**”按钮。

将导入资产信息。

此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

要将资产移动到所选的管理组：

1. 按下列方式之一打开资产详情窗口：

   - 在主菜单中，转到“**资产管理**” → “**资产(设备)**” → “**检测和响应**”，选择相关资产的类别，然后选择一个资产，并单击“**详情**”。
   - 在主菜单中，转到“**监控**” → “**警报**”，单击相关警报的链接，然后在“**资产**”部分选择该资产，并单击“**查看属性**”。

2. 在资产详情窗口中，单击**响应→ 移至群组**。
3. 在打开的窗口中选择该组。

   所选的组必须与资产属于同一租户。

4. 单击“**保存**”按钮。

所选资产将被移动。

要将多个资产移动到所选的管理组：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 选择具有相关资产的类别。
3. 选中要移动到该组的资产旁边的复选框。
4. 单击**响应→移至群组**。

   如果所有选定资产都属于同一管理服务器，则该按钮处于活动状态。

5. 在打开的窗口中选择该组。
6. 单击“**保存**”按钮。

所选资产将被移动。

资产的具体组显示在资产详细信息中。

从 Kaspersky Security Center 导入资产信息时，Kaspersky Security Center 资产信息会在 OSMP 中更新。这意味着可能会出现资产在 Kaspersky Security Center 中的管理组之间移动，但该信息尚未在 OSMP 中显示。若尝试将此类资产移至其已所属的管理组，OSMP会返回**将资产移至另一个 KSC 群组失败**这一错误消息。

资产审计

OSMP 可配置为在以下条件下生成资产审计事件：

- 资产已添加到 OSMP。该应用程序监控手动创建资产，以及通过 REST API 导入期间和从 **Kaspersky Security Center** 或 KICS for Networks 导入期间的创建情况。

  受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

  KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

  - 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
  - 资产属性信息：漏洞；软件，包括操作系统；资产所有者

  若要导入卡巴斯基安全管理中心资产信息：

  1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
  2. 点击**导入**，然后选择以下操作之一：
     - 如要导入资产基本属性信息，请点击**导入KSC资产**。
       这将打开**导入KSC资产**窗口。
     - 若要导入资产其他属性信息，请点击**导入KSC资产属性**。
       这将打开**导入KSC资产属性**窗口。
  3. 在下拉列表中，选择要为其执行导入操作的租户。
     在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。
     如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。
  4. 单击“**导入**”按钮。

     将导入资产信息。

  此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

- 资产参数已更改。监控以下资产字段值的变化：
  - 名称
  - IP 地址

- MAC 地址。
- FQDN
- 系统

在导入期间更新资产时，字段可能会更改。

- 资产已从 OSMP 中删除。该程序监控手动删除资产，以及自动删除从 Kaspersky Security Center 和 KICS for Networks 导入的、不再接收其数据的资产的情况。
- 漏洞信息已添加到资产中。该程序监控资产新漏洞数据的出现情况。例如，从 Kaspersky Security Center 或 KICS for Networks 导入资产时，可以将漏洞信息添加到资产中。
- 资产漏洞已解决。该应用程序监控从资产中删除漏洞信息的情况。如果不再从此前获取该漏洞发生信息的任何源接收该漏洞相关数据，则判定该漏洞已修复。
- 资产已添加到类别。该应用程序监控为资产分配资产类别的情况。
- 资产已从类别中删除。该应用程序监控从资产类别中删除资产的情况。

默认情况下，如果启用了资产审计，在上述条件下，OSMP 不仅会创建审计事件（`Type = 4`），还会创建基础事件（`Type = 1`）。

例如，资产审计事件可以发送到存储或关联器。

配置资产审计

要配置资产审计：

1. 在应用程序主窗口中，转到**设置→租户**部分。
2. 选择您要配置资产审计的租户。

   这将打开“租户属性”窗口。

   如果要为新租户配置资产审核，请先创建租户。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产审计**。
4. 对于生成资产审计事件的每个条件，选择要将已创建的事件发送到哪个目标位置：

   a. 在相关类型的资产审计事件的设置区块中，使用“**添加目标位置**”下拉列表，选择要将已创建的事件发送到的目标位置类型：

   - 如果要将事件发送到存储，请选择“**存储**”。
   - 如果要将事件发送到关联器，请选择“**关联器**”。
   - 如果要选择不同的目标位置，请选择“**其他**”。

     此类资源包括在程序早期版本中创建的关联器和存储服务。

   在打开的“**添加目标位置**”窗口中，您必须定义事件转发的设置。

b. 使用**目标位置**下拉列表，选择现有目标位置，或者如果要创建新目标位置，请选择**创建**。
如果要创建新目标位置，请按照目标位置描述中所示的设置进行填写。

c. 单击“**保存**”按钮。

已将目标位置添加到生成资产审计事件的条件中。每个条件可以添加多个目标位置。

5. 单击“**保存**”按钮。

资产审计已配置完成。将为已添加目标位置的条件生成资产审计事件。单击“**保存**”按钮。

存储和搜索资产审计事件

资产审计事件被视为基本事件，不会取代审计事件（审计事件、审计事件）。可以根据以下参数搜索资产审计事件：

事件字段	值
DeviceVendor	`"Kaspersky"`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

启用和禁用资产审计

您可以为租户启用或禁用资产审计。

要为租户启用或禁用资产审计：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要启用或禁用资产审计的租户。
这将打开“租户属性”窗口。
3. 在**设置**选项卡上的**检测和响应**下，点击**资产审计**。
4. 启用或禁用**审计事件集合**切换开关。
5. 单击“**保存**”按钮。

默认情况下，当启用资产审计时，如果出现审计条件，会同时创建两种类型的事件：基础事件和审计事件。

您可以禁用与审计事件相关的基础事件的生成。

要启用或禁用单个条件的基本事件创建：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。
2. 选择要启用或禁用生成资产审计事件条件的租户。
这将打开“租户属性”窗口。

3. 在**设置**选项卡上的**检测和响应**下，点击**资产审计**。

4. 点击条件操作名称以启用或禁用相应基本事件的创建。

5. 单击“**保存**”按钮。

对于已禁用的条件，仅创建审计事件，不创建基本事件。

自定义资产字段

除了资产数据模型的现有字段外，您还可以创建自定义资产字段。查看有关资产的信息时，会显示自定义资产字段的数据。您可以手动或使用 API 在自定义字段中输入数据。

您可以在OSMP的**“资产”**部分的**“自定义字段”**表中创建或编辑自定义字段。该表包含以下列：

- **名称** – 查看有关资产的信息时显示的自定义字段的名称。
- **默认值** – 将资产添加到KUMA时写入自定义字段的值。
- **掩码** – 自定义字段中的值必须匹配的正则表达式。

要创建自定义资产字段：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。

2. 选择您要更改存档资产保留期的租户。
   这将打开“租户属性”窗口。

3. 在“**设置**”选项卡上，点击“**资产设置**”。

4. 在**常规**选项卡的**自定义字段**字段下，点击**添加**按钮。
   系统会在**自定义字段**表中添加一个空行。您可以一次性添加多个包含自定义字段设置的行。

5. 使用自定义字段的设置填写以下列：

   - **名称**（必填） – 1 到 128 个 Unicode 编码字符。
   - **默认值** – 1到1,024个Unicode字符。
   - **掩码** – 1 到 1,024 个 Unicode 字符。

6. 单击“**保存**”按钮。

自定义字段已添加到资产数据模型。

要删除或编辑自定义资产字段：

1. 在应用程序主窗口中，转到**设置**→**租户**部分。

2. 选择您要更改存档资产保留期的租户。
   这将打开“租户属性”窗口。

3. 在“**设置**”选项卡上，点击“**资产设置**”。

4. 在**常规**选项卡上，对**自定义字段**表进行必要的更改：

   - 若要删除自定义字段，请选中所需字段旁边的复选框，然后点击**删除**按钮。删除字段也会一并删除所有资产写入该字段的数据。
   - 您可以更改字段设置的值。更改默认值不会影响之前写入资产字段的数据。
   - 若要更改字段的显示顺序，请使用**上移**和**下移**按钮。

5. 单击“**保存**”按钮。

更改已完成。

关键信息基础设施资产

在 OSMP 中，您可以标记与俄罗斯联邦关键信息基础设施 (CII) 相关的资产。这允许您限制 OSMP 用户处理与 CII 对象相关资产关联的警报和事故的能力。

如果 OSMP 中 GosSOPKA 模块的授权许可处于活动状态，则可以将 CII 类别分配给资产。

主管理员和在其配置文件中选中“**访问 CII 设施**”复选框的用户可以将 CII 类别分配给资产。如果不满足上述任何条件，则对用户适用以下限制：

- **CII 类别**的设置组不会显示在“**资产详情**”和“**编辑资产**”窗口中。您无法查看或更改资产的 CII 类别。
- 无法查看与 CII 类别的资产关联的警报和事故。您无法对此类警报和事故执行任何操作；它们不会显示在警报和事故表中。
- 警报和事故表中不显示“**CII**”列。
- 无法使用 REST API 搜索或关闭警报。

CII 类别的资产会显示在“**资产详情**”窗口的“**CII 类别**”设置组中。

要更改资产的 CII 类别：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 选择具有相关资产的类别。

   将显示资产表。
3. 选择一个资产，然后单击“**详情**” 。

   “**资产详情**”窗口打开。
4. 单击“**编辑**”按钮并在下拉列表中选择一个可用值：

   - **信息资源不是 CII 对象** – 默认值，表示资产没有 CII 类别。在配置文件中未选中“**访问 CII 设施**”复选框的用户仍可操作此类资产及与这些资产相关的警报和事故。
   - **无重要性类别的 CII 对象**。

- **重要性类别为第三级的 CII 对象**。
- **重要性类别为第二级的 CII 对象**。
- **重要性类别为第一级的 CII 对象**。

5. 单击“**保存**”按钮。

部署 Kaspersky 应用程序

本部分介绍通过 OSMP 控制台在组织中的客户端设备上部署卡巴斯基应用程序。

方案：Kaspersky 应用程序部署

此方案说明如何通过 OSMP 控制台部署卡巴斯基应用程序。您可以使用保护部署向导，也可以手动完成所有必要步骤。

阶段

卡巴斯基应用程序部署分阶段进行：

1. **下载并创建安装包**

   手动下载安装包。

   如果您无法通过 Kaspersky Next XDR Expert 在某些设备（例如远程员工的设备）上安装卡巴斯基应用程序，则可以为应用程序创建独立安装包。如果您使用独立软件包安装卡巴斯基应用程序，则不必创建和运行远程安装任务，也不必为 Kaspersky Endpoint Security for Windows 创建和配置任务。

   或者，您可以从卡巴斯基网站下载网络代理和安全应用程序的分发包。如果由于某种原因无法远程安装应用程序，您可以使用下载的分发包在本地安装应用程序。

2. **创建、配置和运行远程安装任务**

   此步骤是保护部署向导的一部分。如果您选择不运行保护部署向导，您必须手动创建该任务并手动配置它。

   您也可以为不同管理组或不同设备分类手动创建几个远程安装任务。您可以在这些任务中部署应用程序的不同版本。

   确保您网络中的所有设备均已被发现；然后运行远程安装任务。

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

3. **创建和配置任务**

   必须配置 Kaspersky Endpoint Security 的“*更新*”任务。

   手动创建此任务并手动配置。请确保任务计划符合您的要求。（默认情况下，任务的计划开始被设置为**手动**，但您可能希望选择其他选项。）

4. **创建策略**

   手动创建 Kaspersky Endpoint Security 策略。您可以使用默认策略设置。您还可以随时根据需要修改策略的默认设置。

5. **验证结果**

   确保部署成功完成：您的每个应用程序都拥有策略和任务，这些应用程序被安装到受管理设备。

结果

完成方案可以导致如下：

- 所选应用程序的所有所需策略和任务被创建。
- 任务计划根据您的需要被配置。
- 所选应用程序被部署，或者计划在所选客户端设备上部署。

保护部署向导

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

保护部署向导执行以下操作：

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

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

步骤 1：开始保护部署向导

您可以随时手动启动保护部署向导。

要手动启动保护部署向导，

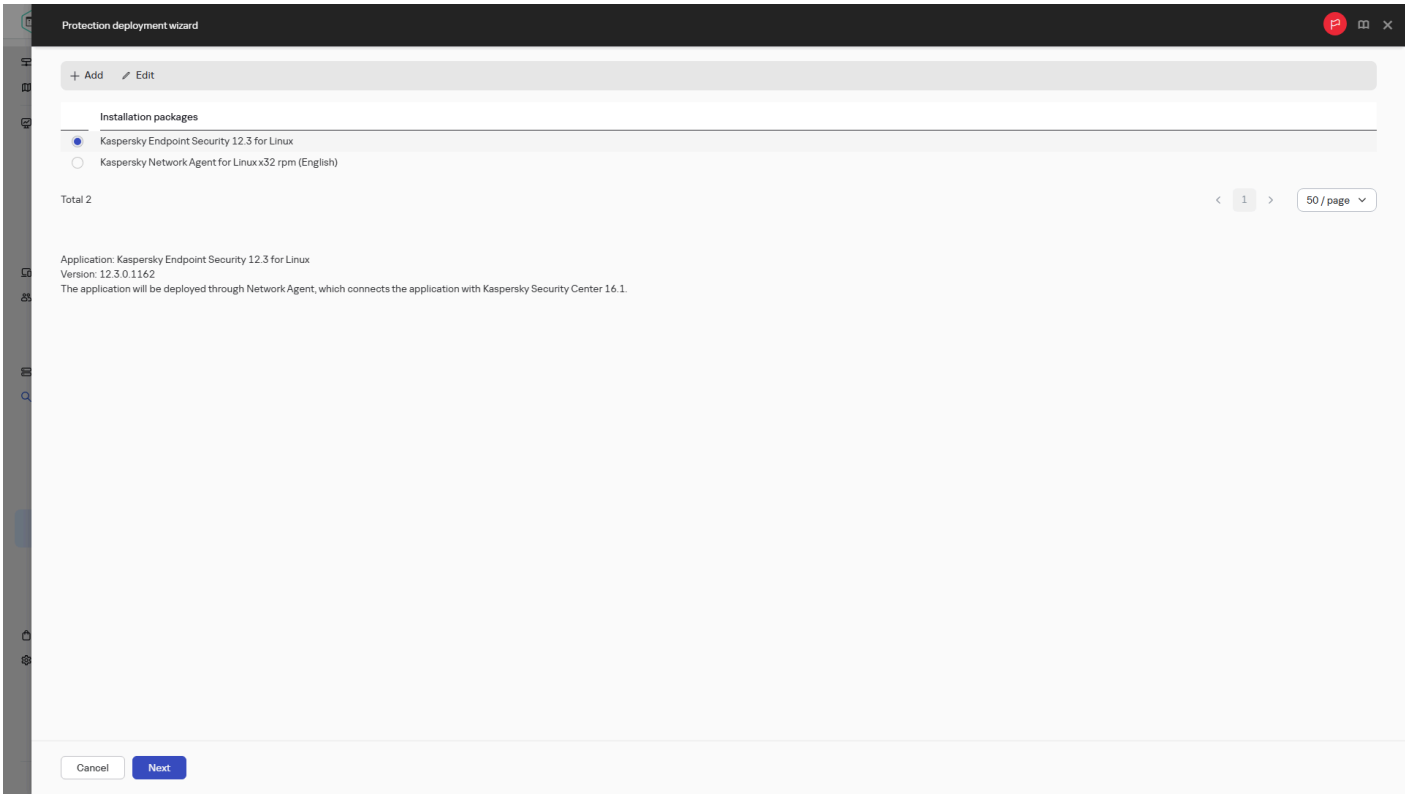
在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**保护部署向导**”。

保护部署向导启动。使用“**下一步**”按钮继续向导操作。

步骤 2：选择安装包

选择您要安装的应用程序安装包。

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



选择安装包

步骤 3：选择分发密钥文件或激活码的方法

选择分发密钥文件或激活码的方法：

- **不添加授权许可密钥到安装包**

  密钥被自动分发到所兼容的所有设备：

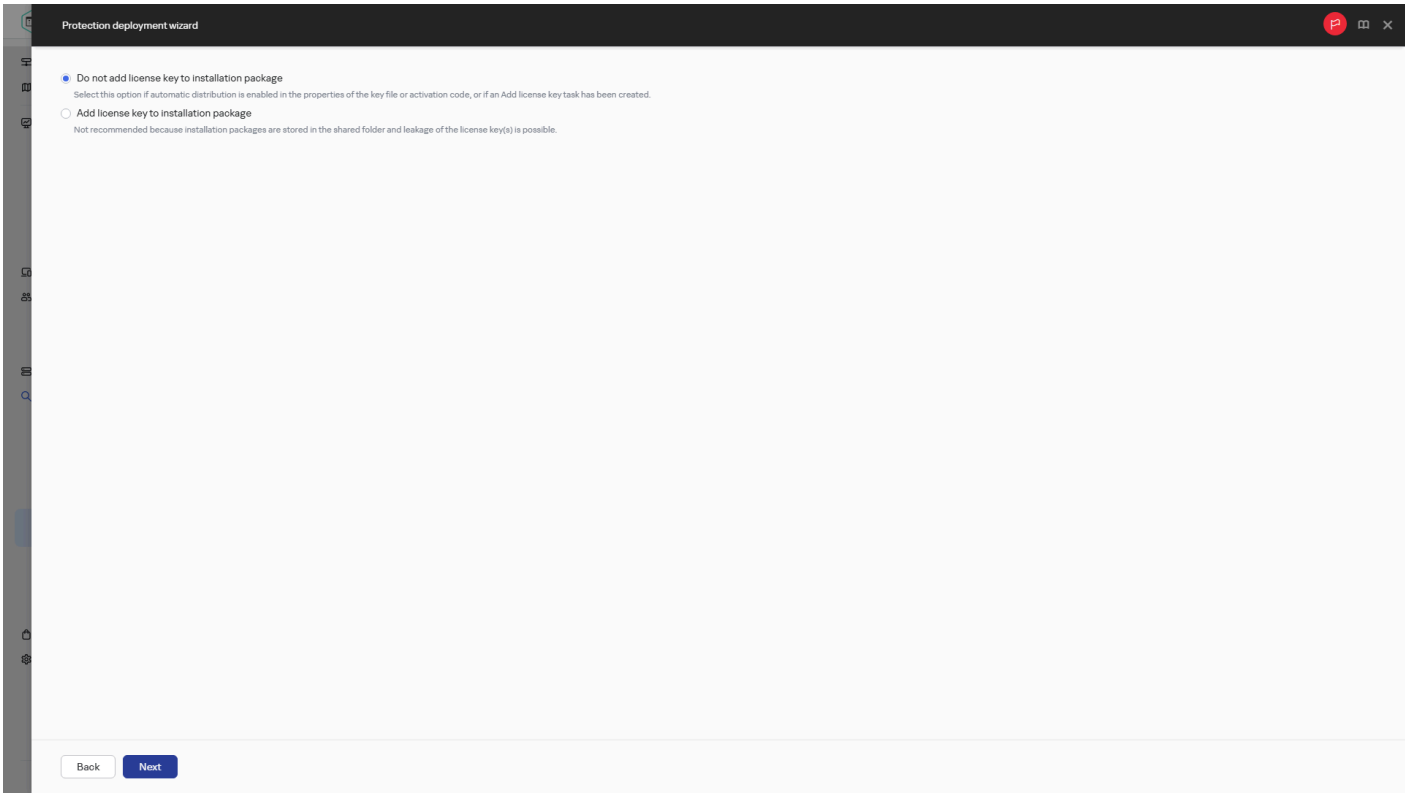
  - 如果自动分发在密钥属性中启用。
  - 如果**添加密钥**任务已创建。

- **添加授权许可密钥到安装包**

  密钥与安装包一起被分发到设备。

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

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

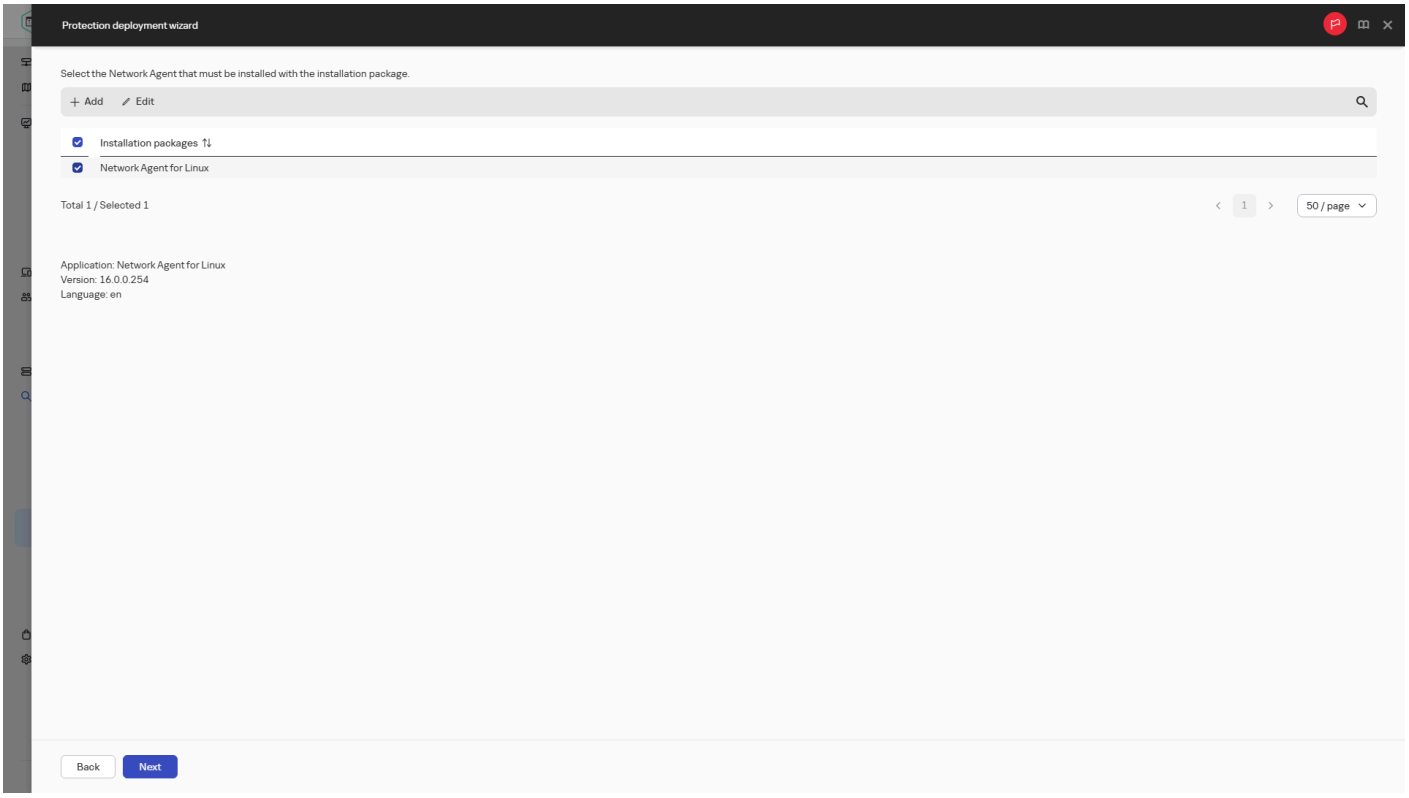


选择分发密钥文件或激活码的方法

步骤 4：选择网络代理版本

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

选择网络代理的最新版本。



选择网络代理版本

步骤 5：选择设备

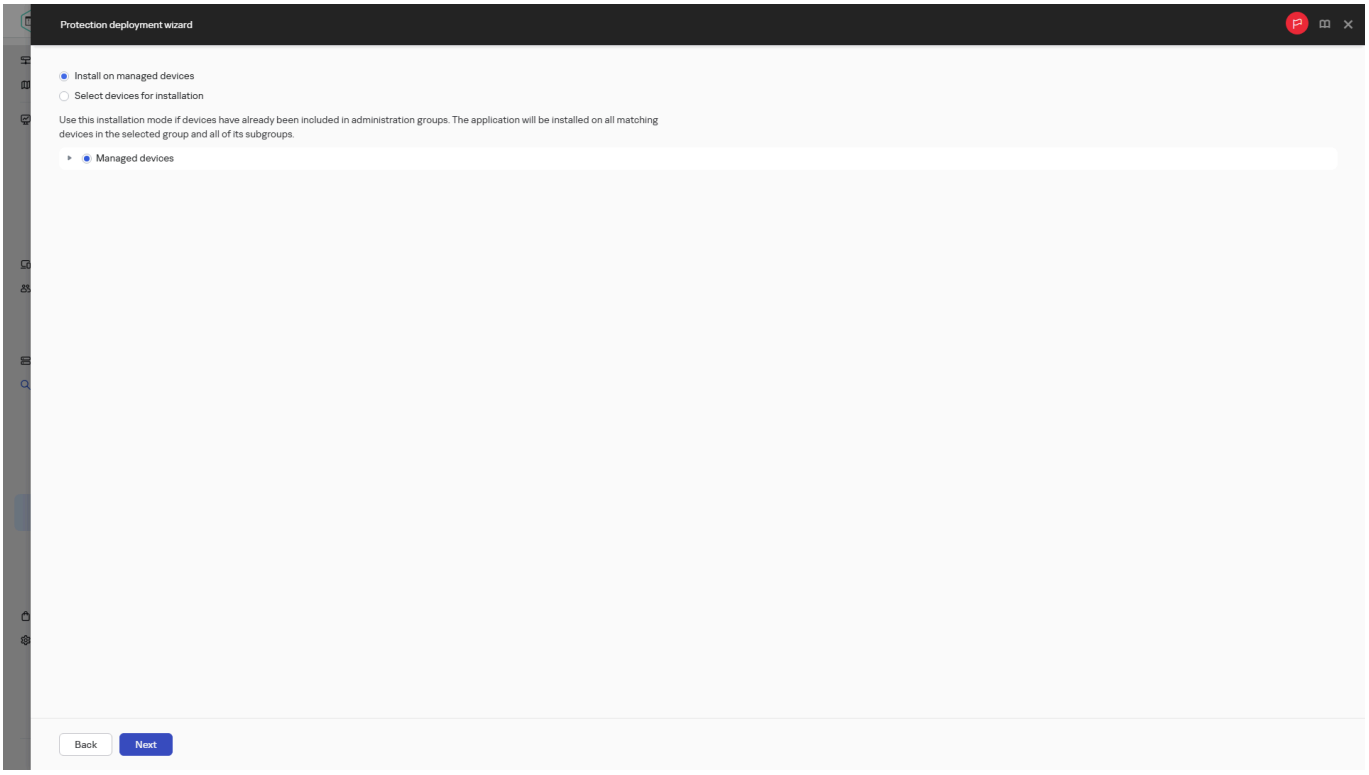
指定要安装应用程序的设备列表：

- **安装到受管理设备**

  如果选择该选项，程序将为该设备组创建远程安装任务。

- **选择设备以安装**

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



指定要在上面安装应用程序的设备列表

步骤 6：指定远程安装任务设置

在“**远程安装任务设置**”页面，指定应用程序远程安装设置。

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

- **使用网络代理**

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

- **通过分发点使用操作系统资源**

  如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。

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

  默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。

  在未安装网络代理的设备上安装 Windows 应用程序（包括 Windows 网络代理）的唯一方法是使用基于 Windows 的分发点。因此，当您安装 Windows 应用程序时：

  - 选择此选项。
  - 确保为目标客户端设备分配了分发点。
  - 确保分发点基于 Windows。

- **通过管理服务器使用操作系统资源**

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

  默认情况下已启用该选项。

定义附加设置：

- **如果已经安装应用程序则不再重新安装**

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

  如果禁用此选项，仍将安装应用程序。

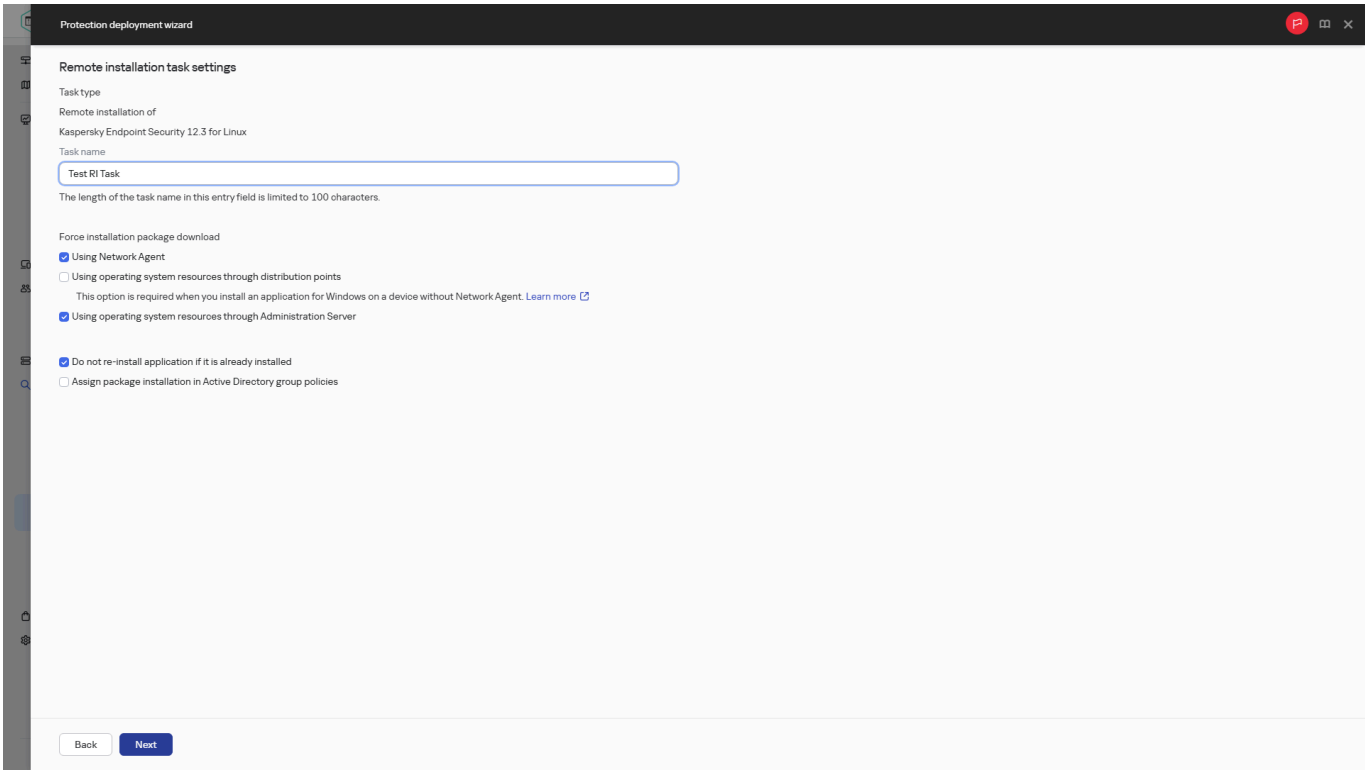
  默认情况下已启用该选项。

- **在 Active Directory 组策略中指定安装包的安装**

  如果启用此选项，安装包将使用 Active Directory 组策略进行安装。

  如果选择网络代理安装包，则该选项可用。

默认情况下已禁用该选项。



指定远程安装任务设置

步骤 7：重启管理

如果安装应用程序时操作系统必须重启，指定要执行的操作：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

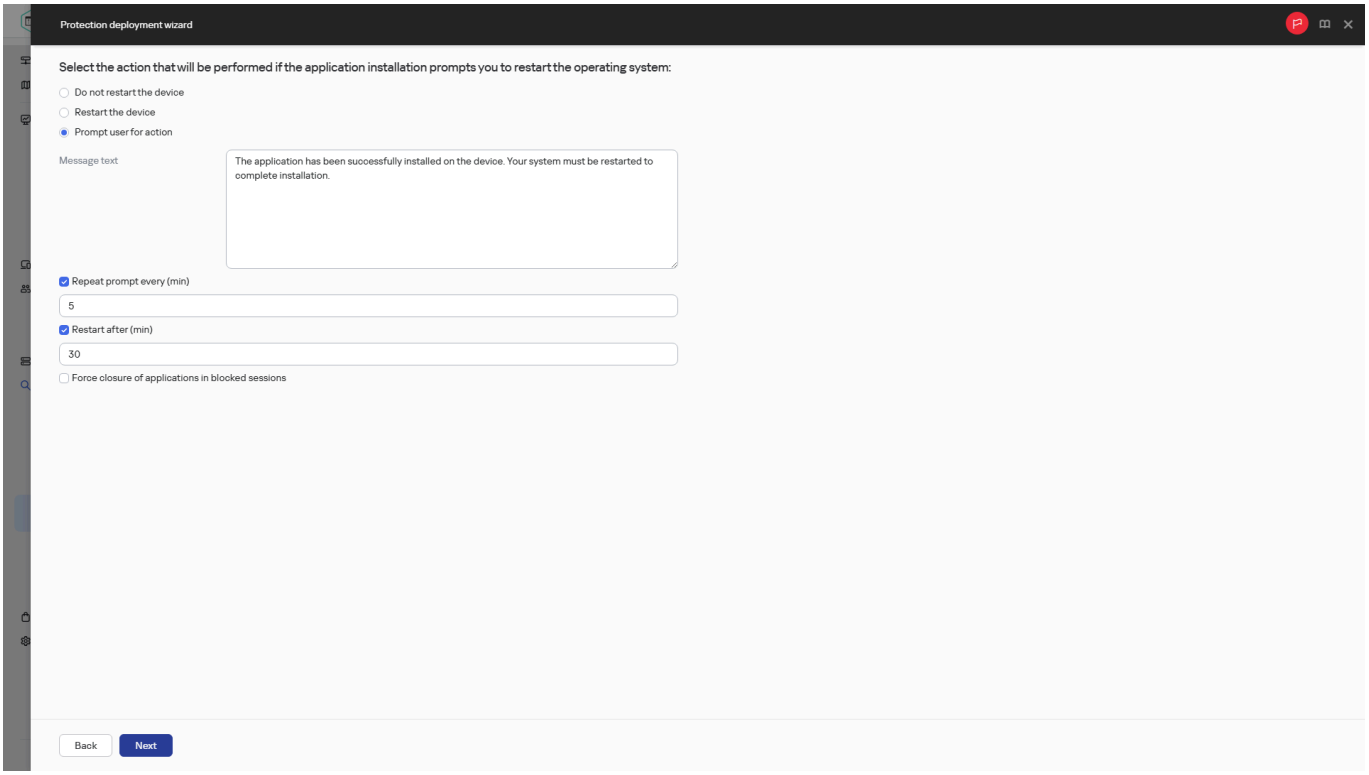
- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。



选择操作系统重启选项

步骤 8：安装前删除不兼容的应用程序

该步骤仅在您部署的应用程序已知与其他应用程序不兼容时才显示。

如果您希望 Kaspersky Next XDR Expert 自动删除与所部署应用程序不兼容的应用程序，请选择此选项。

不兼容应用程序列表也被显示。

如果您不选择该选项，应用程序将仅被安装到没有不兼容应用程序的设备。

步骤 9：移动设备到受管理设备

指定设备是否在安装网络代理后必须被移动到管理组。

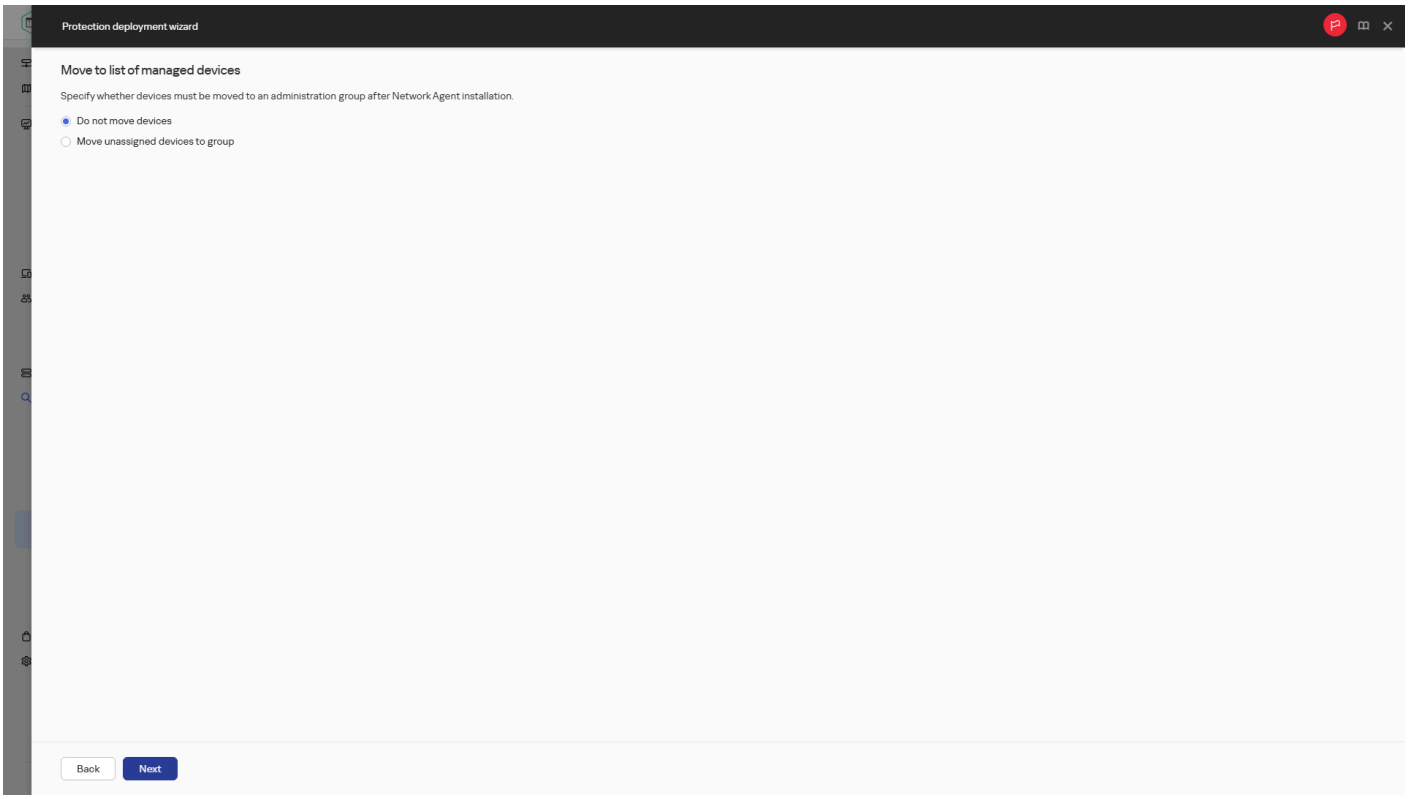
- **不移动设备**

  设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

- **将未分配的设备移动到此组**

  设备被移动到您选择的管理组。

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



选择将设备移动到管理组的选项

步骤 10：选择访问设备的账户

如果必要，添加要用于启动远程安装任务的账户：

- **不需要账户(网络代理已安装)**

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

  如果网络代理未安装在客户端设备，该选项不可用。

- **需要账户(不使用网络代理)**

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

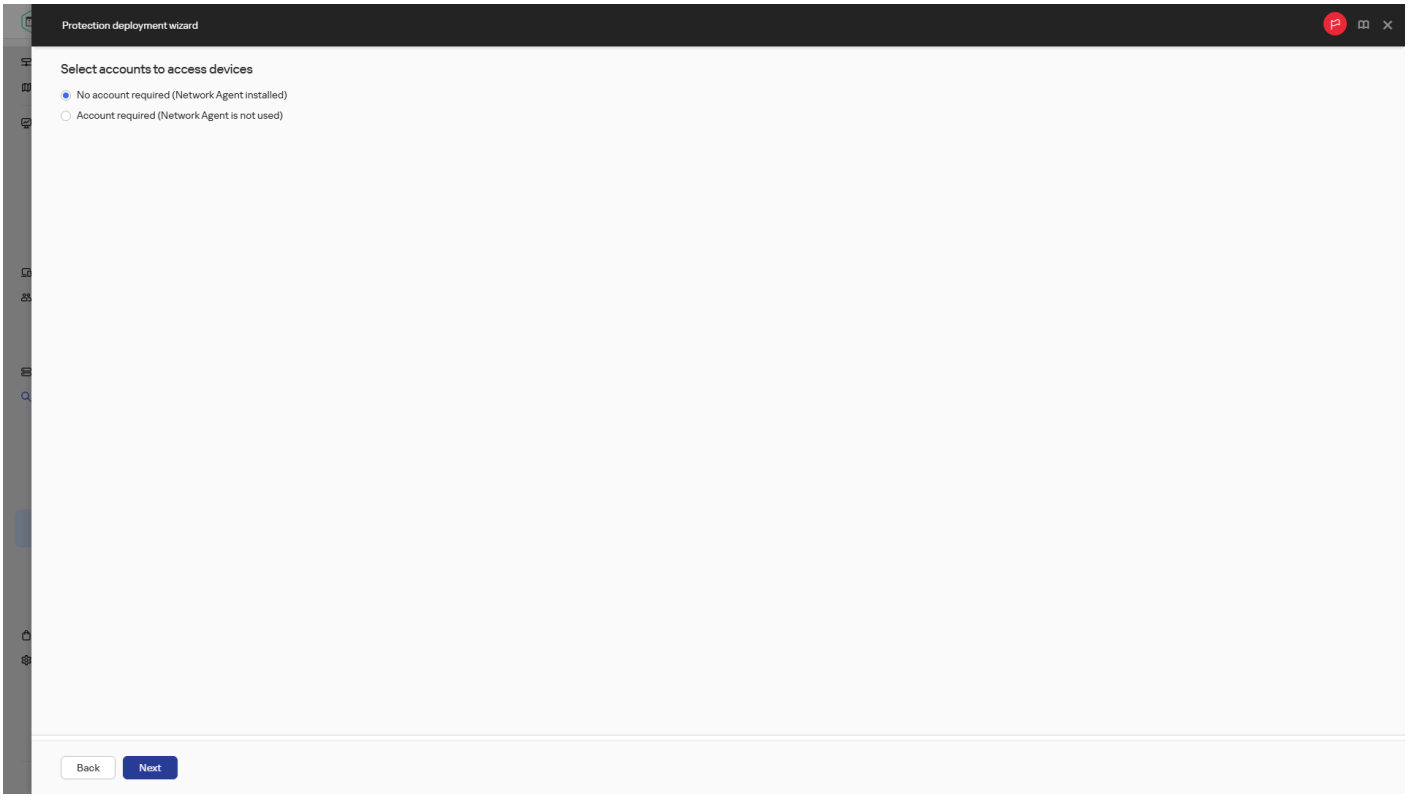
  - **本地或域账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地或域账户**，然后指定用户账户凭据。

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

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

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

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<用户电子邮箱>"
```



选择访问设备的账户

步骤 11：开始安装

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

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

单击“**确定**”完成保护部署向导的最后一步。

添加 Kaspersky 应用程序的管理插件

要使用OSMP控制台远程管理卡巴斯基应用程序，您必须使用管理网页插件。部署Kaspersky Next XDR Expert后，管理网页插件会自动安装。

如果您需要手动重新安装管理网页插件，请联系卡巴斯基技术支持，以接收包含所需管理插件的存档。

要重新安装卡巴斯基应用程序的管理网页插件：

1. 将管理 Web 插件压缩文件移动到 KDT 实用程序所在的管理员主机。
2. 如有必要，在管理员主机上导出当前版本的配置文件。
   如果没有添加或修改安装参数，则无需导出配置文件。

3. 运行以下命令以安装插件：

   ```
   ./kdt apply -k <path_to_plugin_archive> -i <path_to_configuration_file>
   ```

   在命令中，指定插件压缩文件的路径和当前配置文件的路径。如果没有添加或修改安装参数，则无需在命令中指定配置文件的路径。

管理网络插件随即重新安装。重新加载OSMP控制台以更新插件。

您可以使用 KDT 查看与 OSMP 相关的组件列表（包括管理 Web 插件）。此外，您还可以查看 OSMP 控制台版本和已安装的管理 Web 插件列表。为此，请在 OSMP 控制台的上部窗格中，转到您的账户菜单，然后选择“**关于**”。

卸载管理 Web 插件

您可以删除为 Kaspersky Next XDR Expert 提供附加功能的卡巴斯基应用程序的管理 Web 插件。Kaspersky Next XDR Expert 服务插件用于确保 Kaspersky Next XDR Expert 正确运行，因此无法删除（例如，事故响应平台的插件）。

要删除管理 Web 插件：

1. 如果需要，请运行以下命令获取要删除的插件的名称：

   ```
   ./kdt state
   ```

   显示组件列表。

2. 在管理员主机上，运行以下命令。指定要删除的插件的名称：

   ```
   ./kdt remove --cnab <plug-in_name>
   ```

KDT 删除指定的管理 Web 插件。

查看集成到 Open Single Management Platform 中的组件列表

您可以使用 KDT 查看 OSMP 中集成的组件列表（包括管理 Web 插件的组件）。

要查看组件列表，

在 KDT 所在的管理员主机上，运行以下命令：

```
./kdt state
```

OSMP 中集成的组件列表（包括管理 Web 插件的组件）将显示在命令行窗口中。

查看 Kaspersky Next XDR Expert 组件的名称、参数和自定义操作

KDT 允许您查看传输压缩文件中包含的 Kaspersky Next XDR Expert 组件列表，以及已安装组件的列表。此外，您还可以查看 Kaspersky Next XDR Expert 组件的参数列表和自定义操作列表。如果组件有可用的自定义操作，您还可以使用 KDT 查看指定自定义操作的描述和参数。

*自定义操作*允许您执行特定于Kaspersky Next XDR Expert组件的其他操作。例如，恢复管理服务器数据以及增加管理服务器及其日志使用的磁盘空间量，都是通过自定义操作执行的。

自定义操作使用 KDT 运行，如下所示：

```
./kdt invoke <component_name> --action <custom_action> --param
<custom_action_parameter>
```

要查看传输压缩文件中包含的 Kaspersky Next XDR Expert 组件列表：

在 KDT 实用程序所在的管理员主机上，运行以下命令。在命令中，指定传输存档文件的路径及其名称：

```
./kdt describe -k <transport_archive_name_with_path>
```

要查看 Kaspersky Next XDR Expert 组件列表：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt describe
```

将显示 Kaspersky Next XDR Expert 组件列表。

要查看 Kaspersky Next XDR Expert 组件的参数列表和自定义操作列表：

在 KDT 实用程序所在的管理员主机上，运行以下命令并指定 Kaspersky Next XDR Expert 组件的名称：

```
./kdt describe <component_name>
```

将显示指定组件可用的参数和自定义操作的列表。

要查看自定义操作的描述和参数列表：

在 KDT 实用程序所在的管理员主机上，运行以下命令并指定 Kaspersky Next XDR Expert 组件名称及其命令：

```
./kdt describe <component_name> <custom_action>
```

将显示指定组件自定义操作的描述和参数列表。

下载和创建卡巴斯基应用程序的安装包

如果管理服务器可以访问 Internet，则可以从 Kaspersky Web 服务器创建卡巴斯基应用程序的安装包。

要下载并创建卡巴斯基应用程序的安装包：

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。

   您可以在屏幕通知列表中查看关于卡巴斯基应用程序的新安装包的通知。如果有关于新安装包的通知，您可以单击通知旁边的链接并转到可用安装包列表。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击**添加**。

   新安装包向导启动。使用“**下一步**”按钮进行向导。

3. 选择“**为卡巴斯基应用程序创建安装包**”。

   将显示 Kaspersky Web 服务器上的可用安装包列表。该列表仅包含与当前版本的 Open Single Management Platform 兼容的应用程序的安装包。默认情况下，列表仅显示与界面语言匹配的应用程序。要显示其他语言，请单击“**过滤器**”并配置过滤器设置。

4. 单击安装包名称。例如，Kaspersky Endpoint Security for Linux。

   带有安装包信息的窗口打开。

   > 如果符合适用的法律法规，您可以下载并使用包含实施强加密的加密工具的安装包。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 安装包，请参考组织的客户端设备所在国家/地区的法律。

5. 阅读相关信息，然后单击“**下载并创建安装包**”按钮。

   如果分发包无法转换为安装包，将显示“**下载并创建安装包**”按钮而不是“**下载分发包**”。

   下载安装包到管理服务器开始。您可以关闭向导窗口。在这种情况下，下载过程将在后台模式下继续。您可以跟踪安装包的下载状态以及在**包状态**列中过滤和排序状态。

   如果下载过程停止并且下载状态切换为“**接受 EULA**”，则单击安装包名称，然后继续执行说明的第 6 步。默认情况下，状态为“**进行中**”和“**接受 EULA**”的安装包会放在列表的开头。

   > 如果所选分发包中包含的数据大小超过当前限制，将显示错误消息。您可以更改限制值，然后继续创建安装包。

6. 对于一些卡巴斯基应用程序，下载过程中将显示“**显示 EULA**”按钮。如果它不显示，做以下操作：

   a. 单击“**显示 EULA**”按钮以阅读最终用户授权许可协议（EULA）。

   b. 阅读屏幕上显示的 EULA，然后单击“**接受**”。

   在您接受 EULA 后，下载继续。如果您单击“**拒绝**”，下载将停止。

7. 下载完成后，单击“**关闭**”按钮。

该安装包将出现在安装包列表中。

从文件创建安装包

您可以使用自定义安装包执行以下操作：

- 在客户端设备上安装任何应用程序（例如文本编辑器），例如通过任务。
- 创建独立安装包。

自定义安装包是一个包含一组文件的文件夹。创建自定义安装包的源是*存档文件*。存档文件包含一个或多个必须包含在自定义安装包中的文件。

创建自定义安装包时，您可以指定命令行参数，例如以静默模式安装应用程序。

要创建自定义安装包：

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击**添加**。

   新安装包向导启动。使用**下一步**按钮进行向导。

3. 选择“**从文件创建安装包**”

4. 指定包名称并单击“**浏览**”按钮。

5. 在打开的窗口中，选择可用磁盘上的压缩文件。

   您可以上传 ZIP、CAB、TAR 或 TAR.GZ 压缩文件。无法从 SFX（自解压存档）文件创建安装包。

   开始上传文件到管理服务器。

6. 如果您指定了卡巴斯基应用程序的文件，则系统可能会提示您阅读并接受该应用程序的最终用户授权许可协议 (EULA)。要继续，您必须接受 EULA。仅当您完全阅读、理解并接受 EULA 条款后，才选中“**接受该最终用户授权许可协议的条款和条件**”选项。

   此外，系统还可能会提示您阅读并接受隐私策略。要继续，您必须接受隐私策略。仅当您理解并同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家）后，才选中“**我接受隐私策略**”选项。

7. 选择一个文件（从所选压缩文件中提取的文件列表中选择），然后指定可执行文件的命令行参数。

   您可以指定命令行参数，以静默模式从安装包中安装应用程序。指定命令行参数是可选的。

   创建安装包的过程将开始。

   该向导将在过程完成时通知您。

   如果未创建安装包，则会显示相应的消息。

8. 单击**完成**按钮关闭向导。

安装包出现在安装包列表。

在管理服务器上的可用安装包列表中，通过单击带有自定义安装包名称的链接，您可以：

- 查看安装包的以下属性：
  - **名称**。自定义安装包名称。
  - **包状态**。安装包下载状态。
  - **源**。应用程序供应商名称。
  - **应用程序**。打包到自定义安装包中的应用程序名称。
  - **版本**。应用程序版本。
  - **语言**。打包到自定义安装包中的应用程序的语言。
  - **大小(MB)**。安装包的大小。
  - **操作系统**安装包适合的操作系统的类型。
  - **创建日期**。安装包创建日期。
  - **已修改**。安装包修改日期。
  - **类型**。安装包的类型。
- 更改命令行参数。

创建独立安装包

您和组织中的设备用户可以使用独立安装包在设备上手动安装应用程序。

独立安装包是一个可执行文件，您可以将其存储在 Web 服务器或共享文件夹中，通过电子邮件发送或通过另一种方式传输到客户端设备。在客户端设备上，用户可以在本地运行收到的文件来安装应用程序，而无需使用 Kaspersky Next XDR Expert。您可以为卡巴斯基应用程序和第三方应用程序创建独立安装包。要为第三方应用程序创建独立安装包，必须创建自定义安装包。

如果管理服务器可以访问互联网，则使用**将更新下载至管理服务器存储库**任务来下载创建网络代理程序独立安装包所需的依赖项。如果管理服务器无法访问互联网，请执行以下步骤：

1. 执行以下命令创建RIUtilsArchiveDirUsed标志：

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. 运行以下命令来重新启动tomcat服务：

   ```
   systemctl restart kladminserver_srv.service
   ```

3. 从卡巴斯基网站下载以下压缩包，并将压缩包放置在/var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives文件夹中：
   - ri_utils_win32.zip
   - ri_utils_arm64.zip

请勿重命名存档文件。

管理服务器现在已具备所需的依赖项。

确保独立安装包不适用于第三方。

要创建独立安装包：

1. 在主菜单中，转到“**软件管理**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。

2. 在安装包列表中选择安装包，然后在列表上方单击“**部署**”按钮。

3. 选择**使用独立包**选项。

   独立安装包创建向导启动。使用**下一步**按钮进行向导。

4. 如果随着所选的应用程序安装网络代理，请确保已启用“**网络代理和该应用程序一起安装**”选项。

   显示的选项取决于您为其创建独立安装包的应用程序。

   默认情况下已启用该选项。如果不确定设备上是否安装了网络代理，建议启用此选项。如果设备上已经安装了网络代理，则在安装带有网络代理的独立安装包之后，网络代理将更新为较新的版本。

   如果禁用此选项，则网络代理将不会安装在设备上，并且该设备将不受管理。

   如果管理服务器上已经存在用于所选应用程序的独立安装包，则向导会通知您这一事实。在这种情况下，您必须选择以下操作之一：

   - **创建独立安装包**。例如，如果要为新的应用程序版本创建独立安装包，并且还希望保留为先前的应用程序版本创建的独立安装包，请选择此选项。新的独立安装包位于另一个文件夹中。
   - **使用现有的独立安装包**。如果要使用现有的独立安装包，请选择此选项。安装包创建过程将不会开始。
   - **重新编译现有的独立安装包**。如果要再次为同一应用程序创建独立安装包，请选择此选项。独立安装包位于同一文件夹中。

5. 在“**移动到受管理设备列表**”步骤中，默认已选择“**不移动设备**”选项。如果您不希望在安装网络代理后将客户端设备移至任何管理组，则不要更改选项选择。

   如果要在安装网络代理后移动客户端设备，请选择“**将未分配的设备移动到此组**”选项并指定要将客户端设备移至的管理组。默认情况下，设备移至“**受管理设备**”组。

6. 独立安装包创建过程完成后，单击“**完成**”按钮。

   独立安装包创建向导关闭。

独立安装包已创建并放置在 Web 服务器上。您可以通过单击安装包列表上方的“**查看独立包列表**”按钮来查看独立包列表。

更改自定义安装包数据大小的限制

创建自定义安装包期间解压缩的数据总大小受到限制。默认限制为 1 GB。

如果尝试上传的压缩文件所包含的数据超出当前限制，将显示一条错误消息。从大型分发包创建安装包时，可能必须增加此限制值。

要更改自定义安装包大小的限制值，

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n MaxArchivePkgSize -t d -v <字节数>'
```

其中 <number of bytes> 是十六进制或十进制格式的字节数。

例如，如果要求的限制为 2 GB，您可以指定十进制值 2147483648 或十六进制值 0x80000000。在这种情况下，对于管理服务器的本地安装，您可以使用以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648'
```

自定义安装包数据大小的限制即被更改。

准备 Linux 设备以安装网络代理

在 Linux 设备上安装网络代理之前，您必须执行 Linux 设备所需的准备步骤。

要准备运行 Linux 的设备以远程安装网络代理：

1. 确保您要在上面安装 Network Agent for Linux 的设备运行受支持的 Linux 分类。
2. 如果要在 AltOS 上以封闭软件环境模式安装网络代理，请在安装完成前禁用封闭软件环境模式。
3. 使用 Web Console 下载网络代理安装包，或使用应用程序分发包。
   如果您需要在运行含glibc 2.5的 Linux操作系统的设备上安装网络代理，则必须使用云控制台界面或从卡巴斯基网站下载 *Kaspersky Network Agent for Linux Legacy*安装包。
4. 确保目标 Linux 设备上安装了以下软件：
   - Sudo（对于 Ubuntu 10.04，Sudo 版本为 1.7.2p1 或更高）
   - Perl 语言解释器版本 5.10 或更高版本
   - ps实用程序
5. 测试设备配置：
   a. 检查是否您可以通过 SSH 客户端（例如 PuTTY）连接到设备。
      如果您无法连接到设备，请打开 `/etc/ssh/sshd_config` 文件，并确保以下设置具有下列相应值：
      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

如果您可以毫无问题地连接到设备，请不要修改 /etc/ssh/sshd_config 文件；否则在运行远程安装任务时可能会遇到 SSH 认证失败的情况。

保存文件（如有必要），并使用 `sudo service ssh restart` 命令重启 SSH 服务。

b. 确保在Linux的未分配设备上，TCP端口22已打开且可访问。

要成功安装Linux的网络代理程序，必须启用TCP端口22。

c. 禁用要连接设备的用户账户的 sudo 密码。

d. 在 sudo 中使用 `visudo` 命令打开 sudoers 配置文件。

在打开的文件中，将以下行添加到文件末尾：`<username> ALL = (ALL) NOPASSWD: ALL`。此种情况下，< 用户名 > 是将用于通过 SSH 连接设备的用户账户。如果您使用的是 Astra Linux 操作系统，请在 /etc/sudoers 文件中添加包含以下文本的最后一行：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. 保存并关闭 sudoers 文件。

f. 通过 SSH 再次连接设备并确保 Sudo 服务不会提示您输入密码；您可以使用 `sudo whoami` 命令进行操作。

6. 如果要在运行具有 systemd 初始化系统的操作系统的设备上远程安装网络代理，请打开 `/etc/systemd/logind.conf` 文件，然后执行以下操作之一：

- 将 no 指定为 `KillUserProcesses` 设置的值：`KillUserProcesses=no`。
- 对于 `KillExcludeUsers` 设置，输入要执行远程安装的账户的用户名，例如，`KillExcludeUsers=root`。

Astra Linux 目标设备

如果目标设备运行的是 Astra Linux，请在 `/home/<` 用户名 `>/.bashrc` 文件中添加 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 字符串，其中 < 用户名 > 是将用于通过 SSH 连接设备的用户账户。

OSnova 目标设备

如果目标设备正在运行 OSnova，请执行以下操作：

a. 打开 `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` 文件，然后注释掉 `#KillUserProcess=yes` 行。

b. 打开 `/usr/lib/NESS/pam-user-session` 文件，然后注释掉 `#loginctl terminate-session "$XDG_SESSION_ID"` 行。

要应用更改的设置，重启 Linux 设备或执行以下命令：

```
sudo systemctl restart systemd-logind.service
```

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

8. 如果要在封闭软件环境模式下运行 Astra Linux 操作系统的设备上安装网络代理，请执行额外的步骤来准备 Astra Linux 设备。

9. 如果您想在运行 Ubuntu Server 或 Ubuntu 桌面版本 10.04 的设备上安装网络代理，请执行额外步骤来准备这些设备。

10. 如果要在运行 Linux 操作系统且安装了 glibc 2.5 的设备上安装网络代理，请执行额外步骤来准备目标设备。

11. 如果您在 AltOS 上以封闭软件环境模式安装网络代理，请重新启用封闭软件环境模式。

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

Linux 设备已准备好安装网络代理。您可以远程、在交互模式下或在静默模式下安装网络代理。

准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理

在运行 SUSE Linux Enterprise Server 15 的设备上安装网络代理之前，您必须执行两个准备过程：下面说明中的一个步骤和适用于任何 Linux 设备的常规准备步骤。

要在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理：

在安装网络代理之前，运行以下命令：

```
sudo zypper install insserv-compat
```

这使您能够安装 insserv-compat 软件包并正确配置网络代理。

运行 `rpm -q insserv-compat` 命令，检查该软件包是否已安装。

如果您的网络包含大量运行 SUSE Linux Enterprise Server 15 的设备，您可以使用配置和管理公司基础架构的专用软件。通过使用此软件，您可以一次在所有必要的设备上自动安装 insserv-compat 软件包。例如，您可以使用 Puppet®、Ansible®、Chef®，也可以编写自己的脚本—使用任何您觉得方便的方法。

如果设备没有 SUSE Linux Enterprise 的 GPG 签名密钥，您可能会遇到以下警告：`Package header is not signed!` 选择 `i` 选项以忽略该警告。

准备好 Linux 设备后，您可以远程、以交互模式或静默模式安装网络代理。

为远程安装准备 Windows 设备

远程安装应用程序到客户端设备时可能会因下列原因返回错误：

- 该任务已成功在该设备上执行。
  在此情况下，该任务无需再执行。
- 任务开始后，设备被关闭。
  在此情况下，请打开设备，然后重新启动此任务。

- 管理服务器与客户端设备上安装的网络代理之间无连接。

  要确定问题原因，请使用客户端设备的远程诊断实用程序 (klactgui)。

- 如果设备上未安装网络代理，远程安装过程中可能出现下列问题：

  - 网络错误
  - 操作系统配置错误
  - 远程安装任务中账户权限配置错误

  为避免在未安装网络代理的客户端设备上安装应用程序时出现问题，您必须使用 Open Single Management Platform 的远程安装任务强制安装选定的安装包，前提是每台设备都拥有一个具备本地管理员权限的用户账户。

之前曾使用 riprep 实用程序为 Windows 设备进行远程安装前的准备工作。现在这被认为是一种配置操作系统的过时方法。不建议在比 Windows XP 和 Windows Server 2003 R2 更新版本的操作系统上使用 riprep 实用程序。

如果管理服务器无法直接访问设备，也可以采用强制安装的方式。例如，如果设备位于隔离网络或本地网络上，而管理服务器位于隔离区域 (DMZ) 中。在这种情况下，需要借助分发点来向此类设备进行部署。

当在子网内的设备上执行安装操作时，若这些设备通过低带宽通道与管理服务器通信，而同一子网内的设备之间有更宽的带宽通道可用，那么也可以将分发点用作本地安装中心。

初始部署时，不会安装网络代理。因此，在远程安装任务的设置中，无法选择使用网络代理安装应用程序所需的文件分发。您只能选择通过管理服务器或分发点使用操作系统资源来分发文件。

您应该在远程安装任务的设置中指定有权访问 admin$ share 的账户。

您可以通过以下方式指定目标设备：明确指定（列出设备清单），选择它们所属的 Open Single Management Platform 管理组；或通过基于指定标准创建设备分类。安装开始时间定义在任务计划中。如果任务属性中启用了**运行错过的任务**设置，任务可以在设备开启时立即运行，或设备被移动到目标管理组时立即运行。

强制安装包括传送安装包到目标设备、随后复制文件到每个目标设备的 admin$ 资源，和在这些设备上远程注册支持服务。向目标设备传送安装包是通过 Open Single Management Platform 中确保网络交互的功能来执行的。以下条件必须在此种情况下被满足：

- 可以从装有 Windows 操作系统的分发点访问目标设备，该分发点执行对客户端设备的远程安装，并被选定为目标设备的分发点。
- 目标设备的名称解析在网络中运行正常。
- 设备上的管理共享(admin$)保持启用。
- 以下系统服务正在目标设备上运行：

  - 服务器（LanmanServer）

    默认情况下，该服务正在运行。

  - DCOM 服务器进程启动器 (DcomLaunch)

- RPC 端点映射器 (RpcEptMapper)
- 远程过程调用 (RpcSs)

- TCP 445 端口在目标设备上打开，以便通过 Windows 工具实现远程访问。

  TCP 139、UDP 137 和 UDP 138 由较旧的协议使用，对于当前应用程序来说不再是必需的。

  防火墙必须允许动态出站访问端口，以便从分发点连接到目标设备。
- 在网络代理部署期间，允许 Active Directory 域策略安全设置提供 NTLM 协议的操作。
- 在运行 Microsoft Windows XP 的目标设备上，简单文件共享模式被禁用。
- 在目标设备上，访问共享和安全模型被设置为"*经典 - 本地用户以自己的身份验证*"。它绝不可以是*仅限访客 – 本地用户需要以访客身份进行身份验证*。
- 目标设备是域成员，或带有管理员权限的统一账户提前在目标设备上被创建。

要成功部署网络代理或其他应用程序到未加入 Windows Server 2003 或更高版本的 Active Directory 域的设备，您必须在该设备上禁用远程 UAC。远程 UAC 是阻止本地管理账户访问 admin$ 的原因之一，这对于强制部署网络代理或其他应用程序必不可少。禁用远程 UAC 不会影响本地 UAC。

在未分配到任何 Open Single Management Platform 管理组的新设备上进行安装时，您可以打开远程安装任务属性，并指定网络代理安装后设备要移入的管理组。

当创建组任务时，记住每个组任务都影响所选组的嵌套组中的所有设备。因此，您必须避免在子组中的重复安装任务。

创建强制安装应用程序的任务的一个简化方法是自动安装。为此，您必须打开管理组属性，打开安装包列表，然后选择必须在该组中设备上安装的包。结果，所选安装包将被自动安装在该组和其所有子组中的所有设备上。包被安装的时间间隔取决于网络吞吐量和网络设备总数。

您可以使用多个分发点来减少将安装包传送到目标设备时的负载。注意，该安装方法给作为分发点的设备增加了大量负载。如果您使用分发点，您必须确保它们存在于托管目标设备的每个隔离子网中。

文件夹 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 所在分区的可用磁盘空间必须超过所安装应用程序的分发包总大小的好几倍。

准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理

在封闭软件环境模式下运行 Astra Linux 的设备上安装网络代理之前，您必须执行两个准备过程：下面说明中的一个和适用于任何 Linux 设备的常规准备步骤。

以拥有 root 权限的账户运行本说明中提供的命令。

要准备在封闭软件环境模式下运行 Astra Linux 的设备来安装网络代理：

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在命令行中，运行以下命令来安装兼容包：

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

3. 为应用程序密钥创建一个目录：

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

4. 将应用程序密钥/opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg放在上一步创建的目录中：

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

   > 如果 Open Single Management Platform 分发包中不包含 kaspersky_astra_pub_key.gpg 应用程序密钥，您可以通过单击以下链接下载：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. 更新 RAM 磁盘：

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

   重新启动系统。

Linux 设备已准备好安装网络代理。您可以远程、在交互模式下或在静默模式下安装网络代理。

以静默模式安装 Linux 网络代理（使用应答文件）

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

在基于 Linux 的设备上安装网络代理之前，您必须完成所有基于 Linux 的设备所需的常规准备步骤。

完成常规步骤后，您可以按照您的操作系统特定的附加说明进行操作：

- 准备运行 SUSE Linux Enterprise Server 15 的设备
- 准备在封闭软件环境模式下运行 Astra Linux 的设备
- 准备运行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的设备
- 准备一台运行 Linux 操作系统且安装了 glibc 2.5 的设备

要以静默模式安装 Linux 网络代理：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。
2. 创建应答文件（TXT 格式）。将变量列表以 VARIABLE_NAME=variable_value 的格式添加到应答文件，每个变量一行。

   为了正确使用应答文件，必须在其中包含至少三个必需变量：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

您还可以添加任意可选变量以使用更具体的远程安装参数。下表列出了可以包含在应答文件中的所有变量：

用作以静默模式安装 Linux 网络代理的参数的应答文件变量

用作以静默模式安装 Linux 网络代理的参数的应答文件变量

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

KLNAGENT_DEVICEOWNER_REGISTRATION_START	否	允许在网络代理安装后作为设备所有者实用程序运行用户注册。如果关闭，则用户无法注册为设备所有者。	1 – 用户注册为设备所有者实用程序将在网络代理安装后运行。 其他–已关闭。
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	否	定义是否为"*未定义*"状态的网络代理自动安装下载的更新。	true（默认）–自动安装这些更新。 false–不会自动安装这些更新。

3. 运行网络代理安装程序。环境变量 KLAUTOANSWERS 指定应答文件的路径，该变量会被传递给安装命令。运行以下命令之一：

   - 要将网络代理通过 RPM 包安装到 32 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件的路径> yum install ./klnagent-<内部版本号>.i386.rpm`
   - 要将网络代理通过 RPM 包安装到 64 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件的路径> yum install ./klnagent64-<内部版本号>.x86_64.rpm`
   - 要在 Arm 架构的 64 位操作系统上通过 RPM 包安装网络代理，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件的路径> yum install ./klnagent64-<内部版本号>.aarch64.rpm`
   - 要将网络代理通过 DEB 包安装到 32 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件的路径> apt install ./klnagent_<内部版本号>_i386.deb`
   - 要将网络代理通过 DEB 包安装到 64 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件的路径> apt install ./klnagent64_<内部版本号>_amd64.deb`
   - 要在 Arm 架构的 64 位操作系统上通过 DEB 包安装网络代理，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件的路径> apt install ./klnagent64_<内部版本号>_arm64.deb`

   根据操作系统配置，您还可以使用 rpm、dpkg 或 dnf 包管理器来安装网络代理。

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

查看独立安装包列表

您可以查看独立安装包列表以及每个独立安装包的属性。

要查看所有安装包中独立安装包的列表：

在列表上方，单击"**查看独立包列表**"按钮。

在独立安装包列表中，其属性显示如下：

- **包名称**。根据安装包中包含的应用程序名称和应用程序版本自动形成的独立安装包名称。
- **应用程序名称**。独立安装包中包含的应用程序名称。
- **应用程序版本**。
- **网络代理安装包名称**。仅当独立安装包中包含网络代理时，才显示该属性。
- **网络代理版本**。仅当独立安装包中包含网络代理时，才显示该属性。

- **大小**。文件大小（MB）。
- **组**。安装网络代理后，客户端设备将移动到的组的名称。
- **创建日期**。独立安装包的创建日期和时间。
- **已修改**。独立安装包的修改日期和时间。
- **路径**。独立安装包所在文件夹的完整路径。
- **网址**。独立安装包位置的网址。
- **文件哈希**。该属性用于证明独立安装包没有被第三方更改，并且用户拥有的文件与您创建并传输给用户的文件相同。

网络代理独立包或在虚拟管理服务器上创建的任何包的安装包列表中没有关于大小、文件哈希和路径的信息。这些独立包在下载时生成。

要查看特定安装包的独立安装包列表：

在列表中选择安装包，然后在列表上方单击“**查看独立包列表**”按钮。

在独立安装包列表中，您可以执行以下操作：

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

将安装包分发至从属管理服务器

通过 Open Single Management Platform，您可以创建用于卡巴斯基应用程序和第三方应用程序的安装包，以及将安装包分发至客户端设备并通过分发包来安装应用程序。要优化主管理服务器上的负载，您可以将安装包分发至从属管理服务器。之后，从属服务器将安装包传输到客户端设备，然后您可以在客户端设备上远程安装应用程序。

要将安装包分发至从属管理服务器：

1. 请确保从属管理服务器连接至主管理服务器。
2. 在主菜单中，转到“**任务**”。
   将显示任务列表。

3. 单击**添加**。

   “新任务向导”启动。遵照向导的说明操作。

4. 在“**新任务设置**”页面的“**应用程序**”下拉列表中，选择“**Kaspersky Security Center**”。然后，从**任务类型**下拉列表中选择**分发安装包**，然后指定任务名称。

5. 在“**任务范围**”页面，通过以下方式之一选择任务分配到的设备：

   - 如果要为特定管理组中的所有从属管理服务器创建任务，选择该组，然后为它创建组任务。
   - 如果要为特定的从属管理服务器创建任务，选择这些服务器，然后为它们创建任务。

6. 在“**分发的安装包**”页面，选择要复制到从属管理服务器的安装包。

7. 指定一个账户，以该账户来运行“*分发安装包*”任务。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。

8. 在**完成任务创建**页面上，您可以启用**创建完成时打开任务详情**选项以打开任务属性窗口，然后修改默认任务设置。或者，您可以稍后随时配置任务设置。

9. 单击“**完成**”按钮。

   为了将安装包分发至从属管理服务器而创建的任务显示在任务列表中。

10. 手动运行该任务，或者按照任务设置中指定的计划等待任务启动。

    任务完成后，所选的安装包将复制到指定的从属管理服务器。

将 Kaspersky Next XDR Expert 与 Kaspersky Endpoint Security for Linux 一起部署

本节介绍如何在由六台设备组成的集群中部署 Kaspersky Next XDR Expert 和 Kaspersky Endpoint Security 12.5 for Linux。Kaspersky Endpoint Security for Linux 12.5 以标准模式安装在已安装 OSMP 组件的设备上。您可以通过命令行管理 Kaspersky Endpoint Security for Linux，无需安装图形界面。必须在所有设备上安装网络代理。

为了确保 Kaspersky Next XDR Expert 与 Kaspersky Endpoint Security for Linux 实现最佳互操作性，我们建议配置 Kaspersky Endpoint Security for Linux 排除项。

部署 Kaspersky Next XDR Expert 和 Kaspersky Endpoint Security 12.5 for Linux

1. 准备一个由六台设备组成的集群。

   此时请勿安装 Kaspersky Next XDR Expert。

2. 从卡巴斯基网站下载 Kaspersky Endpoint Security for Linux 分发包。

3. 在集群中的每台设备上：

a. 将下载的文件（例如 kesl_12.5.0-1569_amd64.deb）放入 /root 目录。

b. 运行以下命令安装 Kaspersky Endpoint Security：

```
apt install /root/kesl_12.5.0-1569_amd64.deb
```

c. 运行以下命令启动配置向导：

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

d. 使用配置向导指定安装参数：

- 是否要在轻代理模式下使用 Kaspersky Endpoint Security？[n]: **Enter**
- 是否要在 Endpoint Detection and Response 代理模式下使用 Kaspersky Endpoint Security？[n]: **Enter**
- 是否要使用 EDR Expert Cloud 组件？**Enter**
- [ru_RU.UTF-8]: **Enter**
- 按 Enter 键显示最终用户授权许可协议和隐私策略： y **Enter**
  要退出协议阅读模式，请按 **q**。
- 我确认我已完全阅读、理解并接受该最终用户授权许可协议的条款和条件 [y/n]: y **Enter**
- 我了解并同意按照隐私策略所述来处理和传输我的数据(包括传输到第三方国家/地区)。我确认我已完全阅读并理解隐私策略 [y/n]: y **Enter**
- 我确认我已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件（KSN 声明的文本位于 /opt/kaspersky/kesl/doc/ksn_license.en 文件中）[y/n]: y **Enter**
- 输入要授予管理员角色的用户名。要跳过此步骤，请按 Enter 键： **Enter**
- 为拦截系统事件，应用程序可以使用可更新的内核模块或 fanotify 技术。是否要使用可更新的内核模块？[n]: **Enter**
- 指定更新源。可选值：KLServers|SCServer|<customsource> [KLServers]: **Enter**
- 如果不使用代理服务器，请输入 [n]： **Enter**
- 是否立即下载最新的应用程序数据库更新？[y]: **Enter**
- 是否启用应用程序数据库自动更新？[y]: **Enter**
- 您需要先激活应用程序才能使用它。要立即激活应用程序，请输入密钥文件的路径或激活码。要使用试用密钥激活应用程序，请按 Enter 键： **<your_activation_code> Enter**

e. 依次运行以下命令，创建 Kaspersky Endpoint Security 设置的备份副本：

```
kesl-control --get-app-settings > kesl_app_before.txt
kesl-control --get-settings File_Threat_Protection > kesl_ftp_before.txt
kesl-control --get-settings Behavior_Detection > kesl_bd_before.txt
kesl-control --get-settings System_Integrity_Monitoring > kesl_fim_before.txt
findmnt -o TARGET,SOURCE,FSTYPE > mounts_before.txt
```

f. 将包含设置和排除项的文件放在 /root 目录中。

g. 依次运行以下命令，应用文件中的排除项：

- `kesl-control --set-app-settings --file /root/kesl_app.txt`

  kesl_app.txt 文件示例：

```
SambaConfigPath=/etc/samba/smb.conf
NfsExportPath=/etc/exports
TraceFolder=/var/log/kaspersky/kesl/
TraceLevel=None
TraceMaxFileCount=10
TraceMaxFileSize=500
BlockFilesGreaterMaxFileNamePath=16384
DetectOtherObjects=No
UseKSN=Extended
CloudMode=Yes
UseMDR=No
UseEdrOptimum=No
UseProxy=No
ProxyServer=
ProxyBypass=
ProxyBypassEdr=No
ProxyBypassSandbox=No
ProxyBypassNdr=No
MaxEventsNumber=500000
LimitNumberOfScanFileTasks=5
UseSyslog=Yes
EventsStoragePath=/var/opt/kaspersky/kesl/private/storage/events.db
FileBlockDuringScan=Yes
NamespaceMonitoring=No
PowerSaveMode=Yes
UseOnDemandCPULimit=No
OnDemandCPULimit=100
BackupSizeLimit=1024
BackupDaysToLive=30
QuarantineSizeLimit=200
QuarantineFillingNotification=90
QuarantineBackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
ShowPopUpNotifications=Yes
InterceptorMode=UseFanotify
InterceptorFallbackStrategy=FallbackToFanotify
InterceptorApplyStrategy=RestartServiceManually
SystemEventsTransmission=No
ExcludedMountPoint.item_0000=/run/netns/**
ExcludedMountPoint.item_0001=/run/k0s/containerd/io.containerd.grpc.v1.cri/sandboxes/**
ExcludedMountPoint.item_0002=/run/k0s/containerd/io.containerd.runtime.v2.task/**
ExcludedMountPoint.item_0003=/var/lib/k0s/kubelet/pods/**
ExcludedMountPoint.item_0004=/var/lib/k0s/kubelet/plugins/**
ExcludedMountPoint.item_0005=/opt/kaspersky/**
ExcludedMountPoint.item_0006=/var/log/pods
ExcludedMountPoint.item_0007=/var/tmp/alert-rules
ExcludedMountPoint.item_0008=/var/tmp/scripts
ExcludedMountPoint.item_0009=/*-metrics-data
ExcludedMountPoint.item_0010=/var/run/nats
ExcludedMountPoint.item_0011=/data
ExcludedMountPoint.item_0012=/storage
ExcludedMountPoint.item_0013=/var/loki
ExcludedMountPoint.item_0014=/var/lib/ksc64
ExcludedMountPoint.item_0015=/var/lib/grafana
ExcludedMountPoint.item_0016=/tmp/apttmp
```

- `kesl-control --set-settings File_Threat_Protection --file /root/kesl_ftp.txt`

kesl_ftp.txt 文件示例：

```
ScanArchived=No
ScanSfxArchived=No
ScanMailBases=No
ScanPlainMail=No
TimeLimit=60
SizeLimit=8
ActionOnThreat=DisinfectDeleteIfNotPossible
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanByAccessType=SmartCheck
SkipPlainTextFiles=No
SkipDatabaseJournals=No
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0000]
AreaDesc=postgres
UseScanArea=Yes
Path=/var/lib/postgresql
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0001]
AreaDesc=Host_Kuber
UseScanArea=Yes
Path=/var/lib/k0s/kubelet
AreaMask.item_0000='*'
[ExcludedFromScanScope.item_0003]
AreaDesc=Host_TMP
UseScanArea=Yes
Path=/tmp
AreaMask.item_0000='*'
[ExcludedFromScanScope.item_0004]
AreaDesc=KUMA
UseScanArea=Yes
Path=/opt/kaspersky/kuma
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0005]
AreaDesc=CONT_TMP
UseScanArea=Yes
Path=/tmp/tmp**
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0006]
AreaDesc=CONT_TMP
UseScanArea=Yes
Path=/tmp/resultworker**
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0007]
AreaDesc=k0s_runtime
UseScanArea=Yes
Path=/run/k0s
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0008]
AreaDesc=containerd_runtime
UseScanArea=Yes
Path=/run/containerd
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0009]
AreaDesc=pod_logs
UseScanArea=Yes
Path=/var/log/pods
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0010]
AreaDesc=container_logs
UseScanArea=Yes
Path=/var/log/containers
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0011]
AreaDesc=calico_logs
UseScanArea=Yes
Path=/var/log/calico
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0012]
```

```
AreaDesc=kaspersky_logs
UseScanArea=Yes
Path=/var/log/kaspersky
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0013]
AreaDesc=kaspersky_data
UseScanArea=Yes
Path=/var/opt/kaspersky
AreaMask.item_0000=*
[ExcludedForProgram.item_0000]
ProgramPath=/var/lib/k0s/bin/containerd
ApplyToDescendants=Yes
AreaDesc=k0s_containerd
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
[ExcludedForProgram.item_0001]
ProgramPath=/var/lib/k0s/bin/containerd-shim-runc-v2
ApplyToDescendants=Yes
AreaDesc=k0s_shim
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
[ExcludedForProgram.item_0002]
ProgramPath=/var/lib/k0s/bin/runc
ApplyToDescendants=Yes
AreaDesc=k0s_runc
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
[ExcludedForProgram.item_0003]
ProgramPath=/opt/kaspersky/kuma
ApplyToDescendants=No
AreaDesc=KUMA
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
```

- `kesl-control --set-settings Behavior_Detection --file /root/kesl_bd.txt`

  kesl_bd.txt 文件示例：

```
UseTrustedPrograms=Yes
TaskMode=Block
UseAEP=No
AEPMode=Block
UseTelemetryMonopolyMode=Yes
TelemetrySource=Default
[TrustedPrograms.item_0000]
ProgramPath=/var/lib/k0s/bin/containerd
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=k0s_containerd
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0001]
ProgramPath=/var/lib/k0s/bin/runc
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=k0s_runc
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0002]
ProgramPath=/var/lib/k0s/bin/containerd-shim-runc-v2
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=k0s_shim
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0003]
ProgramPath=/usr/sbin/iptables-legacy
ApplyToDescendants=No
UseTrustedProgram=Yes
ProgramDesc=calico_iptables
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0004]
ProgramPath=/usr/sbin/xtables-nft-multi
ApplyToDescendants=No
```

```
UseTrustedProgram=Yes
ProgramDesc=calico_xtables
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0005]
ProgramPath=/usr/bin/calico-node
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=calico_node
UseTrustedProgramForDetects=Yes
[TrustedPrograms.item_0006]
ProgramPath=/opt/kaspersky/kuma
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
```

- `kesl-control --set-settings System_Integrity_Monitoring --file /root/kesl_fim.txt`

  kesl_fim.txt 文件示例：

```
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=Kaspersky internal objects
UseScanArea=Yes
Path=/opt/kaspersky/kesl/
AreaMask.item_0000=*
[ScanScope.item_0001]
AreaDesc=etc
UseScanArea=Yes
Path=/etc
AreaMask.item_0000=*
[ScanScope.item_0002]
AreaDesc=ksc
UseScanArea=Yes
Path=/opt/kaspersky/ksc64
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0000]
AreaDesc=klnagent_flags
UseScanArea=Yes
Path=/etc/opt/kaspersky/klnagent
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0001]
AreaDesc=cni_config
UseScanArea=Yes
Path=/etc/cni/net.d
AreaMask.item_0000=*
```

h. 应用排除项后，依次运行以下命令，创建 Kaspersky Endpoint Security 设置的快照：

```
kesl-control --get-app-settings > kesl_app_after.txt
kesl-control --get-settings File_Threat_Protection > kesl_ftp_after.txt
kesl-control --get-settings Behavior_Detection > kesl_bd_after.txt
kesl-control --get-settings System_Integrity_Monitoring > kesl_fim_after.txt
findmnt -o TARGET,SOURCE,FSTYPE > mounts_after.txt
```

i. 运行以下命令停止 Kaspersky Endpoint Security：

```
systemctl stop kesl-control
```

4. 在 Kaspersky Next XDR Expert 操作员的设备上，运行以下命令安装 Kaspersky Next XDR Expert：

```
./xdr/kdt/bin/kdt apply -k xdr/<full_path_to_transport_archive> -i xdr/param.yml --accept-eula
```

如果在使用 KDT 部署 Kaspersky Next XDR Expert 期间出现错误，请通过指定不带 `-i` 标志的配置文件路径来重新启动部署。

5. 在集群中的所有设备上运行以下命令，启动 Kaspersky Endpoint Security 服务：

```
systemctl start kesl
```

6. 在 Kaspersky Next XDR Expert 控制台中，下载并创建安装包。

7. 在 **软件管理 → 下载和创建安装包** 中，选择您创建的安装包，然后单击 **部署**。

8. 选择 **使用独立包**，然后选择 **下载独立安装包**。

9. 在每台集群设备上，将下载的文件（例如 klnagent64_16.3.0-1207_amd64.sh）放入 /root 目录，赋予其执行权限，然后运行该文件：

```
./klnagent64_16.3.0-1207_amd64.sh
```

10. 在 Kaspersky Next XDR Expert 控制台中，转到 **资产管理 → 资产(设备) → 管理和保护**，确保表格中包含一个以安装了网络代理的设备命名的资产。

11. 转到 **资产管理 → 资产(设备) → Detection and response**，单击三点按钮，选择 **导入 → 导入 KSC 资产 → 全部**，然后单击 **导入**。

12. 转到 **资产管理 → 资产(设备) → Detection and response**，单击三点按钮，选择 **导入 → 导入 KSC 资产属性 → 全部**，然后单击 **导入**。

    该资产会显示在 **资产管理 → 资产(设备) → Detection and response** 中。

13. 转到 **资产管理 → 策略**，然后单击 **添加**。

14. 选择 **Kaspersky Endpoint Security for Linux 12.5**，然后选择 **标准模式**。

15. 如果您想使用卡巴斯基安全网络，请接受 KSN 声明。

16. 配置 Kaspersky Endpoint Security 策略。

    如何配置 Kaspersky Endpoint Security 策略

    1. 转到 **应用程序设置** 选项卡，然后执行以下操作：

       a. 解锁以下部分中的所有设置：

       - **主机威胁防护 → 文件威胁防护**。
       - **主机威胁防护 → 行为分析 → 行为检测**。
       - **信任区域**。
       - **常规设置 → 容器扫描**。

       b. 在 **主机威胁防护 → 行为分析 → 漏洞利用防御** 部分中，解锁 **漏洞利用防御** 设置。

       c. 在 **通信和 Web 保护 → 邮件威胁防护** 部分中，将切换开关设置为 **邮件威胁防护已禁用**。

       d. 在 **通信和 Web 保护 → Web 威胁防护** 部分中，将切换开关设置为 **Web 威胁防护已禁用**。

       e. 在 **通信和 Web 保护 → 网络威胁防护** 部分中，将切换开关设置为 **网络威胁防护已禁用**。

f. 在 **通信和 Web 保护** → **防火墙** 部分中，将切换开关设置为 **防火墙已关闭**。

g. 在 **安全控制** → **系统完整性监控** 中，将切换开关设置为 **系统完整性监控已禁用**。

h. 在 **常规设置** → **检测设置** 中，解锁 **文件操作拦截模式** 设置。

i. 在 **常规** 选项卡上，将 **策略状态** 设置为 **活动**，然后单击 **发送并关闭**。

策略完全应用大约需要 20 分钟。

17. 要在策略中配置 EDR 遥测，请选择 **应用程序设置** → **内置代理配置** → **Endpoint Detection and Response Expert（本地部署）** 选项卡，然后单击 **设置**。

18. 启用 **Endpoint Detection and Response Expert（本地部署）**。

19. 选择 **[[HmgP9nbh]]Endpoint Detection and Response Expert（8.0 或更高版本）** 模式。

20. 在 **连接到遥测采集服务器** 下，单击 **添加** → **选择服务器**，然后选择唯一可用的地址。

21. 在 **连接到响应服务器** 下，单击 **添加** → **选择服务器**，然后选择唯一可用的地址。

22. 单击**保存并关闭**。

有关管理Kaspersky Endpoint Security for Linux的详细信息，请参阅在线帮助文件：

- 安装、卸载和更新应用程序。
- 使用命令行管理应用程序。
- 使用Kaspersky Security Center管理应用程序

使用远程安装任务安装应用程序

Kaspersky Next XDR Expert 允许您使用远程安装任务在设备上远程安装应用程序。那些任务通过专门向导被创建被分配到设备。要更快和更便捷地分配任务，您可以在向导窗口中指定设备（最多 1000 部设备），使用以下方法之一：

- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定默认分类或您所创建的自定义分类。您最多只能选择 1000 部设备。

在未安装网络代理的客户端设备上，为避免在安装应用程序时可能出现的问题，您必须按照 Open Single Management Platform 的远程安装任务中所述的强制部署方式进行操作。

远程安装应用程序

本部分包含有关如何在管理组、具有特定地址的设备或选择的设备上远程安装应用程序的信息。

要在特定设备上安装应用程序：

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。
3. 在**任务类型**字段中，选择**远程安装应用程序**。
4. 选择以下选项之一：

   - **分配任务到管理组**

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

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

   - **手动指定设备地址或从列表导入地址**

     您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

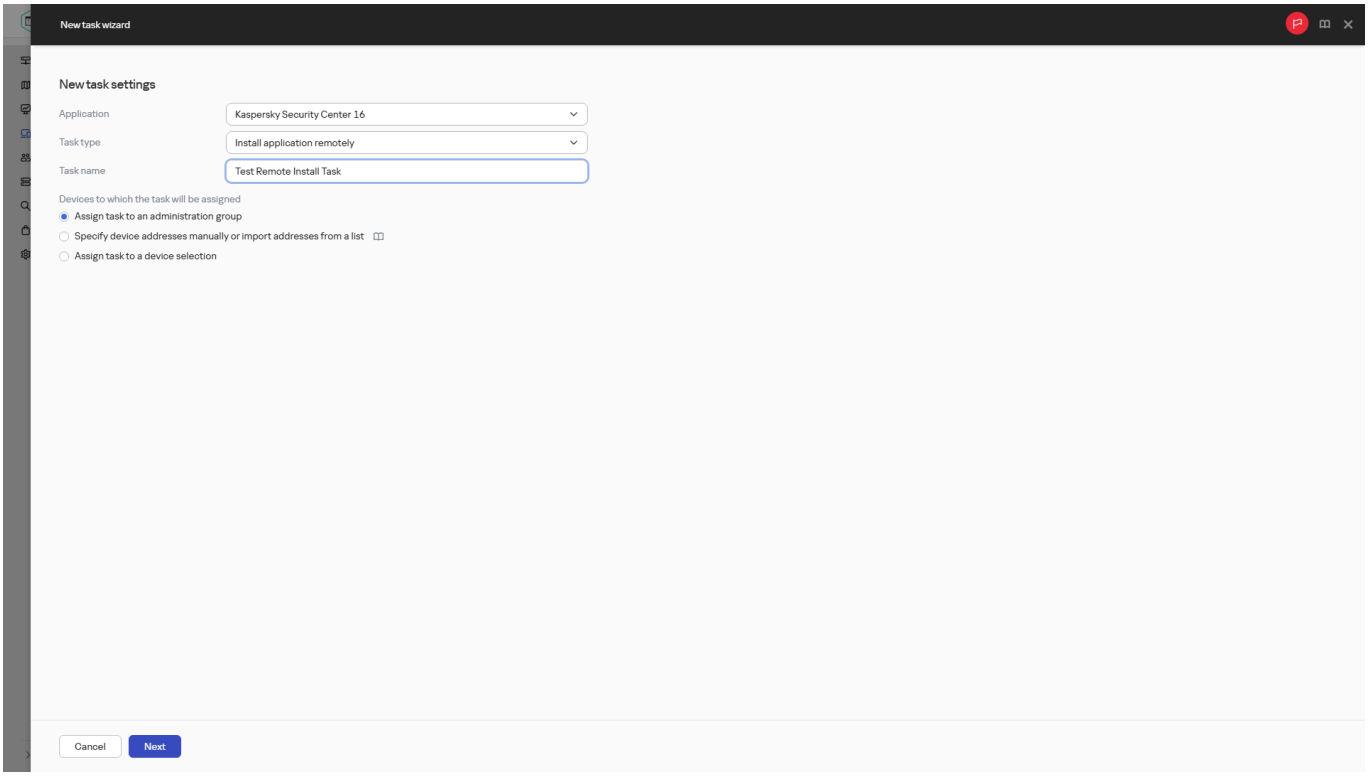
     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **分配任务到设备分类**

     该任务被分配到设备分类中的设备。您可以指定现有分类之一。

     例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

*远程安装应用程序*任务为指定设备创建。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。



创建远程安装应用程序任务

5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。

   可用设置取决于在上一步中选择的选项。

6. 在**安装包**步骤中，指定以下设置：

   - 在“**选择安装包**”字段中，选择要安装的应用程序的安装包。
   - 在“**强制下载安装包**”设置组中，指定如何将安装程序所需的文件分发到客户端设备中。

     - **使用网络代理**

       如果启用此选项，安装包通过安装在客户端设备上的网络代理传送到客户端设备。

       如果禁用此选项，则使用客户端的操作系统传送安装包。

       如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。

       默认情况下已启用该选项。

     - **通过分发点使用操作系统资源**

       如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。

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

       默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。

       在未安装网络代理的设备上安装 Windows 应用程序（包括 Windows 网络代理）的唯一方法是使用基于 Windows 的分发点。因此，当您安装 Windows 应用程序时：

       - 选择此选项。
       - 确保为目标客户端设备分配了分发点。
       - 确保分发点基于 Windows。

     - **通过管理服务器使用操作系统资源**

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

       默认情况下已启用该选项。

   - 在**同时下载的最大数量**字段中，指定管理服务器可以同时向其传输文件的最大允许客户端设备数。
   - 在**安装尝试最大数量**字段中，指定安装程序运行的最大允许次数。

     如果超过参数中指定的尝试次数，Kaspersky Next XDR Expert 将不再在该设备上启动安装程序。若要重新启动*远程安装应用程序*任务，请增加**安装尝试最大数量**参数的值然后启动任务。或者，您可以创建新的“*远程安装应用程序*”任务。

   - 如果您从一个卡巴斯基应用程序迁移到另一个应用程序，且当前应用程序受到密码保护，请在“**卸载当前卡巴斯基应用程序的密码**”字段中输入密码。请注意，在迁移期间，您当前的卡巴斯基应用程序将被卸载。

     > 仅当您在**卸载当前卡巴斯基应用程序的密码**设置组中选择了**使用网络代理**选项时，**强制下载安装包**字段才可用。

当使用远程安装应用程序任务安装 Kaspersky Endpoint Security for Windows for Windows 时，您只能使用卸载密码来执行 Kaspersky Security for Windows Server 到 Kaspersky Endpoint Security for Windows 的迁移场景。在安装其他组件时使用卸载密码可能会导致安装错误。

要成功完成迁移方案，请确保满足以下先决条件：

- 您正在使用适用于 Windows 的 Kaspersky Security Center Network Agent 14.2 或更高版本。
- 您正在运行 Windows 的设备上安装应用程序。

- 定义附加设置：
  - **如果已经安装应用程序则不再重新安装**

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

    如果禁用此选项，仍将安装应用程序。

    默认情况下已启用该选项。

  - **下载之前验证操作系统类型**

    在将文件传输到客户端设备之前，Open Single Management Platform 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Open Single Management Platform 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

    当您在未分配的设备上远程安装网络代理程序时，无论**下载之前验证操作系统类型**设置如何，Open Single Management Platform或分发点都会自动确定设备的操作系统类型。

  - **在 Active Directory 组策略中指定安装包的安装**

    如果启用此选项，安装包将使用 Active Directory 组策略进行安装。

    如果选择网络代理安装包，则该选项可用。

    默认情况下已禁用该选项。

  - **提示用户关闭运行中应用程序**

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

    如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

    默认情况下已禁用该选项。

- 选择要在哪些设备上安装应用程序：
  - **在所有设备上安装**

    应用程序将被安装到由其他管理服务器管理的设备。

    默认情况下已选中该选项。如果您在网络中只有一台管理服务器，您不必更改该设置。

- **仅安装到通过该管理服务器管理的设备**

  应用程序将仅被安装到由该管理服务器管理的设备。如果您在网络中有多个管理服务器且需要避免它们之间的冲突，请选择该选项。

- 指定设备是否在安装后必须被移动到管理组：

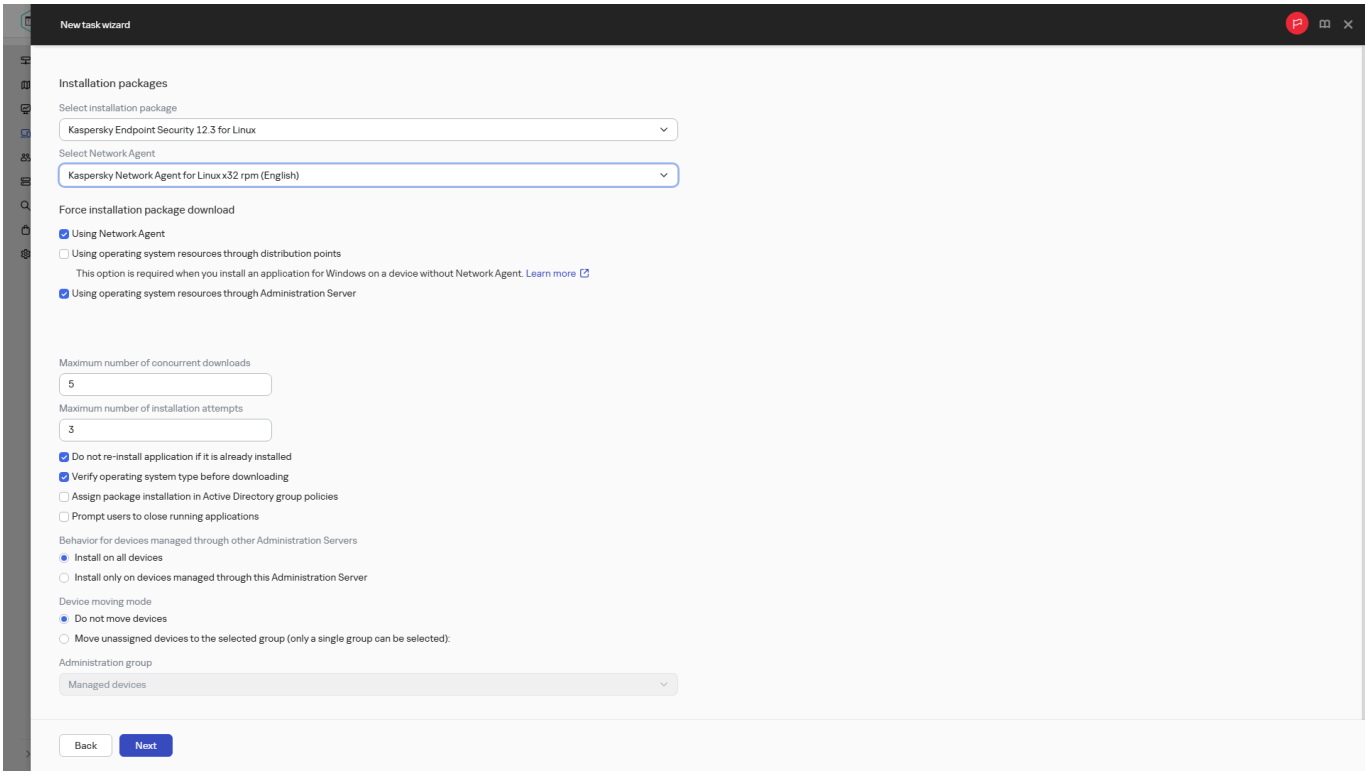
  - **不移动设备**

    设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

  - **移动未分配的设备到所选组 (仅可以选择单一组)**

    设备被移动到您选择的管理组。

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



指定任务设置

7. 在向导的这一步，指定在安装应用程序期间是否必须重新启动设备：

   - **不重启设备**

     如果选择该选项，安全应用程序安装后设备不被重启。

   - **重启设备**

     如果选择该选项，安全应用程序安装后设备将被重启。

8. 如有必要，在**选择账户以访问设备**步骤，添加将用于启动*远程安装应用程序*任务的账户：

   - **不需要账户(网络代理已安装)**

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

     如果网络代理未安装在客户端设备，该选项不可用。

- **需要账户(不使用网络代理)**

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

  - **本地或域账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地或域账户**，然后指定用户账户凭据。

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

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

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

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<用户电子邮箱>"
    ```

9. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。

   如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。

10. 在任务列表中，选择已创建的任务，然后单击**启动**。

    或者等待任务按照您在任务设置中指定的时间表启动。

远程安装任务完成后，选定的应用程序即安装在指定设备上。

在从属管理服务器上安装应用程序

如果您的管理服务器版本为 15.4 或更高版本，则您只能在版本为 15.4 或更高版本的从属管理服务器上安装应用程序。

要在从属管理服务器上安装应用程序：

1. 与控制相关从属管理服务器的管理服务器建立连接。
2. 确保每个所选的从属管理服务器上都有与要安装的应用程序对应的安装包。如果在任何从属服务器上都找不到安装包，请分发它。为此，请创建一个分发安装包**分发安装包的任务**。
3. 创建在从属管理服务器上远程安装应用程序的任务。选择**将应用程序远程安装到从属管理服务器**任务类型。

   “新任务向导”将创建一个任务，用于在特定从属管理服务器上远程安装向导中选择的应用程序。
4. 手动运行该任务，或者按照任务设置中指定的计划等待任务启动。

远程安装任务完成后，选定的应用程序即安装在从属管理服务器上。

指定 Unix 设备上的远程安装设置

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

要为远程安装任务指定 Unix 特定的设置：

1. 在主菜单中，转到“**任务**”。
2. 单击要为其指定 Unix 特定设置的远程安装任务的名称。

   任务属性窗口打开。
3. 转到“**应用程序设置**”→“**Unix 特定的设置**”。
4. 指定下列设置：

   - **为根账户设置密码(仅对通过 SSH 的部署)**

     如果在目标设备上必须指定密码才能使用 sudo 命令，则选择此选项，然后指定 root 账户的密码。Kaspersky Next XDR Expert 会将密码以加密形式传输到目标设备，对密码进行解密，然后使用指定密码以根账户的身份启动安装过程。

     > Kaspersky Next XDR Expert 不会使用该账户或指定的密码创建 SSH 连接。

   - **指定目标设备上具有执行权限的临时文件夹的路径(仅对通过 SSH 的部署)**

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

指定的任务设置即被保存。

启动和停止卡巴斯基应用程序

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

要创建启动或停止应用程序任务：

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在**应用程序**下拉列表中，选择要为其建立任务的应用程序。
4. 在**任务类型**列表中，选择**启动或停止应用程序**任务。

5. 在**任务名称**字段中，指定新任务的名称。

   任务名称不能超过 100 个字符并且不能包括任何特殊字符 ("*<>?\:|)。

6. 选择要分配任务的设备。

7. 在"**应用程序**"窗口中，执行以下操作：

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

8. 如果要修改默认任务设置，请启用"**创建完成时打开任务详情**"步骤的"**完成任务创建**"选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时更改默认设置。

9. 单击"**完成**"按钮。

   任务被创建并显示在任务列表。

10. 点击创建的任务的名称以打开任务属性窗口。

11. 在任务属性窗口中，根据需要指定常规任务设置，然后保存设置。

    任务被创建和配置。

要运行任务，请在任务列表中选择它，然后单击"**开始**"按钮。

替换第三方安全应用程序

通过 Kaspersky Next XDR Expert 安装卡巴斯基安全应用程序时，可能需要删除与待安装应用程序不兼容的第三方软件。Open Single Management Platform 提供几种卸载第三方应用程序的方法。

当配置应用程序远程安装时卸载不兼容应用程序

您可以在保护部署向导中配置安全应用程序远程安装时启用"**自动卸载不兼容的应用程序**"选项。启用该选项后，Open Single Management Platform 会在受管理设备上安装安全应用程序之前卸载不兼容的应用程序。

通过专用任务卸载不兼容的应用程序

要通过任务卸载不兼容的应用程序，请使用*远程卸载应用程序*任务。该任务应该在安全应用程序安装任务运行之前运行在设备。例如，在安装任务中，可以选择"**在完成其他任务时**"作为计划类型，其中其他任务为"*远程卸载应用程序*"。

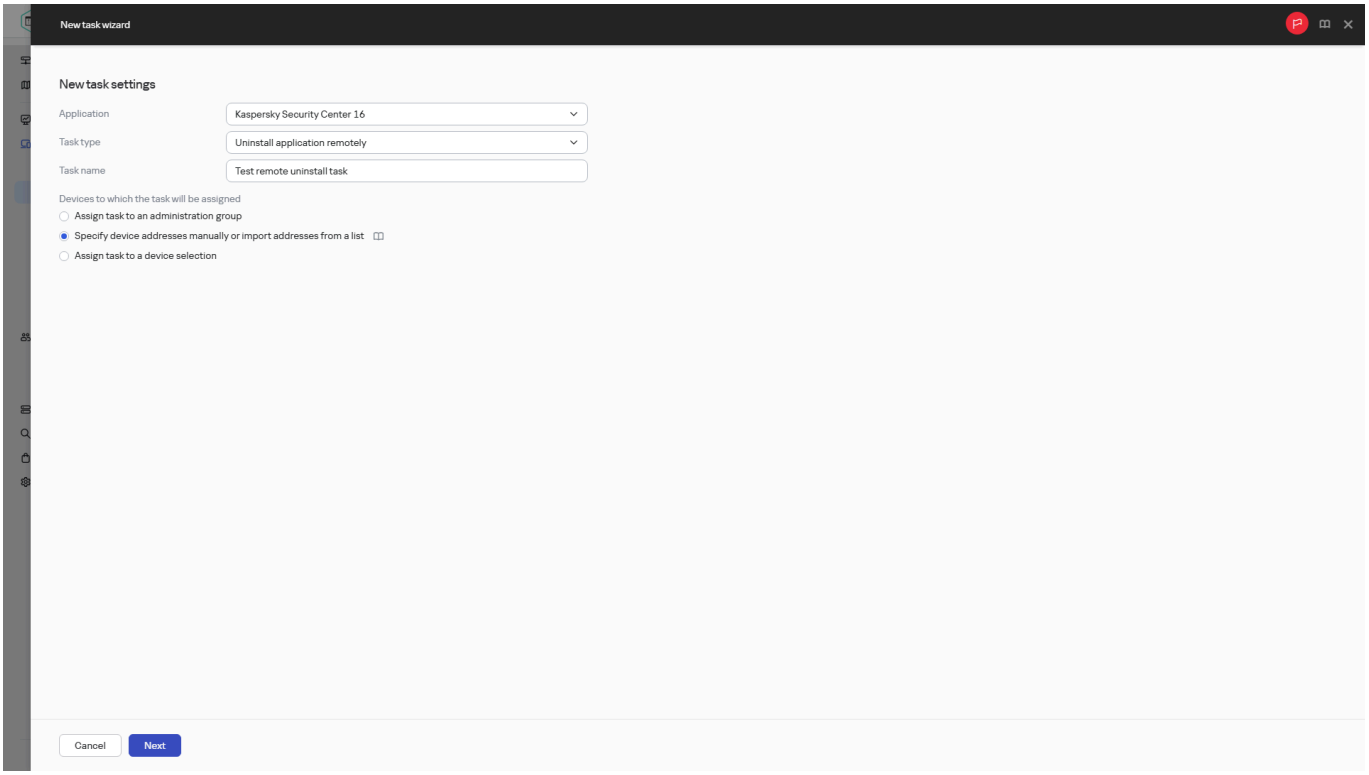
该卸载方法在安全应用程序无法正确卸载不兼容应用程序时是很有用的。

远程删除应用程序或软件更新

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

要从选定设备中远程删除应用程序或软件更新：

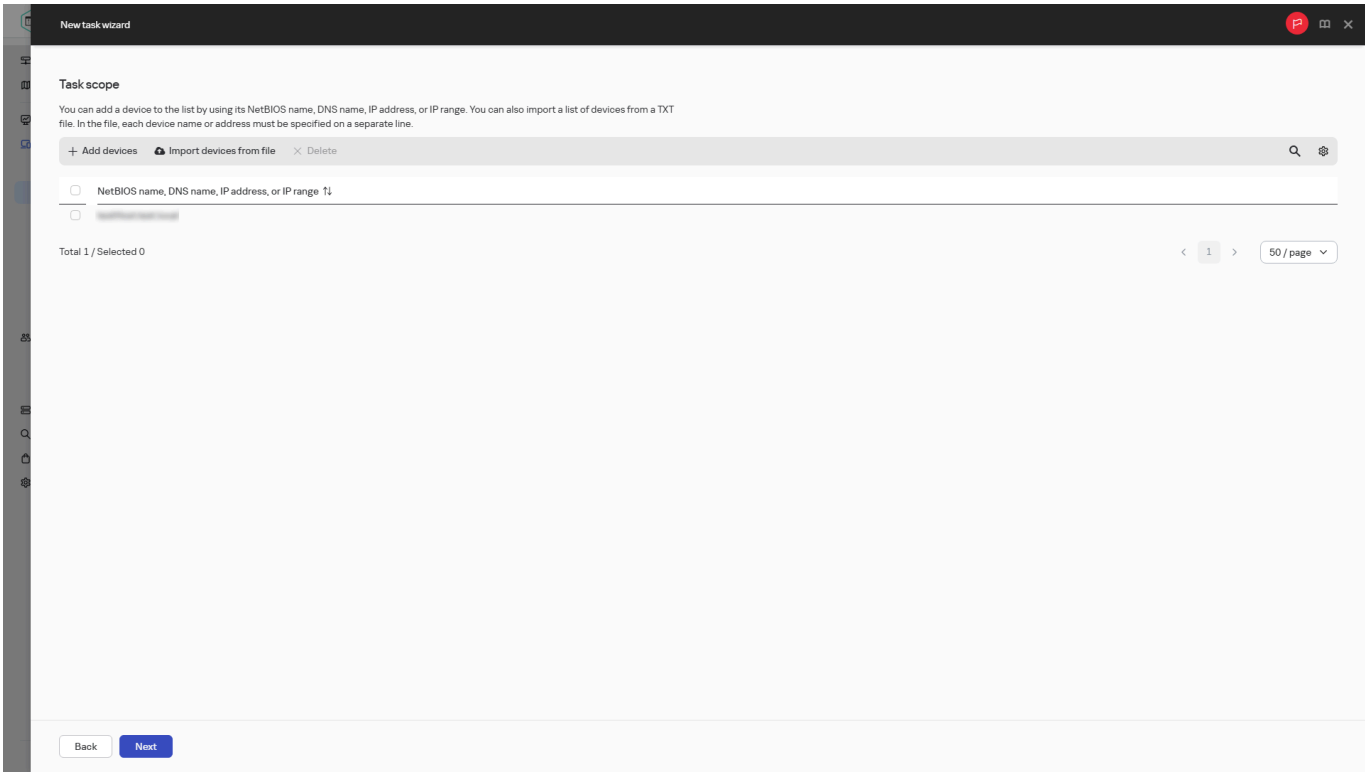
1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在“**应用程序**”下拉列表中，选择 Kaspersky Next XDR Expert。
4. 在**任务类型**列表中，选择**远程卸载应用程序**任务类型。
5. 在**任务名称**字段中，指定新任务的名称。
   任务名称不能超过 100 个字符并且不能包括任何特殊字符 ("*<>?\:|)。



创建远程卸载应用程序任务

6. 选择要分配任务的设备。

继续执行向导的下一步。



指定任务范围

7. 选择要删除的软件种类，然后选择要删除的特定应用程序、更新或补丁：

- **卸载受管理应用程序**

  显示卡巴斯基应用程序列表。选择要删除的应用程序。

  确认已为受管理应用程序禁用**使用卸载密码**策略设置。

- **卸载不兼容的应用程序**

  显示与卡巴斯基安全应用程序或 Open Single Management Platform 不兼容的应用程序列表。选中要删除的应用程序旁边的复选框。

- **从应用程序注册表中卸载应用程序**

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

  要从应用程序注册表中选择应用程序：

  a. 单击“**要卸载的应用程序**”字段，然后选择要删除的应用程序。

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

b. 指定卸载选项：

- **卸载模式**

  选择要如何删除应用程序：

  - **自动定义卸载命令**

    如果应用程序具有其供应商定义的卸载命令，则 Open Single Management Platform 将使用此命令。我们建议您选择此选项。

  - **指定卸载命令**

    如果要指定您自己的应用程序卸载命令，请选择此选项。

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

    在该字段中键入卸载命令，然后指定以下选项：

    仅当未自动检测到默认命令时使用此命令进行卸载

    Open Single Management Platform 会检查所选应用程序是否具有其供应商定义的卸载命令。如果找到，Open Single Management Platform 将使用该命令，而不使用在“**应用程序卸载命令**”字段中指定的命令。

    我们建议您启用此选项。

- **应用程序成功卸载后执行重启**

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

- **卸载指定的应用程序更新、补丁或第三方应用程序**

  显示更新、补丁和第三方应用程序的列表。选择要删除的项目。

  显示的列表是常规的应用程序和更新列表，并不对应于受管理设备上安装的应用程序和更新。选择项目之前，建议您确保在任务范围中定义的设备上安装了应用程序或更新。您可以通过属性窗口查看安装了应用程序或更新的设备列表。

  要查看设备列表：

  a. 单击应用程序或更新的名称。

  属性窗口打开。

  b. 打开“**设备**”区域。

  还可以在设备属性窗口中查看已安装的应用程序和更新列表。

8. 指定客户端设备将如何下载卸载实用程序：

- **使用网络代理**

  通过这些客户端设备上安装的网络代理将文件传送到客户端设备。

  如果禁用此选项，则使用 Linux 操作系统工具传送文件。

  如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。

- **通过管理服务器使用操作系统资源**

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

  使用管理服务器操作系统工具将文件传输到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。

- **通过分发点使用操作系统资源**

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

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

- **同时下载的最大数量**

  管理服务器可以同时向其传输文件的最大允许客户端设备数。该数字越大，应用程序的卸载速度越快，但管理服务器上的负载也越高。

- **尝试卸载的最大次数**

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

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

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

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

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

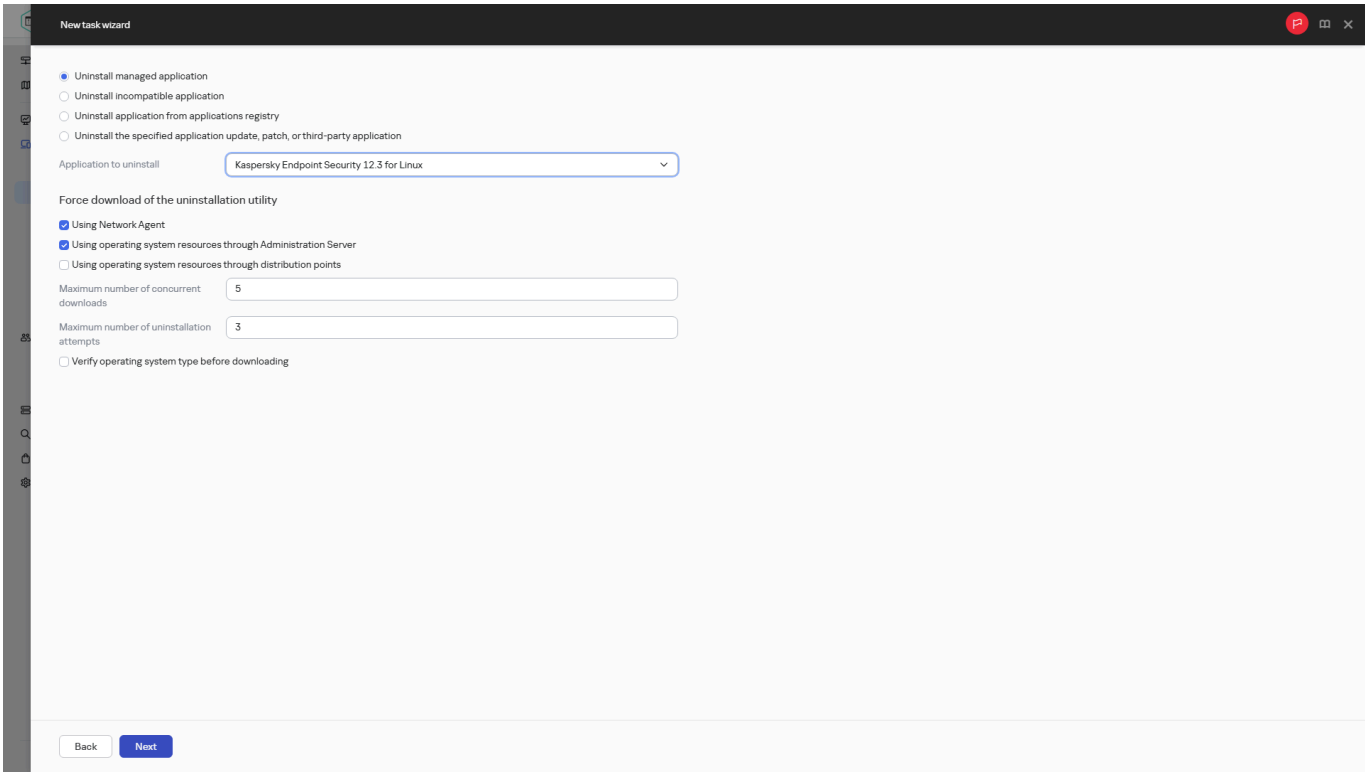
  如果已超过参数中指定的尝试次数，且设备已准备好应用程序卸载，您可以增加"**尝试卸载的最大次数**"参数的值并启动任务以卸载应用程序。或者，您可以创建新的"*远程卸载应用程序*"任务。

- **下载之前验证操作系统类型**

  在将文件传输到客户端设备之前，Open Single Management Platform 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Open Single Management Platform 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

  当您在未分配的设备上远程安装网络代理程序时，无论**下载之前验证操作系统类型**设置如何，Open Single Management Platform或分发点都会自动确定设备的操作系统类型。

继续执行向导的下一步。



指定任务设置

9. 指定操作系统重新启动设置：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**
  - **在该时间后重启(分钟)**

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

默认情况下已禁用该选项。

继续执行向导的下一步。

10. 如果必要，添加要用于启动远程卸载任务的账户：

- **不需要账户(网络代理已安装)**

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

  如果网络代理未安装在客户端设备，该选项不可用。

- **需要账户(不使用网络代理)**

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

  - **本地或域账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地或域账户**，然后指定用户账户凭据。

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

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

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

    例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<用户电子邮箱>"
    ```

11. 如果在向导的**完成任务创建**步骤中启用**创建完成时打开任务详情**选项，则可以编辑任务的默认设置。

    如果您不启用该选项，任务使用默认设置创建。您可以稍后修改默认设置。

12. 单击“**完成**”按钮。

    向导将创建任务。如果启用了“**创建完成时打开任务详情**”选项，任务属性窗口将自动打开。在此窗口中，您可以指定常规任务设置，并根据需要更改任务创建期间指定的设置。

    > 您还可以通过单击任务列表中已创建任务的名称来打开任务属性窗口。

    任务被创建、配置并显示在**任务**的任务列表中。

13. 要运行任务，请在任务列表中选择它，然后单击“**开始**”按钮。

    您还可以在任务属性窗口的**计划**选项卡上设置任务启动计划。

    有关计划启动设置的详细说明，请参阅常规任务设置。

当任务完成时，所选的应用程序被从所选设备中删除。

远程卸载问题

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

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

因此，按用户发放的应用程序必须在用户登录时才能卸载。

有关安装的应用程序的信息源

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

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

配置卡巴斯基应用程序

本部分包含有关手动配置策略和任务、用户角色、构建管理组结构和任务层级的信息。

方案：配置网络保护

创建和配置网络所需的策略和任务。

先决条件

在您开始之前，确保您已做了如下：

- 已安装管理服务器
- 已安装 OSMP 控制台
- 已完成 Open Single Management Platform 主安装场景

分阶段配置网络保护：

1. **设置和传播卡巴斯基应用程序策略和策略配置文件**

   要为安装在受管理设备上的卡巴斯基应用程序配置和传播设置，您可以使用两种不同的安全管理方法–以设备为中心或以用户为中心。这两种方法也可以被合并。

2. **配置任务以远程管理卡巴斯基应用程序**

   在**受管理设备**管理组中手动创建和配置以下策略和任务：

   - Kaspersky Endpoint Security 策略
   - 更新 Kaspersky Endpoint Security 的组任务
   - 网络代理策略

   使用说明：设置更新 Kaspersky Endpoint Security 的组任务。

   如果必要，创建附加任务以管理安装在客户端设备上的卡巴斯基应用程序。

3. **评估和限制数据库上的事件负载**

   受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   使用说明：设置最大事件数。

结果

当您完成该方案时，您将通过配置卡巴斯基应用程序、任务以及管理服务器接收的事件来保护您的网络：

- 卡巴斯基应用程序是根据策略和策略配置文件配置的。
- 应用程序通过一组任务进行管理。
- 设置可以存储在数据库中的最大事件数。

当网络保护配置完成时，您可以继续配置 Kaspersky 数据库和应用程序的常规更新。

关于以设备为中心和以用户为中心的安全管理方法

您可以从设备功能的立场和从用户角色的立场管理安全设置。第一种方法叫做*以设备为中心的安全管理*，第二种叫做*以用户为中心的安全管理*。要应用不同的应用程序设置到不同的设备，您可以使用两种方法的任意一种或两者组合。

以设备为中心的安全管理使您可以根据特定于设备的功能将不同的安全应用程序设置应用于受管理设备。例如，您可以将不同的设置应用于分配给不同管理组的设备。

以用户为中心的安全管理使您可以将不同的安全应用程序设置应用于不同的用户角色。您可以创建多个用户角色，为每个用户分配合适的用户角色，并为具有不同角色的用户所拥有的设备定义不同的应用程序设置。例如，您可能要应用不同的应用程序设置到会计和人力资源（HR）人员的设备。结果，当实现了以用户为中心的安全管理时，每个部门–财务部门和人事部门–具有自己的卡巴斯基应用程序设置配置。设置配置定义了哪些应用程序设置可以被用户更改以及哪些被强制设置并被管理员锁定。

通过使用以用户为中心的安全管理，您可以应用特别应用程序设置到单个用户。这可能用在员工在公司有独一角色或您要监控与个别人的设备相关的安全问题时。取决于该员工在公司的角色，您可以扩展或限制该员工更改应用程序设置的权限。例如，您可能要扩展在本地办公室管理客户端设备的系统管理员的权限。

您也可以组合以设备为中心的安全管理和以用户为中心的安全管理方法。例如，您可以为每个管理组配置特定的应用程序策略，然后为企业的一个或几个用户角色创建策略配置文件。此种情况下，策略和策略配置文件按照以下优先级进行应用：

1. 为以设备为中心的安全管理创建的策略被应用。
2. 它们根据策略配置文件属性被策略配置文件修改。
3. 策略被与用户角色关联的策略配置文件修改。

策略设置和传播：以设备为中心的方法

当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

先决条件

在开始之前，确保已安装管理服务器和 OSMP 控制台。您也可能要考虑以用户为中心的安全管理作为以设备为中心的方案的附加选项。了解更多两个管理方法的详情。

阶段

以设备为中心的卡巴斯基应用程序管理方案包含以下步骤：

1 配置应用程序策略

通过为每个应用程序创建策略来配置安装在受管理设备上的卡巴斯基应用程序设置。策略集将被传播到客户端设备。

如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

说明：创建一个策略

2. **创建策略配置文件（可选）**

   如果您想让单一管理组中的设备在不同策略设置下运行，为这些设备创建策略配置文件。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在受管理设备上活动。

   通过使用配置文件激活条件，例如，您可以将不同的策略配置文件应用到具有特定硬件配置或标记了特定标签的设备。使用标签筛选满足特别标准的设备。例如，您可以创建名为 *CentOS* 的标签，使用该标签标记所有运行 CentOS 操作系统的设备，然后指定该标签作为策略配置文件激活条件。结果，安装在所有 CentOS 设备上的卡巴斯基应用程序将被使用它们自己的策略配置文件管理。

   说明：

   - 创建策略配置文件
   - 创建策略配置文件激活规则

3. **传播策略和策略配置文件到受管理设备**

   默认情况下，管理服务器每 15 分钟自动与受管理设备同步一次。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。您可以避免自动同步并通过使用强制同步命令手动运行同步。一旦同步完成，策略和策略配置文件被传送和应用到安装的卡巴斯基应用程序。

   您可以检查策略和策略配置文件是否被传送到了设备。Open Single Management Platform 在设备属性中指定传送日期和时间。

   说明：强制同步

结果

当以设备为中心的方案完成时，卡巴斯基应用程序根据指定的设置被配置并通过策略层级传播。

配置的应用程序策略和策略配置文件将被自动应用到添加到管理组的新设备。

策略设置和传播：以用户为中心的方法

本部分介绍以用户为中心的集中配置安装到受管理设备上的卡巴斯基应用程序的方案。当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

先决条件

在开始之前，确保已成功安装管理服务器和 OSMP 控制台，并已完成主要部署方案。您也可能要考虑以设备为中心的安全管理作为以用于为中心的方案的附加选项。了解更多两个管理方法的详情。

过程

以用户为中心的卡巴斯基应用程序管理方案包含以下步骤：

1. **配置应用程序策略**

   通过为每个应用程序创建策略来配置安装在受管理设备上的卡巴斯基应用程序设置。策略集将被传播到客户端设备。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：创建一个策略

2. **指定设备所有者**

   分配受管理设备到对应用户。

   说明：指派用户作为设备所有者

3. **为您的企业定义用户角色**

   联想您企业的员工所做的不同工作。您必须根据他们的角色划分所有员工。例如，您可以按照部门、专业或职位划分他们。然后您将需要为每个组创建用户角色。记住，每个用户角色将拥有其自己的策略配置文件，包含该角色特有的应用程序设置。

4. **创建用户角色**

   为每个员工组创建和配置用户角色或使用预定义用户角色。用户角色将包含到应用程序功能的访问权限组。

   说明：创建一个用户角色

5. **定义每个用户角色范围**

   对于每个创建的用户角色，定义用户和/或安全组以及管理组。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

   说明：编辑用户角色范围

6. **创建策略配置文件**

   为您企业中的每个用户角色创建策略配置文件。策略配置文件决定了哪些设置将被根据用户角色应用到用户设备上的应用程序。

   说明：创建一个策略配置文件

7. **关联策略配置文件与用户角色**

   关联创建的策略配置文件与用户角色。此后：策略配置文件对具有特定角色的用户活动。策略配置文件中配置的设置将被应用到安装于用户设备上的卡巴斯基应用程序。

   说明：关联策略配置文件到角色

8. **传播策略和策略配置文件到受管理设备**

   默认情况下，Open Single Management Platform 每 15 分钟自动同步管理服务器与受管理设备。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。您可以避免自动同步并通过使用强制同步命令手动运行同步。一旦同步完成，策略和策略配置文件被传送和应用到安装的卡巴斯基应用程序。

   您可以检查策略和策略配置文件是否被传送到了设备。Open Single Management Platform 在设备属性中指定传送日期和时间。

说明：强制同步

结果

当以用户为中心的方案完成时，卡巴斯基应用程序根据指定的设置被配置并通过策略和策略配置文件层级传播。

对于新用户，您将必须创建新账户，分配一个创建的用户角色，并分配设备到用户。配置的应用程序策略和策略配置文件将被自动应用到该用户的新设备。

关于将网络代理切换到其他管理服务器

如果网络的以下设置发生更改，Kaspersky Next XDR Expert 可以将客户端设备上的网络代理切换到其他管理服务器：

- **DHCP 服务器地址条件** – 网络 Dynamic Host Configuration Protocol (DHCP) 服务器的 IP 地址已更改。

  DHCP 服务器地址条件设置当前不可用。

- **默认连接网关地址条件** – 主要网络网关的地址已更改。
- **DNS 域条件** – 子网的 DNS 后缀已更改。
- **DNS 服务器地址条件** – 网络 DNS 服务器的 IP 地址已更改。
- **WINS 服务器地址条件** – 网络 WINS 服务器的 IP 地址已更改。此设置仅适用于运行 Windows 的设备。
- **名称可解析性条件** – 客户端设备的 DNS 或 NetBIOS 名称已更改。
- **子网条件** – 更改子网地址和掩码。
- **Windows 域可访问性条件** – 更改客户端设备连接到的 Windows 域的状态。此设置仅适用于运行 Windows 的设备。
- **SSL 连接地址可访问性条件** – 客户端设备可以或无法（取决于您选择的选项）与指定服务器建立SSL连接（名称：端口）。您必须使用具有能够处理高负载和频繁的网络代理连接请求的软件的专用服务器。请勿指定管理服务器的端口。对于每个服务器，都可以额外指定一个 SSL 证书。在这种情况下，网络代理除了检查 SSL 连接的功能外，还会验证服务器证书。如果证书不匹配，连接将失败。

网络代理连接至管理服务器的初始设置在安装网络代理时定义。此后，如果创建了将网络代理切换至其他管理服务器的规则，网络代理将以下列方式响应网络设置的更改：

- 如果网络设置符合已创建的规则之一，网络代理将连接至该规则中指定的管理服务器。如果该规则中已经启用漫游切换策略，客户端设备上的应用程序将切换至漫游策略。
- 如果未应用任何规则，网络代理将回滚至安装过程中指定的管理服务器连接默认设置。客户端设备上安装的应用程序将回滚至活动策略。
- 如果无法访问管理服务器，网络代理将使用用户漫游策略。

> 仅当在网络代理策略设置中启用“**当管理服务器不可用时启用漫游模式**”选项时，网络代理才会切换到漫游策略。

网络代理连接至管理服务器的设置保存在连接配置文件中。在连接配置文件中，您可以创建将客户端设备切换至漫游策略的规则，并可对配置文件进行配置，使其仅可用于下载更新。

为漫游用户创建连接配置文件

若要为漫游用户创建网络代理连接至管理服务器的连接配置文件，请执行以下操作：

1. 如果要为一组受管理设备创建连接配置文件，请打开该组的网络代理策略。为此，请执行以下操作：
   a. 在主菜单中，转到“**资产管理**”→“**策略**“。
   b. 选择要为其创建连接配置文件的管理组：
      - 对于根组，您可以继续进行下一步。
      - 对于子组，单击页面顶部的“**显示层级**”按钮，然后在打开的窗口中单击所需子组的名称。

      所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。
   c. 为受管理设备组添加网络代理策略。如果您已经创建网络代理策略，请单击其名称以打开策略属性。
2. 如果要为特定的受管理设备创建连接配置文件，请执行以下操作：
   a. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
   b. 单击受管理设备的名称。
   c. 在打开的受管理设备属性窗口中，转到“**应用程序**”选项卡。
   d. 单击仅应用于选定的受管理设备的网络代理策略的名称。
3. 在打开的属性窗口中，转到“**应用程序设置**”→“**连接**”→“**连接配置文件**”。
4. 在“**管理服务器连接配置文件**”区域中，单击“**添加**”按钮。
   默认下，连接配置文件列表包含<离线模式>和<归属管理服务器>配置文件。您不能编辑或删除配置文件。

<离线模式>配置文件不指定任何服务器以连接。因此，网络代理，当切换到该配置文件时，当客户端设备上的应用程序工作在漫游策略下时不试图连接到任何管理服务器。如果设备与网络断开连接，可以使用 <离线模式> 配置文件。

<归属管理服务器> 配置文件用于指定在网络代理安装过程中选择的管理服务器的连接。当设备在外部网络中运行了一段时间后重新连接到管理服务器时，<归属管理服务器>配置文件被应用。

5. 在打开的“**配置配置文件**”窗口中，配置连接配置文件：

- **配置文件名称**

  在该输入字段中，您可以查看或更改连接配置文件名称。

- **管理服务器地址**

  客户端设备在配置文件激活期间必须连接的管理服务器地址。

- **端口号**

  用于连接的端口号。

- **SSL 端口**

  使用 SSL 协议时的连接端口号。

- **使用 SSL 连接**

  如果启用此选项，则使用 SSL 协议通过安全端口建立连接。

  默认情况下已启用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- 如果您要在连接到互联网时使用代理服务器，请选择“**使用代理服务器**”选项。如果选择此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

  - **地址**

    Kaspersky Next XDR Expert 连接到互联网时使用的代理服务器地址。

  - **端口号**

    用于建立 Kaspersky Next XDR Expert 代理连接的端口号。

  - **代理服务器身份验证**

    如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭据。

  - **用户名**

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

  - **密码**

    建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

    要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

- **连接网关地址**

  通过客户端设备连接管理服务器的网关地址。

- **当管理服务器不可用时启用漫游模式**

  选中此复选框，当管理服务器不可用时，允许客户端设备上安装的应用程序在任何连接尝试中使用处于漫游模式的设备的策略配置文件以及漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下，此复选框未被选中。

- **仅用来接收更新**

  如果启用此选项，则该配置文件将仅被客户端设备上安装的应用程序用来下载更新。对于其他操作，程序将使用在网络代理安装过程中定义的初始连接设置连接管理服务器。

  默认情况下已启用该选项。

- **与此配置文件中指定的管理服务器设置同步连接设置**

  如果启用此选项，网络代理将使用配置文件属性中指定的设置连接至管理服务器。

  如果禁用此选项，网络代理将使用安装期间已指定的原始设置连接至管理服务器。

  如果禁用“**仅用来接收更新**”选项，则此选项可用。

  默认情况下已禁用该选项。

程序将为漫游用户创建一个用于将网络代理连接至管理服务器的配置文件。当网络代理使用此配置文件连接到管理服务器后，客户端设备上安装的应用程序将使用处于漫游模式的设备的策略或漫游策略。

策略和策略配置文件

在 OSMP 控制台中，您可以为卡巴斯基应用程序创建策略。该部分描述了策略和策略配置文件，并提供创建和修改它们的说明。

关于策略和策略配置文件

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

策略的状态

状态	描述
活动	应用于设备的当前策略。对于每个管理组中的卡巴斯基应用程序，只能有一个策略处于活动状态。设备对卡巴斯基应用程序应用活动策略的设置值。
非活动	当前未应用于设备的策略。
漫游	如果选择该选项，策略将在设备离开企业网络时变为活动状态。

策略根据以下规则发挥作用：

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

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

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

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

策略配置文件根据以下规则发挥作用：

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

关于“锁定”和锁定的设置

每个策略设置都有一个锁定按钮图标 (🔒)。下表显示了锁定按钮的状态：

锁定按钮状态

状态	描述
Undefined	如果设置旁边显示打开的锁，并且禁用了切换按钮，则策略中未指定该设置。用户可以在受管理应用程序界面中更改这些设置。这些设置的类型称为“*未锁定*”。
Enforce	如果设置旁边显示关闭的锁，并且启用了切换按钮，则该设置应用于实施策略的设备。用户无法在受管理应用程序界面中修改这些设置的值。这些设置的类型称为“*已锁定*”。

我们强烈建议您关闭要在受管理设备上应用的策略设置的锁定。解锁的策略设置可以由卡巴斯基应用程序设置在受管理设备上重新分配。

您可以使用锁定按钮执行以下操作：

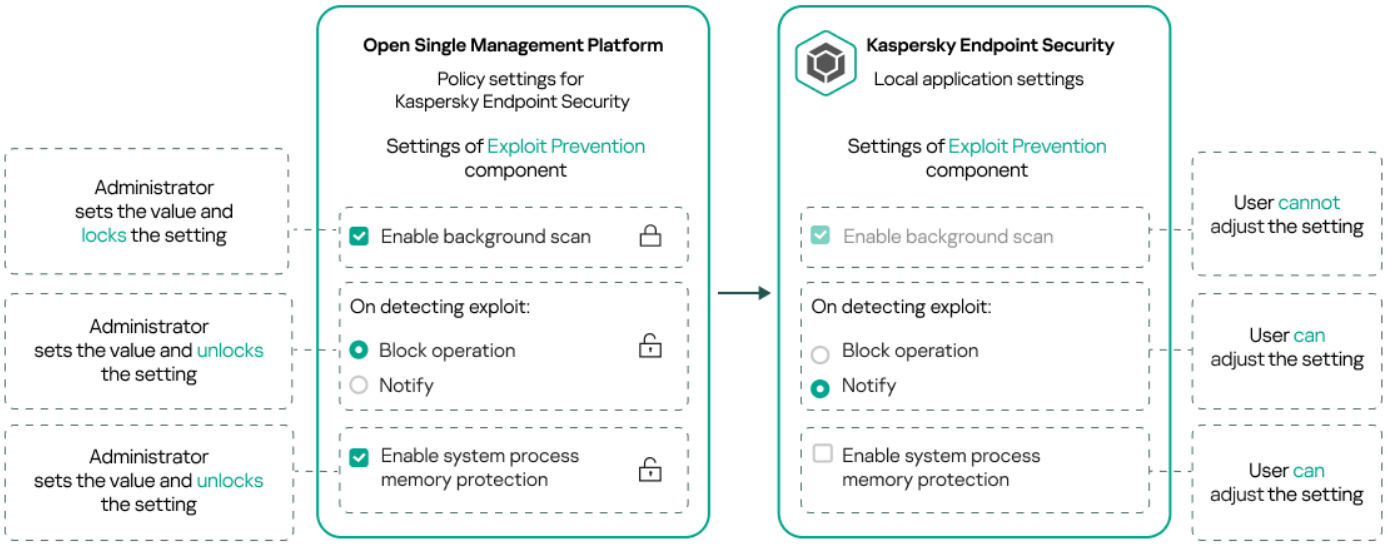
- 锁定管理子组策略的设置
- 在受管理设备上锁定本地卡巴斯基应用程序的设置

因此，已锁定设置用于在受管理设备上实施有效设置。

有效设置实施的过程包括以下操作：

- 受管理设备将应用卡巴斯基应用程序的设置值。
- 受管理设备应用策略的锁定设置值。

策略和受管理卡巴斯基应用程序包含相同的一组设置。配置策略设置时，受管理设备上的卡巴斯基应用程序设置会更改值。您无法调整受管理设备上的已锁定设置（请参见下图）：



锁定和卡巴斯基应用程序设置

策略继承和策略配置文件

本部分提供有关策略和策略配置文件的层级和继承的信息。

策略层级

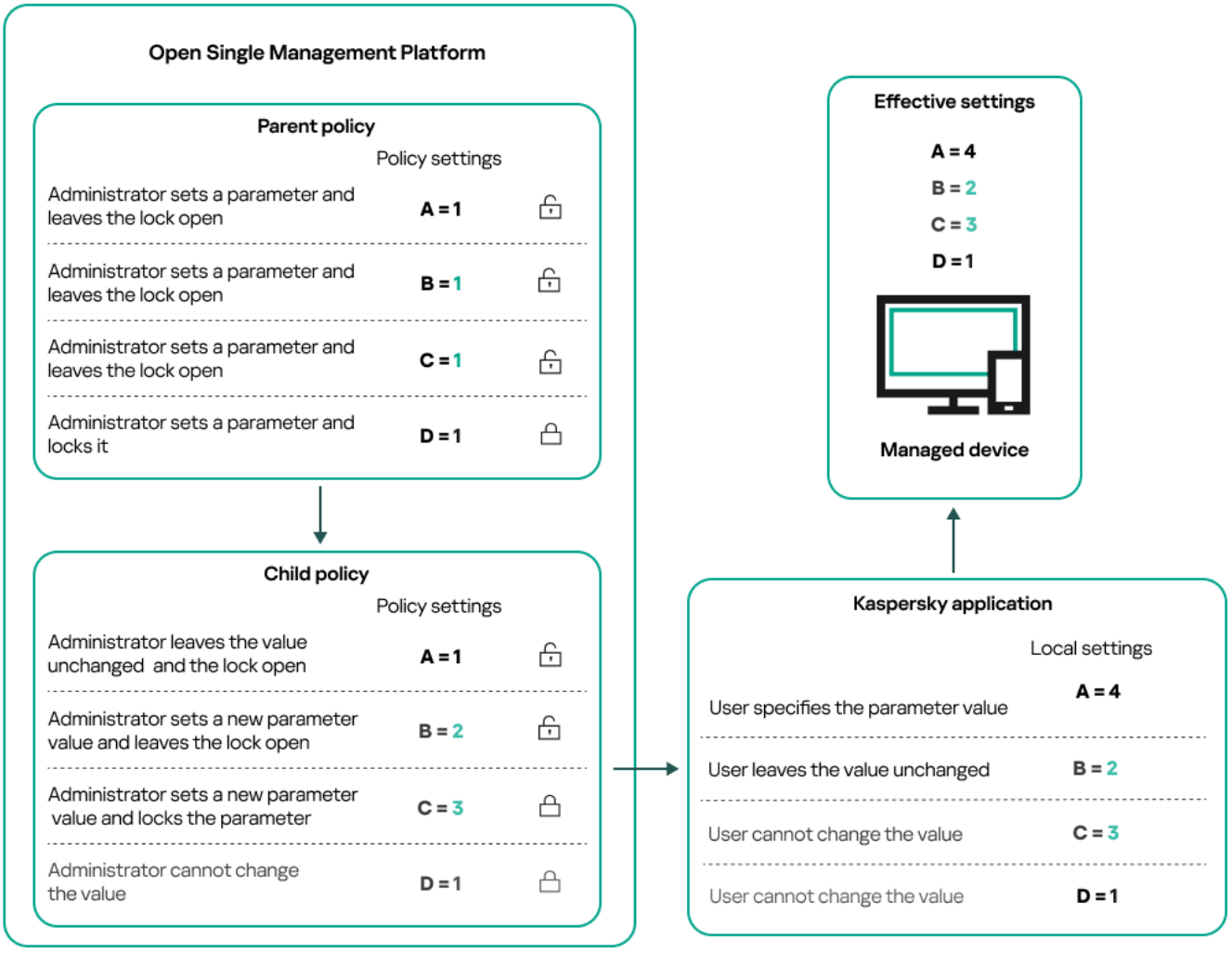
如果不同的设备需要不同的设置，则可以将设备组织到管理组中。

您可以为单个管理组指定策略。策略设置可以被*继承*。继承意味着子组中的策略设置值接收自更高级别的（父）管理组的策略。

因此，父组策略也叫*父策略*。子组策略也称为*子策略*。

默认情况下，管理服务器上存在至少一个受管理设备组。如果要创建自定义组，它们将创建为受管理设备组内的子组。

根据管理组的层级，同一应用程序的策略会互相作用。更高级别（父）管理组的策略中的锁定设置将重新分配子组的策略设置值（请参见下图）。

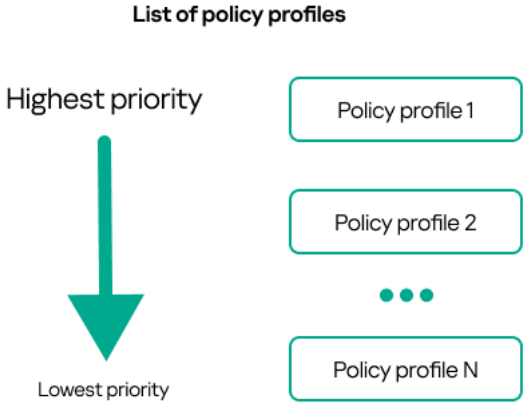


策略层级

策略层级中的策略配置文件

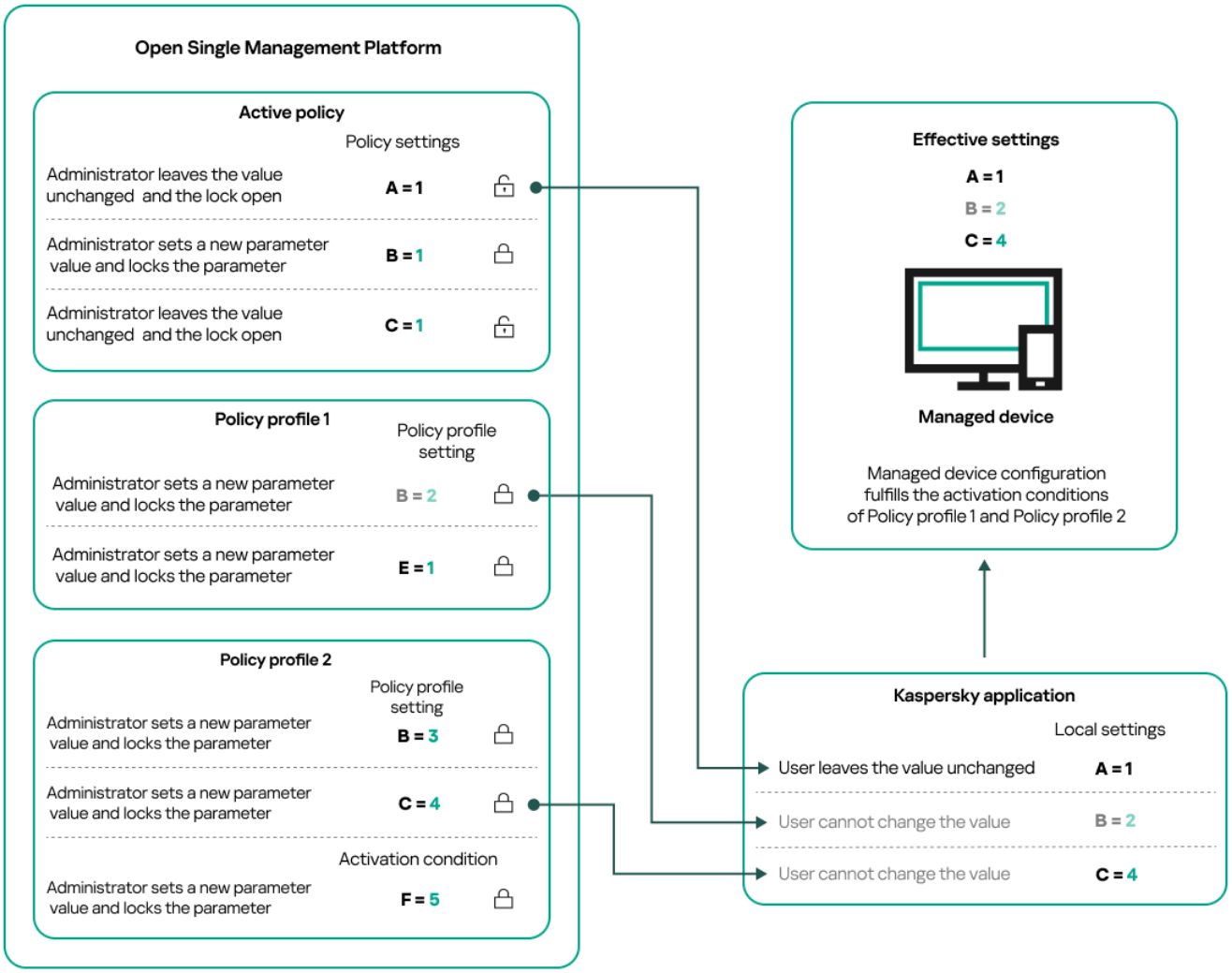
策略配置文件具有以下优先级分配条件：

- 配置文件在策略配置文件列表中的位置指示了其优先级。您可以更改策略配置文件优先级。列表中的最高位置指示最高优先级（请参见下图）。



策略配置文件的优先级定义

- 策略配置文件的激活条件互不依赖。可以同时激活多个策略配置文件。如果多个策略配置文件影响同一设置，则设备将采用策略配置文件中具有最高优先级的设置值（请参见下图）。

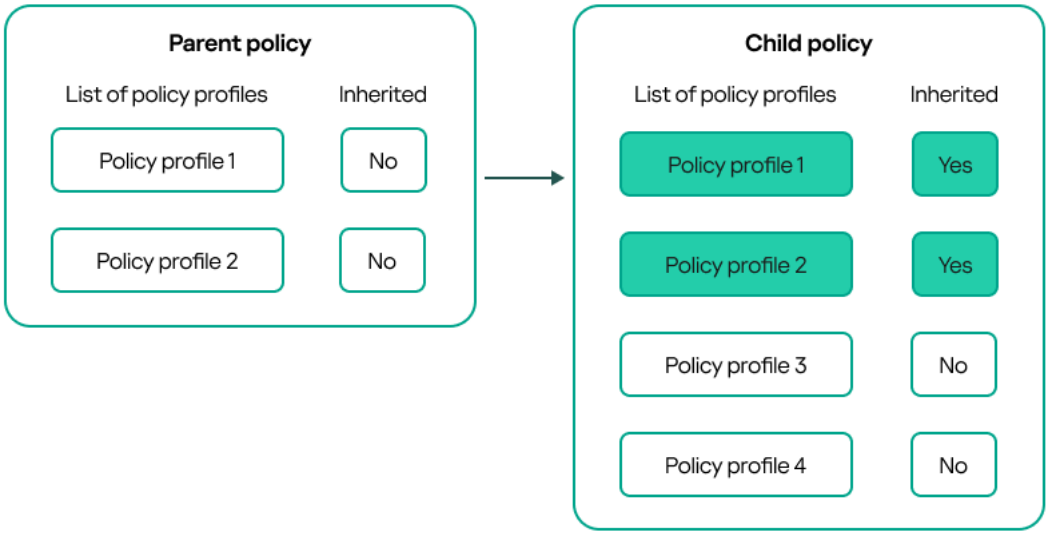


受管理设备配置满足多个策略配置文件的激活条件

继承层级中的策略配置文件

来自不同层次结构级别策略的策略配置文件符合以下条件：

- 较低级别的策略继承较高级别的策略的策略配置文件。从较高级别策略继承的策略配置文件比原始策略配置文件的级别具有更高的优先级。
- 您不能更改继承的策略配置文件的优先级（请参见下图）。

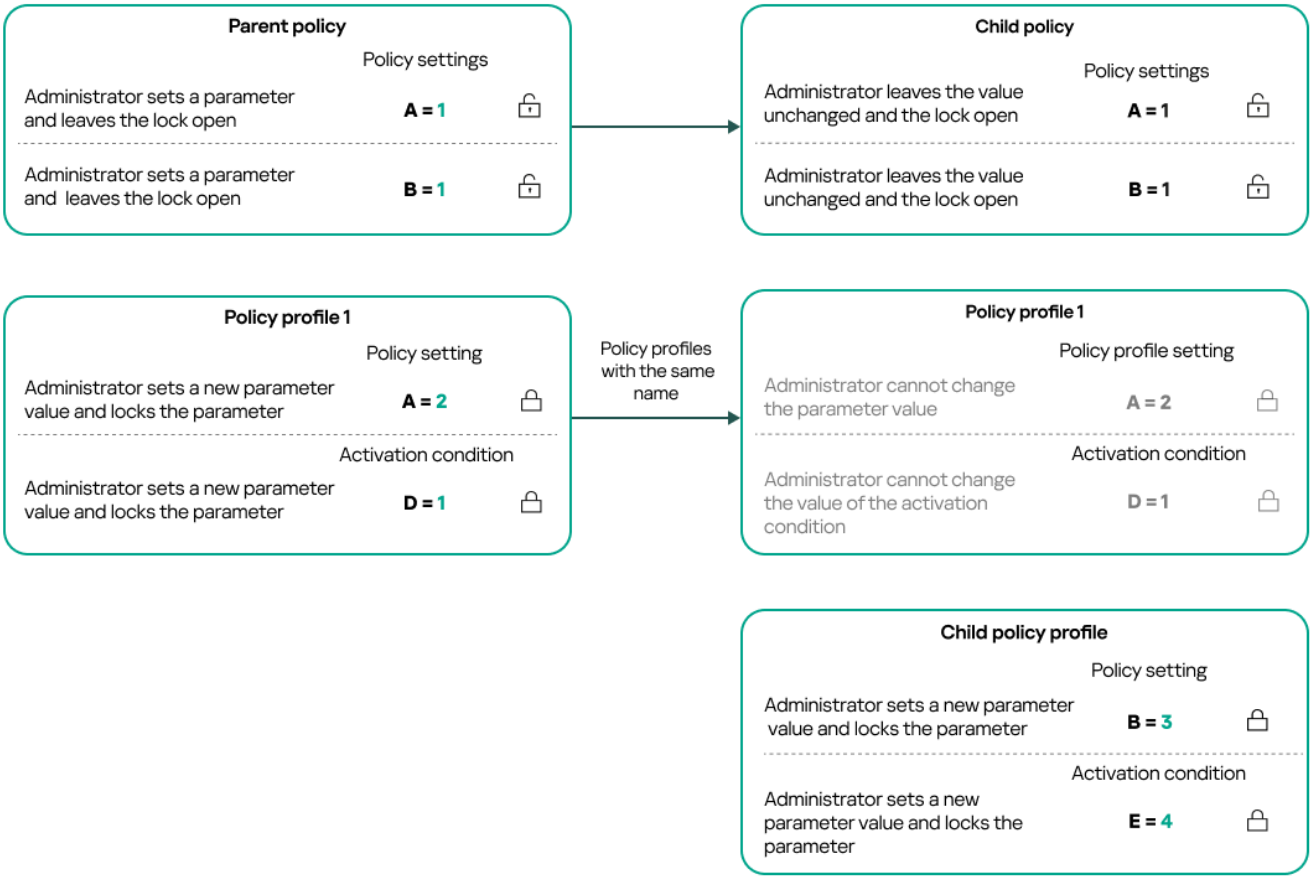


继承策略配置文件

具有相同名称的策略配置文件

如果在不同的层次结构级别中有两个名称相同的策略，则这两个策略按照以下规则起作用：

- 较高级别的策略配置文件的锁定设置和配置文件激活条件将更改较低级别的策略配置文件的设置和配置文件激活条件（请参见下图）。



子配置文件继承父策略配置文件的设置值

- 较高级别的策略配置文件的未锁定设置和配置文件激活条件不会更改较低级别的策略配置文件的设置和配置文件激活条件。

如何在受管理设备上实施设置

在受管理设备上有效设置的实现可以描述如下：

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

管理策略

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

查看策略列表

您可以查看为管理服务器或任何管理组创建的策略列表。

要查看策略列表，请执行以下操作：

1. 在主菜单中，转到“**资产管理**”→“**组层级**”。
2. 在管理组结构中，选择您要查看其策略列表的管理组。

策略列表以表格格式出现。如果没有策略，表格为空。您可以显示或隐藏表格的列，更改它们的顺序，仅查看包含指定值的行，或者使用查找。

创建新策略

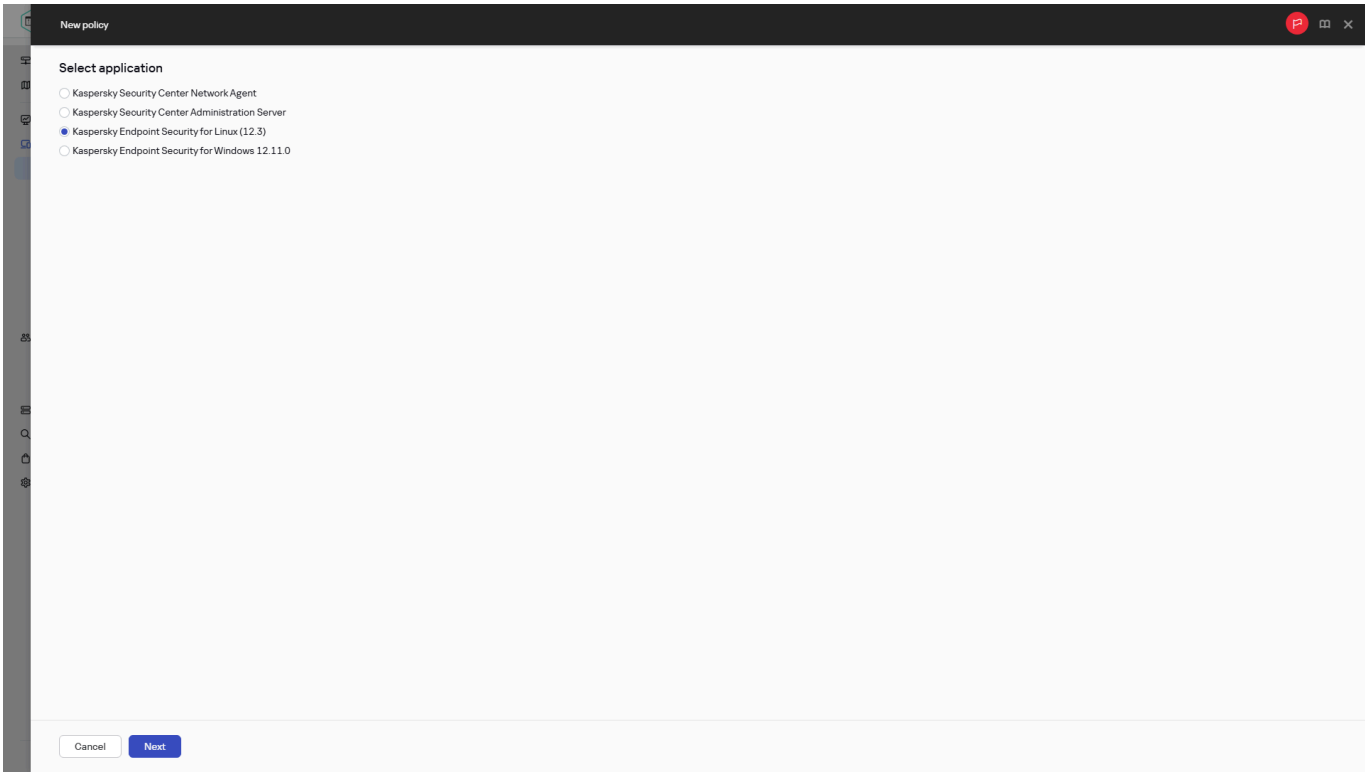
您可以创建策略；您也可以修改和删除现有策略。

要创建策略：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 选择要为其创建策略的管理组：
   - 对于根组。
     在这种情况下，您可以继续下一步。
   - 对于子组：
     a. 单击页面顶部的“**显示层级**”按钮。
     b. 按钮名称将更改为“**隐藏层级**”。
     c. 在打开的窗口中，单击带有所需子组的名称。

   所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。
3. 单击**添加**。

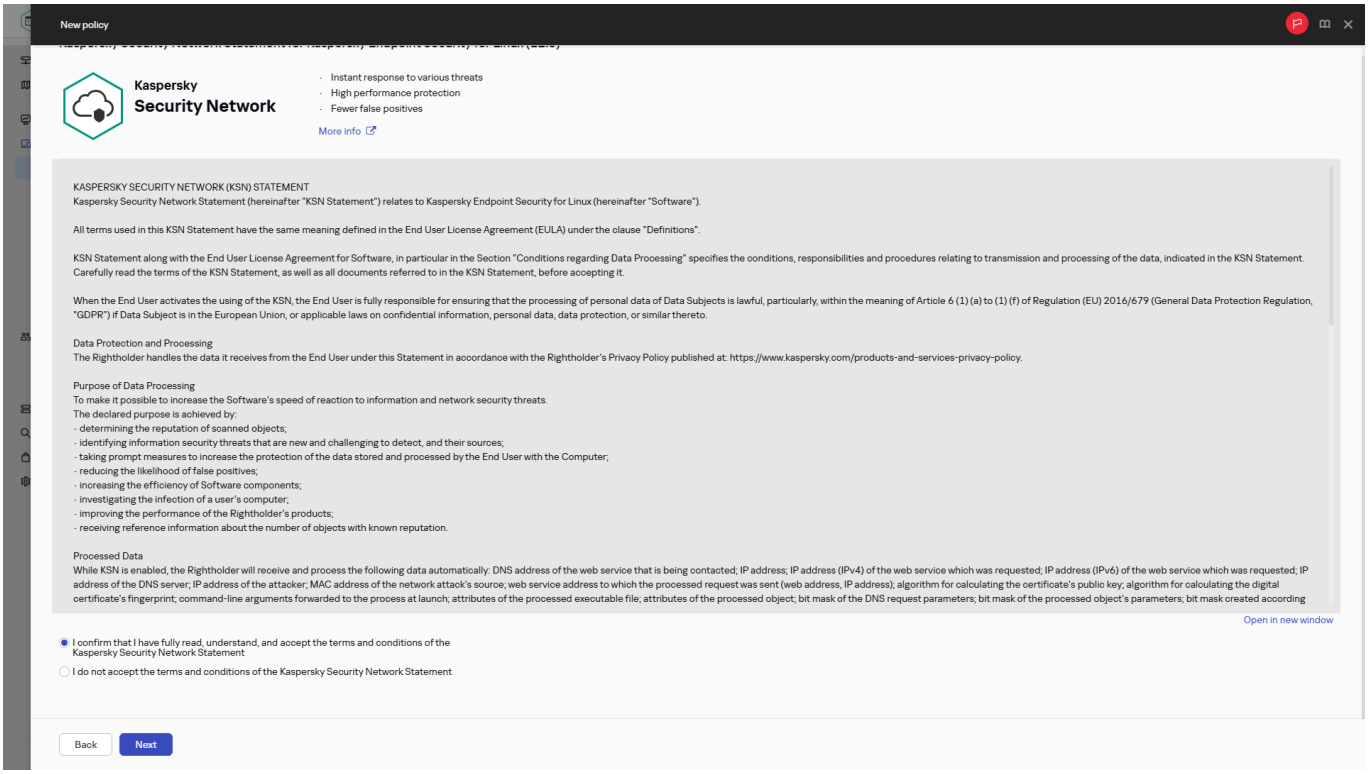
“**选择应用程序**”窗口将打开。



创建新策略

4. 选择您要为其创建策略的应用程序。

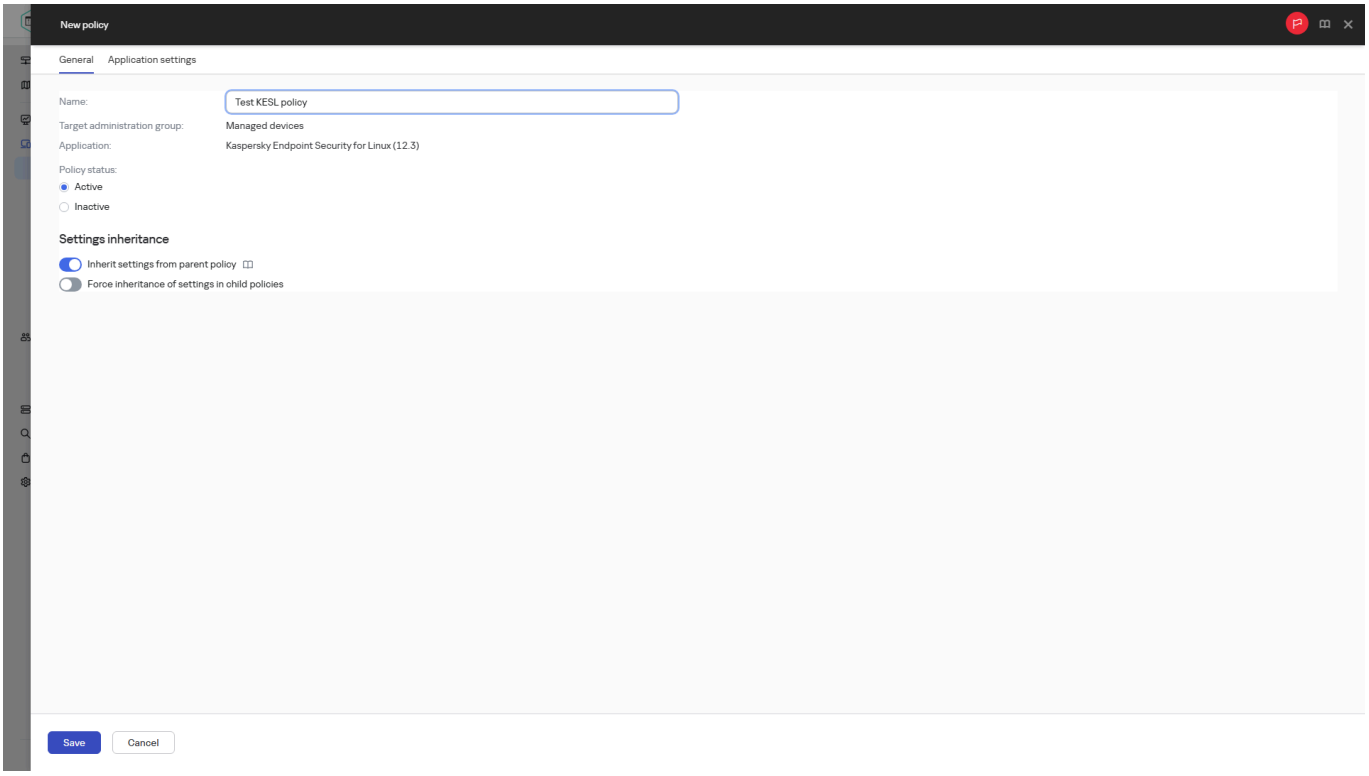
5. 如果您正在为其创建策略的卡巴斯基应用程序支持卡巴斯基安全网络，系统将提示您接受 KSN 声明。如果您想使用卡巴斯基安全网络，请接受 KSN 声明。



接受 KSN 声明

6. 单击“**下一步**”。

新策略设置窗口打开，在其中已选择“**常规**”选项卡。如果您需要，更改策略的默认名称、默认状态和默认继承设置。



新策略设置窗口

7. 选择“**应用程序设置**”选项卡。

   或者，您可以单击“**保存**”并退出。策略将出现在策略列表，且您可以稍后编辑其设置。

8. 在“**应用程序设置**”选项卡的左侧窗格中选择您需要的类别，并在右侧的结果窗格中编辑策略设置。您可以在每个类别中（区域）编辑策略设置。

   设置集合取决于您为其创建策略的应用程序。有关详细信息，请参阅以下内容：

   - 配置管理服务器
   - 网络代理策略设置
   - Kaspersky Endpoint Security for Linux 帮助
   - Kaspersky Endpoint Security for Windows 帮助

   有关其他安全应用程序设置的详细信息，请参阅相应应用程序的文档。

   当编辑设置时，您可以单击“**取消**”以取消上一次操作。

9. 单击“**保存**”保存策略。

   将显示包含以下消息的通知：**正在通过管理服务器的层次结构保存和分发策略。**

   如果策略通过验证，则会显示以下通知：**策略已保存。**

   如果策略验证失败，则会显示以下通知：**通过管理服务器的层次结构保存和分发策略 失败。请联系技术支持。**您可以查看并修改策略设置，然后重试。如果问题仍然存在，请联系技术支持。

该策略显示在策略列表中。创建策略后，如果启用了此选项，则会将策略变更事件导出到 SIEM 系统。

常规策略设置

常规

在“**常规**”选项卡中，可以修改策略状态并指定策略设置的继承：

- 在“**策略状态**”块，您可以选择策略的模式：
  - **活动**

    如果选择该选项，策略将变为活动状态。
    默认情况下已选定该选项。
  - **漫游**

    如果选择该选项，策略将在设备离开企业网络时变为活动状态。
  - **不活动**

    如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。
- 在“**设置继承**”设置组中，您可以配置策略继承：
  - **从父策略继承设置**

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。
  - **在子策略中强制继承设置**

    如果启用此选项，则在应用策略更改之后，将执行以下操作：
    - 策略设置的值将被传送到管理子组的策略，也就是子策略。
    - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

    如果启用此选项，则子策略设置被锁定。
    默认情况下已禁用该选项。

事件配置

“**事件配置**”区域允许您配置事件记录和事件通知。事件根据重要级别用下面的标签分布：

- **严重**

  “**严重**”区域不显示在网络代理策略属性中。
- **功能失败**
- **警告**
- **信息**

在每个区域，列表显示在管理服务器上事件类型和默认事件存储的期限（天）。单击事件类型允许您指定以下设置：

- **事件注册**
  您可以指定存储事件的天数和选择存储事件的位置：
  - **使用 Syslog 导出到 SIEM 系统**
  - **存储在设备的 OS 事件日志中**
  - **存储在管理服务器的 OS 事件日志中**
- **事件通知**
  您可以选择您是否想由以下方法之一被通知事件：
  - **通过邮件通知**
  - **通过 SMS 通知**
  - **通过运行可执行文件或脚本通知**
  - **通过 SNMP 通知**

  默认下，使用在管理服务器属性选项卡中指定的通知设置（例如收件人地址）。如果需要，可以在“**电子邮件**”、“**SMS**”和“**要运行的可执行文件**”选项卡中更改这些设置。

此外，当添加新的事件类型（例如，在应用程序的新版本中）时，**事件配置**选项卡会显示通知，并允许您通过单击**保存**或**保存并关闭**按钮来应用新设置。

修订历史

修订历史选项卡允许您查看政策版本列表，比较政策版本，并在必要时恢复对政策所做的更改。

修改策略

要修改策略：

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。
2. 单击您要修改的策略。
   策略设置窗口打开。
3. 指定“通用设置”和为其创建策略的应用程序的设置。有关详细信息，请参阅以下内容：
   - 配置管理服务器
   - 网络代理策略设置
   - Kaspersky Endpoint Security for Windows 文档
   有关其他安全应用程序设置的详细信息，请参阅该应用程序的文档。
4. 单击“**保存**”按钮。

将显示包含以下消息的通知：**正在通过管理服务器的层次结构保存和分发策略**。

如果策略通过验证，则会显示以下通知：**策略已保存**。

如果策略验证失败，则会显示以下通知：**通过管理服务器的层次结构保存和分发策略 失败。请联系技术支持**。您可以查看并修改策略设置，然后重试。如果问题仍然存在，请联系技术支持。

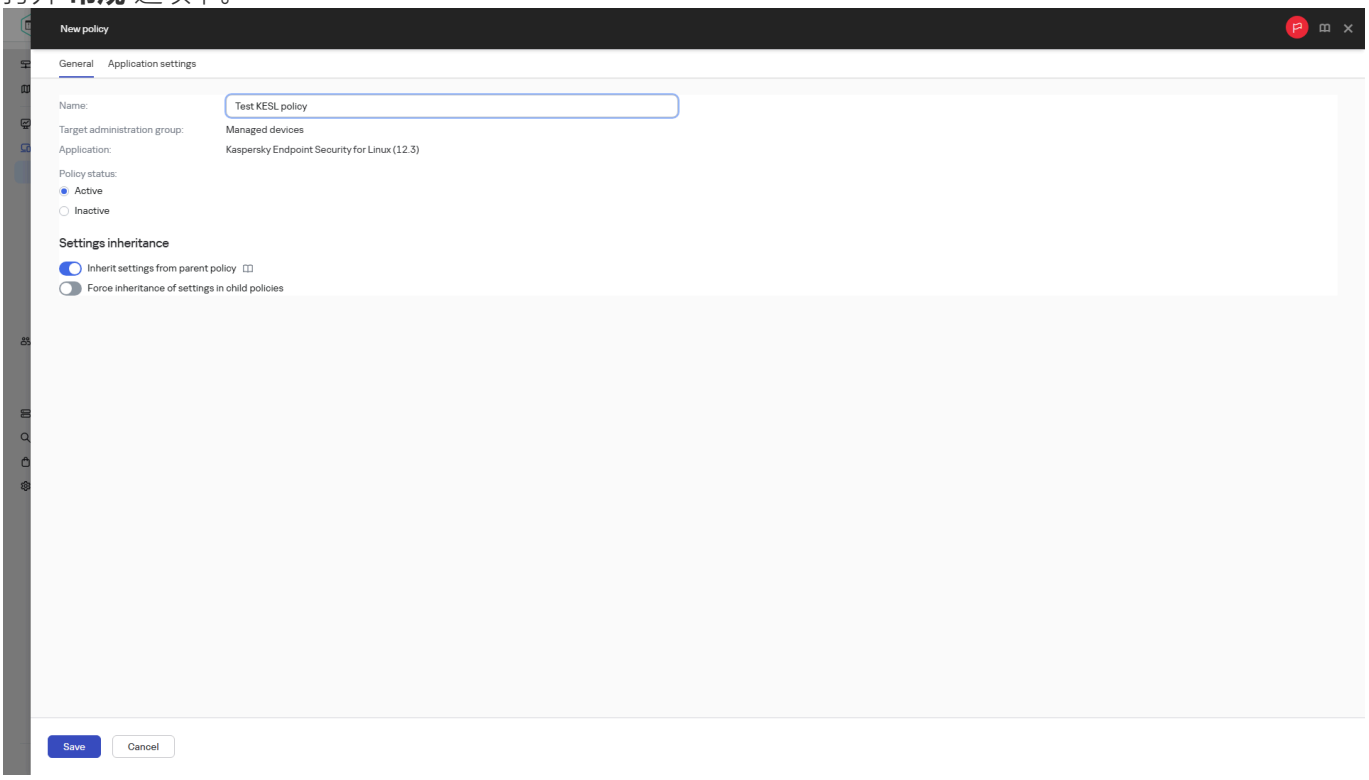
对策略所做的更改将保存在策略属性中，并将显示在“**修订历史**”区域中。策略修改后，如果已启用此选项，则会将策略更改事件导出到 SIEM 系统。

如有必要，您可以比较政策修订版本。此选项适用于管理服务器、网络代理、 Kaspersky Endpoint Security for Windows （从 14.0 Web 插件版本开始）以及 Kaspersky Endpoint Security for Mac（从 12.2.1 Patch A Web 插件版本开始）的策略。

启用和禁用策略继承选项

要在策略中启用或禁用继承选项：

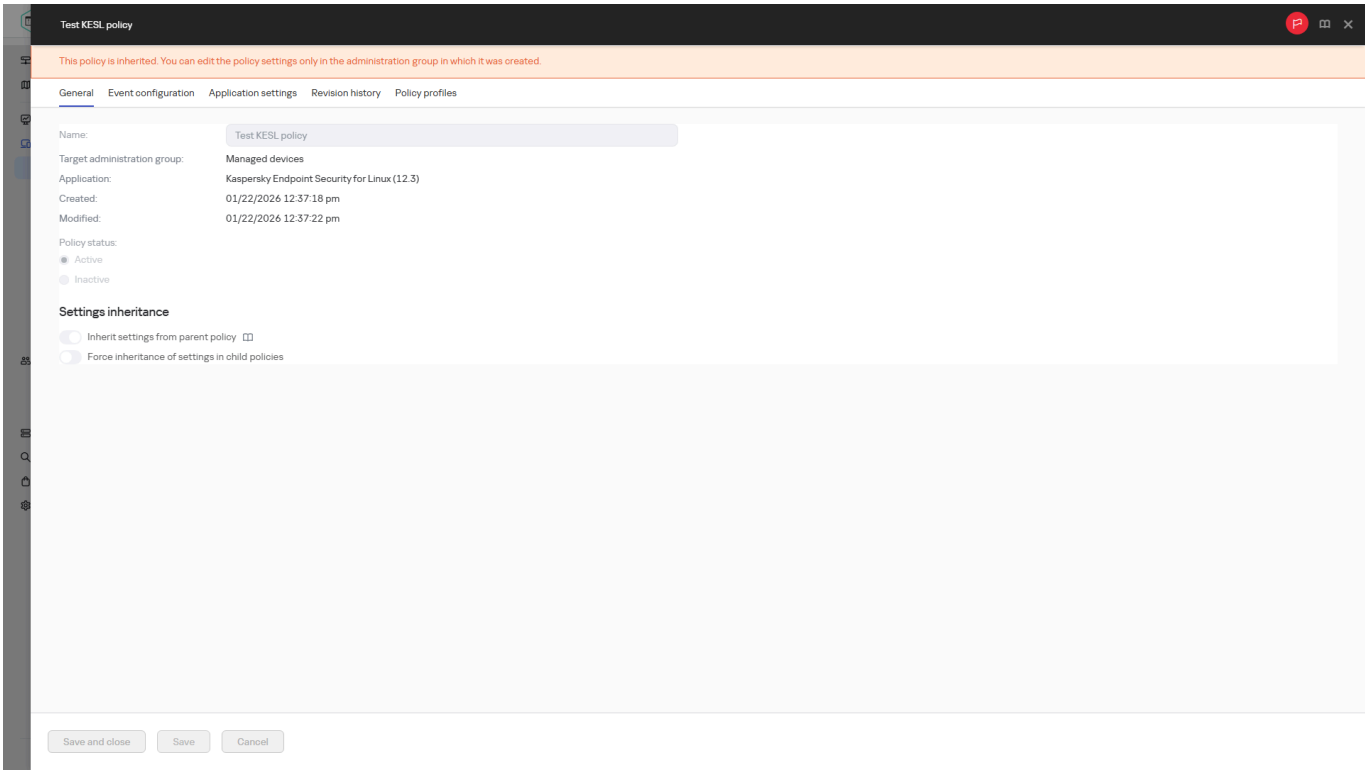
1. 打开所需策略。
2. 打开“**常规**”选项卡。



创建新策略

3. 启用或禁用策略继承：

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



锁定的策略设置

4. 单击“**保存**”按钮保存更改，或单击“**取消**”按钮拒绝更改。

默认情况下，为新策略启用“**从父策略继承设置**”选项。

如果一个策略具有配置文件，所有子策略都继承这些配置文件。

复制策略

您可以从一个管理组复制策略到另一个。

要复制策略到其他管理组：

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。
2. 选择您要复制的策略旁边的复选框。
3. 单击**复制**。

   在屏幕的右侧，管理组树被显示。

4. 在树中，选择目标组，即，要将策略复制到的组。

5. 单击屏幕底部的“**复制**”按钮。

6. 单击“**确定**”以确认操作。

策略将连带其所有配置文件被复制到目标组。目标组中每个复制的策略的状态将是“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如： （1） 。

移动策略

您可以从一个管理组移动策略到另一个。例如，您要删除一个组，但您要为其他组使用其策略。此种情况下，您最好在删除旧组之前将策略从旧组移动到新组。

将政策移动到另一个管理群组时，政策的版本历史记录将被清除。**修订历史**选项卡仅显示有关最新更改的信息。

要移动策略到其他管理组：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。

2. 选择您要移动的策略旁边的复选框。

3. 单击“**移动**”按钮。
   在屏幕的右侧，管理组树被显示。

4. 在树中，选择目标组，即，要将策略移动到的组。

5. 单击屏幕底部的“**移动**”按钮。

6. 单击“**确定**”以确认操作。

   如果策略不是从资源组继承的，它连带所有配置文件被移动到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

   如果策略是从资源组继承的，它保持在资源组。它连带所有其配置文件被复制到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如： （1） 。

导出策略

Open Single Management Platform 支持将策略、其设置和策略配置文件保存到 KLP 文件中。您可以使用此 KLP 文件将保存的策略导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要导出策略，请执行以下操作：

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。
2. 选中要导出的策略旁边的复选框。

   您不能同时导出多个策略。如果您选择了多个策略，**导出**按钮将被禁用。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定策略文件的名称和路径。单击“**保存**”按钮。

   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则策略文件会自动保存在“**下载**”文件夹。

导入策略

Open Single Management Platform 支持从 KLP 文件导入策略。KLP 文件包含导出的策略、其设置和策略配置文件。

要导入策略，请执行以下操作：

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的策略文件。
4. 在打开的窗口中，指定 KLP 策略文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个策略文件。

   策略处理启动。
5. 策略成功处理后，选择要向其应用策略的管理组。
6. 单击**完成**按钮以完成策略导入。

出现包含导入结果的通知。如果策略成功导入，可以单击“**详细信息**”链接以查看策略属性。

成功导入后，策略会显示在策略列表中。策略的设置和配置文件也将会导入。无论导出期间选择的策略处于什么状态，导入的策略均处于非活动状态。您可以在策略属性中更改策略状态。

> 如果新导入的策略与现有策略有相同的名称，则导入的策略在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

强制同步

尽管 Kaspersky Next XDR Expert 会自动同步受管理设备的状态、设置、任务和策略，但在某些情况下，管理员必须确切了解在特定时刻是否已对指定设备执行同步。

同步单个设备

要强制同步管理服务器和受管理设备：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
2. 单击要与管理服务器同步的设备名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 单击**强制同步**按钮。

应用程序将所选设备与管理服务器同步。

同步多个设备

要在管理服务器和多台受管理设备之间强制同步：

1. 打开管理组的设备列表或设备分类：
   - 运行设备分类以查看设备列表。
   - 在主菜单中，转到**资产管理** → **资产(设备)**，然后选择包含要同步的设备的管理组：
     - 对于根组，您可以继续进行下一步。
     - 对于子组，单击页面顶部的“**显示层级**”按钮，然后在打开的窗口中，单击子组的名称。
       所选组的路径显示在页面顶部。如果需要，您可以单击带有管理组名称的链接前往该组。默认情况下，路径中的最后一个链接不活动。您也可以单击“**隐藏层级**”按钮关闭层次结构窗口。
2. 选中要与管理服务器同步的设备旁边的复选框。
3. 在受管理设备列表上方，单击省略号按钮 (...)，然后单击“**强制同步**”按钮。
   应用程序将所选设备与管理服务器同步。
4. 在设备列表中，检查所选设备与管理服务器的上次连接时间是否已更改为当前时间。如果时间未更改，则单击“**刷新**”按钮更新页面内容。

所选设备即与管理服务器同步。

查看策略传送时间

在管理服务器上更改卡巴斯基应用程序策略后，管理员可以检查是否被更改的策略被传输到了特定受管理设备。策略可以在定期同步或者强制同步中传输。

要查看应用程序策略被传输到受管理设备的日期和时间：

1. 在主菜单中，转到“**资产管理**” → “**资产(设备)**”。
2. 单击要与管理服务器同步的设备名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 选择“**应用程序**”选项卡。

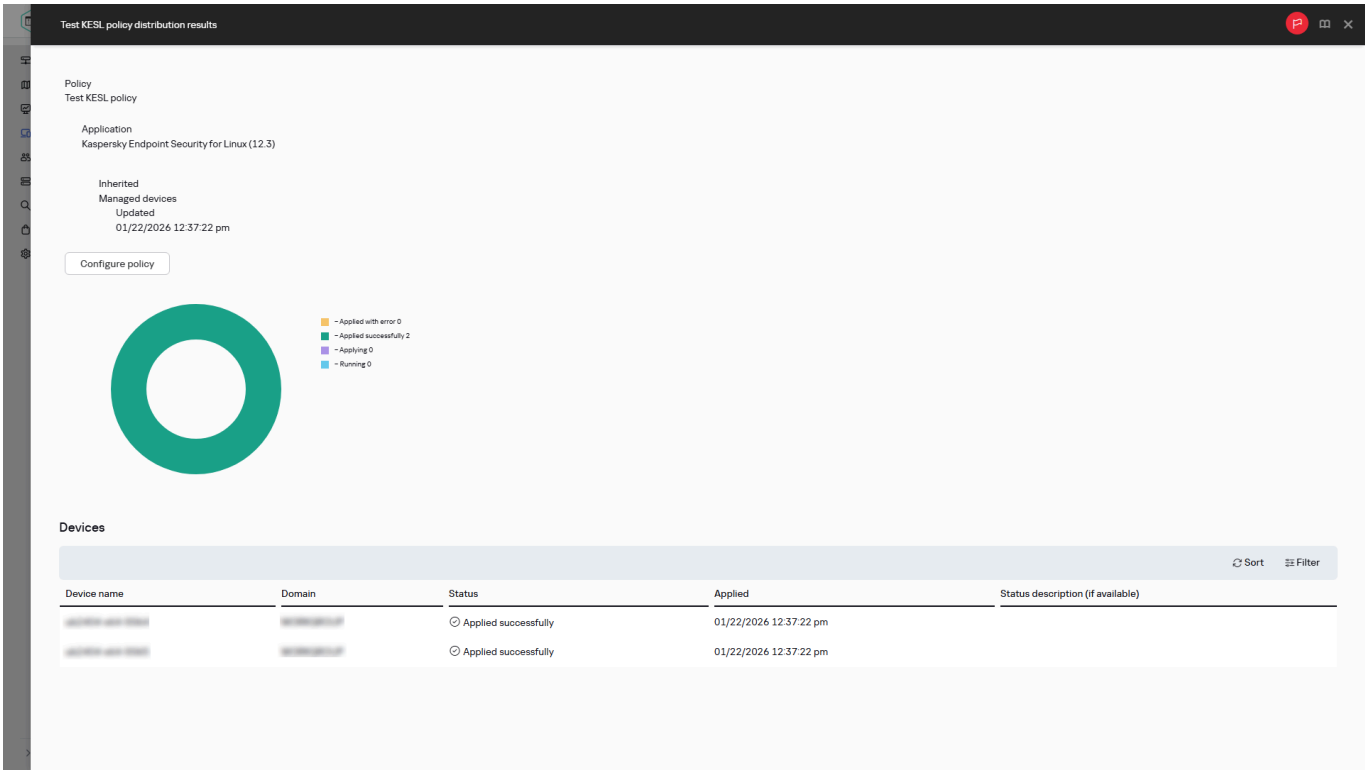
4. 选择您要查看策略同步日期的应用程序。
   应用程序策略窗口打开，在其中已选择“**常规**”区域并显示策略传送日期和时间。

查看策略分发状态图

在 Open Single Management Platform 中，您可以在策略分发状态图中查看每个设备上的策略应用状态。

要查看每个设备上的策略分发状态：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 选中要针对其查看设备上的分发状态的策略名称旁边的复选框。
3. 在出现的菜单中，选择“**分发**”链接。
   将打开“**<策略名称> 分发结果**”窗口。



策略分发状态图

4. 在打开的“**<策略名称> 分发结果**”窗口中，将显示策略的**状态描述**。

您可以更改列表中显示的策略分发结果数量。最大设备数量为 100,000。

要更改带有策略分发结果的列表中显示的设备数量：

1. 在主菜单中，转到“**设置**” → “**界面选项**”。
2. 在**策略分发结果中显示的设备数量限制**中，输入设备数量（最多 100,000）。
   默认情况下，该数字为 5000。
3. 单击“**保存**”按钮。
   设置已保存并应用。

在出现病毒爆发事件时自动激活策略

要使策略在出现病毒爆发事件时自动激活，请执行以下操作：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口打开，**常规**选项卡被选中。

2. 选择**病毒爆发**区域。

3. 在右侧窗格中，单击“**配置在病毒爆发事件发生时要激活的策略**”链接。

   “**策略激活**”窗口将开启。

4. 在与检测病毒爆发的组件有关的区域中–用于工作站和文件服务器的反病毒、用于邮件系统的反病毒或用于周边防护的反病毒–选择所需条目旁边的选项按钮，然后单击“**添加**”。

   将打开含有“**受管理设备**”管理组的窗口。

5. 单击“**受管理设备**”旁边的 V 形图标 (>)。

   管理组层级和它们的策略被显示。

6. 在管理组层级和它们的策略中，单击策略名称或检测到病毒爆发时激活的策略的名称。

   要在列表或组中选择所有策略，选择所需名称旁边的复选框。

7. 单击“**保存**”按钮。

   管理组层级和它们的策略的窗口被关闭。

所选的策略被添加到检测到病毒爆发时激活的策略列表。所选策略在病毒爆发中被激活，无论它们是活动的还是非活动的。

如果策略在病毒爆发事件中激活，您仅可以使用手动模式返回到先前策略。

删除策略

如果您不再需要一个策略，您可以删除它。您仅可以删除一个在指定管理组中继承的策略。如果一个策略是继承的，您仅可以在其被创建的上级组删除它。

要删除策略，请执行以下操作：

1. 在主菜单中，转到“ **资产管理**” → “**策略**”。

2. 选中您要删除的策略旁边的复选框，然后单击“**删除**”。

   如果选择继承的策略，“**删除**”按钮变为不可用（变暗）。

3. 单击“**确定**”以确认操作。

策略连带其所有配置文件被删除。策略删除后，如果启用此选项，策略更改事件将导出到 SIEM 系统。

管理策略配置文件

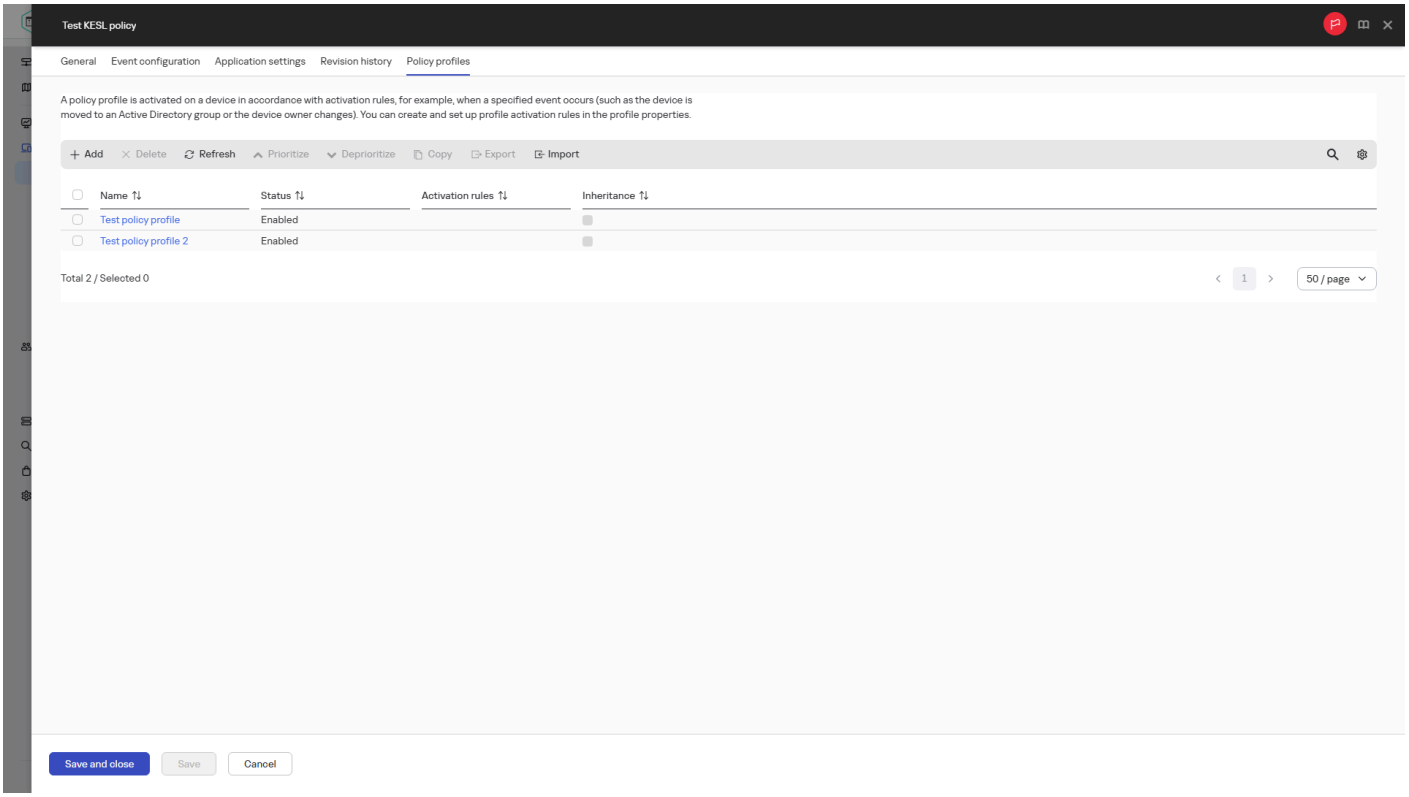
本节介绍管理策略配置文件并提供有关查看策略配置文件、更改策略配置文件优先级、创建策略配置文件、复制策略配置文件、创建策略配置文件激活规则、删除、导出和导入策略配置文件的信息。

查看策略配置文件

要查看策略配置文件：

1. 在主菜单中，转到“**资产管理**” → “**策略**”。
2. 单击您要查看其配置文件的策略名称。
   策略属性窗口打开，在其中已选择“**常规**”选项卡。
3. 打开“**策略配置文件**”选项卡。

策略配置文件列表以表格格式出现。如果策略没有配置文件，将显示空表。



策略配置文件列表

更改策略配置文件优先级

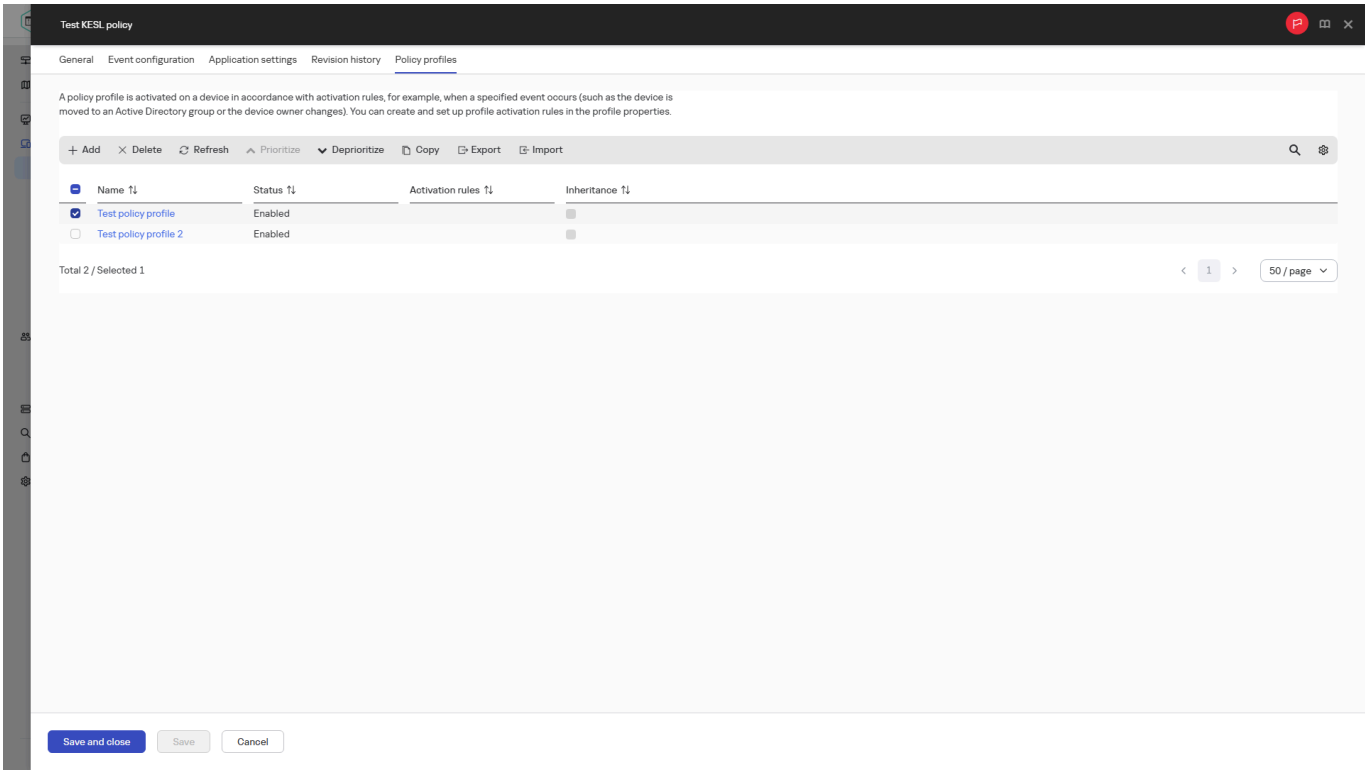
要更改策略配置文件优先级：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。

2. 在“**策略配置文件**”选项卡上，选中您要更改其优先级的策略配置文件旁边的复选框。

3. 通过单击“**提高优先级**”或“**降低优先级**”来设置策略配置文件在列表中的新位置。

   策略配置文件在列表中的位置越高，其优先级越高。



4. 单击“**保存**”按钮。

   所选策略配置文件的优先级被更改并应用。

创建策略配置文件

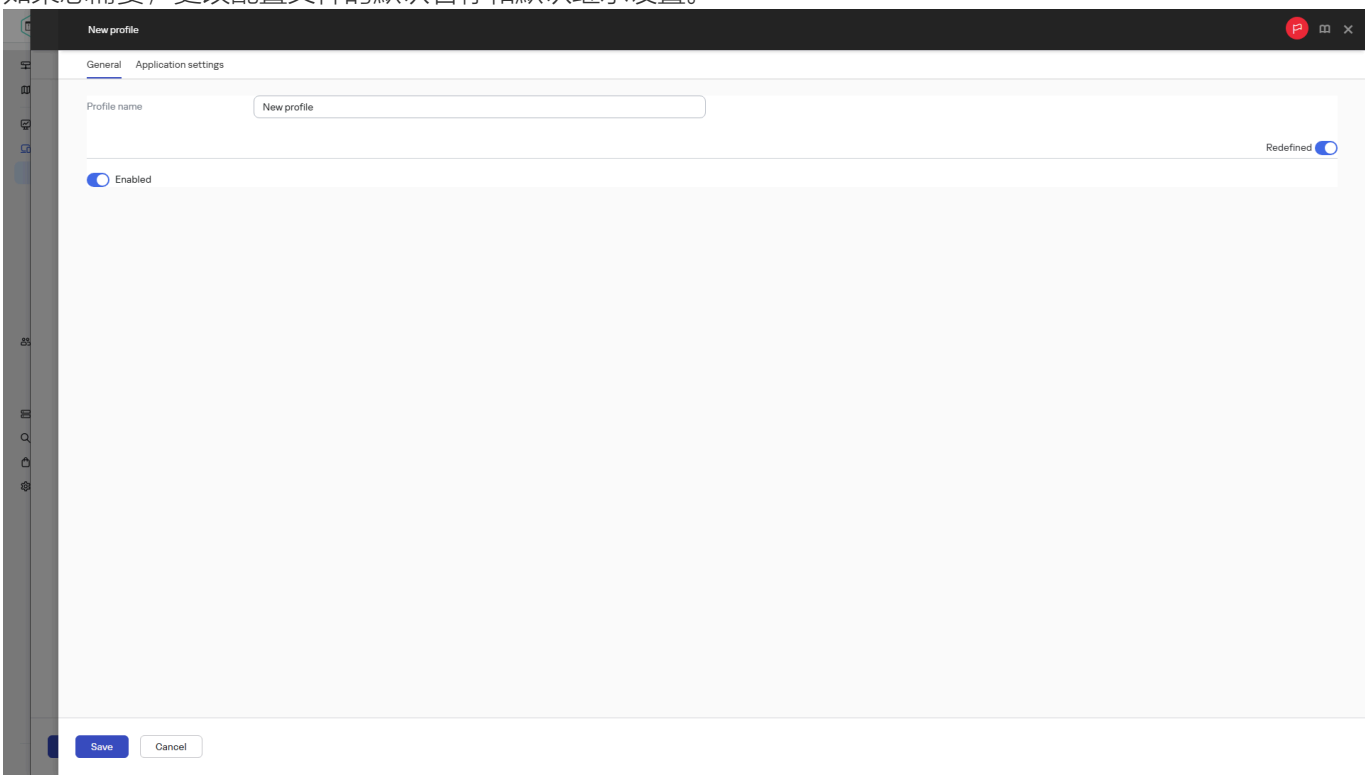
要创建策略配置文件：

1. 转到您要的策略的配置文件列表。

   将出现策略配置文件列表。如果策略没有配置文件，将显示空表。

2. 单击**添加**。

3. 如果您需要，更改配置文件的默认名称和默认继承设置。



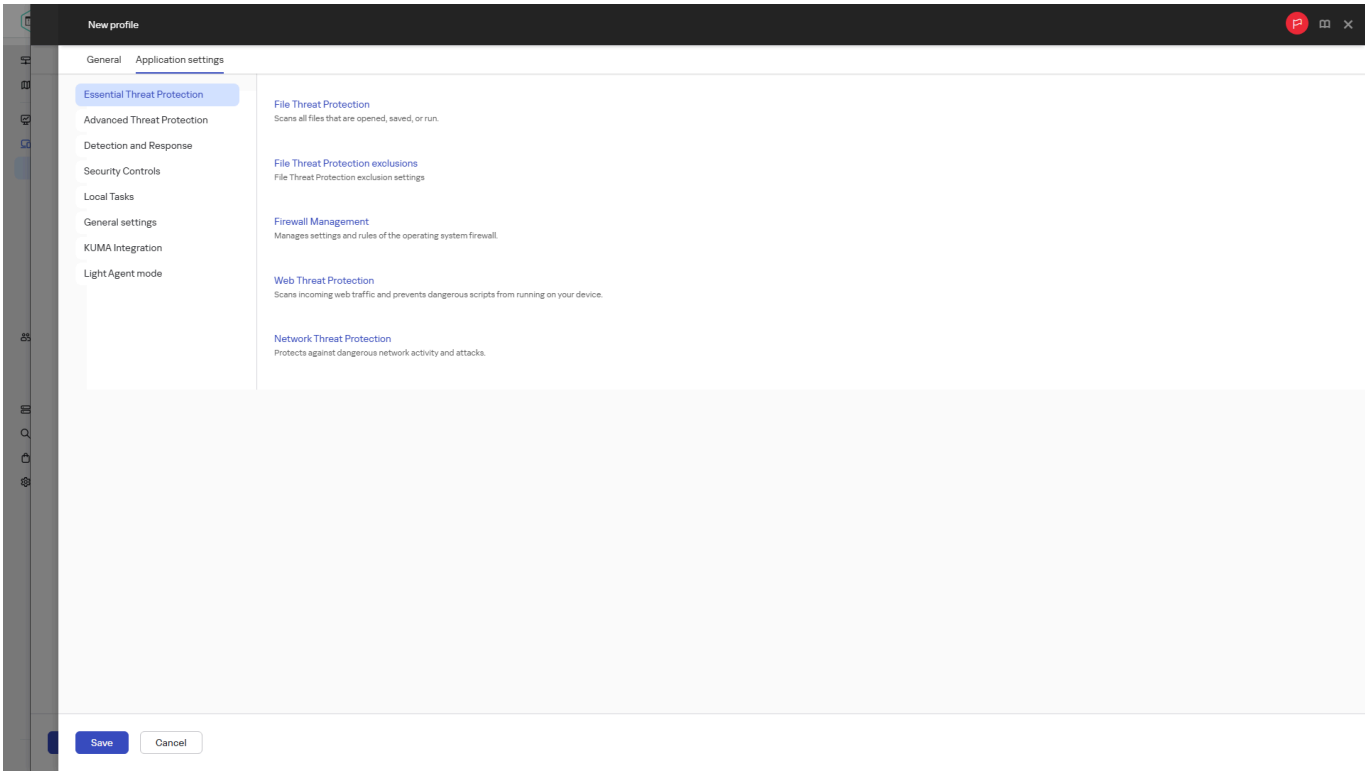
创建策略配置文件

4. 选择“**应用程序设置**”选项卡。

   或者，您可以单击“**保存**”并退出。您创建的配置文件会出现在策略配置文件列表中，您可以稍后编辑其设置。

5. 在“**应用程序设置**”选项卡的左侧窗格中选择您需要的类别，并在右侧的结果窗格中编辑策略设置。您可以在每个类别中（区域）编辑策略配置文件设置。

   当编辑设置时，您可以单击“**取消**”以取消上一次操作。



指定策略配置文件设置

6. 单击“**保存**”保存配置文件。

该配置文件显示在策略配置文件列表中。

复制策略配置文件

您可以复制策略配置文件到当前策略或其他策略，例如，如果您要对不同策略拥有相同配置文件。您也可以使用复制，如果您想拥有两个或更多仅在少数设置不同的配置文件。

要复制策略配置文件：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。如果策略没有配置文件，将显示空表。
2. 在“**策略配置文件**”选项卡上，选择要复制的策略配置文件。
3. 单击**复制**。
4. 在打开的窗口中，选择您要复制配置文件的策略。
   您可以复制策略配置文件到相同策略或您指定的策略。
5. 单击**复制**。

策略配置文件被复制到您选择的策略。新复制的配置文件具有最低优先级。如果您复制配置文件到相同策略，新复制的配置文件名称将附加 () 索引，例如：(1)、(2)。

之后，您可以更改策略配置文件的设置，包括其名称和优先级。在这种情况下，原始策略配置文件不会更改。

创建策略配置文件激活规则

要创建策略配置文件激活规则：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在“**策略配置文件**”选项卡上，单击需要为其创建激活规则的策略配置文件。
   如果策略配置文件列表为空，您可以创建策略配置文件。
3. 在“**激活规则**”选项卡上，单击“**添加**”按钮。
   策略配置文件激活规则窗口打开。
4. 指定规则名称。
5. 选择影响您当前创建的策略配置文件的激活的条件的复选框：

   - **策略配置文件激活常规规则**

     选择该复选框根据设备离线模式状态设置设备上的策略配置文件激活规则、连接管理服务器规则和分配给设备的标记。

对于该选项，在下一步指定：

- **设备状态**

  定义设备出现在网络的条件：

  - **在线**—设备在网络中，因此管理服务器可用。
  - **离线**—设备在外部网络，这意味着管理服务器不可用。
  - **N/A**—将不应用标准。

- **设备的网络位置**

  选择策略配置文件激活条件（规则是否被执行）并选择规则名称。

  规则定义设备网络位置以便连接到管理服务器，它的条件必须被满足(或不满足)以便激活策略配置文件。

  用于连接到管理服务器的设备网络位置描述可以在网络代理切换规则中被创建或配置。

- **特别设备所有者规则**

  对于该选项，在下一步指定：

  - **设备所有者**

    启用此选项可根据设备所有者在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 设备属于指定的拥有者（"="符号）。
    - 设备不属于指定的拥有者（“#”符号）。

      如果启用该选项，配置文件根据配置的标准在设备上激活。启用此选项时，您可以指定设备所有者。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **设备所有者在内部安全组中**

    启用此选项可配置并启用根据设备所有者是否属于 Kaspersky Next XDR Expert 内部安全组来激活设备上的配置文件的规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 设备所有者是指定安全组的成员（"="符号）。
    - 设备所有者不是指定安全组的成员（“#”符号）。

      如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定 Kaspersky Next XDR Expert 的安全组。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **硬件说明书规则**

  选择该复选框根据内存和逻辑处理器数量设置设备上的策略配置文件激活规则。

对于该选项，在下一步指定：

- **内存大小(MB)**

  启用此选项可通过设备上可用 RAM 容量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 该设备内存大小小于指定值("<" 符号)。
  - 该设备内存大小大于指定值(">" 符号)。

  如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的 RAM 卷。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **逻辑处理器数量**

  启用此选项可通过设备上逻辑处理器数量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 设备上逻辑处理器数量少于或等于指定值 （"<" 符号）。
  - 设备上逻辑处理器数量大于或等于指定值 （">" 符号）。

  如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的逻辑处理器数量。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **角色分配规则**

  对于该选项，在下一步指定：

  - **由设备所有者特定角色激活策略配置文件**

    选择该选项以在设备上根据所有者角色配置和启用配置文件激活规则。从现有角色列表手动添加角色。

    如果启用该选项，配置文件根据配置的标准在设备上激活。

- **标签使用规则**

  选择该复选框根据分配到设备的标签设置设备上的策略配置文件激活规则。您可以激活策略配置文件到有或没有所选标签的设备。

  对于该选项，在下一步指定：

  - **标签列表**

    在标签列表中，通过选中与相应标签对应的选框，可以指定策略配置文件中的设备包含规则。

    您可以通过列表上方的字段添加新标签到列表，并单击“**添加**”按钮。

    策略配置文件包含具有选定标签的设备。如果清除选框，则将不应用该标准。默认情况下已清除这些选框。

  - **应用到没有指定标签的设备**

    如果必须转换标签分类，则启用此选项。

    如果启用此选项，策略配置文件将包含未带有所选标签的描述的设备。如果禁用此选项，则不应用该标准。

    默认情况下已禁用该选项。

- **Active Directory 使用规则**

  选择该复选框根据设备在活动目录组织单元中的出现或者设备在活动目录安全组中的成员关系设置设备上的策略配置文件激活规则。

  对于该选项，在下一步指定：

  - **在 Active Directory 安全组中的设备所有者成员关系**

    如果启用此选项，其所有者是指定安全组成员的设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **在 Active Directory 安全组中的设备成员关系**

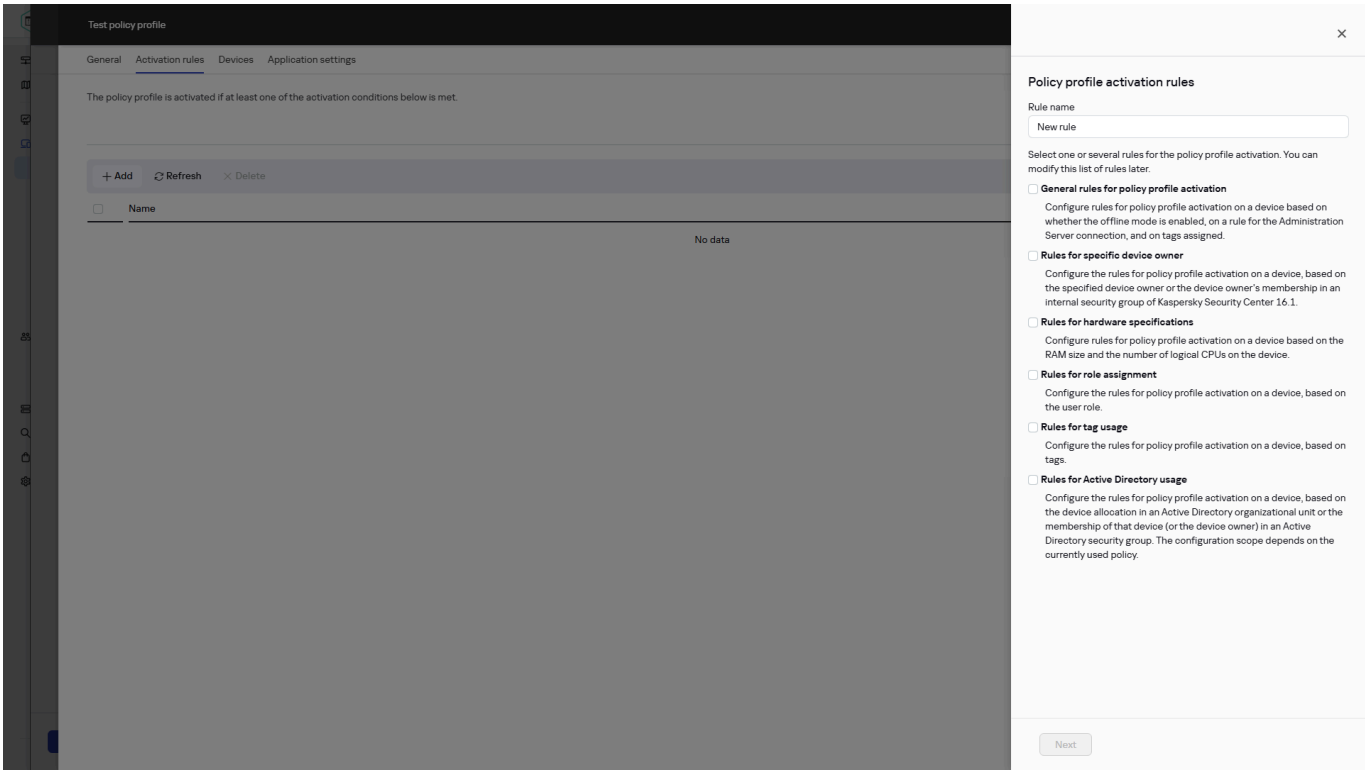
    如果启用此选项，设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **在 Active Directory 组织单元中的设备分配**

    如果启用此选项，指定 Active Directory 组织单元 (OU) 中包括的设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。

    默认情况下已禁用该选项。

向导的附加页面数量取决于您在第一步选择的设置。您可以稍后修改策略配置文件激活规则。



创建策略配置文件激活规则

6. 检查所配置参数的列表。如果列表正确，请单击“**创建**”。

配置文件将被保存。当触发激活规则时，将在设备上激活该配置文件。

为配置文件创建的策略配置文件激活规则显示在“**激活规则**”选项卡上的策略配置文件属性中。您可以修改或删除任何策略配置文件激活规则。

多个激活规则可以被一起触发。

删除策略配置文件

要删除策略配置文件：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在“**策略配置文件**”选项卡上，选中要删除的策略配置文件旁边的复选框，然后单击“**删除**”。
3. 在打开的窗口中，单击“**删除**”。

策略配置文件即被删除。如果策略从低级别组继承，配置文件会保留在该组，但变成该组的策略配置文件。这可以消除低级别组设备上安装的受管理应用程序的设置的显著修改。

导出和导入策略配置文件

您可以将政策配置文件保存到 KLPROF 文件，而无需导出政策，然后使用此 KLPROF 文件将保存的配置配置文件导入到政策中。

这样，您可以快速恢复策略配置文件设置，而无需重新配置。

政策配置文件会被导入到与从其导出该配置文件的应用程序版本相同的应用程序的政策中。对于支持政策向后兼容的应用程序（例如，Kaspersky Endpoint Security for Windows），此操作也适用。您可以将政策配置文件导入到不同版本的政策中。

要导出政策配置文件：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在**策略配置文件**选项卡上，单击要导出的政策配置文件。
3. 在工具栏上，单击**导出**按钮。
4. 在打开的窗口中，指定要保存包含政策配置文件的文件的目录。
   如有必要，您可以更改文件名。
5. 单击“**保存**”按钮。

如果操作成功完成，屏幕上将显示相应的消息。否则，将显示错误消息。

要导入政策配置文件：

1. 转到您要的策略的配置文件列表。
   将出现政策配置文件列表。
2. 在工具栏上，单击**导入**按钮。

3. 在打开的窗口中，选择包含所需政策配置文件的 KLPROF 文件，然后单击**打开**按钮。
   导入文件的最大大小是 4 MB。

如果操作成功完成，屏幕上将显示相应的消息。否则，将显示错误消息。

策略配置文件会以导出时的名称导入，而不是以 KLPROF 文件的名称导入。
无论导出前策略配置文件的优先级如何，该文件都会以**已禁用**状态和最低优先级导入。

以下情况无法执行导入：

- 政策中已存在同名配置文件；
- 政策中的配置文件数量为 100。

网络代理策略设置

若配置网络代理程序政策：

1. 在应用程序的主菜单中，转到 **资产管理** → **策略**。
2. 单击网络代理程序政策的名称。
   网络代理程序政策的属性窗口打开。属性窗口包含如下所述的选项卡和设置。

请参阅比较表格，它详细介绍了根据使用的操作系统类型如何应用以下设置。

常规

在该选项卡上，您可以修改策略名称、策略状态并指定策略设置的继承：

- 在“**名称**”字段中，您可以修改策略名称。
- 在“**策略状态**”块，您可以选择策略的模式：
  - **活动**

    如果选择该选项，策略将变为活动状态。
    默认情况下已选定该选项。
  - **不活动**

    如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。

- 在“**设置继承**”设置组中，您可以配置策略继承：

  - **从父策略继承设置**

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。

  - **在子策略中强制继承设置**

    如果启用此选项，则在应用策略更改之后，将执行以下操作：
    - 策略设置的值将被传送到管理子组的策略，也就是子策略。
    - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

    如果启用此选项，则子策略设置被锁定。
    默认情况下已禁用该选项。

事件配置

在该选项卡上，您可以配置事件记录和事件通知。事件根据重要性级别分布在以下部分：

- **功能失败**
- **警告**
- **信息**

在每个区域，列表显示在管理服务器上事件类型和默认事件存储的期限（天）。单击事件类型后，您可以指定有关列表中选择的事件的事件记录和通知的设置。默认下，为整个管理服务器指定的通用通知设置被用于所有事件类型。然后，您可以更改所需事件类型的特别设置。

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

> 如果网络代理检测到安全问题，您可以使用受管理设备的设置管理此问题。

应用程序设置

设置

在“**设置**”区域，您可以配置网络代理策略：

- **仅通过分发点分发文件**

  如果启用此选项，则受管理设备上的网络代理只从分发点检索更新。

如果禁用此选项，则受管理设备上的网络代理从分发点或管理服务器检索更新。

> 请注意，受管理设备上的安全应用程序从每个安全应用程序的更新任务中设置的源检索更新。如果启用“**仅通过分发点分发文件**”选项，请确保在更新任务中将 Open Single Management Platform 设置为更新源。

默认情况下已禁用该选项。

- **事件队列的最大大小(MB)**

  在该字段中，您可以指定事件队列可在驱动器上占据的最大空间。

  默认设置为 2 MB。

- **应用程序被允许在设备上检索策略扩展数据**

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

  网络代理传输以下信息：

  - 策略传输至受管理设备的时间。
  - 策略传输至受管理设备时的活动策略的名称。
  - 策略传输至受管理设备时漫游策略的名称（对于Linux 版网络代理不可用）。
  - 策略传输至受管理设备时包含受管理设备的管理组的名称和完整路径。
  - 策略传输至受管理设备时包含其名称和优先级的活动策略配置文件列表。

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

- **保护网络代理服务免遭非授权的卸载或终止，并防止设置更改**

  当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

  启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

  默认情况下已禁用该选项。

- **使用卸载密码**

  如果已启用此选项，则单击“**修改**”按钮可以指定 klmover 实用程序的密码。

  默认情况下已禁用该选项。

  禁用此选项以远程卸载网络代理。

存储库

在“**存储库**”区域，您可以选择将其信息从网络代理发送到管理服务器的对象类型：

- **已安装应用程序详情**

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

  默认情况下已启用该选项。

- **包括补丁信息**

  有关在客户端设备上安装的应用程序补丁的信息将发送到管理服务器。启用此选项可能会增加管理服务器和 DBMS 的负载，并导致数据库数据量的增加。

  默认情况下已启用该选项。它仅适用于 Windows。

- **Windows Update 更新详情**

  如果启用此选项，则有关客户端设备上必须安装的 Microsoft Windows Update 更新的信息将发送至管理服务器。

  默认情况下已启用该选项。它仅适用于 Windows。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **软件漏洞和对应更新的详情**

  如果启用此选项，则将有关在受管理设备上检测到的第三方软件（包括 Microsoft 软件）中的漏洞信息以及有关修复第三方漏洞（不包括 Microsoft 软件）的软件更新信息发送到管理服务器。

  选择此选项（**软件漏洞和对应更新的详情）**会增加网络负载、管理服务器磁盘负载和网络代理资源消耗。

  默认情况下已启用该选项。它仅适用于 Windows。

  要管理 Microsoft 软件的软件更新，请使用“**Windows Update 更新详情**”选项。

- **硬件注册表的详细信息**

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

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

如果本区域中的某些设置被网络代理策略禁止，则您无法修改它们。

软件更新和漏洞

在“**软件更新和漏洞**”区域，您可以启用对可执行文件的漏洞扫描：

- **当运行可执行文件时扫描其漏洞**

  如果启用此选项，系统将在运行可执行文件时扫描漏洞。

  默认情况下已启用该选项。

重启管理

如果受管理设备的操作系统必须重启才能正确使用、安装或卸载应用程序，您可以在“**重启管理**”区域指定要执行的操作：

- **不重启操作系统**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **如有必要，自动重启操作系统**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后强制重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

  - **强行关闭锁定会话中的应用程序**

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

    如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

    默认情况下已禁用该选项。

管理补丁和更新

在“管理补丁和更新”区域，您可以配置受管理设备的更新下载和分发以及补丁的安装：

- **对未定义状态的组件自动安装可应用更新和补丁**

  如果启用此选项，带有*未定义*批准状态的 Kaspersky 应用程序在从更新服务器下载后将被自动安装在受管理设备。

如果禁用此选项，被下载和标注为*未定义*状态的 Kaspersky 补丁将仅在您改变其状态为*已批准*是被安装。

默认情况下已启用该选项。

- **提前从管理服务器下载更新和反病毒数据库(推荐)**

  如果启用此选项，离线模式更新下载被使用。当管理服务器接收更新时，它通知网络代理(安装网络代理的设备)将用于受管理应用程序的更新。当网络代理接收更新的信息后，它提前从管理服务器下载相关文件。在第一次连接网络代理时，管理服务器发起更新下载。网络代理下载所有更新到客户端设备后，更新对该设备上的应用程序可用。

  当客户端设备上的受管理应用程序尝试访问网络代理以更新时，该网络代理检查其是否具有所有的更新。如果在受管理应用程序请求更新之前 25 小时内，更新已从管理服务器收到，则网络代理不连接到管理服务器，而是从本地缓存提供更新给受管理应用程序。当网络代理提供更新到客户端设备上的应用程序时，到管理服务器的连接可能不被建立，但是更新不需要连接。

  如果禁用此选项，离线模式更新下载不被使用。更新根据更新下载任务的计划被分发。

  默认情况下已启用该选项。

连接

“**连接**”区域包含三个子区域：

- **网络**
- **连接配置文件**
- **连接计划**

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

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

  - **同步间隔(分钟)**

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

  - **压缩网络流量**

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

    > 客户端设备上的 CPU 负载可能会增加。

    默认情况下启用该复选框。

  - **在 Microsoft Windows 防火墙中打开网络代理端口**

    如果启用此选项，网络代理工作所需的端口将添加到 Microsoft Windows 防火墙排除列表中。

    默认情况下已启用该选项。

- **使用 SSL 连接**

  如果启用此选项，则使用 SSL 协议通过安全端口连接管理服务器。

  默认情况下已启用该选项。

- **以默认连接设置在分发点(如果可用)上使用连接网关**

  如果启用此选项，分发点上的连接网关在管理组属性指定的设置下使用。

  默认情况下已启用该选项。

- **使用 UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

- **UDP 端口号**

  在该字段中，您可以输入 UDP 端口号。默认端口号是 15000。

  使用十进制系统记录。

- **使用分发点强制连接到管理服务器**

  如果在分发点设置窗口中选择了“**将此分发点用作推送服务器**”选项，则选择此选项。否则，分发点不会用作推送服务器。

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

- **网络位置设置**

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

- **管理服务器连接配置文件**

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

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

- **当管理服务器不可用时启用漫游模式**

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

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下已禁用该选项。

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

- **必要时连接**

  如果选中此选项，当网络代理需要发送数据到管理服务器时连接才被建立。

  默认情况下已选定该选项。

- **在指定时间间隔连接**

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

通过分发点的网络轮询

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

- **Windows 网络**

  此选项仅适用于基于 Windows 的分发点。

  如果启用此选项，则管理服务器将按照所配置的计划自动轮询网络，单击“**设置快速轮询计划**”和“**设置完整轮询计划**”链接可配置轮询计划。

  如果禁用此选项，管理服务器将以**网络轮询频率(分钟)**字段中指定的时间间隔轮询网络。

  可以在“**Windows 域的轮询频率(分钟)**（适用于快速 Windows 网络轮询）和 **网络轮询频率(分钟)**（适用于完整 Windows 网络轮询）”字段中配置网络代理版本的设备发现间隔。

  默认情况下已禁用该选项。

- **IP 范围**

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

  如果禁用此选项，则分发点将不轮询 IP 范围。

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

  默认情况下已禁用该选项。

- **Zeroconf**

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

  要开始使用 Zeroconf，必须满足以下条件：

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

  如果禁用此选项，分发点不会轮询带有 IPv6 设备的网络。

  默认情况下已禁用该选项。

- **域控制器**

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

  如果禁用此选项，则分发点将不轮询域控制器。

  对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置域控制器轮询频率。如果启用此选项，则字段可用。

  默认情况下已禁用该选项。

分发点网络设置

在“**分发点网络设置**”区域中，可以指定互联网连接设置：

- **使用代理服务器**

  如果启用此选项，则使用互联网代理服务器将分发点连接到卡巴斯基更新服务器。

- **地址**

- **端口号**

- **对本地地址不使用代理服务器**

  如果启用此选项，将不使用代理服务器连接本地网络的设备。

  默认情况下已禁用该选项。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  默认情况下，此复选框未被选中。

KSN 代理(分发点)

在“**KSN 代理(分发点)**”区域，您可以配置应用程序使用分发点从受管理设备转发 Kaspersky Security Network (KSN) 请求：

- **在分发点端启用 KSN 代理**

  KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

  分发点发送列在Kaspersky Security Network声明中的KSN统计信息到卡巴斯基。

  默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器** 和 **我同意使用卡巴斯基安全网络** 选项在管理服务器属性窗口中被启用时起作用。

  您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

- **转发 KSN 请求到管理服务器**

  分发点从受管理设备转发 KSN 请求到管理服务器。

  默认情况下已启用该选项。

- **通过互联网直接访问 KSN 云/KPSN**

  分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

- **TCP 端口**

  受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

- **UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

- **HTTPS 端口**

  如果您需要受管理设备通过 HTTPS 端口连接到 KSN 代理服务器，请启用“**使用 HTTPS**”选项，然后在“**HTTPS 端口**”字段中指定端口号。默认情况下已禁用该选项。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

更新(分发点)

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

本地账户管理(仅限 Linux)

“**本地账户管理(仅限 Linux)**”部分包括三个子部分：

- **用户证书管理**
- **添加或编辑适用的本地管理员组**
- **上传参考文件以保护用户设备上的 sudoers 文件以防更改**

在“**用户证书管理**”子部分中，您可以指定要安装的根证书。例如，这些证书可用于验证网站或网络服务器的真实性。

- **安装根证书**

  如果启用此选项，则添加到表中的证书将安装在指定的设备上。

  如果禁用此选项，则不会在指定设备上安装任何证书。

  默认情况下已禁用该选项。

- **添加**

  单击此按钮会打开一个窗口，您可以在其中添加证书。

  证书必须小于 10 MB。

  Kaspersky Security Center 支持具有 CER、CRT、CERT、PEM 和 KEY 扩展名的证书。

在“**添加或编辑适用的本地管理员组**”子部分中，您可以管理本地管理员组。例如，在撤销本地管理员权限时会使用这些组。您还可以使用“**特权设备用户报告(仅限 Linux)**”检查特权用户账户列表。

- **添加**

  单击此按钮会打开一个窗口，您可以在其中添加本地管理员组。

- **编辑**

  单击此按钮会打开一个窗口，您可以在其中编辑本地管理员组。

如果选中本地管理员组旁边的复选框，则此按钮可用。

- **删除**

  单击此按钮会从表中删除所选的本地管理员组。

  如果选中本地管理员组旁边的复选框，则此按钮可用。

在“**上传参考文件以保护用户设备上的 sudoers 文件以防更改**”子部分中，您可以配置对 sudoers 文件的控制。特权组和设备用户由设备上的 sudoers 文件定义。sudoers 文件位于 `/etc/sudoers`。您可以上传参考 sudoers 文件，以保护 sudoers 文件以防更改。这可以防止对 sudoers 文件进行不必要的更改。

无效的参考 sudoers 文件可能会导致用户的设备出现故障。

- **控制 sudoer 文件**

  如果启用此选项，sudoers 文件将由当前参考 sudoers 文件替换。

  如果禁用此选项，sudoers 文件将保持不变。

  默认情况下已禁用该选项。

- **参考 sudoer 文件**

  此字段显示上传的参考 sudoers 文件的名称。

- **上传**

  单击此按钮会打开一个窗口，您可以在其中上传参考 sudoers 文件。

- **当前参考 sudoer 文件**

  单击此按钮会显示当前 sudoers 文件的内容。

修订历史

在“**修订历史**”选项卡上，您可以：

- 查看和保存策略修订的历史记录。
- 回滚至策略修订。
- 添加和编辑策略修订描述。
- 比较策略修订。

Windows、Linux 和 macOS 网络代理的使用：比较

网络代理的使用取决于设备的操作系统。网络代理策略和安装包设置也根据操作系统不同而不同。下表比较了适用于 Windows、Linux 和 macOS 操作系统的网络代理的功能和使用方案。

网络代理功能	Windows	Linux	macOS
安装			
通过使用第三方工具克隆带有操作系统和网络代理的管理员硬盘驱动器镜像进行安装	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	✓
使用用于远程安装应用程序的第三方工具进行安装	✓	✓	✓
通过在设备上运行应用程序安装程序来手动安装	✓	✓	✓
在静默模式下安装网络代理	✓	✓	✓
手动连接客户端设备至管理服务器。klmover 实用程序	✓	✓	✓
自动安装 Kaspersky Next XDR Expert 组件的更新和补丁	✓	✓	—
自动分发密钥	✓	✓	✓
强制同步	✓	✓	✓ 推送服务器除外
分发点			
用作分发点	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	✓
计算分发点的数量和配置	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓ 不使用网络定位感知 (NLA)。	✓ 不使用网络定位感知 (NLA)。
离线模式更新下载	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	✓
网络轮询	✓ • IP 范围轮询 • 域控制器轮询（Microsoft Active Directory） 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓ IP 范围轮询 Zeroconf 轮询 域控制器轮询（Microsoft Active Directory、Samba 4 Active Directory、FreeIPA, ALD Pro）	—
在分发点端运行 KSN 代理服务	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	—
通过卡巴斯基更新服务器将更新下载到将更新分发到受管理设备的分发点存储库	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	— （如果一个或多个运行 Linux 或 macOS 的设备在“将更新下载至分发点存储库”任务范围内，则该任务将以“失败”状态完成，即使该任务在所有 Windows 设备上均已成功完成。）
推送应用程序安装	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	受限制：无法使用 Linux 分发点在 Windows 设备上执行推送安装。	受限制：无法使用 macOS 分发点在 Windows 设备上执行推送安装。
用作推送服务器	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	—

网络代理功能	Windows	Linux	macOS
处理第三方应用程序			
在设备上远程安装应用程序	✓	✓	✓ 请参阅以下文章了解详细信息：在 macOS 设备上远程安装应用程序。
在网络代理策略中配置操作系统更新	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	–	–
查看软件漏洞信息	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	–	–
扫描应用程序以查找漏洞	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	–	–
软件更新	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	–	–
清查设备上所安装的软件	✓	✓	–
虚拟机			
在虚拟机上安装网络代理	✓	✓	✓
虚拟桌面基础架构 (VDI) 的优化设置	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	✓
对动态虚拟机的支持	✓ 限制：不受适用于 Arm 架构 Microsoft Windows 的网络代理的支持。	✓	✓
其他			
使用 Windows 桌面共享来审核远程客户端设备上的操作	✓	–	–
监控反病毒保护状态	✓	✓	✓
管理设备重启	✓	–	–
支持文件系统回滚	✓	✓	✓
使用网络代理作为连接网关	✓	✓	✓
连接管理器	✓	✓	✓
漫游用户的连接配置文件	✓	✓	✓
网络代理从一个管理服务器切换到另一个管理服务器（根据网络位置自动切换）	✓	✓	✓
检查客户端设备与管理服务器之间的连接。Klnagchk 工具	✓	✓	✓
远程连接至客户端设备桌面	✓	✓	✓ 通过使用虚拟网络计算 (VNC) 系统。

网络代理功能	Windows	Linux	macOS
通过迁移向导下载独立安装包	✓	✓	✓
查看客户端设备硬件的信息	✓	✓ 安装在这些设备上的网络代理发送给管理服务器的 Linux 设备硬件信息仅限于受管理设备设置描述中指定的信息。	✓ 安装在这些设备上的网络代理发送给管理服务器的 macOS 设备硬件信息仅限于受管理设备设置描述中指定的信息。

按操作系统比较网络代理设置

下表显示了可用的网络代理策略设置，具体取决于安装了网络代理的受管理设备的操作系统。

网络代理设置：按操作系统比较

“设置”区域	Windows	Linux	macOS
常规	✓	✓	✓
事件配置	✓	✓	✓
设置	✓	✓ 下列选项可用： • **仅通过分发点分发文件** • **事件队列的最大大小(MB)** • **应用程序被允许在设备上检索策略扩展数据**	✓
存储库	✓	✓ 下列选项可用： • **已安装应用程序详情** • **硬件注册表的详细信息**	✓ “**硬件注册表的详细信息**”选项可用。
连接→网络	✓	✓ 除了**在 Microsoft Windows 防火墙中打开网络代理端口**选项之外。	✓
连接→连接配置文件	✓	✓	✓
连接→连接计划	✓	✓	✓
通过分发点的网络轮询	✓ 下列选项可用： • **Windows 网络** • **IP 范围** • **域控制器**	✓ 下列选项可用： • **Zeroconf** • **IP 范围** • **域控制器**	—
分发点网络设置	✓	✓	✓
KSN 代理(分发点)	✓	✓	—
更新(分发点)	✓	✓	—
修订历史	✓	✓	✓

配置受管理应用程序的保护

若要配置受管理卡巴斯基应用程序的保护设置，您可以使用策略。

有关配置 Kaspersky Endpoint Security 策略的更多信息，请参阅相应帮助：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Mac 帮助

Kaspersky Endpoint Security 更新组任务的手动设置

Kaspersky Endpoint Security 的最优和建议计划选项是“**当新更新下载至存储库时**”（当“**使用任务启动自动随机延迟**”复选框被选中时）。

卡巴斯基安全网络和卡巴斯基私人安全网络

本节介绍如何使用卡巴斯基安全网络 (KSN) 和卡巴斯基私人安全网络 (KPSN) 在线服务的基础架构。本节提供有关 KSN 和 KPSN 的信息，以及有关如何启用 KPSN、配置 KPSN 访问权限和查看 KSN 代理服务器使用统计信息的说明。

应用程序的认证版本仅允许使用 KPSN。不允许使用 KSN，因为这会导致应用程序失去认证状态。我们建议使用 KPSN，或避免使用 KSN。

关于 KSN

卡巴斯基安全网络 (KSN) 是一种在线服务的基础架构，可提供对 Kaspersky 在线知识库的访问，其中包含与文件信誉、网络资源和软件相关的信息。使用卡巴斯基安全网络的数据，可确保卡巴斯基应用程序更快地响应威胁，提高某些保护组件的有效性，并降低误报风险。KSN 允许您使用 Kaspersky 的信誉数据库检索有关安装在受管理设备上的应用程序信息。

通过参与卡巴斯基安全网络，即表示您同意自动向卡巴斯基提供有关安装在使用 Open Single Management Platform 管理的计算机和移动设备上的安全应用程序运行情况的信息。依照当前KSN 访问设置发送信息。

使用卡巴斯基安全网络会导致应用程序失去认证状态。您必须使用卡巴斯基私人安全网络，或者不使用 KSN。

Open Single Management Platform 支持以下 KSN 基础架构解决方案：

- *全球 KSN* 是一种允许您与 Kaspersky Security Network 交换信息的解决方案。一旦加入 KSN，即表示您同意以自动模式将通过 Open Single Management Platform 管理的客户端设备上安装的卡巴斯基应用程序的相关操作信息发送给卡巴斯基。依照当前KSN 访问设置发送信息。卡巴斯基分析师还分析收到的信息，并将其包含在卡巴斯基安全网络的信誉数据库和统计数据库中。Open Single Management Platform 默认使用此解决方案。

- *卡巴斯基私有安全网络 (KPSN)* 是一种解决方案，允许安装了卡巴斯基应用程序的设备用户访问卡巴斯基安全网络的信誉数据库和其他统计数据，而无需从用户自己的计算机向 KSN 发送数据。KPSN 用于由于以下原因无法参与卡巴斯基安全网络的企业客户：

  - 用户设备未连接到互联网。

  - 传输任何数据到国家以外或企业局域网以外被法律或企业安全政策禁止。

  您可以在管理服务器属性窗口的“**KSN 代理**”部分对卡巴斯基私人安全网络设置访问设置。

您可以随时启用或者停用 KSN。

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您更新或升级管理服务器时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的先前版本继续使用 KSN。

启用 KSN 后，Open Single Management Platform 会检查 KSN 服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保保持受管理设备的安全级别是必要的。

管理服务器管理的客户端设备通过 KSN 代理服务器与 KSN 交互。KSN 代理服务器提供以下功能：

- 即使无法直接访问互联网，客户端设备也可以向 KSN 发送请求以及向 KSN 传送信息。

- KSN 代理服务器可缓存处理后的数据，从而减少发送通道的工作负荷以及为等待客户端设备所请求的信息而花费的时间。

您可以在管理服务器的属性窗口的“**KSN 代理**”部分配置 KSN 代理服务器。

设置对 KSN 的访问

您可以在管理服务器和分发点上设置到卡巴斯基安全网络 (KSN) 的访问。

KSN功能仅适用于当前的Kaspersky EDR Expert授权许可。

要设置管理服务器到 KSN 的访问：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。

3. 将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置。

   数据被从客户端设备发送到 KSN，与在这些客户端设备上活动的 Kaspersky Endpoint Security 政策一致。如果清除此复选框，则不会通过 Kaspersky Next XDR Expert 从管理服务器和客户端设备向 KSN 发送任何数据。但是，客户端设备可以根据各自的设置直接向 KSN 发送数据（绕过 Kaspersky Next XDR Expert）。客户端设备上处于活动状态的 Kaspersky Endpoint Security 策略决定将哪些数据从这些设备直接发送到 KSN（绕过 Kaspersky Next XDR Expert）。

4. 将切换按钮切换到**使用卡巴斯基安全网络已启用**位置。

   如果启用此选项，客户端设备将发送补丁安装结果到 Kaspersky。启用此选项时，请确保阅读并接受 KSN 声明的条款。

   如果要使用 KPSN，请将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置，然后单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（带有 pkcs7 和 pem 扩展名的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。

   将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置时，将显示一条消息，其中包含有关 KPSN 的详细信息。

   以下卡巴斯基应用程序支持 KPSN：

   - Kaspersky Next XDR Expert
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   如果在 Kaspersky Next XDR Expert 中启用 KPSN，这些应用程序将收到有关支持 KPSN 的信息。在应用程序设置窗口，在**高级威胁保护**区域的**卡巴斯基安全网络**子区域中，将显示有关选定 KSN 提供者的信息：KSN 或 KPSN。

   > 如果在管理服务器属性窗口的“**KSN 代理**”部分中配置了 KPSN，Kaspersky Next XDR Expert 不会向卡巴斯基安全网络发送任何统计数据。

5. 如果您在管理服务器属性中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，请启用“**当连接到 KPSN 时忽略代理服务器设置**”选项。否则，从受管理应用程序的请求无法到达 KPSN。

6. 在“**连接设置**”下，配置管理服务器到 KSN 代理服务的连接：

   - TCP 端口 13111 用于连接到 KSN 代理服务器。对于根管理服务器，此端口号无法更改。
   - 如果希望管理服务器通过 UDP 端口连接到 KSN 代理服务器，请启用“**使用 UDP 端口**”选项。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，则默认使用 UDP 端口 15111。对于根管理服务器，此端口号无法更改。

7. 将切换按钮切换到**通过主管理服务器连接从属管理服务器到 KSN 已启用**位置。

   如果启用此选项，从属管理服务器使用主管理服务器作为 KSN 代理服务器。如果禁用此选项，从属管理服务器自己连接到 KSN。该情况下，受管理设备使用从属管理服务器作为 KSN 代理服务器。

   > 如果在从属管理服务器属性的“**KSN 代理**”区域的右侧面板中将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置，则从属管理服务器将使用主管理服务器作为代理服务器。

8. 单击“**保存**”按钮。

KSN 访问设置将被保存。

您也可以设置分发点访问 KSN，例如，如果您想降低管理服务器负载。作为 KSN 代理服务器的分发点从受管理设备直接发送 KSN 请求到 Kaspersky，不使用管理服务器。

要设置分发点到卡巴斯基安全网络（KSN）的访问：

1. 确保分发点是手动分配。
2. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
3. 在“**常规**”选项卡上，选择“**分发点**”区域。
4. 单击分发点的名称以打开其属性窗口。
5. 在分发点属性窗口的“**KSN 代理**”区域中，启用“**在分发点端启用 KSN 代理**”选项，然后启用“**通过互联网直接访问 KSN 云/KPSN**”选项。
6. 单击“**确定**”。

该分发点将作为 KSN 代理服务器。

请注意，分发点不支持使用 NTLM 协议进行受管理设备身份验证。

启用和禁用 KSN 的使用

您可以在管理服务器设置中启用 KSN 的使用。要为集成解决方案启用 KSN 的使用，您还必须在 OSMP 设置中启用它。

在管理服务器设置中启用和禁用 KSN 的使用

要启用 KSN，请执行以下操作：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。
3. 将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置。

KSN 代理服务器已启用，并将数据发送到 KSN，以提升 Kaspersky Next XDR Expert 组件的效率并改善 Kaspersky 应用程序的性能。

1. 根据您使用的KSN 基础设施解决方案，启用相应的切换按钮。
   - 如果使用的是全球 KSN，请将切换按钮切换到“**使用卡巴斯基安全网络已启用**”位置。
     现在可以将数据发送到 KSN。启用此选项时，您必须阅读并接受 KSN 声明的条款。

- 如果您使用 KPSN，请将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置，然后单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（扩展名为 pkcs7 和 pem 的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。

  将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置时，将显示一条消息，其中包含有关 KPSN 的详细信息。

2. 单击“**保存**”按钮。

要禁用 KSN，请执行以下操作：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。

3. 将切换按钮切换到**在管理服务器上启用 KSN 代理 已禁用**位置，以禁用 KSN 代理服务。

4. 单击“**保存**”按钮。

在 OSMP 设置中启用和禁用 KSN 的使用

具有以下角色的用户可以在 OSMP 设置中查看和编辑 KSN 和 KPSN 参与状态：

- 常规管理员
- SOC 管理员
- 租户管理员（编辑状态仅适用于根租户，对于层次结构中的其他租户，设置会自动应用）

具有审计员角色的用户只能查看 KSN 和 KPSN 参与状态。

要在 OSMP 设置中启用 KSN 的使用，请执行以下操作：

1. 在主菜单中，前往**设置 → 卡巴斯基安全网络**。

2. 在**Kaspersky EDR Expert**部分，选择**KSN**连接模式。

3. 打开**参与 KSN**切换按钮。

4. 请阅读KSN声明。

5. 如果您同意 KSN 声明的条款和条件，请选择“**我确认我已完整阅读、理解并接受 KSN 声明的条款和条件**”选项，然后单击“**接受**”。

   KSN将启用，Open Single Management Platform会将统计信息发送到KSN，供卡巴斯基专家进行分析。

6. 如果您不同意 KSN 声明的条款和条件，请单击“**拒绝**”。

   KSN将不会启用。

To enable the usage of KPSN in the OSMP settings:

1. 在主菜单中，前往“**设置**”→“**卡巴斯基安全网络**”。
2. 在**Kaspersky EDR Expert**部分，选择**KPSN**连接模式。
3. 打开**参与 KPSN**切换按钮。
4. 单击**上传**按钮，选择 KPSN 配置文件（扩展名为 .pkcs7 或 .pem 的文件），然后单击**打开**。

   加入KPSN功能随即启用。

要在 OSMP 设置中禁用 KSN 或 KPSN 的使用：

1. 在主菜单中，前往“**设置**”→“**卡巴斯基安全网络**”。
2. 如果您想禁用加入KSN功能，请选择**KSN**连接模式，然后关闭**参与 KSN**切换按钮。
   加入KSN功能随即禁用。
3. 如果您想禁用加入KPSN功能，请选择**KPSN**连接模式，然后关闭**参与 KPSN**切换按钮。

   加入KPSN功能随即禁用。

配置与KPSN本地信誉数据库的连接

Kaspersky Next XDR Expert可以将沙盒组件警报信息保存到KPSN本地信誉数据库中。在这种情况下，对象将被标记为*不受信任*。本地信誉数据库的数据仅对企业局域网计算机可见。

该应用程序允许具有以下角色的用户查看和编辑Kaspersky Private Security Network API集成设置：

- 常规管理员
- SOC 管理员
- 租户管理员（设置编辑功能仅适用于根租户，对于层级结构中的其他租户，设置将自动应用）。

具有审计员角色的用户只能查看Kaspersky Private Security Network API集成设置。

若要配置Kaspersky Next XDR Expert与KPSN本地信誉数据库的连接：

1. 在应用程序主窗口中，转到**设置→租户**部分。
2. 点击**根租户**，然后转到**设置 → KPSN信誉数据库**子部分。
3. 在**“资产”**字段中，指定存储KPSN本地信誉数据库的KPSN服务器的IP地址。
4. 点击**用户证书公钥**字段右侧的**上传**，然后选择所需的.pem证书。
5. 点击**用户证书私钥**字段右侧的**上传**，然后选择所需的.pem证书。

6. 点击KPSN**服务器受信任根证书**字段右侧的**上传**按钮，然后选择所需的.pem证书。

7. 单击“**保存**”按钮。

与KPSN本地信誉数据库的连接随即配置。

查看已接受的 KSN 声明

启用卡巴斯基安全网络 (KSN) 时，必须阅读并接受 KSN 声明。您可以随时查看已接受的 KSN 声明。

要查看已接受的 KSN 声明：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理**”区域。

3. 单击**查看卡巴斯基安全网络声明**链接。

在打开的窗口中，可以查看已接受的 KSN 声明的文本。

接受更新的 KSN 声明

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您升级管理服务器的版本时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的版本继续使用 KSN。

升级管理服务器版本后，将自动显示更新的 KSN 声明。如果您拒绝更新的 KSN 声明，您仍然可以在以后查看并接受它。

要查看然后接受或拒绝更新的 KSN 声明：

1. 单击应用程序主窗口右上角的“**查看通知**”链接。
   “**通知**”窗口打开。

2. 单击“**查看更新的 KSN 声明**”链接。
   卡巴斯基安全网络声明更新窗口打开。

3. 阅读 KSN 声明，然后单击以下按钮之一做出决定：

   - **我接受更新的 KSN 声明**
   - **在旧声明下使用 KSN**

根据您的选择，KSN 会按照当前或更新的 KSN 声明的条款继续工作。您可以随时在管理服务器的属性中查看接受的 KSN 声明的文本。

检查分发点是否充当 KSN 代理服务器

在分配为充当分发点的受管理设备上，可以启用 Kaspersky Security Network (KSN) 代理。当 ksnproxy 服务在设备上运行时，受管理设备充当 KSN 代理服务器。您可以在设备上本地检查、打开或关闭此服务。

您可以将基于 Windows 或基于 Linux 的设备分配为分发点。检查分发点的方法取决于该分发点的操作系统。

要检查基于 Linux 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上，运行 `ps aux` 命令以显示正在运行的进程列表。
2. 在正在运行的进程列表中，检查 `/opt/kaspersky/klnagent64/sbin/ksnproxy` 进程是否正在运行。

如果 `/opt/kaspersky/klnagent64/sbin/ksnproxy` 进程正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

要检查基于 Windows 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上的 Windows 中，打开“**服务**”（“**所有程序**”→“**管理工具**”→“**服务**”）。
2. 在服务列表，检查 ksnproxy 服务是否正在运行。

   如果 ksnproxy 服务正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

如果您想，您可以关闭 ksnproxy 服务。在这种情况下，分发点上的网络代理停止参与卡巴斯基安全网络。该需要本地管理员权限。

查看 KSN 代理服务器的统计信息

您可通过 OSMP 控制台查看 KSN 代理服务器的使用统计信息。

统计信息包括以下参数：

- 与 KSN 的连接状态
- 缓存记录数
- 缓冲中处理的包数
- 收到的数据包数量

如果您使用 KPSN 作为基础设施解决方案，则会显示 KPSN 的使用统计信息。

查看统计信息：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。
2. 在**常规**选项卡上，选择**KSN 代理**部分，然后打开**统计**选项卡。

   该选项卡将显示 KSN 代理服务器使用的实际统计。统计数据每 15 秒刷新一次。

您可以通过单击**复制到剪贴板**按钮来复制统计数据。

管理端点保护任务

本部分介绍 Open Single Management Platform 使用的任务。

关于任务

Open Single Management Platform 通过创建和运行*任务*来管理安装在设备上的卡巴斯基安全应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

仅当 OSMP 控制台服务器上安装了特定应用程序的管理插件后，才能通过 OSMP 控制台为该应用程序创建任务。

任务可以在管理服务器和设备上执行。

管理服务器上执行的任务包含以下：

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

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以由管理员通过 OSMP 控制台进行修改，或者由远程设备用户进行修改（例如，通过安全应用程序界面）。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

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

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

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务执行结果保存在每台设备的操作系统事件日志、管理服务器上的操作系统事件日志和管理服务器数据库中。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

关于任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

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

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

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

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

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

- 指定设备分类。

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

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

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

创建任务

要创建任务：

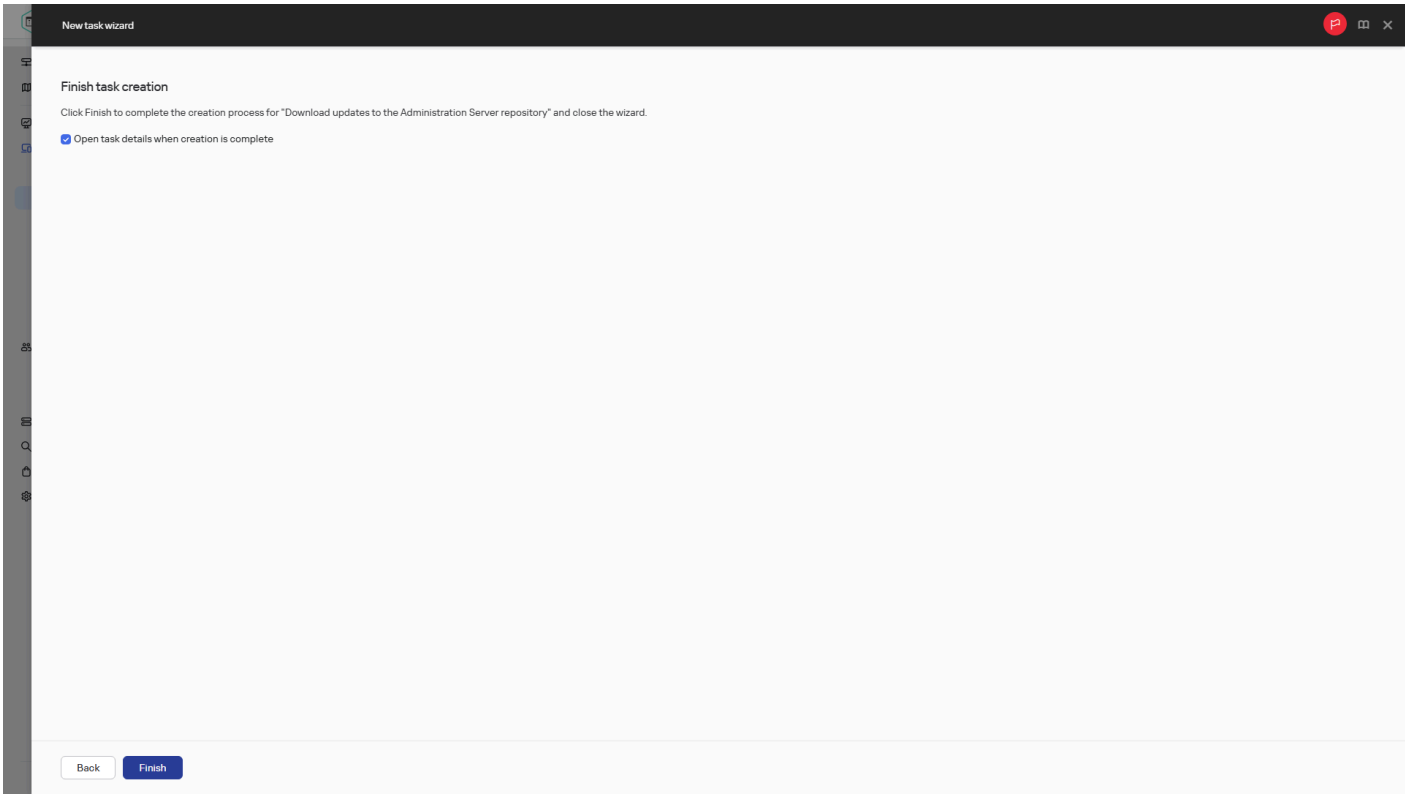
1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵循其说明。

3. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时更改默认设置。

4. 单击“**完成**”按钮。

任务被创建并显示在任务列表。



完成任务创建

要创建分配给所选设备的新任务：

1. 在主菜单中，转到“**资产管理**”→“**资产(设备)**”。

   将显示受管理设备列表。

2. 在受管理设备列表中，选中设备旁边的复选框以为其运行任务。您可以使用搜索和过滤功能来查找您正在寻找的设备。

3. 单击**运行任务**按钮，然后选择**添加一个新任务**。

   “新任务向导”启动。

   在向导的第一步中，您可以删除被选择包括在任务范围中的设备。按照向导的说明进行操作。

4. 单击“**完成**”按钮。

任务为选定的设备创建。

手动启动任务

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

要手动启动任务：

1. 在主菜单中，转到“**任务**”。
2. 在任务列表中，选中要启动的任务旁边的复选框。
3. 单击“**开始**”按钮。

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

为选择的设备执行任务

您可以在设备列表中选择一台或多台客户端设备，然后启动之前为它们创建的任务。这可让您运行之前为一组特定设备创建的任务。

这会更改应用任务的设备列表。
旧的任务范围将被删除，并替换为所选范围。

要为选择的设备启动任务：

1. 在主菜单中，转到**资产管理 → 资产(设备)**。将显示受管理设备列表。
2. 在受管理设备列表中，选中要为其运行任务的设备的复选框。您可以使用搜索和过滤功能来查找您正在寻找的设备。
3. 单击**运行任务**按钮，然后选择**应用现有任务**。

现有任务列表将得到显示。

4. 所选设备显示在任务列表上方。如有必要，您可以从此列表中删除设备。除一台设备之外您可以删除所有设备。
5. 在列表中选择所需的任务。您可以使用列表上方的搜索框按名称搜索所需的任务。只能选择一项任务。
6. 单击**保存并启动任务**。

所选任务立即为所选设备启动。任务中的计划启动设置不会更改。

查看任务列表

您可以查看在 Kaspersky Next XDR Expert 中创建的任务列表。

要查看任务列表，

在主菜单中，转到“**任务**”。

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

要查看任务的属性，

单击任务的名称。

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

常规任务设置

本部分包含您可以查看并为大多数任务配置的设置。可用设置列表取决于您正在配置的任务。

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- 操作系统重启设置：
  - **不重启设备**

    客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。
  - **重启设备**

    如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。
  - **强行关闭锁定会话中的应用程序**

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

    如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

    默认情况下已禁用该选项。
- 任务计划设置：

> 计划的类型可能根据任务而有所不同。

某些类型的计划可能不适用于其他卡巴斯基应用程序。

- **启动任务设置：**
  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。
  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。
  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。
  - **按星期中的天数**

    任务在每周指定日期的指定时间定期运行。

    默认情况下，任务在每周五 6:00:00 PM 运行。
  - **每月**

    任务定期运行，在指定月日的指定时间。

    在缺少指定日的月份，任务在最后一天运行。

    默认下，任务在每月的第一天运行，在当前系统时间。
  - **手动**

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。
  - **一次**

    该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。
  - **立即**

    任务在设置保存后立即运行。
  - **每月在所选工作日**

    任务定期运行，在指定月日的指定时间。

默认情况下，开始时间为18:00，且未选择任何日期。

请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

您可以选择一周中的多个日期。

- **当新更新下载至存储库时**

  当新更新下载至存储库后任务运行。例如，您可能想要对"*更新*"任务使用该计划。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。
    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是"**手动**"、"**一次**"或"**立即**"，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于"**手动**"、"**一次**"和"**立即**"计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- 要分配任务的设备：

  - **选择管理服务器检测到的网络设备**

    任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。

    例如，您可能要在安装网络代理到未分配的设备的任务中使用该选项。

  - **手动指定设备地址或从列表导入地址**

    您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

    您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

  - **分配任务到设备分类**

    该任务被分配到设备分类中的设备。您可以指定现有分类之一。

    例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

  - **分配任务到管理组**

    任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

    例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

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

- 账户设置：

  - **默认账户**

    在与执行该任务的应用程序相同的账户下运行该任务。

    默认情况下已选定该选项。

  - **指定账户**

    填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **登录名。**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

任务创建后指定的设置

您可以在创建任务后指定以下设置。

- 组任务设置：
  - **分发到子组**

    此选项仅在组任务的设置中可用。

    启用此选项后，任务范围包括：
    - 您在创建任务时选择的管理组。
    - 从属于按组层次结构向下的任何级别的选定管理组的管理组。

    禁用此选项后，任务范围仅包括您在创建任务时选择的管理组。

    默认情况下已启用该选项。
  - **分发到从属和虚拟管理服务器**

    启用此选项后，在主管理服务器上有效的任务也将应用于从属管理服务器（包括虚拟管理服务器）。如果从属管理服务器上已经存在相同类型的任务，则两个任务都将应用于从属管理服务器—现有任务和从主管理服务器继承的任务。

    仅当启用“**分发到子组**”选项时，此选项才可用。

    默认情况下已禁用该选项。
- 高级计划设置：
  - **使用 Wake-On-LAN 功能在任务启动之前开启设备**

    设备上的操作系统在任务开始之前的指定时间启动。默认时间段为五分钟。

    如果您想要任务在任务范围内的所有客户端设备上运行，包括任务要启动时关闭的设备，则启用该选项。

    如果您希望在任务完成后自动关闭设备，请启用“**任务完成后关闭设备**”选项。可以在同一窗口中找到此选项。

    默认情况下已禁用该选项。
  - **任务完成后关闭设备**

    例如，您可能想为每周五工作时间后安装更新到客户端设备的更新安装任务启用该选项，然后在周末关闭这些设备。

    默认情况下已禁用该选项。
  - **如果任务运行超过该时间则停止**

    在指定时间段过后，任务被自动停止，无论它是否完成。

    如果您想要中断或停止执行时间太长的任务，则启用该选项。

    默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

- 通知设置：
  - **保存任务历史记录**块：
    - **存储在管理服务器数据库上(天)**

      有关任务范围内所有客户端设备上的任务执行的应用程序事件在指定的天数内被存储在管理服务器。当该时间段过后，信息被从管理服务器删除。

      默认情况下已启用该选项。

    - **存储在设备的 OS 事件日志中**

      与任务执行相关的应用程序事件本地存储在每个客户端设备的 Syslog 事件日志中。

      默认情况下已禁用该选项。

    - **存储在管理服务器的 OS 事件日志中**

      与任务范围内所有客户端设备上的任务执行相关的应用程序事件集中存储在管理服务器操作系统 (OS) 的 Syslog 事件日志中。

      默认情况下已禁用该选项。

    - **保存所有事件**

      如果选择该选项，所有任务相关事件被保存到事件日志。

    - **保存任务进度相关事件**

      如果选择该选项，仅任务执行相关事件被保存到事件日志。

    - **仅保存任务执行结果**

      如果选择该选项，仅任务结果相关事件被保存到事件日志。

  - **通知管理员任务执行的结果**

    您可以选择管理员接收任务执行通知的方法：通过电子邮件、通过 SMS 和通过运行可执行文件。要配置通知，请单击“**设置**”链接。

    默认下，所有通知方法被禁用。

  - **仅通知错误**

    如果该选项被启用，管理员仅在任务执行完成但带有错误时被通知。

    如果该选项被禁用，管理员在每次任务执行完成后被通知。

    默认情况下已启用该选项。

- 安全设置。
- 任务范围设置。

取决于任务范围决定的方式，以下设置被展现：

- **设备。**

  如果任务范围由管理组决定，您可以查看该组。这里不可以更改。然而，您可以设置**任务范围排除项**。

  如果任务范围由设备列表决定，您可以通过添加和删除设备修改该列表。

- **设备分类**

  您可以更改应用程序任务的设备分类。

- **任务范围排除项**

  您可以指定应用任务的设备组。要排除的组仅可以是应用任务的管理组的子组。

- **修订历史**。

导出任务

Open Single Management Platform 支持将任务及其设置保存到 KLT 文件。您可以使用此 KLT 文件将保存的任务导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要导出任务，请执行以下操作：

1. 在主菜单中，转到“**任务**”。
2. 选中要导出的任务旁边的复选框。
   您不能同时导出多个任务。如果您选择了多个任务，**导出**按钮将被禁用。管理服务器任务也将无法导出。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定任务文件的名称和路径。单击“**保存**”按钮。
   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则任务文件会自动保存在“**下载**”文件夹。

导入任务

Open Single Management Platform 支持从 KLT 文件导入任务。KLT 文件包含导出的任务及其设置。

> 为了正确导入卡巴斯基应用程序任务，您必须安装相应的管理插件。

要导入任务，请执行以下操作：

1. 在主菜单中，转到“**任务**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的任务文件。

4. 在打开的窗口中，指定 KLT 任务文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个任务文件。
   任务处理启动。

5. 任务成功处理后，选择要向其分配任务的设备。为此，请选择以下选项之一：

   - **分配任务到管理组**

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

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

   - **手动指定设备地址或从列表导入地址**

     您可以指定要为其分配任务的设备的 DNS 名称、IP 地址和 IP 子网。

     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **分配任务到设备分类**

     该任务被分配到设备分类中的设备。您可以指定现有分类之一。

     例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

6. 指定任务范围。

7. 单击**完成**按钮以完成任务导入。

出现包含导入结果的通知。如果任务成功导入，可以单击“**详细信息**”链接以查看任务属性。

成功导入后，任务会显示在任务列表中。任务设置和时间表也会一起导入。任务将根据其时间表启动。

> 如果新导入的任务与现有任务具有相同的名称，则导入的任务在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

启动更改任务密码向导

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

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

要启动更改任务密码向导：

1. 在主菜单中，转到“**任务**”。

2. 单击**管理启动任务的账户凭证**。

   遵照向导的说明操作。

步骤 1：指定凭证

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

要指定新账户，请选择一个选项：

- **使用当前账户**

  该向导使用您当前登录 OSMP 控制台所使用的账户名。然后手动在“**在任务中使用的当前密码**”字段中指定账户密码。

- **指定不同账户**

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

如果您填写“**先前密码(可选，如果您要使用当前密码替换它)**”字段，Open Single Management Platform 将仅对同时匹配账户名与原密码的任务执行密码替换操作。替换将自动执行。在所有其他情况下，您必须选择要在向导的下一步执行的操作。

步骤 2：选择要采取的操作

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

要选择对任务的操作：

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

移至向导的下一步后，将应用所选操作。

步骤 3：查看结果

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

浏览保存在管理服务器中的任务运行结果

Kaspersky Next XDR Expert 允许您查看组任务、特定设备任务和管理服务器任务的结果。

要查看任务结果：

在任务属性窗口中，转到 **结果** 选项卡。

要查看从属管理服务器的任务结果：

1. 在任务属性窗口中，选择“**常规**”区域。
2. 单击“**结果**”链接打开“**任务结果**”窗口。
3. 单击“**从属服务器的统计信息**”。
4. 选择要显示“**任务结果**”窗口的从属服务器。

Kaspersky Endpoint Security 设备扫描组任务的手动设置

如果自动指定的组扫描任务计划不适合您的组织，您必须根据组织采用的工作场所规则手动设置最方便的计划。

例如，为任务分配“**在星期五下午 7:00 运行**”计划，并且取消选中“**运行错过的任务**”复选框。这意味着如果组织中的设备在星期五关闭，例如在下午 6:30 关闭，设备扫描任务将永远不会运行。在这种情况下，您需要手动设置组扫描任务。

管理检测和响应任务

管理程序控制台时，您可以使用任务来执行各种操作。例如，您可以导入资产或将 KUMA 事件信息导出为 TSV 文件。

查看任务表

任务表包含已创建任务的列表，位于程序控制台窗口的“**任务**” → “**Detection and Response**”部分。您可以查看您（当前用户）创建的任务。

具有主管理员角色的用户可以查看所有用户的任务。

任务表包含以下信息：

- **状态** – 任务的状态。可以为任务分配以下状态之一：
  - *绿点闪烁* – 任务处于活动状态。
  - **已完成** – 任务已完成。
  - **取消** – 用户取消了任务。
  - **错误** – 由于错误，任务未完成。如果将鼠标悬停在感叹号图标上，则会显示错误消息。

- **任务** — 任务类型。该程序提供以下类型的任务：
  - **事件导出** — 导出事件。
  - **在后台运行查询**—在后台运行 SQL 查询。
  - **Threat Lookup** — 从卡巴斯基威胁情报门户请求数据。
  - **回溯扫描** — 重放事件的任务。
  - **OSMP 资产导入** — 从 Kaspersky Security Center 服务器导入资产数据。
  - **账户导入** — 从 Active Directory 导入用户数据。
  - **KICS for Networks 资产导入** — 从 KICS for Networks 导入资产数据。
  - **存储库更新** — 更新 KUMA 存储库以从设置中指定的源接收资源包。
  - **分区备份** 备份分区并将备份文件保存到指定路径。
  - **从备份恢复分区** 从备份副本恢复分区。
  - **导入分区** 从外部 KUMA 安装中导入分区。
- **创建者** — 创建任务的用户。如果任务是自动创建的，则该列将显示“**已排定的任务**”。
  此列仅对具有常规管理员和租户管理员角色的用户显示。
- **创建时间** — 任务创建时间。
- **更新时间** — 任务上次更新的时间。
- **租户** — 启动任务的租户的名称。

任务日期格式取决于应用程序设置中选择的本地化语言。可用的日期格式选项：

- 英语本地化：YYYY-MM-DD。
- 俄语本地化：DD.MM.YYYY。

查看任务运行结果

要查看任务运行结果：

1. 在主菜单中，转到 **任务** → **Detection and Response**。
   任务表随即显示。
2. 单击“**任务**”列中包含任务类型的链接。
   将显示此任务类型可用的操作列表。
3. 选择“**显示结果**”。

   任务结果窗口打开。

重新启动任务

要重新启动任务：

1. 在主菜单中，转到 **任务** → **Detection and Response**。
   任务表随即显示。
2. 选中要重启的任务旁边的复选框。
3. 单击“**重启**”按钮。

任务将重新启动。

应用程序标签

Kaspersky Next XDR Expert 允许您标记应用程序注册表中的应用程序。标签是应用程序标志，可以用于分组或查找应用程序。分配给应用程序的标签可以作为设备分类中的条件。

例如，您可以创建 [浏览器] 标签，并将其分配给所有浏览器，例如 Microsoft Internet Explorer®、Google Chrome、Mozilla Firefox。

创建应用程序标签

要创建应用程序标签：

1. 在主菜单中，转到“**软件管理** ”→“**第三方应用程序**” →“**应用程序标签**”。
2. 单击**添加**。
   新标签窗口打开。
3. 输入标签名称。
4. 单击“**确定**”保存更改。

新标签出现在应用程序标签列表。

重命名应用程序标签

要重命名应用程序标签：

1. 在主菜单中，转到“**软件管理**” → “**第三方应用程序**” → “**应用程序标签**”。
2. 选中要重命名的标签旁边的复选框，然后单击“**编辑**”。
   标签属性窗口打开。

3. 更改标签名称。

4. 单击“**确定**”保存更改。

更新的标签出现在应用程序标签列表。

分配标签到应用程序

要分配一个或多个标签到一个应用程序：

1. 在主菜单中，转到“**软件管理**”→“**第三方应用程序**”→“**应用程序注册表**”。

2. 单击您要分配标签的应用程序名称。

3. 选择“**标签**”选项卡。

标签显示所有存在于管理服务器的应用程序标签。对于分配到所选应用程序的标签，“**分配的标签**”列中的复选框处于选中状态。

4. 对于要分配的标签，请选中“**分配的标签**”列中的复选框。

5. 单击“**保存**”保存更改。

标签被分配到应用程序。

从应用程序上删除分配的标签

要从应用程序删除一个或多个标签：

1. 在主菜单中，转到“**软件管理**”→“**第三方应用程序**”→“**应用程序注册表**”。

2. 单击您要删除标签的应用程序名称。

3. 选择“**标签**”选项卡。

标签显示所有存在于管理服务器的应用程序标签。对于分配到所选应用程序的标签，“**分配的标签**”列中的复选框处于选中状态。

4. 对于要删除的标签，请清除“**分配的标签**”列中的复选框。

5. 单击“**保存**”保存更改。

标签被从应用程序删除。

已卸载应用程序的标签不被删除。如果您想，您可以手动删除它们。

删除应用程序标签

要删除应用程序标签：

1. 在主菜单中，转到“**软件管理**” → “**第三方应用程序**” → “**应用程序标签**”。
2. 在列表中，选择您想要删除的应用程序标签。
3. 下一步，单击“**删除**”按钮。
4. 在打开的窗口中，单击“**确定**”。

应用程序标签被删除。删除的标签被从其分配的所有应用程序上自动删除。

在 OSMP 控制台中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序

要通过 OSMP Console 开始使用 Kaspersky Industrial CyberSecurity for Networks 应用程序，必须先在 OSMP Console 中对其进行注册。

要注册 Kaspersky Industrial CyberSecurity for Networks 应用程序：

1. 确保完成以下操作：
   - 您已下载并安装 Kaspersky Industrial CyberSecurity for Networks Web 插件。

     您可以稍后在等待 Kaspersky Industrial CyberSecurity for Networks Server 与管理服务器同步时执行此操作。下载并安装插件后，“**KICS for Networks**”部分将显示在 OSMP Console 的主菜单中。
   - 在 Kaspersky Industrial CyberSecurity for Networks Web 界面中，已配置并启用与 Kaspersky Next XDR Expert 的交互。详情请参阅 Kaspersky Industrial CyberSecurity for Networks 在线帮助。
2. 将安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备从未分配设备组移动到受管理设备组：
   a. 在主菜单中，转到“**Asset management**” → “**Unassigned devices**”。
   b. 选中安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备旁边的复选框。
   c. 单击**移动到组**按钮。
   d. 在管理组的层次结构中，选中**受管理设备**组旁边的复选框。
   e. 单击“**移动**”按钮。
3. 打开安装了 Kaspersky Industrial CyberSecurity for Networks Server 的设备的属性窗口。
4. 在设备属性页面的 **General** 部分，选择“**不要断开与管理服务器的连接**”选项，然后单击“**保存**”按钮。
5. 在设备属性页面，选择**应用程序**区域。

6. 在**应用程序**区域，选择 Kaspersky Security Center 网络代理。

7. 如果应用程序的当前状态是“*已停止*”，等到它变为“*正在运行*”。

   这最多需要 15 分钟。如果您尚未安装 Kaspersky Industrial CyberSecurity for Networks Web 插件，您可以立即安装。

8. 如果想查看 Kaspersky Industrial CyberSecurity for Networks 的统计信息，您可以在仪表板上添加小部件。要添加小部件，请执行以下操作：

   a. 在主菜单中，转到“**监控**”→“**仪表板**”。

   b. 在仪表板上，单击“**添加或恢复网页小部件**”按钮。

   c. 在打开的小部件菜单中，选择“**其它**”。

   d. 选择您要添加的小部件：

      - KICS for Networks 部署图
      - 有关 KICS for Networks Servers 的信息
      - KICS for Networks 的最新活动
      - KICS for Networks 中存在问题的设备
      - KICS for Networks 中的关键事件
      - KICS for Networks 中的状态

9. 要继续访问 Kaspersky Industrial CyberSecurity for Networks Web 界面，请执行以下操作：

   a. 在主菜单中，转至**KICS for Networks →搜索**。

   b. 单击**查找事件或设备**按钮。

   c. 在打开的**查询参数**窗口中，单击**服务器**字段。

   d. 从与 Kaspersky Next XDR Expert 集成的服务器下拉列表中选择 Kaspersky Industrial CyberSecurity for Networks 服务器，然后单击**查找**按钮。

   e. 单击 Kaspersky Industrial CyberSecurity for Networks 服务器名称旁边的“**转至服务器**”链接。

      Kaspersky Industrial CyberSecurity for Networks 登录页面将显示。

      要登录 Kaspersky Industrial CyberSecurity for Networks Web 界面，您需要提供应用程序用户账户凭据。

管理用户和用户角色

该部分描述了用户和用户角色，并提供创建和修改它们、分配角色和组到用户以及关联策略配置文件到角色的说明。

关于用户账户

Kaspersky Next XDR Expert 允许您管理用户账户和安全组。应用程序支持四种账户类型：

- 组织员工的账户。在轮询组织的域控制器时管理服务器检索数据的域用户的账户。
- 本地用户账户。受管理设备上的本地账户，以及安装了管理服务器的设备上的本地账户。
- Kaspersky Next XDR Expert 内部用户的账户。您可以创建内部用户账户。这些账户仅在 Kaspersky Next XDR Expert 中使用。
- 服务账户。这些账户仅用于将 Kaspersky Next XDR Expert 服务连接到管理服务器。服务账户在部署解决方案时自动添加，不能删除或更改。这些账户的权限和角色也不能更改。您不能使用服务账户登录到 OSMP Console。

Linux 操作系统中的本地用户账户和 kladmins 本地组不能用于访问 Open Single Management Platform 中的 OSMP Console。kladmins 组只能包含被用来启动 Open Single Management Platform 服务的账户。配置域身份验证后，组织员工便可以使用其用户账户登录。

OSMP 控制台中的默认身份验证方法是输入用户名、密码和用于双重身份验证的附加一次性安全代码。从 Kaspersky Next XDR Expert 2.0开始，双重身份验证默认自动启用，并默认禁用登录时配置双重身份验证的选项。

您可以通过Kerberos协议配置域身份验证。域身份验证可让您在 OSMP Console 中启用安全身份验证，而无需在公司网络上重新输入密码（单点登录）。

查看用户账户和安全组表：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”。
2. 选择**用户**或**组**选项卡。

用户或安全组表将打开。

如果您只想查看包含内部用户、本地用户或域用户或用户组的表格，请将**账户类型**筛选条件设置为相应的值。

如果用户表包含超过 50,000 个用户，则仅显示前 50,000 个用户，其余用户将不显示。

关于用于角色

用户角色（也叫*角色*）是包含一组权限集的对象。角色可以与安装在用户设备上的卡巴斯基应用程序设置关联。您可以分配角色到用户集，或者到管理组层级的任何级别、管理服务器或特定对象级别的安全组集。

如果您通过包含虚拟管理服务器的管理服务器层级来管理设备，请注意，您仅可从物理管理服务器创建、修改或删除用户角色。这样，您可以将用户角色传输到从属管理服务器，包括虚拟服务器。

您可以关联用户角色到策略配置文件。如果用户被分配角色，用户将获得执行工作职能所需的安全设置。

一个用户角色可以与特定管理组中的设备用户关联。

用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

使用角色的好处

使用角色的好处之一是您不必为每个受管理设备或用户指定安全设置。公司中的用户和设备数量可能相当庞大，但需要不同安全设置的职位描述数量则少得多。

与使用策略配置文件的不同点

策略配置文件是为每个卡巴斯基应用程序创建的策略的属性。角色与许多为不同应用程序创建的策略配置文件相关联。因此，角色是联合特定用户类型的设置到一处的方法。

配置对应用程序功能的访问权限。基于角色的访问控制

Kaspersky Next XDR Expert 支持对其自身功能及受管理的 Kaspersky 应用程序实施基于角色的访问控制。

您可以采用以下方式之一，为 Kaspersky Next XDR Expert 用户配置应用程序功能的访问权限：

- 通过为每个用户或用户组单独配置权限。
- 通过使用一组预定义的权限创建标准用户角色并根据用户的职责范围将这些角色分配给用户。

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

可为用户角色分配与其各自的目的对应的名称。您可在程序中创建无限数量的角色。

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

应用程序功能的访问权限

下表列出了 Kaspersky Next XDR Expert 的功能，以及管理相关任务、报告和设置以及执行相关用户操作所需的访问权限。

要执行表中列出的用户操作，用户必须拥有该操作旁边指定的权限。

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

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

应用程序功能的访问权限

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：**管理组的管理**	**写入**	• 将设备添加到管理组：**写入** • 从管理组中删除设备：**写入** • 将管理组添加到另一个管理组：**写入** • 将管理组从另一个管理组中删除：**写入**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：**访问对象而不考虑它们的** ACL	**读取**	获取对所有对象的读取权限：**读取**	无	无	**常规功能：访问对象而不考虑它们的ACLs**功能区域用于审计目的。此功能区域中的**读取**权限授予对所有对象的完整**读取**权限。我们建议谨慎地将这些权限授予有限数量的用户，这些用户需要这些权限来履行工作职责。 即使其他权限禁止对特定对象的读取访问，访问权限也会被授予。
常规功能：**基本功能**	• **读取** • **写入** • **执行** • **对设备分类执行操作**	• 虚拟服务器的设备移动规则（创建、修改或删除）：**写入**、**对设备分类执行操作** • 获取移动 (LWNGT) 协议自定义证书：**读取** • 设置移动 (LWNGT) 协议自定义证书：**写入** • 获取 NLA 定义的网络列表：**读取** • 添加、修改或删除 NLA 定义的网络列表：**写入** • 查看组的访问控制列表：**读取** • 查看操作系统日志：**读取**	• “将更新下载至管理服务器存储库” • “提交报告” • “分发安装包” • “在从属管理服务器上远程安装应用程序”	• “保护状态报告” • “威胁报告” • “感染最严重的设备报告” • “反病毒数据库状态报告” • “错误报告” • “网络攻击报告” • “已安装的周边防护应用程序汇总报告” • “已安装的应用程序类型汇总报告” • “受感染的设备用户报告” • “事故报告” • “事件报告” • “分发点活动报告” • “从属管理服务器报告” • “设备控制事件报告” • “漏洞报告” • “禁止的应用程序报告” • “Web 控制报告” • “受管理设备加密状态报告” • “大容量存储设备加密状态报告” • “加密设备访问权限报告” • “文件加密错误报告” • “加密文件访问被阻止报告” • “有效用户权限报告” • “权限报告”	无
常规功能：**已删除对象**	• **读取** • **写入**	• 查看回收站中的已删除对象：**读取** • 删除回收站中的对象：**写入**	无	无	无
常规功能：**事件处理**	• **删除事件** • **编辑事件通知设置** • **编辑事件记录设置** • **写入**	• 更改事件注册设置：**编辑事件记录设置** • 更改事件通知设置：**编辑事件通知设置** • 删除事件：**删除事件**	无	无	设置： • 数据库中存储的最大事件数量 • 已删除设备中事件的存储时间段
常规功能：**对管理服务器的操作**	• **读取** • **写入** • **执行**	• 指定用于连接网络代理的管理服务器端口：**写入** • 指定在管理服务器上启动的激活代理端口：**写入**	• “备份管理服务器数据” • “数据库维护”	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
	• **修改对象 ACL** • **对设备分类执行操作**	• 指定在管理服务器上启动的移动激活代理端口：**写入** • 指定用于分发独立安装包的 Web 服务器端口：**写入** • 指定用于分发 MDM 配置文件的 Web 服务器端口：**写入** • 指定用于通过 OSMP 控制台连接的管理服务器 SSL 端口：**写入** • 指定用于移动连接的管理服务器端口：**写入** • 指定管理服务器数据库中存储的最大事件数量：**写入** • 指定管理服务器可以发送的最大事件数量：**写入** • 指定管理服务器可以发送事件的时间段：**写入**			
常规功能：Kaspersky **软件部署**	• **管理 Kaspersky 补丁** • **读取** • **写入** • **执行** • **对设备分类执行操作**	批准或拒绝安装补丁：**管理 Kaspersky 补丁**	无	• “虚拟管理服务器授权许可密钥使用报告” • “Kaspersky 软件版本报告” • “不兼容的应用程序报告” • “Kaspersky 软件模块更新版本报告” • “保护部署报告”	安装包： "Kaspersky"
常规功能：**密钥管理**	• **导出密钥文件** • **写入**	• 导出密钥文件：**导出密钥文件** • 修改管理服务器授权许可密钥设置：**写入**	无	无	无
常规功能：**强制报告管理**	• **读取** • **写入**	• 创建报告而不考虑它们的 ACL：**写入** • 执行报告而不考虑它们的 ACL：**读取**	无	无	无
常规功能：**管理服务器层级**	**配置管理服务器的层级**	• 注册、更新或删除从属管理服务器：**配置管理服务器层级**	无	无	无
常规功能：**用户权限**	**修改对象 ACL**	• 更改任何对象的“安全”属性：**修改对象 ACL** • 管理用户角色：**修改对象 ACL** • 管理内部用户：**修改对象 ACL** • 管理安全组：**修改对象 ACL** • 管理别名：**修改对象 ACL**	无	无	无
常规功能：**虚拟管理服务器**	• **管理虚拟管理服务器** • **读取** • **写入** • **执行** • **对设备分类执行操作**	• 获取虚拟管理服务器列表：**读取** • 获取关于虚拟管理服务器的信息：**读取** • 创建、更新或删除虚拟管理服务器：**管理虚拟管理服务器**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
		• 将虚拟管理服务器移动到另一个组：**管理虚拟管理服务器** • 设置管理虚拟服务器权限：**管理虚拟管理服务器**			
常规功能：**加密密钥管理**	**写入**	在训练模式下启动行动手册的审批，需将加密密钥权限配置为：**写入**	无	无	无
系统管理：**漏洞和补丁管理**	• **读取** • **写入** • **执行** • **对设备分类执行操作**	• 查看第三方补丁属性：**读取** • 更改第三方补丁属性：**写入**	• “修复漏洞” • “安装所需更新并修复漏洞”	“软件更新报告”	无

预定义用户角色

分配给 Kaspersky Next XDR Expert 用户的用户角色可为其提供一组应用程序功能访问权限。

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

特定职位角色示例

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

下表显示了分配给每个预定义用户角色的访问权限。

预定义用户角色的访问权限

角色	描述
基本角色	
管理服务器管理员	允许在以下功能区域的所有操作： • **常规功能**： • **基本功能** • **加密密钥管理** • **事件处理** • **管理服务器层级** • **虚拟管理服务器** • **系统管理**： • **连接** • **设备清单** • **软件清查**

角色	描述
管理服务器操作员	授予在以下所有功能区域的**读取**和**执行**权限： • **常规功能**： • **基本功能** • **加密密钥管理** • **虚拟管理服务器** • **系统管理**： • **连接** • **设备清单** • **软件清查**
审计员	在“**常规功能**”中，允许以下功能区域中的所有操作： • **访问对象而不考虑它们的** ACL • **删除对象** • **管理报告** 您可以分配该角色到执行您组织的审计的人。
安装管理员	在“**常规功能**”中，允许以下功能区域中的所有操作： • **基本功能** • **部署卡巴斯基应用程序** • **授权许可密钥管理** 授予在“**常规功能：虚拟管理服务器**”功能区域的**读取**和**执行**权限。
安装操作员	在“**常规功能**”中授予以下所有功能区域的**读取**和**执行**权限： • **基本功能** • **Kaspersky 软件部署**（也授予在该区域的**管理 Kaspersky Lab 补丁**权限） • **虚拟管理服务器**
Kaspersky Endpoint Security 管理员	允许在以下功能区域的所有操作： • **常规功能：基本功能** • Kaspersky Endpoint Security 区域，包括所有功能 授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。
Kaspersky Endpoint Security 操作员	授予在以下所有功能区域的**读取**和**执行**权限： • **常规功能：基本功能** • Kaspersky Endpoint Security 区域，包括所有功能
常规管理员	在“**常规功能**”中，*除*以下区域外，允许功能区域内的所有操作： • **访问对象而不考虑它们的** ACL • **管理报告** 授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。
主要操作员	授予在以下所有功能区域的**读取**和**执行**（如果适用）权限： • **常规功能**： • **基本功能** • **删除对象** • **管理服务器操作** • **部署卡巴斯基应用程序** • **虚拟管理服务器** • Kaspersky Endpoint Security 区域，包括所有功能
“移动设备管理”管理员	允许“**常规功能：基本功能**”功能区域中的所有操作。
安全官	在“**常规功能**”中，允许以下功能区域中的所有操作： • **访问对象而不考虑它们的** ACL • **管理报告** 授予在“**系统管理：连接**”功能区域的“**读取**”、“**写入**”、“**执行**”、“**将设备中的文件保存到管理员工作站**”和“**对设备分类执行操作**”权限。 您可以分配该角色到负责您组织的 IT 安全的安全官。
Self Service Portal 用户	允许在“**移动设备管理：Self Service Portal**”功能区域的所有操作。Kaspersky Security Center 11 和更高版本不支持此功能。

角色	描述
管理者	授予在“**常规功能**：**无论对象的 ACL 如何均可访问对象**”和“**常规功能**：**强制报告管理**”功能区域的“**读取**”权限。 您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。
XDR 角色	
常规管理员	允许在以下功能区域的所有操作： • **警报和事故** • Detection and response • **行动手册和响应** • **管理资产** • IAM • **租户** • **卡巴斯基集成** • **第三方集成** • **授权许可**
租户管理员	允许在以下功能区域的所有操作： • **警报和事故** • Detection and response • **行动手册和响应** • **管理资产** • IAM • **租户** • **卡巴斯基集成** • **第三方集成** • **授权许可** 此角色相当于主管理员角色，但有一项限制。在 KUMA 中，租户管理员对预设对象的访问权限有限。
SOC 管理员	在 XDR 功能区域授予以下权限： • Detection and response：**读取**、**写入** • **行动手册和响应**：**读取**、**写入**、**删除** • IAM：**读取用户和角色**、**分配角色**和**列出用户** • **租户**：**读取**、**写入** • **卡巴斯基集成**：**读取**、**写入** • **第三方集成**：**读取**、**写入** • **授权许可**：**读取** • **资产管理**：**读取**、**写入**、**删除**

角色	描述
初级分析师	在 XDR 功能区域授予以下权限： • **警报和事故**：**读取**和**写入** • Detection and response：**读取** • **资产管理**：**读取** **查看详细信息** 读取： • 查看类别列表。 • 按类别添加设备列表。 • 以CSV格式导出设备。 • 查看符合活动分类条件的设备。 • 查看资产卡。 • 查看自定义字段列表。 • 查看已归档设备的事件保留期（TTL）。 • 查看资产审核设置。 • 查看与 Kaspersky Next XDR Expert 的集成设置。 • 查看用于定义设备活动状态的阈值设置。 写入： • 添加类别。 • 修改类别。 • 添加设备。 • 修改设备（包括类别）。 • 对 Kaspersky Next XDR Expert 设备执行强制同步。 • 手动执行活动分类。 • 添加资产自定义字段。 • 修改资产自定义字段。 • 修改已归档设备的事件保留期（TTL）。 • 添加资产审核设置。 • 修改资产审核设置。 • 复制资产审核设置。 • 添加与 Kaspersky Next XDR Expert 的集成设置。 • 修改与 Kaspersky Next XDR Expert 的集成设置。 • 修改用于定义设备活动状态的阈值设置。 删除： • 删除类别。 • 归档设备。 • 删除资产自定义字段。 • 删除资产审核设置。 • IAM：**读取用户和角色**和**列表用户** • **租户**：**读取** • **卡巴斯基集成**：**读取** • **第三方集成**：**读取** • **授权许可**：**读取**

角色	描述
2 级分析师	在 XDR 功能区域授予以下权限： • **警报和事故**：**读取**和**写入** • Detection and response：**读取** • **行动手册和响应**：**读取**、**写入**、**执行** • **管理资产** • IAM：**读取用户和角色**和**列表用户** • **租户**：**读取** • **卡巴斯基集成**：**读取** • **第三方集成**：**读取** • **授权许可**：**读取**
1级分析师	在 XDR 功能区域授予以下权限： • **警报和事故**：**读取**和**写入** • Detection and response：**读取** • **行动手册和响应**：**读取**、**写入**、**执行** • **资产管理** • IAM：**读取用户和角色**和**列表用户** • **租户**：**读取** • **卡巴斯基集成**：**读取** • **第三方集成**：**读取** • **授权许可**：**读取** 该角色与 2 级分析师角色相对应，但存在一个限制。在 KUMA 中，1级分析师只能修改自己的对象。

角色	描述
SOC 经理	在 XDR 功能区域授予以下权限： • **警报和事故**：**读取**和**写入** • **Detection and response**：**读取** • **行动手册和响应**：**读取** • **资产管理**：**读取** **查看详细信息** 读取： • 查看类别列表。 • 按类别添加设备列表。 • 以CSV格式导出设备。 • 查看符合活动分类条件的设备。 • 查看资产卡。 • 查看自定义字段列表。 • 查看已归档设备的事件保留期（TTL）。 • 查看资产审核设置。 • 查看与 Kaspersky Next XDR Expert 的集成设置。 • 查看用于定义设备活动状态的阈值设置。 写入： • 添加类别。 • 修改类别。 • 添加设备。 • 修改设备（包括类别）。 • 对 Kaspersky Next XDR Expert 设备执行强制同步。 • 手动执行活动分类。 • 添加资产自定义字段。 • 修改资产自定义字段。 • 修改已归档设备的事件保留期（TTL）。 • 添加资产审核设置。 • 修改资产审核设置。 • 复制资产审核设置。 • 添加与 Kaspersky Next XDR Expert 的集成设置。 • 修改与 Kaspersky Next XDR Expert 的集成设置。 • 修改用于定义设备活动状态的阈值设置。 删除： • 删除类别。 • 归档设备。 • 删除资产自定义字段。 • 删除资产审核设置。 • IAM：**读取用户和角色**和**列表用户** • **租户**：**读取** • **卡巴斯基集成**：**读取** • **第三方集成**：**读取** • **授权许可**：**读取**

角色	描述
审批人	在 XDR 功能区域授予以下权限： • **警报和事故**：**读取、写入、关闭** • Detection and response：**读取** • **行动手册和响应**：**读取**和**响应确认** • **资产管理**：**读取** **查看详细信息** 读取： • 查看类别列表。 • 按类别添加设备列表。 • 以CSV格式导出设备。 • 查看符合活动分类条件的设备。 • 查看资产卡。 • 查看自定义字段列表。 • 查看已归档设备的事件保留期（TTL）。 • 查看资产审核设置。 • 查看与 Kaspersky Next XDR Expert 的集成设置。 • 查看用于定义设备活动状态的阈值设置。 写入： • 添加类别。 • 修改类别。 • 添加设备。 • 修改设备（包括类别）。 • 对 Kaspersky Next XDR Expert 设备执行强制同步。 • 手动执行活动分类。 • 添加资产自定义字段。 • 修改资产自定义字段。 • 修改已归档设备的事件保留期（TTL）。 • 添加资产审核设置。 • 修改资产审核设置。 • 复制资产审核设置。 • 添加与 Kaspersky Next XDR Expert 的集成设置。 • 修改与 Kaspersky Next XDR Expert 的集成设置。 • 修改用于定义设备活动状态的阈值设置。 删除： • 删除类别。 • 归档设备。 • 删除资产自定义字段。 • 删除资产审核设置。 • IAM：**读取用户和角色以及列出用户**。 • **租户**：**读取** • **卡巴斯基集成**：**读取** • **第三方集成**：**读取** • **授权许可**：**读取**

角色	描述
审计员	在 XDR 功能区域授予以下权限： • **警报和事故**：**读取** • Detection and response：**读取** • **行动手册和响应**：**读取** • **资产管理**：**读取** **查看详细信息** 读取： • 查看类别列表。 • 按类别添加设备列表。 • 以CSV格式导出设备。 • 查看符合活动分类条件的设备。 • 查看资产卡。 • 查看自定义字段列表。 • 查看已归档设备的事件保留期（TTL）。 • 查看资产审核设置。 • 查看与 Kaspersky Next XDR Expert 的集成设置。 • 查看用于定义设备活动状态的阈值设置。 写入： • 添加类别。 • 修改类别。 • 添加设备。 • 修改设备（包括类别）。 • 对 Kaspersky Next XDR Expert 设备执行强制同步。 • 手动执行活动分类。 • 添加资产自定义字段。 • 修改资产自定义字段。 • 修改已归档设备的事件保留期（TTL）。 • 添加资产审核设置。 • 修改资产审核设置。 • 复制资产审核设置。 • 添加与 Kaspersky Next XDR Expert 的集成设置。 • 修改与 Kaspersky Next XDR Expert 的集成设置。 • 修改用于定义设备活动状态的阈值设置。 删除： • 删除类别。 • 归档设备。 • 删除资产自定义字段。 • 删除资产审核设置。 • IAM：**读取用户和角色**和**列表用户** • **租户**：**读取** • **卡巴斯基集成**：**读取** • **第三方集成**：**读取** • **授权许可**：**读取**

角色	描述
与子事故交互	在 XDR 功能区域授予以下权限： • **子事故**：**读取**和**写入** • IAM：**读取用户和角色以及列出用户**。 除了此角色之外，您还必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、2 级分析师、1 级分析师、SOC 经理、审批人、审计员。
管理共享资源	授予对共享租户中共享资源的编辑访问权限。 除了此角色之外，您还必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、2 级分析师、1 级分析师、SOC 经理、审批人。
读取共享资源	授予对共享租户中共享资源的读取访问权限。 除了此角色之外，您还必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、2 级分析师、1 级分析师、SOC 经理、审批人。
SLA 管理	授予编辑事故剩余 SLA 时间的权利。 除了此角色之外，您还必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、2 级分析师、1 级分析师、SOC 经理、审批人。
查看通用控制板布局	授予查看通用控制板布局的权利。 除了此角色之外，您还必须拥有以下 XDR 角色之一：主管理员、租户管理员、初级分析师、2 级分析师、1 级分析师、SOC 经理、审批人。
服务角色	
自动威胁响应器	授予服务账户响应威胁的权利。 访问权限根据 Kaspersky Security Center Linux 和受管理卡巴斯基应用程序基于角色的访问控制策略进行自动配置。 您只能将此角色分配给服务账户。 该角色无法编辑。

分配对特定对象的访问权限

除了分配服务器级别的访问权限，您还可以配置对特定对象的访问，例如对特定任务的访问。该应用程序允许您指定对以下对象类型的访问权限：

- 管理组
- 任务
- 报告
- 设备分类
- 事件分类

要分配对特定对象的访问权限：

1. 根据对象类型，在主菜单中转到相应区域：
   - **资产管理 → 组层级**
   - **任务**
   - **监控→报告**
   - **资产管理→设备分类**
   - **监控→事件分类**
2. 打开要为其配置访问权限的对象的属性。
   要打开管理组或任务的属性窗口，单击对象名称。其他对象的属性可以使用工具栏上的按钮打开。
3. 在属性窗口中，打开**访问权限**部分。
   用户列表将打开。列出的用户和安全组具有对象的访问权限。默认情况下，如果您使用管理组或服务器的层级，则列表和访问权限是从父管理组或主服务器继承的。
4. 为了能够修改列表，启用**使用自定义权限**选项。
5. 配置访问权限：
   - 使用**添加**和**删除**按钮修改列表。
   - 指定用户或安全组的访问权限。执行以下操作之一：
     - 如果要手动指定访问权限，请选择用户或安全组，单击“**访问权限**”按钮，然后指定访问权限。
     - 如果要分配一个用户角色到用户或安全组，请选择用户或安全组，单击“**角色**”按钮，然后选择要分配的角色。
6. 单击“**保存**”按钮。

配置对象的访问权限。

分配权限到用户和组

您可以为用户和安全组分配访问权限，使其能够使用管理服务器以及您已安装管理插件的卡巴斯基应用程序（例如 Kaspersky Endpoint Security for Windows）的各类功能。

将权限分配给用户或安全组：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**访问权限**”选项卡上，选中要分配权限的用户或安全组名称旁边的复选框，然后单击“**访问权限**”按钮。
   您不能同时选择多个用户或安全组。如果您选择了多个条目，“**访问权限**”按钮将被禁用。

3. 配置用户或组的权限集：

   a. 使用管理服务器或其他卡巴斯基应用程序的功能扩展节点。

   b. 选择所需功能或访问权限旁边的**允许**或**拒绝**复选框。

   *示例 1：*选中**应用程序集成**节点旁边的**允许**复选框，向用户或组授予对应用程序集成功能（**读取**、**写入**和**执行**）的所有可用访问权限。

   *示例 2：*展开**加密密钥管理**节点，然后选中写入权限旁边**的允许**复选框，以授予用户或组对加密密钥管理功能的**写入**访问权限。

4. 配置访问权限集后，单击**确定**。

用户或用户组的权限集将被配置。

管理服务器（或管理组）的权限被分成以下部分：

- 常规功能：
  - 对管理组进行管理
  - 访问对象而不考虑它们的 ACL
  - 基本功能
  - 删除对象
  - 加密密钥管理
  - 事件处理
  - 管理服务器操作
  - 设备标签
  - 部署卡巴斯基应用程序
  - 授权许可密钥管理
  - 管理报告
  - 服务器层级
  - 用户角色权限
  - 虚拟管理服务器
- 移动设备管理：
  - 常规
- 系统管理：
  - 连接
  - 设备清单

- 网络访问控制
- 操作系统部署
- 管理漏洞和补丁
- 远程安装
- 软件清查

如果没有为权限选择“**允许**”或“**拒绝**”，则该权限被认为是*未定义*的：它将被拒绝，直到被用户明确拒绝或允许为止。

用户权限是以下各项的集合：

- 用户自己的权限
- 分配给该用户的所有角色的权限
- 用户所属的所有安全组的权限
- 分配到用户所属安全组的所有角色的权限

如果至少一个权限集对权限“**拒绝**”，那么用户被拒绝该权限，即便其他集允许它或保持未定义。

您还可以将用户和安全组添加至用户角色范围，以使用管理服务器的不同功能。与用户角色相关联的设置，仅适用于两类条件同时满足的设备：一是设备归属于拥有该角色的用户，二是设备归属于与该角色相关联的组（包括子组）。

添加内部用户账户

要将新的内部用户账户添加到 Kaspersky Next XDR Expert：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击**添加**。
3. 在打开的“**添加用户**”窗口中，指定新用户账户设置：
   - **名称**。
   - **密码**，供用户连接 Kaspersky Next XDR Expert 时使用。
     密码必须符合以下规则：
     - 密码长度必须为10到256个字符。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)

- 数字 (0-9)
- 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- 密码不得包含任何空格、Unicode 字符，也不得包含“.”在“@”之前的“.”和“@”组合。

要查看您输入的字符，请单击并按住“**显示**”按钮。

> 输入密码的尝试次数有限。默认下，允许的最大密码输入尝试次数是 3。您可以管理允许的密码输入尝试次数，描述在“更改允许的密码输入尝试次数”。

> 如果用户输入无效的密码指定次数，用户账户被锁定一小时。您仅可以通过更改密码解除阻止用户账户。

4. 单击“**保存**”保存更改。
5. 如有必要，为租户中已创建的内部用户账户分配角色。

新的用户账户将被添加到用户列表中。

> 要在OSMP控制台上使用已创建的内部用户账户登录，必须先为该帐户分配角色。登录前，请确保该内部用户账户已分配角色。否则，将会出现登录错误。

创建安全组

要创建安全组：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**组**选项卡。
2. 单击**添加**。
3. 在打开的**创建安全组**窗口中，为新安全组指定以下设置：
   - **组名称**
   - **描述**
4. 单击“**保存**”保存更改。

新的安全组已被添加到组列表中。

编辑内部用户账户

要在 Kaspersky Next XDR Expert 中编辑内部用户账户：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击您要编辑的用户账户名称。
3. 在打开的用户设置窗口中的“**常规**”选项卡上，更改用户账户设置：
   - **描述**
   - **完整名称**
   - **邮件地址**
   - **主电话**
   - 为用户连接到 Kaspersky Next XDR Expert **设置新密码**。
     密码必须符合以下规则：
     - 密码长度必须为10到256个字符。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)
       - 数字 (0-9)
       - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密码不得包含任何空格、Unicode 字符，也不得包含“.”在“@”之前的“.”和“@”组合。

     要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

     > 输入密码的尝试次数有限。默认下，允许的最大密码输入尝试次数是 3。您可以更改允许的尝试次数；但是，出于安全原因，我们不建议您减少此数字。如果用户输入无效的密码指定次数，用户账户被锁定一小时。您仅可以通过更改密码解除阻止用户账户。

   - 如果必要，将切换按钮切换到“**已禁用**”以禁止用户连接到应用程序。您可以禁用账户，例如，在员工离职后。
4. 在“**双重身份验证**”选项卡上，可以指定此账户的安全设置。
5. 在“**组**”选项卡上，可以添加用户到安全组。
6. 在“**设备**”选项卡上，可以分配设备到用户。

7. 在“**角色**”选项卡上，可以分配角色到用户。

8. 单击“**保存**”保存更改。

更新的用户账户出现在用户列表中。

更改用户工作状态

用户工作状态显示您是否可以向用户分配警报和事故。

用户可能具有以下状态之一：

- **可用** – 用户已准备好处理警报和事故。
- **繁忙** – 用户尚未准备好处理警报和事故。警报和事故无法自动分配给用户。

默认情况下，当用户登录 OSMP 控制台或 KUMA 控制台时，用户工作状态会自动更新为“**可用**”。

您可以手动更改您的工作状态或当前登录用户的工作状态。

更改您自己账户的工作状态

您当前的工作状态显示在主菜单中您账户名称的旁边：如果状态为“**可用**”，则为绿点 ( )；如果状态为“**繁忙**”，则为红点 ( )。

如果要更改当前的工作状态，在上部窗格中，请转到您的账户设置，然后选择要分配给您账户的状态。

更改内部用户账户的工作状态

仅当用户当前已登录 OSMP 控制台或 KUMA 控制台时，用户设置窗口中才会显示“**工作状态**”字段。
要更改内部用户的工作状态，您必须具有以下 XDR 角色 之一：主管理员、租户管理员、SOC 管理员。

要更改内部用户的工作状态：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**用户**”选项卡。
   用户列表将打开。
2. 单击您要更改状态的用户账户的名称。
   用户设置窗口将打开，且“**常规**”选项卡已被选中。
3. 在“**工作状态**”字段中，选择您要分配的状态：“**可用**”或“**繁忙**”。
4. 单击“**保存**”按钮。

窗口将关闭，用户的工作状态已更改。

编辑安全组

要编辑安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**组**选项卡。
2. 单击您要编辑的安全组名称。
3. 在打开的组设置窗口中，更改安全组设置：
   - 在“**常规**”选项卡上，您可以更改“**名称**”和“**描述**”设置。这些设置仅适用于内部安全组。
   - 在“**用户**”选项卡上，您可以执行以下操作：
     - 查看组用户表格。
     - 将用户添加到安全组。为此，请单击**添加**按钮，然后在打开的**添加用户**窗格中，选中要添加的用户账户旁边的复选框，然后单击**保存**。
       在**添加用户**窗格中，您可以按租户筛选用户。为此，请将**租户所有者**筛选条件设置为所需值。

       > 只有内部用户和内部安全组才能将用户添加到安全组。

     - 从安全组中删除用户。为此，请选中用户账户名称旁边的复选框，单击**删除**，然后确认操作。
   - 在“**角色**”选项卡上，可以分配角色到安全组。
4. 单击“**保存**”保存更改。

更改将应用于安全组。

为用户或安全组分配角色

为用户或安全组分配角色：

1. 在主菜单中，转至**用户和角色**→**用户和组**，然后选择**用户**或**组**选项卡。
2. 选择要向其分配角色的用户或安全组的名称。
   您可以选择多个名称。
3. 在菜单项目上，单击“**分配角色**”按钮。
   角色分配向导启动。
4. 按照向导的说明进行操作：选择要分配给所选用户或安全组的角色，然后选择角色的范围。
   *用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

拥有一组管理服务器使用权限的角色将被指派给用户（或多个用户，或安全组）。在用户或安全组列表中，**已分配角色**列中会出现一个复选框。

添加用户账户到内部安全组

您仅可以添加内部用户账户到内部安全组。

要添加用户账户到内部安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 选择您要添加到安全组的用户账户旁边的复选框。
3. 单击“**分配组**”按钮。
4. 在打开的“**分配组**”窗口中，选择要将用户账户添加到的安全组。
5. 单击“**保存**”按钮。

用户账户被添加到安全组。您还可以使用组设置将内部用户添加到安全组。

将用户指定为设备所有者

有关如何将用户指定为移动设备所有者的信息，请参阅Kaspersky Secure Mobility Management帮助文档。

要指派用户作为设备所有者：

1. 如果要分配连接到虚拟管理服务器的设备的所有者，请先切换到虚拟管理服务器：
   a. 在主菜单中，单击当前管理服务器名称右侧的 V 形图标 ()。
   b. 选择所需的管理服务器。
2. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
   用户列表将打开。如果您当前连接到虚拟管理服务器，则该列表包括来自当前虚拟管理服务器和主管理服务器的用户。
3. 单击您要分配为设备所有者的用户账户名称。
4. 在打开的用户设置窗口中，选择“**设备**”选项卡。
5. 单击**添加**。
6. 从设备列表中，选择您要分配给用户的设备。
7. 单击“**确定**”。

所选的设备被添加到分配给用户的设备列表。

您可以在“**资产管理**”→“**资产(设备)**”中执行相同操作，方法是单击要分配的设备名称，然后单击“**管理设备所有者**”链接。

配置双重身份验证

从Kaspersky Next XDR Expert 2.0开始，双重身份验证将自动启用。不支持禁用双重身份验证的全局选项。本方案提供了在首次登录时配置双重身份验证以及在管理服务器上配置双重身份验证设置的步骤。

阶段

分阶段配置双重身份验证：

1. **在设备上安装认证应用**

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

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

   要检查Kaspersky Next XDR Expert是否支持要使用的身份验证应用程序，请为所有用户或特定用户启用双重身份验证。

   其中一个步骤会建议您指定由身份验证器应用生成的安全代码。如果成功，则Kaspersky Next XDR Expert支持选定的身份验证器。

   > 强烈建议不要将认证应用安装在对管理服务器进行管理的同一台设备上。

2. **将安装了认证应用的设备的时间与安装了管理服务器的设备的时间同步**

   确保已安装认证应用的设备上的时间和已部署管理服务器的设备上的时间与 UTC 同步。为了提高准确性，建议在整个基础架构中使用相同的 NTP 服务器。否则，在配置双重身份验证时可能会出现故障。

3. **在用户账户登录 Web Console 时，为其配置双重身份验证**

   登录 Web Console 并配置双重身份验证。

   如果您无法配置双重身份验证，请联系具有常规功能：用户权限功能区域中**修改对象**ACL权限且已配置双重身份验证的用户，将您的帐户添加到双重身份验证允许列表中。

4. **在管理服务器上配置双重身份验证设置**

如果您已配置双重身份验证并具有常规功能**常规功能**用户权限**用户权限修改对象**ACL权限，则可以按如下方式在管理服务器上配置双重身份验证设置：

1. 查看可在登录时配置双重身份验证的用户列表：

   - 要从头开始安装Kaspersky Next XDR Expert 2.0：将所需的用户添加到双重身份验证允许列表中，使他们能够在首次登录时配置双重身份验证。
   - 要升级到Kaspersky Next XDR Expert 2.0：查看双重身份验证允许列表，并删除必须无法访问管理服务器的帐户。

2. 排除不需要启用双重身份验证的用户账户（可选）

   将用户账户从双重身份验证中排除，允许这些账户即使未配置双重身份验证，也能登录管理服务器。对于在身份验证期间无法提供安全代码的集成账户，可能有必要从双重身份验证中排除这些账户。集成账户用于通过 OpenAPI 运行脚本。

3. 重置或删除双重身份验证 secret key（可选）

   当用户无法访问其双重身份验证设备或需要在新设备上设置双重身份验证时，您可以重置双重身份验证的密钥。您还可以重置自己账户的 secret key。

   您可以删除 secret key，从而完全阻止用户登录 Web Console 和访问管理服务器。

4. 编辑安全码颁发者的名称（可选）

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

结果

完成此方案后：

- 您的用户账户和另一个需要访问管理服务器的用户账户均已配置双重身份验证。
- 集成账户即从双重身份验证中排除。

关于账户的双重身份验证

Kaspersky Next XDR Expert 为 OSMP Console 用户提供了双重身份验证。双重身份验证基于 RFC 6238 标准（TOTP：基于时间的一次性密码算法）。

每次登录 OSMP 控制台时，您都需要输入用户名、密码和一个额外的一次性安全码。要接收一次性安全码，移动设备或计算机上必须安装了认证应用。

任何支持基于时间的一次性密码算法 (TOTP) 的认证软件都可以用作认证应用，例如 Google Authenticator。为了生成一次性安全码，您必须将安装了认证应用的设备上的时间与管理服务器设备上的时间同步。为了提高准确性，建议在整个基础架构中使用相同的 NTP 服务器。

若要检查 Kaspersky Next XDR Expert 是否支持您要使用的身份验证应用，请尝试使用此身份验证应用配置双重身份验证。

其中一个步骤会建议您指定由认证应用生成的一次性安全码。如果成功，则Kaspersky Next XDR Expert支持选定的身份验证器。

使用认证应用生成密码

认证应用会生成安全代码，如下所示：

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

安全代码具有一个称为*颁发者名称*的标识符。安全代码颁发者名称用作管理服务器在认证应用中的标识符。您可以更改安全码颁发者的名称。安全代码颁发者名称的默认值与管理服务器的名称相同。下次登录后，新的安全码颁发者名称会被分配给管理服务器。安全码为一次性，有效期最长为 30 秒（具体时间可能会有所不同）。

我们强烈建议您保存 secret key 或二维码，并将其保管在安全的地方。万一您失去对安装了认证应用的设备的访问权限，这将帮助您恢复对 OSMP 控制台的访问权限。

双重身份验证具有以下功能：

- 从 Kaspersky Next XDR Expert 2.0 开始，双重身份验证默认自动启用，并默认禁用登录时配置双重身份验证的选项。登录时配置双重身份验证仅适用于包含在双重身份验证允许列表中的用户。
- 用户只能为自己的账户配置双重身份验证。
- 您可以从双重身份验证中排除指定账户。对于无法接收一次性安全码进行身份验证的集成账户，此功能可能非常重要。集成帐户用于通过OpenAPI运行脚本以及运行KUMA脚本。
- 若要重新生成双重身份验证的密钥，用户必须重置其自身帐户的密钥。
- 若要重置或删除其他用户帐户的双重身份验证的密钥，用户必须拥有已配置双重身份验证的帐户，并且在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限。
- 要将其他用户的账户从双重身份验证中排除或修改双重身份验证允许列表，用户必须拥有已配置双重身份验证的账户，并且在**常规功能**：**用户权限**功能区中拥有修改对象ACL权限。
- 应该始终至少有一个用户配置了双重身份验证，以便该用户可以管理双重身份验证允许列表和排除列表。
- 双重身份验证仅在 Kaspersky Next XDR Expert 2.0 或更高版本中自动启用。如果其他主要管理服务器或从属管理服务器运行的是版本 1.4 或更早版本，则它们的双重身份验证设置将保持不变。
- 虚拟管理服务器继承物理管理服务器的双重身份验证设置，因此如果在物理管理服务器上启用了双重身份验证，则在虚拟管理服务器上也会启用双重身份验证。您无法在虚拟管理服务器上配置双重身份验证设置。

若要通过双重身份认证实现全面保护，不仅需要对管理服务器采取安全防护措施，还需保障其部署设备的安全性。为此，请参照强化指南中的建议。

在OSMP云控制台登录时配置双重身份验证密钥

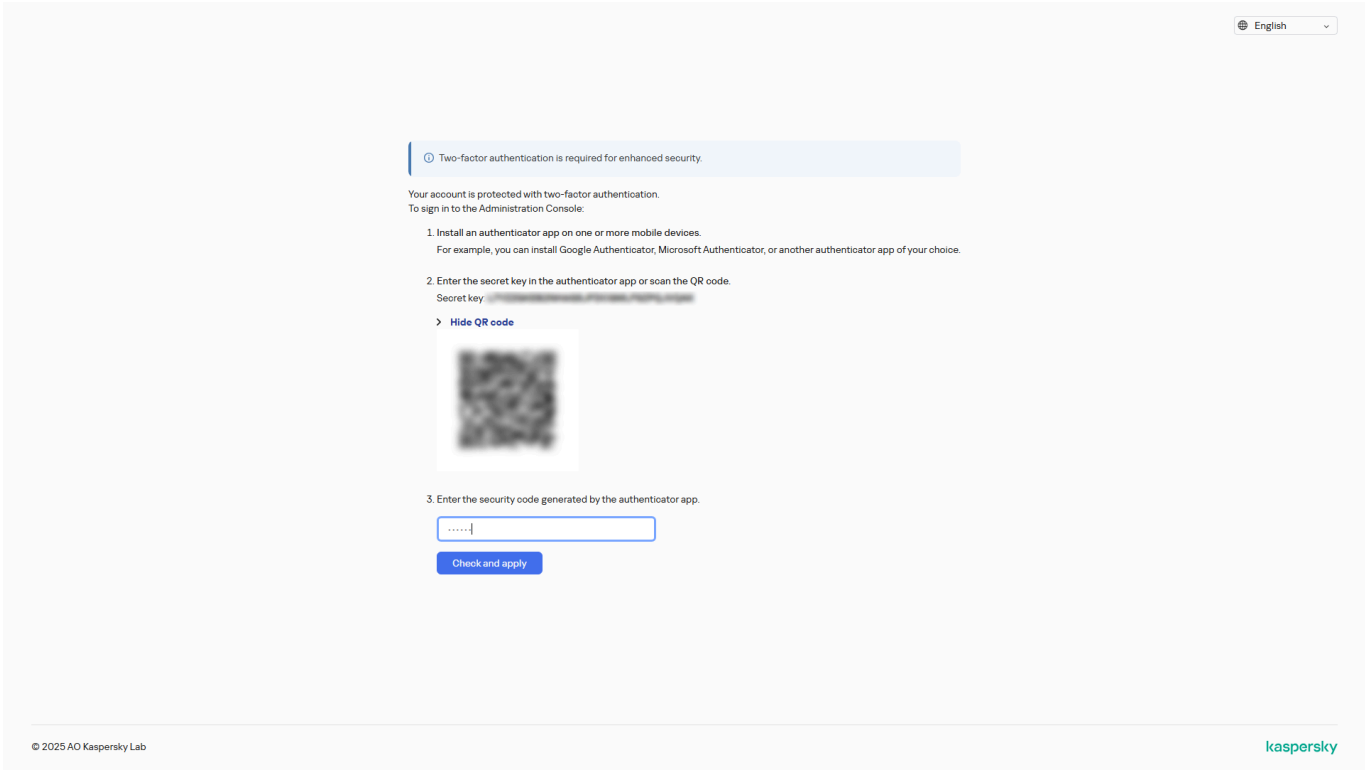
首次登录Kaspersky Next XDR Expert 2.0或更高版本时，会打开双重身份验证的设置窗口。

要为您的账户配置双重身份验证：

1. 请在移动设备或计算机上安装任何支持基于时间的一次性密码算法的应用程序，例如：
   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 验证器
   - Aladdin 2FA
   - Rutoken OTP

   强烈建议不要将认证应用安装在对管理服务器进行管理的同一台设备上。
2. 确保已安装认证应用的设备上的时间和已部署管理服务器的设备上的时间与 UTC 同步。为了提高准确性，建议在整个基础架构中使用相同的 NTP 服务器。
3. 使用移动设备或计算机上的认证应用来生成一次性安全码。为此，请执行以下步骤之一：
   - 在认证应用中手动输入双重身份验证 secret key。
   - 单击**查看二维码**并使用身份验证器应用扫描二维码。

移动设备上将显示一个 6 位数的一次性安全码。



在OSMP云控制台登录时配置双重身份验证密钥

4. 在“**双重身份验证**”窗口中，指定由认证应用生成的一次性安全码，然后单击“**检查和应用**”按钮。

Rutoken OTP 配置

如果您使用 Rutoken OTP，则需要一台安装了 Rutoken OTP 应用程序的 Android 移动设备。Android 移动设备必须满足以下要求：

- 操作系统是 Android 7 或更高版本。
- NFC 模块可用且已启用。

在 Rutoken OTP 应用程序中，您必须配置以下参数：

- 扫描两步配置向导中显示的二维码。
- 将时间间隔设置为 30 秒。
- 选择 SHA1 作为算法。

要配置 Rutoken OTP：

1. 将 Rutoken OTP 设备放在带有 NFC 模块的移动设备旁边。
2. 在 Rutoken OTP 应用程序中，按下“**连接令牌**”。
3. 在 Rutoken OTP 应用程序中，按下“**配置设置**”，然后按下“**保存 secret key**”。

如果令牌成功连接到移动设备，Rutoken OTP 应用程序将显示以下状态消息：

- **令牌已连接。**
- **设置已配置。**
- **密钥已保存。**

4. 在 Rutoken OTP 设备上，按下按钮。
   设备上会显示一个安全码。
5. 在 OSMP Console 的双重身份验证窗口中，输入安全码。

您的账户已配置双重身份验证。您可以根据您的权限访问管理服务器。

> 如果您无法配置双重身份验证，请联系在**常规功能**： **用户权限**功能区域中拥有修改对象ACL权限且已配置双重身份验证的用户，将您的账户添加到双重身份验证允许列表中。

允许用户配置双重身份验证

双重身份验证允许列表是允许在登录云控制台时初始配置双重身份验证的用户列表。此列表包含未配置双重身份验证的用户账户。默认情况下，新用户账户不会包含在双重身份验证允许列表中，必须由管理员添加到该列表中。如果新帐户是用于运行OpenAPI脚本的集成帐户，则必须将其从双重身份验证中排除。

当用户帐户配置了双重身份验证或被排除在双重身份验证之外时，用户帐户将自动从允许双因素身份验证列表中删除。

对于已配置双重身份验证且在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限的帐户，可以手动修改双重身份验证允许列表。

若要手动将用户账户添加到允许列表：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在属性窗口的**双重身份验证**选项卡中，在**允许生成 Secret 密钥的用户**表中，单击**添加**按钮。
3. 在打开的窗口中：
   a. 选择要添加的用户账户。
      只有未被排除在双重身份验证之外且没有双重身份验证密钥的用户才能添加到允许列表中。
   b. 如果账户已开启防止未经授权修改的保护功能，您必须确认您有修改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。
   c. 保存更改。

选定的用户账户将被添加到双重身份验证允许列表中。下次登录时，用户将能够生成密钥。

在为该用户账户配置双重身份验证之前，可以从双重身份验证允许列表中删除该用户账户。

若要手动从双重身份验证允许列表中删除用户账户：

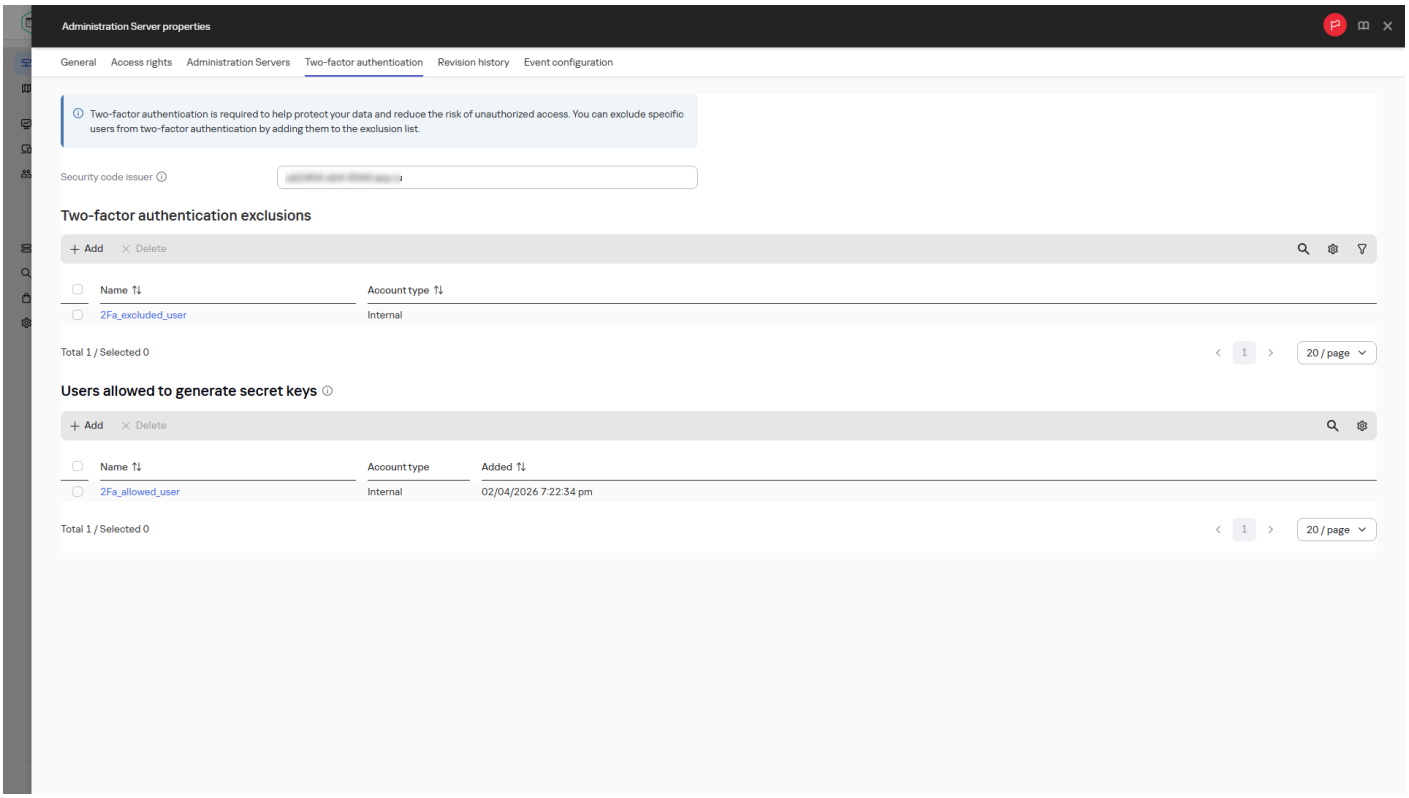
1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在属性窗口的**双重身份验证**选项卡上的**允许生成 Secret 密钥的用户**表中，选择要删除的用户账户，然后单击**删除**。

3. 如果账户已开启防止未经授权修改的保护功能，您必须确认您有修改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

选定的用户账户将从允许列表中删除。



配置双重身份验证允许列表

如果在管理服务器上的活动会话期间，您的双重身份验证密钥被其他用户删除，或者您自行重置了密钥但未创建新密钥，则修改允许列表的功能将被阻止。

用户账户也可以自动添加到双重身份验证允许列表或从中删除。

重置其他帐户的双重身份验证密钥时，这些帐户会自动添加到允许列表中，以便它们可以生成新密钥。

将 Kaspersky Next XDR Expert 从 1.4 版本升级到 2.0 或更高版本时，如果满足以下所有条件，用户账户将自动添加到双重身份验证权限列表中：

- 用户在*常规功能功能区域中具有"读取"权限：基本功能*直接分配给用户（而不是通过安全组）。具有此权限的用户和角色范围必须包含所有已管理和未分配的设备，并且必须在管理服务器级别设置。
- 该用户未被排除在双重身份验证之外。
- 该用户没有双重身份验证密钥。
- 更早版本的管理服务器上并非所有用户都启用了双重身份验证。

即使未能满足其中一项条件，用户也无法被添加到双重身份验证允许列表中。

> 升级或恢复后，我们建议确保允许列表中仅包含必须有权访问管理服务器的用户账户。查看允许列表，并从中删除所有其他帐户。将用于通过OpenAPI运行脚本的集成帐户添加到排除项列表中，以防止脚本运行失败。

如果满足以下所有条件，则用户帐户在升级或恢复后将失去对管理服务器的访问权限：

- 用户在*常规功能功能区拥有"读取"权限：基本功能*是通过安全组分配的（不是直接分配给用户），或者根本没有此权限。
- 该用户未被排除在双重身份验证之外。
- 该用户没有双重身份验证密钥。
- 在先前版本的管理服务器上，并非所有用户都启用了双重身份验证。

如有需要，可手动将这些帐户添加到双重身份验证允许列表中。

重置和删除双重身份验证密钥

当用户无法访问其双重身份验证设备或需要在新设备上设置双重身份验证时，您可以重置密钥。重置密钥后，用户可以再次登录云控制台并生成新密钥。

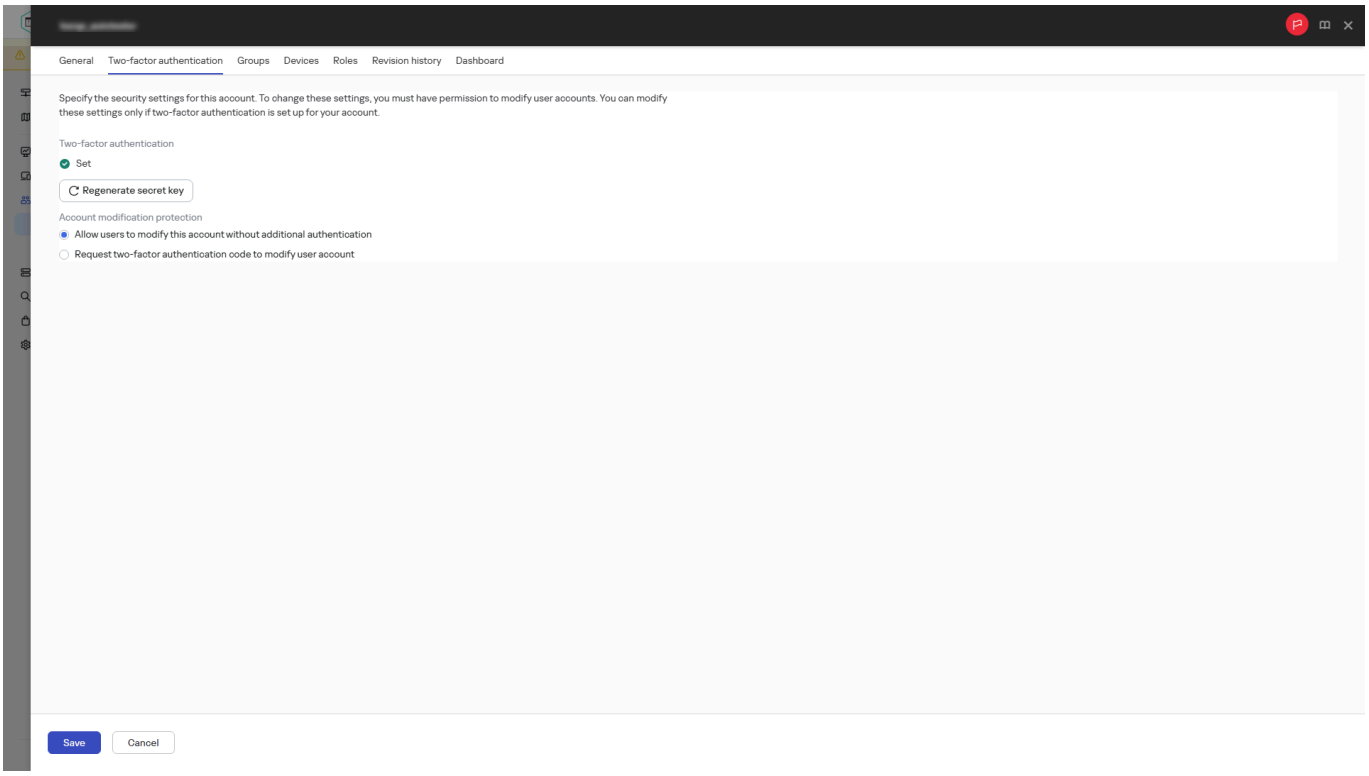
> 只有当您已配置双重身份验证，并且在**常规功能**：**用户权限**功能区域中拥有修改对象ACL权限时，才能重置或删除其他用户的双重身份验证密钥。您也可以重新生成自己的密钥。

要重置某个帐户的密钥：

1. 在主菜单中，转至"**用户和角色**" → "**用户和组**"，然后选择"**用户**"选项卡。
2. 单击要重置密钥的用户账户名称。

3. 如果要重置自己帐户的密钥：

a. 在**双重身份验证**选项卡上，单击**重新生成 Secret 密钥**按钮。

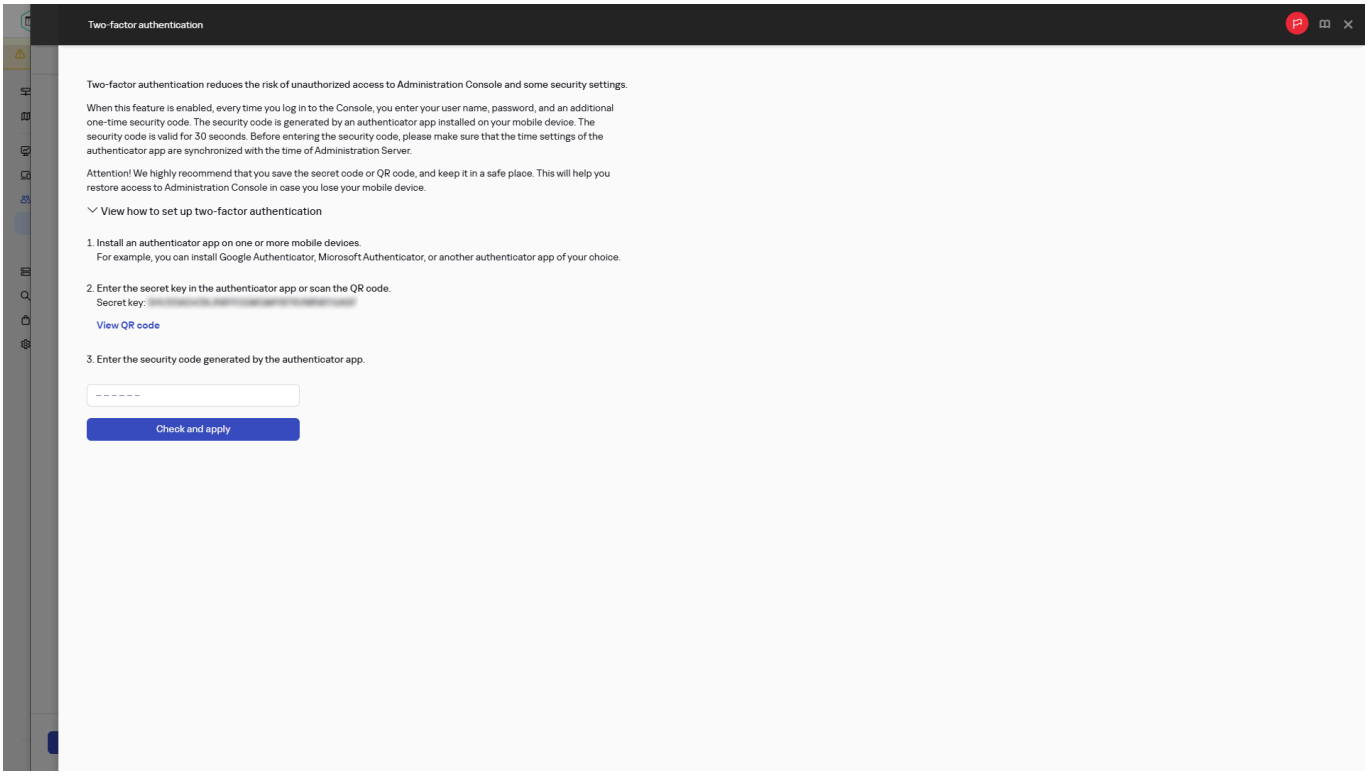


为当前用户账户重新生成双重身份验证密钥

a. 如果您的账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证安全码。

b. 在**双重身份验证**窗口中，点击**查看如何建立双重身份验证**，然后点击**查看二维码**。

c. 使用移动设备上的身份验证应用扫描二维码并接收一次性安全码。



a. 在**双重身份验证**窗口中，指定由身份验证应用生成的安全码，然后单击**检查和应用**按钮。

Rutoken OTP 配置

如果您使用 Rutoken OTP，则需要一台安装了 Rutoken OTP 应用程序的 Android 移动设备。Android 移动设备必须满足以下要求：

- 操作系统是 Android 7 或更高版本。
- NFC 模块可用且已启用。

在 Rutoken OTP 应用程序中，您必须配置以下参数：

- 扫描两步配置向导中显示的二维码。
- 将时间间隔设置为 30 秒。
- 选择 SHA1 作为算法。

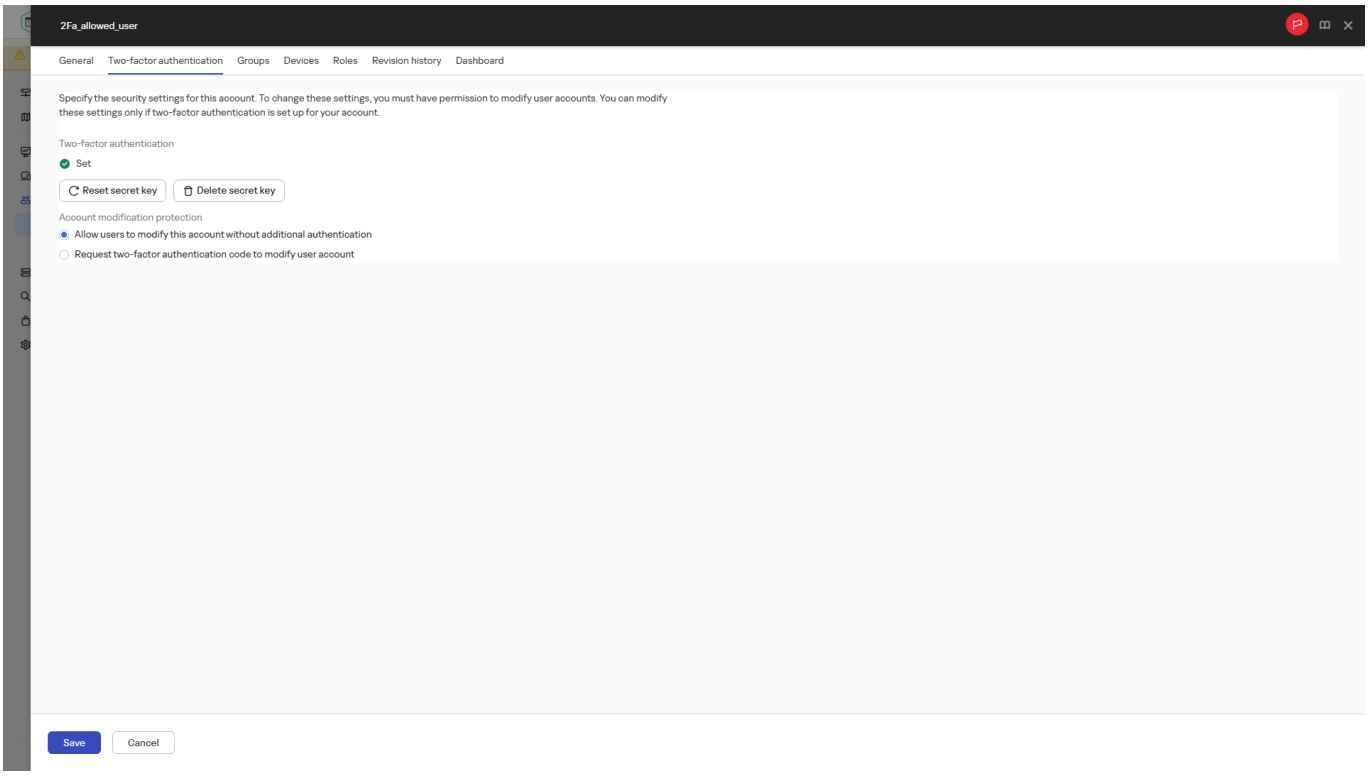
要配置 Rutoken OTP：

1. 将 Rutoken OTP 设备放在带有 NFC 模块的移动设备旁边。
2. 在 Rutoken OTP 应用程序中，按下“**连接令牌**”。
3. 在 Rutoken OTP 应用程序中，按下“**配置设置**”，然后按下“**保存 secret key**”。
   如果令牌成功连接到移动设备，Rutoken OTP 应用程序将显示以下状态消息：
   - **令牌已连接。**
   - **设置已配置。**
   - **密钥已保存。**
4. 在 Rutoken OTP 设备上，按下按钮。
   设备上会显示一个安全码。
5. 在 OSMP 控制台的两步验证窗口中，输入安全码。

您的帐户密钥已更改。

4. 若要重置其他帐户的密钥：

   a. 在**双重身份验证**选项卡上，单击**重置 Secret 密钥**按钮。



重置另一个用户账户的双重身份验证密钥

   a. 如果账户已开启防止未经授权修改的保护功能，您必须确认您有修改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

   b. 确认重置密钥，然后保存更改。

   当您为另一个账户重置密钥时，现有密钥将被删除，并且该用户账户将被添加到管理服务器属性中的双重身份验证允许列表中。下次登录时，该用户将能够生成新密钥。

   用户账户的密钥将被重置。

您可以删除 secret key，从而完全阻止用户登录 Web Console 和访问管理服务器。

若要删除密钥：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**用户**”选项卡。

2. 单击要删除密钥的内部用户帐户的名称。

   > 您无法删除自己帐户的密钥。

3. 在**双重身份验证**选项卡上，单击**删除 Secret 密钥**按钮。

4. 如果账户已开启防止未经授权修改的保护功能，您必须确认您有修改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

5. 确认删除密钥，然后保存更改。

   用户账户的密钥将被删除。

您可以通过将用户添加到管理服务器属性中的双重身份验证允许列表中来恢复访问权限。在这种情况下，用户下次登录时将能够生成新密钥。

从双重身份验证中排除账户

您可以将用户账户从双重身份验证中排除，允许这些账户即使未配置双重身份验证，也能登录管理服务器。对于在身份验证期间无法提供一次性安全码的集成账户，从双重身份验证中排除这些账户可能是有必要的。集成帐户用于通过OpenAPI运行脚本以及运行KUMA脚本。

如果您的帐户已配置双重身份验证，并且您在常规功能**常规功能**用户权限**用户权限修改对象**ACL权限，则可以修改排除项列表。

要从双重身份验证中排除某个用户账户：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在属性窗口的“**双重身份验证**”选项卡上，在“**双重身份验证排除项**”表中单击“**添加**”按钮。

3. 在打开的窗口中：

   a. 选择要排除的用户账户。

   b. 如果账户已开启防止未经授权修改的保护功能，您必须确认您有修改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

   c. 保存更改。

选定的用户账户将被排除在双重身份验证之外，若其 secret key 已存在，则会被一并删除。当您将 Kaspersky Next XDR Expert 升级到 2.0 或更高版本时，排除账户列表不会更改。如果排除项列表中的账户在 Kaspersky Next XDR Expert 的先前版本中有 secret key，则这些 secret key 将在 2.0 版本中被删除。

您可以从排除项列表中删除用户账户，以完全阻止用户登录 Web Console 和访问管理服务器。

要从排除项列表中删除用户账户：

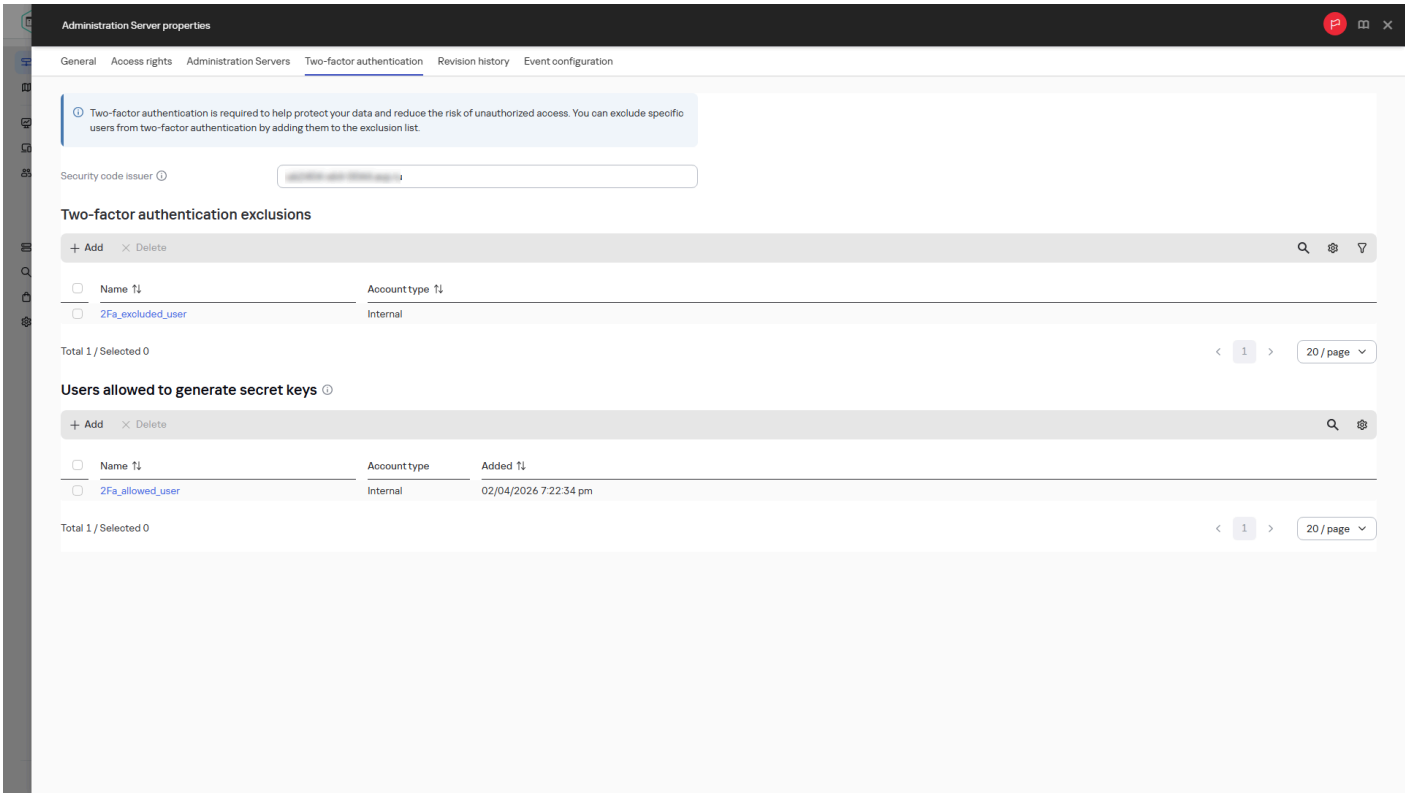
1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在属性窗口的“**双重身份验证**”选项卡上的**双重身份验证排除项**表中，选择要删除的用户账户，然后单击“**删除**”。

3. 如果账户已开启防止未经授权修改的保护功能，您必须确认您有修改此账户的权限。在**账户保护**窗口中，指定您自己帐户的登录凭据和双重身份验证的一次性安全码。

选定的用户账户将从排除项列表中删除。



配置双重身份验证排除列表

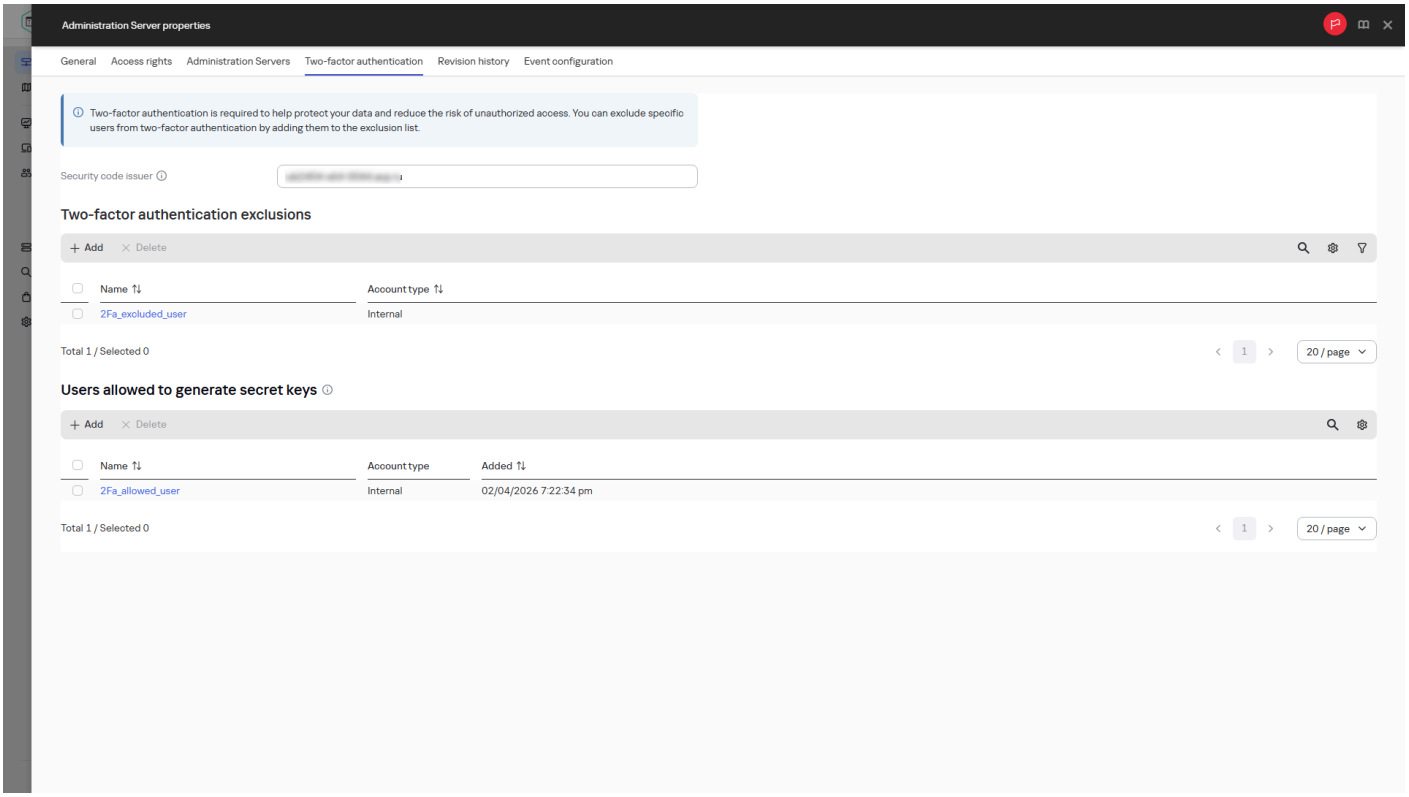
编辑安全码签发者名称

您可以为不同的管理服务器配置多个不同标识符（称为颁发者）。您可以更改安全码颁发者的名称，例如，当该管理服务器与其他管理服务器使用的安全码颁发者名称相似时。默认情况下，安全代码颁发者的名称与管理服务器的名称相同。

要指定安全代码颁发者的新名称：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在属性窗口的“**双重身份验证**”选项卡中，在“**安全码发布者**”字段中输入新名称，然后保存更改。

下次登录后，新的安全码颁发者名称会被分配给管理服务器。



指定安全码签发者的名称

允许的密码输入尝试次数

Kaspersky Next XDR Expert 用户输入无效密码的次数有限。达到限制后，用户账户被锁定一小时。

默认下，允许的最大密码输入尝试次数是 3。此数值是固定的，无法更改。

配置用户 SSO 会话和身份验证令牌的生命周期

令牌（或用户会话）的生命周期是指令牌或会话保持有效并可用于身份验证的一段时间。该时间段结束后，令牌或会话会自动过期，需要续期或重新登录。Kaspersky Next XDR Expert 允许您配置访问令牌、用于刷新访问令牌的刷新令牌以及空闲单点登录 (SSO) 会话的生命周期。通过缩短令牌或 SSO 会话的生命周期，可以降低令牌泄露时发生未经授权访问的风险。

您也可以在以多节点和单节点模式部署 Kaspersky Next XDR Expert 之前，通过配置文件中的相应参数（`tokenhub_access_token`、`tokenhub_refresh_token`、`credentials_session_ttl`）配置令牌的生命周期和 SSO 会话的空闲时间。如果在部署期间未指定这些设置，则使用以下默认值：

- 访问令牌（`tokenhub_access_token`）：1小时
- 刷新令牌（`tokenhub_refresh_token`）：24 小时
- 空闲 SSO 会话（`credentials_session_ttl`）：1小时。

要更改已部署解决方案中的设置，请使用 KDT 命令。

要检查当前生命周期值：

请在管理员主机上运行以下命令：

```
./kdt invoke iam -a getAuthTTLs
```

命令输出中会以 < 小时数 >h< 分钟数 >m< 秒数 >s 的形式显示访问令牌和刷新令牌的当前生命周期值，以及 SSO 会话的当前空闲时间值，例如：

- `2h`
- `23h30m`
- `12h55m`

要配置访问令牌的生命周期：

请在管理员主机上运行以下命令：

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_access_token=< 时间段 >
```

其中，`< time_period >` 表示所需的时间段，以小时、分钟和秒为单位。例如，`1h` 或 `1h30m`。对于访问令牌，`< time_period >` 的最小值为 `5m`，最大值为 `2h`。

要配置刷新令牌的生命周期：

请在管理员主机上运行以下命令：

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_refresh_token=< time_period >
```

其中，`< time_period >` 表示所需的时间段，以小时、分钟和秒为单位。例如，`24h` 或 `720h30m`。对于刷新令牌，< 时间段 > 的最小值为 `12m`，最大值为 `4320h`。

要配置空闲单点登录会话的生命周期：

在管理员主机上，运行以下命令：

```
./kdt invoke iam -a setAuthTTLs --param credentials_session_ttl=< time_period >
```

其中，`<time_period>` 表示所需的时间段，以小时、分钟和秒为单位。例如，`2h` 或 `1h30m`。对于空闲 SSO 会话，< 时间段 > 的最小值为 `5m`，最大值为 `96h`。

要一次性配置所有参数的生命周期：

请在管理员主机上运行以下命令：

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_access_token=<time_period> --param tokenhub_refresh_token=<time_period> --param credentials_session_ttl=<time_period>
```

其中，`<time_period>` 表示所需的时间段，以小时、分钟和秒为单位。

身份验证令牌和 SSO 会话的生命周期已配置完成。如果输入的值超出最小值和最大值限制，则会被替换为默认值。

新配置的生命周期仅适用于保存更改后创建的令牌和会话。活动令牌和会话将根据其颁发时生效的生命周期参数值过期。

删除用户或安全组

> 您仅可以删除内部用户或内部安全组。

要删除用户或安全组：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**用户**”或“**组**”选项卡。
2. 选择您要删除的用户或安全组旁边的复选框。

   > 应该始终至少有一个用户配置了双重身份验证，以便该用户可以管理双重身份验证允许列表和排除列表。

3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**确定**”。

   用户或安全组被删除。

更改用户账户密码

如果当前密码即将过期或者您想使用更安全的密码，则可能需要更改用户账户的密码。

密码必须符合以下规则：

- 密码长度必须为10到256个字符。
- 密码必须包含以下各组中的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ~ " ( ) < > ;)
- 密码不得包含任何空白字符或 Unicode 字符。

更改内部用户账户的密码

要编辑内部用户账户的密码：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击您要编辑的用户账户名称。
3. 在打开的用户设置窗口的**常规**选项卡上，单击**更改密码**按钮。
4. 为连接到 Open Single Management Platform 的用户设置新密码。
   要查看输入的密码，请单击👁。
5. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定在常规功能：用户权限功能区域中具有修改对象 ACL权限的账户的凭据。
6. 使用移动设备上的身份验证应用来生成一次性安全码。

首次登录时强制更改密码

您可以要求用户在首次登录 Open Single Management Platform 控制台时更改密码。如果为多个新账户设置了相同的临时密码，建议使用此选项，因为它可以确保每个用户在首次登录时设置自己的密码。

要强制用户在首次登录时更改密码：

1. 在主菜单中，转到**设置** → **身份验证策略**，然后启用**首次登录时强制更改密码**选项。
2. 保存更改。

已启用首次登录时强制更改密码。

是否强制更改密码是在创建用户账户时确定的，不会追溯适用：

- 启用此选项时创建的账户在首次登录后始终需要更改密码，即使此选项后来被禁用也是如此。
- 禁用此选项时创建的账户在首次登录后不需要更改密码，即使此选项后来被启用也是如此。

配置密码有效期

您可以配置用户账户的密码有效期，以确保更频繁地更改密码。默认情况下已启用该选项。

要更改密码有效期：

1. 在主菜单中，转到**设置** → **身份验证策略**，然后启用**强制定期更改密码**选项。
2. 在**密码有效期(天)**输入字段中，指定密码过期前的时间段。默认密码有效期为 365 天。
3. 保存更改。

密码有效期已更改。

在登录页面添加自定义消息区块

您可以在登录页面添加自定义消息区块，以便在授权前向用户显示重要信息。例如，您可以通知用户为确保信息安全而采取的措施。

要添加自定义消息区块：

1. **创建消息区块字符串**。

   要创建消息区块字符串：

   1. 为您的消息区块编写HTML代码，例如：

      ```
      <div>
        <h4>Protected system of ACME Corporation </h4>
        <p>Only authorized employees are allowed to work with the system.</p>
      </div>
      ```

      不支持添加图片。

      将此代码保存在文件中，例如markup.html。

2. 在Base64中对HTML进行编码。在Linux中，编码命令如下：

```
base64 -w 0 markup.html > banner.b64
```

该命令返回一个编码字符串，例如：

```
PGRpdj4KPGg0PtCX0LDRidC40YnQtdC90L3QsNGPINGB0LjRgdGC0LXQvNCwINCe0J7QniDCq9Cg0L7QvNCw0YjQutCwwrs8aDQ+CjxwPtCaIN(
```

2. 将字符串添加到Kaspersky Next XDR Expert配置中。您可以通过不同的方式将消息区块字符串添加到配置中：

- **在初始设置期间添加消息区块**

  要在初始设置期间添加消息区块：

  1. 在运行Kaspersky Next XDR Expert安装程序之前，请将以下行添加到param.yaml文件的`parameters`部分：

     ```
     - name: login_markup_b64
       source:
       value: "<以Base64编码的消息区块字符串>"
     ```

  2. 运行Kaspersky Next XDR Expert安装程序。

- **在更新期间添加消息区块**

  要在升级期间添加消息区块：

  1. 在管理员主机上，使用以下命令导出当前配置文件：

     ```
     ./kdt ec -e <configuration_file_name_with_path>
     ```

     配置文件的当前版本将以指定的名称保存到指定的目录中。

  2. 在导出的配置文件的`parameters`部分，添加以下行：

     ```
     - name: login_markup_b64
       source:
       value: "<以Base64编码的消息区块字符串>"
     ```

  3. 升级Kaspersky Next XDR Expert和Bootstrap组件。运行升级命令时，使用`-i`标志指定步骤1中导出的配置文件的完整路径：

     ```
     ./kdt apply -k <XDR 更新存档的完整路径> --force --accept-eula -i <带路径的配置文件名>
     ```

- **通过命令行添加消息区块**

  要通过命令行添加消息区块：

  1. 将ConfigMap导出到文件：

     ```
     kubectl get configmap credentials -n iam -o yaml > credentials.yaml
     ```

     Credentials.yaml文件包含您需要修改的初始配置。

2. 将编码的消息区块字符串插入到creents.yaml中：

```
sed -i 's|public:\\n|public:\\n      login_markup_b64: \\"'"$(sed 's|[\/&\\]|\\&|g'
banner.b64)"'\\"\\n|' credentials.yaml
```

此命令会查找包含“public:\n”的行，并在其后立即插入`login_markup_b64`字段。

3. 使用任何文本编辑器，确保`login_markup_b64`参数前后正好各有 6 个空格字符，并且引号已正确转义。例如：

```
前面 6 个空格字符 login_markup_b64:
\"PGRpdj4KICA8aDQ+WW91ckNvbXBhbnkgU2VjdXJlIFN5c3RlbTwvaDQ+CiAgPHA+T25seSBhdXRob3JpemVkIGVtcGxveWVlcyBhcmUgY
后面 6 个空格字符
```

4. 将您的本地更改应用于Kubernetes集群：

```
kubectl apply -f credentials.yaml
kubectl -n iam rollout restart deployment credentials
```

如果您之后想要编辑或删除消息区块：

1. 运行以下命令：

```
kubectl edit configmap credentials -n iam
```

2. 更改`login_markup_b64`参数的值或删除该参数。

3. 将您的本地更改应用于Kubernetes集群：

```
kubectl apply -f credentials.yaml
kubectl -n iam rollout restart deployment credentials
```

- **通过IDE Lens添加消息区块**

要通过IDE Lens添加消息区块：

1. 下载并安装IDE Lens。

2. 复制`~/.kdt/cluster.config`文件的内容。

3. 在 Lens IDE 中，前往**本地 Kubeconfigs → + → 通过粘贴添加 kubeconfig**部分，然后粘贴`cluster.config`文件的内容。

4. 打开添加的命名空间（`iam`），然后前往**配置→配置映射**，找到`credentials`配置映射。

5. 打开`credentials`配置映射，并在末尾添加以下行（无需缩进）：

```
credentials.server.public.login_markup_b64: "<以Base64编码的您的消息区块字符串>"
```

例如：

```
credentials.server.public.login_markup_b64:
"PGRpdiBzdHlsZT0idGV4dC1hbGlnbjogY2VudGVyOyI+CiAgPGltZyBzcmM9ImZpbGU6Ly8vaG9tZS90b29yLzUwLmpwZyIgYWx0PSJTZW
```

6. 单击“**保存**”按钮。

7. 重新加载pod：

```
kubectl -n iam rollout restart deployment credentials
```

要稍后编辑或删除消息区块：

1. 重复上述步骤1到4。

2. 打开`credentials`配置映射，并编辑或删除`login_markup_b64`参数。

3. 单击“**保存**”按钮。

4. 重新加载pod：

```
kubectl -n iam rollout restart deployment credentials
```

应用新配置后，您的自定义消息区块将显示在登录页面上。

创建用户角色

要创建用户角色：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。

2. 单击**添加**。

3. 在打开的“**新角色名称**”窗口中，输入新角色名称。

4. 单击“**确定**”应用更改。

5. 在打开的角色属性窗口中，更改角色设置：

- 在“**常规**”选项卡上，编辑角色名称。
  您无法编辑预定义角色名称。

- 在“**设置**”选项卡上，编辑角色范围和策略以及与角色关联的配置文件。
- 在“**访问权限**”选项卡上，编辑卡巴斯基应用程序的访问权限。

6. 单击“**保存**”保存更改。

新角色出现在用户角色列表。

编辑用户角色

要编辑用户角色：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。
2. 单击您要编辑的角色名称。
3. 在打开的角色属性窗口中，更改角色设置：
   - 在“**常规**”选项卡上，编辑角色名称。
     您无法编辑预定义角色名称。
   - 在“**设置**”选项卡上，编辑角色范围和策略以及与角色关联的配置文件。
   - 在“**访问权限**”选项卡上，编辑卡巴斯基应用程序的访问权限。
4. 单击“**保存**”保存更改。

更新的角色出现在用户角色列表。

编辑用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

要添加用户、安全组和管理组到用户角色范围，您可以使用以下方法之一：

方法 1：

1. 在主菜单中，转至**用户和角色**→**用户和组**，然后选择**用户**或**组**选项卡。
2. 选择您要添加到用户角色范围的用户或安全组旁边的复选框。
3. 单击“**分配角色**”按钮。
   角色分配向导启动。使用“**下一步**”按钮继续向导操作。
4. 在“**选择角色**”步骤中，选择要分配的用户角色。

5. 在“**定义范围**”步骤中，选择要添加到用户角色范围的管理组。

6. 单击“**分配角色**”按钮关闭窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

方法 2：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。

2. 单击您要定义范围的角色名称。

3. 在打开的角色属性窗口中，选择“**设置**”选项卡。

4. 在“**角色范围**”区域中，单击“**添加**”。
角色分配向导启动。使用“**下一步**”按钮继续向导操作。

5. 在“**定义范围**”步骤中，选择要添加到用户角色范围的管理组。

6. 在“**选择用户**”步骤中，选择要添加到用户角色范围的用户和安全组。

7. 单击“**分配角色**”按钮关闭窗口。

8. 单击“**关闭**”按钮（×）以关闭角色属性窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

方法 3：

1. 在主菜单中，单击管理服务器名称。
管理服务器属性窗口将打开。

2. 在“**访问权限**”选项卡上，选中要添加到用户角色范围的用户或安全组名称旁边的复选框，然后单击“**角色**”按钮。
您不能同时选择多个用户或安全组。如果您选择了多个条目，“**角色**”按钮将被禁用。

3. 在“**角色**”窗口中，选择要分配的用户角色，然后应用并保存更改。
所选用户或安全组被添加到用户角色范围。

删除用户角色

要删除用户角色：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。

2. 选择您要删除的角色旁边的复选框。

3. 单击“**删除**”按钮。

4. 在打开的窗口中，单击“**确定**”。

用户角色被删除。

关联策略配置文件到角色

您可以关联用户角色到策略配置文件。此种情况下，该策略配置文件的激活规则基于角色：策略配置文件对具有指定角色的用户可用。

例如，策略禁止在管理组的所有设备上运行 GPS 导航软件。GPS 导航软件仅在“用户”管理组中的单个设备上是必须的——该设备属于导游。此种情况下，您可以分配“导游”角色给其所有者，然后创建一个策略配置文件，允许 GPS 导航软件仅在分配了“导游”角色的用户的设备上运行。所有其他策略设置被保留。仅带有“导游”角色的用户将被允许运行 GPS 导航软件。然后，如果其他员工被分配了“导游”角色，该新员工也在组织的设备上运行导航软件。运行 GPS 导航软件在相同管理组的其他设备上仍将被禁止。

要关联角色到策略配置文件：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。

2. 选择您要关联策略配置文件的角色名称。

   角色属性窗口打开，在其中已选择“**常规**”选项卡。

3. 选择“**设置**”选项卡并向下滚动至“**策略**”区域。

4. 单击**编辑**。

5. 要关联角色到：

   - **现有策略配置文件** — 单击所学策略名称旁边的臂章图标(>)，然后选择您要关联角色的配置文件旁边的复选框。

   - **新策略配置文件**：

     a. 选择您要创建配置文件的策略旁边的复选框。

     b. 单击**新策略配置文件**。

     c. 为新配置文件指定名称并对配置文件设置进行配置。

     d. 单击“**保存**”按钮。

     e. 选择新配置文件旁边的复选框。

6. 单击**分配到角色**。

配置文件被关联到角色并显示在角色属性中。配置文件自动应用到分配了该角色的用户的任意设备。

配置 Kerberos 域身份验证

Kaspersky Next XDR Expert 使您能够通过 Kerberos 协议使用域身份验证。域身份验证可让您在 OSMP Console 中启用安全身份验证，而无需在公司网络上重新输入密码（单点登录）。

您必须首先配置域控制器以使用 Kerberos 并生成 keytab 文件。要了解更多信息，请参阅您的域控制器的文档。

Microsoft Active Directory支持SCRIL（交互式登录需要智能卡）。

为 FreeIPA 和 AldPro 生成 keytab 文件

要生成 keytab 文件，请执行以下操作：

1. 创建一个用户账户，供 IAM 用于访问域控制器。
2. 如果管理服务器位于 FreeIPA/AldPro 域之外，请添加 DNS 记录条目和主机条目：

```
ipa dnsrecord-add <zoneName> <recordName> --a-rec <Administration Server IP address>
ipa host-add --password=<password> <Administration Server host address>
```

3. 为管理服务器创建 HTTP 服务时，请指定 PAC 类型：

```
ipa service-add HTTP/<console_host>.<smp_domain>@<DOMAIN WRITTEN IN CAPITAL LETTERS> --ok-to-auth-as-
delegate=true --pac-type PAD
```

其中，`<console_host>` 是服务主机名，`<smp_domain>` 是域名。服务主机名和域名是服务 FQDN 的一部分。例如，如果 `console_host` 变量的值为 `console`，并且 `smp_domain` 变量的值为 `smp.local`，则提供对 OSMP 控制台的访问权限的服务的完整名称为 `console.smp.local`。

4. 指定用于身份验证的用户账户：

```
ipa service-allow-retrieve-keytab HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN CAPITAL LETTERS>
--user=<user>
```

5. 导出 keytab 文件：

```
ipa-getkeytab -s <domain controller address> -p HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN
CAPITAL LETTERS> -k /tmp/h.keytab
```

为 Microsoft Active Directory 生成 keytab 文件

要生成 keytab 文件，请执行以下操作：

1. 创建一个用户账户，供 IAM 用于与域控制器通讯。
2. 为该用户账户启用以下选项：
   - **用户无法更改密码**
   - **Kerberos AES 256 位加密**

   您可以启用**密码永不过期**选项，以避免每次密码过期时都重新发放 keytab 文件。
3. 为用户账户添加服务主体名称 (SPN)：

```
setspn -S HTTP/<> <DOMAIN WRITTEN IN CAPITAL LETTERS>\<user>
```

4. 导出 keytab 文件：

```
ktpass -out C:\<folder>\<keytab file name> -princ HTTP/<console_host>.<smp_domain>@<DOMAIN WRITTEN IN CAPITAL
LETTERS> -mapuser <user>@<DOMAIN WRITTEN IN CAPITAL LETTERS> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
<user password> -mapop set
```

   其中，`<console_host>` 是服务主机名，`<smp_domain>` 是域名。服务主机名和域名是服务 FQDN 的一部分。例如，如果 `console_host` 变量的值为 `console`，并且 `smp_domain` 变量的值为 `smp.local`，则提供对 OSMP 控制台的访问权限的服务的完整名称为 `console.smp.local`。

为 Samba 生成 keytab 文件

要生成 keytab 文件，请执行以下操作：

1. 创建一个用户账户，供 IAM 用于与域控制器通讯：

```
samba-tool user add <user>
```

2. 将 SPN 添加到用户账户：

```
samba-tool spn add HTTP/<console_host>.<smp_domain> <user>
```

   其中，`<console_host>` 是服务主机名，`<smp_domain>` 是域名。服务主机名和域名是服务 FQDN 的一部分。例如，如果 `console_host` 变量的值为 `console`，并且 `smp_domain` 变量的值为 `smp.local`，则提供对 OSMP 控制台的访问权限的服务的完整名称为 `console.smp.local`。

3. 导出 keytab 文件：

```
samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<console_host>.<smp_domain>
```

启用 Kerberos 域身份验证

要启用 Kerberos 域身份验证：

1. 执行域控制器轮询。
2. 在主菜单中，转到 **设置** → **单点登录** 部分。
3. 启用“**Kerberos 身份验证**”选项。
4. 上传 keytab 文件。
5. 为域用户分配角色，以授予对 OSMP Console 的访问权限。
   已为域用户启用 Kerberos 域身份验证。

更新 Kaspersky 数据库和应用程序

您只能安装已通过认证程序的应用程序模块更新。启用模块自动更新会导致应用程序失去认证状态。

安装未按既定程序通过认证测试的 Kaspersky 应用程序可执行模块更新（消除已知漏洞的更新除外），会导致应用程序失去认证状态。

该部分描述了定期更新以下内容必须采取的步骤：

- Kaspersky 数据库和软件模块
- 已安装卡巴斯基应用程序，包括 Open Single Management Platform 组件和安全应用程序

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

方案：定期更新 Kaspersky 数据库和应用程序

本部分提供定期更新 Kaspersky 数据库、软件模块和应用程序的方案。在您完成配置网络保护方案后，您必须维持保护系统的可靠性以确保管理服务器和受管理设备保持受保护状态以防范各种威胁，包括病毒、网络攻击和钓鱼攻击。

网络保护通过更新以下内容保持最新：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Next XDR Expert 组件和安全应用程序

当您完成方案时，您可以确保：

- 您的网络受到最新 Kaspersky 软件的保护，包括 Kaspersky Next XDR Expert 组件和安全应用程序。
- 对网络安全至关重要的反病毒数据库和其他 Kaspersky 数据库始终保持最新。

先决条件

受管理设备必须连接到管理服务器。如果未建立连接，请考虑手动更新 Kaspersky 数据库和软件模块，或者直接从 Kaspersky 更新服务器更新。

管理服务器必须连接到互联网。

在您开始之前，确保您已做了如下：

1. 根据通过 OSMP 控制台部署卡巴斯基应用程序的方案，将卡巴斯基安全应用程序部署到受管理设备。
2. 创建了配置了所有所需策略、策略配置文件和任务，根据网络保护配置方案。
3. 分配了适当数量的分发点，与受管理设备和网路拓扑一致。

更新 Kaspersky 数据库和应用程序分阶段进行：

1. **选择更新 scheme**

   您可以使用多种方案，将更新安装到 Open Single Management Platform 组件和安全应用程序中。选择一个或多个满足您网络需求的 scheme。

2. **创建管理服务器的“将更新下载至存储库”任务**

   手动创建*将更新下载至管理服务器存储库*任务。

   此任务用于从卡巴斯基更新服务器下载更新至管理服务器的存储库，同时更新卡巴斯基数据库以及 Open Single Management Platform 的软件模块。更新被下载后，它们可以被传播到受管理设备。

   如果您的网络被分配了分发点，更新被从管理服务器存储库自动下载到分发点存储库。此种情况下，分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。

   使用说明：创建管理服务器的“将更新下载至存储库”任务

3. **创建“将更新下载至分发点存储库”任务（可选）**

   默认下，更新被从管理服务器下载到分发点。您可以将 Open Single Management Platform 配置成直接从卡巴斯基更新服务器下载更新到分发点。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

   当您的网络已分配分发点并已创建“*将更新下载至分发点存储库*”任务时，分发点从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库下载。

   操作说明：创建将更新下载至分发点存储库的任务

4. **配置分发点**

   当您的网络已分配分发点时，确保在所有所需分发点的属性中启用“**已启用**”选项。当该选项对分发点禁用时，包含在分发点范围中的设备从管理服务器存储库下载更新。

5 通过使用差异文件优化更新过程（可选）

您可以使用差异文件优化管理服务器和受管理设备之间的流量。启用此功能后，管理服务器或分发点将下载差异文件，而不是整个 Kaspersky 数据库或软件模块文件。diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。因此，diff 文件比整个文件占用更少的空间。这导致降低管理服务器之间或分发点和受管理设备之间的流量。要使用此功能，请在“*将更新下载至管理服务器存储库*”任务和/或“*将更新下载至分发点存储库*”任务的属性中启用“**下载差异文件**”选项。

使用说明：使用差异文件更新 Kaspersky 数据库和软件模块

6 为安全应用程序配置更新的自动安装

为受管理应用程序创建“*更新*”任务，以提供对软件模块和 Kaspersky 数据库（包括反病毒数据库）的及时更新。要确保定期更新，我们建议您在配置任务计划时选择“**当新更新下载至存储库时**”选项。

如果更新需要查看和接受最终用户授权许可协议的条款，您需要先接受它们。此后，更新可以被传播到受管理设备。

7 批准和拒绝受管理的卡巴斯基应用程序的更新

默认下，下载的软件更新具有*未定义*状态。您可以更改状态到*已批准*或*已拒绝*。批准的更新总是被安装。如果更新受管理的卡巴斯基应用程序时需要查看和接受最终用户授权许可协议的条款，则您需要先接受这些条款。此后，更新可以被传播到受管理设备。您设置了*已拒绝*状态的更新将不被安装到设备。如果受管理应用程序此前安装了已拒绝的更新，Open Single Management Platform 将尝试从所有设备上卸载该更新。

批准和拒绝更新仅适用于安装在 Windows 客户端设备上的网络代理和受管理的卡巴斯基应用程序。不支持管理服务器、OSMP 控制台和管理 Web 插件的无缝更新。

操作说明：批准和拒绝软件更新

有时，网络代理更新后，您可能会被提示重新启动受管理设备。如果显示所需重启通知，单击通知中的**查看设备**链接，选中要重新启动的设备旁边的复选框，然后单击**重新启动**按钮以完成网络代理更新。

结果

场景完成后，Kaspersky Next XDR Expert 将配置为在更新下载到管理服务器的存储库后更新 Kaspersky 数据库。您然后可以继续监控网络状态。

关于更新 Kaspersky 数据库、软件模块和应用程序

为了确保管理服务器和受管理设备的保护是最新的，您必须提供以下内容的定期更新：

- Kaspersky 数据库和软件模块

  在下载卡巴斯基数据库和软件模块之前，Open Single Management Platform 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保更新反病毒数据库并保持受管理设备的安全级别是必要的。

- 已安装卡巴斯基应用程序，包括 Open Single Management Platform 组件和安全应用程序

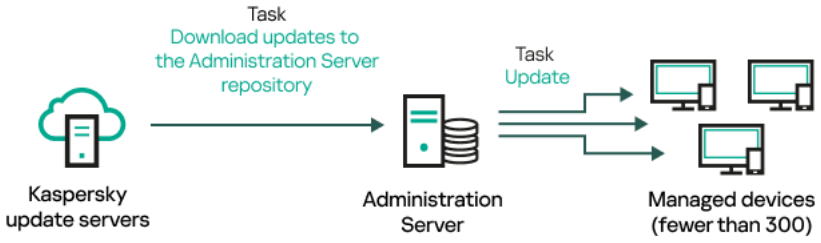
  通过 Open Single Management Platform，您可以自动更新安装在 Windows 客户端设备上的网络代理和卡巴斯基应用程序。不支持管理服务器、OSMP 控制台和管理 Web 插件的无缝更新。要更新这些组件，您必须从卡巴斯基网站下载最新版本，然后手动进行安装。

取决于您网络的配置，您可以使用以下方案来下载和分发所需更新到受管理设备：

- 通过使用单个任务：*将更新下载至管理服务器存储库*
- 通过使用两个任务：
  - "*将更新下载至管理服务器存储库*"任务
  - 创建"*将更新下载至分发点存储库*"任务
- 通过共享文件夹或 FTP 服务器手动操作
- 直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security
- 如果管理服务器没有互联网连接，则通过网络文件夹进行操作

使用"将更新下载至管理服务器存储库"任务

在此方案中，Open Single Management Platform 通过"*将更新下载至管理服务器存储库*"任务来下载更新。在单一网段包含少于 300 台受管理设备或每个网段包含少于 10 台受管理设备的小网络中，更新直接从管理服务器存储库被分发到受管理设备（参见下图）。



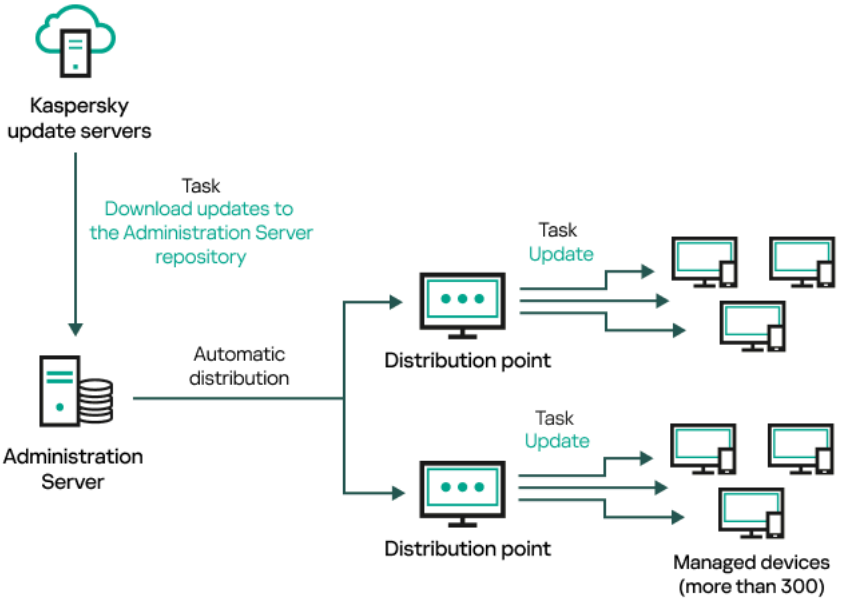
通过使用"*将更新下载至管理服务器存储库*"任务更新，而不使用分发点

更新源不仅可以是卡巴斯基更新服务器，还可以是网络文件夹。

默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

如果您的网络中的单一网段包含 300 台或更多受管理设备，或者每个网段包含多于 9 台受管理设备，我们建议您使用分发点传播更新到受管理设备（参见下图）。分发点降低管理服务器负载并优化管理服务器和受管理设备之间的流量。您可以计算数字并配置您网络所需的分发点。

此种方案中，更新被从管理服务器存储库自动下载到分发点存储库。分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。



通过使用"*将更新下载至管理服务器存储库*"任务更新，并使用分发点

"*将更新下载至管理服务器存储库*"任务完成后，Kaspersky Endpoint Security 的 Kaspersky 数据库和软件模块的更新即下载到管理服务器存储库。这些更新通过Kaspersky Endpoint Security *更新*任务安装。

> "*将更新下载至管理服务器存储库*"任务在虚拟管理服务器上不可用。虚拟管理服务器的存储库将显示已下载至主管理服务器的更新。

您可以配置在测试设备集上进行更新的操作和错误验证。如果验证成功，更新被分发到其他受管理设备。

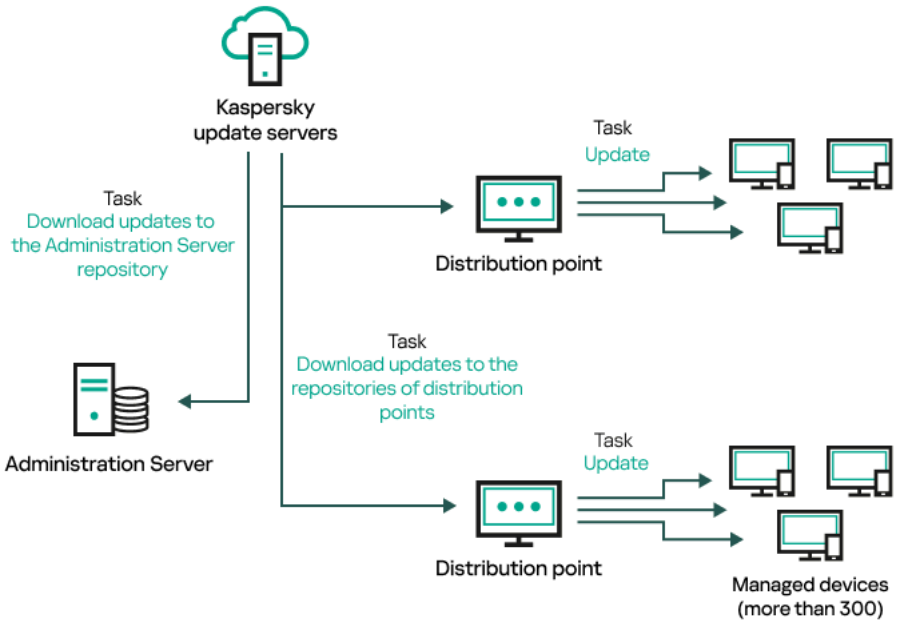
每个卡巴斯基应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行"*将更新下载至管理服务器存储库*"任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 应用程序 ID 和版本
- 应用程序启动 ID
- 活动密钥 ID
- "*将更新下载至管理服务器存储库*"任务运行 ID

传输的信息都不包含个人数据或其他机密数据。AO Kaspersky Lab 依照法律需求保护信息。

使用两个任务：“将更新下载至管理服务器存储库”任务和“将更新下载至分发点存储库”任务

您可以直接从 Kaspersky 更新服务器下载更新到分发点存储库，而不是从管理服务器存储库，然后分发更新到受管理设备（参见下图）。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。



使用“*将更新下载至管理服务器存储库*”和“*将更新下载至分发点存储库*”任务进行更新

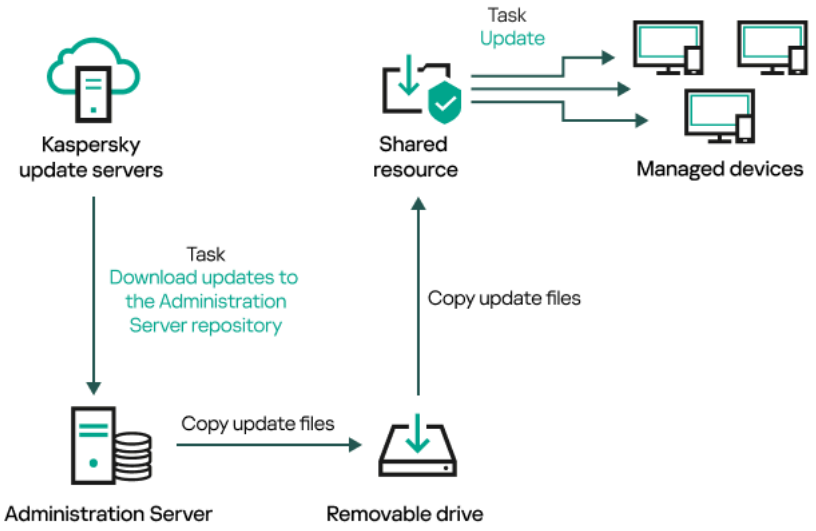
默认下，管理服务器和分发点与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器和/或分发点使用 HTTP 协议，而不是 HTTPS。

要实施此方案，除了“*将更新下载至管理服务器存储库*”任务外，请创建“*将更新下载至分发点存储库*”任务。此后，分发点将从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库。

此方案也需要配置“*将更新下载至管理服务器存储库*”任务，因为此任务用于为 Open Single Management Platform 下载卡巴斯基数据库及软件模块。

通过共享文件夹或 FTP 服务器手动操作

如果客户端设备未连接到管理服务器，您可以使用共享资源作为卡巴斯基数据库、软件模块和应用程序的更新源。在此方案中，您需要将所需更新从管理服务器存储库复制到可移动驱动器，然后将更新复制到在 Kaspersky Endpoint Security 设置中指定为更新源的共享资源（参见下图）。



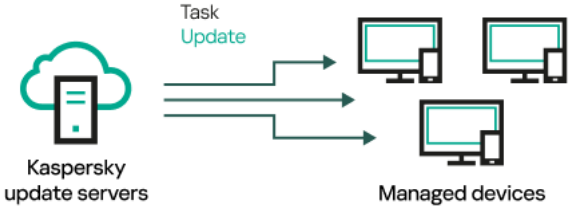
通过共享文件夹或 FTP 服务器执行更新

有关 Kaspersky Endpoint Security 中更新源的更多信息，请参见以下帮助文档：

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

直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security

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



直接从 Kaspersky 更新服务器更新安全应用程序

在此方案中，安全应用程序不使用 Open Single Management Platform 提供的存储库。要直接从 Kaspersky 更新服务器接收更新，请在安全应用程序中指定 Kaspersky 更新服务器作为更新源。有关这些设置的详细信息，请参见以下帮助文档：

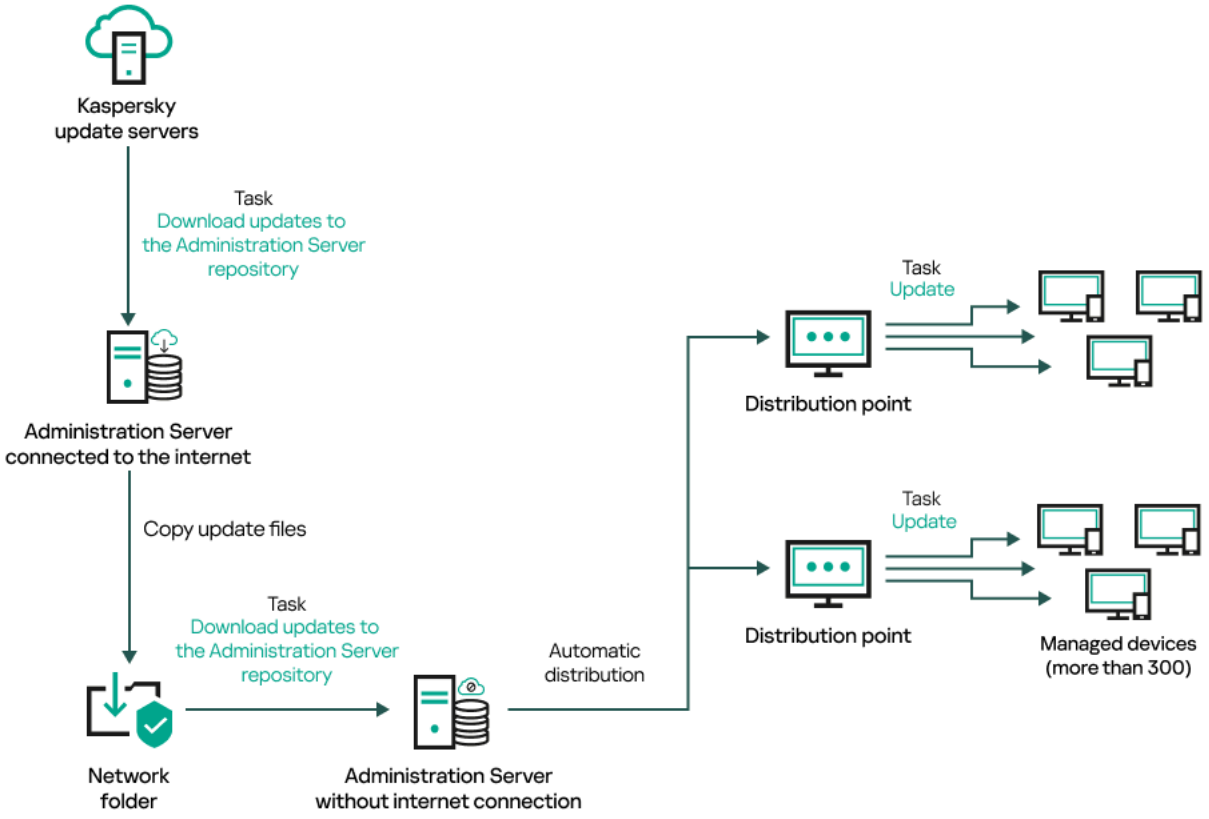
- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Endpoint Security for Windows 帮助

如果管理服务器没有互联网连接，则通过网络文件夹进行操作

如果管理服务器没有互联网连接，您可以配置“*将更新下载至管理服务器存储库*”任务以从网络文件夹下载更新。在这种情况下，必须不时地将所需的更新文件复制到指定文件夹。例如，您可以从以下来源之一复制所需的更新文件：

- 具有互联网连接的管理服务器（请参见下图）

  由于管理服务器只下载安全应用程序请求的更新，管理服务器管理的安全应用程序集（有互联网连接的应用程序和没有互联网连接的应用程序）必须匹配。



如果管理服务器没有互联网连接，则通过网络文件夹进行更新

- 卡巴斯基更新实用程序

  由于此实用程序使用旧方案下载更新，请打开“*将更新下载至管理服务器存储库*”任务，然后启用“*使用旧方案下载更新*”选项。如有必要，您还可以配置*自动下载更新请求文件*选项，以便卡巴斯基更新实用程序仅下载所需的更新。

创建“将更新下载至管理服务器存储库”任务

“*将更新下载至管理服务器存储库*”任务允许您将卡巴斯基安全应用程序的数据库和软件模块的更新从卡巴斯基更新服务器下载到管理服务器存储库。任务列表中只能有一个“*将更新下载至管理服务器存储库*”任务。

完成“*将更新下载至管理服务器存储库*”任务并下载更新后，可以将它们传播到受管理设备。

如果您在集群中安装管理服务器，则会自动创建“*将更新下载至管理服务器存储库*”任务。

在向受管理设备分发更新之前，可以运行“*更新验证*”任务。这样可以确保管理服务器将正确安装下载的更新，并且安全级别不会由于更新而降低。要在分发更新之前对其进行验证，请配置“*将更新下载至管理服务器存储库*”任务设置中的“**运行更新验证**”选项。

要创建“将更新下载至管理服务器存储库”任务：

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明操作。
3. 对于 Kaspersky Next XDR Expert 应用程序，请选择“**将更新下载至管理服务器存储库**”任务类型。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 在**完成任务创建**页面上，您可以启用**创建完成时打开任务详情**选项以打开任务属性窗口并修改默认任务设置。或者，您可以稍后随时配置任务设置。
6. 单击“**完成**”按钮。

   任务被创建并显示在任务列表。
7. 单击创建的任务名称以打开任务属性窗口。
8. 在任务属性窗口中的“**应用程序设置**”选项卡上，指定以下设置：

   - **更新源**

     您可以使用卡巴斯基更新服务器或网络文件夹作为更新源。如果您要为辅助管理服务器或虚拟管理服务器创建任务，还可以选择本地目录或主管理服务器作为更新源。

     在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Open Single Management Platform 不需要您输入凭证。

   - **更新存储文件夹**

     用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

- **强制从属管理服务器更新**

  如果启用该选项，当新更新下载后管理服务器立刻在从属管理服务器上启动更新任务。更新任务通过使用在从属管理服务器上的任务属性中配置的更新源来启动。

  如果禁用此选项，从属管理服务器上的更新任务将根据计划启动。

  默认情况下已禁用该选项。

- **复制下载的更新到附加文件夹**

  管理服务器接收更新后，它复制它们到指定文件夹。如果您想要在您的网络上手动管理更新的分发，则使用该选项。

  例如，您可能要在以下情况下使用该选项：您组织的网络包含几个独立子网，且每个子网的设备不能访问其他子网。然而，所有子网中的设备都可以访问通用网络共享。此种情况下，您在子网之一设置管理服务器从 Kaspersky 更新服务器下载更新，启用该选项，然后指定该网络共享。对于其他管理服务器的"将更新下载至存储库"任务中，指定与更新源相同的网络共享。

  如果您选择将下载的更新复制到本地文件夹，则必须在已安装管理服务器的设备上指定文件夹。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

  选择位于基于 Linux 的管理服务器上的网络文件夹时，您必须预先确保已安装管理服务器的设备可以通过挂载该文件夹来访问该网络文件夹。对文件夹的访问使用 SMB 协议执行。

  默认情况下已禁用该选项。

- **下载差异文件**

  该选项启用下载 diff 文件功能。

  默认情况下已禁用该选项。

- **使用旧方案下载更新**

  Open Single Management Platform 根据新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用"**使用旧方案下载更新**"选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹作为更新源，并且该文件夹中的更新文件是由卡巴斯基更新实用程序使用旧方案下载的，则必须启用此选项。

  默认情况下已禁用该选项。

- **运行更新验证**

  管理服务器从源下载更新并将其保存到临时存储库，然后运行"**更新验证任务**"字段中定义的任务。如果任务成功完成，则将更新从临时存储库复制到管理服务器上的共享文件夹，然后分发到所有将管理服务器作为更新源的设备（启动具有"**当新更新下载至存储库时**"计划类型的任务）。只有在执行"*更新验证*"任务之后，将更新下载至存储库的任务才完成。

  默认情况下已禁用该选项。

- **自动下载更新请求文件**

  如果您想要卡巴斯基更新实用程序仅下载具有适当配置的所需更新，请启用此选项并指定 Kaspersky Next XDR Expert 将创建更新请求文件（其中包含有关要下载的更新的信息）的路径。更新请求文件包含用于版本控制的时间戳和 MD5 哈希。

  请确保禁用**使用旧方案下载更新**选项。

此外，必须配置卡巴斯基更新实用程序中的更新下载。

默认情况下指定以下路径：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml。如有必要，您可以更改默认名称（retranslation_request）和路径。

请求文件可以放在本地或共享文件夹中。使用共享文件夹时，您必须确保可以从安装了管理服务器的设备访问该文件夹。确保访问的方法和使用的工具取决于您的基础设施。

运行*将更新下载到管理服务器存储库*任务时，Kaspersky Next XDR Expert 会在您指定的路径中创建一个 .xml 格式的更新请求文件。卡巴斯基更新实用程序自动从请求文件中获取信息，然后仅下载所需的更新。如果卡巴斯基更新实用程序无法自动获取信息（例如，卡巴斯基更新实用程序无权访问 Kaspersky Next XDR Expert 在其中创建请求文件的文件夹），您必须使用第三方工具传输该文件。

9. 在任务属性窗口中的"**计划**"选项卡上，创建任务启动计划。如果必要，配置以下设置：

- **启动任务**：
  - **手动**（默认选择）

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期五于当前系统时间运行一次。

  - **每天(不支持夏令时)**

    任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

    我们不建议您使用该计划。这是 Kaspersky Next XDR Expert 实现向后兼容所必需的。

    默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **每月在所选工作日**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- 其他任务设置：

  - **运行错过的任务**

    该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

    如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

    如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

    默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- **如果任务运行超过该时间则停止**

  在指定时间段过后，任务被自动停止，无论它是否完成。

  如果您想要中断或停止执行时间太长的任务，则启用该选项。

  默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

10. 单击“**保存**”按钮。

    任务被创建和配置。

当管理服务器执行“*将更新下载至管理服务器存储库*”任务时，数据库和软件模块的更新将从更新源下载并存储在管理服务器中。如果您为管理组创建此任务，它将仅被应用到包含在指定管理组中的网络代理。

如果您通过代理服务器连接互联网，则必须在管理服务器属性中指定代理服务器地址。否则，“*将更新下载至管理服务器存储库*”任务将无法执行。

浏览已下载的更新

当管理服务器执行“*将更新下载至管理服务器存储库*”任务时，数据库和软件模块的更新将从更新源下载并存储在管理服务器中。您可以在“**卡巴斯基数据库和软件模块更新**”区域中查看下载的更新。

要查看已下载的更新，

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

可用更新列表被显示。

验证已下载的更新

安装更新到受管理设备之前，您可以先通过“*更新验证*”任务检查更新。作为“*将更新下载至管理服务器存储库*”任务的一部分，“*更新验证*”任务会自动执行。管理服务器从更新源下载更新，将其保存在临时存储库并执行“*更新验证*”任务。如果任务成功完成，更新将从临时存储库复制到管理服务器存储库。它们被分发到所有以该管理服务器为更新源的客户端设备。

如果“*更新验证*”任务的结果显示位于临时存储库中的更新是错误的，或“*更新验证*”任务发生错误，这些更新不会被复制到管理服务器存储库。管理服务器保留之前的更新集。此外，计划类型为“**当新更新下载至存储库时**”的任务也不会启动。如果新更新扫描成功完成，在下次启动“*将更新下载至管理服务器存储库*”任务时将执行这些操作。

如果在一台或多台测试设备上出现以下情况，那么更新集合就被认为是无效的：

- 发生了更新任务错误。
- 安全应用程序的实时保护状态在应用更新后更改。
- 运行按需扫描任务过程中发现了一个被感染的对象。
- Kaspersky 程序出现运行时错误。

如果在任何测试设备上未出现以上情况，该更新集就被认为是有效的，“*更新验证*”任务被认为已成功完成。

在开始创建“*更新验证*”任务之前，请执行先决条件：

1. 创建包含多台测试设备的管理组。您将需要此组来验证更新。

   建议使用网络中具有最可靠的保护和最常用的应用程序配置的设备。这种方法可提高扫描期间病毒检测的质量和可能性，并将误报的风险降至最低。如果在测试设备上检测到病毒，“*更新验证*”任务将被视为不成功。

2. 为 Open Single Management Platform 支持的应用程序（例如 Kaspersky Endpoint Security for Linux）创建更新和恶意软件扫描任务。创建更新和恶意软件扫描任务时，请指定具有测试设备的管理组。

   “*更新验证*”任务会在测试设备上依次运行更新和恶意软件扫描任务，以检查所有更新是否有效。此外，在创建“*更新验证*”任务时，您需要指定更新和恶意软件扫描任务。

3. 创建“*将更新下载至管理服务器存储库*”任务。

要使 Kaspersky Next XDR Expert 在将下载的更新分发到客户端设备之前对其进行验证：

1. 在主菜单中，转到“**任务**”。
2. 单击“**将更新下载至管理服务器存储库**”任务。
3. 在打开的任务属性窗口中，转到“**应用程序设置**”选项卡，然后启用“**运行更新验证**”选项。
4. 如果“*更新验证*”任务存在，请单击“**选择任务**”按钮。在打开的窗口中，在具有测试设备的管理组中选择“*更新验证*”任务。
5. 如果您先前未创建“*更新验证*”任务，请执行以下操作：

   a. 单击“**新任务**”按钮。

   b. 如果要更改预设名称，则在打开的“新任务向导”中指定任务名称。

c. 选择您先前创建的具有测试设备的管理组。

d. 首先，选择 Open Single Management Platform 支持的所需应用程序的更新任务，然后选择恶意软件扫描任务。

之后，会出现以下选项。我们建议将这些选项保持启用状态：

- **在数据库更新后重启设备**

  在设备上更新反病毒数据库后，建议重新启动设备。

  默认情况下已启用该选项。

- **在数据库更新和设备重启后检查实时保护状态**

  如果启用此选项，则“*更新验证*”任务将检查下载到管理服务器存储库的更新是否有效，以及在反病毒数据库更新和设备重启后保护级别是否降低。

  默认情况下已启用该选项。

e. 指定运行“*更新验证*”任务将使用的账户。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。

6. 单击“**保存**”关闭“*将更新下载至管理服务器存储库*”任务的属性窗口。

自动更新验证被启用。现在，您可以运行“*将更新下载至管理服务器存储库*”任务，它将从更新验证开始。

创建“将更新下载至分发点存储库”任务

您可以为管理组创建“*将更新下载至分发点存储库*”任务。该任务将为包含在指定管理组中的分发点运行。

您可以使用该任务，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

此任务需要从 Kaspersky 更新服务器下载更新到分发点的存储库。更新列表包含：

- Kaspersky 安全应用程序的数据库和软件模块的更新
- Kaspersky Next XDR Expert 组件更新
- Kaspersky 安全应用程序更新

更新被下载后，它们可以被传播到受管理设备。

*要创建“**将更新下载至分发点存储库**”任务，对于选定的管理组：*

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明操作。
3. 对于 Kaspersky Next XDR Expert 应用程序，在“**任务类型**”字段中选择“**将更新下载至分发点存储库**”。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

5. 选择一个选项按钮以指定管理组、设备分类或应用程序任务的设备。

6. 在“**完成任务创建**”步骤，如果要修改默认任务设置，请启用“**创建完成时打开任务详情**” 选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时更改默认设置。

7. 单击“**创建**”按钮。

   任务被创建并显示在任务列表。

8. 点击创建的任务的名称以打开任务属性窗口。

9. 在任务属性窗口的“**应用程序设置**”选项卡上，指定以下设置：

   - **更新源**

     以下资源可以用作分发点的更新源：

     - Kaspersky 更新服务器

       Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

       默认情况下已选中该选项。

     - 本地或网络文件夹

       包含最新更新的本地或网络文件夹。只有已安装的 SMB 共享才能用作网络文件夹。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

       > 在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Open Single Management Platform 不需要您输入凭证。

   - **更新存储文件夹**

     用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

   - **下载差异文件**

     该选项启用下载 diff 文件功能。

     默认情况下已禁用该选项。

   - **使用旧方案下载更新**

     Open Single Management Platform 根据新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

     例如，当指定本地或网络文件夹作为更新源，并且该文件夹中的更新文件是由卡巴斯基更新实用程序使用旧方案下载的，则必须启用此选项。

     默认情况下已禁用该选项。

10. 为任务启动创建计划。如果必要，配置以下设置：

- **启动任务**：
  - **手动**（默认选择）

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期五于当前系统时间运行一次。

  - **每天(不支持夏令时)**

    任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

    我们不建议您使用该计划。这是 Kaspersky Next XDR Expert 实现向后兼容所必需的。

    默认下，任务每天于当前系统时间运行一次。

  - **每周**

    任务每周在指定星期和指定时间运行。

  - **按星期中的天数**

    任务在每周指定日期的指定时间定期运行。

    默认情况下，任务在每周五 6:00:00 PM 运行。

  - **每月**

    任务定期运行，在指定月日的指定时间。

    在缺少指定日的月份，任务在最后一天运行。

    默认下，任务在每月的第一天运行，在当前系统时间。

- **每月在所选工作日**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是"**手动**"、"**一次**"或"**立即**"，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于"**手动**"、"**一次**"和"**立即**"计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

11. 单击“**保存**”按钮。

任务被创建和配置。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

执行“*将更新下载至分发点存储库*”任务时，数据库和软件模块的更新从更新源下载并存储在分发点存储库中。下载的更新将仅被包含在指定管理组的分发点和没有更新下载任务的更新代理使用。

添加“将更新下载至管理服务器存储库”任务的更新源

在创建或使用“将更新下载至管理服务器存储库”任务时，可以选择以下更新源：

- Kaspersky 更新服务器
- 主管理服务器

  此资源适用于为从属或虚拟管理服务器创建的任务。
- 本地或网络文件夹

  此资源适用于为从属或虚拟管理服务器创建的任务。
- 网络文件夹

在“*将更新下载至管理服务器存储库*”任务和“*将更新下载至分发点存储库*”任务中，如果选择受密码保护的本地或网络文件夹作为更新源，则用户身份验证不起作用。要解决此问题，首先挂载受密码保护的文件夹，然后指定所需的凭据，例如，通过操作系统。之后，您可以选择此文件夹作为更新下载任务中的更新源。Open Single Management Platform 不需要您输入凭证。

默认使用 Kaspersky 更新服务器，但您也可以从本地或网络文件夹下载更新。如果您的网络没有互联网访问权限，您可能希望使用文件夹。在这种情况下，您可以从 Kaspersky 更新服务器手动下载更新并将下载的文件放在所需的文件夹中。

您只能指定一个本地或网络文件夹路径。作为本地文件夹，您必须指定管理服务器所在设备上的文件夹。作为网络文件夹，您可以使用 FTP 或 HTTP 服务器，或者 SMB 共享。如果 SMB 共享需要身份验证，则必须提前使用所需的凭据将其挂载在系统中。我们建议不要使用 SMB1 协议，因为它不安全。

如果同时添加 Kaspersky 更新服务器和本地或网络文件夹，将首先从文件夹下载更新。如果下载时出错，将使用 Kaspersky 更新服务器。

如果包含更新的共享文件夹受密码保护，请启用“**指定账户以访问更新源的共享文件夹(如果有)**”选项并输入访问所需的账户凭据。

要添加更新源：

1. 在主菜单中，转到“**任务**”。
2. 单击**将更新下载至管理服务器存储库**。
3. 转到“**应用程序设置**”选项卡。
4. 在“**更新源**”行，单击“**配置**”按钮。
5. 在打开的窗口中，单击“**添加**”按钮。
6. 在更新源列表中，添加所需的源。如果选中“**网络文件夹**”或“**本地或网络文件夹**”复选框，请指定文件夹的路径。
7. 单击“**确定**”，然后关闭更新源属性窗口。
8. 在更新源窗口中，单击“**确定**”。
9. 单击任务窗口中的“**保存**”按钮。

现在更新将从指定的源下载到管理服务器存储库。

批准和拒绝软件更新

更新安装任务的设置可能需要对要安装的更新进行批准。您可以批准必须安装的更新并拒绝不能安装的更新。

例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些更新到客户端设备。

> 批准和拒绝更新仅适用于安装在 Windows 客户端设备上的网络代理和受管理应用程序。不支持管理服务器、OSMP 控制台和管理 Web 插件的无缝更新。要更新这些组件，您必须手动安装它们。

要批准或拒绝一个或几个更新：

1. 在主菜单中，前往**软件管理→卡巴斯基应用程序→无缝更新**。
   可用更新列表被显示。

   > 受管理应用程序的更新可能需要安装 Kaspersky Security Center 的特定最低版本。如果此版本高于当前版本，则会显示这些更新，但无法批准。此外，在升级 Kaspersky Security Center 之前，无法从此类更新创建安装包。系统会提示您将 Kaspersky Security Center 实例升级到所需的最低版本。

2. 如有必要，请单击“**查看和接受授权许可协议**”按钮来接受 EULA。

3. 选择您要批准或拒绝的更新。

4. 单击“**批准**”批准所选更新或单击“**拒绝**”拒绝所选更新。

   默认值是 *未定义*。

您分配了*已批准*状态的更新被放置在安装队列。

您分配了*已拒绝*状态的更新被从先前将其安装的设备上卸载（如果可能）。而且，它们将来也不会被安装到其他设备。

卡巴斯基应用程序的一些更新无法被卸载。如果您为这些更新设置了*已拒绝*状态，Kaspersky Next XDR Expert 将不会从之前已安装这些更新的设备上卸载它们。然而，这些更新将来也不会被安装到其他设备。

如果您为第三方软件更新设置了*已拒绝*状态，这些更新将不会安装在计划将其安装但并未将其安装的设备上。更新将保持在已将其安装的设备上。如果您必须删除更新，您可以在本地手动删除它们。

自动安装 Kaspersky Endpoint Security for Windows 的更新

您可以在客户端设备上配置 Kaspersky Endpoint Security for Windows 自动更新数据库和软件模块。

要在设备上配置下载和自动安装 Kaspersky Endpoint Security for Windows 更新：

1. 在主菜单中，转到“**任务**”。

2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明。

3. 对于 Kaspersky Endpoint Security for Windows 应用程序，选择**更新**作为任务子类型。

4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

5. 选择任务范围。

6. 指定管理组、设备分类或应用程序任务的设备。

7. 在“**完成任务创建**”步骤，如果要修改默认任务设置，请启用“**创建完成时打开任务详情**” 选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时更改默认设置。

8. 单击“**创建**”按钮。

   任务被创建并显示在任务列表。

9. 点击创建的任务的名称以打开任务属性窗口。

10. 在任务属性窗口的“**应用程序设置**”选项卡上，以本地或移动模式定义更新任务设置：

    - **本地模式**: 连接在设备和管理服务器之间建立。
    - **移动模式**：Kaspersky Next XDR Expert 与设备之间未建立连接（例如，当设备未连接到互联网时）。

11. 启用您要使用的更新源以更新 Kaspersky Endpoint Security for Windows 的数据库和应用程序模块。如果需要，使用“**上移**”和“**下移**”按钮更改列表中的更新源位置。如果启用了多个更新源，Kaspersky Endpoint Security for Windows 会尝试从列表顶部开始依次进行连接，并通过从第一个可用的更新源处获取更新包来执行更新任务。

12. 启用**安装批准的应用程序模块更新**选项，在更新应用程序数据库同时下载和安装软件模块。

    如果启用该选项，Kaspersky Endpoint Security for Windows 在运行更新任务时，通知用户有可用的软件模块更新并将软件模块更新包含在更新包中。Kaspersky Endpoint Security for Windows 仅安装已设置为*已批准*状态的更新；这些更新将通过应用程序界面或 Kaspersky Next XDR Expert 在本地安装。

    您也可以启用**自动安装关键应用程序模块更新**选项。如果软件模块有任何更新，Kaspersky Endpoint Security for Windows 将自动安装状态为“*关键*”的更新；其余的更新会在您批准后安装。

    如果软件模块更新需要审查并接受授权许可协议和隐私策略，程序将在用户接受用户授权许可协议和隐私策略的条款后安装更新。

13. 选择**复制更新到文件夹**复选框，程序将已下载的更新保存到指定的文件夹。

14. 计划任务。为确保及时更新，建议您选择“**当新更新下载至存储库时**”选项。

15. 单击“**保存**”按钮。

更新任务正在运行时，程序发送请求到 Kaspersky 更新服务器。

一些更新需要安装最新版本的管理插件。

关于使用 diff 文件更新 Kaspersky 数据库和软件模块

当 Kaspersky Next XDR Expert 从卡巴斯基更新服务器下载更新时，会使用差异文件来优化流量。您也可以对从网络中其他设备（管理服务器、分发点和客户端设备）获取更新的设备启用对 diff 文件的使用。

关于下载 diff 文件功能

diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。使用 diff 文件节省您公司网络内的流量，因为 diff 文件相比数据库和软件模块的完整文件占据更少的空间。如果对管理服务器或分发点启用 *下载 diff 文件*功能，diff 文件被保存到该管理服务器或分发点。结果，从该管理服务器或分发点获取更新的设备可以使用保存的 diff 文件更新它们的数据库和软件模块。

要优化对 diff 文件的使用，我们建议您根据管理服务器或分发点的更新计划同步从管理服务器或更新代理获取更新的设备的更新计划。然而，即便设备更新频率小于从其获取更新的管理服务器或分发点，流量也被节省。

分发点不对 diff 文件的自动分发使用 IP 多点传送。

启用下载 diff 文件功能

阶段

1. **在管理服务器上启用该功能**

   在*"将更新下载至管理服务器存储库"任务的设置*中启用该功能。

2. **为分发点启用该功能**

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

   然后在网络代理策略设置中对从管理服务器接收更新的分发点启用该功能。

   然后对从管理服务器接收更新的分发点启用该功能。

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

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

通过分发点下载更新

Kaspersky Next XDR Expert 允许分发点从管理服务器、Kaspersky 服务器或本地或网络文件夹接收更新。

要为分发点配置更新下载：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在"**常规**"选项卡上，选择"**分发点**"区域。
3. 单击将用于将更新传送到组中的客户端设备的分发点的名称。
4. 在分发点属性窗口中选择"**更新源**"区域。
5. 为分发点选择更新源：

   - **更新源**

     为分发点选择更新源：

     - 要允许分发点从管理服务器接收更新，请选择"**从管理服务器检索**"。
     - 要允许分发点使用任务接收更新，请选择"**使用更新下载任务**"，然后指定"*将更新下载至分发点存储库*"任务：
       - 如果设备上已存在此类任务，请在列表中选择该任务。
       - 如果设备上尚不存在此类任务，请单击"**创建任务**"链接创建任务。"新任务向导"启动。遵照向导的说明操作。

- **下载差异文件**

  该选项启用下载 diff 文件功能。

  默认情况下已启用该选项。

分发点将从指定的更新源接收更新。

更新离线设备上的 Kaspersky 数据库和软件模块

安装未按既定程序通过认证测试的 Kaspersky 应用程序可执行模块更新（消除已知漏洞的更新除外），会导致应用程序失去认证状态。

更新受管理设备上的 Kaspersky 数据库和软件模块对于保持设备对病毒和其他威胁的防护是非常重要的任务。管理员通常通过使用管理服务器存储库来配置定期更新。

当您需要在未连接到管理服务器（主或从）、分发点或互联网的设备（或设备组）上更新数据库和软件模块时，您必须使用其他更新源，例如 FTP 服务器或本地文件夹。此种情况下，您必须使用大容量存储设备传送所需更新的文件，例如闪存驱动器或外部硬盘驱动器。

您可以从这里复制所需更新：

- 管理服务器。

  为确保管理服务器存储库包含所需的安装在离线设备上的安全应用程序的更新，至少一台受管理的在线设备必须安装了相同的安全应用程序。该应用程序必须配置为通过“*将更新下载至管理服务器存储库*”任务从管理服务器存储库接收更新。

- 任何安装了相同安全应用程序，并配置为从管理服务器存储库、分发点存储库或直接从 Kaspersky 更新服务器接收更新的设备。

以下是通过从管理服务器存储库复制而更新数据库和软件模块的例子。

要更新离线设备上的 Kaspersky 数据库和软件模块：

1. 连接可移动驱动器到管理服务器所在设备。

2. 复制更新文件到可移动驱动器。

   默认下，更新位于：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   或者，您可以将 Open Single Management Platform 配置成定期将更新复制到您选择的文件夹中。为此，请使用“*将更新下载至管理服务器存储库*”任务的属性中的“**复制下载的更新到附加文件夹**”选项。如果您指定闪存驱动器或外部硬盘驱动器上的文件夹作为该选项的目标文件夹，该大容量存储设备将总是包含更新的最新版本。

3. 在离线设备上，配置 Kaspersky Endpoint Security 以从本地文件夹或共享文件夹接收更新，例如 FTP 服务器或共享文件夹。

   说明：

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

4. 从可移动驱动器复制更新到您想用作更新源的本地文件夹或共享资源。

5. 在需要安装更新的离线设备上，启动 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的*更新*任务，具体取决于离线设备的操作系统。

更新任务完成后，设备上的 Kaspersky 数据库和软件模块为最新。

客户端设备的远程诊断

您可以使用远程诊断在 Windows 和 Linux客户端设备上远程执行以下操作：

- 启用和禁用跟踪、更改跟踪等级、下载跟踪文件
- 下载系统信息和应用程序设置
- 下载事件日志
- 为应用程序创建内存转储文件
- 开始诊断并下载诊断报告
- 开始、停止和重新启动应用程序

您可以使用从客户端设备下载的事件日志和诊断报告以自行定位问题。此外，如果您联系 Kaspersky 技术支持，一名技术支持专家可能让您从客户端设备下载跟踪文件、转储文件、事件日志和诊断报告以便让 Kaspersky 进一步分析。

打开远程诊断窗口

要对 Windows 和 Linux 客户端设备执行远程诊断，首先必须打开远程诊断窗口。

要打开远程诊断窗口：

1. 要选择要为其打开远程诊断窗口的设备，请执行以下操作之一：
   - 如果该设备属于管理组，请在主菜单中转到**资产管理 → 资产(设备)**。
   - 如果该设备属于未分配的设备群组，请在主菜单中，前往**资产管理 → 未分配的设备**。
2. 单击所需设备的名称。
3. 在打开的设备属性窗口中，选择“**高级**”选项卡。
4. 在“**高级**”选项卡上，单击“**远程诊断**”。
   这将打开客户端设备的“**远程诊断**”窗口。如果管理服务器和客户端设备之间未建立连接，则会显示错误消息。

或者，如果需要立即获取有关基于 Linux 的客户端设备的所有诊断信息，您可以在此设备上运行 collect.sh 脚本。

启用和禁用应用程序跟踪

您可以启用和禁用应用程序跟踪，包括 Xperf 跟踪。

启用和禁用跟踪

要在远程设备上启用或禁用跟踪：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   “**应用程序管理**”区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择您要启用或禁用跟踪的应用程序。
   远程诊断选项列表将打开。
4. 如果要启用跟踪：
   a. 在列表的“**跟踪**”区域中，单击“**启用跟踪**”。
   b. 在打开的“**修改跟踪级别**”窗口中，我们建议您保留设置的默认值。当需要时，技术支持专家将指导您配置过程。下列选项可用：
      - **跟踪级别**

        跟踪级别定义跟踪文件包含的详情数据量。
      - **基于循环的跟踪**

        应用程序覆盖跟踪信息以防止跟踪文件过量增长。指定用于存储跟踪信息的文件最大数量，以及每个文件的最大大小。如果写入了最大数量的最大大小的跟踪文件，最旧的文件被删除以便新跟踪文件可以被写入。

        此设置仅适用于 Kaspersky Endpoint Security。
   c. 单击“**保存**”按钮。

   将为所选应用程序启用跟踪。某些情况下，要启用跟踪，必须重新启动安全应用程序及其任务。

   > 在 Linux 客户端设备上，网络代理组件更新程序的跟踪由网络代理设置管理。因此，在运行 Linux 的客户端设备上，此组件的“**启用跟踪**”和“**修改跟踪级别**”选项被禁用。

5. 如果要禁用对所选应用程序的跟踪，请单击“**禁用跟踪**”按钮。
   对所选应用程序的跟踪即被禁用。

启用 Xperf 跟踪

对于 Kaspersky Endpoint Security，技术支持专家可能要求您对系统性能信息启用 Xperf 跟踪。

要启用和配置 Xperf 跟踪或禁用它：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择“Kaspersky Endpoint Security for Windows”。
   Kaspersky Endpoint Security for Windows 的远程诊断选项列表将显示。
4. 在“**Xpref 跟踪**”区域中，单击“**启用 Xperf 跟踪**”。
   如果已经启用 Xperf 跟踪，将显示“**禁用 Xperf 跟踪**”按钮。如果您想要禁用 Kaspersky Endpoint Security for Windows的 Xperf 跟踪，请单击此按钮。
5. 在打开的“**更改 Xperf 跟踪级别**”窗口中，根据技术支持专家的请求，执行以下操作：

   a. 选择以下跟踪级别之一：

   - **轻度级别**

     该类型的跟踪文件包含系统最少量信息。

     默认情况下已选定该选项。

   - **深度级别**

     相比于*轻度*类型的跟踪文件，该类型的跟踪文件包含更多详细信息，且可能在*轻度*类型跟踪文件不足以评估性能时被技术支持专家要求。*深度*跟踪文件包含关于系统的硬件、操作系统、应用程序的启动和结束进程列表、用于性能评估的事件和来自 Windows System Assessment 工具的事件的技术信息。

   b. 选择以下 Xperf 跟踪类型之一：

   - **基本类型**

     跟踪信息在 Kaspersky Endpoint Security 应用程序运行期间被接收。

     默认情况下已选定该选项。

   - **重启时类型**

     跟踪信息在操作系统从受管理设备上启动时接收。该跟踪类型在影响系统性能的问题发生时，在设备被开启后和 Kaspersky Endpoint Security 启动之前有效。

   您可能被要求启用“**循环文件大小(MB)**”选项以防止跟踪文件的过量增长。然后指定跟踪文件的最大大小。当文件达到最大大小时，最旧的跟踪信息被新信息覆盖。

   c. 定义循环文件大小。

   d. 单击“**保存**”按钮。

将启用并配置 Xperf 跟踪。

6. 如果您想要禁用 Kaspersky Endpoint Security for Windows的 Xperf 跟踪，请单击“**Xpref 跟踪**”区域中的“**禁用 Xperf 跟踪**”。

   Xperf 跟踪即被禁用。

下载应用程序的跟踪文件

要下载应用程序的跟踪文件：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。

   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择要为其下载跟踪文件的应用程序。
4. 在“**跟踪**”区域，单击“**跟踪文件**”按钮。

   这将打开“**设备跟踪日志**”窗口，其中显示了跟踪文件列表。
5. 在跟踪文件列表中，选择要下载的文件。
6. 执行以下操作之一：

   - 单击“**下载**”下载所选文件。您可以选择一个或多个文件进行下载。
   - 下载所选文件的一部分：

     a. 单击“**下载一部分**”。

     您无法同时下载多个文件的部分内容。如果您选择多个跟踪文件，**下载一部分**按钮将被禁用。

     b. 在打开的窗口中，根据需要指定名称和要下载的文件部分。

     对于 Linux 设备，无法编辑文件部分名称。

     c. 单击“**下载**”。

所选文件或其一部分将下载到您指定的位置。

删除跟踪文件

您可以删除不再需要的跟踪文件。

要删除跟踪文件：

1. 打开客户端设备的远程诊断窗口。
2. 在打开的远程诊断窗口中，选择“**事件日志**”选项卡。
3. 在“**跟踪文件**”区域中，单击“**Windows Update 日志**”或“**远程安装日志**”，具体取决于要删除哪些跟踪文件。

Windows Update 日志链接仅适用于基于 Windows 的客户端设备。

这将打开“**设备跟踪日志**”窗口，其中显示了跟踪文件列表。

4. 在跟踪文件列表中，选择一个或多个要删除的文件。
5. 单击“**删除**”按钮。

所选跟踪文件即被删除。

下载应用程序设置

要从客户端设备下载应用程序设置：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
3. 在“**应用程序设置**”区域中，单击“**下载**”按钮下载有关客户端设备上安装的应用程序的设置的信息。

包含信息的 ZIP 存档将被下载到指定位置。

从客户端设备下载系统信息

要从客户端设备下载系统信息：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**系统信息**选项卡。
3. 单击“**下载**”按钮可下载有关客户端设备的系统信息。
   如果您获取有关 Linux 设备的系统信息，紧急终止应用程序的转储文件将被添加到结果文件中。

该压缩文件可能包含明文形式的敏感数据（例如，密钥和密码）。建议您在将压缩文件发送给卡巴斯基技术支持之前，检查压缩文件中的文件并移除此类数据。

包含信息的文件将被下载到指定位置。

下载事件日志

要从远程设备下载事件日志：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口的“**事件日志**”选项卡上，单击“**所有设备日志**”。

3. 在“**所有设备日志**”窗口中，选择一个或多个相关日志。

4. 执行以下操作之一：

- 单击“**下载整个文件**”下载所选日志。
- 下载所选日志的一部分：

  a. 单击“**下载一部分**”。
  您无法同时下载多个日志的部分内容。如果您选择了多个事件日志，**下载一部分**按钮将被禁用。

  b. 在打开的窗口中，根据需要指定名称和要下载的文件部分。
  对于 Linux 设备，无法编辑日志部分名称。

  c. 单击“**下载**”。

所选事件日志或其一部分将被下载到指定的位置。

启动、停止和重新启动应用程序

您可以启动、停止和重新启动客户端设备上的应用程序。

若要启动、停止和重新启动应用程序，请执行以下操作：

1. 打开客户端设备的远程诊断窗口。

2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。

3. 在应用程序列表中，选择要启动、停止或重新启动的应用程序。

4. 单击以下按钮之一来选择操作：

- **停止应用程序**
  仅当应用程序当前正在运行时，此按钮才可用。
- **重启应用程序**
  仅当应用程序当前正在运行时，此按钮才可用。
- **启动应用程序**
  仅当应用程序当前未运行时，此按钮才可用。

根据您选择的操作，客户端设备上将启动、停止或重新启动所需应用程序。

如果重新启动网络代理，将显示一条消息，指示设备与管理服务器的当前连接将丢失。

运行 Kaspersky Security Center 网络代理的远程诊断并下载结果

要在远程设备上启动 Kaspersky Security Center 网络代理的诊断并下载结果：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择**Kaspersky Security Center 网络代理**。
   远程诊断选项列表将打开。
4. 在“**诊断报告**”部分中，单击“**运行诊断**”按钮。
   这将启动远程诊断过程并生成诊断报告。诊断过程完成后，“**下载诊断报告**”按钮变为可用。
5. 单击“**下载诊断报告**”按钮下载报告。

报告将被下载到指定位置。

在客户端设备上运行应用程序

如果 Kaspersky 支持专家要求，您可能需要在客户端设备上运行应用程序。您不必在该设备上安装应用程序。

如果要在客户端设备上运行自定义脚本，您可以使用 `KLACDT_SAVE_SETTING` 环境变量来确定保存执行结果的路径。例如：

- 对于基于 Windows 的设备：

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- 对于基于 Linux 的设备：

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

要在客户端设备上运行应用程序：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**运行远程应用程序**选项卡。
3. 在**对象类型**字段中，选择要上传的对象类型：
   - 选择**文件**来上传可执行文件。
   - 选择**文件夹**以上传包含要在客户端设备上运行的应用程序的文件夹。
     如果选择此对象类型，则会出现**要运行的可执行文件的名称**字段。在此字段中，指定文件夹中可执行文件的名称。您还可以指定文件的相对路径。
   - 选择**存档**上传包含要在客户端设备上运行的应用程序的 ZIP 存档。

如果选择此对象类型，则会出现**要运行的可执行文件的名称**字段。在此字段中，指定文件夹中可执行文件的名称。您还可以指定文件的相对路径。

ZIP 存档必须包含实用程序文件夹。此文件夹包含要在远程设备上运行的可执行文件。

4. 通过在系统窗口中选择对象或将其拖到上传字段来上传对象。
5. 如果需要，在**命令行参数**字段中指定运行可执行文件时要传递的命令行参数。
6. 单击**上传和运行**按钮以在客户端设备上运行选定的应用程序。
7. 应用程序执行成功完成后，单击**下载应用程序执行结果**按钮下载执行结果。

应用程序执行结果将保存，直到您运行新的诊断或关闭窗口为止。

使用该应用程序对客户端设备进行远程诊断已完成。

为应用程序创建内存转储文件

应用程序转储文件允许您查看某个时间点在客户端设备上运行的应用程序的参数。该文件还包含有关为应用程序加载的模块的信息。

不支持从基于 Linux 的设备获取转储文件。

为了通过远程诊断获取转储文件，可以使用 kldumper 实用程序。此实用程序旨在根据技术支持专家的要求获取卡巴斯基应用程序进程的转储文件。有关使用 kldumper 实用程序的要求的详细信息，请参阅Kaspersky Security Center 知识库。

要为应用程序创建转储文件：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**运行远程应用程序**选项卡。
3. 在**生成进程内存转储文件**区域中，指定要为其生成转储文件的应用程序的可执行文件。
4. 单击**下载转储文件**按钮。

   包含指定应用程序的转储文件的档案被下载。

   如果客户端设备上未运行指定的应用程序，则下载的存档中包含的“结果”文件夹将为空。

   如果指定的应用程序正在运行，但下载失败并出现错误，或者下载的压缩文件中包含的“result”文件夹为空，请参阅Kaspersky Security Center 知识库。

在基于 Linux 的客户端设备上运行远程诊断

Open Single Management Platform 允许您从客户端设备下载基本诊断信息。或者，您可以使用卡巴斯基的 collect.sh 脚本获取有关基于 Linux 的设备的诊断信息。该脚本必须在需要诊断的 Linux 客户端设备上运行。随后将创建一个文件，其中包含诊断信息、设备的系统信息、应用程序跟踪文件、设备事件日志，以及崩溃和已终止进程的转储文件。

我们建议您使用 collect.sh 脚本一次性获取有关 Linux 客户端设备的所有诊断信息。如果通过 Open Single Management Platform 远程下载诊断信息，您将需要浏览远程诊断界面的所有部分。此外，可能无法完全获得 Linux 设备的诊断信息。

如果您需要将生成的包含诊断信息的文件发送给卡巴斯基技术支持，请在发送文件之前删除所有机密信息。

要使用 collect.sh 脚本从 Linux 客户端设备下载诊断信息：

1. 下载 collect.sh 脚本，它在collect.tar.gz 存档中。
2. 将下载的压缩包复制到需要诊断的 Linux 客户端设备上。
3. 运行以下命令解压 collect.tar.gz 存档：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 执行以下命令指定脚本执行权限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理员权限的账户运行 collect.sh 脚本：

   ```
   # ./collect.sh
   ```

一个包含诊断信息的文件将生成并被保存到 /tmp/$HOST_NAME-collect.tar.gz 文件夹中。

管理客户端设备上的第三方应用程序和可执行文件

本节介绍 Kaspersky Next XDR Expert 中与管理客户端设备上运行的第三方应用程序和可执行文件相关的功能。

使用应用程序控制来管理可执行文件

您可以使用“应用程序控制”组件来允许或阻止可执行文件在用户设备上启动。“应用程序控制”组件支持基于 Windows 和基于 Linux 的操作系统。

对于基于 Linux 的操作系统，从 Kaspersky Endpoint Security 11.2 for Linux 开始，均提供应用程序控制组件。

先决条件

- Kaspersky Next XDR Expert 已部署在您的组织中。
- Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的策略已创建并处于活动状态。策略中启用了“应用程序控制”组件。

阶段

“应用程序控制”使用方案分阶段进行：

1. **形成并查看客户端设备上的可执行文件列表**

   此阶段帮助您了解在受管理设备上发现了哪些可执行文件。查看可执行文件列表，并将其与允许和禁止的可执行文件列表进行比较。对可执行文件的使用限制可能与组织中的信息安全策略有关。

   使用说明：获取并查看客户端设备上存储的可执行文件列表

2. **为组织中使用的可执行文件创建类别**

   分析受管理设备上存储的可执行文件列表。根据分析，为可执行文件创建类别。建议创建一个“工作应用程序”类别，以覆盖组织中使用的标准可执行文件集。如果不同的安全组在工作中使用不同的可执行文件集，则可以为每个安全组创建单独的类别。

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

   - *拒绝列表*。如果要允许启动除了阻止规则中指定的可执行文件外的所有可执行文件，则使用该模式。默认情况下选择此模式。
   - *允许列表*。如果要阻止启动除了允许规则中指定的可执行文件外的所有可执行文件，则使用该模式。

   应用程序控制规则是通过可执行文件的类别来实施的。在 Kaspersky Next XDR Expert 中，可执行文件类别分为三种类型：

   - 含有手动添加内容的类别。您定义将可执行文件包括在类别中的条件，例如元数据、文件哈希码、文件证书、文件路径。
   - 包含来自所选设备的可执行文件的类别。您指定自动包含在该类别中的可执行文件所属的设备。
   - 包含来自所选文件夹的可执行文件的类别。您指定自动包含在该类别中的可执行文件所来自的文件夹。

3. **在 Kaspersky Endpoint Security 策略中配置“应用程序控制”**

   使用您在上一阶段创建的类别，在 Kaspersky Endpoint Security for Linux 策略中配置应用程序控制组件。

   操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

4. **在测试模式下开启“应用程序控制”组件**

   为确保应用程序控制规则不会阻止用户工作所需的可执行文件，建议在创建新规则后启用应用程序控制规则测试并分析其操作。启用测试后，Kaspersky Endpoint Security for Windows 将不会阻止被应用程序控制规则禁止启动的可执行文件，而是将有关其启动的通知发送到管理服务器。

测试应用程序控制规则时，建议执行以下操作：

- 确定测试周期。测试周期从几天到两个月不等。
- 检查由测试“应用程序控制”操作生成的事件。

OSMP 控制台操作指南：在 Kaspersky Endpoint Security for Windows 策略中配置应用程序控制组件。请按照此说明操作，并在配置过程中启用**测试模式**选项。

5. **更改应用程序控制组件的设置**

   如有必要，请更改“应用程序控制”设置。根据测试结果，您可以将与应用程序控制组件事件相关的可执行文件添加到含有手动添加内容的类别中。

   OSMP 控制台操作说明：将事件相关的可执行文件添加到应用程序类别

6. **在操作模式下应用“应用程序控制”的规则**

   测试应用程序控制规则并完成类别的配置后，您可以在操作模式下应用这些应用程序控制规则。

   OSMP 控制台操作指南：在 Kaspersky Endpoint Security for Windows 策略中配置应用程序控制组件。请按照此说明操作，并在配置过程中禁用**测试模式**选项。

7. **验证“应用程序控制”配置**

   确保已完成以下操作：

   - 为可执行文件创建类别。
   - 已使用类别来配置应用程序控制。
   - 已在操作模式下应用“应用程序控制”的规则。

结果

方案完成后，可执行文件在受管理设备上的启动受到控制。用户只能运行组织中允许的可执行文件，而不能运行组织中禁止的可执行文件。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Endpoint Security for Windows 帮助。

应用程序控制模式和类别

应用程序控制组件监控用户启动可执行文件的尝试。您可以使用应用程序控制规则来控制可执行文件的启动。

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

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

- *拒绝列表*。如果要允许启动除了阻止规则中指定的可执行文件外的所有可执行文件，则使用该模式。默认情况下选择此模式。
- *允许列表*。如果要阻止启动除了允许规则中指定的可执行文件外的所有可执行文件，则使用该模式。

应用程序控制规则是通过可执行文件的类别来实施的。Kaspersky Next XDR Expert 中有三种类型的类别：

- 含有手动添加内容的类别。您定义将可执行文件包括在类别中的条件，例如元数据、文件哈希码、文件证书、文件路径。
- 包含来自所选设备的可执行文件的类别。您指定自动包含在该类别中的可执行文件所属的设备。
- 包含来自所选文件夹的可执行文件的类别。您指定自动包含在该类别中的可执行文件所来自的文件夹。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Endpoint Security for Windows 帮助。

获取并查看客户端设备上安装的应用程序列表

Kaspersky Next XDR Expert 可清点运行 Linux 和 Windows 的受管理客户端设备上安装的所有软件。

网络代理编辑安装在设备上的应用程序列表，并把该列表传给管理服务器。网络代理更新应用程序列表大约需要 10-15 分钟。

对于基于 Windows 的客户端设备，网络代理从 Windows 注册表接收有关已安装应用程序的大部分信息。对于基于 Linux 的客户端设备，包管理器向网络代理提供有关已安装应用程序的信息。

要查看受管理设备上安装的应用程序列表：

1. 在主菜单中，转到“**软件管理**”→“**第三方应用程序**”→“**应用程序注册表**”。

   该页面显示一个表格，其中包含安装在受管理设备上的应用程序。选择应用程序以查看其属性，例如，供应商名称、版本号、可执行文件列表、安装了该应用程序的设备列表、可用软件更新列表和检测到的软件漏洞列表。

2. 您可以按如下方式对包含已安装应用程序的表中的数据进行分组和筛选：

   - 单击表格右上角的“设置”图标 ( )。

     在调用的“**表格设置**”菜单中，选择要在表中显示的列。要查看安装应用程序的客户端设备的操作系统类型，请选择“**OS 类型**”列。

   - 单击表格右上角的过滤器图标 ( )，然后在调用的菜单中指定并应用过滤条件。

     显示筛选出的已安装应用程序表。

要查看特定受管理设备上安装的应用程序列表，

在主应用程序窗口中，转到“**设备**” →“**受管理设备**” →“**设备名称**” →“**高级**” →“**应用程序注册表**”部分。在此菜单中，您可以将应用程序列表导出到 CSV 文件或 TXT 文件。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Security for Windows 帮助。

获取并查看客户端设备上存储的可执行文件列表

您可以通过以下方式之一获取存储在客户端设备上的可执行文件列表：

- 在 Kaspersky Endpoint Security 策略中启用应用程序启动通知。
- 创建清查任务。

在 Kaspersky Endpoint Security 策略中启用应用程序启动通知

要启用有关应用程序启动的通知：

1. 打开 Kaspersky Endpoint Security 策略设置，然后转到**常规设置 → 报告和存储**。
2. 在**到管理服务器的数据传输**设置组中，选择**关于启动的应用程序**复选框，保存更改。

当用户尝试启动可执行文件时，关于这些文件的信息将被添加到客户端设备上的可执行文件列表中。Kaspersky Endpoint Security 会将该信息发送到网络代理，然后网络代理将其发送到管理服务器。

创建清查任务

对于 Kaspersky Endpoint Security for Linux，清查可执行文件的功能在 11.2 之前的版本中不可用。

您可以在获取已安装应用程序相关信息的同时减少数据库的负载。为了节省数据库空间，在安装了一组标准软件的参考设备上运行清查任务。建议设备数量为 1-3。

要在客户端设备上为可执行文件创建清查任务：

1. 在主菜单中，转到“**任务**”。

   将显示任务列表。
2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明。
3. 在“**新任务设置**”页面上的“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows，具体取决于客户端设备的操作系统。
4. 在“**任务类型**”下拉列表中，选择“**清单**”。
5. 在**完成任务创建**页面上，单击**完成**按钮。

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

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

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

清查过程中可检测以下格式的可执行文件（具体取决于您在清单任务属性中选择的选项）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

查看受管理设备上存储的可执行文件列表

要查看客户端设备上存储的可执行文件列表：

在主菜单中，前往**软件管理→第三方应用程序→可执行文件**。

该页面显示客户端设备上存储的可执行文件列表。

如有必要，您可以将受管理设备的可执行文件发送到已打开 OSMP 控制台的设备。

要发送可执行文件：

1. 在主菜单中，前往**软件管理→第三方应用程序→可执行文件**。
2. 单击要发送的可执行文件的链接。
3. 在打开的窗口中，转到**设备**部分，然后选中要从其发送可执行文件的受管理设备的复选框。

   在发送可执行文件之前，请通过选中**不断开与管理服务器的连接**复选框，确保受管理设备与管理服务器直接连接。

4. 单击“**发送**”按钮。

   所选可执行文件将在下载完成后发送至已打开 OSMP 控制台的设备。

创建含有手动添加内容的应用程序类别

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

要创建含有手动添加内容的应用程序类别：

1. 在主菜单中，前往**软件管理 → 第三方应用程序 → 应用程序类别**。
   将显示含有应用程序类别列表的页面。
2. 单击**添加**。
   新类别向导启动。使用**下一步**按钮进行向导。

3. 在“**选择策略创建方法**”步骤中，指定应用程序类别名称并选择“**含有手动添加内容的类别。可执行文件的数据被手动添加到该类别中**”选项。

4. 在“**条件**”步骤中，单击“**添加**”按钮以添加在所创建类别中包含文件的条件标准。

5. 在**条件标准**步骤中，执行以下操作：

   a. 选择用于创建类别的规则类型：

   - **从 KL 类别**

     如果选中此选项，您可以指定卡巴斯基应用程序类别作为添加应用程序到用户类别的条件。来自指定 Kaspersky 类别的应用程序将被添加到用户应用程序类别。

   - **从存储库选择证书**

     如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

     如果您创建并启动了清查任务并在Kaspersky Endpoint Security策略中勾选了**关于已启动的应用程序**复选框，则会将证书添加到存储库中。您可以执行以下两项操作。

     > 证书信息只能从 PE 格式（.exe、.dll、.sys）的可执行文件中提取。

   - **指定应用程序路径 (支持掩码)**

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

   - **可移动驱动器**

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

   - **哈希、元数据或证书**：

     - **从可执行文件列表选择**

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

     - **从应用程序注册表选择**

       如果选择此选项，将显示应用程序注册表。从注册表中选择一个应用程序后，窗口将打开，其中的参数将使用您选择的应用程序的元数据进行填充：

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

请注意，仅阻止满足指定参数的可执行文件的启动，而不阻止您选择的应用程序的启动。如果选定的应用程序元数据与启动应用程序时启动的可执行文件的元数据相匹配，那么您可以继续下一步。否则，您必须手动更改值以匹配可执行文件的元数据。

- **手动指定**

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

  文件哈希

  根据网络中设备上安装的安全应用程序版本，您应选择 Kaspersky Next XDR Expert 用于计算此类别中文件哈希值的算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

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

  请选择 Kaspersky Next XDR Expert 用于计算此类别中文件哈希值的以下任一选项：

  - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security for Linux，请选中“**SHA256**”复选框。
  - 仅当使用 Kaspersky Endpoint Security for Windows 时，才选择 **MD5 哈希**复选框。Kaspersky Endpoint Security for Linux 不支持 MD5 哈希函数。

  元数据

  如果选择此选项，则可以指定文件名、文件版本、供应商形式的文件元数据。类别条件仅匹配具有相同元数据的可执行文件。

  证书

  如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

  如果您创建并启动了清查任务并在Kaspersky Endpoint Security策略中勾选了**关于已启动的应用程序**复选框，则会将证书添加到存储库中。您可以执行以下两项操作。

- **从压缩文件夹**

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

  - **文件哈希**

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

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

  - **元数据**

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

  - **证书**

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

  如果您想使用这些标准，必须在上传文件或存档文件夹后手动指定**元数据**和**证书**标准。

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

- **文件哈希**

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

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

- **元数据**

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

- **证书**

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

如果您想使用这些标准，必须在上传文件或存档文件夹后手动指定**元数据**和**证书**标准。

b. 如有必要，请在**描述**字段中添加注释。符号数量不能超过 1000 个。

之后，您可以编辑或删除该注释。为此，请在应用程序类别属性中打开**条件**选项卡，然后在**条件标准**列中，单击要编辑或删除其注释的条件链接。

选择**从 KL 类别**规则类型时，您可以为基于此规则类型创建的所有条件添加一条注释。您可以单独编辑或删除每个条件的注释。

所选条件将添加到条件列表中。

您可以为要创建的应用程序类别添加所需的任意数量的标准。

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

   如有必要，您可以在**描述**字段中添加注释。符号数量不能超过 1000 个。

   之后，您可以编辑或删除该注释。为此，请在应用程序类别属性中打开**排除项**选项卡，然后在**条件标准**列中，单击要编辑或删除其注释的条件链接。

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

向导结束后，应用程序类别将被创建并显示在应用程序类别列表中。配置“应用程序控制”时，可以使用已创建的应用程序类别。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助 和 Kaspersky Endpoint Security for Windows 帮助 。

创建包括选定设备中的可执行文件的应用程序类别

您可以将选定设备中的可执行文件用作要允许或阻止的可执行文件的模板。基于选定设备中的可执行文件，您可以创建一个应用程序类别，并在“应用程序控制”组件配置中使用该应用程序类别。

请确保满足以下先决条件：

- 应用程序控制组件已在 Kaspersky Endpoint Security 策略中启用。
- 已获取存储在受管理设备上的可执行文件列表。

要创建包括选定设备中的可执行文件的应用程序类别：

1. 在主菜单中，前往**软件管理 → 第三方应用程序 → 应用程序类别**。
   显示包含可执行文件类别列表的页面。
2. 单击**添加**。
   新类别向导启动。使用**下一步**按钮进行向导。
3. 在**选择策略创建方法**步骤中，指定类别名称，然后选择**包含所选设备上可执行文件的类别。这些可执行文件被自动处理，它们的度量数据被添加到类别中**。
4. 单击**添加**。
5. 在打开的窗口中，选择一个或多个设备，其可执行文件将用于创建应用程序类别。
6. 指定下列设置：

   - **哈希值计算算法**

     根据网络中设备上安装的安全应用程序版本，您应选择 Kaspersky Next XDR Expert 用于计算此类别中文件哈希值的算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

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

     请选择 Kaspersky Next XDR Expert 用于计算此类别中文件哈希值的以下任一选项：

     - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security for Linux，请选中“**SHA256**”复选框。

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

     “**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”复选框被默认选中。

     为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)复选框被默认清空。

   - **与管理服务器存储库同步数据**

     如果您希望该管理服务器定期检查指定文件夹中的更改，则选择此选项。

     默认情况下已禁用该选项。

     如果启用此选项，请指定检查指定文件夹中的更改的周期（以小时为单位）。默认情况下，扫描间隔为 24 小时。

   - **文件类型**

     在此区域中，可以指定用于创建应用程序类别的文件类型。

     所有文件。创建类别时会考虑所有文件。默认情况下已选定该选项。

     仅应用程序类别之外的文件。创建类别时仅考虑应用程序类别之外的文件。

- **文件夹**

  在此区域中，可以指定选定设备中的哪些文件夹包含用于创建应用程序类别的文件。

  所有文件夹。创建类别时会考虑所有文件夹。默认情况下已选定该选项。

  指定文件夹。创建类别时仅考虑指定文件夹。如果选择此选项，则必须指定文件夹的路径。

向导完成后，会创建可执行文件类别。它显示在类别列表中。配置应用程序控制时，可以使用已创建的类别。

创建包括选定文件夹中的可执行文件的应用程序类别

您可以将选定文件夹中的可执行文件用作要在组织中允许或阻止的可执行文件的标准。在选定文件夹中的可执行文件的基础上，您可以创建一个应用程序类别，并在"应用程序控制"组件配置中使用该应用程序类别。

要创建包括选定文件夹中的可执行文件的类别：

1. 在主菜单中，前往**软件管理 → 第三方应用程序 → 应用程序类别**。

   显示含有类别列表的页面。

2. 单击**添加**。

   新类别向导启动。使用**下一步**按钮进行向导。

3. 在"**选择策略创建方法**"步骤中，指定类型名称并选择"**包含指定文件夹内可执行文件的类别。复制到指定文件夹的应用程序可执行文件被自动处理，它们的度量数据被添加到类别中**"选项。

4. 指定将用于创建该类别的可执行文件所在的文件夹。

5. 配置以下设置：

   - **包含动态链接库 (DLL) 到该类别**

     应用程序类别包含动态链接库(DLL 格式的文件)，应用程序控制组件记录系统中运行的此类库的操作。将 DLL 文件包含在该类别中可能会降低 Kaspersky Next XDR Expert 的性能。

     默认情况下，此复选框未被选中。

   - **包含脚本数据到该类别**

     应用程序类别包含脚本数据，脚本不被 Web 威胁防护阻止。将脚本数据包含在该类别中可能会降低 Kaspersky Next XDR Expert 的性能。

     默认情况下，此复选框未被选中。

   - **哈希值计算算法**：**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持) / 为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**

     根据网络中设备上安装的安全应用程序版本，您应选择 Kaspersky Next XDR Expert 用于计算此类别中文件哈希值的算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

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

     请选择 Kaspersky Next XDR Expert 用于计算此类别中文件哈希值的以下任一选项：

     - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security for Linux，请选中"**SHA256**"复选框。

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

“**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”复选框被默认选中。

为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)复选框被默认清空。

- **强制扫描文件夹以查找更改**

  如果启用此选项，应用程序会定期检查“类别内容添加”文件夹的任何变化。您可以在该选框旁的输入字段中指定检查频率（小时）。默认情况下，强制检查的时间间隔为 24 小时。

  如果禁用此选项，应用程序不会强制检查文件夹。如果文件被修改、添加或删除，服务器会尝试访问这些文件。

  默认情况下已禁用该选项。

向导完成后，会创建可执行文件类别。它显示在类别列表中。您可以在“应用程序控制”配置中使用该类别。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助 和 Kaspersky Endpoint Security for Windows 帮助 。

查看应用程序类别列表

您可以查看已配置的可执行文件类别列表以及每个类别的设置。

要查看应用程序类别列表，

在主菜单中，前往**软件管理 → 第三方应用程序 → 应用程序类别**。

显示含有类别列表的页面。

要查看应用程序类别的属性，

单击该类别的名称。

显示该类别的属性窗口。这些属性被分组在几个选项卡上。

在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

创建“应用程序控制”类别后，可以在 Kaspersky Endpoint Security for Windows 策略中使用它们配置“应用程序控制”。

在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
   将显示含有策略列表的页面。

2. 单击 **Kaspersky Endpoint Security for Windows** 策略。

   策略设置窗口打开。

3. 转到“**应用程序设置**”→“**安全控制**”→“**应用程序控制**”。

   将显示带“应用程序控制”设置的“**应用程序控制**”窗口。

4. “**应用程序控制**”选项默认启用。开启切换按钮**应用程序控制已禁用**以禁用该选项。

5. 在“**应用程序控制设置**”区块设置中，启用操作模式以应用“应用程序控制”规则并允许 Kaspersky Endpoint Security for Windows 阻止应用程序启动。

   如果要测试应用程序控制规则，请在“**应用程序控制设置**”区域启用测试模式。在测试模式中，Kaspersky Endpoint Security for Windows 不会阻止应用程序启动，但会在报告中记录有关所触发规则的信息。单击**查看报告**链接可查看此信息。

6. 如果您希望 Kaspersky Endpoint Security for Windows 在用户启动应用程序时监控 DLL 模块的加载，请启用“**控制 DLL 模块加载**”选项。

   有关模块和加载了模块的应用程序的信息将保存到报告中。

   Kaspersky Endpoint Security for Windows 仅监控在选择“**控制 DLL 模块加载**”选项后加载的 DLL 模块和驱动程序。如果您希望 Kaspersky Endpoint Security for Windows 监控所有 DLL 模块和驱动程序，包括在启动 Kaspersky Endpoint Security for Windows 之前加载的 DLL 模块和驱动程序，请在选择“**控制 DLL 模块加载**”选项后重新启动设备。

7. （可选）在“**消息模板**”块中，更改当应用程序被阻止启动时显示的消息模板以及发送给您的电子邮件模板。

8. 在“**应用程序控制模式**”区块设置中，选择“**拒绝列表**”或“**允许列表**”模式。

   默认情况下，选择“**拒绝列表**”模式。

9. 单击“**规则列表设置**”链接。

   将打开“**拒绝列表和允许列表**”窗口，您可以在其中添加应用程序类别。默认情况下，如果选择“**拒绝列表**”模式则选定“**拒绝列表**”选项卡，如果选择“**允许列表**”模式则选定“**允许列表**”选项卡。

10. 在“**拒绝列表和允许列表**”窗口中，单击“**添加**”按钮。

    “**应用程序控制规则**”窗口将开启。

11. 单击“**请选择类别**”链接。

    将打开“**应用程序类别**”窗口。

12. 添加您先前创建的应用程序类别。

    可以单击“**编辑**”按钮来编辑已创建类别的设置。

    可以单击“**添加**”按钮来创建新类别。

    可以单击“**删除**”按钮以从列表中删除类别。

13. 完成应用程序类别列表后，单击“**确定**”按钮。

    “**应用程序类别**”窗口关闭。

14. 在“**应用程序控制规则**”窗口的“**主题及其权限**”区域中，创建要应用“应用程序控制”规则的用户和用户组列表。

15. 单击“**确定**”按钮以保存设置并关闭“**应用程序控制规则**”窗口。

16. 单击“**确定**”按钮以保存设置并关闭“**拒绝列表和允许列表**”窗口。

17. 单击“**确定**”按钮以保存设置并关闭“**应用程序控制**”窗口。

18. 关闭含有 Kaspersky Endpoint Security for Windows 策略设置的窗口。

“应用程序控制”已配置。策略传播到客户端设备后，可执行文件的启动将受到管理。

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助和 Kaspersky Endpoint Security for Windows 帮助。

添加事件相关的可执行文件到应用程序类别

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

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

建议创建事件分类以查看与“应用程序控制”操作相关的事件。

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

要将与“应用程序控制”事件相关的可执行文件添加到应用程序类别：

1. 在主菜单中，转到“**监控**” → “**事件分类**”。
   将显示事件分类列表。

2. 选择事件分类以查看与“应用程序控制”相关的事件并启动此事件分类。
   如果尚未创建与“应用程序控制”相关的事件分类，可以选择并启动预定义分类，例如“**最近的事件**”。
   将显示事件列表。

3. 选择要将其相关可执行文件添加到应用程序类别的事件，然后单击“**分配到类别**”按钮。
   新类别向导启动。使用**下一步**按钮进行向导。

4. 在向导页面上，指定相关设置：

   - 在“**对事件相关可执行文件所采取的操作**”区域中，选择以下选项之一：

     - **添加到新的应用程序类别**

       如果要基于事件相关的可执行文件创建新的应用程序类别，则选择此选项。
       默认情况下已选定该选项。
       如果选择了此选项，请指定新的类别名称。

     - **添加到现有应用程序类别**

       如果要将事件相关的可执行文件添加到现有应用程序类别，则选择此选项。
       默认情况下未选定该选项。

如果选择了此选项，请选择要将可执行文件添加到的含有手动添加内容的应用程序类别。

- 在“**规则类型**”区域中，选择以下选项之一：
  - **添加到包含的规则**
  - **添加到排除的规则**
- 在**用作条件的参数**部分中，选择以下选项之一：
  - **证书详情(或没有证书的文件的 SHA256 哈希)**

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

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

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

    默认情况下已选定该选项。
  - **证书详情(没有证书的文件将被跳过)**

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

    如果您要将可执行文件的证书详情添加到类别规则，则选择该选项。如果可执行文件没有证书，该文件将被跳过。该文件的信息将不被添加到类别。
  - **仅 SHA256 (没有哈希的文件将被跳过)**

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

    如果您要仅添加可执行文件的 SHA256 哈希详情，则选择该选项。
  - **仅 MD5 (停产模式，仅对 Kaspersky Endpoint Security 10 Service Pack 1 版本)**

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

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

5. 单击“**确定**”。

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

有关“应用程序控制”的详细信息，请参阅 Kaspersky Endpoint Security for Linux 帮助 和 Kaspersky Endpoint Security for Windows 帮助 。

创建“安装所需更新并修复漏洞”任务

“*安装所需更新并修复漏洞*”任务仅在漏洞和补丁管理授权许可下可用。

“*安装所需更新并修复漏洞*”任务用于更新和修复在受管理设备上安装的第三方软件存在的漏洞。此任务允许您根据在任务设置中指定的规则安装多个更新并修复多个漏洞。

要使用“*安装所需更新并修复漏洞*”任务安装更新或修复漏洞，可以执行以下任一操作：

- 运行更新安装向导或漏洞修复向导。
- 创建“*安装所需更新并修复漏洞*”任务。
- 向现有的“*安装所需更新并修复漏洞*”任务添加更新安装规则。

要创建“安装所需更新并修复漏洞”任务：

1. 在主菜单中，转到“**任务**”。
2. 单击**添加**。

   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在“**应用程序**”下拉列表中，选择 Kaspersky Next XDR Expert。
4. 在“**任务类型**”列表中，选择“**安装所需更新并修复漏洞**”任务类型。

   如果未显示任务，请检查您的账户是否有对“**系统管理**：**漏洞和补丁管理**”功能区域的**读取**、**写入**和**执行**权限。如果没有这些访问权限，您无法创建和配置“*安装所需更新并修复漏洞*”任务。
5. 在**任务名称**字段中，指定新任务的名称。

   任务名称不能超过 100 个字符并且不能包括任何特殊字符 ("*<>?\:|)。
6. 选择要分配任务的设备。
7. 在向导的**指定更新安装规则**步骤中，添加更新安装规则。

   这些规则被应用到客户端设备上的更新安装。如果规则未被指定，任务无可执行。有关按照规则进行操作的信息，请参考更新安装规则。

   这些规则被应用到客户端设备上的更新安装。如果不指定任何规则，则该任务无可执行。
8. 指定下列设置：

   - **在设备重启或关闭时开始安装**

     如果启用该选项，更新在设备被重启或关闭时安装。否则，更新根据计划安装。

     如果安装更新可能影响设备性能则使用该选项。

     默认情况下已禁用该选项。

- **安装所需的常规系统组件**

  如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

  如果禁用该选项，您可能必须手动安装先决条件。

  默认情况下已禁用该选项。

- **更新过程中允许安装新应用程序版本**

  如果启用该选项，则允许执行会导致安装软件应用程序新版本的更新。

  如果禁用该选项，软件不被升级。您可以稍后手动或通过其他任务安装软件的新版本。例如，如果公司基础架构不被新软件版本支持，或者如果您想要在测试基础架构中检查升级，您可能使用该选项。

  默认情况下已启用该选项。

  > 升级应用程序可能导致安装在客户端设备上的独立应用程序功能异常。

- **下载更新到设备而不安装**

  如果启用该选项，应用程序下载更新到设备但是不自动安装它们。您可以稍后手动安装下载的更新。

  Microsoft 更新被下载到系统 Windows 存储。第三方应用程序更新（由非 Kaspersky 和 Microsoft 软件供应商开发的应用程序）将会下载到"**下载更新到**"字段中指定的文件夹中。

  如果禁用该选项，更新被自动安装到设备。

  默认情况下已禁用该选项。

  - **下载更新到**

    该文件夹用于下载第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新。

- **启用高级诊断**

  如果启用该功能，即便在 Open Single Management Platform 远程诊断实用程序中对网络代理禁用了写入跟踪文件功能，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由"**高级诊断文件的最大大小，MB**"值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Open Single Management Platform 远程诊断实用程序中的设置写入跟踪文件。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

  - **高级诊断文件的最大大小，MB**

    默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

继续执行向导的下一步。

9. 指定操作系统重新启动设置：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **在该时间后强制关闭阻止会话中的应用程序(分钟)**

  用户设备锁定时，程序以强制模式关闭（指定不活动间隔之后自动锁定，或手动锁定）。

  如果启用此选项，当输入字段中指定的时间间隔结束后，锁定设备上的应用程序将被强制关闭。

  如果禁用此选项，应用程序在锁定的设备上不关闭。

  默认情况下已禁用该选项。

10. 在向导的“**完成任务创建**”步骤启用“**创建完成时打开任务详情**”选项以修改默认任务设置。

    如果您不启用该选项，任务使用默认设置创建。您可以稍后修改默认设置。

11. 单击“**完成**”按钮。

    新任务向导将创建任务。如果启用了“**创建完成时打开任务详情**”选项，任务属性窗口将自动打开。在此窗口中，您可以指定常规任务设置，并根据需要更改任务创建期间指定的设置。

    > 您还可以通过单击任务列表中已创建任务的名称来打开任务属性窗口。

    任务被创建、配置并显示在任务列表中。

12. 要运行任务，请在任务列表中选择它，然后单击“**开始**”按钮。

    您还可以在任务属性窗口的**计划**选项卡上设置任务启动计划。

    有关计划启动设置的详细说明，请参阅常规任务设置。

任务完成后，安装所需的更新并修复漏洞。

如果您的组织网络中使用了 WSUS 服务器（本地 WSUS 服务器），并且您希望将其与管理服务器一起使用，则必须首先确保管理服务器未用作 WSUS 服务器，然后执行以下操作：

a. 在运行 Windows 的受管理设备上，为 Windows 更新服务指定本地 WSUS 服务器。您可以在 Windows 注册表中手动执行此操作，也可以使用 Windows 组策略执行此操作。

b. 在本地 WSUS 服务器上，指定更新所需的分类以及要分发更新的应用程序。

c. 将您的 WSUS 服务器与上游服务器同步（这可以是 Microsoft WSUS 服务器，也可以是另一个本地上游 WSUS 服务器）。

在设备上运行*安装所需更新和修复漏洞*任务后，网络代理使用 Windows 更新服务安装 Windows 更新。Windows 更新服务从注册表中获取外部 WSUS 服务器的地址，并直接从该外部服务器下载更新。

“查找漏洞和所需更新”任务设置

除了常规任务设置外，您还可以在创建“*查找漏洞和所需更新*”任务或稍后配置已创建任务的属性时指定以下设置：

- **搜索 Microsoft 列出的漏洞和更新**

  搜索漏洞和更新时，Kaspersky Next XDR Expert 使用 Microsoft 更新源中有关当前适用的 Microsoft 更新的信息。

  例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **连接更新服务器更新数据**

  受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

  - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
  - Microsoft 更新服务器

  如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

  如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

  到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

  默认情况下已启用该选项。

网络代理策略设置的以下选项的组合定义了获取更新的方式：

- 仅当在*查找漏洞和所需更新*任务的属性中启用了**连接更新服务器更新数据**设置，并且在网络代理策略设置中将**Windows Update 搜索模式**设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以接收更新。

- 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。

- 无论**连接更新服务器更新数据**选项处于启用还是禁用状态，如果**已禁用**选项设置为**Windows Update 搜索模式**，Kaspersky Next XDR Expert 都不会请求任何有关更新的信息。

如果您的组织网络中使用了 WSUS 服务器（本地 WSUS 服务器），并且您希望将其与 Kaspersky Security Center 管理服务器一起使用，则必须首先确保 Kaspersky Security Center 管理服务器未用作 WSUS 服务器，然后执行以下操作：

1. 在运行 Windows 的受管理设备上，为 Windows 更新服务指定本地 WSUS 服务器。您可以在 Windows 注册表中手动执行此操作，也可以使用 Windows 组策略执行此操作。

2. 在本地 WSUS 服务器上，指定更新所需的分类以及要分发更新的应用程序。

3. 将您的 WSUS 服务器与上游服务器同步（这可以是 Microsoft WSUS 服务器，也可以是另一个本地上游 WSUS 服务器）。

在设备上运行"*查找漏洞和所需更新*"任务后，网络代理使用 Windows 更新服务发起适用于该设备的 Windows 更新请求。Windows 更新服务从注册表中获取外部 WSUS 服务器的地址，并直接从该外部 WSUS 服务器搜索更新。然后，Windows 更新服务通过网络代理将此列表转发到管理服务器。因此，管理服务器拥有了最新的数据库。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用此选项，Kaspersky Next XDR Expert 将在 Windows 注册表以及**指定文件系统中应用程序高级搜索的路径**下指定的文件夹中，搜索第三方应用程序（由 Kaspersky 和 Microsoft 以外的软件供应商开发的应用程序）的漏洞和所需更新。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用此选项，Kaspersky Next XDR Expert 将不会搜索第三方应用程序的漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

- **指定文件系统中应用程序高级搜索的路径**

  Kaspersky Next XDR Expert 在这些文件夹中搜索需要进行漏洞修复和安装更新的第三方应用程序。您可以使用系统变量。

  指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

- **启用高级诊断**

  如果启用该功能，即便在 Open Single Management Platform 远程诊断实用程序中对网络代理禁用了写入跟踪文件功能，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由"**高级诊断文件的最大大小，MB**"值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

如果禁用该功能，网络代理根据 Open Single Management Platform 远程诊断实用程序中的设置写入跟踪文件。没有附加跟踪被写入。

当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

关于任务计划的建议

计划“*查找漏洞和所需更新*”任务时，请确保两个选项“**运行错过的任务**”和“**使用任务启动自动随机延迟**”已启用。

默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。如果组织的工作场所规则规定此时关闭所有设备，则在设备再次开机后（即第二天早上）将运行“*查找漏洞和所需更新*”任务。此活动可能不是必须的，因为漏洞扫描可能增加 CPU 和磁盘子系统负载。您必须基于组织的工作规则为该任务设置最方便的计划。

OPENAPI 参考指南

本OpenAPI参考指南旨在协助以下任务：

- 自动化和自定义。您可以将您可能不想手动处理的任务自动化。例如，作为管理员，您可以使用OpenAPI创建和运行脚本，这将有助于开发管理群组的结构，并使该结构保持最新状态。
- 自定义开发。使用 OpenAPI 可以开发客户端应用程序。

您可以使用屏幕右侧的搜索字段在 OpenAPI 参考指南中查找所需的信息。

OPENAPI 参考指南

脚本示例

OpenAPI 参考指南包含下表中列出的 Python 脚本示例。这些示例展示了如何调用 OpenAPI 方法并自动完成保护网络的各种任务，例如，创建“主要/从属”层级，在 Open Single Management Platform 中运行任务，或分配分发点。您可以按原样运行示例，也可以基于示例创建您自己的脚本。

用户应用场景和OpenAPI方法样本之间的匹配

示例	示例目的	方案
Log KlAkParams	您可以使用 `KlAkParams` 数据结构提取和处理数据。该示例展示了如何使用此数据结构。 该示例输出可以以不同的方式呈现。您可以获取数据以发送 HTTP 方法或在您的代码中使用它。	监控和报告
创建和删除“主要/从属”层次结构	您可以添加从属管理服务器，并建立“主要/从属”层次结构。或者，您可以断开从属管理服务器与层次结构的连接。	创建管理服务器层次结构，添加从属管理服务器和删除管理服务器层次结构

示例	示例目的	方案
通过连接网关下载网络列表文件到指定主机	您可以通过使用连接网关连接到所需设备上的网络代理，然后将包含网络列表的文件下载到您的设备。	分发点和连接网关的调整
将主管理服务器存储库中存储的授权许可密钥安装到从属管理服务器上	您可以连接到主管理服务器，从中下载所需的授权许可密钥，然后将此密钥传输到层次结构中包含的所有从属管理服务器。	受管理应用程序的授权许可
创建有效用户权限报告	您可以创建不同的报告。例如，您可以使用此示例生成有效用户权限的报告。此报告描述了用户拥有的权限，具体取决于他或她的组和角色。 您可以下载 HTML、PDF 或 Excel 格式的报告。	生成和浏览报告
启动设备任务	您可以通过使用连接网关连接到所需设备上的网络代理，然后允许必要的任务。	手动启动任务
为组中的设备注册分发点	您可以将受管理设备分配为分发点（以前称为更新代理）。	更新 Kaspersky 数据库和应用程序
对所有组进行枚举	您可以对管理组采取不同操作。该示例显示了如何执行以下操作： • 获取"受管理设备"根组的标识符 • 在组层次结构中移动 • 检索完整的、扩展的组层次结构以及它们的名称和嵌套	配置管理服务器
枚举任务、查询任务统计信息和运行任务	您可以找到以下信息： • 任务进度历史 • 当前任务状态 • 不同状态的任务数 您还可以运行任务。默认情况下，示例在输出统计信息后运行任务。	手动启动任务
创建并运行任务	您可以创建任务。在示例中指定以下任务参数： • 类型 • 运行方法 • Name。 • 将使用任务的设备组 默认情况下，示例创建了一个"显示消息"类型的任务。您可以为管理服务器的所有受管理设备运行此任务。如有需要，您可以指定自己的任务参数。	创建任务
枚举授权许可密钥	您可以获得安装在管理服务器受管理设备上的卡巴斯基应用程序的所有活动授权许可密钥的列表。该列表包含关于每个授权许可密钥的详细数据，例如名称、类型或到期日期。	授权许可
创建自定义类别	您可以根据所需参数创建应用程序类别。	创建含有手动添加内容的应用程序类别
使用 SrvView 枚举用户	您可以使用 SrvView 类向管理服务器请求详细信息。例如，您可以使用此示例获取用户列表。	管理用户和用户角色

应用程序通过 OpenAPI 与 Open Single Management Platform 交互

某些应用程序通过 OpenAPI 与 Open Single Management Platform 交互。此类应用程序包括，例如，Kaspersky Anti Targeted Attack Platform。这也可以是您基于 OpenAPI 开发的自定义客户端应用程序。

通过 OpenAPI 与 Open Single Management Platform 交互的应用程序连接到管理服务器。要了解您使用的应用程序是否通过 OpenAPI 工作，请参阅此应用程序的帮助。

监控和报告

本节介绍 Kaspersky Next XDR Expert 的监控和报告功能。这些功能给您一个基础架构、保护状态和统计信息的总览。

部署 Kaspersky Next XDR Expert 后或在其运行期间，您可以配置监控和报告功能，以最大限度地满足您的需求。

方案：监控和报告

本节提供了在 Kaspersky Next XDR Expert 中配置监控和报告功能的方案。

先决条件

在组织网络中部署 Kaspersky Next XDR Expert 后，您可以使用 Kaspersky Security Center 监控网络的安全状态并生成报告。

组织网络中的监控和报告分步骤进行：

1. **配置设备状态切换**

   熟悉取决于特定条件的设备状态设置。通过更改这些设置，您可以更改带有*严重*或*警告*重要级别的设备数量。当配置设备状态切换时，确保以下：

   - 新设置不与您组织的安全策略信息冲突。
   - 您可以及时对您组织网络中的重要安全事件做出反应。

2. **配置客户端设备上的事件通知**

   说明：

   配置客户端设备上的事件通知（通过邮件、SMS 或运行可执行文件）。

3. **对严重、警告、信息通知执行推荐的操作**

   说明：

   对您的组织网络执行推荐的操作

4. **查看您组织网络的安全状态**

   说明：

   - 查看“保护状态”小组件
   - 生成并查看保护状态报告
   - 生成并查看错误报告

5. **定位不被保护的客户端设备**

说明：

- 查看新设备小组件
- 生成并查看保护部署报告

6. **检查客户端设备保护**

   说明：

   - 根据保护状态和威胁统计类别生成并查看报告
   - 启动并查看“严重”事件分类

7. **评估和限制数据库上的事件负载**

   受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   说明：

   - 限制最大事件数量

8. **查看授权许可信息**

   说明：

   - 将“授权许可密钥使用”小组件添加到仪表板并查看
   - 生成并查看授权许可密钥使用报告

结果

完成方案后，您被通知您组织网络的保护，因此可以为进一步保护计划操作。

关于监控和报告的类型

组织网络的安全事件信息存储在管理服务器数据库。OSMP 控制台会根据这些事件，在您组织的网络中提供以下类型的监控和报告功能：

- 仪表板
- 报告
- 事件分类
- 通知

仪表板

仪表板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

在 OSMP 控制台界面中，您可以根据可用的设置，创建并查看用户自定义的事件分类。

通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

智能培训模式中的规则触发

该部分提供了客户端设备上的 Kaspersky Endpoint Security for Windows 中的自适应异常控制规则执行的检测信息。

规则检测客户端设备上的异常行为并可能阻止它。如果规则在智能培训模式下工作，就会检测异常行为，并向管理服务器发送关于每次此类情况的报告。您可以通过以下路径来查看有关检测到的异常行为的报告：**存储库 → 智能培训状态下的规则触发器**。您可以确认检测为正确或添加它们为排除，因此该行为类型不再被认为是异常。

检测信息存储在管理服务器的事件日志中（与其他事件一起）和自适应异常控制报告中。

关于自适应异常控制、规则以及它们的模式和状态的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

查看并确认使用自适应异常控制规则执行的检测

要查看使用自适应异常控制规则执行的检测列表：

1. 在主菜单中，转到**存储库 → 智能培训状态下的规则触发器**。
   列表显示使用自适应异常控制规则执行的检测的以下信息：

   - **管理组**

     设备所属管理组的名称。

   - **虚拟管理服务器**

     管理设备的虚拟管理服务器。

   - **设备名称**

     应用规则的客户端设备名称。

   - **名称**

     应用的规则名称。

   - **状态**

     正在排除—如果管理员处理该条目并添加其到排除规则列表。该状态保持到下一次客户端设备与管理服务器同步时，同步之后，该条目从列表消失。
     正在确认—如果管理员处理该条目并确认。该状态保持到下一次客户端设备与管理服务器同步时，同步之后，该条目从列表消失。
     空—如果管理员不处理该条目。

   - **检测数量**

     一个启发式规则中的检测数量，一个进程和一个客户端设备。该数量由 Kaspersky Endpoint Security 计算。

   - **用户名**

     运行进程的生成检测的客户端设备用户名称。

   - **源进程路径**

     源进程路径，例如，执行操作的进程路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

   - **源进程哈希**

     源进程文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

   - **源对象路径**

     启动进程的对象路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

   - **源对象哈希**

     源文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标进程路径**

  目标进程的路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标进程哈希**

  目标文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标对象路径**

  目标对象的路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标对象哈希**

  目标文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **已处理**

  异常被检测的日期。

要查看检测的属性：

1. 在主菜单中，转到**存储库 → 智能培训状态下的规则触发器**。
2. 执行以下操作之一：
   - 在**名称**列中，单击带有您要查看的检测名称的链接。
   - 在检测列表中，选中想要查看的检测旁边的复选框，然后单击“**属性**”按钮。

   所选检测的属性窗口将打开，显示有关它的信息。

您可以从自适应异常控制规则的检测列表或所选检测的属性窗口中确认任何检测。

确认检测：

- 在检测列表中选择一项或者多项检测，然后单击“**确认**”按钮。
- 打开所选检测的属性窗口，然后单击“**确认**”按钮。

  检测状态被更改为“**正在确认**”。客户端设备与管理服务器下次同步后，检测将从检测列表中消失。

  您的确认将被计入规则使用的统计数据中。有关详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

从自适应异常控制规则添加排除

“添加到自适应异常控制排除项”向导允许您从 Kaspersky Endpoint Security 的自适应异常控制规则添加排除项。

要通过向导添加自适应异常控制规则的排除项：

1. 通过下列其中一种方式启动向导：
   - 在主菜单中，转到**存储库→智能培训状态下的规则触发器**，选择一个或多个检测，然后单击**排除**按钮。

您可以一次添加 1000 个排除项。

在将检测添加到排除项之前，您可以通过单击检测名称或“**属性**”按钮来查看检测的属性。在打开的检测属性窗口中，您还可以单击“**排除**”按钮。

- 在主菜单中，转到“**监控**”→“**事件分类**”，单击包含所需事件分类的链接，选中要排除的检测旁边的复选框，然后单击“**从自适应异常控制中排除**”按钮。

“添加到自适应异常控制排除项”向导启动。使用“**下一步**”按钮继续向导操作。

2. 选择您要添加排除项的策略和配置文件。

   继承的策略无法被更新。如果您没有修改策略的权限，该策略将不会更新。

3. 单击**完成**关闭向导。

检测状态被更改为“**正在排除**”。客户端设备与管理服务器下次同步后，检测将从检测列表中消失。已配置并应用“自适应异常控制”规则的排除。

仪表板和小部件

本部分包含有关仪表板和仪表板提供的小部件的信息。本节包括有关如何管理小部件和配置小部件设置的说明。

使用仪表板

仪表板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

仪表板位于 OSMP 控制台的“**监控**” → “**控制板**”部分。

仪表板提供可以自定义的部件。您可以选择大量不同的部件，显示为饼图、表格、图表和列表。小部件中显示的信息会自动更新，更新周期为一到两分钟。更新间隔根据不同部件而不同。您可以随时通过设置菜单在小部件上手动刷新数据。

仪表板包括“**管理和保护**”和“**检测和响应**”选项卡，您可以在其中添加小部件。

“管理和保护”选项卡

“**管理和保护**”选项卡可以包含显示有关存储在管理服务器数据库中的所有事件信息的小部件。

在“**管理和保护**”选项卡中，可以使用以下组的小部件：

- **保护状态**
- **部署**
- **更新**

- **威胁统计**
- **其他**

“检测和响应”选项卡

“**检测和响应**”选项卡可以包含显示有关检测到和注册的警报和事故以及对它们采取的响应操作的信息的小部件。您只能查看您有权访问的租户的数据。

在“**检测和响应**”选项卡中，可以使用以下组的小部件：

- **事件**
- **活动列表**
- **上下文表**
- **警报**
- **资产**
- **事故**
- **行动手册**
- **事件源**
- **用户**

管理和保护小部件

配置仪表板的“**管理和保护**”选项卡时，您可以添加小部件、隐藏小部件、更改小部件的大小或外观、移动小部件以及更改其设置。

一些部件具有带链接的文本信息。您可以通过单击链接查看详细信息。

仪表板的“**管理和保护**”选项卡上提供以下小部件组和小部件：

- **保护状态**
  该组包含以下小部件：
  - **软件漏洞历史**
  - **漏洞设备的数量**
  - **按照漏洞严重级别的设备分发**
  - **所选设备的状态**
  - **保护状态**

- **部署**
  该组包括**新设备**小部件。
- **更新**
  该组包括以下小部件：
  - **有关 Windows Update 更新的统计信息**
  - **反病毒数据库分发**
  - **活动警报**
  - **基于更新类别的更新安装结果统计信息**
  - **基于更新类别的更新安装状态统计信息**
  - **更新安装状态统计信息**
- **威胁统计**
  该组包括以下小部件：
  - **根据病毒清除结果分发且由指定应用程序组件检测到的威胁**
  - **被应用程序组件检测到威胁**
  - **禁止的应用程序**
  - **网络攻击类型**
  - **检测到病毒类型和清除结果**
  - **隔离历史**
  - **检测到疑似被感染对象的历史**
  - **网络攻击历史**
  - **根据应用程序类型排序的威胁活动历史**
  - **威胁活动**
  - **10 台受感染最严重设备的所属用户**
  - **被感染最严重的设备**
  - **最经常被感染的虚拟管理服务器**
  - **最常见到的威胁**
  - **最经常被感染的 Windows 域**
  - **最经常被感染的组**
  - Alerts

- **其他**

  该组包括以下小部件：

  - **授权许可密钥使用**
  - **所选严重级别的通知**
  - **数据库中 10 个最经常发生的事件**
  - **所选管理服务器任务的当前状态**
  - **任务历史**

添加小部件到仪表板

要添加小部件到仪表板：

1. 在主菜单中，转到“**监控**” → “**控制板**”。
2. 单击“**添加或还原小部件**”按钮。
3. 在可用小部件列表，选择您要添加到仪表板的小部件。

   小部件按类别分组。要查看包含在类别中的小部件列表，单击类别名称旁边的臂章图标(>)。
4. 单击**添加**。

所选的小部件被添加到仪表板结尾。

您现在可以编辑所添加小部件的展示和参数。

从控制板隐藏工具

要从仪表板隐藏小部件：

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

所选小部件被隐藏。稍后，您可以再次添加该小部件到仪表板。

移动工具到控制板

要移动小部件到仪表板：

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

所选小部件的地方被清扫。

更改小部件的大小或外观

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

要更改小部件展示：

1. 在主菜单中，转到“**监控**” → “**控制板**”。
2. 单击您要编辑的小组件旁边的设置图标（⚙）。
3. 执行以下操作之一：
   - 要显示条形图形式的小组件，请选择“**图表类型：线条**”。
   - 要显示折线图形式的小组件，请选择“**图表类型：线形**”。
   - 要更改小组件占用的区域，请选择以下值之一：
     - **最小**
     - **最小 (仅线条)**
     - **中度 (饼图)**
     - **中度 (线条图)**
     - **最大**

所选小部件的展示被更改。

更改小部件设置

要更改小部件设置：

1. 在主菜单中，转到“**监控 → 控制板**”。
2. 单击您要编辑的小组件旁边的设置图标（⚙）。
3. 选择**显示设置**。
4. 在打开的小部件设置窗口，更改所需的小部件设置。
5. 单击“**保存**”保存更改。

   所选小部件的设置被更改。

设置集合取决于特定小部件。以下是一些通用设置：

- **小部件范围**（小组件显示其信息的对象集）—例如，管理组或设备分类。
- **选择任务**用于设置小部件显示其信息的任务。
- **时间间隔**（在小组件中显示信息的时间间隔）—两个指定日期之间；从指定日期到当前日期；或从当前日期减去指定天数。
- **如果指定了以下设置，则设置为“严重”**和**如果指定了以下设置，则设置为“警告”**规则用于控制状态图表中的颜色分配方式。

更改小部件设置后，您可以手动刷新小部件上的数据。

要刷新小部件上的数据：

1. 在主菜单中，转到“**监控**” → “**控制板**”。
2. 点击您要移动的工具旁边的设置图标（⚙）。
3. 选择**刷新**。

   小部件上的数据得到刷新。

检测和响应小部件

在“**检测和响应**”选项卡上，您可以添加、配置和删除小部件。

“**检测和响应**”选项卡中使用的小部件集合称为*布局*。所有小部件都必须放置在布局中。Kaspersky Next XDR Expert 允许您创建、编辑和删除布局。此外，系统也提供了预配置的布局。您可以根据需要在预配置的布局中编辑小部件设置。在“**检测和响应**”选项卡上，“**警报预览**”布局默认被选中。

小部件仅针对小部件或布局设置中选择的租户，显示在小部件或布局设置中选择的时间段所对应的数据。

单击有关事件、警报、事故或活动列表的小部件名称的链接，即可转到 Kaspersky Next XDR Expert 界面的相应部分。请注意，某些小部件不支持该选项。

仪表板的“**检测和响应**”选项卡上提供了以下小部件组和小部件：

- **事件**。用于基于事件创建分析的小部件。
- **活动列表**。用于基于活动关联器列表创建分析的小部件。
- **警报**。与警报相关的分析组。包括 Kaspersky Next XDR Expert 提供的有关警报和事故的信息。
  该组包含以下小部件：
  - **活动警报**。尚未关闭的警报数量。
  - **按租户分组的活动警报**。每个租户未关闭的警报数量。
  - **按租户分组的警报**。每个租户所有状态的警报数量。
  - 未分配**的警报**。未分配负责人的警报数量。
  - **按状态分组的警报**。状态为“*新建*”、“*已打开*”、“*已分配*”或“*已升级*”的警报数量。按状态分组。
  - **最新警报**。该表格包含有关布局中选定租户的最近 10 个未关闭警报的信息。
  - **警报分布**。在小部件配置时间段内创建的警报数量。
  - **按用户分组的警报**。状态为“*已分配*”的警报数量。按账户名称分组。
  - **按用户组分组的警报**。分配给每个组及其内部分析师的警报数量。分配给分析师的警报数量在其所属的每个组中均被统计。
  - **按严重级别分组的警报**。按严重级别分组的未关闭警报数量。
  - **按规则分组的警报**。按关联规则分组的未关闭警报数量。
  - **按时间段分组的警报状态**。所选时间段内按状态划分的警报数量。
  - **按技术分组的警报**。生成警报的防护技术名称。
  - **按哈希值分组的警报**。按扫描对象哈希值分组的警报数量。支持的哈希值类型：MD5和SHA-256。
  - **按检测来源分组的警报**。按检测来源分组的警报数量。
  - **按文件名分组的警报**。按扫描文件名分组的警报数量。
- **资产**。该分组旨在基于已处理事件生成有关资产的分析数据。该组包括以下小部件：
  - **警报中受影响的资产**。包含资产和相关租户名称以及与这些资产关联的未关闭警报数量的表格。无法从小部件移动到包含资产列表的部分。
  - **受影响的资产类别**。链接到未关闭警报的资产类别。
  - **资产数量**。添加到 Kaspersky Next XDR Expert 的资产数量。

- **按租户分组的事故中的资产**。与未关闭事故关联的资产数量。按租户分组。
- **按租户分组的警报中的资产**。按租户分组的与未关闭警报关联的资产数量。

- **事故**。与事故相关的分析组。
  该组包含以下小部件：
  - **活动事故**。尚未关闭的事故数量。
  - **未分配的事故**。状态为“*已打开*”的事故数量。
  - **事故分布**。小部件配置时间段内创建的事故数量。
  - **按状态分组的事故**。按状态分组的事故数量。
  - **按类型分组的事故**。按类型分组的处于任何状态的事故数量。
  - **按租户分组的活动事故**。可供用户账户使用的按租户分组的未关闭事故数量。
  - **所有事故**。所有状态的事故数量。
  - **按租户分组的所有事故**。按租户分组的所有状态的事故数量。
  - **事故中受影响的资产类别**。与未关闭事故关联的资产类别。
  - **最新事故**。该表格包含有关布局中选定租户的最近 10 个未关闭事故的信息。
  - **按用户分组的事故**。状态为“*已分配*”的事故数量。按用户账户名称分组。
  - **按用户组分组的事故**。分配给每个组及其内部分析师的事故数量。分配给分析师的事故数量在其所属的每个组中均被统计。
  - **按严重级别分组的事故**。按严重级别分组的未关闭事故数量。
  - **事故中受影响的资产**。与未关闭事故关联的资产数量。无法从小部件移动到包含资产列表的部分。
  - **事故中受影响的用户**。与事故关联的用户。无法从小部件移动到包含用户列表的部分。
- **事件源**。与事件源相关的分析组。该组包含以下小部件：
  - **按警报数量统计的事件源排名**。按事件源分组的未关闭警报数量。
  - **按转化率统计的事件源排名**。与未关闭警报关联的事件数量。按事件源分组。

    在某些情况下，按来源统计的生成警报数量可能不准确。为了获得准确的统计数据，建议在关联规则中将“设备产品”事件字段指定为唯一，并允许在关联事件中存储所有基础事件。但是，具有这些设置的关联规则会消耗更多资源。

- **用户**。该分组旨在基于已处理事件生产有关用户的分析数据。该组包含以下小部件：
  - **警报中受影响的用户**。与未关闭警报相关的账户数量。无法从小部件移动到包含用户列表的部分。
  - **AD 用户数量**。小部件配置时间段内通过 LDAP 接收的 Active Directory 账户数量。

    在事件表、事件详情区域、警报窗口和小部件中，以下字段将显示资产、账户和服务的名称（而非对应的 ID）：SourceAssetID、DestinationAssetID、DeviceAssetID、SourceAccountID、DestinationAccountID 和 ServiceID 字段。将事件导出到文件时，会保存 ID，但会将包含名称的列添加到文件中。将鼠标悬停在资产、用户账户或服务的名称上时，也会显示 ID。
    对于包含 ID 的字段，只能按 ID 进行搜索。

- **行动手册**。与行动手册相关的分析组。

  要查看此组中的小部件，您必须拥有以下 XDR 角色之一：主管理员、租户管理员、SOC 管理员、SOC 经理、1 级分析师、2 级分析师、批准人、审计员。

  该组包含以下小部件：

  - **MTTR 统计**。显示指定时间段内（默认为 30 天）首次响应警报和事故的时间变化。该小部件以柱状图形式呈现。

    MTTR 统计小部件提供以下配置参数：
    - **MTTR 类型**：
      - **均值**。首次响应警报和事故的平均时间变化。
      - **最小值**。首次响应警报和事故的最短时间变化。
      - **最大值**。首次响应警报和事故的最长时间变化。
    - **响应模式**：
      - **手动**。仅显示首次手动响应的时间变化。
      - **自动**。仅显示首次自动响应的时间变化。
      - **所有**。显示所有首次响应的时间变化。
    - **范围**：
      - **警报**。仅显示针对警报的首次响应时间变化。
      - **事故**。仅显示针对事故的首次响应时间变化。
      - **所有**。显示警报和事故的首次响应时间变化。
  - **自动和手动启动行动手册**。特定时间段内自动和手动启动行动手册的总次数。该小部件以柱状图形式呈现。

    小部件的“**启动类型**”参数可指定为仅显示特定时间段内自动启动次数、仅显示手动启动次数或显示行动手册总启动次数。

对于“**MTTR 统计**”和“**行动手册自动和手动启动**”小部件，您还可以设置“**时间段长度**”参数。此参数指定数据分组的时间间隔。您可以按每小时、每 4 小时或每 24 小时对数据进行分组。在柱形图上，**时间段长度**参数决定了列宽。

- **行动手册对警报和事故的覆盖情况**。活动警报和事故的数量。您可以选择要显示的组件：事故、警报或全部。

  环形图显示以下扇区的警报/事故：

  - 已启动“**自动**”操作模式行动手册的警报/事故。
  - 已启动“**训练**”操作模式行动手册的警报/事故。
  - 所有其他警报/事故。

- **使用行动手册节省的时间**。启动所有操作状态为*成功*或*警告*的行动手册所节省的时间。

  默认情况下不显示该小部件。

您可以通过单击任何行动手册小部件的名称来查看完整的行动手册列表。

- **触发沙盒扫描的IOA规则**。最常导致Kaspersky Anti Targeted Attack Platform提交文件供沙盒组件扫描的前10条IOA规则。
- **触发次数最多的IOA规则**。目标攻击分析器（TAA）技术检测到的事件中最常触发的10大IOA规则。
- **触发IOA规则的设备**。IOA触发频率最高的10台设备。

有关管理小部件的基础操作

小部件中数据显示的原则取决于图的类型。KUMA 支持以下图类型：

- 饼图 ( )。
- 计数器 ( )。
- 表格 ( )。
- 柱状图 ( )。
- 日期直方图 ( )。
- 折线图

有关常规小部件管理的基础操作

小部件的名称显示在小部件的左上角。通过单击包含事件、警报、事故或活动列表的小部件名称的链接，您可以转到 OSMP Console 的相应部分。

显示数据的租户列表位于小部件名称下方。

在小部件的右上角，显示了小部件上展示的数据所对应的时间段（例如，30 天 30d ）。请注意，由于缓存机制，控制板中显示的数据可能存在延迟。您可以将鼠标悬停在时间段图标上查看上次更新的日期和时间。

如果在小部件属性中启用了**显示上一时间段的数据**选项，并且小部件显示的是相对时间段的数据，则工具提示中还会显示上一时间段。上一时间段是相对于当前时间段计算的，即分别从当前时间段的开始时间和结束时间中减去当前时间段的持续时长。例如，如果数据每日更新并显示一个月，但该月只过去了前 10 天，则上一时间段为上个月的最后 10 天。

您可以单击时间段图标，然后在显示的窗口中选择确切日期或相对时间段，来更改小部件的数据显示时间段。如果您希望小部件显示布局中选择的时间段的数据，请单击**"重置"**按钮。更改布局中显示的时间段也会更改小部件中显示的时间段。

> 小部件中的时间以浏览器中设置的本地时区显示。

"**CSV**"按钮位于时间段图标的左侧。您可以按照 CSV 格式（UTF-8 编码）下载小部件上显示的数据。下载的文件名格式为：<小部件名称>_<下载日期 (YYYYMMDD)>_<下载时间 (HHMMSS)>.CSV。

小部件仅针对小部件或布局设置中选择的租户，显示在小部件或布局设置中选择的时间段所对应的数据。

如果您在小部件设置中启用了"**显示总计**"切换开关，则小部件会显示**总计**值，但当您以 CSV 格式下载小部件时，**总计**值不会显示。要在报告中显示**总计**值，您可以使用 Excel 公式或手动从小部件复制总计值。

有关管理饼图的基础操作

租户列表下方会显示一个带有图例的饼图。图例列出了与图表各扇形对应的类别名称。您可以左键单击图例中的类别，跳转到 OSMP 控制台中包含相关数据的部分。该部分中的数据根据小部件中指定的过滤器和/或搜索查询进行排序。

从小部件图例跳转到事件详情部分时，请注意您单击以跳转到事件部分的图例项的文本内容。文本中使用的任何反斜杠 (\) 或单引号 (') 字符在 SQL 查询文本中都会被转义。但是，斜杠 (/) 字符不会被转义。

在时间段图标下，将显示数据显示时间段内根据选定条件分组的事件、活动列表、资产、警报或事故的数量。

> 示例：
> - 在"**按状态分组的警报**"小部件中，在时间段图标下，显示了按"**新建**"、"**打开**"、"**已分配**"或"**已升级**"状态分组的警报数量。
>   如果只想查看状态为"**已打开**"和"**已分配**"的警报的图例，可以取消选中"**新建**"和"**已升级**"状态左侧的复选框。
> - 在"**事件**"小部件中，为其指定了 SQL 查询 `SELECT count(ID) AS `metric`, Name AS `value` FROM `events` GROUP BY Name ORDER BY `metric` DESC LIMIT 10`，时间段图标下方会显示 10 个事件，这些事件按名称分组并按降序排列。
>   如果要在图例中查看具有特定名称的事件，可以取消选中不想在图例中看到的事件名称左侧的复选框。

有关管理计数器图的基础操作

此类型的图显示所选数据的总和。

示例 1
"**资产数量**"小部件显示添加到 KUMA 的资产总数。
示例 2
如果您想查看趋势并将当前数据与过去一段时间的数据进行比较，可以创建一个显示上升或下降趋势的小部件。趋势可以在以下小部件中配置：

- **资产** → **资产数量**。
- **资产** → **自定义小部件**。
- **告警** → **活动告警**。
- **告警** → **未分配的告警**。
- **事故** → **活动事故**。
- **事故** → **未分配的事故**。
- **事故** → **所有事故**。
- **用户** -> AD **用户数量**。
  要配置趋势的显示，您需要启用"**显示上一时间段数据**"切换开关，然后在"外观"选项卡上选择一个趋势。如果无法计算百分比值，或者值相等，则会显示（ — ）图标。如果选择"**向上更佳**"，图表中将用绿色箭头表示上升趋势，红色箭头表示下降趋势。如果选择"**向下更佳**"，图表中将用红色箭头表示上升趋势，绿色箭头表示下降趋势。
  您可以点击数值来更改数据在小部件中的显示方式（例如，显示绝对值而不是百分比）。当小部件显示在仪表板上且电视模式已开启时，此功能可用。

有关管理表格图的基础操作

此类图以表格格式显示数据。

例如：
在 **事件** 小部件中，指定了 SQL 查询 `SELECT TenantID , Timestamp , Name , DeviceProduct , DeviceVendor FROM `events` LIMIT 10`，显示包含 **TenantID**、**Timestamp**、**Name**、**DeviceProduct** 和 **DeviceVendor** 列的事件表。该表包含 10 行。

您可以使用双色（红色和绿色）或三色（红色、黄色和绿色）渐变填充来自定义表格中数据的显示。选择渐变类型后，您可以点击切换方向图标 (⇆) 来调整填充方向并设置阈值。双色渐变需要指定两个值，三色渐变需要指定三个值。这些值会显示在图例中，并决定添加到所选列单元格的标记的颜色。该列在**渐变指示器字段**下拉列表中指定。

有关管理柱状图的基础操作

租户列表下方显示一个带图例的柱状图。图例列出了与图表中各柱条对应的类别名称。左键单击图例中的某个类别，即可跳转到 OSMP 控制台中包含对应数据的部分。该部分中的数据根据小部件中指定的过滤器和/或搜索查询进行排序。

从小部件图例跳转到事件详情部分时，请注意您单击以跳转到事件部分的图例项的文本内容。文本中使用的任何反斜杠 (\) 或单引号 (') 字符在 SQL 查询文本中都会被转义。但是，斜杠 (/) 字符不会被转义。

例如：
在指定了 SQL 查询 `SELECT sum(BytesIn) AS metric, DestinationAddress AS value FROM `events` WHERE (DeviceProduct = 'netflow' OR DeviceProduct = 'sflow') AND (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16')) GROUP BY DestinationAddress ORDER BY metric DESC LIMIT 10` 的 **Netflow 热门内部 IP** 小部件中，图表的 x 轴对应于总流量（以字节为单位），y 轴对应于目标端口地址。数据按目标地址分组，按总流量降序排列。

您还可以使用双色（红色和绿色）或三色（红色、黄色和绿色）渐变填充来自定义各柱条的显示。选择渐变类型后，您可以点击切换方向图标 (⇆) 来调整填充方向并设置阈值。双色渐变需要指定两个值，三色渐变需要指定三个值。这些值会显示在图例中，并决定各柱条的颜色。

有关管理日期直方图的基础操作

租户列表下方显示一个带图例的日期直方图。图例列出了与图表中各柱条对应的类别名称。左键单击图例中的某个类别，即可跳转到 OSMP 控制台中包含对应数据的部分。该部分中的数据根据小部件中指定的过滤器和/或搜索查询进行排序。

从小部件图例跳转到事件详情部分时，请注意您单击以跳转到事件部分的图例项的文本内容。文本中使用的任何反斜杠 (\) 或单引号 (') 字符在 SQL 查询文本中都会被转义。但是，斜杠 (/) 字符不会被转义。

如果在创建**日期直方图**类型的小部件时选择了**柱状图**视图，则可以使用双色（红色和绿色）或三色（红色、黄色和绿色）渐变填充来自定义各柱条的显示。选择渐变类型后，您可以点击切换方向图标 (⇆) 来调整填充方向并设置阈值。双色渐变需要指定两个值，三色渐变需要指定三个值。这些值会显示在图例中，并决定各柱条的颜色。

例如：

```
SELECT count(ID) AS `metric`, Timestamp AS `value`
FROM `events`
GROUP BY Timestamp
ORDER BY `metric` DESC
LIMIT 250
```

图表的 X 轴表示事件创建日期，Y 轴表示事件数量。图表中的各柱条从左到右按事件数量降序排列。

如果 SQL 查询中使用了带有`category`别名的附加字段，该柱状图将以堆叠柱状图的形式显示。在这种情况下，不会应用渐变填充。

例如：

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, Type AS `value`
FROM `events`
GROUP BY Timestamp, Type
ORDER BY metric DESC
LIMIT 250
```

X 轴表示时间间隔，Y 轴表示事件数量。柱条的每个分段对应标记为"**类型**"的字段的一个取值。

如果在创建**日期直方图**类型的小部件时选择了**折线图**视图，则有两种图表显示选项：单线图（如果查询中仅指定了`metric`和`value`字段）和多线图（如果使用了带有`category`别名的附加字段）。这样，您可以根据查询中用于分组的字段，比较不同组的值。例如，可以使用关联规则、用户或主机。此类图表不应用渐变填充。

例如：

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, CorrelationRuleName AS `value`
FROM `events`
WHERE Type = 3
GROUP BY Timestamp, CorrelationRuleName
ORDER BY metric DESC
LIMIT 250
```

图表在 X 轴上显示间隔（指定为`category`的字段）。Y 轴显示关联规则被触发的次数（标记为`metric`的字段）。图表中的每条折线对应`value`字段中的一个唯一值（在这种情况下为关联规则名称）。

您可以使用以下时间字段在日期直方图中进行分组：

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> 为了方便起见，建议使用支持的 ClickHouse 函数将时间字段（**时间戳**）中的值四舍五入，例如四舍五入到1小时或1天。

对于提供**折线图**视图的**日期直方图**小部件，您还可以配置平均值的显示。为此，在**外观**选项卡上的**回归分析**设置中，选择**局部加权回归**。

有关管理折线图的基础操作

租户列表下方显示一个带图例的折线图。图例显示了与图表中各折线对应的类别名称。左键单击图例中的某个类别，即可跳转到 OSMP 控制台中包含对应数据的部分。该部分中的数据根据小部件中指定的过滤器和/或搜索查询进行排序。

从小部件图例跳转到事件详情部分时，请注意您单击以跳转到事件部分的图例项的文本内容。文本中使用的任何反斜杠 (\) 或单引号 (') 字符在 SQL 查询文本中都会被转义。但是，斜杠 (/) 字符不会被转义。

例如：

在指定了 SQL 查询 `SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY `value` ASC LIMIT 250` 的 **事件** 小部件中，x 轴对应于近似端口号，y 轴对应于事件数。数据按端口号升序分组。

对于**折线图**小部件，您还可以配置平均值的显示。为此，在**外观**选项卡上的**回归分析**设置中，选择**线性回归**。如果图表显示多个类别，则会显示每个类别的平均值。

有关管理堆叠柱状图类型图表的基础操作

租户列表下方显示一个带图例的堆叠柱状图。图例显示构成每个柱条各部分的类别名称。每个类别左侧都有一个复选框，可用于隐藏或显示该类别。图表中柱条的数量与所选分组中的值数量相对应。各个柱条都带有标题。柱条中对应类别的颜色会自动分配。将鼠标悬停在柱条区域上时，会显示一个工具提示，其中包含值及其描述。您可以左键单击图例中的类别，跳转到 OSMP 控制台中包含相关数据的部分。

从小部件图例跳转到事件详情部分时，请注意您单击以跳转到事件部分的图例项的文本内容。文本中使用的任何反斜杠 (\) 或单引号 (') 字符在 SQL 查询文本中都会被转义。但是，斜杠 (/) 字符不会被转义。

柱条高度的含义取决于**格式**设置：

- 如果配置了“**绝对值**”格式，则柱条高度对应于所测指标的数值总和。
- 如果配置了“**相对值 (%)**”格式，则所有柱条的高度均为 100%，柱条上彩色区域的相对高度与数值比例相对应。

如果在基于堆叠柱状图创建自定义小部件时，您选择了**显示上一时间段数据**选项，并且查询中使用了标准的 `value`、`category`、`metric` 别名，则图表会将上一时间段的数据显示为单独的柱条。但是，如果查询中未使用标准的 `metric`，而是使用了带有非标准别名的自定义指标计算，则在显示图表时，**显示上一时间段数据**设置不会生效（请参阅下方查询示例）。

示例：
当基于**事件**小部件的 SQL 查询创建"**堆叠柱状图**"类型的自定义小部件时，适用以下规则：

- 查询中标记为 `value` 别名的字段（必填字段）在图表中用作创建图例并将柱条划分为类别的字段。
- 查询中标记为 `category` 别名的字段（必填字段）在图表中用作定义柱条沿 X 轴排列方式的字段。
- 查询中标记为 `metric` 别名的字段在图表中用作定义柱条区域计数方式的字段。在这种情况下，会自动执行分布。

但是，您可以通过使用标准聚合函数（`sum`、`avg`、`min`、`max`、`count`）以及您自己任意命名的别名作为指标来管理计数，而不是使用标准的 `metric` 别名（在这种情况下，不支持显示上一时间段的数据）。

示例 1：
对于"**事件**"小部件，指定了以下带有标准别名的 SQL 查询，并且在创建小部件时选择了"**显示上一时间段数据**"选项：

```
SELECT count(ID) AS `metric`,

Type AS `value`,

TenantID AS `category`

FROM `events`

GROUP BY value, category

ORDER BY metric DESC
```

X 轴表示租户（标记为 `category` 的字段），Y 轴表示特定类型事件的数量（标记为"值"的字段）。在每个柱条中，特定类型对应的数量用特定颜色表示。在图例中，用于划分柱条的事件类型名称会以类别的形式显示。每个类别在柱条上都有自动分配的对应颜色。如果您只想在图表中查看某些事件类型，可以取消选中或选中图例中对应事件类型左侧的复选框。

如果查询响应中收到了历史数据，则每个柱条旁边还会显示一个包含历史数据的附加柱条。

示例 2：
对于 **"事件"** 小部件，以下 SQL 查询中的自定义指标被标记为 `Base` 和 `Audit` 别名，而不是标准 `metric` 别名：

```
SELECT SUM(IF (Type = 1,1,0)) AS `Base`,

SUM(IF (Type = 4,1,0)) AS `Audit`,

TenantID as `category`

FROM `events`

GROUP BY category
```

X 轴表示租户（标记为 `category` 的字段），Y 轴表示每种类型事件的数量（标记为"基础"和"审计"别名的自定义指标）。在每个柱条中，特定指标对应的数量用特定颜色表示。在图例中，用于将柱条划分为不同类别的 `Base` 和 `Audit` 指标会以类别名称的形式显示。每个类别在柱条上都有自动分配的对应颜色。如果您只想在图表中查看与特定指标对应的事件，可以取消选中或选中图例中相关指标左侧的复选框。

即便在创建部件时选择了"显示上一时间段数据"选项，使用自定义指标的查询也不会显示带有历史数据的附加柱条。

示例 3：
对于"**事件**"小部件，可以使用标准别名指定以下 SQL 查询：

```
SELECT count(ID) AS `metric`,

TenantID as `value`,

Type as `category`

FROM events

GROUP BY value, category

ORDER BY metric DESC
```

与示例 1 中的类似查询不同，在本例中，X 轴代表事件类型（标记为 `category` 的字段），而租户（标记为 `value` 的字段）通过柱条中的数值范围（沿 X 轴方向）及图例中对应的标题来表示。

示例 4：
对于"**事件**"小部件，可以使用标准别名指定以下 SQL 查询：

```
SELECT count(ID) AS `metric`,

CAST(fromUnixTimestamp64Milli(Timestamp) AS DATE) AS `category`,

Type as `value`

FROM `events`

GROUP BY category, value

ORDER BY category DESC
```

图表 X 轴（标记为`category`的字段）显示的是月份中的日期。Y 轴显示特定类型事件的数量（标记为`value`的字段）。

要创建柱条按日期和/或时间排列的类似图表，请使用按以下`timestamp`类型的字段进行分组和排序的查询：

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> 建议使用**日期直方图**来处理按日期和/或时间排列的数据。

有关管理速度表图的基础操作

此类图表显示所选类别对象数量占特定时间段内对象总数的百分比。**速度表图**可用于以下对象：

- 某一类别中满足特定条件的资产数量与同一类别下资产总数或未分类资产数量的比较
- 满足特定条件的警报数量与特定时间段内警报总数的比较
- 满足特定条件的事故数量与事故总数的比较
- 满足特定条件的事件数量与特定时间段内事件总数的比较

图表上的值以百分比形式显示，颜色与已配置的数值范围相匹配。默认指定以下范围：0–30、30–70、70–100。

示例 1:
在“**资产**”自定义小部件中，用户可以选择一个资产类别，以便将该类别中的资产数量与资产总数进行比较。用户可以指定图表刻度的阈值。然后，系统会根据 Y 轴的一个或多个条件，使用现有的资产数据库进行计算。

示例 2:
在**警报**小部件中，您可以为**活动警报**和**未分配警报**类别选择**速度表图**图表类型。对于警报，需要选择租户和分析时间段。默认情况下，这些值与相关控制板中指定的值一致。在警报总数中，您还可以显示上一时间段的数据。

在“**事故**”小部件中，“**活动事故**”和“**未分配事故**”类别的百分比值按相同方式计算。

示例 3:
在**事件**小部件中，对于**速度表图**图表类型，用户可以指定租户、分析时间段和事件数据存储。SQL 查询如下所示：

```
SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

在小部件中显示数据的特殊注意事项

所显示数据的限制

为了提高可读性，KUMA 根据小部件的类型对显示的数据进行了限制：

- 饼图最多显示 20 个扇区。
- 柱状图最多显示 40 个柱形。
- 表格最多显示 500 个条目。
- 日期直方图最多显示 365 天。

超过指定限制的数据将显示在小部件的“**其他**”类别中。

您可以按照 CSV 格式下载完整数据，用于在小部件中构建分析数据。

汇总数据

日期直方图、柱状图和饼图上显示数据总和的格式取决于语言环境：

- 英语语言环境：每三位数字（千分位）用逗号分隔，小数部分用句点分隔。
- 俄语语言环境：每三位数字（千分位）用空格分隔，小数部分用逗号分隔。

创建小部件

您可以在创建或编辑布局时，在仪表板布局中创建小部件。

要创建小部件：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 创建布局或切换到所选布局的编辑模式。
3. 单击“**添加小部件**”。

4. 从下拉列表中选择一种小部件类型。
   将打开包含小部件参数的窗口。
5. 编辑小部件设置。
6. 如果要查看在小部件中的数据显示方式，请单击“**预览**”。
7. 单击“**添加**”。

小部件将出现在仪表板布局中。

编辑小部件

要编辑小部件：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 展开窗口右上角的列表。
3. 将鼠标光标悬停在相关布局上。
4. 单击编辑按钮（ ）。
   “**自定义布局**”窗口打开。
5. 在要编辑的小部件中，单击设置图标 ( )。
6. 选择“**编辑**”。
   将打开包含小部件参数的窗口。
7. 编辑小部件设置。
8. 在小部件设置窗口中，单击“**保存**”。
9. 在“**自定义布局**”窗口中，单击“**保存**”。

小部件已被编辑。

删除小部件

要删除小部件：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 展开窗口右上角的列表。
3. 将鼠标光标悬停在相关布局上。
4. 单击编辑按钮（ ）。
   “**自定义布局**”窗口打开。
5. 在要删除的小部件中，单击设置图标 ( )。

6. 选择“**删除**”。

7. 在打开的确认窗口中，单击“**确定**”。

8. 单击“**保存**”按钮。

小部件将被删除。

小部件设置

本部分介绍 KUMA 中所有可用小部件的设置。

事件小部件

您可以使用“**事件**”小部件来获取基于 SQL 查询的分析数据。

创建此小部件时，必须指定下表中描述的设置。

“常规”选项卡

下表描述了“**常规**”选项卡上的设置。

参数描述

设置	描述
名称	小部件名称。 以Excel格式保存报告时，工作表标题中显示的小部件名称长度限制为31个字符。建议您在命名小部件时留意此限制。
图表	图表类型。可用的图类型包括： • **饼图**。 • **柱状图**。 • **计数器**。 • **折线图**。 • **表格**。 • **日期直方图**。 • **堆叠柱状图** • **速度表图**
格式	数据显示格式：**绝对值**或**相对值 (%)**。此设置适用于**堆叠柱状图**。 如果选择“**绝对值**”格式，柱状图的高度对应于所测量指标值的总和。如果选择了**相对值（%）**格式，则所有柱条的高度均为100%，柱条上彩色区域的相对高度与指标数值比例相对应。 默认选择“**绝对值**”。
时间线视图	时间数据显示格式：**柱状图**或**折线图**。此设置适用于“**日期直方图**”类型的图表。 选择“**柱状图**”格式时，数据默认以垂直柱条显示。如果 SQL 查询包含带有类别别名的附加字段，则图表将变为堆叠柱状图，即每个柱条根据该字段的值划分成若干分段。 选择“**折线图**”格式时，数据将显示为一条或多条（取决于查询）贯穿时间轴上各点的折线。 默认选中“柱状图”格式。
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。
时间段	小部件中显示的数据所对应的时间段。默认值为“**按布局**”，表示将显示针对布局所选时间段内的数据。 您还可以通过以下方式之一为小部件指定时间段： • 在日历中选择时间段的确切开始和结束日期及时间，然后单击“**应用**”。 • 在“**相对时间段**”列表中选择相对于当前时间的时间段。 • 手动指定一个值：选择确切的日期和时间，或相对时间段，也可两者结合。 详情请参见下方的“*配置时间段*”小节。
显示上一时间段数据	启用同时显示两个时间段的数据：当前时间段和上一时间段。 使用**堆叠柱状图**时，如果查询包含标准别名：`value`、`category`、`metric`，则会考虑**显示上一时间段数据**设置。但是，如果查询不使用标准的`metric`，而是使用带有非标准别名的自定义指标计算，则不会考虑**显示上一时间段数据**设置。

设置	描述
定义的变量	可用于过滤小部件数据的局部或全局变量。 单击“**添加**”。如果要添加本地变量，请输入变量的任意名称，然后输入变量的值。如果要添加全局变量，请在列表中选择您在控制板属性中指定的变量名称。
存储	用于搜索事件的存储。此列表显示可用空间。您只能选择一个存储，但可以选择一个或多个空间。“**存储**”字段中的值与“**租户**”字段中选择的租户无关。该字段显示存储和空间，与“**事件**”部分中一样。在存储中创建新空间时，默认情况下不会在小部件设置中选中该新空间。 您必须手动选择新空间。 如果用户有权访问小部件中列出的所有空间，则小部件可以显示用户权限中所设空间内指定租户的事件信息。 如果用户对存储中的一个或多个空间无访问权限，小部件将无法显示信息；用户无法编辑该小部件，但可通过“**复制**”按钮复制小部件。复制操作与存储空间的访问权限无关。如果在具有用户不可访问空间的小部件中复制模板，“**存储**”字段的值将被重置。此类小部件将显示错误：“访问被拒绝”（由于允许和已选事件空间的限制，操作未返回任何结果）。要保存模板，您需要在小部件中指定空间。 在具有用户可访问空间的小部件中，“**存储**”字段的值不会被重置，并且在复制模板时会被保存。 当用户下载模板时，下载文件中会隐藏不可访问文件的数据。 如果用户的电子邮件地址包含在计划报告的收件人列表中，则无论哪些空间可访问，用户都将收到完整版本的报告。

设置	描述

SQL 查询字段	用于手动过滤和搜索事件的查询。您可以通过单击“**使用 SQL 构建器**”在构建器中创建查询。
	您可以使用扩展事件模式字段来创建“**表格**”类型的图表。
	示例
	先决条件：
	事件来自 FWSaaS 系统。
	10.08.2023 12:12:12 src=10.10.10.10 ReqUrls=[https://google.com, https:/ya.ru]
	10.08.2023 12:12:23 src=10.10.10.20 ReqUrls=[https://google.com, https:/yndex.ru]
	10.08.2023 12:12:33 src=10.10.10.30 ReqUrls=[https://google.com, https:/ya.ru, https://mail.ru]
	KUMA 主管理员已在 KUMA 的“**设置**” →“**其他**” →“**高级事件模式字段**”部分添加了一个扩展事件模式字段。在 KUMA 规范化器中，已为“**ReqUrls**”和“**SA.urls**”字段配置了字段映射。
	在 KUMA 中，规范化事件的格式如下：
	DeviceReceiptTime=10.08.2023 12:12:12 SourceAddress=10.10.10.10 SA.urls=[https://google.com, https:/ya.ru]
	DeviceReceiptTime=10.08.2023 12:12:23 SourceAddress=10.10.10.20 SA.urls=[https://google.com, https:/yandex.ru]
	DeviceReceiptTime=10.08.2023 12:12:30 SourceAddress=10.10.10.30 SA.urls=[https://google.com, https:/ya.ru, https://mail.ru]
	您想要构建一个“30 分钟内访问量最高的 URL”控制板。以下是“**事件**”部分和小部件中的请求示例：
	SELECT res.1 AS url, res.2 AS count FROM (SELECT arrayJoin(groupArray((url, count))) AS res FROM (SELECT url, count() AS count FROM (SELECT SA.urls AS urls FROM `events`) ARRAY JOIN urls AS url GROUP BY url) GROUP BY url)
	结果：
	url count
	google.com 3
	ya.ru 2
	mail.ru 1
	yandex.ru 1
	KUMA 支持以下允许在查询中使用数组的函数：
	• `groupArray` 函数将 x 参数的所有值打包到一个数组中，并在对数据进行分组时用于聚合函数。
	• `arrayJoin` 函数会将数组展开为独立的字符串，并作为查询结果返回。
	您可以在 SQL 查询中使用变量。您只能在手动创建查询时指定变量。您不能在 SQL 构建器中使用变量。
	使用变量的示例
	带有局部变量的 SQL 查询示例
	`SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name) GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250`
	此查询使用局部变量 `$Name`。`Name` 事件字段的值将代入此变量。您可以通过点击小部件上的漏斗图标（ ）来应用该变量。这将打开一个窗口；在该窗口中，您可以为变量指定一个值。小部件会根据 `Name` 字段的选定值筛选数据。
	请注意，如果在 SQL 查询中为接收数值的字段指定了变量，则必须将该值转换为字符串。您可以使用 `toString` 函数执行此操作。否则，SQL 查询将返回错误。
	示例
	`SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250`
	在此查询中，`SourcePort` 事件字段的值为数值，因此该值将转换为字符串：`toString(SourcePort)`。
	有关在查询构造函数中创建 SQL 查询的详细信息，请参见下文。
	应用以下限制条件：
	• 除表格外，任何类型的事件分析小部件都无法编辑 SQL 查询中的 `metric` 和 `value` 别名。
	• 在采用“**表格**”类型图表的部件中，别名可包含拉丁和西里尔字符，以及空格。使用空格或西里尔字符时，别名必须用引号括起来：`"An alias with a space"`、`` `Another alias` ``。
	• `ARRAY JOIN` SQL 查询不受支持。
	• 在显示前一时间段的数据时，按 `count(ID)` 参数进行排序可能无法正常生效。建议按 `metric` 参数排序。例如，`SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`。
	• 在采用 **“计数器”** 类型图表的小部件中，必须为 `SELECT` 函数的值指定数据处理方式：`count`、`max`、`min`、`avg`、`sum`。

设置	描述
	• 在采用 **"表格"** 类型图表的小部件中，渐变效果会依据 SQL 查询中指定的数值或时间字段（例如 `Timestamp`）的值来绘制。可从"**渐变指示器字段**"下拉列表中选择此字段（若查询包含多个数值或时间字段，可任选其一）。之后，所选列的单元格将以渐变填充标记突出显示。如果查询中不存在某个字段，**外观**选项卡不会显示**渐变**和**渐变指示器字段**这两个字段。 • 在采用 **堆叠柱状图** 的小部件中，使用标准查询时，X 轴上不显示 `Timestamp` 值。如果要沿 X 轴显示时间，建议使用**折线图**。如果需要使用 **堆叠柱状图**，必须将 `Timestamp` 值转换为字符串：`toString(Timestamp) AS `category``。

配置时间段

要配置数据显示时间段，请执行以下操作之一：

- 如有必要，请按以下方式之一更改"**时间段**"设置中的日期和时间：
  - 如果要指定**确切日期**，请在日历中选择时间段的开始日期和结束日期，然后单击**应用**。

    您可以选择包括当前日期在内的任意日期。日期和时间格式取决于浏览器的设置。如果 **开始时间**或 **结束时间**字段已有值，且您没有手动修改时间值，则在日历中选择日期时，**开始时间**字段会自动填入 `00:00:00,000`，**结束日期**字段会自动填入 `23:59:59,999`。如果您手动删除了 **开始时间**或 **结束时间**字段中的值，则在日历中选择日期时，该字段会自动填入当前时间。在一个字段中选择值后，焦点会切换到另一个字段。如果 **结束时间**的值早于 **开始时间**的值，系统会自动将这个较早的值填入 **开始时间**字段。

  - 如果要指定**相对时间段**，请从**相对时间段**列表中选择一个时间段。

    时间段是相对于当前时间计算的。

  - 如果要指定**自定义时间段**，请手动设置或修改 **开始时间**和 **结束时间**字段的值。

    您可以按俄语本地化版本的 `DD.MM.YYYY HH:mm:ss.SSS` 格式或英语本地化版本的 `YYYY-MM-DD HH:mm:ss.SSS` 格式输入确切的日期和时间，也可以使用公式输入相对于当前时间的时间段。您也可以组合使用这些方法。如果输入确切日期时未指定毫秒数，系统会自动补入 `000`。如果您修改了 **开始时间**或 **结束时间**字段中的时间，在日历中选择日期不会更改时间部分。

    在相对时间段公式中，您可以使用表示当前日期和时间的参数 `now`，以及时间间隔参数化语法：`+`（仅用于 **结束时间**字段）、`-`、`/`（舍入到最接近的值）；还可以使用以下时间单位：`y`（年）、`M`（月）、`w`（周）、`d`（天）、`h`（小时）、`m`（分钟）、`s`（秒）。例如，您可以指定时间段 `now-5d`，以获取过去五天的数据；也可以指定 `now/w`，以获取从本周第一天开始时（00:00:00:000 UTC）到当前时间（`now`）的数据。

    > **开始时间**字段为必填项，其值不能晚于 **结束时间**字段的值；如果指定确切日期或相对时间段，其值也不能早于 1970-01-01。**结束时间**不能早于**开始时间**。如果未在**结束时间**字段中指定值，系统会自动填入 `now`。

卡巴斯基 SIEM 以 UTC 存储时间值，但 Web 界面会将时间转换为浏览器所在时区的时间。这与相对时间段相关：**今天**、**昨天**、**本周**和**本月**。例如，如果浏览器所在的时区是 UTC+3，并且您选择"**今天**"作为数据显示时间段，则将显示从 03:00:00.000 到现在的数据，而不是从 00:00:00.000 到现在的数据。

如果希望在选择**今天**、**昨天**、**本周**或**本月**等相对数据显示时间段时考虑您所在的时区，则需要在 **开始时间**和 **结束时间**（如果指定的值不是 `now`）中，通过增加或减去相应的小时数来手动调整时间偏移量。例如，如果浏览器所在的时区是 UTC+3，而您想显示**昨天**的数据，则需要将**开始时间**改为 `now-1d/d-3h`，并将**结束日期**改为 `now/d-3h`。如果要显示**今天**的数据，只需将**开始时间**字段的值改为 `now/d-3h`。

> 如果您需要截至昨天 23:59:59:999 UTC 的结果，可以使用带有时间戳过滤器的 SQL 查询，或者指定确切的日期和时间。

时间段的边界为闭区间（包含端点）：例如，对于"**今天**"的时间范围，将显示从当天起始时刻 (00:00:00:000 UTC) 到当前时刻（**now**）包含两端点的事件；而对于"**昨天**"的时间段，将显示从前一日起始时刻 (00:00:00:000 UTC) 到当日起始时刻 (00:00:00:000 UTC) 的事件。将鼠标悬停在小部件中的时间段图标上，即可查看上次数据更新的日期和时间以及数据显示所对应的确切时间段。

如果小部件启用了**"显示上一时间段数据"**设置，并且小部件显示的是相对时间段的数据，则工具提示也会显示上一时间段。上一时间段的计算方法是：用当前时间段的开始时间和结束时间减去当前时间段的持续时间。例如，如果数据每日更新并显示一个月，但该月只过去了前 10 天，则上一时间段为上个月的最后 10 天。

- 如果您希望小部件显示布局中选择的时间段的数据，请单击**"重置"**按钮。更改布局中显示的时间段也会更改小部件中显示的时间段。

如何在"构建器"中创建查询

要在"构建器"中创建查询：

1. 指定以下参数的值：

   a. **SELECT** — 应返回的事件字段。可用字段的数量取决于所选的图类型。

   - 在左侧的下拉列表中，选择要在窗口小部件中显示数据的事件字段。
   - 中间字段显示所选字段在窗口小部件中的用途："**指标**"或"**值**"。

     > 如果您选择了"**表格**"图类型，则在中间字段中，必须使用 ANSII-ASCII 字符指定列名。

   - 在右侧的下拉列表中，您可以选择要对数据执行的操作：
     - **计数** — 事件计数。此操作仅适用于"ID"事件字段。默认情况下用于折线图、饼图、柱状图和计数器。这是日期直方图的唯一选项。
     - "**最大值**"是事件分类中"**事件**"字段的最大值。
     - "**最小值**"是事件分类中"**事件**"字段的最小值。
     - "**平均值**"是事件分类中"**事件**"字段的平均值。
     - "**总和**"是来自事件分类中"事件"字段值的总和。

   b. "**源**"是数据源的类型。仅"**事件**"值可供选择。

   c. "**条件**" — 事件过滤条件。

   - 在左侧下拉列表中，选择要用于过滤的事件字段。
   - 从中间下拉列表中选择必要的运算符。可用的运算符取决于所选事件字段的值的类型。
   - 在右侧下拉列表中，输入条件的值。根据所选字段类型，您可能需要手动输入、从下拉列表中选择或在日历上选择该值。

   您可以单击"**添加条件**"来添加搜索条件，或单击 ✕ 来删除搜索条件。

   您还可以单击"**添加组**"来添加条件组。默认情况下，使用"AND"运算符来添加条件组，也可以根据需要进行更改。可用值：**AND**、 **OR**、**NOT**。单击"**删除组**"按钮可删除条件组。

   d. **分组依据** — 用于对返回的数据进行分组的事件字段或别名。此参数不适用于"**计数器**"图类型。

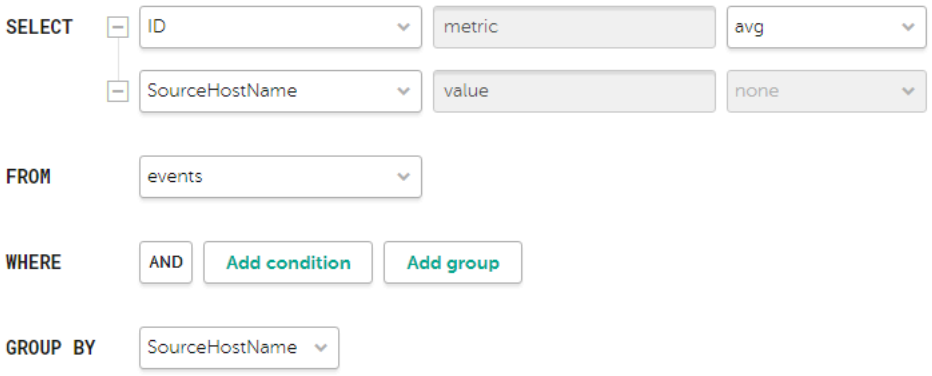
e. **排序依据** – 作为返回数据排序依据的列。此参数不适用于“**日期直方图**”和“**计数器**”图类型。

- 在左侧的下拉列表中，选择将用于排序的值。
- 从右侧的下拉列表中选择排序顺序：“**ASC**”表示升序，“**DESC**”表示降序。
- 对于“**表格**”类型的图，可以通过单击“**添加列**”来添加排序条件。

f. “**LIMIT**”表示小部件的最大数据点数。此参数不适用于“**日期直方图**”和“**计数器**”图表类型。

2. 单击“**应用**”。

查询构建器中的搜索条件示例



用于在小部件中显示每个主机平均字节数的搜索条件参数

“坐标轴”选项卡

下表描述了“**坐标轴**”选项卡上的设置。

> 如果您在“**常规**”选项卡的“**图表**”字段中选择了以下值之一，则会显示此选项卡：“**柱状图**”、“**折线图**”或“**日期直方图**”。

参数描述

设置	描述
点大小	图上的点大小。“**折线图**”图类型会显示此字段。
线宽	图表上线条的宽度。“**折线图**”图类型会显示此字段。
Y 轴的最小值和最大值	Y 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非“**自动**”）来修正。
X 轴的最小值和最大值	X 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非“**自动**”）来修正。
小数	显示值需要四舍五入后保留的小数位数。

“外观”选项卡

下表描述了**外观**选项卡上的设置。

参数描述

设置	描述
描述	小部件描述。
显示图例	显示分析数据图例。默认情况下，切换开关处于打开状态。
在图例中显示空值	显示图例中用于分析数据的带有空值的参数。默认情况下，切换开关处于打开状态。 仅当启用了"**显示上一时间段数据**"设置且当前时间段没有数据，但上一时间段有数据时，才会显示空值。
颜色	用于显示信息的颜色： • "**默认**"表示浏览器的默认字体颜色 • **绿色** • **红色** • **蓝色** • **黄色** 此设置适用于**柱状图**、**计数器图**、**折线图**、**日期直方图**等图表。
渐变	图表的渐变填充： • 两种颜色（红色和绿色） • 三种颜色（红色、黄色和绿色） 此设置适用于**柱状图**、**日期直方图**（类型为**柱状图**）、**表格**等图表。 您可以通过点击切换方向图标 (⇆) 来调整填充方向并设置阈值。 如果未手动设置，渐变阈值将根据数据自动计算。如果在指定的阈值之间没有数据，则不会应用渐变。而是使用两种颜色：一种用于低于下限阈值的值，另一种用于高于上限阈值的值。
渐变指示器字段	显示渐变填充指示器的列。 此设置适用于"**表格**"类型的图表。
水平	将直方图水平显示，而非垂直显示。 启用此选项后，当小组件显示大量数据时，将不支持水平滚动，所有可用信息会自适应调整以适配小部件的固定尺寸。如果要显示大量数据，建议扩大小部件的尺寸。
显示总和	显示所有值的总和。 数值的舍入方式由**小数位数**设置决定。 此设置适用于**饼图**、**柱状图**和**日期直方图**类型的图表。 默认情况下，此切换开关处于关闭状态。
时间段的分段长度	您希望将该时间段拆分为若干分段后，每个分段的持续时长。适用于"**日期直方图**"类型的图表。
刻度	数据显示刻度。适用于**堆叠柱状图**。可用值如下： • **线性图** • **方形图** • **对数图** 默认值为**线性图**。
回归分析	用于在图表上指示平均值的选项。可用值如下： • **未设置**。 • **线性图** • **局部加权回归**（局部估计散点平滑曲线）。 适用于"**日期直方图**"和"**折线图**"类型。

"操作"选项卡

> 如果您在**常规**选项卡的**图表**字段中选择了以下值之一，则不会显示此选项卡：**计数器**、**速度表图**、**表格**。

此选项卡上的设置允许您配置对小部件各种元素（例如图表分段或图例项的文本）的左键单击操作。您可以选择以下操作：

- 转到事件。
- 按变量过滤。

  这些设置已在过滤多个小部件中的数据场景中进行了描述。

- 向下钻取到另一个控制板。

  这些设置已在深层探究到另一个控制板场景中进行了描述。

活动列表小部件

您可以使用“**活动列表**”小部件来获取基于 SQL 查询的分析数据。

创建此小部件时，必须指定下表中描述的设置。

“常规”选项卡

下表列出了必须在“**通用**”选项卡上指定的设置。

参数描述

设置	描述
图表	图表类型。可用的图类型包括： • **柱状图** • **饼图** • **计数器** • **表格**
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。
关联器	包含您要接收数据的活动列表的关联器名称。
活动列表。	您要接收数据的活动列表的名称。 不同的关联器可以使用相同的活动列表。但是，每个关联器都会创建一个单独的活动列表实体。因此，即使活动列表具有相同的名称和 ID，不同关联器使用的活动列表内容也会有所不同。

设置	描述
SQL 查询字段	此字段允许您手动输入查询，用于过滤和搜索活动列表数据。 查询结构与事件搜索中使用的查询结构类似。 基于活动列表创建查询时，必须考虑以下几点： • 对于 FROM 函数，必须指定“记录”值。 • 如果要接收名称包含空格和西里尔字符的字段数据，还必须在查询中将这些名称括在引号中： • 在 SELECT 函数中，将别名括在双引号或反引号中："alias"、`another alias`。 • 在 ORDER BY 函数中，将别名括在反引号中：`另一个别名`。 • “事件”字段值括在直单引号中：WHERE DeviceProduct = 'Microsoft'。 • 事件字段名称无需用引号括起来。 • 如果活动列表字段名称以空格开头或结尾，则小部件不会显示这些空格。字段名称不能仅包含空格。 • 如果活动列表字段的值包含尾随空格或前导空格，建议使用 LIKE '%field value%' 函数进行搜索。 • 您可以在查询中使用服务字段：_key（包含活动列表记录键的字段）和 _count（此记录添加到活动列表的次数），以及自定义字段。 • 除表格外，任何类型的活动列表分析小部件都无法编辑 SQL 查询中的“指标”和“值”别名。 • 如果在 SQL 查询中使用了日期和时间转换函数（例如 fromUnixTimestamp64Milli），并且正在处理的字段不包含日期和时间，则小部件中将显示错误。为避免这种情况，请使用可以处理空值的函数。示例：SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250。 • LIMIT 函数的值过大可能会导致浏览器错误。 • 如果选择“计数器”作为图表类型，则必须为 SELECT 函数的值指定数据处理方式：`count`、`max`、`min`、`avg`、`sum`。 • 在采用**“表格”**类型图表的小部件中，渐变效果是根据 SQL 查询中指定的字段（例如`_count`、`value`、`temp`或`name`）的值绘制的。可从“**渐变指示器字段**”下拉列表中选择此字段（若查询包含多个数值或时间字段，可任选其一）。之后，所选列的单元格将以渐变填充标记突出显示。如果查询中不存在某个字段，**外观**选项卡不会显示**渐变**和**渐变指示器字段**这两个字段。 在 SQL 函数和 SELECT 中使用别名时，需要特别注意，可以使用双引号和反引号："、`。 如果选择“计数器”作为图类型，别名可以包含拉丁字符、西里尔字符以及空格。使用空格或西里尔字符时，别名必须使用引号括起来："An alias with a space"、`Another alias`。 在显示前一时间段的数据时，按 count(ID) 参数进行排序可能无法正常使用。建议按照指标参数排序。例如，SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250。

您可以在小部件中获取租户的名称，而不是他们的 ID。

如果您希望在活动列表小部件中显示租户名称而非租户 ID，请在关联器的关联规则中配置用于使用相应租户信息填充活动列表的函数。配置过程包括以下步骤：

1. 导出租户列表。
2. 创建一个“**表格**”类型的字典，并将之前获取的租户列表导入该字典。
3. 在关联规则中添加一个局部变量，通过“**dict**”函数将租户名称映射到租户 ID。
   例如：
   - 变量：`TenantName`
   - 值：`dict ('<Name of the previously created dictionary with tenants>', TenantID)`
4. 在关联规则中添加一个包含活动列表的操作。此操作将使用 **Set** 函数将先前创建的变量的值以“键-值”对格式写入活动列表。将活动列表的字段（例如 `Tenant`）指定为密钥，并在“**值**”字段中引用先前创建的变量（例如 `$TenantName`）。

当此规则触发时，通过 **dict** 函数将租户字典中的 ID 映射得到的租户名称会被放入活动列表中。创建活动列表的小部件时，您可以通过引用活动列表的字段名称来获取租户名称（在上例中为 `Tenant`）。

上述方法可应用于其他带有 ID 的事件字段。

用于接收基于活动列表的分析数据的 SQL 查询示例：

- `SELECT * FROM `records` WHERE "Event source" = 'Johannesburg' LIMIT 250`
  此查询返回活动列表中字段名称为"事件源"且该字段值为"约翰内斯堡"的键。
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  饼图查询：返回活动列表中的键数量（对"_key"字段执行"count"聚合）以及"状态"自定义字段的所有取值。该小部件显示一个饼图，其中包含活动列表中的记录总数，并按"**状态**"字段的可能值数量进行比例划分。
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  查询表：返回"**名称**"和"**状态**"自定义字段的值，以及活动列表中"描述"自定义字段值与 ILIKE '%ftp%' 匹配的记录所对应的服务字段"_count"。该小部件显示一个包含"**状态**"、"**名称**"和"**编号**"列的表格。

"坐标轴"选项卡

下表列出了必须在"**坐标轴**"选项卡中指定的设置。

当在"**通用**"选项卡的"**图表**"字段中选择了"**柱状图**"时会显示此选项卡。

参数描述

设置	描述
Y 轴最小值和最大值	Y 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非"**自动**"）来修正。
X 轴最小值和最大值	X 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非"**自动**"）来修正。

"外观"选项卡

下表列出了必须在"**外观**"选项卡中指定的设置。

参数描述

设置	描述
名称	小部件名称。
描述	小部件描述。
颜色	用于显示信息的颜色： • "**默认**"表示浏览器的默认字体颜色 • **绿色** • **红色** • **蓝色** • **黄色**
渐变	图表的渐变填充： • 两种颜色（红色和绿色） • 三种颜色（红色、黄色和绿色） 此设置适用于柱状图和表格。 您可以通过点击切换方向图标 (⇆) 来调整填充方向并设置阈值。 如果未手动设置，渐变阈值将根据数据自动计算。如果在指定的阈值之间没有数据，则不会应用渐变。而是使用两种颜色：一种用于低于下限阈值的值，另一种用于高于上限阈值的值。
渐变指示器字段	显示渐变填充指示器的列。 此设置适用于"**表格**"类型的图表。
水平	将直方图水平显示，而非垂直显示。 启用此设置后，所有可用信息都将适配至配置的小部件尺寸。如果数据量很大，您可以增加小部件的尺寸以获得最佳显示效果。
显示总和	显示值的总和。

设置	描述
显示图例	显示分析数据图例。默认情况下，切换开关处于打开状态。
在图例中显示空值	显示图例中用于分析数据的带有空值的参数。默认情况下，切换开关处于打开状态。 仅当启用了“**显示上一时间段数据**”设置且当前时间段没有数据，但上一时间段有数据时，才会显示空值。

上下文表小部件

您可以使用“**上下文表**”小部件获取基于 SQL 查询的分析。

创建此类型的小部件时，必须设置以下设置的值：

选项卡：

下表列出了必须在“**通用**”选项卡上指定的设置。

参数描述

设置	描述
图表	可用的图类型包括： • **柱状图** • **饼图** • **计数器** • **表格**
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。
关联器	包含您要接收信息的上下文表的关联器名称。
上下文表	您要接收信息的上下文表名称。 同一个上下文表可用于多个关联器。但是，每个关联器都会创建一个单独的上下文表实体。因此，即使上下文表具有相同的名称和 ID，不同关联器使用的上下文表的内容也不同。

设置	描述
SQL 查询字段	此字段允许您手动输入查询，用来过滤和搜索上下文表数据。默认情况下，对于每种小部件类型，该字段包含一个查询，用于获取上下文表架构以及按关键字段获取的键。 查询结构与事件搜索中使用的查询结构类似。 基于上下文表创建查询时，必须考虑以下事项： • 对于 FROM 函数，必须指定 `records` 值。 • 您只能获取上下文表架构中指定字段的数据。 • 您可以使用受支持的 ClickHouse 功能。 • 如果要接收名称包含空格和西里尔字符的字段数据，还必须在查询中将这些名称括在引号中： • 在 SELECT 函数中，将别名括在双引号或反引号中："<别名>"、`<另一个别名>`。 • 在 ORDER BY 函数中，将别名括在反引号中：`<另一个别名>`。 • 事件字段值括在直引号中：WHERE DeviceProduct = 'Microsoft'. • 事件字段名称无需用引号括起来。 • 如果活动列表字段名称以空格开头或结尾，则小部件不会显示这些空格。字段名称不能仅包含空格。 • 如果活动列表字段的值包含尾随空格或前导空格，建议使用 LIKE '%< 字段值 >%' 函数按这些值进行搜索。 • 您可以使用 _count 服务字段（此记录已添加到上下文表的次数）以及自定义字段。 • 除表格外，对于任何类型的活动列表分析小部件，都无法编辑 SQL 查询中的 metric 和 value 别名。 • 如果在 SQL 查询中使用了日期和时间转换函数（例如 fromUnixTimestamp64Milli），并且正在处理的字段不包含日期和时间，则小部件中将显示错误。为避免这种情况，请使用可以处理空值的函数。示例：SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250。 • LIMIT 函数的值过大可能会导致浏览器错误。 • 如果选择 **计数器** 作为图表类型，则必须为 SELECT 函数的值指定数据处理方法：count、max、min、avg、sum。 • 在图表类型为 **表格** 的小部件中，渐变仅适用于 **INT** 和 **FLOAT** 类型的字段以及 **_count** 字段。您可以从**渐变指示器字段**下拉列表中选择字段。之后，所选列的单元格将以渐变填充标记突出显示。 在 SQL 函数和 SELECT 语句中使用别名时的特别注意事项：可以使用双引号和反引号："、`。 使用空格或西里尔字符时，别名必须用双引号括起来：<带空格的别名>"，值必须用直单引号括起来：'<带空格的值>' 显示上一时间段的数据时，按 count(ID) 参数排序可能无法正常工作。我们建议按 metric 参数排序。例如，SELECT count(ID) AS "metric"、Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250。

您可以在小部件中获取租户的名称，而不是他们的 ID。

如果您希望在活动列表小部件中显示租户名称而非租户 ID，请在关联器的关联规则中配置用于使用相应租户信息填充活动列表的函数。配置过程包括以下步骤：

1. 导出租户列表。
2. 创建一个“**表格**”类型的字典，并将之前获取的租户列表导入该字典。
3. 在关联规则中添加一个局部变量，通过“**dict**”函数将租户名称映射到租户 ID。
   例如：
   - 变量：TenantName
   - 值：dict ('<Name of the previously created dictionary with tenants>', TenantID)
4. 在关联规则中添加一个包含活动列表的操作。此操作将使用 **Set** 函数将先前创建的变量的值以“键-值”对格式写入活动列表。将活动列表的字段（例如 Tenant）指定为密钥，并在“**值**”字段中引用先前创建的变量（例如 $TenantName）。

当此规则触发时，通过 **dict** 函数将租户字典中的 ID 映射得到的租户名称会被放入活动列表中。创建活动列表的小部件时，您可以通过引用活动列表的字段名称来获取租户名称（在上例中为 Tenant）。

上述方法可应用于其他带有 ID 的事件字段。

用于接收基于活动列表的分析数据的 SQL 查询示例：

- `SELECT * FROM `records` WHERE "Event source" = 'Johannesburg' LIMIT 250`
  此查询返回活动列表中字段名称为"`Event source`"且该字段值为"`Johannesburg`"的密钥。
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  饼图查询：返回活动列表中的密钥数量（对"**_key**"字段执行"`count`"聚合）以及"状态"自定义字段的所有取值。该小部件显示一个饼图，其中包含活动列表中的记录总数，并按"**状态**"字段的可能值数量进行比例划分。
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  查询表：返回"**名称**"和"**状态**"自定义字段的值，以及活动列表中"描述"自定义字段值与`ILIKE '%ftp%'`匹配的记录所对应的服务字段"**_count**"。该小部件显示一个包含"**状态**"、"**名称**"和"**编号**"列的表格。

选项卡：

下表列出了必须在"**坐标轴**"选项卡中指定的设置。

当在"**通用**"选项卡的"**图表**"字段中选择了"**柱状图**"时会显示此选项卡。

参数描述

设置	描述
Y 轴 and **最小值 - 最大值**	Y 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非"**自动**"）来修正。
X 轴 and **最小值 - 最大值**	X 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非"**自动**"）来修正。

选项卡：

下表列出了必须在"**外观**"选项卡中指定的设置。

参数描述

设置	描述
名称	小部件名称。
描述	小部件描述。
颜色	用于显示信息的颜色： • "**默认**"表示浏览器的默认字体颜色 • **绿色** • **红色** • **蓝色** • **黄色**
渐变	图表的渐变填充： • 两种颜色（红色和绿色） • 三种颜色（红色、黄色和绿色） 此设置适用于**柱状图**和**表格**。 您可以通过点击切换方向图标 (⇆) 来调整填充方向并设置阈值。 如果未手动设置，渐变阈值将根据数据自动计算。如果在指定的阈值之间没有数据，则不会应用渐变。而是使用两种颜色：一种用于低于下限阈值的值，另一种用于高于上限阈值的值。
渐变指示器字段	显示渐变填充指示器的列。 此设置适用于"**表格**"类型的图表。

设置	描述
水平	将直方图水平显示，而非垂直显示。 启用此设置后，所有可用信息都将适配至配置的小部件尺寸。如果数据量很大，您可以增加小部件的尺寸以获得最佳显示效果。
显示总和	显示值的总和。
显示图例	显示分析数据图例。默认情况下，切换开关处于打开状态。
在图例中显示空值	显示图例中用于分析数据的带有空值的参数。默认情况下，切换开关处于打开状态。 仅当启用了"**显示上一时间段数据**"设置且当前时间段没有数据，但上一时间段有数据时，才会显示空值。

资产自定义小部件

您可以使用**资产→自定义小部件**，通过查询构建器从已处理的事件中获取高级资产分析。在查询中，您需要指定资产字段以及用于统计资产的相应条件或条件集（Y轴）。您还可以指定一个或多个附加条件（类别），用于比较每个字段的资产数量。

为资产创建自定义小部件时，您必须指定下表中描述的设置。

"常规"选项卡

下表描述了"**常规**"选项卡上的设置。

参数描述

设置	描述
名称	小部件名称。 以Excel格式保存报告时，工作表标题中显示的小部件名称长度限制为31个字符。建议您在命名小部件时留意此限制。
图表	图表类型。可用的图类型包括： • **饼图**。 所有选定的租户都会显示按指定类别划分的资产分布情况。 • **计数器**。 资产根据单一条件进行统计。图表显示所有选定租户中符合该条件的资产总数。 • **表格**。 资产根据所有选定租户的指定类别进行统计。图表中的每个类别都对应一行。类别名称显示在**值**列中。符合条件的资产数量显示在**指标**列中。 • **堆叠柱状图** 资产按所有选定租户的指定类别进行统计，您可以按租户对资产进行分组（在这种情况下，各个租户沿X轴排列）。每个类别在图表的柱条上都有自己的区域，并以不同的颜色表示。类别名称显示在图例中。您可以使用类别名称左侧的复选框来隐藏或显示柱条上的相应区域。 • **速度表图** 此图表显示符合指定条件的资产数量占资产总数的比例。 图表中的数值以百分比表示。
格式	此设置适用于**堆叠柱状图**。数据显示格式：**绝对值**或**相对值 (%)**。如果选择"**绝对值**"格式，柱状图的高度对应于所测量指标值的总和。如果选择了**相对值（%）**格式，则所有柱条的高度均为100%，柱条上彩色区域的相对高度与指标数值比例相对应。 默认选择"**绝对值**"。
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。
资产类别	小部件显示其数据的资产类别。
在未分类资产中搜索	此设置允许您显示没有类别的资产。 默认情况下，此复选框未被选中。
选择图表坐标轴设置群组	
Y轴	必需设置。资产字段以及为该字段指定的条件或条件集，用于定义如何统计资产。
Y 轴分类	所选字段的类别。不适用于**计数器**类型的图表。对于值为列举的Y轴字段（可以从有限的值列表中选择），此设置是可选的。对于其他所有字段，此参数均为必填项。
按租户分组	此设置适用于**堆叠柱状图**类型的图表。支持按租户对资产进行进一步分组。如果选中该复选框，图表上的资产将沿X轴分解成与各个租户对应的柱条。如果取消选中该复选框，则所有资产将显示在同一栏中。默认情况下，此复选框未被选中。

“外观”选项卡

下表描述了**外观**选项卡上的设置。

参数描述

设置	描述
描述	小部件描述。
显示总和	此设置适用于**表格**类型的图表。除了选定的类别外，还可以在图表中显示总计。如果选中此复选框，则所有指定类别的值的总和将显示在饼图的中心，并在图例的单独**总计**列中显示。默认情况下，此切换开关处于关闭状态。
颜色	此设置适用于**计数器**类型的图表。用于显示信息的颜色： • “**默认**”表示浏览器的默认字体颜色 • **绿色** • **红色** • **蓝色** • **黄色**
渐变	图表的渐变填充： • 两种颜色（红色和绿色） • 三种颜色（红色、黄色和绿色） 此设置适用于“**表格**”类型的图表。 您可以通过点击切换方向图标 (⇆) 来调整填充方向并设置阈值。 如果未手动设置，渐变阈值将根据数据自动计算。如果在指定的阈值之间没有数据，则不会应用渐变。而是使用两种颜色：一种用于低于下限阈值的值，另一种用于高于上限阈值的值。
渐变指示器字段	显示渐变填充指示器的列。此列由下拉列表中选择的**指标**字段决定。 此设置适用于“**表格**”类型的图表。
水平	将直方图水平显示，而非垂直显示。 启用此选项后，当小组件显示大量数据时，将不支持水平滚动，所有可用信息会自适应调整以适配小部件的固定尺寸。如果要显示大量数据，建议扩大小部件的尺寸。
显示图例	显示分析数据图例。默认情况下，切换开关处于打开状态。
在图例中显示空值	显示图例中用于分析数据的带有空值的参数。默认情况下，切换开关处于打开状态。 仅当启用了“**显示上一时间段数据**”设置且当前时间段没有数据，但上一时间段有数据时，才会显示空值。
在图例中显示百分比	在图例中显示百分比值。默认情况下，切换开关处于打开状态。
小数	显示值需要四舍五入后保留的小数位数。
刻度	适用于**堆叠柱状图**。数据显示刻度。可用值如下： • **线性图** • **方形图** • **对数图** 默认值为**线性图**。
阈值	可用于**速度表图**。默认指定以下范围：0–30、30–70、70–100。

其他小部件

本节介绍除 **事件**、**活动列表**、**上下文表**和自定义**资产**小部件之外的所有小部件的设置。

小部件可用的参数集取决于小部件上显示的图类型。KUMA 支持以下图类型：

- 饼图 ()。
- 计数器 ()。
- 表格 ()。
- 柱状图 ()。

- 日期直方图 ( )。
- 折线图

饼图设置

下表列出了**饼图**的设置。

参数描述

设置	描述
名称	小部件名称。
描述	小部件描述。
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。
时间段	小部件中显示的数据所对应的时间段。默认值为"**按布局**"，表示将显示针对布局所选时间段内的数据。 您还可以通过以下方式之一为小部件指定时间段： • 在日历中选择时间段的确切开始和结束日期及时间，然后单击"**应用**"。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动指定一个值：选择确切的日期和时间，或相对时间段，也可两者结合。 详情请参见下方的"*配置时间段*"小节。
显示总和	显示值的总和。
显示图例	显示分析数据图例。默认情况下，切换开关处于打开状态。
在图例中显示空值	显示图例中用于分析数据的带有空值的参数。默认情况下，切换开关处于打开状态。
小数	显示值需要四舍五入后保留的小数位数。

计数器设置

下表列出了**计数器**的设置。

参数描述

设置	描述
名称	小部件名称。
描述	小部件描述。
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。
时间段	小部件中显示的数据所对应的时间段。默认值为"**按布局**"，表示将显示针对布局所选时间段内的数据。 您还可以通过以下方式之一为小部件指定时间段： • 在日历中选择时间段的确切开始和结束日期及时间，然后单击"**应用**"。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动指定一个值：选择确切的日期和时间，或相对时间段，也可两者结合。 详情请参见下方的"*配置时间段*"小节。

表格设置

下表列出了**表格**的设置。

参数描述

设置	描述
名称	小部件名称。
描述	小部件描述。
租户	小部件中显示的数据所对应的租户。您可以选择多个租户。默认情况下，显示布局设置中所选租户的数据。

设置	描述
时间段	小部件中显示的数据所对应的时间段。默认值为"**按布局**"，表示将显示针对布局所选时间段内的数据。 您还可以通过以下方式之一为小部件指定时间段： • 在日历中选择时间段的确切开始和结束日期及时间，然后单击"**应用**"。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动指定一个值：选择确切的日期和时间，或相对时间段，也可两者结合。 详情请参见下方的"*配置时间段*"小节。
渐变	图表的渐变填充： • 两种颜色（红色和绿色） • 三种颜色（红色、黄色和绿色） 您可以通过点击切换方向图标 (⇆) 来调整填充方向并设置阈值。 如果未手动设置，渐变阈值将根据数据自动计算。如果在指定的阈值之间没有数据，则不会应用渐变。而是使用两种颜色：一种用于低于下限阈值的值，另一种用于高于上限阈值的值。
渐变指示器字段	显示渐变填充指示器的列。 此列由下拉列表中选择的字段决定。字段类型取决于小部件的类型： • 对于**受影响资产**，它是**频率**字段。 • 对于**事故中受影响的资产**、**KSC资产的实时保护扩展保护状态**和**事故中受影响的用户**，它是**计数**字段。
小数	显示值需要四舍五入后保留的小数位数。

柱状图和日期直方图的设置

下表列出了**坐标轴**选项卡上的**柱状图**和**日期直方图**类型的图表的设置。

参数描述

设置	描述
Y 轴 and **最小值 - 最大值**	Y 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非"**自动**"）来修正。
X 轴 and **最小值 - 最大值**	X 轴刻度。 图表轴上可以显示负值。这是由于小部件中图表的缩放方式导致的，可通过将图表最小值设置为 0（而非"**自动**"）来修正。
小数	显示值需要四舍五入后保留的小数位数。

下表列出了**外观**选项卡上的**柱状图**、**堆叠柱状图**和**日期直方图**类型的图表的设置。

参数描述

设置	描述
名称	小部件名称。
描述	小部件描述。
时间段	小部件中显示的数据所对应的时间段。默认值为"**按布局**"，表示将显示针对布局所选时间段内的数据。 您还可以通过以下方式之一为小部件指定时间段： • 在日历中选择时间段的确切开始和结束日期及时间，然后单击"**应用**"。 • 在"**相对时间段**"列表中选择相对于当前时间的时间段。 • 手动指定一个值：选择确切的日期和时间，或相对时间段，也可两者结合。 详情请参见下方的"*配置时间段*"小节。
格式	数据显示格式：**绝对值**或**相对值 (%)**。此设置适用于**堆叠柱状图**。 如果选择"**绝对值**"格式，柱状图的高度对应于所测量指标值的总和。如果选择了**相对值（%）**格式，则所有柱条的高度均为100%，柱条上彩色区域的相对高度与指标数值比例相对应。 默认选择"**绝对值**"。
时间线视图	时间数据显示格式：**柱状图**或**折线图**。此设置适用于"**日期直方图**"类型的图表。 选择"**柱状图**"格式时，数据默认以垂直柱条显示。如果 SQL 查询包含带有类别别名的附加字段，则图表将变为堆叠柱状图，即每个柱条根据该字段的值划分成若干分段。 选择"**折线图**"格式时，数据将显示为一条或多条（取决于查询）贯穿时间轴上各点的折线。 默认选中"柱状图"格式。

设置	描述
显示上一时间段数据	启用同时显示两个时间段的数据：当前时间段和上一时间段。
颜色	用于显示信息的颜色： • "**默认**"表示浏览器的默认字体颜色 • **绿色** • **红色** • **蓝色** • **黄色**
渐变	图表的渐变填充： • 两种颜色（红色和绿色） • 三种颜色（红色、黄色和绿色） 您可以通过点击切换方向图标 (⇆) 来调整填充方向并设置阈值。 如果未手动设置，渐变阈值将根据数据自动计算。如果在指定的阈值之间没有数据，则不会应用渐变。而是使用两种颜色：一种用于低于下限阈值的值，另一种用于高于上限阈值的值。 堆叠柱状图不应用渐变填充。在这种情况下，颜色会自动分配。
水平	将直方图水平显示，而非垂直显示。启用此设置后，所有可用信息都将适配至配置的小部件尺寸。如果数据量很大，您可以增加小部件的尺寸以获得最佳显示效果。
显示总和	显示值的总和。
显示图例	显示分析数据图例。默认情况下，切换开关处于打开状态。
在图例中显示空值	显示图例中用于分析数据的带有空值的参数。默认情况下，切换开关处于打开状态。 仅当启用了"**显示上一时间段数据**"设置且当前时间段没有数据，但上一时间段有数据时，才会显示空值。
时间段的分段长度	您希望将该时间段拆分为若干分段后，每个分段的持续时长。适用于"**日期直方图**"类型的图表。

速度计图表设置

下表列出了**速度表图**的设置。

> 图表中的数值以百分比表示。

参数描述

设置	描述
"**常规**"选项卡	
名称	小部件名称。
租户	其数据显示在小部件中的租户。您只能选择之前在控制板设置中选择的租户。
资产类别	将要搜索值的选定类别的资产。
在未分类资产中搜索	在搜索图表的资产时，资产类别将被忽略。
Y轴	用于搜索资产并随后计算速度计读数的参数值。 您可以指定多个参数值来搜索资产。
"**外观**"选项卡	
描述	小部件上显示的图表的描述。
阈值	为了帮助您直观地识别事件的严重等级，速度计的表盘分为三个区域：绿色、黄色和红色。默认情况下，这些区域配置了以下间隔： • 绿色： 0–30 • 黄色： 30–70 • 红色： 70–100 您可以根据需要更改范围。

配置时间段

对于**饼图**、**计数器**、**表格**、**条形图**、**堆叠条形图**、**日期直方图**等图表，您可以使用**时间段**设置来配置小部件中数据的显示时间段。默认情况下，小部件的数据显示时间段与控制板的数据显示时间段相同。

要配置数据显示时间段，请执行以下操作之一：

- 如有必要，请按以下方式之一更改“**时间段**”设置中的日期和时间：

  - 如果您想指定确切日期，请在左侧日历中选择时间段的开始日期和结束日期，然后单击**“应用”**。

    您可以选择包括当前日期在内的任意日期。日期和时间格式取决于浏览器的设置。如果**“范围起始”**或**“范围结束”**字段已有值，且您未手动编辑时间值，则当您在日历中选择日期时，**“范围起始”**字段会自动填充 00:00:00.000，“**范围结束**”字段会自动填充 23:59:59.999。如果您已手动删除**“范围起始”**或**“范围结束”**字段中的值，则当您在日历中选择日期时，该字段会自动填充当前时间。在其中一个字段中选择值后，焦点将切换到另一个字段。如果您的**“范围结束”**早于**“范围起始”**，则较早的值会自动插入到**“范围起始”**字段中。

  - 如果您想指定相对时间段，请在右侧的**“相对时间段”**列表中选择一个可用时间段。

    时间段是相对于当前时间计算的。

  - 如果要指定自定义时间段，请编辑**“范围起始”**和**“范围结束”**字段的值。

    您可以按 **DD.MM.YYYY HH:mm:ss.SSS** 格式（俄语本地化版本）和 **YYYY-MM-DD HH:mm:ss.SSS**（英语本地化版本）输入确切的日期和时间，或者通过公式输入相对时间段。如果需要，您还可以结合使用这些方法。如果在输入确切日期时未指定毫秒，系统会自动补填 000。如果您已编辑**“范围起始”**或**“范围结束”**字段中的时间，则在日历中选择日期不会更改时间部分。

    在相对时间段公式中，您可以使用“**now**”参数表示当前日期和时间以及间隔参数化语言：**+**（仅在“**范围结束**”字段中）、**-**、**/**（四舍五入到最接近的数），以及时间单位：**y**（年）、**M**（月）、**w**（周）、**d**（天）、**h**（小时）、**m**（分钟）、**s**（秒）。例如，您可以指定“**now-5d**”时间段以获取过去五天的数据，或指定“**now/w**”时间段以获取从本周第一天开始时间 (00:00:00:000 UTC) 到当前时间 (**now**) 的数据。

    > “**范围起始**”字段为必填项，其值不能超过“**范围结束**”字段的值，且不能早于 1970 年 1 月 1 日（如果指定确切日期或相对时间段）。“**范围结束**”不能早于“**范围起始**”。如果未在“**范围结束**”字段中指定值，则自动指定 **now**。

KUMA 以 UTC 格式存储时间值，但在用户界面中，时间会转换为浏览器所在的时区。这与相对时间段相关：**今天**、**昨天**、**本周**和**本月**。例如，如果浏览器所在的时区是 UTC+3，并且您选择“**今天**”作为数据显示时间段，则将显示从 03:00:00.000 到现在的数据，而不是从 00:00:00.000 到现在的数据。

如果在选择相对数据显示时间段（例如**今天**、**昨天**、**本周**或**本月**）时要考虑时区，则需要通过添加或减去正确的小时数在“**范围起始**”和“**范围结束**”中手动添加时间偏移量（如果指定了 now 以外的值），即加上或减去正确的小时数。例如，如果您的浏览器时区为 UTC+3，并且您想显示**昨天**的数据，则需要将**“范围起始”**更改为“**now-1d/d-3h**”，并将“**范围结束**”更改为“**now/d-3h**”。如果您想显示**今天**的数据，则只需将“**范围起始**”字段的值更改为**“now/d-3h”**。

> 如果您需要截至昨天 23:59:59:999 UTC 的结果，可以使用带有时间戳过滤器的 SQL 查询，或者指定确切的日期和时间。

时间段的边界为闭区间（包含端点）：例如，对于“**今天**”的时间范围，将显示从当天起始时刻 (00:00:00:000 UTC) 到当前时刻（**now**）包含两端点的事件；而对于“**昨天**”的时间段，将显示从前一日起始时刻 (00:00:00:000 UTC) 到当日起始时刻 (00:00:00:000 UTC) 的事件。将鼠标悬停在小部件中的时间段图标上，即可查看上次数据更新的日期和时间以及数据显示所对应的确切时间段。

如果小部件启用了“显示上一时间段数据”设置，并且小部件显示的是相对时间段的数据，则工具提示也会显示上一时间段。上一时间段的计算方法是：用当前时间段的开始时间和结束时间减去当前时间段的持续时间。例如，如果数据每日更新并显示一个月，但该月只过去了前 10 天，则上一时间段为上个月的最后 10 天。

如果您希望小部件显示布局中选择的时间段的数据，请单击**"重置"**按钮。更改布局中显示的时间段也会更改小部件中显示的时间段。

过滤小部件数据

KUMA 允许您通过在控制板中选择过滤参数，对**事件**类型的小部件中的数据进行过滤。在以下情况下，您可以过滤数据：

- 过滤单个小部件上的数据

  对于此类过滤，您需要在小部件属性的SQL查询中指定一个或多个局部变量。这些变量允许您通过将控制板小部件的数据替换到查询中来修改此SQL查询。小部件会根据变量的新值过滤数据并刷新图表。您无需在小部件属性中手动更改SQL查询。

  您可以通过点击小部件上的漏斗图标（ ）来应用局部变量。这将打开一个窗口，您可以在其中选择或输入局部变量的值。

- 过滤同一控制板中多个小部件的数据

  对于此类过滤，您需要在控制板属性中指定一个或多个全局变量。然后，将全局变量添加到要应用这些全局变量的小部件的SQL查询中。当您为全局变量分配新值时，所有使用此变量的小部件都会根据新值自动重建图表。

  点击图表的某个部分或图例中的文本即可应用全局变量。KUMA将显示一个菜单，其中包含将所选图表部分或图例项的数据类别应用于变量的命令。

- 深层探究到另一个控制板时，可以使用全局变量传递过滤参数

  全局变量可用于将值传递到另一个控制板。从一个控制板深层探究到另一个仪表板时，KUMA会替换所选变量值和所选时间段，并自动重建新控制板的图表。

  深层探究到另一个控制板时，不能使用局部变量。

不建议在一个控制板中设置超过五个变量。这可能会导致控制板运行不稳定。

过滤单个小部件上的数据

KUMA 允许您通过在控制板中选择过滤参数，对**事件**类型的小部件中的数据进行过滤。

要过滤单个小部件中的数据，您需要在小部件属性的SQL查询中指定一个或多个局部变量。这些变量允许您通过将控制板小部件的数据替换到查询中来修改此SQL查询。小部件会根据变量的新值过滤数据并刷新图表。您无需在小部件属性中手动更改SQL查询。

不建议在一个控制板中设置超过五个变量。这可能会导致控制板运行不稳定。

配置单个小部件中的数据过滤

若要在小部件中配置用于过滤数据的局部变量：

1. 在**控制板**部分，选择一个控制板，然后点击**编辑**按钮，进入控制板编辑模式。
2. 选择一个现有的**事件**小部件，或者点击**添加小部件**按钮，然后选择**事件**小部件类型。
3. 在小部件属性窗口中，选择**一般**选项卡。

4. 在**定义的变量**下，点击**添加**。

5. 输入变量的任意名称，然后指定变量的值。局部变量和全局变量的名称在控制板必须是唯一的。

   将变量的值指定为`value`或`category`，即查询中使用的字段别名。如果要在小部件中过滤数据时手动输入此变量的值，请将此字段留空。

   对于表格类型的图表，您可以将事件字段的名称指定为变量的值。这样，您就可以根据此字段的选定值过滤表格中的数据。事件字段的名称会显示在表格列的标题中。

6. 在**SQL查询**字段的WHERE子句中，添加一个函数来处理这些变量。

   具有特定值的变量的语法如下：

   `filter(<event_field_name> = $variable_name)`

   手动输入具有任意值的变量的语法如下：

   `filter(<event_field_name> like $variable_name)`

   在这种情况下，在手动输入时，您可以使用%元字符来搜索部分文本匹配。有关详细信息，请参阅ClickHouse文档。

   > 您不能使用SQL构建器向SQL查询添加变量。

   查看示例

   带有局部变量的 SQL 查询示例

   ```
   SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name)
   GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250
   ```

   此查询使用局部变量`$Name`。`Name`事件字段的值将代入此变量。您可以通过点击小部件上的漏斗图标（）来应用该变量。这将打开一个窗口；在该窗口中，您可以为变量指定一个值。小部件会根据`Name`字段的选定值筛选数据。

   请注意，如果在 SQL 查询中为接收数值的字段指定了变量，则必须将该值转换为字符串。您可以使用`toString`函数执行此操作。否则，SQL 查询将返回错误。

   示例

   ```
   SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like
   $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250
   ```

   在此查询中，`SourcePort event`字段的值为数值，因此将其转换为字符串：`toString(SourcePort)`。

7. 保存更改。

对单个小部件应用数据过滤

若要在小部件内应用局部变量进行数据过滤：

1. 在**控制板**部分，选择包含相关小部件的控制板。此小部件的属性中必须至少设置一个局部变量。

2. 在小部件上，点击漏斗图标（）。

3. 这将打开一个窗口；在该窗口中，选择要应用的局部变量。

4. 保存更改。

   该小部件会根据变量的新值重新构建图表。

过滤多个小部件中的数据

KUMA 允许您通过在控制板中选择过滤参数，对**事件**类型的小部件中的数据进行过滤。

要在一个控制板中的多个小部件中过滤数据，您需要在控制板的属性中指定一个或多个全局变量。然后，将全局变量添加到要应用这些全局变量的小部件的SQL查询中。当您为全局变量分配新值时，所有使用此变量的小部件都会根据新值自动重建图表。

点击图表的某个部分或图例中的文本即可应用全局变量。KUMA将显示一个菜单，其中包含将所选图表部分或图例项的数据类别应用于变量的命令。

> 不建议在一个控制板中设置超过五个变量。这可能会导致控制板运行不稳定。

在控制板级别为多个小部件配置数据过滤

若要在控制板级别为多个小部件配置数据过滤：

1. 在**控制板**部分，选择一个控制板，然后点击**编辑**按钮，进入控制板编辑模式。
2. 点击**设置**按钮。
3. 这将打开一个窗口；在该窗口的**变量**部分，选择**全局变量**选项卡。
4. 然后单击"**添加**"按钮。
5. 在新的一行中，输入变量的名称。局部变量和全局变量的名称在控制板必须是唯一的。

   您添加全局变量的所有控制板小部件的名称都列在**已在小部件中使用**列中。

   点击图表的某个分段或图例中的某个项目时，全局变量的名称将显示在上下文菜单的命令中。
6. 保存更改。
7. 选择一个现有的**事件**小部件，或者点击**添加小部件**按钮，然后选择**事件**小部件类型。在此小部件中，您将配置点击操作。
8. 在小部件属性窗口中，选择**一般**选项卡。
9. 在**定义的变量**部分，添加您在控制板属性中添加的一个或多个全局变量。
10. 如有必要，请在SQL查询字段中使用filter()函数将全局变量添加到WHERE子句中。这也会将配置的操作应用于此小部件。
11. 选择**操作**选项卡。

    如果您希望在单击图表中的某个分段时显示一个菜单，其中包含按所选分段类别过滤数据的命令：

    a. 在**图表分段**部分，启用**按变量筛选**选项。

    b. 在**类别**列表中，选择要替换SQL查询中指定的`category`别名值的变量。

    类别选项仅适用于堆叠柱状图类型。

    c. 在**值**列表中，选择要替换SQL查询中指定的`value`别名值的变量。

如果您希望在点击图例项目时显示一个菜单，其中包含按所选值过滤数据的命令：

a. 在**图例项目**部分，启用**按变量筛选**选项。

如有必要，单击**从图表分段设置复制**按钮，将选定的参数值从**图表分段**设置组自动传输到**图例项目**设置群组。

b. 在**值**列表中，选择要能够替换图例项目变量的变量。

12. 在要应用全局变量的其他小部件的属性中：

- 在**一般**选项卡上的**定义的变量**部分，添加一个或多个全局变量。
- 在小部件的SQL查询字段中，使用filter()函数将全局变量添加到WHERE子句。

在控制板级别对多个小部件应用数据过滤

若要应用全局变量以过滤小部件之间的数据：

1. 在**控制板**部分，选择要应用全局变量的小部件所在的控制板。
2. 找到已配置点击操作的小部件。点击图表的分段或图例项目旁边的箭头图标（ ⌄ ）以打开菜单。
3. 在菜单中，点击**将类别应用于变量<变量名称>**或**将值应用于变量<变量名称>**。

将选定类别或图例项目的值分配给该变量。在当前控制板中，所有使用此变量的小部件都会根据该变量的新值重建其图表。此类小部件标有漏斗图标（ 1 ），其中包含一个数字，表示应用的过滤器数量。屏幕上方会显示已应用的全局变量列表。若要清除小部件的数据过滤，请点击带有数字的漏斗图标（ 1 ）。若要清除控制板所有小部件的数据过滤，请点击控制板上部的**全部重置**。

深层探究到相关控制板

KUMA 允许在当前控制板的**事件**类型小部件中筛选数据，并在保留已配置的筛选参数和时间段的情况下深层探究到另一个控制板。

这是通过全局变量实现的。必须在两个控制板以及小部件的属性中配置全局变量：在目标控制板上，变量在SQL查询中指定，在来源控制板中，在管理**深层探究到另一个控制板**设置时指定变量。从一个控制板深层探究到另一个控制板时，KUMA会自动替换所选变量值和时间段，之后重建目标控制板中的图表。两个控制板必须在同一租户内。

深层探究到另一个控制板时，不能使用局部变量。

配置目标控制板

若要配置目标控制板：

1. 在KUMA网页界面中，进入**控制板**部分，选择一个控制板并创建一个全局变量。

变量名只能包含英文字母和数字，不能包含空格。

2. 保存更改。
3. 在控制板上，选择一个现有的**事件**小部件，或者点击**添加小部件**按钮，然后选择**事件**小部件类型。

4. 在**一般**选项卡上，指定之前创建的变量：

   - 在**定义的变量**下
   - 在**SQL查询**字段中，为使 SQL 查询考虑变量的值，请将`filter()`函数添加到`WHERE`子句中。

     具有特定值的变量的语法如下：

     `filter(<event_field_name> = $variable_name)`

     手动输入任意值的变量的语法如下：

     `filter(<event_field_name> like $variable_name)`

     查询示例

     带有`$ServiceName`变量的查询：

     ```
     SELECT DestinationHostName AS Host, Name AS Status, Message AS Reason, ServiceName,
     Timestamp AS Time
     FROM events
     WHERE DeviceEventClassID = 'KLSRV_HOST_STATUS_CRITICAL' OR DeviceEventClassID =
     'KLSRV_HOST_STATUS_WARNING' AND filter(ServiceName = $ServiceName)
     ORDER BY Time DESC
     LIMIT 25
     ```

     如果在下钻至目标控制板时通过`$ServiceName`变量传递了值，该值将自动代入查询并筛选数据。如果未指定变量的值，则查询将如同该变量不存在一样执行。

5. 保存更改。

配置来源控制板

若要配置来源控制板：

1. 在KUMA网页界面中，进入**控制板**部分，选择一个控制板并创建一个全局变量。

   变量名称必须与目标控制板中创建的变量名称相同。名称只能包含英文字母和数字，不能包含空格。

2. 保存更改。

3. 在控制板上，选择一个现有的**事件**小部件，或者点击**添加小部件**按钮，然后选择**事件**小部件类型。

4. 在**一般**选项卡的**定义的变量**部分，指定之前创建的变量。

5. 在“**操作**”选项卡上，指定以下设置：

   a. 在**图表分段**或**图例项目**部分，启用**深层探究到另一个控制板**。

   b. 在**控制板**下拉列表中，选择目标控制板。

   c. 在**值**下拉列表中，选择要在深层探究到另一个控制板时传递其值的变量。这必须是您之前创建的同一个变量。

   所选变量必须在目标控制板小部件的SQL查询中指定，以便在深层探究后自动过滤此小部件上的数据。

6. 保存更改。

从来源控制板深层探究到目标控制板

若要深层探究到目标控制板：

1. 在KUMA网页界面中，在**控制板**下，选择来源控制板。

2. 找到已启用**深层探究到另一个控制板**选项的小部件。点击已配置此操作的图表图例中的分段或项目。

   这将在新选项卡中打开目标控制板。原始小部件的时间段自动应用于整个控制板，从**值**下拉列表中选择的值作为变量传递给**事件**类型的小部件，其中该变量通过`filter()`函数在SQL查询中使用。其他控制板上的小部件中的图表会根据传递的值重新构建。

   如果您更改或删除目标控制板（即您要深层探究的目标控制板）上操作中指定的变量，则仍会执行深层探究操作，但不会传递该变量的值。

在活动列表类型小部件中显示租户名称

如果您希望**活动列表**小部件显示租户名称而非租户 ID，请在关联器的关联规则中配置相应函数，以使用对应租户的信息填充活动列表。

配置过程包括以下步骤：

1. 导出租户列表。

2. 创建“表格”类型的字典。

3. 将在步骤 1 中获得的租户列表导入在这些说明的步骤 2 中创建的字典中。

4. 在关联规则中添加一个局部变量，通过“**dict**”函数将租户名称映射到租户 ID。

   例如：

   - 变量：`TenantName`
   - 值：`dict ('<Name of the previously created dictionary with tenants>', TenantID)`

5. 在关联规则中添加一个 **Set** 操作，以<键>-<值>格式将先前创建变量的值写入活动列表。指定活动列表的字段（例如，`Tenant`）作为密钥，然后在“**值**”字段中指定变量（例如，`$TenantName`）。

当此规则触发时，通过“**dict**”函数在租户字典中与 ID 映射的租户名称会被放入活动列表中。基于活动列表创建小部件时，小部件显示租户名称而不是租户 ID。

检测和响应控制板

在“**仪表板**”部分，您可以监控组织网络的安全状态。

仪表板是一组显示网络安全数据分析的小部件。您只能查看您有权访问的租户的数据。

仪表板中使用的小部件组合称为*布局*。您可以手动创建布局或使用预定义布局。您可以根据需要编辑预定义布局中的小部件设置。默认情况下，仪表板显示“警报概览”预定义布局。

仅具有主管理员、租户管理员、2 级分析师和 1 级分析师角色的用户才能创建、编辑或删除布局。具有所有这些角色的用户账户都可以查看布局和设置默认布局。如果将某个布局设置为默认布局，则每次用户进入“**仪表板**”部分时，该账户都会显示此布局。所选的默认布局将保存至当前用户账户。

仪表板上的信息将根据布局设置中配置的计划进行更新。如有必要，您可以强制更新数据。

为了方便在仪表板上显示信息，您可以启用 TV 模式。此模式允许您以全屏模式（全高清分辨率）查看仪表板。在 TV 模式下，您还可以为所选布局配置幻灯片显示。

创建仪表板布局

要创建布局：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 打开窗口右上角的下拉列表，然后选择“**创建布局**”。
   “**新布局**”窗口将打开。
3. 在“**租户**”下拉列表中，选择将拥有所创建布局的租户，其数据将用于填充布局。
   如果您要创建通用布局（步骤 8），则此下拉列表中的租户选择无关紧要。
4. 在“**时间段**”下拉列表中，选择您需要分析数据对应的时间段：
   - **1 小时**
   - **1 天**（默认选择此值）
   - **7 天**
   - **30 天**
   - **指定时间段**：获取所选时间段的分析数据。选择此选项后，可使用显示的日历设置时间段。

     > 时间段的上限不包括在其定义的时间片段中。换句话说，要接收 24 小时的分析数据，您应该将时间段配置为“第 1 天 00:00:00 - 第 2 天 00:00:00”，而不是“第 1 天 00:00:00 - 第 1 天 23:59:59”。
5. 在“**刷新间隔**”下拉列表中，选择布局小部件中数据的更新频率：
   - **1 分钟**
   - **5 分钟**
   - **15 分钟**
   - **1 小时**（默认选择此值）
   - **24 小时**
6. 在“**添加小部件**”下拉列表中，选择所需的小部件并配置其设置。
   您可以向布局添加多个小部件。
   您也可以在窗口中拖动小部件，并使用对角线按钮 (↘) 调整大小（将鼠标悬停在小部件上时会出现该按钮）。
   您可以编辑或删除添加到布局的小部件。为此，请单击设置图标 (⚙) 并选择“**编辑**”以更改其配置或选择“**删除**”以将其从布局中删除。
7. 在“**布局名称**”字段中，输入此布局的唯一名称。必须包含 1 到 128 个 Unicode 字符。
   自定义控制板不能与预定义控制板同名。

尝试在主租户中创建与预定义控制板同名的控制板，或将自定义控制板的名称更改为预定义控制板的名称时，系统将传回错误。在主租户以外的其他租户中，您可以创建或复制与预定义控制板同名的自定义控制板。

8. 如有必要，请单击布局名称字段右侧的设置图标 ( )，然后选中“**通用**”设置旁边的复选框。

   布局小部件将显示来自您在左侧菜单的“**选定租户**”部分中所选择租户的数据。这意味着布局小部件中的数据将根据所选择的租户而变化，而无需编辑布局设置。对于通用布局，在“**租户**”下拉列表中选择的租户不予考虑。

   如果清除该复选框，布局小部件将显示在布局设置的“**租户**”下拉列表中所选择租户的数据。如果您无法使用布局中选择的任何租户，则其数据将不会显示在布局小部件中。

   > 您不能在通用布局中使用“**活动列表**”小部件。
   > 通用布局只能由已分配“主管理员角色”的用户创建和编辑。所有用户都可以查看此类布局。

9. 单击“**保存**”按钮。

新布局已创建，并显示在仪表板的“**检测和响应**”选项卡上。

选择仪表板布局

要选择仪表板布局：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 展开窗口右上角的列表。
3. 选择相关布局。

所选布局将显示在仪表板的“**检测和响应**”选项卡上。

将某个仪表板布局设置为默认布局

要将某个仪表板布局设置为默认布局：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 展开窗口右上角的列表。
3. 将鼠标光标悬停在相关布局上。
4. 单击星形图标 ( )。

默认情况下，所选布局显示在仪表板的“**检测和响应**”选项卡上。

编辑仪表板布局

要编辑仪表板布局：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。
2. 展开窗口右上角的列表。
3. 将鼠标光标悬停在相关布局上。
4. 单击编辑图标 ( )。

   “**自定义布局**”窗口打开。

5. 编辑仪表板布局。可供编辑的设置与创建布局时可用的设置相同。

6. 单击“**保存**”按钮。

仪表板布局已编辑，并显示在“**检测和响应**”选项卡上。

如果在编辑布局时将其删除或分配给其他租户，则单击“**保存**”时会显示错误。布局未保存。刷新 Kaspersky Next XDR Expert 界面页面，即可在下拉列表中查看可用布局的列表。

删除仪表板布局

删除布局：

1. 在主菜单中，转到“**监控**” → “**控制板**”，然后选择“**Detection and response**”选项卡。

2. 展开窗口右上角的列表。

3. 将鼠标光标悬停在相关布局上。

4. 单击删除图标 ( ) 并确认此操作。

布局被删除。

启用和禁用 TV 模式

建议创建一个单独的用户，并授予其在 TV 模式下显示分析数据所需的最低权限。

要启用 TV 模式：

1. 在 KUMA 控制台中，选择“**仪表板**”部分。

2. 单击右上角的 按钮。
“**设置**”窗口打开。

3. 将 **TV 模式**切换开关移动至“**已启用**”位置。

4. 要配置布局的幻灯片显示，请执行以下操作：

   a. 将“**幻灯片**”切换开关移动至“**已启用**”位置。

   b. 在“**超时**”字段中，指定切换布局前等待的秒数。

   c. 在“**队列**”下拉列表中，选择要查看的布局。如果未选择任何布局，幻灯片模式将依次显示用户可用的所有布局。

   d. 如有必要，可通过单击 按钮对布局进行拖放操作，更改其显示顺序。

5. 单击“**保存**”按钮。

TV 模式将启用。要恢复使用 KUMA 控制台，请禁用 TV 模式。

要禁用 TV 模式：

1. 在 KUMA 控制台中，选择“**仪表板**”部分。
2. 单击右上角的 按钮。
   “**设置**”窗口打开。
3. 将 **TV 模式**切换开关移动至“**已禁用**”位置。
4. 单击“**保存**”按钮。

TV 模式将被禁用。屏幕左侧显示一个窗格，其中包含 KUMA 控制台的各个部分。

当您对幻灯片选择的布局进行更改时，这些更改将自动应用到活动的幻灯片会话。

预配置仪表板布局

Kaspersky Next XDR Expert 包括一组预定义布局，其中包含以下小部件：

- **警报概览**布局（警报概览）：
  - 活动警报 — 尚未关闭的警报数量。
  - 未分配的警报 — 未分配负责人的警报数量。
  - 最新警报 — 该表格包含有关布局中选定租户的最近 10 个未关闭警报的信息。
  - 警报分布 — 在小部件配置时间段内创建的警报数量。
  - 按优先级分组的警报 — 按优先级分组的未关闭警报数量。
  - 按用户分组的警报 — 状态为“**进行中**”的警报数量。按账户名称分组。
  - 按状态分组的警报 — 按状态分组的警报数量。
  - 按用户组分组的警报 — 按用户组分组的警报数量。
  - 警报中受影响的用户 — 与未关闭警报关联的用户。
  - “受影响资产”是一个表格，其中包含资产、资产的重要级别以及与资产关联的未关闭警报数量等信息。资产的重要级别根据该资产所属的类别计算，包括层次结构中一直到根节点的所有父类别。
  - 受影响资产类别 — 显示未关闭警报和事件中指定的资产类别数量的图表。对于警报或事件中引用的每个资产，其重要性级别基于资产所属的类别计算，包括层级结构根节点之前的所有父类别。
  - 按警报数量统计的事件源排名 — 按生成警报的事件源分组的未关闭警报数量进行统计。

    该小部件最多显示 10 个事件源。

  - 按规则分类的警报 — 按关联规则分组的未关闭警报的数量。

未关闭警报是指具有以下状态之一的警报：“**新建**”、“**进行中**”、“**事故中**”。

- **事故概览**布局（事故概览）：
  - 活动事故 — 不属于“**已完成**”状态类别的事故数量。
  - 未分配的事故 — 未分配负责人的事故数量。
  - 最新事故 — 该表格包含有关布局中选定租户的最近 10 个未关闭事故的信息。
  - 事故分布 — 在小部件所配置时间段内创建的事故数量。
  - 按优先级分组的事故 — 按优先级分组的事故数量。
  - 按用户分组的事故 — 状态为“**进行中**”的事故数量。按用户账户名称分组。
  - 按状态分组的事故 — 按状态分组的事故数量。
  - 按用户组分组的事故 — 按用户组分组的事故数量。
  - 事件中受影响的资产 — 显示与未关闭事件关联的资产数量的表格。该表格列出了资产及其重要级别，重要性级别基于资产所属的类别以及层级结构根节点之前的所有父类别计算得出。
  - 事故中受影响的用户 — 与未关闭事故关联的用户。
  - 事件中的受影响资产类别——显示与未关闭事件关联的资产类别数量的图表。对于关联到事件的每个资产，其重要性级别基于资产所属的类别计算，包括层级结构根节点之前的所有父类别。
  - 按租户分组的活动事故 — 按租户分组的未关闭事故的数量。

未关闭事故是指未处于“**已完成**”状态类别的事故。

- **网络概览**布局（网络活动概览）：
  - Netflow 顶级内部 IP — 资产接收的 Netflow 流量总量（以字节为单位）。数据按资产的内部 IP 地址分组。该小部件最多显示 10 个 IP 地址。
  - Netflow 顶级外部 IP — 资产接收的 Netflow 流量总量（以字节为单位）。数据按资产的外部 IP 地址分组。
  - Netflow 远程控制主机排名前列 — 与访问以下端口之一的尝试相关的事件数：3389、22、135。数据按资产名称分组。
  - Netflow 按内部端口统计的总字节数 — 发送到资产内部端口的字节数。数据按端口号分组。
  - 按事件数排名的顶级日志源 — 收到事件数最多的前 10 个源。
- NGFW **聚合仪表板**布局：
  - NGFW。防火墙会话和操作 — 已触发并设置了防火墙选项的防火墙配置文件操作数量。
  - NGFW。DNS 安全会话和操作 — 已触发并设置了日志记录选项的 DNS 安全配置文件操作数量。

- NGFW。Web 控制会话和操作 — 已触发并设置了日志记录选项的 Web 控制配置文件操作数量。
- NGFW。IDPS 会话和操作 — 已触发并设置了日志记录选项的 IDPS 配置文件操作数量。
- NGFW。反病毒会话和操作 — 已触发并设置了日志记录选项的反病毒配置文件操作数量。

- “**NGFW IDPS & File Web Antivirus**”布局：
  - NGFW。IDPS。前 5 种威胁名称 — IDPS 配置文件检测到的五种最常见的威胁。
  - NGFW。IDPS。前 5 种 MITRE 策略和技术 — IDPS 配置文件检测到的五种最常见的 MITRE ATT&CK 策略和技术。
  - NGFW。IDPS。前 5 种威胁类型 — IDPS 配置文件检测到的五种最常见的威胁类型。
  - NGFW。IDPS。阻止 Web 流量最多的前 5 个目标 IP 地址 — IDPS 配置文件阻止的 Web 流量最大的五个目标 IP 地址。
  - NGFW。IDPS。阻止 Web 流量最多的前 5 个源 IP 地址 — IDPS 配置文件阻止的 Web 流量最大的五个源 IP 地址。
  - NGFW。File Web Antivirus。前 5 种威胁名称 — 反病毒配置文件检测到的五种最常见的威胁。
  - NGFW。File Web Antivirus。阻止 Web 流量最多的前 5 个源 IP 地址 — 反病毒配置文件阻止的 Web 流量最大的五个目标 IP 地址。
  - NGFW。File Web Antivirus。阻止 Web 流量最多的前 5 个目标 IP 地址 — 反病毒配置文件阻止的 Web 流量最大的五个源 IP 地址。

- “**NGFW DNS Security**”布局：
  - NGFW。DNS 安全。阻止地址的前 5 个威胁 — 来自 DNS 安全配置文件阻止的 IP 地址中出现频率最高的五大威胁。
  - NGFW。DNS 安全。重定向地址的前 5 个威胁 — 来自 DNS 安全配置文件重定向的 IP 地址的五个最常见的威胁。
  - NGFW。DNS 安全。阻止 Web 流量最多的前 5 个源 IP 地址 — 被 DNS 安全配置文件阻止的 Web 流量最大的五个源 IP 地址。
  - NGFW。DNS 安全。重定向主机名前 5 位 — 被 DNS 安全配置文件最常执行重定向的五个域名。
  - NGFW。DNS 安全。阻止 Web 流量最多的前 5 个目标 IP 地址 — DNS 安全配置文件阻止的 Web 流量最大的五个目标 IP 地址。
  - NGFW。DNS 安全。重定向 Web 流量最多的前 5 个源 IP 地址 — 被 DNS 安全配置文件最常重定向的五个源 IP 地址。

- “**NGFW Web Control & URL Web Antivirus**”布局：
  - NGFW。URL Web Antivirus。阻止 URL 的前 5 个 Web 类别 — 被 Web 反病毒配置文件阻止的五个最常见的 URL 类别。
  - NGFW。URL Web Antivirus。阻止 Web 流量最多的前 5 个目标 IP 地址 — 被 Web 反病毒配置文件阻止 Web 流量最大的五个目标 IP 地址。

- NGFW。Web 控制。警告 Web 流量最高的前 5 个网站类别 — Web 控制配置文件显示警告提示频率最高的五个网站类别。
- NGFW。Web 控制。被阻止网络流量最多的前 5 类网站 — 被网络反病毒配置文件阻止的网络流量最大的五类网站。
- NGFW。Web 控制。警告 Web 流量最多的前 5 个目标 IP 地址 — Web 控制配置文件显示警告提示频率最高的五个目标 IP 地址。
- NGFW。Web 控制。阻止的 Web 流量最多的前 5 个目标 IP 地址 — 被 Web 控制配置文件阻止的网络流量最大的五个目标 IP 地址。
- NGFW。Web 控制。阻止地址的前 5 个 Web 控制类别来源 — 最常获取阻止 URL 类别的五个来源。
- NGFW。Web 控制。重定向地址的前 5 个 Web 控制类别来源 — 最常获取重定向 URL 类别的五个来源。

- **NGFW 防火墙**布局：
  - NGFW。按会话数量排名的前 5 个应用程序服务 — 按会话数量排名的前五个应用程序服务。
  - NGFW。按流量 (MB) 排名的前 5 个应用程序服务 — 按网络流量 (MB) 排名的前五个应用程序服务。
  - NGFW。按会话数量排名的前 5 个应用程序协议 — 按会话数量排名的前五个应用程序协议。
  - NGFW。按流量 (MB) 排名的前 5 个应用程序协议 — 按网络流量 (MB) 排名的前五个应用程序协议。
  - NGFW。按会话数量排名的前 5 个客户端应用程序 — 按会话数量排名的前五个客户端应用程序。
  - NGFW。按流量 (MB) 排名的前 5 个客户端应用程序 — 按网络流量 (MB) 排名前五的客户端应用程序。
  - NGFW。按流量 (MB) 排名的前 5 个源 IP — 网络流量 (MB) 最大的五个源 IP 地址。
  - NGFW。按流量 (MB) 排名的前 5 个目标 IP — 网络流量 (MB) 最大的五个目标 IP 地址。
  - NGFW。按会话数量排名的前 5 个网站 — 会话数量最多的五个网站。
  - NGFW。按流量排名的前 5 个网站 (MB) — 网络流量 (MB) 最大的五个网站。

预定义布局的默认刷新周期为“**从不**”。您可以根据需要编辑这些布局。

关于仅仪表板模式

您可以为不管理网络但希望在 Open Single Management Platform 中查看网络保护统计信息的员工（例如高层管理人员）配置“仅仪表板模式”。当用户启用此模式后，只会向用户显示带有一组预定义小部件的仪表板。因此，用户可以监视小部件中指定的统计信息，例如，所有受管理设备的保护状态、最近检测到的威胁数量或网络中最常见的威胁列表。

当用户在仅仪表板模式下工作时，将应用以下限制：

- 主菜单不向用户显示，因此用户无法更改网络保护设置。
- 用户不能对小部件执行任何操作，例如，添加或隐藏小部件。因此，您需要将用户需要的所有小部件都放在仪表板上并进行配置，例如，设置对象计数规则或指定时间间隔。

您不能为自己分配仅仪表板模式。如果要在此模式下工作，请联系系统管理员、受管理服务提供商 (MSP) 或在“**常规功能：用户权限**”功能区域中拥有“**修改对象 ACL**”权限的用户。

配置仅仪表板模式

在开始配置仅仪表板模式之前，确保满足以下先决条件：

- 您在“**常规功能：用户权限**”功能区域中拥有“**修改对象 ACL**”权限。如果您没有此权限，则用于配置模式的选项卡将缺失。
- 您在“**常规功能：基本功能**”功能区域中拥有“**读取**”权限。

如果您的网络中安排了管理服务器层级，若要配置仅仪表板模式，请转到在**用户和角色 → 用户和组** 区域中**用户**选项卡上提供了用户账户的服务器。可以是主服务器或物理从属服务器。无法在虚拟服务器上调整模式。

要配置仅仪表板模式：

1. 在主菜单中，转至**用户和角色 → 用户和组**，然后选择**用户**选项卡。
2. 单击要使用小部件调整仪表板的用户账户名。
3. 在打开的账户设置窗口中，选择“**仪表板**”选项卡。

   在打开的选项卡上，您和用户将看到相同的仪表板。
4. 如果启用了“**在仅仪表板模式下显示控制台**”选项，则对切换按钮进行切换以将其禁用。

   启用此选项后，您也无法更改仪表板。禁用该选项后，您可以管理小部件。
5. 配置仪表板外观。“**仪表板**”选项卡上准备的小部件级供具有可自定义账户的用户使用。用户不能更改小部件的任何设置或大小，也不能从仪表板添加或删除任何小部件。因此，请为用户调整好，以便用户可以查看网络保护统计信息。为此，在“**仪表板**”选项卡上，您可以像在“**监控 → 控制板**”部分中一样，对小部件执行以下操作：
   - 向仪表板添加新的小部件。
   - 隐藏用户不需要的小部件。
   - 移动小部件到特定文件夹。
   - 更改小部件的大小或外观。
   - 更改小部件设置。
6. 对切换按钮进行切换以启用“**在仅仪表板模式下显示控制台**”选项。

   之后，只有仪表板可供用户使用。用户可以监视统计信息，但不能更改网络保护设置和仪表板外观。由于为您显示的仪表板与为用户显示的仪表板相同，您也无法更改仪表板。

   如果禁用该选项，则会为用户显示主菜单，因此用户可以在 Open Single Management Platform 中执行各种操作，包括更改安全设置和小部件。

7. 完成配置仅仪表板模式后，单击“**保存**”按钮。只有这样，准备好的仪表板才会显示给用户。

8. 如果用户想要查看支持的卡巴斯基应用程序的统计信息并需要访问权限来执行此操作，请为用户配置权限。之后，卡巴斯基应用程序数据将在这些应用程序的小部件中显示给用户。

现在用户可以在自定义账户下登录 Open Single Management Platform 并在仅仪表板模式下监控网络保护统计信息。

管理和防护报告

本部分介绍如何使用报告、管理自定义报告模板、使用报告模板生成新报告以及创建报告交付任务。

使用报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

在 OSMP 控制台的“**监控**”区域中单击“**报告**”可打开报告。

默认下，报告包含 30 天内的信息。

Kaspersky Next XDR Expert 默认提供以下类别的报告：

- **保护状态**
- **部署**
- **更新**
- **威胁统计**
- **其他**

您可以创建自定义报告模板、编辑报告模板和删除它们。

您可以基于现有模板创建报告、导出报告到文件和创建报告传送任务。

报告模板

报告模板用于指定报告所依据的条件和数据，以及报告时间段。具有主管理员、租户管理员、2 级分析师和 1 级分析师角色的用户可以创建、编辑或删除报告模板。使用报告模板生成的报告显示在“**生成的报告**”选项卡中。

报告模板可从“**报告**”部分的“**模板**”选项卡中获取，其中会显示现有模板表。表包含以下信息：

- “**名称**”是报告模板的名称。

  您可以通过在列标题中点击排序图标 ⌄ 并选择**升序**或**降序**对报告模板进行排序。

  您还可以使用表格上方的“**搜索**”字段搜索报表模板。

搜索报告模板时使用正则表达式。

- “**租户**”是拥有该报告模板的租户的名称。
- “**更新时间**”是资源模板上次更新的日期和时间。
  您可以通过在列标题中点击排序图标 ⌄ 并选择**升序**或**降序**按此列对表格进行排序。
- “**创建者**”是创建报告模板的用户的姓名。
- “**描述**”是关于报表模板的可选信息。
- “**标签**”有助于查找报表模板。您可以通过在列标题中点击排序图标 ⌄ 来搜索报告模板，通过在**“搜索”**字段中指定要搜索的值，或使用复选框选择标签。
- “**计划**”是必须使用该模板生成报告的频率。如果未配置报告计划，则显示 `disabled` 值。
- “**上次报告**”是上次根据报告模板生成报告的日期和时间。
- “**包名称**”是用于处理事件的工具包的名称。
- “**通过电子邮件发送**”表示已配置为对生成的报告发送电子邮件通知。

如有必要，您可以点击齿轮 ⚙ 图标来自定义列。

在列表中选择报表模板后，您可以单击菜单图标 ⋮ 打开可用操作的下拉列表：

- “**显示依赖项**”可打开所选报表模板的依赖项图窗口。如有必要，您可以在该图表窗口中下载 SVG 格式的依赖项数据，并配置要应用于图表中显示的依赖项的过滤器。
- **查看版本历史**显示报表模板的版本历史记录。如有必要，您可以在侧边栏中比较版本并恢复到以前的版本。
- “**运行报告**”生成报告。生成的报告显示在**“生成的报告”**选项卡上。
- **查看所有已生成的报告**会显示为所选报告模板生成的所有报告列表。如有必要，您可以将所选报告保存为支持的格式之一，或将其删除。
- “**编辑计划**”允许您配置报告计划，并选择要接收有关生成的报告的电子邮件通知的用户。

您还可以在**资源 → 列表**部分查看您可以使用的报告模板列表。为此，请在**资源类型**列中选择**资源类型**。

创建报告模板

要创建报告模板：

1. 在主菜单中，转到“**监控**”→“**报告**”。
2. 单击**添加**。
   程序将启动“新报告模板向导”。使用“**下一步**”按钮继续向导操作。
3. 输入报告名称并选择报告类型。

4. 在向导的“**范围**”步骤中，选择基于该报告模板，其数据会显示在报告中的客户端设备集合（管理组、设备分类、所选设备或所有网络设备）。

5. 在向导的“**报告周期**”步骤中，指定报告期间。可用值：

   - 在两个指定日期之间
   - 从指定日期到报告创建日期
   - 从报告创建日期减去指定天数，到报告创建日期

   该页对一些报告可能不显示。

6. 单击“**确定**”关闭向导。

7. 执行以下操作之一：

   - 单击“**保存和运行**”按钮以保存新报告模板并基于其运行报告。
     报告模板被保存。报告被生成。
   - 单击“**保存**”按钮保存新报告模板。
     报告模板被保存。

您可以使用新模板来生成和查看报告。

查看和编辑报告模板属性

您可以查看和编辑报告模板的基本属性，例如，报告模板名称或显示在报告中的字段。

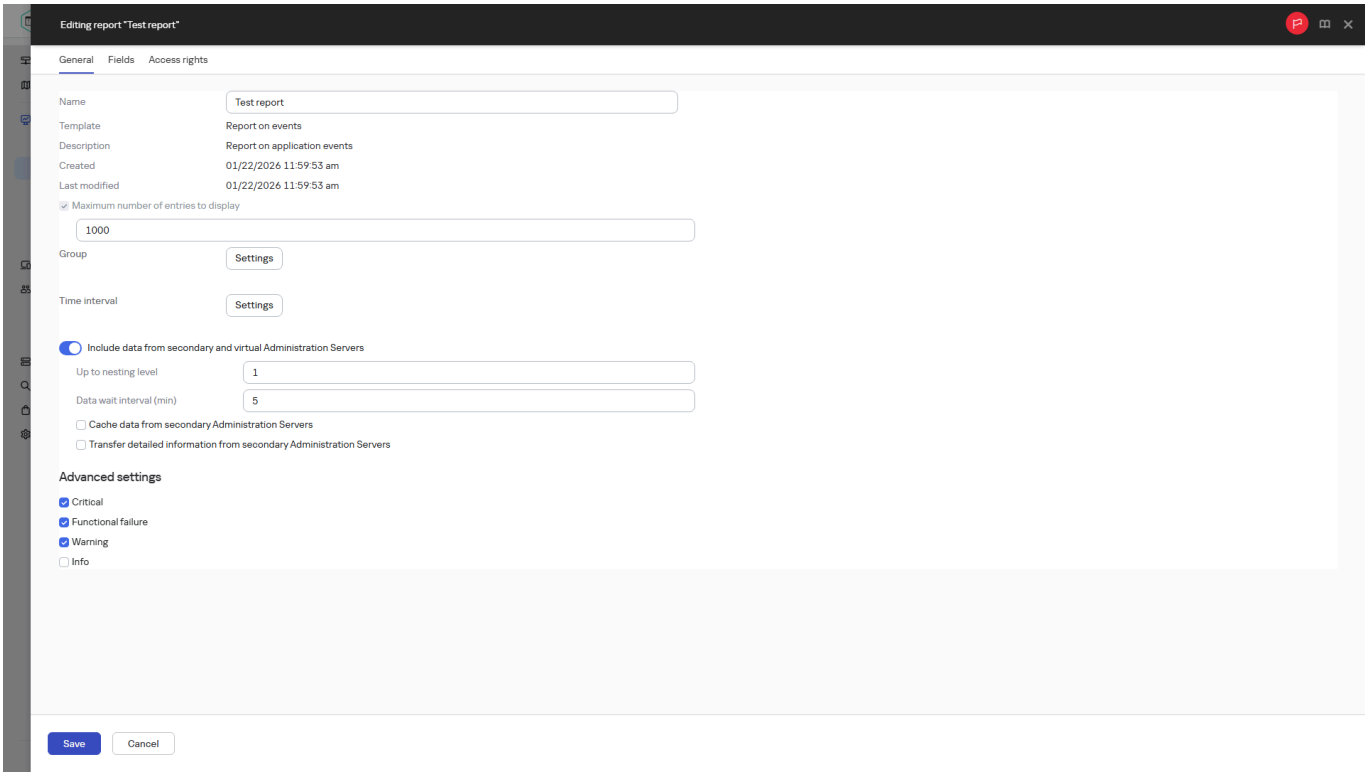
要查看和编辑报告模板属性：

1. 在主菜单中，转到“**监控**” → “**报告**”。

2. 选中您要查看和编辑其属性的报告模板旁边的复选框。
   另外，您可以先生成报告，然后单击“**编辑**”按钮。

3. 单击**打开报告模板属性**按钮。

“**编辑报告 <报告名称>**”窗口打开，其中已选择“**常规**”选项卡。



报告模板属性

4. 编辑报告模板属性：

- “**常规**”选项卡：
  - 报告模板名称
  - **显示条目的最大数量**

    如果启用该选项，显示在表格中的带有详细报告数据的条目数量不超过指定值。请注意，此选项不会影响将报告导出到文件时可包含在报告中的最大事件数。

    报告条目首先根据报告模板属性的**字段 → 详细信息字段**区域中指定的规则进行排序，然后仅保存第一个结果条目。带有详细报告数据的表头展示显示的条目数量和匹配其他报告模板设置的可用条目总数。

    如果禁用该选项，带有详细报告数据的表显示所有可用条目。我们不建议您禁用该选项。限制显示的报告条目数量降低数据库管理系统 (DBMS) 负载，也降低生成和导出报告的所需时间。一些报告包含太多条目。如果是这样，您可能难于阅读和分析所有。此外，设备在生成此类报告时可能会耗尽内存。这可能会导致您无法查看报告。

    默认情况下已启用该选项。默认值是 1000。
  - **组**

    单击“**设置**”按钮以更改为其创建报告的客户端设备集合。对于一些报告类型，按钮可能不可用。实际设置取决于创建报告模板时指定的设置。
  - **时间间隔**

    单击“**设置**”按钮以修改报告周期。对于一些报告类型，按钮可能不可用。可用值：
    - 在两个指定日期之间
    - 从指定日期到报告创建日期
    - 从报告创建日期减去指定天数，到报告创建日期

- **包含来自从属和虚拟管理服务器的数据**

  如果启用该选项，报告包含属于创建模板的管理服务器的从属和虚拟管理服务器的信息。

  如果您要仅从当前管理服务器查看数据，禁用该选项。

  默认情况下已启用该选项。

- **嵌套级别**

  报告包含位于当前管理服务器下小于或等于指定嵌套级别的从属和虚拟管理服务器的数据。

  默认值是 1。如果您必须从树中位于低级别的从属管理服务器接收信息，您可能要更改该值。

- **数据等待间隔(分钟)**

  在生成报告之前，创建报告模板的管理服务器等待从属管理服务器的数据指定分钟数。如果在该时间段后未从从属管理服务器接收到数据，报告依然运行。除了实际数据，报告还显示从缓存获取的数据（如果启用了“**缓存从属管理服务器数据**”选项），否则为 **N/A**（不可用）。

  默认值是 5 分钟。

- **缓存从属管理服务器数据**

  从属管理服务器定期传输数据到创建报告模板的管理服务器。传输的数据存储在缓存。

  如果在生成报告时当前管理服务器无法从从属管理服务器接收数据，报告显示从缓存接收的数据。数据传输到缓存的日期也被显示。

  启用该选项允许您查看从属管理服务器信息，即便实时数据无法被获取。然而，所显示数据可能过期。

  默认情况下已禁用该选项。

- **缓存更新频率(小时)**

  从属管理服务器定期传输数据到创建报告模板的管理服务器。您可以指定此时间段（以小时为单位）。如果指定 0 小时，则仅在生成报告时传输数据。

  默认值是 0。

- **从从属管理服务器传输详细信息**

  在生成的报告中，带有详细报告数据的表格包含创建报告模板的管理服务器的从属管理服务器的数据。

  启用该选项减慢报告生成并增加管理服务器之间的流量。然而，您可以在一个报告中查看所有数据。

  除了启用该选项，您可能想分析详细报告数据以检测故障从属管理服务器，然后仅为该故障管理服务器生成相同报告。

  默认情况下已禁用该选项。

- **字段**选项卡

  选择要在报告中显示的字段。使用 **上移**和**下移**按钮更改字段的显示顺序。使用“**添加**”按钮或“**编辑**”按钮指定是否报告中的信息必须排序并按照每个字段进行筛选。

  在“**详细字段过滤器**”区域中，还可以单击“**转换过滤器**”按钮以开始使用扩展筛选格式。通过这种格式可以使用逻辑或运算来组合各个字段中指定的筛选条件。单击该按钮后，“**转换过滤器**”面板在右侧打开。单击“**转换过滤器**”按钮以确认转换。您现在可以使用“**详细信息字段**”区域中的条件来定义转换的筛选器，这些条件通过逻辑或运算进行应用。

  将报告转换为支持复杂筛选条件的格式将使该报告与 Kaspersky Security Center 的早期版本（11 及更早版本）不兼容。此外，转换后的报告将不包含运行此类不兼容版本的从属管理服务器的任何数据。

5. 单击“**保存**”保存设置。

6. 关闭**编辑报告<Report name>**窗口。

更新的报告模板显示在报告模板列表。

删除报告模板

要删除一个或几个报告模板：

1. 在主菜单中，转到“**监控**”→“**报告**”。

2. 选择您要删除的报告模板旁边的复选框。

3. 下一步，单击“**删除**”按钮。

4. 在打开的窗口中，单击“**确定**”以确认您的选择。

所选报告模板被删除。如果这些报告模板被包含在报告传送任务中，它们也被从任务删除。

通用报告模板

在 KUMA 中，如果报告模板是在共享租户中创建的，则该模板被视为通用模板。在其他租户中创建的报告模板则为非通用模板。

要管理通用报告模板，用户需要以下角色：

- 创建、管理或删除报告模板需要“管理共享资源”角色。此角色权限授予对所有共享资源的权限。
  如果用户的角色涉及管理 CII 资源，则任何具有“管理共享资源”角色的用户都可以设置 CII 属性。
- “读取共享资源”角色允许查看通用报告模板列表。拥有此权限的用户将获得对所有共享资源的读取权限。

通用报告模板中的小部件的显示基于以下因素：

- 租户的小部件数据根据用户对租户的访问权限、全局租户过滤器以及报告模板或小部件的配置进行显示。
- 您可以通过单击“**更新预览**”按钮，在管理报告模板设置时查看小部件数据。
- 事件小部件数据根据用户的空间设置从数据库接收。如果在生成报告时发现用户没有权限访问一个或多个租户的空间，KUMA 将生成一个空白报告，并显示一条消息，指出由于缺乏对相关空间的访问权限，无法提供其他结果。
- 报告中的小部件数据可以包含或排除 CII。要访问包含 CII 数据的报告，用户必须具有“与 CII 交互”角色。
- 活动列表和上下文表小部件的限制适用于通用报告。

导出报告到文件

您可以将一份或多份报告保存为 XML、HTML 或 PDF。Open Single Management Platform 支持您同时将最多 10 个报告导出为指定格式的文件。

仅在您连接到 OSMP 控制台中的从属管理服务器时才可使用 PDF 格式。

要导出报告到文件：

1. 在主菜单中，转到“**监控**” → “**报告**”。
2. 选择您要导出的报告。

   如果您选择超过 10 个报告，**导出报告**按钮将被禁用。
3. 单击“**导出报告**”按钮。
4. 在打开的窗口中，指定以下导出参数：

   - **文件名**。

     如果您选择导出一份报告，请指定报告文件名。

     如果您选择多个报告，报告文件名将与所选报告模板的名称一致。
   - **最大条目数**。

     指定报告文件中包含的最大条目数。默认值是 10,000。

     您可以导出包含无限数量条目的报告。请注意，如果您的报告包含大量条目，则生成和导出报告所需的时间会增加。
   - **文件格式**。

     选择报告文件类型：XML、HTML 或 PDF。如果导出多个报告，所有选定的报告都会以指定格式保存为单独文件。

     仅在您连接到 OSMP 控制台中的从属管理服务器时才可使用 PDF 格式。

     将报告转换为 PDF 需要 wkhtmltopdf 工具。选择 PDF 选项后，从属管理服务器会检查设备上是否安装了 wkhtmltopdf 工具。如果未安装该工具，应用程序将显示一条消息，提示必须在管理服务器设备上安装该工具。手动安装该工具，然后继续下一步。
5. 单击“**导出报告**”按钮。

报告以指定格式保存到文件。

生成和浏览报告

要创建和查看报告，请执行以下操作：

1. 在主菜单中，转到“**监控**” → “**报告**”。
2. 单击要用于创建报告的报告模板的名称。

   将生成并显示使用所选模板的报告。

将根据为管理服务器设置的本地化集显示报告数据。

在生成的报告中，某些字体可能无法正确显示在图表上。要解决此问题，请安装 fontconfig 库。另外，请检查操作系统中是否安装了与您的操作系统区域设置相对应的字体。

该报告将显示下列数据：

- 在“**概要**”选项卡上：
  - 报告名称和类型、简要描述和报告时间段，以及为哪个设备组生成该报告的相关信息。
  - 图表显示最有代表性的报告数据。
  - 带有计算好的报告指示器的加固表格。
- 在“**详细信息**”选项卡上，显示一个包含详细报告数据的表格。

创建报告发送任务

您可以创建传送所选报告的任务。

要创建报告传送任务：

1. 在主菜单中，转到“**监控**” → “**报告**”。
2. 选择您要创建报告传送任务的报告模板旁边的复选框。
3. 单击“**创建传送任务**”按钮。

   “新任务向导”启动。使用下一步按钮进行向导。
4. 在向导的“**新任务设置**”步骤中，输入任务名称。

   默认名称为“**传送报告”。**如果已存在同名任务，则添加序列号 (<N>) 到任务名称中。

5. 在向导的“**报告配置**”步骤中，指定以下设置：

   a. 要使用任务传送的报告模板。

   b. 报告格式：HTML、XLS 或 PDF。

      将报告转换为 PDF 需要 wkhtmltopdf 工具。选择 PDF 选项后，管理服务器会检查设备上是否安装了 wkhtmltopdf 工具。如果未安装该工具，应用程序将显示一条消息，提示必须在管理服务器设备上安装该工具。手动安装该工具，然后继续下一步。

   c. 报告是否使用电子邮件连同邮件通知设置一起发送。

      您最多可以指定 20 个电子邮件地址。要分隔电子邮件地址，请按 **Enter** 键。您还可以粘贴以逗号分隔的电子邮件地址列表，然后按 **Enter** 键。

   d. 是否将报告保存到文件夹中，以及相应的设置。

      启用 **保存到文件夹**选项后，您必须指定该文件夹的 POSIX 路径。如果要将报告保存到共享文件夹，您还必须选择**指定账户以访问共享文件夹**复选框，然后指定用于访问此文件夹的用户账户和密码。

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

      将报告保存到本地文件夹时通常不需要凭证，因为运行管理服务器的账户可以访问此文件夹。如有必要，您可以在向导的**选择账户以运行任务**步骤中指定用户凭证。

      无论选择哪个文件夹，如果您希望新的报告文件覆盖上次任务启动时保存在报告文件夹中的文件，您也可以选择**覆盖相同类型的旧报告**复选框。

6. 在向导的“**配置任务计划**”步骤中，选择任务启动计划。

   有以下任务计划选项可用：

   - **手动**

     任务不自动运行。您仅可以手动启动。

     默认情况下已选定该选项。

   - **每 N 分钟**

     任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

     默认下，任务每 30 分钟运行一次，从当前系统时间开始。

   - **每 N 小时**

     任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

     默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

   - **每 N 天**

     任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

     默认下，任务每天运行一次，从当前系统日期和时间开始。

   - **每 N 星期**

     任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

默认下，任务每星期五于当前系统时间运行一次。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **在指定的日期**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击"**应用**"按钮。

7. 在向导的此步骤中，配置其他任务计划设置：

   - 在“**任务计划**”部分中，检查或重新配置先前选择的计划并设置时间间隔、月份或星期中的日期，设置病毒爆发条件或完成另一项任务作为启动任务的触发条件。如果选择了适用的计划，还可以在此部分指定开始时间。

   - 在“**附加设置**”部分，指定以下设置：

     - **运行错过的任务**

       该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

       如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

       如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

       默认情况下已禁用该选项。

     - **使用任务启动自动随机延迟**

       如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

       当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

       如果该选项被禁用，任务根据计划在客户端设备上启动。

     - **使用任务启动自动随机延迟间隔**

       如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

       如果该选项被禁用，任务根据计划在客户端设备上启动。

       默认情况下已禁用该选项。默认时间间隔为一分钟。

     - **如果任务运行超过该时间则停止**

       在指定时间段过后，任务被自动停止，无论它是否完成。

       如果您想要中断或停止执行时间太长的任务，则启用该选项。

       默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

8. 在向导的“**选择账户以运行任务**”步骤中，指定用于运行任务的用户账户的凭据。

9. 如果您希望在创建任务后修改其他任务设置，请在向导的“**完成任务创建**”步骤中，启用“**创建完成时打开任务详情**”选项。默认情况下已启用该选项。

10. 单击“**完成**”按钮创建任务并关闭向导。

报告传送任务被创建。如果启用了“**创建完成时打开任务详情**”选项，任务设置窗口会打开。

检测和响应报告

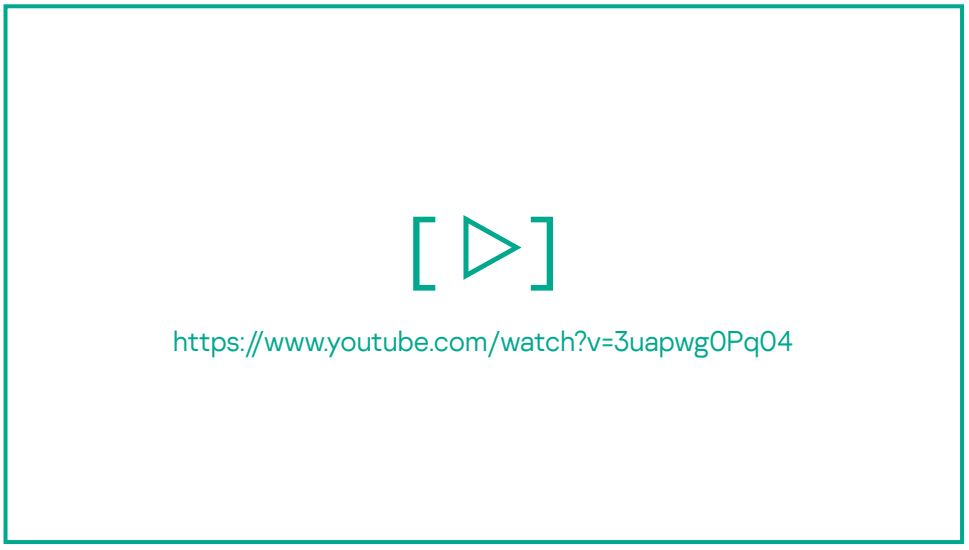
您可以在 KUMA 中计划进程和对象状态报告的生成。

报告使用“*报告模板*”*生成*。您可以在**“模板”**选项卡的“**报告**”部分找到报告模板。

您可以在“生成的报告”选项卡的**“报告”**部分找到**已生成的报告**。

要将生成的报告保存为 HTML 和 PDF 格式，请在装有 KUMA Core 的设备上安装所需的软件包。

在高可用性版本中部署 KUMA 时，KUMA Core 服务器的时区和用户浏览器中的时间可能不一致。这种差异表现为按计划生成的报告中的时间与用户可以从小部件导出的数据之间不一致。为避免这种差异，建议配置报告生成计划，考虑用户时区和 UTC 之间的差异。



报告模板

报告模板用于指定报告所依据的条件和数据，以及报告时间段。具有主管理员、租户管理员、2 级分析师和 1 级分析师角色的用户可以创建、编辑或删除报告模板。使用报告模板生成的报告显示在“**生成的报告**”选项卡中。

报告模板可从“**报告**”部分的“**模板**”选项卡中获取，其中会显示现有模板表。表包含以下信息：

- “**名称**”是报告模板的名称。
  您可以通过在列标题中点击排序图标 ⌄ 并选择**升序**或**降序**对报告模板进行排序。
  您还可以使用表格上方的“**搜索**”字段搜索报表模板。

  搜索报告模板时使用正则表达式。

- “**租户**”是拥有该报告模板的租户的名称。
- “**更新时间**”是资源模板上次更新的日期和时间。
  您可以通过在列标题中点击排序图标 ⌄ 并选择**升序**或**降序**按此列对表格进行排序。
- “**创建者**”是创建报告模板的用户的姓名。
- “**描述**”是关于报表模板的可选信息。
- “**标签**”有助于查找报表模板。您可以通过在列标题中点击排序图标 ⌄ 来搜索报告模板，通过在**“搜索”**字段中指定要搜索的值，或使用复选框选择标签。

- "**计划**"是必须使用该模板生成报告的频率。如果未配置报告计划，则显示 `disabled` 值。
- "**上次报告**"是上次根据报告模板生成报告的日期和时间。
- "**包名称**"是用于处理事件的工具包的名称。
- "**通过电子邮件发送**"表示已配置为对生成的报告发送电子邮件通知。

如有必要，您可以点击齿轮 图标来自定义列。

在列表中选择报表模板后，您可以单击菜单图标 打开可用操作的下拉列表：

- "**显示依赖项**"可打开所选报表模板的依赖项图窗口。如有必要，您可以在该图表窗口中下载 SVG 格式的依赖项数据，并配置要应用于图表中显示的依赖项的过滤器。
- **查看版本历史**显示报表模板的版本历史记录。如有必要，您可以在侧边栏中比较版本并恢复到以前的版本。
- "**运行报告**"生成报告。生成的报告显示在"**生成的报告**"选项卡上。
- **查看所有已生成的报告**会显示为所选报告模板生成的所有报告列表。如有必要，您可以将所选报告保存为支持的格式之一，或将其删除。
- "**编辑计划**"允许您配置报告计划，并选择要接收有关生成的报告的电子邮件通知的用户。

您还可以在**资源 → 列表**部分查看您可以使用的报告模板列表。为此，请在**资源类型**列中选择**资源类型**。

创建报告模板

要创建报告模板：

1. 打开 OSMP Console，然后转到以下部分之一：
   - **报告 → 模板**
   - **资源 → 列表**
     如果您选择了此部分，为了方便查看对象，您可以在表格的**资源类型**列中选择**报告模板**。
2. 根据所选部分，执行以下操作之一：
   - 在**报告 → 模板**部分，单击报告模板表格上方的**创建新模板**按钮。
   - 在**资源→列表**部分，单击**创建新模板**按钮，然后在资源列表中选择**报告模板**。
3. 这将打开一个窗口；在该窗口中，输入报告模板的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。
   自定义报告模板不能与主租户中预定义的报告模板同名。
   在主租户中，如果您尝试创建与预定义报告模板同名的报表模板，或者将预定义报告模板的名称分配给自定义报告模板，则会传回错误。在主租户之外的其他租户中，您可以创建或复制与预定义报告模板同名的自定义报告模板。我们建议为自定义报告模板使用自定义名称。
4. 在**模板租户**下拉列表中，选择将拥有所创建报告模板的租户。
5. 在**"从租户收集数据"**下拉列表中，选择一个或多个租户。系统会根据所选租户的数据生成报告。

6. 如有必要，请在“**时间段”**下拉列表中选择要获取分析数据的时间段，方法如下：

   - 如果您想指定确切日期，请在左侧日历中选择时间段的开始日期和结束日期，然后单击**“应用”**。

     您可以选择包括当前日期在内的任意日期。日期和时间格式取决于浏览器的设置。如果**“范围起始”**或**“范围结束”**字段已有值，且您未手动编辑时间值，则当您在日历中选择日期时，**“范围起始”**字段会自动填充 00:00:00.000，“**范围结束**”字段会自动填充 23:59:59.999。如果您手动删除了**起始日期**或**结束日期**字段中的值，则当您在日历中选择日期时，该字段会自动填充当前时间。在其中一个字段中选择值后，焦点将切换到另一个字段。如果**结束日期**早于**起始日期**，则系统会自动将这一较早的值插入**起始日期**字段。

   - 如果您想指定相对时间段，请在右侧的**“相对时间段”**列表中选择一个可用时间段。

     时间段是相对于当前时间计算的。

   - 如果您想指定自定义时间段，请编辑**起始日期**和**结束日期**字段的值。

     您可以按 **DD.MM.YYYY HH:mm:ss.SSS** 格式（俄语本地化版本）和 **YYYY-MM-DD HH:mm:ss.SSS**（英语本地化版本）输入确切的日期和时间，或者通过公式输入相对时间段。如果需要，您还可以结合使用这些方法。如果在输入确切日期时未指定毫秒，系统会自动补填 000。如果您已编辑**起始日期**或**结束日期**字段中的时间，则在日历中选择日期不会更改时间部分。

     在相对时间段公式中，您可以使用“**now**”参数表示当前日期和时间以及间隔参数化语言：**+**（仅在“**范围结束**”字段中）、**-**、**/**（四舍五入到最接近的数），以及时间单位：**yMM**（月）、**w**（周）、**d**（天）、**h**（小时）、**m**（分钟）、**s**（秒）。例如，您可以指定“**now-5d**”时间段以获取过去五天的数据，或指定“**now/w**”时间段以获取从本周第一天开始时间 (00:00:00:000 UTC) 到当前时间 (**now**) 的数据。

     > “**范围起始**”字段为必填项，其值不能超过“**范围结束**”字段的值，且不能早于 1970 年 1 月 1 日（如果指定确切日期或相对时间段）。**结束日期**不能早于**起始日期**。如果未在“**范围结束**”字段中指定值，则自动指定 **now**。

   默认情况下，选择“**1 天（now-1d）**”相对时间段。时间段的两个边界均包含在内。例如，对于“**今天**”时间范围，将显示从当天开始时间 (00:00:00:000) 到当前时间（**当前时间**，含当前时间）的事件；对于“**昨天**”时间段，将显示从前一天开始时间 (00:00:00:000) 到当天 00:00:00:000 的事件。

   KUMA 以 UTC 格式存储时间值，但在用户界面中，时间会转换为浏览器所在的时区。这与相对时间段相关：**今天**、**昨天**、**本周**和**本月**。例如，如果浏览器所在的时区是 UTC+3，并且您选择“**今天**”作为数据显示时间段，则将显示从 03:00:00.000 到现在的数据，而不是从 00:00:00.000 到现在的数据。

   如果在选择相对数据显示时间段（例如**今天**、**昨天**、**本周**或**本月**）时要考虑时区，则需要通过添加或减去正确的小时数在“**范围起始**”和“**范围结束**”中手动添加时间偏移量（如果指定了 now 以外的值），即加上或减去正确的小时数。例如，如果您的浏览器时区为 UTC+3，并且您想显示**昨天**的数据，则需要将**“范围起始”**更改为“**now-1d/d-3h**”，并将“**范围结束**”更改为“**now/d-3h**”。如果您想显示**今天**时间段的数据，只需将**起始日期**字段中的值更改为**now/d-3h**。

   > 如果您需要截至昨天 23:59:59:999 UTC 的结果，可以使用带有时间戳过滤器的 SQL 查询，或者指定确切的日期和时间。

7. 如果必要，在“**保留期**”字段中，指定您希望存储根据此模板生成的报告的时长。

   默认值是 3 个月。

8. 如有必要，请从**“标签”**下拉列表中选择报告模板的标签。

9. 如有必要，请添加报告模板的描述。

10. 使用“**CII 状态**”切换开关可启用与关键信息基础设施 (CII) 相关的资产、警报和事故信息的显示。启用后，只有在设置中选中“**访问 CII 设施**”复选框的用户才能查看计算数据包含 CII 信息的报告。

    如果此切换开关被禁用，即使用户拥有 CII 设施的访问权限，报告的小部件也不会显示与关键信息基础设施 (CII) 相关的资产、警报和事故信息。

11. 单击“**保存**”按钮。

12. 这将打开一个窗口；在该窗口中，您可以单击**上传文件**链接来更改报告模板的徽标。在文件选择窗口中，选择徽标的图像文件。图片格式必须为 JPEG、PNG 或 GIF，且大小不得超过 3 MB。

    添加的徽标将显示在报告中，以替代 KUMA 徽标。

13. 单击“**添加小部件**”按钮并选择一个小部件。这将打开一个窗口；在该窗口中，配置所选小部件。

14. 您可以添加多个小部件。您可以使用手柄图标（⠿）在窗口中拖动小部件。如果需要调整小部件的大小，可以使用调整大小图标（⤡）。当您将鼠标悬停在小部件右下角时，会显示该图标。

15. 以下限制适用于**饼图**、**条形图**、**折线图**、**计数器**和**日期直方图**图表类型的小部件：

    - 在“`SELECT`”查询中，您可以使用“`String`”、“`Number`”和“`Float`”类型的扩展事件架构字段。
    - 在“`WHERE`”查询中，您可以使用所有类型的扩展事件架构字段（“`String`”、“`Number`”、“`Float`”、“`Array of strings`”、“`Array of numbers`”和“`Array of floats`”）。

    对于具有“`Table`”图表类型的小部件，在“`SELECT`”查询中，您可以使用所有类型的扩展事件架构字段（“`String`”、“`Number`”、“`Float`”、“`Array of strings`”、“`Array of numbers`”和“`Array of floats`”）。

16. 点击小部件右上角的菜单⋮图标，您可以执行以下操作：

    - 管理小部件的设置
    - 创建小部件副本
    - 移除小部件
    - 以 CSV 格式下载小部件数据

17. 单击“**创建**”按钮。

    新的报告模板显示在OSMP控制台的**报告** →**模板**和**资源**→**列表**选项卡中。您可以手动运行此报告。如果要自动生成报告，则需要配置计划。

配置报告计划

要配置报告计划：

1. 打开 KUMA Web 界面，选择**“报告”** → **“模板”**。
2. 在报表模板列表表格中，选择一个报告模板，然后单击菜单图标⋮。
3. 在下拉列表中，选择“**编辑计划**”。

   这会打开“**编辑计划**”窗口。

4. 如果需要定期生成报告：

   a. 启用**按排程发送报告**切换开关。

   b. 在**“每隔”**下，指定生成报告的频率。

   您可以按天、周、月或年指定生成报告的频率。根据所选时间段，您应该指定报告生成的时间、星期几、每月几日或具体日期。

   c. 在“**时间**”字段中，输入必须生成报告的时间。

   d. 在**“时区”**下拉列表中，选择报告生成时间的时区。

5. 在**通知设置**下，指定以下内容：

   a. 在**“通知模板”**下拉列表中，选择要按计划发送给用户的通知表单。

   b. 在“**发送到**”设置组中，单击“**添加**”。

   c. 这将打开一个窗口；在该窗口中，添加要获取报告的用户组，并选择一种格式。为此请执行以下操作：

   - 在**“电子邮件”**下拉列表中，选择报告收件人的电子邮件地址。
   - 在“**格式**”下拉列表中，选择报告格式。可提供以下格式：PDF、HTML、CSV、拆分 CSV、Excel。

   您可以点击**“添加组”**按钮添加多个报告接收者组。

   每次手动生成报告或 KUMA 按计划自动生成报告时，报告都会发送到指定的地址。

   > 如果您希望通过电子邮件发送生成的报告，则需要配置 SMTP 连接。

   如果电子邮件报告的收件人是 KUMA 用户，他们可以通过点击电子邮件中的链接下载或查看报告。如果收件人不是 KUMA 用户，他们可以单击链接但无法登录 KUMA，因此他们只能获取附件。

   建议通过单击 Web 界面中的链接来查看 HTML 报告，因为在某些屏幕分辨率下，附件中的 HTML 报告可能无法正确显示。

   如果您发送的电子邮件没有附件，收件人只能通过点击链接获取报告，并且只有在 KUMA 中获得授权后才能获取报告，不受角色或租户的限制。

   d. 然后单击“**添加**”按钮。

6. 单击“**保存**”按钮。

报告计划已配置。

编辑报告模板

要编辑报告模板：

1. 打开 KUMA Web 界面，并转到以下部分之一：

   - **报告 → 模板**
   - **资源 → 列表**
     如果您选择了此部分，为了方便查看对象，您可以在表格的**资源类型**列中选择**报告模板**。

2. 根据所选部分，执行以下操作之一：

   - 在**报告 → 模板**部分，单击报告模板表中的报告模板名称。
   - 在**资源→列表**部分，点击资源列表中报告模板名称旁边的编辑设置图标（）。

   这将打开**编辑模板**窗口。
   您也可以在“报表”→“生成的报告”选项卡上打开此窗口，方法是选择现有报告并单击“编辑模板”按钮。

   > 您也可以在**报告 → 生成的报告**选项卡上选择现有报告，然后单击**编辑报告**按钮来打开此窗口。

3. 请进行必要的更改：

   - 更改报告模板的名称。
   - 修改发送报告数据的租户列表。
   - 点击**“设置”**按钮，更改获取分析数据的时间段、保留期限、标签和报告模板的描述。
   - 点击**“添加小部件”**按钮，将小部件添加到报告模板中。
   - 点击菜单图标（）查看此模板生成的报告列表，或删除报告模板。
   - 点击**上传文件**链接并上传新徽标，即可更改报告徽标。如果模板已包含徽标，则必须先将其删除。
   - 拖动小部件即可更改其位置。
   - 将鼠标悬停在小部件上时，使用出现的调整大小图标（）调整小部件的大小。
   - 点击小部件上的菜单图标（），您可以管理小部件设置、复制小部件、删除小部件或以 CSV 格式下载小部件数据。

4. 单击“**保存**”按钮。

报告模板已修改，并显示在KUMA网页界面的**报告→模板**和**资源→列表**选项卡上。

复制报告模板

要创建报告模板的副本：

1. 打开 KUMA Web 界面，并转到以下部分之一：

   - **报告 → 模板**
   - **资源 → 列表**
     如果您选择了此部分，为了方便查看对象，您可以在表格的**资源类型**列中选择**报告模板**。

2. 在表格中，选择一个报告模板，然后单击表格上方的**"复制"**按钮。
3. 这将打开一个窗口；在该窗口中，输入报告模板的名称。复制报表模板时，报告名称会注明它是副本。
4. 在**模板租户**下拉列表中，选择将拥有所创建报告模板的租户。
5. 在**"收集租户数据"**下拉列表中，选择一个或多个您希望在报告模板中显示其数据的租户。
6. 根据需要更改以下设置：

   - 报告生成周期。
   - 报告保存期限。
   - 报告模板的标签。
   - 报告模板说明。
   - 生成包含 CII 信息的报告数据。

7. 单击"**保存**"按钮。

报告模板的副本已创建，并显示在KUMA网页界面的**报告→模板**和**资源→列表**选项卡上。

删除报告模板

要删除报告模板，请执行以下操作：

1. 打开 KUMA Web 界面，并转到以下部分之一：

   - **报告 → 模板**
   - **资源 → 列表**
     如果您选择了此部分，为了方便查看对象，您可以在表格的**资源类型**列中选择**报告模板**。

2. 在报告模板表格中，选中报告模板的复选框，然后单击表格上方的**"删除"**按钮。
   确认窗口打开。

3. 执行以下操作之一：

   - 如果您只想删除报告模板，请单击“**删除**”按钮。
   - 如果您想要删除报告模板以及使用该模板生成的所有报告，请单击“**连同报告一起删除**”按钮。

报告模板被删除。

导出或导入报告模板

要导出报告模板：

1. 打开 KUMA Web 界面，并转到以下部分之一：

   - **报告 → 模板**
   - **资源 → 列表**
     如果您选择了此部分，为了方便查看对象，您可以在表格的**资源类型**列中选择**报告模板**。

   这将打开一个窗口，其中列出了 KUMA 中所有可用的报告模板。

2. 使用复选框选择要导出的报告模板。

3. 点击报告模板表格上方的**“导出”**按钮。

4. 在显示的侧边栏中：

   a. 请输入导出资源文件的密码。密码必须满足以下要求：

      - 至少 16 个字符。
      - 至少包含一个小写字母。
      - 至少包含一个大写字母。
      - 至少有一个数字。
      - 至少有一个特殊字符。

   b. 在“**租户**”下拉列表中，选择要从其导出所选资源的租户。

   c. 选中复选框以指定要导出的资源。
      如果选中**所有资源**复选框，则会导出所选租户文件夹中的所有资源。

5. 单击“**导出**”按钮。

导出报表模板时，请考虑以下事项：

- 报表模板导出时不包含租户、存储和空间信息，因为这些参数是针对每个 KUMA 部署单独配置的。
- 报告模板小部件导出时也不包含租户、存储和空间信息。

要导入报告模板：

1. 打开 KUMA Web 界面，并转到以下部分之一：

   - **报告 → 模板**
   - **资源 → 列表**
     如果您选择了此部分，为了方便查看对象，您可以在表格的**资源类型**列中选择**报告模板**。

   这将打开一个窗口，其中列出了 KUMA 中所有可用的报告模板。

2. 使用复选框选择要导入的报表模板。

3. 单击资源表格上方的**"导入"**按钮。

4. 在侧边栏的**"租户"**下拉列表中，选择要将报表模板导入到的租户。

5. 选择导入源：**文件**或**存储库**。

6. 根据所选的导入源，执行以下步骤：

   a. 如果您选择**"文件"**作为导入源，请执行以下步骤：

      - 指定导入文件的密码。
      - 单击"**选择文件**"按钮选择要导入的文件。
      - 选中要导入的资源的复选框。

   b. 如果您选择**"存储库"**作为导入源，请在显示的表格中选择一个或多个存储库包。

7. 单击"**导入**"按钮。

8. 如有必要，请解决从文件中导入的资源与现有资源之间的冲突。

导入报告模板时，请注意以下事项：

- 如果将报告模板导入到任何租户，则导入的报告模板的租户将被指定为资源租户和数据源租户。
- 导入资源后，您需要为包含事件的小部件指定空间，并在必要时展开租户列表。

通用报告模板

在 KUMA 中，如果报告模板是在共享租户中创建的，则该模板被视为通用模板。在其他租户中创建的报告模板则为非通用模板。

要管理通用报告模板，用户需要以下角色：

- 创建、管理或删除报告模板需要"管理共享资源"角色。此角色权限授予对所有共享资源的权限。
  如果用户的角色涉及管理 CII 资源，则任何具有"管理共享资源"角色的用户都可以设置 CII 属性。
- "读取共享资源"角色允许查看通用报告模板列表。拥有此权限的用户将获得对所有共享资源的读取权限。

通用报告模板中的小部件的显示基于以下因素：

- 租户的小部件数据根据用户对租户的访问权限、全局租户过滤器以及报告模板或小部件的配置进行显示。
- 您可以通过单击“**更新预览**”按钮，在管理报告模板设置时查看小部件数据。
- 事件小部件数据根据用户的空间设置从数据库接收。如果在生成报告时发现用户没有权限访问一个或多个租户的空间，KUMA 将生成一个空白报告，并显示一条消息，指出由于缺乏对相关空间的访问权限，无法提供其他结果。
- 报告中的小部件数据可以包含或排除 CII。要访问包含 CII 数据的报告，用户必须具有“与 CII 交互”角色。
- 活动列表和上下文表小部件的限制适用于通用报告。

生成的报告

所有报告均使用“报告模板”生成。生成的报告位于“**报告**”部分的“**生成的报告**”选项卡中，并显示在包含以下信息的表格中：

- **名称** – 报告模板的名称。

  您可以通过在列标题中点击排序图标 ⌄ 并选择**升序**或**降序**对报告模板进行排序。

  您还可以使用表格上方的**搜索**字段按名称搜索报告模板。
- **时间段** – 提取报告分析数据的时间段。
- **上次报告** – 上次生成报告的日期和时间。
- 您可以通过在列标题中点击排序图标 ⌄ 并选择**升序**或**降序**按此列对表格进行排序。
- **租户** – 拥有该报告的租户的名称。
- **用户** – 手动生成报告的用户的名称。如果报告是按计划生成的，则该值为空。如果报告是在版本低于 2.1 的 KUMA 中生成的，则该值为空。

如有必要，您可以点击齿轮 ⚙ 图标来自定义列。

在生成的报告列表中选择一份报告后，您可以：

- 创建报告。
- 打开和查看报告。
- 将生成的报告保存为特定格式。可用格式：HTML、PDF、CSV、拆分 CSV、Excel。默认情况下，所有格式均显示 250 行。PDF 和 HTML 格式的表格最大行数为 500 行。如果要在报告中输出超过 500 行，请在 SQL 查询中设置 LIMIT 参数的值，并将报告保存为 CSV 格式。
- 管理报告模板的设置。
- 删除报告。

查看报告

要打开报告：

1. 打开 KUMA Web 界面，选择**“报告”** → **“生成的报告”**。
2. 在报告表格中，单击已生成报告的名称。

   新的浏览器窗口将打开，其中的小部件显示报告分析数据。如果某个小部件显示有关事件、警报、事故或活动列表的数据，您可以单击其标题以打开 KUMA Web 界面的相应部分，其中包含用于显示该小部件数据的活动过滤器和/或搜索查询。小部件应用默认值。

   要查看完整数据，请使用请求中指定的设置下载 CSV 格式的报告。

   如果您在小部件设置中启用了**“显示总计”**切换开关，则小部件会显示**总计**值，但当您以 CSV 或扩展 CSV 格式附加或上传报告时，不会显示**总计**值。要在报告中显示**总计**值，您可以使用 Excel 公式，或从小部件复制并粘贴总计值，或使用 PDF 或 HTML 附件。
3. 如果必要，您可以单击“**另存为**”按钮将报告保存为选择的格式。

生成报告

您可以手动生成报告或配置计划以自动生成报告。

要手动生成报告：

1. 打开 KUMA Web 界面，转到**“报告”**部分。
2. 执行以下操作之一：

   a. 在**“生成的报告”**选项卡上：

   - 选中报告表格中报告的复选框。
   - 点击表格上方的**“生成报告”**按钮。

   b. 在**“模板”**选项卡上：

   - 通过选中报告模板表中的复选框来选择报告。
   - 点击菜单图标 ⋮ 并从下拉列表中选择“**生成报告**”。

   15 秒内，报告将生成并显示在“报告”→“生成的报告”选项卡上。

您还可以配置报告计划，以实现报告的自动生成。

保存报告

要以所需的格式保存报告：

1. 打开 KUMA Web 界面，选择**“报告”** → **“生成的报告”**。
2. 在已生成报告表格中，选中相应报告的复选框。
3. 在表格上方的**另存为**下拉列表中，选择一种格式：HTML、PDF、CSV、拆分 CSV、Excel。
   报告将保存到您在浏览器中配置的下载文件夹中。

您还可以在查看报告时将其保存为所需的格式。

更新报告

要更新已生成的报告：

1. 打开 KUMA 网页界面，然后转到**报告** → **已生成报告**部分。
2. 在已生成报告表格中，选择一个报告。
3. 点击表格上方的**“生成报告”**按钮。
   报告将在 15 秒内更新，并可在**报告** → **已生成报告**部分中查看。

删除报告

要删除报告：

1. 打开 KUMA Web 界面，选择**“报告”** → **“生成的报告”**。
2. 在已生成报告表格中，选择一个报告。
3. 单击表格上方的“**删除**”按钮。
   确认窗口打开。
4. 单击“**删除**”按钮。
   所选报告被删除。

事件和事件分类

本节介绍事件和事件分类、Kaspersky Next XDR Expert 组件中发生的事件类型，以及频繁事件阻止功能的管理。

关于 Kaspersky Next XDR Expert 中的事件

Kaspersky Next XDR Expert 允许您接收有关管理服务器和受管理设备上安装的 Kaspersky 应用程序运行期间所发生事件的信息。事件信息保存在管理服务器数据库。

按类型分组的事件

Kaspersky Next XDR Expert 提供以下类型的通知：

- 常规事件。这些事件发生在所有受管理卡巴斯基应用程序中。常规事件的一个示例是病毒爆发常规事件具有严格定义的语法和语义。常规事件用于报告和仪表板等方面。
- 受管理卡巴斯基应用程序特定事件。每个受管理卡巴斯基应用程序都拥有自己的事件集。

按来源分组的事件

您可以在应用程序策略的“**事件配置**”选项卡上查看应用程序可以生成的事件的完整列表。对于管理服务器，您还可以在管理服务器属性中查看事件列表。

以下应用程序可以生成事件：

- Kaspersky Next XDR Expert 组件：
  - 管理服务器
  - 网络代理
- 受管理的卡巴斯基应用程序

  有关受管理的卡巴斯基应用程序生成的事件的详细信息，请参阅相应应用程序的文档。

按重要性级别分组的事件

每个事件都有自己的重要级别。取决于发生的条件，一个事件可以被分配不同的重要级别。四个事件重要级别如下：

- *严重事件*指示发生了可能导致数据丢失、操作系统异常或严重错误的严重问题。
- *功能失败*指示在应用程序运行期间或过程执行期间发生了严重问题、错误或功能异常。
- *警告*是不严重的事件，但是也指示了今后可能发生的潜在问题。如果在事件发生后应用程序可以被恢复而不丢失数据或功能，则这些事件是警告级别。
- *信息*事件用于提示成功完成操作、应用程序的正常功能或完成了某过程。

每个事件都有规定的存储期限，在此期间，您可以在 Kaspersky Next XDR Expert 中查看或修改该事件。一些事件默认下不保存在管理服务器数据库，因为它们的存储期限是零。仅可以在管理服务器数据库中保存至少一天的事件可以被导出到外部系统。

Kaspersky Next XDR Expert 组件事件

Kaspersky Next XDR Expert 的每个组件都有自己的一组事件类型。本部分列出了管理服务器和网络代理中发生的事件类型。卡巴斯基应用程序中发生的事件类型不在此区域列出。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型描述的数据结构

对于每个事件类型，它的显示名称、ID、字母码、描述和默认存储期限被提供。

- **事件类型显示名称**。此文本会在您配置事件以及事件发生时显示在 Kaspersky Next XDR Expert 中。
- **事件类型 ID**。该数码在您使用第三方工具分析事件时使用。
- **事件类型**（字母码）。当您使用 Kaspersky Next XDR Expert 数据库中提供的公共视图浏览和处理事件以及将事件导出到 SIEM 系统时，会使用此代码。
- **描述**。该文本包含事件发生的情况以及此种情况下您可以做的事。
- **默认存储期限**。这是事件存储在管理服务器数据库的天数，显示在管理服务器事件列表中。该时间段之后，事件被删除。如果事件存储期限值是 0，此类事件被检测但不显示在管理服务器事件列表。如果您配置了保存此类事件到操作系统事件日志，您可以在那里找到它们。

  您可以更改事件的存储期限：设置事件的存储期限。

管理服务器事件

该部分包含管理服务器相关事件信息。

管理服务器严重事件

下表显示严重级别为**严重**的管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
移动设备的管理服务器证书已过期	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。	180 天
审计：导出到 SIEM 失败	5130	KLAUD_EV_SIEM_EXPORT_ERROR	当由于与 SIEM 系统的连接错误而将事件导出到 SIEM 系统失败时，会发生此类事件。	180 天
设备已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理设备在网络中可见，但指定时间未连接到管理服务器，则该类型的事件发生。 找到什么阻止了设备上网络代理的正常功能。可能的原因包括网络问题和从设备卸载网络代理。	180 天
设备状态是“严重”	4113	KLSRV_HOST_STATUS_CRITICAL	当受管理设备被分配*严重*状态时，该类型的事件发生。您可以配置设备状态被更改到*严重*的条件。	180 天
授权许可即将过期	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	当商业授权许可的失效日期即将到来时，会发生此类事件。 Open Single Management Platform 每天会检查一次授权许可到期日期是否临近。此类型的事件在授权许可到期之前 30 天、15 天、5 天 和 1 天发布。该天数无法被更改。如果管理服务器在授权许可到期日之前的指定日期被关闭，则事件直到第二天才发布。 商业授权许可到期后，Kaspersky Next XDR Expert 仅提供基本功能。 您可以通过以下方式响应事件： • 确保已将备用授权许可密钥添加到管理服务器。 • 如果您使用订阅，请确保续订。如果无限制订阅已在到期日前预付费给服务提供商，则该订阅会自动续订。	180 天
已超过授权许可数量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Next XDR Expert 每天检查一次是否超过授权许可数量限制。 当管理服务器检测到以下两种情况时，会生成此类事件：一是安装在客户端设备上的卡巴斯基应用程序快超过某些授权许可限制；二是单个授权许可所涵盖的当前已使用的授权许可单元数量，超过了该授权许可所涵盖总单元数量的 110%。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Next XDR Expert 确定超过授权许可数量限制时生成事件的规则。	180 天
受限制功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	当 Kaspersky Next XDR Expert 开始仅以基本功能运行，不提供漏洞和补丁管理及移动设备管理功能时，会发生此类事件。 以下是事件发生的原因和正确响应： • 授权许可期限已过期。提供授权许可，以使用 Kaspersky Next XDR Expert 的完整功能模式（将有效激活码或密钥文件添加到管理服务器）。 • 管理服务器管理比授权许可限制更多的设备。从管理服务器的管理组移动设备到其他管理服务器的管理组（如果其他管理服务器的授权许可限制允许）。	180 天
MDM 证书已到期	4132	KLSRV_CERTIFICATE_EXPIRED	当移动设备上的客户端移动证书过期时，就会发生此类事件。	180 天
密钥文件已被添加到拒绝列表	4124	KLSRV_LICENSE_BLACKLISTED	当 Kaspersky 已将您使用的激活码或密钥文件添加到拒绝列表时，会发生该类型事件。 联系技术支持获得更多详情。	180 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
卡巴斯基应用程序模块更新已撤销	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	当卡巴斯基专家撤销更新（例如，为了将其替换为较新版本）时，会发生此类事件。对于此类更新，状态为*已撤销*。该事件涉及 Kaspersky Next XDR Expert 补丁，与受管理的 Kaspersky 应用程序模块无关。事件提供无缝更新未被安装的原因。	180 天
病毒爆发	• 26 (对于文件威胁防护) • 27 (对于邮件威胁防护) • 28 (对于防火墙)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	

管理服务器功能失败事件

下表显示了具有“**功能失败**”重要级别的管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器功能失败事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
将更新复制到指定文件夹失败	4123	KLSRV_UPD_REPL_FAIL	当软件更新被复制到附加共享文件夹时，该类型的事件发生。 您可以通过以下方式响应事件： • 检查用于获取文件夹访问的用户账户是否具有写权限。 • 检查文件夹的用户名和/或密码是否已更改。 • 检查互联网连接，因为它可能是事件原因。遵照指示更新数据库和软件模块。	180 天
轮询云段失败	4143	KLSRV_KLCLOUD_SCAN_ERROR	当管理服务器无法在云环境中轮询网段时，将发生此类事件。读取事件描述中的详细信息，并相应做出响应。	未存储
已授权应用程序组之一的安装已超过限制	4126	KLSRV_INVLICPROD_EXCEDED	管理服务器定期生成该类型的事件（每小时）。如果您在 Kaspersky Next XDR Expert 中管理第三方应用程序的授权许可密钥，并且安装数量已超过第三方应用程序授权许可密钥设定的限制，则会发生此类事件。 您可以通过以下方式响应事件： • 查看受管理设备列表。从未使用第三方应用程序的设备上删除该应用程序。 • 为更多设备使用第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。这是一组由满足您所设标准的第三方应用程序组成的授权应用程序群组。	180 天
没有剩余硬盘空间	4107	KLSRV_DISK_FULL	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	180 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
管理服务器数据库空间不足	4110	KLSRV_DATABASE_FULL	当管理服务器数据库没有剩余空间时，该类型的事件发生。 当管理服务器的数据库达到其容量，以及当不可能再往数据库记录时，管理服务器不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应： • 限制存储在管理服务器数据库的事件数量。 • 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security 策略的设置。 在 DBMS 选项处查看信息。	180 天
运行时错误	4125	KLSRV_RUNTIME_ERROR	由于未知问题，该类型的事件发生。 多数情况下，这些是 DBMS 问题、网络问题和其他软件和硬件问题。 事件详情可以在事件描述中找到。	180 天
共享文件夹不可用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理服务器共享文件夹不可用，则该类型的事件发生。 您可以通过以下方式响应事件： • 检查管理服务器(共享文件夹所在位置)是否已开启并可用。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查网络连接。	180 天
管理服务器数据库不可用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理服务器数据库不可用则该类型的事件发生。 您可以通过以下方式响应事件： • 检查安装了 DBMS 的远程服务器是否可用。 • 查看 DBMS 日志以发现管理服务器数据库不可用的原因。	180 天

管理服务器警告事件

下表显示具有“**警告**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器警告事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
移动设备的管理服务器证书即将过期	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。	90 天
APNs 证书即将过期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	当 APNs 证书距离过期不到 14 天时，会发生此类事件。 当 APNs 证书过期时，您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。 我们建议您在过期日期前安排 APNs 证书续订。	未存储
APNs 证书已过期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	当 APNs 证书过期时，会发生此类事件。 您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。	未存储

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
审计：到 SIEM 服务器的连接测试失败	5120	KLAUD_EV_SIEM_TEST_FAILED	当 SIEM 服务器的自动连接测试失败时，会发生此类事件。	90 天
证书已删除	4134	KLSRV_CERTIFICATE_REMOVED	当管理员删除了移动设备管理的任何类型的证书（通用、邮件、VPN）时，会发生此类事件。 删除证书后，通过此证书连接的移动设备将无法连接到管理服务器。 在调查与移动设备管理相关的故障时，此事件可能会有所帮助。	90 天
证书已被请求	4133	KLSRV_CERTIFICATE_REQUESTED	当自动重新颁发移动设备管理证书失败时，将发生此类事件。 以下是事件的可能原因和对事件的适当响应： • 对禁用了"**如果可能，自动重新发布证书**"选项的证书启动自动重新发布。这可能是由于在证书创建过程中发生的错误所致。可能需要手动重新颁发证书。 • 如果使用与公钥基础结构的集成，则原因可能是用于与 PKI 集成和用于颁发证书的账户缺少 SAM-Account-Name 属性。查看账户属性。	90 天
设备名称冲突	4102	KLSRV_EVENT_HOSTS_CONFLICT	当管理服务器将两台或更多受管理设备视为单台设备时，会发生此类事件。 在受管理设备上使用克隆的硬盘驱动器进行软件部署，而没有将参考设备上的网络代理切换到专用磁盘克隆模式时，通常会发生这种情况。 为避免此问题，请在克隆此设备的硬盘驱动器之前将参考设备上的网络代理切换到磁盘克隆模式。	90 天
到主管理服务器的连接已中断	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	当与主管理服务器的连接中断时，会发生此类事件。 读取安装了主管理服务器的设备上的操作系统日志，并相应做出响应。	90 天
到从属管理服务器的连接已中断	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	当与从属管理服务器的连接中断时，会发生此类事件。 读取安装了从属管理服务器的设备上的操作系统日志，并相应做出响应。	90 天
设备在网络上已长时间没有活动	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	当受管理设备在一段时间内显示出不活动状态时，会发生此类事件。 这种情况通常发生在受管理设备已解除授权时。 您可以通过以下方式响应事件： • 要从受管理设备列表中手动删除该设备。 指定时间间隔，超过该间隔后，使用 OSMP 控制台创建"**设备在网络上已长时间没有活动**"事件。 • 指定时间间隔，超过该间隔后，使用 OSMP 控制台自动将设备从组中删除。	90 天
设备状态是"警告"	4114	KLSRV_HOST_STATUS_WARNING	当受管理设备被分配*警告*状态时，该类型的事件发生。您可以配置设备状态被更改到*警告*的条件。	90 天
将文件下载到设备失败	4165	KLSRV_FILE_DOWNLOAD_FAILED	此类事件会在以下情况下发生： • 您尝试将文件下载到企业容器，但企业容器尚未创建。 • 设备空间不足。 • 从服务器下载文件信息失败。 • 文件内容无法从服务器下载。 • 无法在设备上创建该文件夹。 • 个人设备上缺少文件访问权限。 • 企业容器中缺少文件访问权限。	90 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
发送 FCM 消息到 FCM 服务器失败	4140	KLSRV_GCM_GENERAL_ERROR	使用 Google Firebase Cloud Messaging HTTP 协议时，由于管理服务器端发生意外错误，而发生此类事件。 读取事件描述中的详细信息，并相应做出响应。 如果您自己找不到问题的解决方案，建议与 Kaspersky 技术支持联系。	90 天
发送 FCM 消息到移动设备失败	4138	KLSRV_GCM_DEVICE_ERROR	当移动设备管理配置为使用 Google Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器无法处理从管理服务器收到的某些请求时，会发生此类事件。这意味着某些受管理移动设备不会收到推送通知。 读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FCM 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Google Firebase 服务文档（参见“下游消息错误响应代码”一章）。	90 天
已检测到频繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	当管理服务器在受管理设备上检测到频繁发生的事件时，会发生这种类型的事件。请参阅以下部分了解详情：阻止频繁事件。	90 天
硬盘几乎已满	4105	KLSRV_NO_SPACE_ON_VOLUMES	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	90 天
发送 FCM 消息到 FCM 服务器时发生 HTTP 错误	4139	KLSRV_GCM_HTTP_ERROR	当移动设备管理配置为使用 Google Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器回复管理服务器请求的 HTTP 代码不是 200（正常）时，会发生此类事件。 以下是事件的可能原因和对事件的适当响应： • FCM 服务器端出现问题。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FCM 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Google Firebase 服务文档（参见“下游消息错误响应代码”一章）。 • 代理服务器端出现问题（如果使用代理服务器）。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。	90 天
已超过授权许可数量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Next XDR Expert 每天检查一次是否超过授权许可数量限制。 当管理服务器发现安装在客户端设备上的卡巴斯基应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量达到了该授权许可覆盖的单元总数的 100% 到 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Next XDR Expert 确定超过授权许可数量限制时生成事件的规则。	90 天
已授权应用程序组之一的安装即将达到限制	4128	KLSRV_INVLICPROD_EXPIRED_SOON	当已授权应用程序组中包含的第三方应用程序的授权许可密钥之一即将过期时，就会发生此类事件。这样一来，其中某一组的安装限额将被调低。 您可以通过以下方式响应事件： • 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。 • 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。	90 天
已注册卡巴斯基应用程序模块的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	当管理服务器为需要批准安装的受管理设备上安装的 Kaspersky 软件注册新更新时，会发生此类事件。 使用 Kaspersky Security Center Web Console 批准或拒绝更新。	90 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
管理服务器数据库空间不足	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理服务器数据库受限制则该类型的事件发生。如果您不纠正情况，管理服务器数据库就将达到其容量且管理服务器将不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应。 • 不限制存储在管理服务器数据库的事件数量 • 降低存储在管理服务器数据库的事件数量 在 DBMS 选项处查看信息。	90 天
超过了数据库中事件数的限制，已开始删除事件	4145	KLSRV_EVP_DB_TRUNCATING	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后开始时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储
超过了数据库中事件数的限制，事件已被删除	4146	KLSRV_EVP_DB_TRUNCATED	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后完成时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改允许存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储

管理服务器信息事件

下表显示了具有“**信息**”重要级别的管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器信息事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
移动设备的管理服务器证书正在更新中	6127	KLSRV_EV_SRV_CERT_RENEWED	当管理服务器证书已续费时会发生该事件。	30 天
审计：命令已发送到设备	4170	KLAUD_EV_COMMAND_SENT	当用户向移动设备发送命令时，会发生此类事件。	30 天
审计：到管理服务器的连接已终止	4151	KLAUD_EV_SERVERDISCONNECT		30 天
审计：到管理服务器的连接已建立	4147	KLAUD_EV_SERVERCONNECT	当用户使用 OSMP 控制台连接到管理服务器时，会发生此类事件。这些事件包括 OSMP 控制台服务器所在设备的 IP 地址。	30 天
审计：加密密钥已导入/导出	5100	KLAUD_EV_DPEKEYSEXPORT	例如，在迁移期间发生此类事件。	30 天
审计：组设置已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	当安全组已被编辑时，会发生此类事件。	30 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
审计：对象已修改	4148	KLAUD_EV_OBJECTMODIFY	该事件追踪以下对象中的更改： • 管理组 • 安全组 • 用户 • 包 • 任务 • 策略 • 服务器 • 虚拟服务器	30 天
审计：对象属性已被修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	该事件追踪以下属性中的更改： • 用户 • 授权许可 • 服务器 • 虚拟服务器	30 天
审计：对象状态已更改	4150	KLAUD_EV_TASK_STATE_CHANGED	例如，当任务以错误失败时会发生该事件。	30 天
审计：到 SIEM 服务器的连接测试成功	5110	KLAUD_EV_SIEM_TEST_SUCCESS	当 SIEM 服务器的测试连接成功时，会发生此类事件。	30 天
审计：用户权限已被修改	4153	KLAUD_EV_OBJECTACLMODIFIED	该事件在用户权限被修改了时发生。	30 天
到主管理服务器的连接已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 天
到从属管理服务器的连接已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	有关详细信息，请参阅下文：创建管理服务器层级：添加从属管理服务器。	30 天
数据库已更新	4144	KLSRV_UPD_BASES_UPDATED	当 将更新下载至管理服务器存储库任务完成数据库更新时，会发生此类事件。	30 天
设备已被自动添加到组	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	当设备根据设备移动规则被分配到某个组时，会发生此类事件。	30 天
设备已被根据规则自动移动	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	当设备根据设备移动规则被移动到某个管理组时，会发生此类事件。	30 天
设备已从组中删除：长时间在网络中不活动	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	当设备因处于非活动状态而被自动从组中删除时，会发生此类事件。	30 天
此移动设备上的 FCM 实例 ID 已被更改	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	当设备上的 Firebase Cloud Messaging 令牌发生变化时，会发生此类事件。 有关 FCM 令牌轮换的信息，请参阅 Firebase 服务文档。	30 天
文件已上传到管理服务器	4162	KLSRV_FILE_UPLOADED	当管理员将文件上传到 **资产管理** → **Mobile** → **Apps & files** → **Files**列表时，会发生此类事件。	30 天
文件已从管理服务器删除	4163	KLSRV_FILE_REMOVED	当管理员从 **资产管理** → **Mobile** → **Apps & files** → **Files**列表中删除文件时，会发生此类事件。	30 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
文件已下载到设备	4164	KLSRV_FILE_DOWNLOADED	此类事件会在以下情况下发生： • 管理员已将在 Web Console 中的 **资产管理** → **Mobile** → **Apps & files** → **Files**列表中的文件下载到管理员工作站。 • 文件已从 **资产管理** → **Mobile** → **Apps & files** → **Files**列表下载到安装了 Kaspersky Endpoint Security for Android 的设备。	30 天
将文件下载到设备失败	4165	KLSRV_FILE_DOWNLOAD_FAILED	此类事件会在以下情况下发生： • 管理员尝试将文件从 Web Console 中的 **资产管理** → **Mobile** → **Apps & files** → **Files**列表下载到管理员工作站时发生错误。 • 将文件从 **资产管理** → **Mobile** → **Apps & files** → **Files**列表下载到安装了 Kaspersky Endpoint Security for Android 的设备时发生错误。	30 天
找到了要发送至卡巴斯基以分析的文件	4131	KLSRV_APS_FILE_APPEARED		30 天
已授权应用程序组之一的安装即将超过限制(已经使用 90% 以上)	4127	KLSRV_INVLICPROD_FILLED	当已授权应用程序组中包含的第三方应用程序安装数量达到授权许可密钥属性中指定的最大允许值的 90% 时，将发生此类事件。 您可以通过以下方式响应事件： • 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。 • 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。	30 天
已检测到新设备	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	当发现新的联网设备时，就会发生此类事件。	30 天
授权许可密钥的 90% 已经使用	4097	KLSRV_EV_LICENSE_CHECK_90	当管理服务器检测到以下两种情况时，会生成此类事件：一是安装在客户端设备上的卡巴斯基应用程序快超过某些授权许可限制；二是单个授权许可所涵盖的当前已使用的授权许可单元数量，超过了该授权许可所涵盖总单元数量的 90%。 即使超出许可限制，客户端设备仍受到保护。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Next XDR Expert 确定超过授权许可数量限制时生成事件的规则。	30 天
移动设备的备用管理服务器证书已创建	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	当管理服务器证书已创建时会发生该事件。	30 天
更新已被成功复制到指定文件夹	4122	KLSRV_UPD_REPL_OK	当**将更新下载至管理服务器存储库**任务完成将文件复制到指定文件夹时，会发生此类事件。	30 天

"**备用证书已创建**"和"**证书续费**"这两类事件，仅当对移动设备和 UEFI 设备的管理服务器证书执行相应操作时，才会由管理服务器自动发布，并显示在管理控制台中。

网络代理事件

该部分包含管网络代理相关事件信息。

网络代理警告事件

下表显示具有“**警告**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理警告事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
KSN 代理已启动。检查 KSN 可用性失败	7718	KSNPROXY_STARTED_CON_CHK_FAILED	当所配置的 KSN 代理连接的测试连接失败时，会发生此类事件。	30 天
发生了安全问题	549	GNRL_EV_APP_INCIDENT_OCCURED	在设备上发现事故时，就会发生此类事件。例如，当设备磁盘空间不足时会发生此类事件。	30 天
发现 sudoers 文件与参考值不匹配	7724	KLNAG_EV_SUDOER_DIFFERENT	当 sudoers 文件和参考文件不匹配时，就会发生此类事件。	30 天
第三方软件更新安装已延时	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	例如，当第三方更新安装的 EULA 被拒绝时，会发生此类事件。	30 天
第三方软件更新安装已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	下载跟踪文件并查看 KLRI_PATCH_RES_DESC 字段值以了解详细信息。	30 天
用户管理：警告	7722	KLNAG_EV_USR_MNG_WRN	一般警告事件。	30 天
在安装软件模块更新期间返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	下载跟踪文件并查看 KLRI_PATCH_RES_DESC 字段值以了解详细信息。	30 天

网络代理信息事件

下表显示具有“**信息**”严重级别的网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理信息事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
应用程序已安装	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
应用程序已卸载	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已收到 Web 服务器 HTTPS 端口的证书	—	WEB_SERVER_CERTIFICATE_RENEWED	30 天
设备已被授权	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
已检测到新设备	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
设备已被删除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
软件模块更新安装已启动	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
KSN 代理已启动。KSN 可用性检查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天
已安装监控的应用程序	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已卸载监控的应用程序	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已添加新设备	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
根证书已安装	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 天

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
根证书已删除	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 天
Sudoers 文件成功恢复为参考值	7725	KLNAG_EV_SUDOER_RESTORED	30 天
已安装第三方应用程序	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
第三方软件更新已成功安装	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
第三方软件更新安装已开始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
软件模块更新已成功安装	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
用户管理：信息	7721	KLNAG_EV_USR_MNG_INF	30 天
已在主机上启动 Web 服务器	—	WEB_SERVER_STARTED	30 天
已在主机上停止 Web 服务器	—	WEB_SERVER_STOPPED	30 天
Windows 桌面共享：应用程序已启动	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 桌面共享：文件已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 桌面共享：文件已读取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 桌面共享：已启动	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 桌面共享：已停止	7716	KLUSRLOG_EV_WDS_END	30 天

使用事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

在 OSMP 控制台界面中，您可以根据可用的设置，创建并查看用户自定义的事件分类。

在 OSMP 控制台的“**监控**”区域中单击“**事件分类**”，即可使用事件分类。

默认下，事件分类包含 7 天内的信息。

Kaspersky Next XDR Expert 提供一组默认（预定义）事件分类：

- 不同重要级别的事件：
  - **严重事件**
  - **功能失败**
  - **警告**
  - **信息消息**
- **用户请求**（受管理应用程序事件）

- **最近事件**（上周）
- **审计事件**。

在 Kaspersky Next XDR Expert 中，显示与 OSMP 控制台中的服务操作相关的审计事件。这些事件取决于卡巴斯基专家的行动。这些事件的示例如下：登录管理服务器；更改管理服务器端口；备份管理服务器数据库；创建、修改和删除用户账户。

您也可以创建和配置附加用户定义分类。在用户定义分类中，您可以根据设备属性（设备名称、IP 范围和管理组）、根据事件类型和严重级别、根据应用程序和组件名称、以及根据时间间隔来筛选事件。也可以包含任务结果到搜索范围。您也可以单一搜索字段，可以输入一个词或几个词。所有属性（例如事件名称、描述、组件名称）中包含任意所输入词的事件被显示。

对于预定义和用户定义的分类，您可以限制显示事件的数量或者要搜索的记录的数量。这两个选项都会影响 Kaspersky Next XDR Expert 显示事件所需的时间。数据库越大，过程越耗时。

您可以执行以下操作：

- 编辑事件分类的属性
- 生成事件分类
- 查看事件分类的详细信息
- 删除事件分类
- 从管理服务器数据库中删除事件

创建事件分类

要创建事件分类，请执行以下操作：

1. 在主菜单中，转到“**监控**”→“**事件分类**”。
2. 单击**添加**。
3. 在打开的“**新事件分类**”窗口中，指定新事件分类的设置。在窗口中重复此操作。
4. 单击“**保存**”保存更改。
   确认窗口打开。
5. 要查看事件分类结果，请保持“**转到分类结果**”复选框为选中状态。
6. 单击“**保存**”确认事件分类创建。

如果将“**转到分类结果**”复选框保持选中状态，将显示事件分类结果。否则，新事件分类出现在事件分类列表。

编辑事件分类

要编辑事件分类：

1. 在主菜单中，转到“**监控**” → “**事件分类**”。
2. 选中您要编辑的事件分类旁边的复选框。
3. 单击“**属性**”按钮。
   事件分类设置窗口打开。
4. 编辑事件分类属性。

   > 对于预定义的事件分类，只能编辑以下选项卡上的属性：**常规**（除了分类名称）、**时间**和**访问权限**。

   对于用户定义分类，您可以编辑所有属性。
5. 单击“**保存**”保存更改。

编辑的事件分类显示在列表。

查看事件分类列表

要查看事件分类：

1. 在主菜单中，转到“**监控**”→ “**事件分类**”。
2. 选择您要启动的事件分类旁边的复选框。
3. 执行以下操作之一：
   - 如果您要在事件分类结果中配置排序，做以下：
     a. 单击**重新配置排序并开始**按钮。
     b. 在显示的“**重新配置事件分类排序**”窗口中，指定排序设置。
     c. 单击分类的名称。
   - 否则，如果想要以事件在管理服务器上的顺序查看事件列表，请单击分类名称。

事件分类结果被显示。

导出事件分类

Open Single Management Platform 允许您将事件选择及其设置保存到 KLO 文件。您可以使用此 KLO 文件将保存的事件分类导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

请注意，您只能导出用户定义的事件分类。Open Single Management Platform 默认集中的事件分类（预定义分类）无法保存到文件。

要导出事件分类：

1. 在主菜单中，转到“**监控**”→“**事件分类**”。
2. 选中您要导出的事件分类旁边的复选框。
   您不能同时导出多个事件分类。如果您选择了多个分类，**导出**按钮将被禁用。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定事件分类文件名和路径，然后单击**保存**按钮。
   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则事件分类文件会自动保存在“**下载**”文件夹。

导入事件分类

Open Single Management Platform 支持从 KLO 文件导入事件分类。KLO 文件包含导出的事件分类及其设置。

要导入事件分类：

1. 在主菜单中，转到**监控→ 事件分类**。
2. 单击“**导入**”按钮，然后选择要导入的事件分类文件。
3. 在打开的窗口中，指定 KLO 文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个事件分类文件。
   事件分类处理开始。

出现包含导入结果的通知。如果事件分类导入成功，您可以单击**查看导入详细信息**链接来查看事件分类属性。

成功导入后，事件分类会显示在分类列表中。事件分类的设置也会被导入。

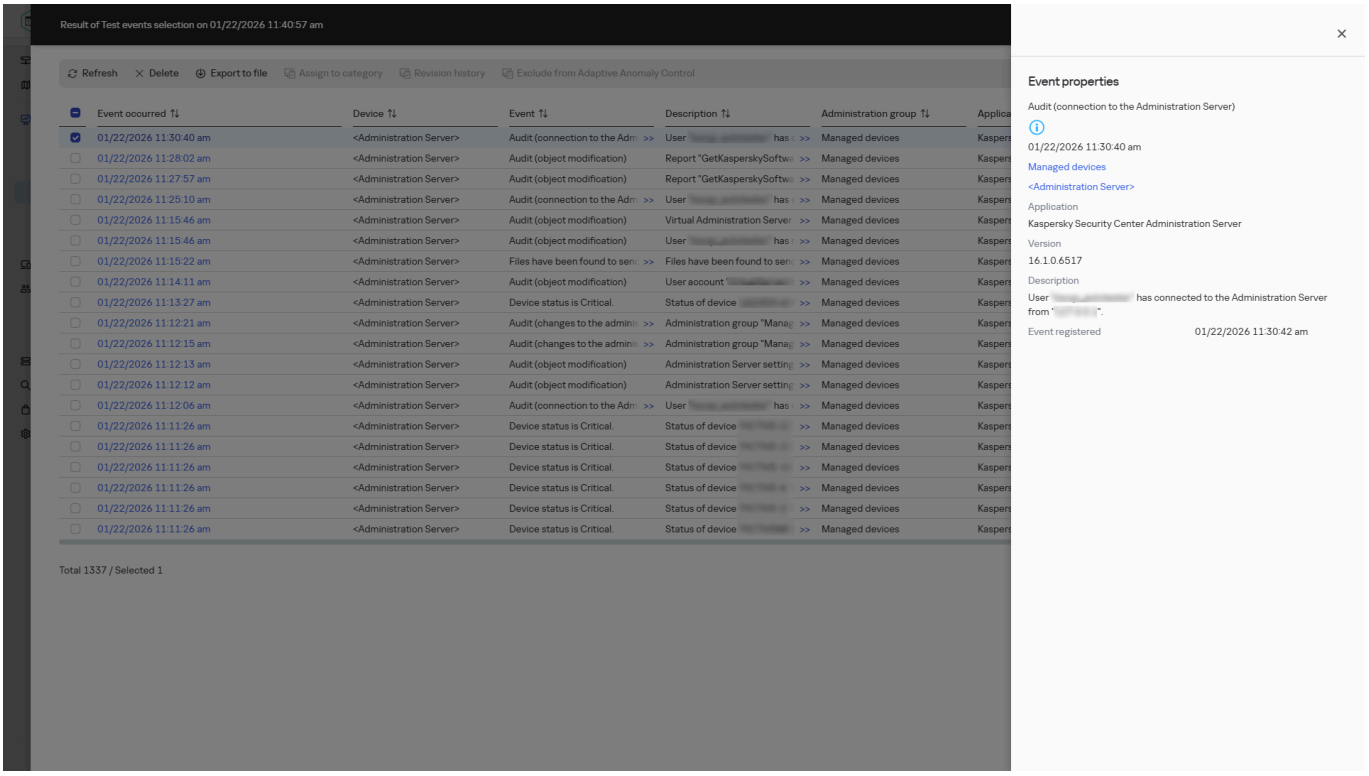
如果新导入的事件分类与现有事件分类有相同的名称，则导入的分类在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

查看事件详细信息区域

要查看事件详情：

1. 启动事件分类。
2. 单击所需事件的时间。

   “**事件属性**”窗口打开。



“事件属性”窗口

3. 在显示的窗口中，您可以做以下：
   - 查看关于所选事件的信息
   - 转到发生事件的设备
   - 转到包含发生事件的设备的管理组
   - 对于任务相关事件，转到任务属性

导出事件到文件

Open Single Management Platform 可让您将事件分类中的事件保存到 TXT 文件。

要导出事件到文件：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
   您还可以选择多个事件或整个事件分类。
3. 单击“**导出到文件**”按钮。

所选事件被导出到 TXT 文件。

从事件查看对象历史

从创建或修改支持修订管理的对象的事件，您可以切换到对象的修订历史。

要从事件查看对象历史：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
3. 单击**修订历史**按钮。

对象修订历史被打开。

删除事件

要从事件分类中删除事件：

1. 启动事件分类。
2. 选择事件：
   - 如果要删除一个或多个事件，请选中其旁边的复选框。
   - 若要删除当前页面上的所有事件，请选中事件列表上方的复选框，然后单击**在当前页面上全选**选项。
   - 如果要删除选定区域中的所有事件，请选中事件列表上方的复选框，然后单击**全部选择**选项。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击**删除**。

若要从设备事件列表中删除事件：

1. 打开设备列表。
   - 对于受管理设备：**资产管理→资产(设备)**。
   - 对于未分配的设备：**资产管理→未分配的设备**。
2. 在设备列表中，单击所需设备名称的链接，然后前往**事件**选项卡。
3. 选择事件：
   - 如果要删除一个或多个事件，请选中其旁边的复选框。
   - 若要删除当前页面上的所有事件，请选中事件列表上方的复选框，然后单击**在当前页面上全选**选项。
   - 如果要删除选定区域中的所有事件，请选中事件列表上方的复选框，然后单击**全部选择**选项。
4. 单击**删除**，然后确认操作。
5. 在打开的窗口中，单击**删除**。

   所选事件被删除且无法恢复。

删除事件分类

> 您仅可以删除用户定义的事件分类。预定义事件分类无法被删除。

要删除一个或几个事件分类：

1. 在主菜单中，转到“**监控**” → “**事件分类**”。
2. 选择您要删除的事件分类旁边的复选框。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**确定**”。

   事件分类被删除。

设置事件存储期限

Kaspersky Next XDR Expert 允许您接收有关管理服务器和受管理设备上安装的 Kaspersky 应用程序运行期间所发生事件的信息。事件信息保存在管理服务器数据库。您可能需要将某些事件存储比默认值指定的时间更长或更短的时间。您可以更改事件存储期限的默认设置。

如果您无意将某些事件存储在管理服务器的数据库中，则可以在管理服务器策略和卡巴斯基应用程序策略或在管理服务器属性（仅对于管理服务器事件）中禁用相应设置。这将降低数据库中的事件类型数量。

事件的存储期限越长，数据库达到最大值速度越快。但是，事件的存储期限越长，执行监控和报告任务的时间就越长。

要为管理服务器中的事件设置存储期限：

1. 在主菜单中，转到“ **资产管理**” → “**策略**“。
2. 单击所需策略的名称。

   您可以选择受管理卡巴斯基应用程序、网络代理或管理服务器的策略。对于管理服务器，您还可以通过单击管理服务器名称来配置事件的存储期限。
3. 选择**事件配置**选项卡。

   将显示与“**严重**”区域有关的事件类型列表。如果需要，您可以移动到**功能失败**、**警告**或**信息**部分。
4. 在右侧面板中的事件类型列表中，单击您要更改其存储期限的事件的链接。

   在打开的窗口的“**事件注册**”区域中，启用“**存储在管理服务器数据库上(天)**”切换开关按钮。
5. 在该开关按钮下面的编辑框中，输入存储事件的天数。
6. 如果您不希望在管理服务器数据库中存储事件，请禁用“**存储在管理服务器数据库上(天)**”选项。

   如果您在管理服务器属性窗口中配置管理服务器事件，并且在管理服务器策略中锁定了事件设置，则无法重新定义事件的存储期限值。
7. 单击**确定**，然后在右侧窗格关闭后，单击**保存**按钮。

   策略的属性窗口关闭。

从现在开始，当管理服务器接收并存储选定类型的事件时，它们将具有更改的存储期限。管理服务器不会更改以前接收的事件的存储期限。

阻止频繁事件

本部分提供有关管理频繁事件阻止和移除阻止频繁事件的信息。

关于阻止频繁事件

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

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

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

- 如果要防止覆盖数据库，可以继续阻止接收此类事件。
- 例如，如果要查找将频繁事件发送到管理服务器的原因，可以解除阻止频繁事件并继续接收此类事件。
- 如果要继续接收频繁事件直到它们被再次阻止，可以将它们从频繁事件的阻止中移除。

管理频繁事件阻止

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

要管理对频繁事件的阻止：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**阻止频繁事件**”区域。
3. 在“**阻止频繁事件**”区域中：
   - 如果要解除阻止接收频繁事件：
     a. 选择要解除阻止的频繁事件，然后单击“**排除**”按钮。
     b. 单击“**保存**”按钮。
   - 如果要阻止接收频繁事件：
     a. 选择要阻止的频繁事件，然后单击“**阻止**”按钮。
     b. 单击“**保存**”按钮。

管理服务器将接收未阻止的频繁事件，并且不接收被阻止的频繁事件。

移除对频繁事件的阻止

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

要移除对频繁事件的阻止：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**阻止频繁事件**”区域。
3. 在“**阻止频繁事件**”区域中，选择要为其移除阻止的频繁事件类型。
4. 单击“**移除阻止**”按钮。

该频繁事件将从频繁事件列表中移除。管理服务器将接收此类事件。

在管理服务器上的事件处理和存储

关于应用程序和受管理设备运行过程中发生的事件的信息保存在管理服务器数据库中。每个事件都归属于特定类型和严重级别（*严重事件*、*功能失败*、*警告*或*信息*）。基于事件发生的条件，应用程序可以分配不同的严重级别到相同类型的事件。

您可以在管理服务器属性窗口的**事件配置**部分查看分配给事件的类型和严重级别。在**事件配置**部分，您也可以配置管理服务器对每个事件的处理：

- 在管理服务器、设备 OS 事件日志和管理服务器计算机 OS 事件日志中注册事件。
- 通知管理员事件的方法（例如，SMS 或者邮件消息）。

在管理服务器属性窗口的**事件存储库**部分，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入操作系统日志。新事件被列队，然后在删除操作后被保存到数据库。默认情况下，事件队列限制为 20,000 个事件。您可以通过编辑 KLEVP_MAX_POSTPONED_CNT 标记值来自定义队列限制。

回溯扫描

在正常模式下，关联器仅实时处理来自收集器的事件。如果您需要调试关联规则或分析数据，**回溯扫描**允许您将关联规则应用于历史事件。

要测试关联规则，您无需实时重放事故。您可以改为在**回溯扫描**模式下运行关联规则，以处理包含所需事故的现有事件。

您可以使用搜索查询来定义要进行回溯扫描的事件列表，还可以指定搜索周期和要搜索事件的存储位置。您可以配置任务，以便在事件回溯扫描期间生成警报并应用响应规则。

要运行回溯扫描：

1. 在解决方案网页界面的**监控 → 威胁搜索**部分，创建所需的事件分类：
   - 选择存储。

     运行回溯扫描前，请确保已选择正确的集群和空间。

- 使用构造函数或搜索查询配置搜索表达式。

  运行回溯扫描前，请确保在SQL查询字段中指定了正确的表达式。

- 根据需要设置时间段。

  运行回溯扫描前，请确保在时间段字段中选择了正确的时间段。

2. 在 ··· 下拉列表中，选择**回溯扫描**。
   回溯扫描窗口将打开。

3. 在"**关联器**"下拉列表中，选择要将选定事件发送到的关联器。

   运行回溯扫描前，请检查SQL查询找到的事件数量。此信息显示在**显示时间线→总计**下。如果SQL查询中未指定**LIMIT**，则会将该时间段内的所有事件发送到关联器，从而延长任务完成时间。如果设置了相对时间段（例如，*now-1h*），则在回溯扫描开始时可能会产生新事件；这些事件也会发送到关联器。如果关联器安装在除主租户（Main、RootTenant）之外的租户中，则它只能接收自己租户的事件。

4. 在**关联规则**下拉列表中，选择处理事件时必须使用的关联规则。如果在此步骤中未选择任何规则，则将应用所有关联规则执行扫描。

5. 在**EPS 上限**字段中，指定回溯扫描要使用的最大EPS值。指定值用于设置执行回溯扫描时的最大负载。默认设置为0，这意味着不会对回溯扫描应用EPS限制。

   不允许出现负的EPS值。

6. 若要在处理事件时执行响应，请打开**执行响应**切换开关。

7. 若要在事件处理期间生成警报，请打开**创建警报**切换开关。

8. 单击"**创建任务**"按钮。

   回溯扫描任务随即创建并显示在**任务管理器**部分。

要查看扫描结果，请在 KUMA Web 界面的**任务管理器**部分中，单击您创建的任务，然后在下拉列表中选择**转至事件**。

回溯扫描结果仅显示生成的关联事件。
回溯扫描结果中，时间段的开始时间显示为<任务创建的日期和时间>，时间段的结束时间显示为<任务创建的日期和时间+一小时>（如果自任务创建以来尚未经过一小时，则显示当前时间）。
如果回溯扫描结果中没有任何事件，则表示发送给关联器的SQL查询结果中的事件未触发关联器。

这将打开一个新的浏览器选项卡，其中包含回溯扫描期间处理的事件，以及事件处理期间创建的聚合事件和关联事件。回溯扫描生成的关联事件有一个额外的ReplayID字段，用于存储回溯扫描的唯一ID。分析员可以从任务的上下文菜单中重新启动回溯扫描。新的关联事件将具有不同的ReplayID。

根据您的浏览器设置，系统可能会提示您确认打开回溯扫描结果选项卡。有关更多详细信息，请参阅您使用的浏览器的说明文档。

作为回溯扫描的一部分处理的事件不会使用来自CyberTrace或 Kaspersky 威胁情报门户的数据进行扩充。

回溯扫描期间会更新活动列表。

无法基于包含算术表达式或仅包含聚合字段的SQL查询执行回溯扫描。只有在查询处理完成后，您才能对使用分组SQL查询获得的事件组进行回溯扫描。为此，首先运行带有数据分组的SQL查询并获取事件组列表，然后对其中一个组运行回溯扫描。

通知和设备状态

本部分包含有关如何查看通知、配置通知传送、使用设备状态和启用更改设备状态的信息。

使用通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

根据选择的通知方法，有以下类型的通知可用：

- 屏幕通知
- 通过 SMS 通知
- 通过电子邮件通知
- 通过可执行文件或脚本通知

屏幕通知

屏幕通知提醒您按照重要级别分组的事件(*严重*、*警告*和*信息*)。

屏幕通知可以有两种状态之一：

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

默认下，通知列表包含*未查看*状态的通知。

您可以通过查看屏幕通知和实时响应它们来监控您的组织网络。

通过电子邮件、SMS 和可执行文件或脚本通知

Kaspersky Next XDR Expert 能够通过发送有关您认为重要的任何事件的通知来监控您组织的网络。对任意事件，您可以配置通过电子邮件、SMS 或运行可执行文件或脚本进行通知。

在通过电子邮件或 SMS 接收通知时，您可以决定您对事件的响应。此响应应该最适合您组织的网络。通过运行可执行文件或脚本，您预定义对事件的响应。您也可以认为运行可执行文件或脚本是对事件的首选响应。可执行文件运行后，您可以采取其他步骤响应事件。

查看屏幕通知

您可以通过三种方式查看屏幕上的通知：

- 在“**监控**”→“**通知**”区域中。这里，您可以查看预定义类别的通知。
- 您可以打开单独的窗口。此种情况下，您可以标记通知为已查看。
- 在“**监控**”→“**控制板**”区域上的“**所选严重级别的通知**”小组件中。在小组件中，可以仅查看处于“*严重*”和“*警告*”重要级别的事件通知。

您可以执行操作，例如，可以响应事件。

要查看预定义类别的通知：

1. 在主菜单中，转到“**监控**”→ “**通知**”。
   在左侧面板选择“**所有通知**”类别，右侧面板会显示所有通知。
2. 在左侧面板，选择类别之一：
   - **部署**
   - **设备**
   - **保护**
   - **更新**
     此通知包括有关可供下载的卡巴斯基应用程序的通知、有关已下载的反病毒数据库更新的通知，以及有关网络代理更新后需要重新启动的设备（如有）的通知。
   - **漏洞利用防御**
   - **管理服务器**。
     这仅包括与管理服务器相关的事件。

- **有用链接**。

  其中包括卡巴斯基资源的链接，例如卡巴斯基技术支持、卡巴斯基论坛、授权许可续费页面或卡巴斯基 IT 百科全书。

所选类别的通知列表被显示。列表包含以下：

- 与通知主题相关的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
- “通知”重要级别。显示以下重要级别的通知：**关键通知** ()、**警告通知** ()、**信息通知**。列表中的通知按重要级别分组。
- **通知**。这包含通知描述。
- **操作**。这包含建议您执行的快速操作链接。例如，通知单击该链接，您可以转到存储库并安装安全应用程序到设备，或查看设备列表或事件列表。您为通知执行推荐操作之后，该通知被分配*已查看*状态。
- **注册的状态**。这包含从通知被注册到管理服务器到现在为止过去的天数或小时数。

要在单独的窗口中按重要级别查看屏幕通知：

1. 在 OSMP 控制台的右上角，单击旗帜图标 ()。

   如果旗帜图标具有红点，表示有未查看的通知。

   列出通知的窗口被打开。默认情况下，将选择“**所有通知**”选项卡，并且通知按重要级别分组：“*严重*”、“*警告*”和“*信息*”。

2. 选择“**系统**”选项卡。

   将显示“*严重*”() 和“*警告*”() 重要级别通知的列表。通知列表包含以下：

   - 颜色标记。严重通知标记为红色。警告通知标记为黄色。
   - 指示通知主题的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
   - 通知描述。
   - 复选标记图标。旗帜图标是灰色的，如果通知被分配了*未查看*状态。当您选择灰色旗帜图标并分配*已查看*状态到通知时，图标更改颜色到白色。
   - 推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
   - 从通知被注册到管理服务器到现在为止过去的天数。

3. 选择“**更多**”选项卡。

   将显示“*信息*”重要级别通知的列表。

   该列表的组织与“**系统**”选项卡上的列表相同（请参见上面说明）。仅有的不同是没有颜色标记。

您可以通过注册在管理服务器上的日期间隔来筛选通知。使用“**显示过滤器**”复选框来管理筛选器。

要在部件上查看屏幕通知：

1. 在“**控制板**”区域中，选择“**添加或还原小部件**”。
2. 在打开的窗口中，单击“**其他**”类别，选择“**所选严重级别的通知**”小组件，然后单击“添加”。

   该小组件现在显示在“**控制板**”选项卡上。默认情况下，小组件上显示“*严重*”重要级别的通知。

   您可以单击小组件上的“**设置**”按钮并更改小组件设置以查看“*警告*”重要级别的通知。或者，您可以添加另一个小组件：**所选严重级别的通知**，带有“*警告*”重要级别。

   部件上的通知列表由尺寸限制并包含两个通知。这两个通知是关于最近事件的。

部件上的通知列表包含以下：

- 与通知主题相关的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
- 通知描述和推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
- 从通知被注册到管理服务器到现在为止过去的天数或小时数。
- 到其他通知的链接。单击该链接后，您将转到“**监控**”区域的“**通知**”区域中的通知视图。

关于设备状态

Kaspersky Next XDR Expert 会为每台受管理设备分配一个状态。具体状态取决于是否满足用户定义的条件。在某些情况下，为设备分配状态时，Kaspersky Next XDR Expert 会考虑该设备在网络上的可见性标志（见下表）。如果 Kaspersky Next XDR Expert 在两小时内未在网络上发现某台设备，则该设备的可见性标志将设置为“*不可见*”。

状态如下：

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

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

分配状态到设备的条件

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

条件	条件描述	可用值
需要重启后的时间	设备在网络上可见，但应用程序要求重启的时间已超过指定时间间隔。	超过 0 分钟。
重启原因	设备在网络上可见，但由于所选原因之一，应用程序需要重新启动设备。	• 未知原因 • 应用程序在重启前不会运行 • 需要重启以完成更新；应用程序正在运行 • 需要重启以启动更新 • 需要重启以完成扫描或清除 • 需要重启以完成远程安装/卸载 • 即将完成磁盘的数据加密
安装了不兼容的应用程序	设备在网络中可见，但通过网络代理执行的软件清查在设备上检测到了不兼容的应用程序。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到软件漏洞	设备在网络中可见且网络代理已安装到设备，但“*查找漏洞和所需更新*”任务在设备应用程序中检测到指定严重级别的漏洞。	• 严重 • 高。 • 中。 • 如果漏洞无法被修复则忽略。 • 如果为安装分配了更新则忽略。
授权许可已过期	设备在网络中可见，但授权许可已过期。	• 开关按钮被关闭。 • 开关按钮被开启。
授权许可即将过期	设备在网络中可见，但设备上的授权许可即将在指定天数内过期。	少于 0 天。
Windows Update 更新检查已长时间未执行	设备在网络中可见，但“*寻找漏洞和所需更新*”任务在指定时间段内未运行。	超过 1 天。
无效的加密状态	网络代理已安装到设备，但设备加密结果等于指定值。	• 由于用户拒绝未遵从策略(仅对外部设备)。 • 由于错误未遵从策略。 • 应用策略时需要重启。 • 未指定加密策略。 • 不支持。 • 当应用策略时。
移动设备设置不遵从策略	移动设备设置不同于 Kaspersky Endpoint Security for Android 策略中指定的设置。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到未处理的安全问题	设备上发现了一些未处理的安全问题。安全问题可以通过安装在客户端设备上的受管卡巴斯基应用程序自动创建，也可以由管理员手动创建。	• 开关按钮被关闭。 • 开关按钮被开启。
应用程序定义的设备状态	设备状态由受管理应用程序定义。	• 开关按钮被关闭。 • 开关按钮被开启。
设备磁盘空间不足	设备剩余磁盘空间少于指定值或设备无法与管理服务器同步。当设备已与管理服务器成功同步且设备上的剩余空间大于或等于指定值时，*严重*或*警告*状态被更改为*正常*状态。	大于 0 MB。
设备已失去管理	在设备发现过程中，设备在网络中可见，但是超过三次尝试与管理服务器同步都失败了。	• 开关按钮被关闭。 • 开关按钮被开启。
保护已禁用	设备在网络中可见，但设备上的安全应用程序已被禁用长于指定的时间段。 在这种情况下，安全应用程序的状态为*stopped*或*failure*，不同于以下状态：*starting*、*running*或*suspended*。	超过 0 分钟。
安全应用程序没有运行	设备在网络中可见且安全应用程序已安装到设备，但其未在运行。	• 开关按钮被关闭。 • 开关按钮被开启。

Kaspersky Next XDR Expert 允许您设置在满足指定条件时自动切换管理组中设备的状态。当指定条件满足时，客户端设备被分配以下状态之一：*严重*或*警告*。未满足指定条件时，客户端设备被分配“*正常*”状态。

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

当 Kaspersky Next XDR Expert 为设备分配状态时，对于某些条件（请参阅上表中的“条件描述”列），会将可见性标志考虑在内。例如，如果某个受管理设备由于满足“数据库已过期”条件而被分配“*严重*”状态，稍后为设备设置了可见性标志，则该设备被分配“*正常*”状态。

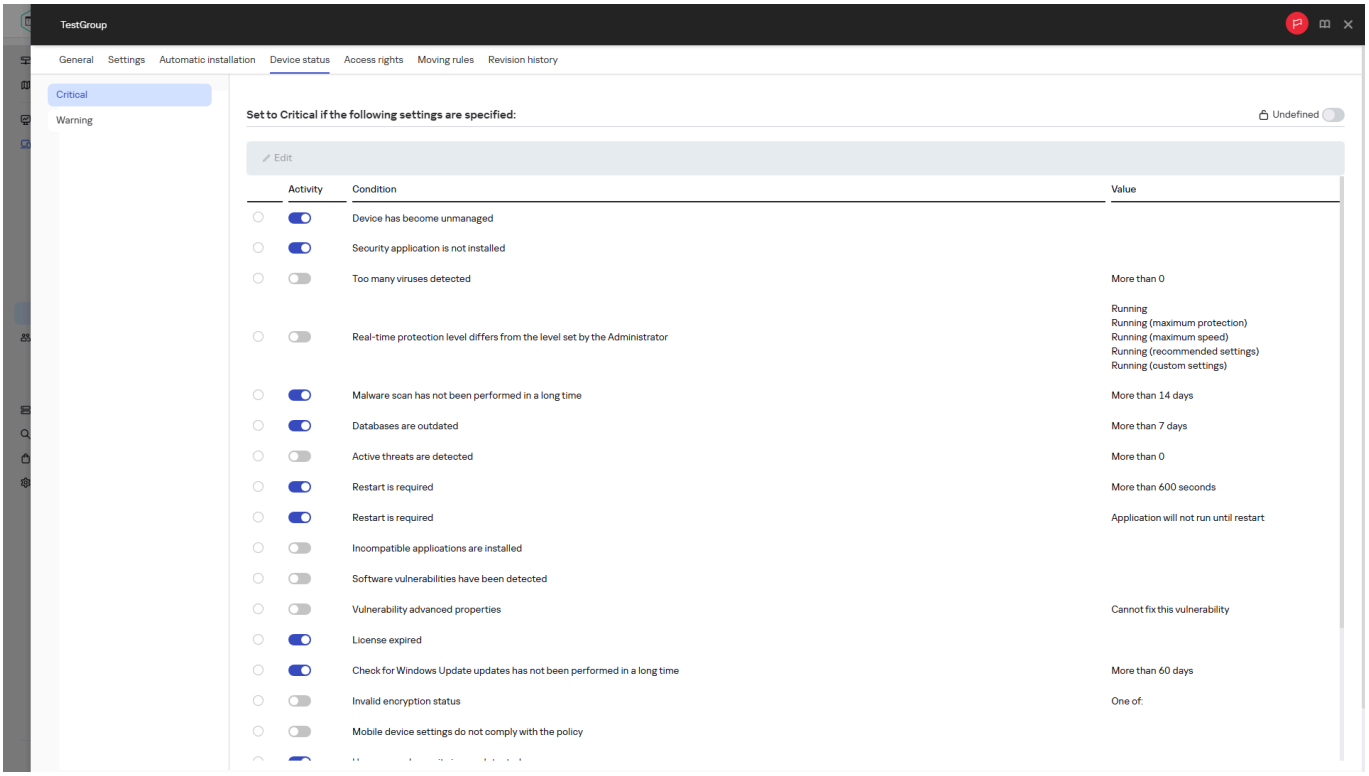
配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 在主菜单中，转到“**资产管理**”→ “**组层级**”。
2. 通过以下方式之一，转到要更改设备状态的管理组的属性：
   - 单击管理组的名称。
   - 单击页面顶部的“**显示层级**”按钮。在打开的导航窗格中，将鼠标光标悬停在所需组的名称上，然后单击设置图标 (⚙)。

   管理组属性窗口将开启。
3. 在属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**严重**”。
5. 在右侧窗格的“**如果指定了以下设置，则设置为“严重”**”区域中，启用将设备切换为“*严重*”状态的条件。



> 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。
10. 单击“**保存**”保存更改。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 在主菜单中，转到“**资产管理**” → “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**警告**”。
5. 在右侧窗格的“**如果指定了以下设置，则设置为“警告”**”区域中，启用将设备切换为“*警告*”状态的条件。

> 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。
10. 单击“**保存**”保存更改。

满足指定条件时，受管理设备被分配*警告*状态。

配置通知传送

您可以配置 Kaspersky Next XDR Expert 中发生的事件通知。根据选择的通知方法，有以下类型的通知可用：

- 电子邮件—当发生事件时，Kaspersky Next XDR Expert 会向指定的电子邮件地址发送通知。
- 短信—当发生事件时，Kaspersky Next XDR Expert 会向指定的电话号码发送通知。
- 可执行文件—当事件发生时，可执行文件被运行在管理服务器。

要配置 Kaspersky Next XDR Expert 中发生的事件通知传送：

1. 在主菜单中，单击管理服务器名称。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 单击“**通知**”区域，在右侧窗格中选择所需通知方法的选项卡：

   - **电子邮件**

     “**电子邮件**”选项卡允许您配置通过电子邮件发送的事件通知。

     在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

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

     在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

     如果启用“**使用 DNS MX 查找**”选项，则可以将多个 IP 地址 MX 记录用于同一个 SMTP 服务器 DNS 名称。同一 DNS 名称可能有多个 MX 记录，这些记录具有不同的电子邮件接收优先级。管理服务器将尝试按 MX 记录优先级的升序向 SMTP 服务器发送电子邮件通知。

     如果启用“**使用 DNS MX 查找**”选项但不启用 TLS 设置，建议您将服务器设备上的 DNSSEC 设置用作发送电子邮件通知的额外保护措施。

     如果启用“**使用 ESMTP 身份验证**”选项，则可以在“**用户名**”和“**密码**”字段中指定 ESMTP 身份验证设置。默认情况下，该选项被禁用，ESMTP 身份验证设置不可用。

     您可以指定 SMTP 服务器连接的 TLS 设置：

     - **不使用 TLS**

     如果要禁用电子邮件加密，则可以选择此选项。

     - **如果 SMTP 服务器支持则使用 TLS**

     如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

     - **始终使用 TLS，检查服务器证书的有效性**

     如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

     建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以单击“**指定证书**”链接来指定用于 TLS 连接的证书：

- 浏览 SMTP 服务器证书文件：

您可以接收含有受信任证书签发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Next XDR Expert 会检查 SMTP 服务器的证书是否也由受信任的证书签发机构签名。如果 SMTP 服务器的证书不是由受信任的证书签发机构签发的，Kaspersky Next XDR Expert 将无法连接到该 SMTP 服务器。

- 浏览客户端证书文件：

您可以使用从任何来源（例如，从任何受信任 CA）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

- X-509 证书：

您必须指定一个证书文件和一个私钥文件。这两个文件彼此独立。文件的加载顺序无关紧要。加载这两个文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

- pkcs12 容器：

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

单击“**发送测试消息**”按钮允许您检查是否正确配置了通知：应用程序发送测试通知到您指定的电子邮件地址。

在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。

在“**主题**”字段中，使用替换参数输入电子邮件主题，例如：`[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`。检测到威胁时的主题行示例：`[KSC-SAMARA-1] [Critical] Threat detected`。您可以置此字段为空。

在“**主题模板**”下拉列表中，选择主题的模板。由所选模板确定的变量自动放置在“**主题**”字段中。您可以选择几个邮件模板构建邮件主题。

在“**发件人邮件地址：如果未指定该设置，收件人地址将被使用。 警告：我们不建议您使用虚假邮件地址**”字段中，指定发件人电子邮件地址。如果您将该字段置空，收件人地址被使用。不建议使用虚假邮件地址。

“**通知消息**”字段包含事件发生时应用程序发送的事件信息标准文本。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有更新事件详情的替代参数编辑消息文本。

字段值示例

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

Sender 字符串是可选的。例如，如果您有多个管理服务器，则可以指定通知接收自的管理服务器名称：Sender - KSC-SAMARA-1。

通知文本示例：

```
Sender - KSC-SAMARA-1

Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access: root; Object type: File; File owner: user; Detection certainty: Sure; File: /home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

> 如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接允许您指定应用程序在指定时间段可以发送的最大通知数量。

- SMS

“**SMS**”选项卡允许您配置将各种事件的 SMS 通知传输到手机。SMS 消息通过邮件网关发送。

在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- SMTP 服务器的 DNS 名称

在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

如果启用“**使用 ESMTP 身份验证**”选项，则可以在“**用户名**”和“**密码**”字段中指定 ESMTP 身份验证设置。默认情况下，该选项被禁用，ESMTP 身份验证设置不可用。

您可以指定 SMTP 服务器连接的 TLS 设置：

- **不使用 TLS**

如果要禁用电子邮件加密，则可以选择此选项。

- **如果 SMTP 服务器支持则使用 TLS**

如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

- **始终使用 TLS，检查服务器证书的有效性**

如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以通过单击“**指定证书**”链接来指定 SMTP 服务器证书文件。您可以接收含有受信任证书签发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Next XDR Expert 会检查 SMTP 服务器的证书是否也由受信任的证书签发机构签名。如果 SMTP 服务器的证书不是由受信任的证书签发机构签发的，Kaspersky Next XDR Expert 将无法连接到该 SMTP 服务器。

在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。通知将被传送到指定邮件地址关联的电话号码。

在“**主题**”字段中，指定电子邮件主题。

在“**主题模板**”下拉列表中，选择主题的模板。取决于所选模板的变量放置在“**主题**”字段中。您可以选择几个邮件模板构建邮件主题。

在“**发件人邮件地址：如果未指定该设置，收件人地址将被使用。 警告：我们不建议您使用虚假邮件地址**”字段中，指定发件人电子邮件地址。如果您将该字段置空，收件人地址被使用。不建议使用虚假邮件地址。

在“**SMS 消息收件人电话号码**”字段中，指定短信通知收件人的手机号码。

在“**通知消息**”字段中，指定事件发生时应用程序发送的事件信息文本。该文本可以包含替代参数，例如事件名称、设备名称和域名。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**发送测试消息**”可检查是否正确配置了通知：应用程序发送测试通知到您指定的收件人。

单击“**配置通知限制数**”链接可指定应用程序在指定时间段可以发送的最大通知数量。

- **要运行的可执行文件**

  可执行文件必须包含您希望管理员接收的事件的环境变量。

  在“**当事件发生时要在管理服务器上运行的可执行文件**”字段中指定要运行的文件的文件夹和名称。

  字段值示例：

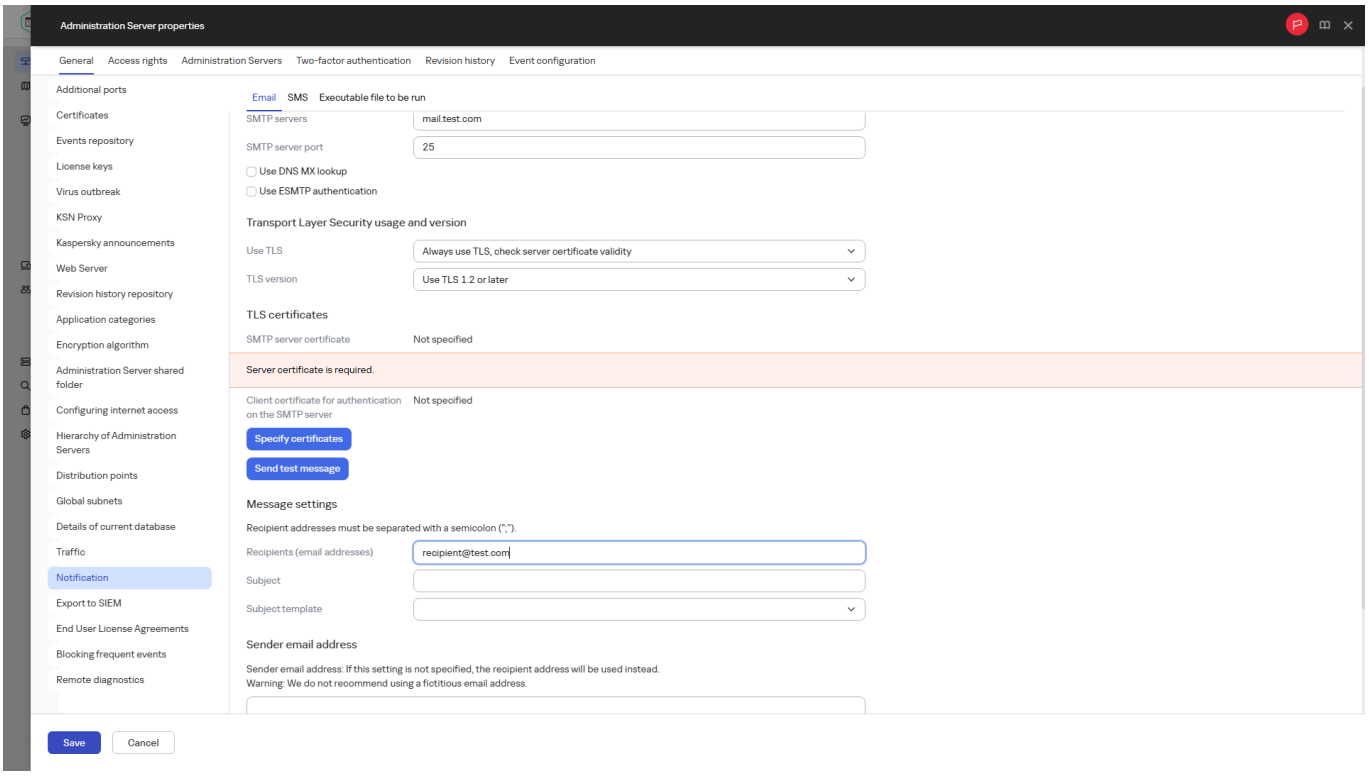
  ```
  /opt/scripts/notifications.sh
  ```

  必须预先指定代表消息中所发送事件信息的替代参数来准备该文件。文件夹和文件必须位于管理服务器上。

  用于测试或调试的脚本示例：

  ```
  #!/usr/bin/env bash
  touch /tmp/ksc_notification.txt
  echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
  ```

  单击“**配置通知限制数**”链接允许您指定应用程序在指定时间段可以发送的最大通知数量。



选择通知方法

3. 在选项卡上，定义通知设置。

4. 点击**保存**以保存更改并关闭管理服务器属性窗口。

   已保存的通知发送设置将应用于 Kaspersky Next XDR Expert 中发生的所有事件。

您可以在管理服务器设置、策略设置或应用程序设置的"**事件配置**"区域中覆盖某些事件的通知传送设置。

测试通知

为了检查事件通知是否可以发送，应用程序将在客户端设备上使用 Eicar 测试病毒检测通知。

要验证事件通知的发送，请执行以下操作：

1. 停止客户端设备上的实时文件系统保护任务，将 EICAR 测试病毒复制到客户端设备。然后，重新启用文件系统的实时保护。

2. 为管理组中的客户端设备或特定设备运行扫描任务，包括带有 EICAR病毒的设备。

   如果扫描任务配置正确，程序会检测到测试病毒。如果通知配置正确，您将收到检测到病毒的通知。

要打开测试病毒检测记录：

1. 在主菜单中，转到“**监控**” → “**事件分类**”。
2. 单击“**最近事件**”选择项名称。
   在打开的窗口中，将显示有关测试病毒的通知。

EICAR 测试病毒不包含任何危害您设备的代码。不过，多数厂商的安全应用程序都将该文件视为病毒。您可以从 EICAR 官方网站 上下载该测试病毒。

用于描述事件的参数和环境变量

配置 Kaspersky Next XDR Expert 事件通知时，您可以使用参数和环境变量来描述事件（请参见下表）。

如果您选择运行可执行文件作为通知方法，请在编写该文件时使用变量。

如果您希望通过电子邮件或短信发送事件通知，则在相应选项卡上配置通知时，还可以在**主题**和**通知消息**字段中指定变量。

用于描述事件的参数和环境变量

替换参数（用于通知）	环境变量（用于脚本）	环境变量说明
%SEVERITY%	$SEVERITY	事件严重级别。可能值： • **信息** • **警告** • **错误** • **严重**
%COMPUTER%	$COMPUTER	发生事件的设备的名称。 设备名称的最大长度为 256 个字符。
%DOMAIN%	$DOMAIN	发生事件的设备的域名称。
%EVENT%	$EVENT	事件类型的名称。 事件类型名称的最大长度为 50 个字符。
%DESCR%	$DESCR	事件描述。 描述的最大长度为 1000 个字符。
%RISE_TIME%	$RISE_TIME	事件创建时间。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	任务名称。 任务名称的最大长度为 100 个字符。
%KL_PRODUCT%	$KL_PRODUCT	应用程序名称。
%KL_VERSION%	$KL_VERSION	应用程序版本号。
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	事件严重编号。可能值： • 1—**信息** • 2—**警告** • 3—Error • 4—**严重**
%HOST_IP%	$HOST_IP	发生事件的设备的 IP 地址。
%HOST_CONN_IP%	$HOST_CONN_IP	发生事件的设备的连接 IP 地址。

监控事件源

本部分提供有关监控事件源的信息。

源状态

在 KUMA 中，您可以监控收集器接收的数据源的状态。一台服务器上可以有多个事件源，并且一个收集器可以接收来自多个源的数据。

您可以使用以下字段集之一配置事件源的自动识别：

- 自定义字段集。您可以按所需顺序指定 1 到 9 个字段。租户 ID 无需单独指定，系统会自动获取。
- **应用默认映射**—DeviceProduct、DeviceHostName、DeviceAddress、DeviceProcessName。字段顺序无法更改。

  如果事件中的以下字段不为空，则可以识别源：DeviceProduct 字段、DeviceAddress 和 / 或 DeviceHostname 字段，以及 TenantID 字段（无需指定 TenantID 字段，其会自动确定）。DeviceProcessName 字段可以为空。如果 DeviceProcessName 字段不为空，并且其他必填字段已填写，则会识别出新的源。

  根据非空事件字段识别事件源

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	租户 ID（自动获取）	
+	+			+	已识别源 1
+		+		+	已识别源 2
+	+	+		+	已识别源 3
+	+		+	+	已识别源 4
+		+	+	+	已识别源 5
+	+	+	+	+	已识别源 6
	+	+		+	未识别源
	+		+	+	未识别源
		+	+	+	未识别源
+			+	+	未识别源

在整个安装过程中，仅应用一个字段集。升级到新的 KUMA 版本时，将应用默认的字段集。仅具有主管理员角色的用户才能配置用于识别事件源的字段集。保存对字段集的更改后，先前识别的事件源将从 KUMA 控制台和数据库中删除。如有必要，您可以恢复使用一组字段来确定默认事件源。为了使编辑后的设置生效，并使 KUMA 能够根据新设置开始识别源，您必须重新启动收集器。

要识别事件源：

1. 在主菜单中，转到“**监控**” → “**源状态**”。
2. 这将打开“**源状态**”窗口；在该窗口中，单击“**设置**”按钮。
3. 这将打开“**事件源检测设置**”窗口；在该窗口中，在“**用于源检测的分组字段**”下拉列表中，选择要用来识别事件源的事件字段。

您可以按所需顺序指定1到9个字段。在自定义配置中，KUMA会识别填充了TenantID字段的源（您无需单独指定此字段，它会自动确定），并且**用于源识别的相同字段**中至少有一个字段已填充。对于数字字段，0被视为空值。如果选择单个数字字段进行源识别，并且该数字字段的值为0，则不会检测到源。

保存修改后的字段集后，将创建一个审计事件，且所有先前识别的源会从KUMA控制台和数据库中删除；分配的策略将被禁用。

4. 如果要返回到用于标识默认事件源的字段列表，请单击"**应用默认映射**"。默认字段顺序无法更改。如果以错误的顺序手动指定字段，则会显示错误并且保存设置按钮将不可用。正确的默认字段序列是DeviceProduct、DeviceHostName、DeviceAddress、DeviceProcessName。使用默认事件集识别事件源的最低配置：DeviceProduct字段、DeviceAddress和/或DeviceHostName字段以及TenantID字段（TenantID会自动确定）中必须有非空值。

5. 单击"**保存**"按钮。

6. 重新启动收集器以应用更改并开始按照指定的字段列表来识别事件源。

源标识已配置。

要查看与事件源关联的事件：

1. 在主菜单中，转到**监控 → "来源状态"**。

   这将打开"**源状态**"窗口。

2. 在"**事件源**"选项卡上，从列表中选择一个事件源。在"**名称**"列中，从所选事件源的下拉列表中选择"**<number>天的事件**"。

   KUMA会将您导航至"**事件**"部分，您可以在其中查看过去5分钟内所选源的事件列表。事件源识别设置中配置的字段值会自动包含在查询中。如有必要，您可以在"**事件**"部分更改查询中的时间段，然后再次单击"**运行查询**"以查看指定时间段的查询数据。

限制

1. 在包含默认字段集的配置中，仅当原始事件包含DeviceProduct字段以及DeviceAddress和/或DeviceHostName字段时，KUMA才会注册事件源。

   如果原始事件不包含DeviceProduct字段以及DeviceAddress和/或DeviceHostName字段，您可以：

   - 在规范化器中配置增强：在规范化器的"**增强**"选项卡上，选择"**事件**"数据类型，指定"**源字段**"设置，对于"**目标字段**"，选择DeviceProduct + DeviceAddress和/或DeviceHostName，然后单击"确定"。

   - 使用增强规则：选择"**事件**"数据源类型，指定"**源字段**"设置，对于"**目标字段**"，选择DeviceProduct + DeviceAddress和/或DeviceHostName，然后单击"**创建**"。创建的增强规则必须在"事件增强"步骤中关联到收集器。

   KUMA将执行增强操作并注册事件源。

2. 如果KUMA收到的事件与标识源的字段值相同，则在满足以下条件的情况下，KUMA会注册不同的源：

   - 必填字段的值相同，但针对这些事件确定的租户不同。

   - 必填字段的值相同，但其中一个事件指定了可选的DeviceProcessName字段。

   - 必填字段的值相同，但这些字段中的数据大小写不同。

如果您希望 KUMA 将此类事件记录在同一源下，则可以在规范化器中进一步配置字段。

源列表在收集器中生成，在 KUMA Core 中合并，并显示在程序 Web 界面的“**事件源列表**”选项卡的“**源状态**”下。数据每分钟更新一次。

传入事件的速率和数量是评估所观察系统状态的重要指标。您可以配置监控策略，以便自动跟踪更改，并在指标达到特定边界值时自动创建通知。监控策略显示在 KUMA 控制台的“**监控**” → “**源状态**”部分中的“**监控策略**”选项卡上。

触发监控策略时，将创建监控事件并包含有关事件源的数据。

事件源列表

事件源显示在“**监控**” → “**源状态**” → “**事件源**”下的表格中。一页最多可显示 250 个来源。您可以通过单击相关参数的列标题并选择“**升序**”或“**降序**”来对表格进行排序。

您可以使用“**搜索**”字段搜索事件源。使用正则表达式 (RE2) 执行搜索。您还可以通过单击相关列的标题并选择要显示的值，按“**状态**”或“**监控策略**”列过滤表格。

如有必要，您可以配置表中数据的更新间隔。可用更新周期：**1 分钟**、**5 分钟**、**15 分钟**、**30 分钟**、**1 小时**。默认值为“**无刷新**”。您可能需要配置更新周期以跟踪对源列表所做的更改。

查看有关事件源的信息

在“**事件源**”选项卡上，有关事件源的信息显示在以下列中：

- “**状态**” – 事件源的状态：
  - 绿色 – 事件接收在已分配监控策略的限制范围内。
  - 红色 – 传入事件的频率或数量超出了至少一个已分配监控策略中定义的界限。
  - 灰色 – 监控策略尚未分配给事件源。

  如果状态为红色，则表示生成了监控类型的事件。监控事件在拥有事件源的租户中生成，并发送到主租户的存储（存储必须已部署在主租户中）。如果您有权访问事件源的租户，但无权访问主租户，您仍然可以在主租户的存储中搜索监控事件；您可访问的租户的监控事件将被显示。您还可以配置要发送到任意电子邮件地址的通知。

  表格可以按状态进行过滤。

- **名称** – 事件源的名称。该名称是根据事件源标识设置中配置的字段值自动生成的。

  将鼠标悬停在事件源表格中的事件源名称上，然后单击铅笔 图标，即可重命名该事件源。名称最多可包含 128 个 Unicode 字符。

- **主机名或 IP 地址** – 如果在事件源标识设置中指定了 DeviceHostName 或 DeviceAddress 字段，则该字段对应事件的来源主机的名称或 IP 地址。

- **监控策略** – 分配给事件源的监控策略列表。

  如果要按应用的监控策略过滤事件源列表，请单击此列的名称，然后选择一个或多个监控策略。如有必要，您可以使用“**搜索**”字段在列表中查找策略。

您可以通过单击源所在行来查看有关分配给事件源的所有监控策略的信息。这将打开一个窗口，显示监控策略的设置以及每个策略对应的源状态。如果为源分配了多个监控策略，则此窗口中源表格中的红色状态可让您识别触发的策略。您还可以查看已启用和已禁用策略，以及禁用的策略何时将再次启用。

- **流** – 从事件源接收事件的频率。如果仅为源分配了 byCount 类型的**监控策略**或不同类型的监控策略，则此值显示为事件数量。如果仅为源分配了 byEPS 类型的**监控策略**，或者未分配任何策略，则此值显示为每秒事件数量。

- **租户** – 拥有从事件源接收的事件的租户。

管理事件源

您可以通过选中表格第一列中的复选框来选择一个或多个事件源。您可以通过选中第一列标题中的复选框并选择“**全选**”或“**在页面中全选**”来一次选择多个事件源以执行组操作。“**全选页面**”选项仅适用于列表中显示的事件源：如果列表中仅显示 1500 个源中的 500 个，则下载、启用或禁用策略或删除事件源的组操作仅适用于所选定的 500 个源。如果要对表中的所有源执行操作，请选择“**全选**”。

如果您选择事件源，则以下按钮可用：

- **启用策略**按钮可用于启用事件源的监控政策。您必须在显示的窗口中选择策略才能应用它们。

- 您可以使用“**禁用策略**”按钮来禁用事件源的监控策略。禁用策略时，您必须选择要禁用该策略的时长：临时禁用或永久禁用。

- “**更新策略**”按钮用于应用为事件源启用的监控策略，或更改已分配的监控策略。策略更新后，任务管理器中会启动一项任务。

  更改分配给事件源的监控策略后，此按钮将变为可用。

- 您可以单击“**移除**”按钮以从表中移除事件源。该源的统计信息也将被移除。如果收集器继续从该源接收数据，该事件源将重新出现在表中，但其旧的统计信息将不予考虑。

  如果您想删除所有事件源，但距离上次刷新表格已过去一段时间，那么在此期间添加的事件源可能不会显示在表格中，但它们仍然会被删除。

  如果您删除了超过 100,000 个应用了筛选或搜索的事件源，则只会删除前 100,000 个事件源。您可以再次选择所有已筛选的事件源并进行删除，然后重复此操作，直到删除所有要删除的事件源。如果未对超过 100,000 个事件源应用任何筛选或搜索，您可以通过使用“**全选**”按钮选择源来进行删除。

- 您可以单击“**CSV**”将所选事件分类的数据下载到 CSV 文件。

  仅当已将监控策略分配给事件源时，才会下载“`Stream`”字段；在这种情况下，下载的文件中会指定从策略中获取的测量单位。如果未分配策略，则“`Stream`”字段为空属于预期行为。

- 您可以单击“**图表**”按钮，为所选事件源绘制过去七天的传入事件图表。您最多可以选择五个事件源。
  .

将事件源信息下载到 CSV 文件

您可以将有关一个或多个事件源以及应用于其中的监控策略的信息下载到 UTF-8 编码的 CSV 文件中。如果将多个监控策略应用于一个源，则在该源的文件中，每个监控策略及其参数都从新行开始。对于应用于源的每个监控策略，以下参数将导出到文件：“**状态**”、“**名称**”、“**监控策略**”、“**下限**”、“**上限**”、“**流**”、“**租户**”。

要将事件源信息下载到 CSV 文件中：

1. 在主菜单中，转到“**监控**” → “**源状态**” → “**事件源**”，通过选中相关源旁边第一列中的复选框来选择表中的一个或多个事件源。

   在表格的左下角，您可以找到所选源的数量以及表格中的源总数。您最多可以选择 150,000 个事件源。

   您可以通过单击第一列标题中的复选框并选择以下选项之一来选择多个事件源：

   - **全选**以选择表格所有页面上的所有事件分类源。如果您已使用搜索功能筛选事件源，这将选择所有符合搜索查询的事件源。
   - 单击“**选择页面全部**”，即可选择当前显示页面上的所有事件源。如果您已使用搜索功能筛选事件源，这将选择当前显示页面上所有符合搜索查询的事件源。

2. 单击表格上方的“**CSV**”按钮。

   > 根据浏览器窗口的大小，“**CSV**”按钮可能位于附加菜单中，您可以通过单击带有三个点的图标 ⋮ 来打开该菜单。

   任务管理器中会创建一个新的事件源导出任务。

3. 转到“**任务管理器**”部分并找到创建的任务。

   文件准备就绪后，任务的“**状态**”列将显示“**已完成**”状态。

4. 单击任务类型名称，然后从下拉列表中选择“**下载**”。

包含事件源信息的 CSV 文件将根据您的浏览器设置下载。默认文件名为 event-source-list.csv。

查看传入事件的动态

您可以通过以下方式之一，检查过去七天从源接收的事件的动态，同时考虑所应用的监控策略：

- 查看单个事件源的图。
- 根据多个（最多五个）源的图绘制图表。

要查看单个事件源的图表，转到“**监控**” → “**源状态**” → “**事件源**”，然后在相关事件源所在的行中单击箭头图标 **›**。传入事件的图显示在源所在行的下方。

图中的数据显示如下：

- 数据显示的是接收事件的日期。最长期限为七天。

  图左上角显示天数，右上角显示数据显示周期。您可以单击“**<number>天的事件**”按钮，以转到“**事件**”部分并查看所选源的事件列表。

- X 轴表示天数，Y 轴表示事件频率 (EPS)。
- 线条分别表示过去七天内每 15 分钟的平均、最大和最小事件数。

  如果要查看特定时间的事件数，请将鼠标悬停在图上的某个点上。系统会显示一个工具提示，其中包含特定日期和时间的平均、最大和最小事件数。

您还可以基于多个事件源的图绘制传入事件图表，例如，如果您需要比较同一类型的事件源的活动（这些事件源的行为应该相似，但实际上却不同），就需要使用该功能。

要基于多个事件源的图绘制图表：

1. 在主菜单中，转到**监控** → **“来源状态”** → **“事件来源”**，通过选中相关来源旁边第一列中的复选框来选择表中的一个或多个事件来源。

   您最多可以同时为 5 个事件源绘制图表。

2. 单击表格上方的“**图表**”按钮。

   > 根据浏览器窗口的大小，**图表**按钮可能位于附加菜单中，您可以通过单击带有三个点⋮的图标来打开该菜单。

   显示的“**图表**”窗格包含所有选定源的传入事件图表，以及一个表格，该表格显示了每个源的当前事件数、最大事件数和平均事件数（基于图表中的数据计算得出）。您可以比较选定源的数据随时间的变化情况。

   图表中的数据显示如下：

   - 数据显示的是接收事件的日期。最长期限为七天。

     图表右上角显示数据显示周期。

   - X 轴表示天数，Y 轴表示事件频率 (EPS)。

   - 图表中的线条表示过去七天内，所选事件源在每 15 分钟时间间隔内的平均入站事件数量。

   您可以将鼠标悬停在图表上，以查看每个源在特定时间的平均事件数。

3. 如有必要，请清除图表下表中您想要隐藏的事件源旁边的复选框。

4. 如果要更详细地显示图表，请单击图表上的两个箭头 ↙↗ 图标以全屏模式打开面板并放大图表。

监控策略

传入事件的速率和数量是系统状态的重要指标。例如，您可以检测到事件过多、过少或根本没有事件。监控策略旨在检测这种情况。在策略中，您可以指定下限阈值、可选的上限阈值以及事件的计数方式：按频率或按总数。

策略必须应用于事件源。您可以将一个或多个监控策略应用于源。应用政策后，您可以在**事件源列表**选项卡上监控源的状态。

用于监控事件源的策略显示在“**监控**” → “**源状态**” → “**监控策略**”下的表格中。您可以通过单击相关设置的列标题对表格进行排序。策略列表的最大大小没有限制。

在**源**列中，您可以单击**显示**按钮以查看应用了该政策的所有事件来源。单击此按钮后，您将进入“**事件源**”选项卡，且源表会按照已选策略完成过滤。

监控策略的算法

监控策略按照以下算法应用于事件源：

1. 事件流在收集器处进行计数。
2. KUMA Core 服务器每 15 秒从收集器获取一次有关流的信息。
3. 获取的数据存储在 KUMA Core 服务器上的 Victoria Metrics 时间序列数据库中，KUMA Core 服务器上的数据存储深度为 15 天。
4. 每分钟清查一次事件源。
5. 每个事件源的流将根据以下规则单独计数：
   - 如果事件源应用了监控策略，则显示的最大事件数将根据当前应用的监控策略在策略指定的时间间隔内计算。

     根据策略类型，事件流的数量将按事件数（对于“**byCount**”策略类型）或每秒事件数（EPS，对于“**byEPS**”策略类型）进行计数。您可以在“**事件源**”选项卡的“**流**”列中查找已应用策略的流计数方式。
   - 如果事件源未应用任何监控策略，则事件流的数量对应于最后一个值。
6. 应用程序每分钟检查一次是否存在必须应用于事件源或根据监控策略计划停止的监控策略。
7. 每分钟根据策略约束检查一次事件流。

如果来自源的事件流超出监控策略中指定的阈值，则有关此信息将以如下方式记录：

- 有关触发监控策略的通知将发送到策略中指定的电子邮件地址。对于每个策略，您还可以配置通知模板。
- 生成类型 `5 (Type=5)` 的流监控信息事件。事件的各字段描述如下表所示。

监控事件的字段

事件字段名称	字段值
ID	事件的唯一 ID。
时间戳	事件时间。
类型	审计事件类型。对于审计事件，该值为“`5`”（监控）。
Name	监控策略的名称。
DeviceProduct	`KUMA`
DeviceCustomString1	通知中“`value`”字段的值。显示触发通知的指标的值。

生成的监控事件将发送到以下资源：

- 主租户的所有存储
- 主租户的所有关联器
- 事件源所在租户的所有关联器

添加监控策略

要添加新监控策略：

1. 在主菜单中，转到“**监控**” → “**源状态**” → “**监控策略**”，然后单击“**添加策略**”并在显示的窗口中配置监控策略：
2. 在“**策略名称**”字段中，输入您正在创建的策略的唯一名称。该名称必须包含 1 到 128 个 Unicode 字符。

   我们建议选择一个能够反映监控策略配置计划的名称。
3. 在“**租户**”下拉列表中，选择要拥有该策略的租户。您选择的租户决定了监控策略可以覆盖的具体事件源。
4. 在“**类型**”字段中，选择以下监控策略类型之一：
   - “**按计数**” — 按特定时间段内的事件数量。
   - “**按 EPS**”统计 — 按特定时间段内每秒事件数量 (EPS) 统计数据。系统会计算整个时间段的平均值。您还可以追踪特定时间段内的峰值。
5. 在“**计数间隔**”字段中，指定监控策略必须考虑监控源数据的时间段。您可以使用右侧的下拉列表选择以分钟、小时或天为单位的值。最大值为 14 天。
6. 如果您选择了“**按 EPS**”的策略类型，请在“**控制间隔（分钟）**”字段中指定控制时间间隔（以分钟为单位）。在此时间间隔内，事件数必须超过阈值才能触发监控策略：
   - 如果在此时间段内，所有检查（每分钟执行一次）发现流超过阈值，则触发监控策略。
   - 如果在此时间段内，其中一项检查（每分钟执行一次）发现流在阈值范围内，则不会触发监控策略，并且检查结果计数将被重置。

   如果您未指定测量频率，则在发现流超过阈值后，监控策略会立即触发。
7. 在“**下限**”和“**上限**”字段中，定义代表正常行为的边界值。超出这些边界值的偏差将触发监控策略、创建警报并转发通知。

   必须设置“**下限**”。
8. 在“**评估间隔**”字段中，指定在将策略应用于事件源时，VMalert 服务向 VictoriaMetrics 查询策略数据的频率。您可以使用右侧的下拉列表选择以分钟、小时或天为单位的值。默认时间间隔为 5 分钟。

   指定评估间隔时，请记住策略时间表。例如，如果您将策略配置为每隔几个小时应用一次，则不建议配置较短的间隔，以避免导致 VictoriaMetrics 负载过重。
9. 如有必要，请在“**发送通知**”字段中，指定必须向其发送 KUMA 监控策略激活通知的电子邮件地址。要添加地址，请在字段中输入该地址，然后按“**Enter**”键或单击“**添加**”按钮。您可以指定多个电子邮件地址。

   要转发通知，必须配置与 SMTP 服务器的连接。
10. 在“**通知模板**”下拉列表中，选择要用于通知的模板。如有必要，请单击“**新建**”按钮开始创建新的通知模板。

    默认情况下，选择基本通知模板。您可以重置模板选择并通过单击 X 图标切换到基本模板。

11. 在“**时间表**”部分，配置您希望将监控策略应用于事件源的频率。默认情况下，每周每天从 00:00 到 23:59 应用该策略。要配置监控策略计划，请执行以下操作：

    - 如果您希望在每周特定日期应用监控策略：

        a. 启用“**按每周星期几配置计划”**切换开关。

        b. 在“**每周星期几**”下拉列表中，选择您希望将策略应用于源的日期。

        如果要清除选择，请单击 X 图标。

        c. 在“**时间**”字段中，指定策略的开始和结束时间，精确到分钟。

        策略适用间隔包含其界限；例如，如果结束时间设置为 23:59，则策略将一直应用到 23:59:59.999。默认间隔为 00:00 至 23:59。开始时间必须早于结束时间。

        d. 如果要添加其他时间段，请单击“**添加期间**”按钮，然后重复步骤“b”和“c”。

        您可以添加任意数量的时间段。

    - 如果要每周在特定日历日期应用监控策略：

        a. 请启用“**按月份中的特定日期配置计划**”切换开关。

        b. 单击“**月份中的日期**”字段，并使用日历选择要将策略应用于源的日期。您可以选择多日或单日的时间段。时间段的开始日期必须早于结束日期。

        日期配置时没有年份值，因此策略将在每年的指定日期应用，直到您删除此时间段。如果要清除选择，请单击 X 图标。

        c. 在“**时间**”字段中，指定策略的开始和结束时间，精确到分钟。

        策略适用间隔包含其界限；例如，如果结束时间设置为 23:59，则策略将一直应用到 23:59:59.999。默认间隔为 00:00 至 23:59。开始时间必须早于结束时间。

        d. 如果要添加其他时间段，请单击“**添加期间**”按钮，然后重复步骤“b”和“c”。

        您可以添加任意数量的时间段。

    如果您同时按星期几和月份应用了计划，则首先应用按月份策略。

12. 单击“**添加**”。

    监控策略将被添加。

编辑监控策略

“**监控**” → “**源状态**” → “**监控策略**”部分显示了已添加的监控策略及您在创建策略时指定的设置。您可以单击某个策略以显示包含其所有设置的侧边栏。如有必要，您可以在此侧边栏中编辑策略设置。

如果已将监控策略应用于事件源，若您编辑了某些策略设置，则可能需要更新该策略以应用更改。每 30 分钟，KUMA 会检查是否有任何监控策略需要更新，如有需要，它会自动运行任务来更新这些监控策略。您也可以通过单击表格顶部的“**更新策略**”按钮手动运行更新任务。一个任务会更新所有需要更新的策略。

仅当某些监控策略需要更新时，“**更新策略**”按钮才会激活。关于政策是否需要更新的信息显示在监控政策表的**策略更新状态**中，状态如下：

- 如果编辑了以下监控策略设置之一，但更改尚未应用于事件源，**则需要更新**：
  - **策略名称**
  - **类型**
  - **下限**
  - **上限**
  - **计数间隔**
  - **控制间隔**
  - **评估间隔**
- 在以下任何情况下，都将显示“**已更新**”：
  - 编辑策略后，应用策略的任务会启动，并会将更改应用于事件源。
  - 您已编辑以下策略设置之一，无需启动更新任务：
    - **发送通知**
    - **通知模板**
    - **计划**

    在这种情况下，已编辑的策略设置会在一分钟后应用于事件源。对**通知模板**设置的更改会立即应用。
  - 修改后的监控策略不会应用于事件源。

上次将策略应用于事件源的日期和时间将显示在“**上次应用策略**”列中。

在策略更新任务运行时，所有用户都无法使用“**更新策略**”按钮。如果其他用户已编辑需要更新的策略设置，则只有在您刷新页面或编辑策略或事件源后，“**更新策略**”按钮才会激活。

应用监控策略

要将监控策略应用于事件源：

1. 在主菜单中，转到“**监控**” → “**源状态**” → “**事件源**”，通过选中相关源旁边第一列中的复选框来选择表中的一个或多个事件源。您可以通过单击第一列标题中的复选框并选择以下选项之一来选择多个事件源：

   - **全选**以选择表格所有页面上的所有事件分类源。如果您已使用搜索功能筛选事件源，这将选择所有符合搜索查询的事件源。
   - 单击“**选择页面全部**”，即可选择当前显示页面上的所有事件源。如果您已使用搜索功能筛选事件源，这将选择当前显示页面上所有符合搜索查询的事件源。

   在表格的左下角，您可以找到所选源的数量以及表格中的源总数。

   选择要应用监控策略的事件源后，工具栏上的“**启用策略**”按钮将变为可用。

2. 单击“**应用策略**”。

3. 这将打开“**应用策略**”窗口。在该窗口中，请选择一个或多个要应用于所选事件源的监控策略。该表仅列出了您可以分配给所选源的监控策略：属于同一租户或共享租户（如果您有权访问）的策略。如果所选事件源不存在共享策略，并且您无权访问共享租户，则策略表为空。

   要选择所有可用的策略，您可以选中第一列标题中的复选框。您还可以按策略名称进行上下文搜索，或通过单击要按其排序的列标题并选择“**升序**”或“**降序**”对表进行排序。

   > 无法对**源**、**时间表**、**策略更新状态**、**上次应用的政策**列进行搜索和排序。

4. 单击“**应用**”。

5. 在源表格中，单击“**更新策略**”以将更改应用于事件更新源。

   监控策略将应用于选定的事件源，这些事件源的状态将变为绿色。应用于源的策略名称将显示在“**监控策略**”列中。同时还会显示一条消息，指示已应用策略的源数量。如果某个事件源触发了监控策略，则该源的新状态将在您手动刷新页面或页面自动刷新后显示。建议配置数据自动刷新周期，以追踪事件源列表中的变化。

如果您选择了超过 100,000 个事件源并对其应用了一个或多个策略，则这些策略将仅应用于尚未应用这些策略的前 100,000 个源。如果您需要将策略应用于其余源，可以执行以下操作之一：

- 再次选择所有源并对其应用策略。
- 按任意参数筛选源表，使其显示的源少于 100,000 个，然后将策略应用于这些源。

重复此操作，直到将策略应用于您需要的所有源。

禁用监控策略

要禁用事件源的监控策略：

1. 在主菜单中，转到**监控 → “源状态” → “事件源”**，通过选中相关源旁边第一列中的复选框来选择表中的一个或多个事件源。

   在表格的左下角，您可以找到所选源的数量以及表格中的源总数。在列表中选择要应用监控策略的事件源后，工具栏上将显示“**禁用策略**”按钮。

   您可以通过单击第一列标题中的复选框并选择以下选项之一来选择多个事件源：

   - **全选**以选择表格所有页面上的所有事件分类源。如果您已使用搜索功能筛选事件源，这将选择所有符合搜索查询的事件源。
   - 单击“**选择页面全部**”，即可选择当前显示页面上的所有事件源。如果您已使用搜索功能筛选事件源，这将选择当前显示页面上所有符合搜索查询的事件源。

2. 单击“**禁用策略**”。

3. 这将打开“**禁用策略**”窗口。在该窗口中，选择要为所选事件源禁用的一个或多个监控策略。该表列出了应用于至少一个所选事件源的所有监控策略。

   要选择所有可用的策略，您可以选中第一列标题中的复选框。您还可以使用上下文搜索或通过单击要排序的列标题并选择“**升序**”或“**降序**”来对策略进行排序。

   无法对**源**、**时间表**、**策略更新状态**、**上次应用的政策**列进行搜索和排序。

4. 在策略表上方的“设置”部分，执行以下操作之一：

   - 如果要暂时中止策略，请选择“**指定时间**”，并指定所选策略在多长时间后重新应用于事件源（以分钟、小时或天为单位）。最大值：
     - 天数：30
     - 小时：743
     - 分钟：44579
   - 如果要永久禁用事件源的选定策略，请选择“**直到手动启用**”。

   默认选择是“**指定时间**”，值设置为“**5 分钟**”。

5. 单击“**禁用**”。

6. 在源表格中，单击“**更新策略**”以将更改应用于事件更新源。

   监控策略将针对选定的事件源禁用，或在指定的时间段内暂停使用。表格中这些源的状态将更改为灰色。将显示一条消息，指示已禁用策略的源的数量。

如果选择了超过 100,000 个事件源并为它们禁用了一个或多个策略，则这些策略仅对前 100,000 个应用了这些策略的源禁用。如果您需要禁用剩余源的策略，可执行以下操作之一：

- 再次选择所有来源并禁用其策略。
- 按任意参数筛选来源表格，使表格显示的来源少于 100,000 个，然后禁用这些源的策略。

重复此操作，直到所有需要的源的策略均已禁用。

基于现有策略添加新的监控策略

基于现有监控策略创建新的监控策略：

1. 在主菜单中，转到“**监控**” → “**源状态**” → “**监控策略**”，然后选择要基于其创建新策略的监控策略。

   如有必要，您可以使用“**搜索**”字段在列表中查找监控策略。搜索将在以下列中执行：“**名称**”、“**租户**”、“**类型**”、“**时间表**”（日期和时间的名称）。

2. 单击“**复制策略**”。

3. 这将打开“**添加策略**”窗口，您可以在其中编辑策略设置。

   默认情况下，会在新策略的名称后附加“`- copy`”。其余设置与您所复制的策略相同。

4. 单击“**添加**”按钮以创建新策略。

监控策略是基于现有策略创建的。

删除监控策略

要删除监控策略：

1. 在主菜单中，转到“**监控**” → “**源状态**” → “**监控策略**”，然后选择要删除的一个或多个监控策略。

   如有必要，您可以使用“**搜索**”字段在列表中查找监控策略。搜索将在以下列中执行：“**名称**”、“**租户**”、“**类型**”、“**时间表**”（日期和时间的名称）。

2. 单击“**删除策略**”并确认操作。

选定的监控策略将被删除。

> 您无法删除预定义的监控策略或已分配给数据源的策略。

卡巴斯基公告

本部分介绍如何使用、配置和禁用卡巴斯基公告。

关于 Kaspersky 公告

Kaspersky 公告部分（**监控 → Kaspersky 公告**）提供与您的 Open Single Management Platform 版本以及受管理设备上安装的受管理应用程序相关的信息，让您及时了解最新情况。Open Single Management Platform 会定期删除过时的公告并添加新信息，以更新此部分的信息。

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

管理服务器必须具有互联网连接才能接收 Kaspersky 公告。

公告包括以下类型的信息：

- 与安全相关的公告

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

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

- 营销公告

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

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

新信息根据重要性分为以下几个类别：

1. 关键信息
2. 警告
3. 信息

当卡巴斯基公告部分出现新信息时，OSMP Console 将显示一个与公告重要级别相对应的通知标签。您可以单击该标签以在“Kaspersky 公告”区域中查看此公告。

如果您不想接收这些公告，可以禁用此功能。

禁用 Kaspersky 公告

卡巴斯基公告部分（“**监控**” → “**Kaspersky 公告**”）提供与您的 Open Single Management Platform 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。如果您不想接收 Kaspersky 公告，可以禁用此功能。

Kaspersky 包括两种类型的信息：与安全相关的公告和营销公告。

要禁用与安全相关的公告：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**Kaspersky 公告**”区域。

3. 将开关按钮切换到“**安全相关公告已禁用**”位置。

4. 单击“**保存**”按钮。

   Kaspersky 公告已禁用。

默认情况下禁用营销公告。仅当启用卡巴斯基安全网络 (KSN) 时，才会收到营销公告。您可以通过禁用 KSN来禁用此类公告。

禁用 KSN 可能会影响使用 KSN 服务的受管理 Kaspersky 应用程序。此类应用程序可能无法再与 Kaspersky 通信以发送或接收信誉数据、遥测数据或统计信息。

Cloud Discovery

Kaspersky Next XDR Expert 允许您监控运行 Windows 的受管理设备上云服务的使用情况，并阻止访问您认为不需要的云服务。Cloud Discovery 跟踪用户通过浏览器和桌面应用程序访问这些服务的尝试。它还会对用户尝试通过未加密的连接（例如，使用 HTTP 协议）来访问云服务的活动进行跟踪。此功能可帮助您检测并阻止影子 IT 对云服务的使用。

仅当您使用 Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 许可证激活了 Kaspersky Next XDR Expert 时，阻止功能才可用。

仅当您使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本时，才可以使用阻止功能。该安全应用程序的较早版本仅允许您监控云服务的使用情况。

您可以启用 Cloud Discovery 功能，并选择要启用该功能的安全策略或配置文件。您也可以在每个安全策略或配置文件中单独启用或禁用该功能。对于您不想让用户访问的云服务，您可以阻止对这些云服务的访问。

为了能够阻止对不需要的云服务进行的访问，请确保满足以下先决条件：

- 您使用的是 Kaspersky Endpoint Security 11.2 for Windows 或更高版本。该安全应用程序的较早版本仅允许您监控云服务的使用情况。
- 您已购买某一级别的 Kaspersky Next 授权许可，因此您可以阻止对不需要的云服务进行的访问。有关详细信息，请参阅 Kaspersky Next 帮助。

Cloud Discovery 小部件和 Cloud Discovery 报告会显示有关成功和被阻止的云服务访问尝试的信息。该小部件还会显示每项云服务的风险级别。Kaspersky Next XDR Expert 从所有仅受已启用该功能的安全配置文件保护的受管理设备获取有关云服务使用情况的信息。

使用小部件启用 Cloud Discovery

Cloud Discovery 功能允许您从所有受安全策略保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。您只能对 Kaspersky Endpoint Security for Windows 策略启用或禁用 Cloud Discovery。

可通过两种方式来启用 Cloud Discovery 功能：

- 使用 Cloud Discovery 小部件。
- 在 Kaspersky Endpoint Security for Windows 策略属性中。

  有关如何在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能的详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助中的 Cloud Discovery 部分。

请注意，您只能在 Kaspersky Endpoint Security for Windows 策略参数中禁用 Cloud Discovery 功能。

为了启用 Cloud Discovery，您必须在“**常规功能：基本功能**”功能区域中具有**写入**权限。

要使用 Cloud Discovery 小部件启用 Cloud Discovery 功能，请执行以下操作：

1. 打开 Kaspersky Next XDR Expert。
2. 在主菜单中，转到“**监控**” → “**控制板**”。
3. 在 **Cloud Discovery** 小部件上，单击“**启用**”按钮。

   如果您安装了 Kaspersky Endpoint Security for Windows 版本 12.4，请在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能。有关详细信息，请参阅 Cloud Discovery 部分。

   如果您的 Kaspersky Endpoint Security for Windows 版本低于 12.4，请将 Kaspersky Endpoint Security for Windows 插件更新至版本 12.5。
4. 在打开的“**启用 Cloud Discovery**”窗口中，选择要启用该功能的安全策略，然后单击“**启用**”按钮。

   以下策略设置将自动启用：**将脚本注入到 Web 流量以与网页进行交互**、**Web 会话监控**和**加密连接扫描**。

Cloud Discovery 功能会启用，小部件会被添加到仪表板。

将 Cloud Discovery 小部件添加到仪表板

您可以将 **Cloud Discovery** 小部件添加到仪表板，以监控受管理设备上云服务的使用情况。

如要将 Cloud Discovery 小部件添加到仪表板，您必须在“**常规功能：基本功能**”功能区域中具有**写入**权限。

要将 Cloud Discovery 小部件添加到仪表板，请执行以下操作：

1. 打开 Kaspersky Next XDR Expert。
2. 在主菜单中，转到“**监控**” → “**控制板**”。
3. 单击“**添加或还原小部件**”按钮。
4. 在可用小部件列表中，单击“**其他**”类别旁边的箭头图标 (>)。
5. 选择 **Cloud Discovery** 小部件，然后单击“**添加**”按钮。

   如果 Cloud Discovery 功能被禁用，请按照“使用小部件启用 Cloud Discovery”部分中的说明进行操作。

所选的小部件会添加到仪表板的末端。

查看有关云服务使用情况的信息

您可以查看 **Cloud Discovery** 小部件，其中会显示有关云服务访问尝试的信息。该小部件还会显示每项云服务的风险级别。Kaspersky Next XDR Expert 从仅受启用了此功能的安全配置文件保护的所有受管理设备获取云服务使用情况信息。

在查看之前，请确保：

- Cloud Discovery 小部件已添加到仪表板。
- Cloud Discovery 功能已启用。
- 您在“**常规功能：基本功能**”功能区域中具有**读取**权限。

要查看 Cloud Discovery 小部件，请执行以下操作：

1. 打开 Kaspersky Next XDR Expert。
2. 在主菜单中，转到“**监控**” → “**控制板**”。

   Cloud Discovery 小部件会显示在仪表板上。
3. 在 **Cloud Discovery** 小部件的左侧，选择云服务类别。

   小部件右侧的表格会显示在所选类别中用户最常尝试访问的最多五项服务。成功和被阻止的尝试均会计入尝试。
4. 在小部件的右侧，选择特定服务。

   下方的表格会显示最常尝试访问该服务的最多十台设备。在此表中，您可以生成两种类型的报告：成功访问尝试报告和被阻止访问尝试报告。

   此外，您还可以在此表中阻止特定设备访问云服务。

小部件会显示所请求的信息。

在显示的小部件中，您可以执行以下操作：

- 继续转到“**监控**”→“**报告**”部分以查看 Cloud Discovery 报告。
- 阻止或允许访问所选的云服务。

只有在通过 Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 授权许可激活 Kaspersky Next XDR Expert 后，才能使用阻止功能。只有在使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本时，才能使用阻止功能。
使用早期版本的安全应用程序时，您只能监控云服务的使用情况。

云服务的风险级别

对于每项云服务，Cloud Discovery 都会为您提供风险级别。风险级别可帮助您确定不符合组织安全要求的服务。例如，在决定是否阻止对特定服务的访问时，您可能需要考虑风险级别。

免责声明：风险级别是一个估计指数，并不能说明云服务的质量或服务制造商的任何信息。风险级别只是卡巴斯基专家的建议。

云服务的风险级别显示在 Cloud Discovery 小部件和所有受监控云服务的列表中。

阻止对不需要的云服务进行的访问

您可以阻止用户访问您不希望他们访问的云服务。您也可以允许对之前被阻止的云服务的访问。

您在决定是否阻止对特定服务的访问时，除其他考虑因素外，还可能需要考虑风险级别。

您可以在安全策略或配置文件中阻止或允许对云服务的访问。

可通过两种方法来阻止对不需要的云服务进行的访问：

- 使用 Cloud Discovery 小部件。
  在这种情况下，您可以逐个阻止对服务的访问。
- 在 Kaspersky Endpoint Security for Windows 策略属性中。
  在这种情况下，您可以逐个阻止对服务的访问，也可以一次性阻止整个类别。
  有关如何在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能的详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助中的 Cloud Discovery 部分。

要使用小部件阻止或允许对云服务的访问，请执行以下操作：

1. 打开 Cloud Discovery 小部件，然后选择所需的云服务。
2. 在**使用该服务的前 10 台设备**面板中，找到要用于阻止或允许该服务的安全策略或配置文件。

3. 在所需行的“**策略或配置文件中的访问状态**”列中，执行以下任一操作：

   - 要阻止该服务，请在下拉列表中选择“**已阻止**”。
   - 要允许该服务，请在下拉列表中选择“**已允许**”。

4. 单击“**保存**”按钮。

安全策略或配置文件将会阻止或允许对所选服务的访问。

导出事件到 SIEM 系统

本部分介绍如何配置导出事件到 SIEM 系统。

配置导出事件到 SIEM 系统

Kaspersky Next XDR Expert 支持通过以下任一方式配置将事件导出到 SIEM 系统：导出到任何使用 Syslog 格式的 SIEM 系统；导出到使用 LEEF 和 CEF 格式的 Kaspersky SIEM、QRadar、Splunk 或 ArcSight SIEM 系统；或者直接从 Kaspersky Security Center 数据库将事件导出到 SIEM 系统。完成此方案后，管理服务器会自动将事件发送到 SIEM 系统。

先决条件

在开始在 Kaspersky Next XDR Expert 中配置事件导出之前：

- 了解有关事件导出方法的更多信息。
- 确保拥有系统设置的值。

> 您可以按任意顺序执行此方案的步骤。

将事件导出到 SIEM 系统的过程包括以下步骤：

- **配置 SIEM 系统以接收来自 Kaspersky Next XDR Expert 的事件**

  说明：配置 SIEM 系统中的事件导出

- **选择要导出到 SIEM 系统的事件**

  标记要导出到 SIEM 系统的事件。首先，标记所有受管理卡巴斯基应用程序中发生的常规事件。然后，可以标记特定受管理卡巴斯基应用程序的事件。

- **配置导出事件到 SIEM 系统**

您可以使用以下方法之一导出事件：

- 使用TCP、UDP或TLS over TCP协议。
- 直接从 Kaspersky Security Center 数据库导出事件。Kaspersky Security Center 数据库包含一组公共视图；您可以在 klakdb.chm 文档中找到这些公共视图的说明。

结果

配置导出事件到 SIEM 系统后，如果您选择了要导出的事件，可以查看导出结果。

先决条件

在 Kaspersky Next XDR Expert 中设置自动导出事件时，您必须指定 SIEM 系统的部分设置。建议您提前检查这些设置，以便做好配置 Kaspersky Next XDR Expert 的准备。

要成功配置自动发送事件到 SIEM 系统，您必须知道以下设置：

- **SIEM 系统服务器地址**

  安装了当前使用的 SIEM 系统的服务器的 IP 地址。在您的 SIEM 系统设置中检查此值。

- **SIEM 系统服务器端口**

  用于在 Kaspersky Next XDR Expert 与 SIEM 系统服务器之间建立连接的端口号。您需要在 Kaspersky Next XDR Expert 设置和 SIEM 系统的接收器设置中指定此值。

- **协议**

  用于将消息从 Kaspersky Next XDR Expert 传输到 SIEM 系统的协议。您需要在 Kaspersky Next XDR Expert 设置和 SIEM 系统的接收器设置中指定此值。

关于事件导出

Kaspersky Next XDR Expert 允许您接收有关管理服务器和安装在受管理设备上的卡巴斯基应用程序运行期间所发生事件的信息。事件信息保存在管理服务器数据库。

您可以在处理组织和技术级别的安全问题的集中式系统内使用事件导出，提供安全监控服务，以及合并来自不同解决方案的信息。即是提供对网络硬件和应用程序生成的安全警告的实时分析的 SIEM 系统，或者安全操作中心 (SOC)。

这些系统可以从许多源接收数据，包括网络、安全、服务器、数据库和应用程序。SIEM 系统也提供功能以集成监控的数据，以便帮助您避免丢失关键事件。而且，系统执行相关事件和警告的自动分析以通知管理员安全问题。警告可以通过仪表板实现，或可以通过第三方渠道发送，例如邮件。

将事件从 Kaspersky Next XDR Expert 导出到外部 SIEM 系统的过程涉及两个参与方：事件发送方（Kaspersky Next XDR Expert）和事件接收方（SIEM 系统）。要成功导出事件，您必须在 SIEM 系统和 Kaspersky Next XDR Expert 中进行配置。您可以先配置任意一端。您可以先在 Kaspersky Next XDR Expert 中配置事件传输，然后配置 SIEM 系统接收事件，也可以按相反的顺序进行配置。

从 Kaspersky Next XDR Expert 发送事件的方法

可通过以下三种方法将事件从 Kaspersky Next XDR Expert 发送到外部系统：

- 通过 Syslog 协议发送事件到任意 SIEM 系统

  使用 Syslog 协议，您可以转发发生在管理服务器上和受管理设备上安装的卡巴斯基应用程序中的任意事件。Syslog 协议是标准消息记录协议。您可以用它将事件导出到任何 SIEM 系统。

  为此，您需要标记希望中继到 SIEM 系统的事件。您可以在OSMP控制台中标记事件。只有标记的事件才会被中继到 SIEM 系统。如果您没有标记任何内容，则不会中继任何事件。

- 通过 CEF 和 LEEF 协议将事件发送到 Kaspersky SIEM、QRadar、Splunk 和 ArcSight 系统

  您可以使用 CEF 和 LEEF 协议导出常规事件。当通过 CEF 和 LEEF 协议导出事件时，您不必能够选择指定事件以导出。相反，所有常规事件都被导出。要将Open Single Management Platform事件转换为CEF和LEEF格式的事件，您需要使用siem_conversion_rules.xml文件。此文件包含 Kaspersky Next XDR Expert 事件属性列表以及 CEF 和 LEEF 格式事件的对应属性。此外，siem_conversion_rules.xml 文件包含用于生成与事件对应的消息的规则。此文件包含在 Kaspersky Next XDR Expert 分发包中。

  不同于 Syslog 协议，CEF 和 LEEF 协议不通用。CEF 和 LEEF 适用于相应的 SIEM 系统（Kaspersky SIEM、QRadar、Splunk 和 ArcSight）。因此，当您选择通过这些协议导出事件时，您使用 SIEM 系统所需解析器。

- 直接从 Kaspersky Next XDR Expert 数据库导出到任何 SIEM 系统

  以该方法导出事件可以用于通过使用 SQL 查询直接从数据库公共视图接收事件。查询结果被保存到 XML 文件，可以用于外部系统的输入数据。仅仅公共视图中的事件可以被直接从数据库中导出。

通过 SIEM 系统接收事件

SIEM 系统必须接收并正确解析从 Kaspersky Next XDR Expert 收到的事件。要实现这一点，您需要正确配置 SIEM 系统。配置取决于特定的 SIEM 系统。然而，有一些配置所有 SIEM 系统的通用步骤，例如配置接收器和解析器。

关于配置 SIEM 系统中的事件导出

将事件从 Kaspersky Next XDR Expert 导出到外部 SIEM 系统的过程涉及两个参与方：事件发送方（Kaspersky Next XDR Expert）和事件接收方（SIEM 系统）。您必须在 SIEM 系统和 Kaspersky Next XDR Expert 中配置事件导出。

您在 SIEM 系统中指定的设置取决于您使用的系统。通常，对于所有 SIEM 系统，您必须设置接收器和消息解析器（可选）以解析接收的事件。

设置接收器

要接收 Kaspersky Next XDR Expert 发送的事件，您必须在 SIEM 系统中设置接收器。通常，必须在 SIEM 系统指定以下设置：

- **导出协议**

  消息传输协议，可以是 UDP、TCP 或基于 TCP 的 TLS。此协议必须与您在 Kaspersky Next XDR Expert 中指定的协议相同。

- **端口**

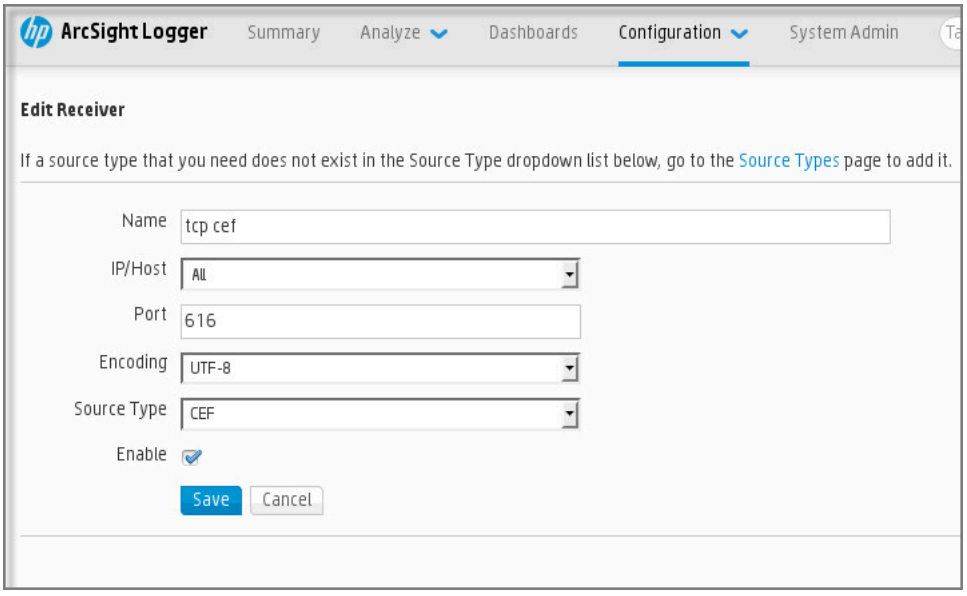
  指定用于连接 Kaspersky Next XDR Expert 的端口号。此端口必须与您在 Kaspersky Next XDR Expert 中配置 SIEM 系统时指定的端口相同。

- **数据格式**

  指定Syslog、CEF或LEEF格式。

根据所使用的 SIEM 系统，您可能需要指定一些附加接收器设置。

下图显示了 ArcSight 的接收器设置截图。



ArcSight 的接收器设置

消息解析器

导出的事件作为消息被传递到 SIEM 系统。然后对这些消息应用解析器，以确保 SIEM 系统可以使用事件信息。消息解析器是 SIEM 系统的一部分；它用于将消息内容拆分为事件代码、严重级别、描述和参数等字段。这样，SIEM 系统便可处理从 Kaspersky Next XDR Expert 接收的事件，以便将其存储在 SIEM 系统数据库中。

标记要以 Syslog 格式导出到 SIEM 系统的事件

在启用自动导出事件后，您必须选择将被导出到外部 SIEM 系统的事件。

您可以配置基于以下条件之一导出 Syslog 格式的事件到外部系统：

- 标记常规事件。如果在事件设置或管理服务器设置中标记要在策略中导出的事件，SIEM 系统将接收由特定策略管理的所有应用程序中发生的所标记事件。如果导出的事件在策略中被选中，您将不能为由该策略管理的个别应用程序重新定义所选事件。
- 为受管理应用程序标记事件。如果为受管理设备上安装的受管理应用程序选择要导出的事件，SIEM 系统将仅接收该应用程序中发生的事件。

对于策略更改事件，您只能启用或禁用将所有此类事件导出到 SIEM 系统。

关于标记要以 Syslog 格式导出到 SIEM 系统的事件

在启用自动导出事件后，您必须选择将被导出到外部 SIEM 系统的事件。

您可以配置基于以下条件之一导出 Syslog 格式的事件到外部系统：

- 标记常规事件。如果在事件设置或管理服务器设置中标记要在策略中导出的事件，SIEM 系统将接收由特定策略管理的所有应用程序中发生的所标记事件。如果导出的事件在策略中被选中，您将不能为由该策略管理的个别应用程序重新定义所选事件。
- 为受管理应用程序标记事件。如果为受管理设备上安装的受管理应用程序选择要导出的事件，SIEM 系统将仅接收该应用程序中发生的事件。

标记要以 Syslog 格式导出的 Kaspersky 应用程序事件

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

要为特定受管理应用程序标记要导出的事件：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 单击您要为其标记事件的应用程序的策略。

   政策设置窗口打开。
3. 转到“**事件配置**”区域。
4. 选中要导出到 SIEM 系统的事件旁边的复选框。
5. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”按钮。

   > 您也可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。
6. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。
7. 单击“**保存**”按钮。

受管理应用程序中的标记事件已准备好导出到 SIEM 系统。

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

要为受管理设备标记要导出的事件：

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

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

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

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

标记要以 Syslog 格式导出的常规事件

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

要标记常规事件以导出到 SIEM 系统：

1. 在主菜单中，执行以下操作之一：
   - 单击管理服务器名称。
   - 转到“**资产管理**”→“**策略**”，然后单击某个策略的链接。
2. 在打开的窗口中，转到“**事件配置**”选项卡。
3. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”。

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

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

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

关于使用 Syslog 格式导出事件

您可以使用 Syslog 格式将管理服务器和受管理设备上安装的其他卡巴斯基应用程序中发生的事件导出到 SIEM 系统。

Syslog 是消息记录协议的标准。它允许分离生成消息的软件、存储消息的系统和报告和分析消息的软件。每个消息都带有设备代码标签，指示生成消息的软件类型，并被分配严重级别。

Syslog 格式由 Request for Comments (RFC) 文档定义，该文档由 Internet Engineering Task Force（互联网标准）发布。RFC 5424 标准用于将 Kaspersky Next XDR Expert 中的事件导出到外部系统。

在 Kaspersky Next XDR Expert 中，您可以配置以 Syslog 格式将事件导出到外部系统。

导出过程包含两个步骤：

1. 启用自动事件导出。在此步骤中，将 Kaspersky Next XDR Expert 配置为向 SIEM 系统发送事件。启用自动导出后，Kaspersky Next XDR Expert 会立即开始发送事件。

2. 选择事件以导出到外部系统。在该步骤，您可以选择导出哪些事件到 SIEM 系统。

关于使用 CEF 和 LEEF 格式导出事件

您可以使用 CEF 和 LEEF 格式将常规事件、策略更改事件以及由卡巴斯基应用程序传输到管理服务器的事件导出到 SIEM 系统。导出事件集是预定义的，您无法选择要导出的事件。在将事件发送到 SIEM 系统（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，必须使用 siem_conversion_rules.xml 文件中指定的规则，将 Open Single Management Platform 事件转换为 CEF 和 LEEF 格式的事件。

基于使用的 SIEM 系统选择导出格式。下表显示了 SIEM 系统和对应的导出格式。

导出事件到 SIEM 系统的格式

SIEM 系统	导出格式
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- LEEF（日志事件扩展格式）是 IBM Security QRadar SIEM 的专用事件格式。QRadar 可以接收、识别和处理通过 LEEF 协议传输的事件。LEEF 事件必须使用 UTF-8 字符编码。您可以在 IBM Knowledge Center 查看 LEEF 协议的详情。

- CEF (通用事件格式)—开放式日志管理标准，涉及来自不同的网络设备和应用程序的安全信息的协同工作。CEF 允许您使用通用日志格式，因此数据可以被简易整合以用企业管理系统分析。CEF 事件必须使用 UTF-8 字符编码。

自动导出是指 Kaspersky Next XDR Expert 将常规事件发送到 SIEM 系统。事件自动导出在您启用后立即开始。该部分详细解释了如何启用自动事件导出。

将事件转换为 CEF 或 LEEF 格式

在将事件发送到 SIEM 系统（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 文件中指定的规则，将 Open Single Management Platform 事件解释为 CEF 和 LEEF 格式的事件。此文件包含在Open Single Management Platform分发包中。

siem_conversion_rules.xml 文件包含将事件转换为 CEF 和 LEEF 格式的预定义解释规则。如果想使用额外的事件解释规则，您可以手动将它们添加到文件中。

siem_conversion_rules.xml 文件包含以下部分：

- `<product name="SP_QRADAR" vendor="IBM">`

  本节包含以LEEF格式生成事件的规则，这些规则可以导出到QRadar SIEM系统。

- `<product name="SP_ARCSIGHT" vendor="HP">`。

  本节包含以CEF格式生成事件的规则，这些事件可以导出到ArcSight或Splunk SIEM系统。

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`。

  本节包含以CEF格式生成事件的规则，这些事件可以导出到KUMA。

每个部分都有 `<common>` 子部分，Open Single Management Platform 事件属性以及 LEEF 格式事件的相应属性位于其中。这些通用属性用于所有可以导出的事件类型。

此外，每个部分都有`<event>`子部分。每个`<event>`子部分都包含其他属性，这些属性会添加到`<common>`部分中列出的属性中。

您可以手动将新的事件生成规则添加到 siem_conversion_rules.xml 文件中。

要添加新的事件生成规则：

1. 向 `<product name="SP_QRADAR" vendor="IBM">`、`<product name="SP_QRADAR" vendor="IBM">` 或 `<product name="Kaspersky SIEM" vendor="Kaspersky">` 部分添加新的 `<event>` 子部分，然后根据需要指定其他事件属性。

2. 如果事件仅由通用属性组成，`<event>`子部分将为空。

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
```

```
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

配置 Kaspersky Next XDR Expert 以将事件导出到 SIEM 系统

要将事件导出到 SIEM 系统，您必须在 Kaspersky Next XDR Expert 中配置导出过程。

在将事件发送到 SIEM 系统（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 文件中指定的规则，将 Kaspersky Next XDR Expert 事件转换为 CEF 和 LEEF 格式的事件。

要在 OSMP Console 中配置导出到 SIEM 系统：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**导出到 SIEM**”区域。

3. 单击“**设置**”链接。

   “**导出设置**”区域将打开。

4. 在“**导出设置**”区域指定设置：

   - **SIEM 系统服务器地址**

     安装了当前使用的 SIEM 系统的服务器的 IP 地址。在您的 SIEM 系统设置中检查此值。

   - **SIEM 系统端口**

     用于在 Kaspersky Next XDR Expert 与您的 SIEM 系统服务器之间建立连接的端口号。您需要在 Kaspersky Next XDR Expert 设置和 SIEM 系统的接收器设置中指定此值。

- **协议**

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

  如果选择 TLS over TCP 协议，则指定以下 TLS 设置：

  - **服务器身份验证**

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

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

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

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

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

  - **添加主题名称/主题备选名称**

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

  - **添加客户端身份验证**

    对于客户端身份验证，可以插入证书或在 Open Single Management Platform 中生成证书。

    - **插入证书**。您可以使用从任何来源（例如，从任何受信任 CA）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

      - **X.509 证书 PEM**。将证书文件上传到“**证书文件**”字段，并将私钥文件上传到“**密钥文件**”字段。这两个文件彼此独立。文件的加载顺序无关紧要。上传这两个文件后，在“**密码或证书验证**”字段中指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

      - **X.509 证书 PKCS12**。在“**证书文件**”字段中上传包含证书及其私钥的单个文件。上传该文件后，在“**密码或证书验证**”字段中指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

    - **生成密钥**。您可以在 Open Single Management Platform 中生成自签名证书。因此，Open Single Management Platform 会存储生成的自签名证书，您可以将证书的公钥部分或 SHA1 指纹传递给 SIEM 系统。

- **数据格式**

  您可以根据 SIEM 系统的要求选择 Kaspersky SIEM、IBM QRadar SIEM、ArcSight、 Splunk 或系统日志格式。

  如果选择系统日志数据格式，则必须指定**最大消息大小，字节**

  指定 SIEM 系统消息的最大大小。每个事件被一条消息转发。如果消息的精确长度超过指定值，消息被截断且数据可能丢失。默认大小是 2048 字节。仅当在“**协议**”字段中选择了系统日志格式后，该字段才可用。

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

   a. 单击**设置导出起始日期**链接。

   b. 在打开的区域的“**导出的起始日期**”字段中，指定开始日期。

   c. 单击“**确定**”。

6. 启用**导出事件到 SIEM**选项。

7. 要将策略更改事件发送到SIEM，请启用**将策略更改的扩展事件导出到 SIEM**选项。系统会为每个已更改的政策设置向SIEM发送一个单独的事件。

8. 要检查 SIEM 系统连接是否已配置，请单击**检查连接**按钮。

   与 SIEM 系统的连接已建立，测试事件已发送。将显示连接状态。

9. 单击“**保存**”按钮。

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

监控策略和策略配置文件的更改

当策略设置发生变更时，会生成策略变更事件，然后您可以将其导出到 SIEM 系统，以监控策略变更并生成警报。只能通过 SIEM 系统访问策略变更事件。

策略变更事件生成后不会存储在管理服务器数据库中，也无法在 OSMP Console 的 **监控 → 事件分类** 区域查看。您也无法在 **事件配置** 选项卡上为这些事件指定通知设置和存储设置。

创建策略时，会为每个策略设置生成策略变更事件。更改策略时，会为策略中每个已更改的设置生成策略变更事件。删除策略会生成一个事件。例如，创建 Kaspersky Security Center 策略会生成大约 1000 个事件，而创建 Kaspersky Endpoint Security 策略会生成超过 7000 个事件。

生成策略变更事件的条件

在以下情况下会创建策略变更事件：

- 以下应用程序策略的创建、修改或删除：
  - Kaspersky Security Center 网络代理
  - Kaspersky Security Center 管理服务器
  - Kaspersky Endpoint Security for Windows 14.1
  - Kaspersky Endpoint Security for Linux 12.5
  - Kaspersky Endpoint Security for Linux 12.4
  - Kaspersky Endpoint Security for Mac 12.2.1。

- 已在管理服务器属性中启用 **将策略更改的扩展事件导出到 SIEM** 选项。
- 通过 OSMP 控制台手动修改策略。

在以下情况下不会创建策略变更事件：

- 修改常规策略设置。
- 修改从父策略继承的策略设置。
- 通过 Kaspersky Security Center OpenAPI 修改策略设置。
- 直接在应用程序中修改 Kaspersky 应用程序设置。

策略变更事件字段

下表显示了一组策略变更事件字段。这些字段的表示形式取决于输出事件格式（例如 Syslog、CEF 或 LEEF）。有关确切的字段名称和事件模板，请参阅 siem_conversion_rules.xml 文件。事件参数仅以英语提供。

事件字段	数据类型	描述
EventType	字符串	事件类型。允许为特定类型的事件创建关联规则。 可能的值："策略已创建"、"策略已修改"、"策略已删除"。
srvName	字符串	管理服务器名称。
eventTime	datetime	事件的日期和时间（UTC）。
eventGroupID	int	修改的事件组 ID。
objectID	int	对象的内部 ID。
objectName	字符串	策略显示名称。
objectGroup	字符串	包含该策略的管理组的完整路径和名称。
user	字符串	作出该修改的用户的名称。
operation	字符串	参数修改类型。 可能的值："Added"、"Removed"、"Changed"。
path	字符串	参数路径。包含末级参数的父节点的路径。该路径基于策略的节和小节的名称创建。该路径结构与网络代理策略设置、常规策略设置和比较策略修订中所述的路径结构相同。
parameter	字符串	末级参数的名称。
oldValue	字符串	末级参数的旧值。
newValue	字符串	末级参数的新值。

直接从数据库导出事件

您可以直接从 Kaspersky Next XDR Expert 数据库检索事件，而无需使用 Kaspersky Next XDR Expert 界面。您可以直接查询公共视图并检索事件数据，也可以基于现有公共视图创建您自己的视图并定位它们以获取所需数据。

公共视图

为方便您使用，Kaspersky Next XDR Expert 数据库中提供了一组公共视图。您可以在 klakdb.chm 文档中找到这些公共视图的描述。

v_akpub_ev_event 公共视图包含一组展示数据库中事件参数的字段集。在 klakdb.chm 文档中，您还可以找到与 Kaspersky Next XDR Expert 的其他实体（例如设备、应用程序或用户）对应的公共视图的相关信息。您可以在您的查询中使用该信息。

该部分包含了使用 klsql2 实用工具执行 SQL 查询的说明以及查询例子。

要创建 SQL 查询或数据库视图，您也可以使用其他程序以操作数据库。有关如何查看 Kaspersky Next XDR Expert 数据库连接参数（例如实例名称和数据库名称）的信息，请参阅相应章节。

使用 klsql2 实用工具执行 SQL 查询

本文描述了如何使用 klsql2 实用工具，以及如何使用该实用工具执行 SQL 查询。请使用已安装的 Kaspersky Next XDR Expert 版本中包含的 klsql2 实用工具版本。

要使用 klsql2 实用程序：

1. 转到安装管理服务器的目录。默认安装路径为/opt/kaspersky/ksc64/sbin。
2. 在此目录中，创建一个扩展名为 .sql 的空白文件。
3. 在任意文本编辑器中打开创建的 .sql 文件。
4. 在 .sql 文件中，键入所需的 SQL 查询，然后保存该文件。
5. 在安装了管理服务器的设备上，在命令行，输入以下命令以从 .sql 文件执行 SQL 查询并保存结果到 result.xml 文件：

   ```
   sudo ./klsql2 -i src.sql -u <用户名> -p <密码> -o result.xml
   ```

   其中 <用户名> 和 <密码> 是有权访问数据库的用户账户的凭证。
6. 如果需要，输入有权访问数据库的用户账户的登录名和密码。
7. 打开新创建的 result.xml 文件以查看 SQL 查询结果。

您可以编辑 .sql 文件并创建到公共视图的任意 SQL 查询。然后，从命令行，执行您的查询并保存结果到文件。

klsql2 实用工具中的 SQL 查询例子

该部分显示 SQL 查询的例子，通过 klsql2 实用工具执行。

以下例子阐述了对过去七天发生在设备上的事件的获取，并根据事件发生时间顺序显示事件。首先显示最近的事件。

PostgreSQL 示例:

```
SELECT
  /* 事件标识符 */
  "e"."nId",

  /* 事件发生时间 */
  "e"."tmRiseTime",

  /* 事件类型的内部名称 */
  "e"."strEventType",

  /* 事件的显示名称 */
  "e"."wstrEventTypeDisplayName",

  /* 事件的显示描述 */
  "e"."wstrDescription",

  /* 事件的显示描述 */
  "e"."wstrGroupName",

  /* 发生事件的设备的显示名称 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 发生事件的设备的 IP 地址 */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 或 MariaDB 示例:

```
SELECT

  /* 事件标识符 */
  `e`.`nId`,

  /* 事件发生时间 */
  `e`.`tmRiseTime`,

  /* 事件类型的内部名称 */
  `e`.`strEventType`,

  /* 事件的显示名称 */
  `e`.`wstrEventTypeDisplayName`,

  /* 事件的显示描述 */
  `e`.`wstrDescription`,

  /* 设备组名称 */
  `e`.`wstrGroupName`,

  /* 发生事件的设备的显示名称 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 发生事件的设备的 IP 地址 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

查看 Kaspersky Next XDR Expert 数据库名称

如果您想通过 MySQL 或 MariaDB 数据库管理工具访问 Kaspersky Next XDR Expert 数据库，则必须知道数据库名称，才能从 SQL 脚本编辑器连接到该数据库。

要查看 Kaspersky Next XDR Expert 数据库的名称：

1. 在主菜单中，单击管理服务器名称。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**当前数据库详情**”区域。

   数据库名称在“**数据库名称**”字段中指定。使用数据库名称在您的 SQL 查询中定位数据库。

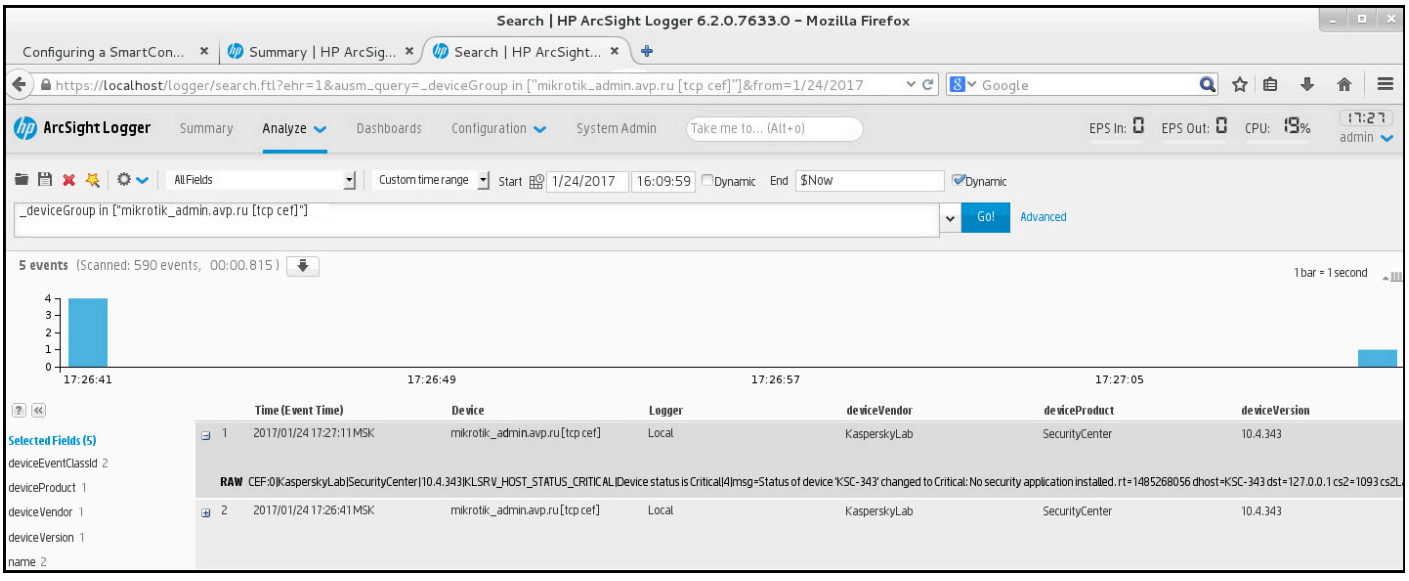
查看导出结果

您可以控制事件导出过程的成功完成。为此，检查带有导出事件的邮件是否被您的 SIEM 系统接收。

如果您的 SIEM 系统能够接收并正确解析 Kaspersky Next XDR Expert 发送的事件，则表示双方均已正确配置。否则，请将您在 Kaspersky Next XDR Expert 中指定的设置与 SIEM 系统中的配置进行比对。

下图显示导出到 ArcSight 的事件。例如，第一个事件是严重的管理服务器事件：“*设备状态为严重*”。

导出事件在您 SIEM 系统中的显示随您使用的 SIEM 系统而不同。



事件例子

将事件从 OSMP 收集器发送到外部 SIEM 系统收集器

要配置向外部SIEM系统的收集器发送事件，必须满足以下条件：

1. 您必须使用具有主管理员权限的用户账户登录 OSMP 控制台。
2. 在OSMP中，必须在Kubernetes集群中安装**[OOTB] Kaspersky EDR**收集器。
3. 必须在KUMA中安装具有以下组件的收集器：
   - 启用TLS和\n分隔符的**tcp**类型的连接器。
   - 不包含映射但包含原始事件的**json**类型规范化器。
   - **存储**类型的目标位置。
4. 必须有安装了curl和openssl实用工具的Unix终端。

配置将事件从OSMP收集器导出到外部SIEM系统的收集器涉及以下步骤：

1. **获取用于向[OOTB]Kaspersky EDR收集器发送事件的证书和密钥**

   1. 在应用程序主窗口中，转到**设置**→**租户**部分。
   2. 点击**根租户**，然后转到**设置** → **证书**子部分。
   3. 选中TLS证书旁边的复选框，然后单击**导出**。
   4. 这将打开一个窗口；在该窗口中，输入密码并单击**导出**按钮。

      PFX格式的证书下载到您的默认下载目录。
   5. 通过运行以下命令，提取下载的证书以获取cert.pem文件和key.pem文件：

      ```
      openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out cert.pem && \
      openssl pkcs12 -in certificate.pfx -nocerts -nodes -out key.pem
      ```

      输入并重新输入导出PFX证书时指定的密码。

   获取用于向收集器发送事件的cert.pem证书和key.pem密钥。

2. **创建并配置用于将事件导出到外部SIEM系统的TCP目标位置**

   1. 在主应用程序窗口中，前往**监控**→**资源和服务**→**活动服务**部分。
   2. 选择**[OOTB]Kaspersky EDR**收集器。
   3. 在显示的收集器编辑窗口中，选择**路由**选项卡，然后单击**添加**按钮。

4. 创建目标位置：

   a. 在**基本设置**选项卡的**类型**下拉列表中，选择**tcp**。

   b. 在**URL**字段中，指定您需要连接的URL。例如：<KUMA_collector_host_name>:<KUMA_collector_port>。

   c. 转到**高级设置**选项卡。

   d. 在**TLS模式**下拉列表中，选择**启用**。

   e. 在**分隔符**下拉列表中，选择**\n**。

   f. 单击“**保存**”按钮。

5. 选择**设置验证**选项卡，然后单击**保存并重新启动服务**按钮。

6. 关闭收集器编辑窗口。

已配置使用TLS模式的TCP目标位置，用于将事件导出到外部SIEM系统。

3 获取[OOTB]Kaspersky EDR收集器的连接器网关URL

1. 在**监控→资源和服务→活动服务**部分，右键单击**[OOTB]Kaspersky EDR**收集器，然后在上下文菜单中选择**部署**。

2. 这将打开一个窗口；在该窗口中，复制**连接器网关URL**设置的值。

4 向[OOTB]Kaspersky EDR收集器发送测试事件

1. 在您的终端中运行以下命令：

```
curl -w "%{http_code}\n" -X POST \
--cert cert.pem \
--key key.pem \
-H "Content-Type: application/json" \
--data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \
https://<Connector gateway URL> -k
```

2. 将 `<Connector gateway URL>` 替换为您之前复制的 **连接器网关 URL** 设置的值。

示例

```
curl -w "%{http_code}\n" -X POST \
--cert cert.pem \
--key key.pem \
-H "Content-Type: application/json" \
--data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \
https://in.mbpeo8s3rqnmjqt8z56cysb9w.kuma.xdr-name.kuma.avp.ru:443 -k
```

您可以在终端中看到响应代码200。该事件已发送至外部SIEM系统的收集器。

5 检查事件是否已到达外部SIEM系统

1. 使用具有主管理员权限的用户帐户登录 KUMA Web 界面。

2. 前往**事件**选项卡。

3. 在**KL_HostOsFamily**字段中查找带有**Test_send_to_external_SIEM_collector**值的事件。

Raw字段的示例内容


```
{
  "ID":"fca85cda-f760-48a8-8060-382bbaf7af14",
  "Timestamp":1776534533425,
  "TenantID":"d22648f7-bd98-4f55-a7ca-90b51f4d3fae",
  "ServiceID":"efd93e7c-1f8c-4035-bc76-a6efdd72197f",
  "ServiceName":"[OOTB] Kaspersky EDR",
  "Priority":0,
  "SpaceID":"",
  "DeviceTimeZone":"+03:00",
  "EndTime":1776534533425,
  "DeviceReceiptTime":1776534533425,
  "Type":1,
  "Extra":{
    "Product":"EDR"
  },
  "S":{
    "KL_HostOsFamily":"Test_send_to_external_SIEM_collector",
    "KL_Product":"EDR"
```


该事件已到达外部SIEM系统的收集器。

管理对象修订

该区域包含了对象修订管理的信息。Kaspersky Next XDR Expert 允许您跟踪对象的修改。每次保存对对象所做的更改时，都会*创建一个修订*。每个修订都有一个数字。

支持修订管理的应用程序对象包括：

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

您可以对对象修订采取以下操作：

- 查看选定的修订（仅适用于策略）
- 回滚对对象所做的更改到所选的修订
- 将修订保存为 JSON 文件（仅适用于策略）

在任何支持修订管理的对象的属性窗口，“**修订历史**”区域显示了包含以下详情的对象修订列表：

- **修订** – 对象修订版本号。
- **时间** – 对象修改的日期和时间。
- **用户** – 修改对象的用户的名称。

- **用户设备 IP 地址** — 从其修改对象的设备的 IP 地址。
- **Web Console IP 地址** — 修改对象的 OSMP 控制台的 IP 地址。
- **操作** — 运行在对象上的操作。
- **描述** — 与对象设置更改相关的修订描述。

  默认下，对象修订描述为空。要添加描述到修订，请选择相关修订并单击“**编辑描述**”按钮。在打开的窗口中，输入一些修订描述的文本。

查看并保存策略修订

通过 Open Single Management Platform，您可以查看在特定时间段内对策略所做的修改，并且将有关这些修改的信息保存在文件中。

如果相应的管理 Web 插件支持此功能，则可以查看和保存策略修订。
这些选项适用于管理服务器、网络代理、Kaspersky Endpoint Security for Windows（从 Web 插件版本 14.0 开始）、Kaspersky Endpoint Security for Linux（从 Web 插件版本 12.4 开始）和 Kaspersky Endpoint Security for Mac（从 Web 插件版本 12.2.1 补丁 A 开始）的策略。

要查看策略修订：

1. 在主菜单中，转到“**资产管理**”→“**策略**”。
2. 单击要查看修订的策略，然后转到“**修订历史**”部分。
3. 在策略修订列表中，单击要查看的修订编号。

   如果修订大小超过 10 MB，您将无法使用 OSMP 控制台进行查看。系统将提示您将所选的修订保存到 JSON 文件。

   如果修订大小不超过 10 MB，则会显示 HTML 格式的报告，其中包含所选策略修订的设置。由于报告显示在弹出窗口中，请确保您的浏览器允许弹出窗口。

对于 Kaspersky Endpoint Security for Windows和 Kaspersky Endpoint Security for Mac 的策略，报告将不包含策略配置文件信息。

要将策略修订保存到 JSON 文件，

在策略修订列表中，选择要保存的修订，然后单击“**保存到文件**”。

修订会保存到 JSON 文件中。

如有必要，您可以比较政策修订版本。

比较策略修订

您可以将政策的历史版本与其当前版本进行比较，比较列表中选定的不同版本，或者将一个政策的版本与另一个政策的版本进行比较。这些选项适用于管理服务器、网络代理、 Kaspersky Endpoint Security for Windows （从 14.0 Web 插件版本开始）以及 Kaspersky Endpoint Security for Mac（从 12.2.1 Patch A Web 插件版本开始）的策略。

要比较策略的修订版本：

1. 在主菜单中，转到“**资产管理 → 策略**”。
2. 点击要比较其版本的政策。
   策略设置窗口打开。
3. 转到**修订历史**选项卡，然后选中要比较的版本旁边的复选框。
4. 在工具栏中，单击**比较**按钮，然后从下拉列表中选择以下选项之一：
   - **与当前版本**，如果您想将在步骤 3 中选择的版本与同一策略的上次保存版本进行比较。
   - **选择版本**，如果您想比较步骤3中选中的两个复选框。

     复选框的选择顺序不会影响比较结果。默认情况下，系统会将所选的较早版本与最新版本进行比较。例如，如果您选中版本5和版本1旁边的复选框，则会将版本1与版本5进行比较。报告将包含版本 1 相对于版本 5 新增、删除或更改的设置信息。
   - **与其他政策的版本比较**，如果您想比较两个不同政策的版本。
     在打开的右侧窗格中，执行以下操作：
     a. 在**应用程序名称**字段中，选择要比较的策略：网络代理或管理服务器。
     b. 在**政策名称**字段中，指定要将其版本与在步骤3中选择的政策进行比较的政策名称。
        政策版本列表随即显示。
     c. 选择所需的修订版，然后单击**比较**按钮。

版本对比报告以HTML格式显示在浏览器的新选项卡中。

如果比较结果超过10MB，则会显示相应的对话框。您可以点击**保存到文件**按钮将报告保存为文件，或者取消操作。

报告以OSMP控制台的界面语言显示。您可以点击向下箭头图标展开报告的某些部分（▼）旁边是该部分，或者点击向上箭头折叠该部分（▲） 图标。

报告包含以下信息：

- 卡巴斯基徽标。
- 报告名称。
- 报告创建的时间和日期。
- 政策名称、管理服务器以及包含该政策（或多个政策）的管理群组，这些政策的修订版本将被进行比较。
- “**另存为 HTML**”按钮。点击该按钮，报告将保存到您的电脑上。
- **摘要**部分显示有关比较版本的常规信息：政策名称、版本号、版本保存的时间和日期、保存版本的用户以及版本描述。

  对于继承的政策，不会显示用户信息。

- 比较各版本之间的差异。差异在以下部分中显示：
  - **被添加设置**
  - **删除的设置**
  - **更改设置**
  - **仅适用于对象1的设置**（如果您比较了两个不同政策的版本）
  - **仅适用于对象2的设置**（如果您比较了两个不同政策的版本）

  如果某个部分没有数据，则不会显示该部分。

对于 Kaspersky Endpoint Security for Windows和 Kaspersky Endpoint Security for Mac 的策略，修订比较报告将不包含策略配置文件信息。

回滚对象到先前修订

如果必要，您可以回滚对对象所做的更改。例如，您可能必须转换策略设置到特定日期的状态。

要回滚对对象所做的更改：

1. 在对象属性窗口中，打开“**修订历史**”选项卡。
2. 在对象修订列表中，选择要回滚更改的修订。

3. 单击**回滚**按钮。

4. 单击“**确定**”以确认操作。

该对象被回滚到所选修订。对象修订列表显示所做的操作记录。修订描述显示了您转换对象所到的修订号的信息。

回滚操作仅适用于策略和任务对象。

对象删除

本部分提供有关删除对象的信息。

您可以删除对象，包括以下：

- 策略
- 任务
- 安装包
- 虚拟管理服务器
- 用户
- 安全组
- 管理组

要删除对象：

1. 打开 OSMP 控制台的所需部分，然后选择对象。

2. 在工具栏上，单击“**删除**”按钮。

3. 在打开的窗口中，单击“**确定**”以确认您的选择。

所选对象被删除。

当您删除对象时，其信息保留在数据库。已删除对象的信息的存储期限与对象修订的存储期限一致（推荐期限是 90 天）。您仅在权限的**已删除对象**区域具有**修改**权限时才能更改存储期限。

关于删除客户端设备

当您从管理组中删除受管理设备时，应用程序会将设备移至未分配的设备组。删除设备后，已安装的卡巴斯基应用程序——网络代理和安全应用程序（例如 Kaspersky Endpoint Security）——将保留在设备上。

Kaspersky Next XDR Expert 根据以下规则处理未分配的设备组中的设备：

- 如果您配置了设备移动规则，并且设备符合移动规则的条件，则该设备会根据规则被自动移动到管理组。
- 设备会被存储在未分配的设备组中，并根据设备保留规则自动从组中删除。

  设备保留规则不会影响具有一个或多个使用完整磁盘加密进行加密的驱动器的设备。此类设备不会被自动删除——您只能手动删除它们。如果您需要删除带有加密驱动器的设备，请先解密驱动器，然后再删除该设备。

  > 当您删除带有加密驱动器的设备时，解密驱动器所需的数据也会被删除。如果在删除此类设备（从“**未分配的设备**”或“**受管理设备**”组）时打开的确认窗口中选中“**我了解风险并想要删除选定的设备**”复选框，则表示您知晓数据随后会被删除。

  要解密驱动器，必须满足以下条件：

  - 设备被重新连接到管理服务器以恢复解密驱动器所需的数据。
  - 设备用户记住解密密码。
  - 用于加密驱动器的安全应用程序（例如 Kaspersky Endpoint Security for Windows）仍安装在设备上。

  如果驱动器由卡巴斯基磁盘加密技术加密，您还可以尝试使用 FDERT Restore Utility 恢复数据。

> 在 VDI 中，如果您的设备包含加密驱动器，则删除该设备后，加密驱动器上的信息也会被删除。

当您从未分配的设备组中手动删除设备时，应用程序会从列表中删除该设备。删除设备后，已安装的卡巴斯基应用程序（如果有）将保留在设备上。然后，如果该设备对管理服务器仍然可见并且您配置了定期网络轮询，Kaspersky Next XDR Expert 会在网络轮询过程中发现该设备并将其添加回未分配的设备组。因此，最好仅当设备对管理服务器不可见时再手动删除设备。

从隔离区和文件备份中下载和删除文件

本部分提供了有关如何从 OSMP Console 的隔离区和文件备份中下载和删除文件的信息。

从隔离区和文件备份区下载文件

只有满足以下两个条件之一，您才能下载隔离区和备份区中的文件：在设备的设置中启用了“**不断开与管理服务器的连接**”选项，或者正在使用连接网关。否则，下载无法进行。

要将隔离区或文件备份中的文件的副本保存到硬盘驱动器，请执行以下操作：

1. 执行以下操作之一：

   - 如果要从隔离区保存文件副本，请在主菜单中转到**操作 → 存储库 → 隔离**。
   - 如果要从备份区保存文件副本，请在主菜单中转到**操作 → 存储库 → 文件备份**。

2. 在打开的窗口中，选择要下载的文件并单击 **下载**。

   下载开始。

如果您是从“**隔离**”部分执行此操作，则客户端设备上隔离目录中存放的文件副本会下载到您的计算机中。该文件保存在受密码保护的 ZIP 压缩包中。密码为：infected。

关于从隔离区、文件备份区或活动威胁存储库中删除对象

当客户端设备上安装的卡巴斯基安全应用程序将对象放置到隔离区、备份或活动威胁存储库时，它们会将已添加对象的相关信息发送到 Open Single Management Platform 中的“**隔离**”、“**文件备份**”或者“**活动威胁**”部分。打开其中一个区域时，可以删除所需的对象。

对于“**文件备份**”或“**活动威胁**”区域，从列表中选择一个对象，然后单击“**移除**”按钮。

对于“ **隔离**”区域，您可以执行以下操作之一：

- 选中要移除的对象名称旁边的复选框，然后在工具栏中单击“**删除**”按钮。
- 单击要移除的对象名称，然后在打开的详细信息窗口中，在工具栏中单击“**删除**”按钮。

  此时，对象将被删除，屏幕上将显示相应的通知，并且详细信息窗口将关闭。

Open Single Management Platform 会从列表中移除选定对象，或从存储库中删除选定对象。要执行的操作由将选定对象放置到存储库的卡巴斯基应用程序定义。卡巴斯基应用程序在“**条目添加者**”字段中予以指定。

有关要执行的操作的详细信息，请参阅卡巴斯基应用程序的文档。

上传文件进行扫描

您可以上传文件，然后立即或稍后进行扫描。Kaspersky Next XDR Expert使用反恶意软件引擎和YARA技术进行扫描，并将文件发送到沙盒。

若要上传文件进行扫描：

1. 在主菜单中，转到 **操作 → 存储库 → 文件**。
2. 单击**上传**。

   上传文件窗口随即打开。
3. 选择要与该文件关联的租户。

4. 如果您希望文件上传完成后立即进行扫描，请确保**上传后扫描**切换按钮已打开。您可以关闭此切换按钮，稍后再扫描文件。

5. 您可以通过拖放或点击**上传文件**来上传文件。您可以选择多个文件。

6. 单击**上传**。

Kaspersky Next XDR Expert随即开始上传文件。上传完成后，如果**上传后扫描**切换按钮处于开启状态，Kaspersky Next XDR Expert将开始扫描。

手动扫描存储库中的文件

如果文件尚未扫描或您想重新扫描该文件，您可以手动开启扫描。Kaspersky Next XDR Expert使用反恶意软件引擎和YARA技术进行扫描，并将文件发送到沙盒。

若要扫描存储库中的文件：

1. 在主菜单中，转到 **操作 → 存储库 → 文件**。

2. 从列表中选择一个或多个文件。

3. 单击列表上方的**扫描**按钮。

Kaspersky Next XDR Expert随即开始扫描选定的文件。您可以在**扫描状态**列中找到扫描状态。

查看扫描状态和扫描结果

若要查看文件扫描状态和扫描结果：

1. 在主菜单中，转到**操作 → 存储库 → 文件**。
   文件列表中的**扫描状态**列包含有关扫描状态和扫描结果的基本信息：

   - **未扫描**
     文件尚未扫描。
   - **正在扫描**
     正在扫描文件。
   - **未检测到**
     文件已扫描，未检测到威胁。
   - **检测到**
     文件已扫描，检测到威胁。

2. 如需了解更多详细信息，请点击您想了解更多信息的文件名。
   在打开的窗口中，您可以找到有关该文件的信息，包括文件扫描的详细结果。

Kaspersky Next XDR Expert 组件的运行诊断

本部分介绍如何获取有关 Kaspersky Next XDR Expert 组件的诊断信息。

获取 Kaspersky Next XDR Expert 组件的日志文件

KDT 允许您获取包含 Kaspersky Next XDR Expert 组件和 Kubernetes 集群诊断信息的日志文件，以便您自行或在卡巴斯基技术支持的帮助下解决问题。

Kaspersky Next XDR Expert 根据以下模板生成日志文件名：pod_name.container_name.log。其中，pod_name 是 Kubernetes pod 名称，container_name 是 Kubernetes 容器名称。

要获取 Kaspersky Next XDR Expert 组件和管理 Web 插件的日志文件：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt logs get <flags>
```

其中，`<flags>` 是命令参数，允许您配置日志记录结果。

您可以指定以下日志记录参数：

- `--app` < 组件列表 > — 获取列出的 Kaspersky Next XDR Expert 组件的日志。
  例如，如果要获取管理服务器最近一小时的日志，请运行以下命令：
  `./kdt logs get --app ksc`
  可用的Kaspersky Next XDR Expert组件列表

  ```
  account

  action-registry

  agent-server-responser

  agentserver

  aggregator

  asset-account

  asset-manager

  backup-operator

  collector

  comment
  ```

component

configuration

core

correlator

credentials

db-operator

decision-point

detects-processor

enricher

file-registry

gateway

gateway-operator

grafana

graph

hierman

iamoperator

istio-cni

istiod

kata-proxy

ksb-facade

ksc

ksc-info

ksc-tenant-binder

kscadapter

kubernetes-event-exporter

kube-state-metrics

kuma-operator

kuma-proxy

licensing-policy

local-path-provisioner

longhorn

loki

metallb

metrics

nats

ncircc

openbao

openbao-agent-injector

openbao-csi-provider

openbao-legacy-vault-csi-provider

operator

orchestra

osmp-scanner-facade

playbook-matcher

playbook-statistics

plugin-admin-agent

plugin-admin-server

plugin-agent-server

plugin-asset-management

plugin-enterprise

plugin-irp

plugin-kata

plugin-kes-linux

plugin-kesw

plugin-kuma

plugin-osmp-scanner

plugin-public-api-token-settings

plugin-spp

plugin-tenant-manager

plugin-tenant-roles

prevention-rules

prometheus-node-exporter

prometheus-redis-exporter

promtail

proxy

public-api

redis

reputation

response-manager

responser

rights

sandbox-scan-api

scan-rules-manager

scheduler

seaweedfs

secrets-store-csi-driver

ssh-remote-executor

storage

tenant-registry

tokenhub

tracker

```
transformer

unsealer

updater

updater-facade

victoria-metrics-operator

vmagent

vmalert

vmsingle

vtproxy

ztunnel
```

- `--auto-dest-dir`—获取日志并将其保存到在当前目录中自动创建的 kdt-default-logs-<当前日期和时间> 目录中。如果未指定日志记录周期，您将获取最近一小时的诊断信息。

  例如，如果您要获取管理服务器和 KUMA 过去一小时的日志，然后将这些日志保存到自动创建的目录中，请运行以下命令：

  ```
  ./kdt logs get --app ksc,core --auto-dest-dir
  ```

- `-d, --destination <` 文件路径 `>`—获取日志并将其保存到指定文件。

- `-D, --destination-dir <` 目录路径 `>`—获取日志并将其保存到指定目录（该目录必须提前创建）。如果 <directory_path> 为空，日志将保存在标准输出流（stdout）中。如果未指定日志记录周期，您将获取最近一小时的诊断信息。

- `--to-archive`—获取日志并将其保存到 kdt-default-logs-<当前日期和时间>.tar.gz 压缩文件中。所创建的压缩文件保存到当前目录。如果未指定日志记录周期，您将获取最近一小时的诊断信息。

- `--last=<` 小时 `>h`—获取截至当前为止指定小时数内的日志。

  例如，如果您要获取过去三小时包含日志的压缩文件，请运行以下命令：

  ```
  ./kdt logs get --to-archive --last=3h
  ```

- `--start=<` 日期和时间 `>`—获取从指定日期和时间（采用 Unix 时间戳格式）开始到当前时间，或到 `--end` 参数指定的日期和时间的日志。

  例如，如果您要获取从 2024/03/26 10:00:00 到现在的日志，然后将它们保存到当前目录中创建的 kdt-default-logs-<current_date_and_time> 目录中，请运行以下命令：

  ```
  ./kdt logs get --auto-dest-dir --start=1711447200
  ```

- `--end=<` 日期和时间 `>`—获取从 `--start` 参数指定的日期和时间开始，到 `--end` 参数指定的日期和时间（采用 Unix 时间戳格式）的日志。如果未指定 `--start` 参数，则获取 `--end` 参数指定的日期和时间前一小时的日志。

  例如，如果您要将 10 分钟（从 2024/03/26 10:00:00 到 2024/03/26 10:10:00）内的日志保存到日志目录，请运行以下命令：

  ```
  ./kdt logs get -D ./logs/ start=1711447200 --end=1711447800
  ```

要查看可用的日志记录参数，您可以运行以下命令之一：

- `./kdt logs get -h`
- `./kdt logs get --help`

查看 OSMP 指标

Kaspersky Next XDR Expert的可观察组件允许您查看OSMP指标，通过仪表板监控每个组件的状态，查看Kubernetes集群的数据存储系统（Longhorn）的指标，并在Kubernetes集群节点性能指标超过正常值时通过电子邮件通知用户。

您可以使用可观测组件监控指标，以便进一步分析其组件的可操作性和性能。

您可以通过以下方式之一查看 OSMP 指标：

- 使用 Grafana 控制板
- 使用您自己的监控工具

要使用 Grafana 控制板查看 OSMP 指标，请执行以下操作：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   其中，`<monitoring_host>` 是主机名，`<smp_domain>` 是域名。这些参数构成了 Kaspersky Next XDR Expert 监控服务的 FQDN，并在部署 Kaspersky Next XDR Expert 时在配置文件中设置。

2. 输入配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

或者，您可以在**控制板**部分查看OSMP指标：

1. 在主菜单中，转到"**监控**"部分。→ **控制板**，然后选择**检测和响应**选项卡。
2. 点击省略号（⋮）图标。
3. 单击"前往OSMP指标"按钮。

将显示 Grafana 界面。您可以查看每个Kaspersky Next XDR Expert组件的诊断信息，查看Kubernetes集群的数据存储系统（Longhorn）的指标，并配置有关Kubernetes集群运行状况事件的电子邮件通知。

要使用您自己的监控工具查看 OSMP 指标，请执行以下操作：

1. 配置您的监控工具以从 Kaspersky Next XDR Expert API 获取指标。
2. 前往 API 地址 `<api_host>.<smp_domain>/api/read-api` 以获取指标。

   其中，`<api_host>` 是主机名，`<smp_domain>` 是域名。这些参数构成提供 Kaspersky Next XDR Expert API 访问权限的服务提供商的 FQDN。这些参数在部署 Kaspersky Next XDR Expert 时在配置文件中设置。

OpenMetrics 格式的 OSMP 指标被获取。

如果要查看有关 KUMA Core 性能、存储、收集器和关联器的信息，则必须查看 KUMA 指标。

监控 Kaspersky Next XDR Expert 组件的状态

控制板以图形方式显示每个 Kaspersky Next XDR Expert 组件的状态。

例如，您可以查看以下组件参数：

- CPU 请求使用情况和限制
- CPU 和 RAM 请求使用情况
- 容器的 CPU 和 RAM 使用情况
- 容器的组件资源分配情况
- 网络性能指标：
  - 带宽
  - 数据包速率（接收到的数据包数量）
  - 丢包数（丢失的数据包数量）
  - 错误数（网络错误数量）

要在控制板查看诊断信息：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   其中，`<monitoring_host>` 是主机名，`<smp_domain>` 是域名。这些参数构成了 Kaspersky Next XDR Expert 监控服务的 FQDN，并在部署 Kaspersky Next XDR Expert 时在配置文件中设置。例如：`monitoring.smp.local`。

2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

3. 在菜单中，前往“**主页→控制板** → **Kubernetes/视图/Pods**”。

4. 在“**名字空间**”下拉列表中，选择要查看其诊断信息的组件。

5. 您还可以指定其他参数来自定义控制板视图。

   此时将显示包含所选 Kaspersky Next XDR Expert 组件诊断信息的控制板。

配置有关Kubernetes集群运行状况事件的电子邮件通知

Kaspersky Next XDR Expert的可观察组件允许您在Kubernetes集群节点性能指标超出正常值时通过电子邮件通知用户。电子邮件通知基于Grafana中的电子邮件通知规则生成。这些规则定义了通知消息、收件人以及发送电子邮件警报的条件。

您可以在Grafana中查看可用电子邮件通知规则的列表。规则可以是预定义的，也可以是自定义的。预定义规则由Kaspersky Next XDR Expert提供，无法更改。自定义规则可以创建、修改或删除。

用于生成电子邮件通知的预定义规则

Kaspersky Next XDR Expert包括以下预定义的规则，用于生成有关Kubernetes集群运行状况事件的电子邮件通知。您无法删除或编辑这些规则。

用于生成电子邮件通知的预定义规则

指标	严重级别	通知消息
CPU使用率过高	警告	<node_name>节点上的CPU使用率已超过警告阈值。这可能表明负载增加或CPU资源不足。
	严重	<node_name>节点的CPU使用率极高。这可能会导致CPU降频、Pod 调度问题以及集群组件性能下降。
磁盘I/O利用率过高	警告	<node_name>节点上的<disk_name>磁盘设备的I/O负载持续升高。应用程序可能会开始出现延迟。
	严重	<node_name>节点上的<disk_name>磁盘设备已过载。这可能会严重降低有状态应用程序的性能。
磁盘延迟过高	警告	<node_name>节点上的<disk_name>存储设备的读/写延迟已超过警告阈值。
	严重	<node_name>节点上的<disk_name>存储设备的I/O延迟极高。
磁盘使用率（文件系统）过高	警告	<node_name>节点上的<mountpoint_name>文件系统已达到高利用率。接近极限可能会影响日志记录、pod调度或kubelet稳定性。
	严重	<node_name>节点上的<mountpoint_name>文件系统几乎已满。这可能会导致写入错误、服务故障和节点不稳定。
内存使用率过高	警告	<node_name>节点上的内存使用率已超过警告阈值。工作负载可能会遇到内存压力。
	严重	<node_name>节点的内存即将耗尽。这可能会触发OOMKill或Pod驱逐。必须立即采取措施以防止工作负载故障。

若要查看用于生成电子邮件通知的预定义规则：

1. 转到 `<monitoring_host>.<smp_domain>` URL。

   其中，`<monitoring_host>` 是主机名，`<smp_domain>` 是域名。这些参数构成了 Kaspersky Next XDR Expert 监控服务的 FQDN，并在部署 Kaspersky Next XDR Expert 时在配置文件中设置。例如：`monitoring.smp.local`。

2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

3. 在菜单中，前往**主页→发送警报→警报规则**。

在**警报规则**部分中，会显示用于生成电子邮件通知的预定义规则列表。

用于生成电子邮件通知的自定义规则

您可以创建自己的规则，用于生成有关Kubernetes集群运行状况事件的电子邮件通知。

如果未在配置文件中指定 SMTP 服务器连接参数，则不会发送电子邮件通知：`grafana_smtp_host`、`grafana_smtp_user`、`grafana_smtp_password`、`grafana_smtp_bundle`、`grafana_smtp_skip_verify`、`grafana_smtp_from_address`、`grafana_smtp_from_name`、`grafana_smtp_ehlo_identity`、`grafana_starttls_policy`、`grafana_smtp_enable_tracing`。如果在部署Kaspersky Next XDR Expert之前没有在配置文件中指定这些参数，您可以稍后添加它们。

若要创建用于生成电子邮件通知的自定义规则：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   其中，`<monitoring_host>` 是主机名，`<smp_domain>` 是域名。这些参数构成了 Kaspersky Next XDR Expert 监控服务的 FQDN，并在部署 Kaspersky Next XDR Expert 时在配置文件中设置。例如：`monitoring.smp.local`。

2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

3. 在菜单中，前往**主页→发送警报→警报规则**。

4. 在**警报规则**部分中，点击**新建警报规则**，然后指定新电子邮件通知规则的参数。

5. 指定规则参数后，点击**保存规则并退出**。

自定义规则随即创建。您还可以创建文件夹并将创建的规则放在其中。

若要创建用于从控制板生成电子邮件通知的自定义规则：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

3. 在菜单中，转到**主页→控制板**。

4. 在控制板列表中，单击包含您要用于警告的性能指标的控制板名称。

   控制板随即打开。

5. 单击控制板所需面板上的**菜单**图标（⋮），然后在上下文菜单中，选择**更多...→新的警报规则**。

6. 在**新建警报规则**面板中，指定新电子邮件通知规则的参数。

7. 点击**保存规则并退出**。

控制板中的自定义规则随即创建。

若要编辑或删除用于生成电子邮件通知的自定义规则：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

3. 在菜单中，前往**主页→发送警报→警报规则**。

4. 在**警报规则**部分中，找到所需的规则，然后执行以下操作之一：

   - 若要编辑规则，请点击铅笔按钮，然后更改规则参数。
   - 若要删除该规则，请点击**更多**，然后点击**删除**。

自定义规则随即更改或删除。

管理Kubernetes集群运行状况事件的电子邮件通知收件人

Kaspersky Next XDR Expert允许您指定、编辑和删除通知收件人电子邮件地址。

如果未在配置文件中指定 SMTP 服务器连接参数，则不会发送电子邮件通知：`grafana_smtp_host`、`grafana_smtp_user`、`grafana_smtp_password`、`grafana_smtp_bundle`、`grafana_smtp_skip_verify`、`grafana_smtp_from_address`、`grafana_smtp_from_name`、`grafana_smtp_ehlo_identity`、`grafana_starttls_policy`、`grafana_smtp_enable_tracing`。如果在部署Kaspersky Next XDR Expert之前没有在配置文件中指定这些参数，您可以稍后添加它们。

若要添加通知收件人电子邮件地址：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   其中，`<monitoring_host>` 是主机名，`<smp_domain>` 是域名。这些参数构成了 Kaspersky Next XDR Expert 监控服务的 FQDN，并在部署 Kaspersky Next XDR Expert 时在配置文件中设置。例如：`monitoring.smp.local`。

2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。

3. 在菜单中，转到**主页→发送警报→联络点**。

4. 在**联络点**工作区中，点击**添加联络点**，然后指定以下收件人参数：

   - **名称**— 收件人或收件人群组的名称。必填字段。
   - **集成**— 集成类型。使用电子邮件接收邮件通知。
   - **地址**— 一个或多个收件人的电子邮件地址。地址可以用逗号、换行符（`\n`）或分号分隔。
   - **单封邮件**— 可选择向所有收件人群发一封邮件。可能的参数值：
     - **已启用**— 所有收件人将收到一封电子邮件通知。
     - **已禁用**— 每个收件人都会收到单独的电子邮件通知。
   - **消息**— 电子邮件正文。您可以使用模板，也可以点击**编辑消息**设置自定义文本。
   - **主题**— 电子邮件主题。您可以使用模板，也可以点击**编辑主题**设置自定义文本。
   - **通知设置**— 常规通知设置。
   - **禁用已解决消息**— 禁用在问题或警报解决时发送消息。
   - **测试**— 发送测试通知。允许检查设置是否正确。
   - **复制**— 创建联络点配置的副本。可以快速创建类似的联络点。
   - **删除**— 正在删除当前联络点配置。

5. 点击**保存联络点**。

若要编辑或删除通知收件人电子邮件地址：

1. 前往 `<monitoring_host>.<smp_domain>` URL。
2. 输入您在配置文件中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password` 参数）。
3. 在菜单中，转到**主页→发送警报→联络点**。
4. 在**联络点**工作区中，找到所需的联络点，然后执行以下操作之一：
   - 若要编辑规则，请点击铅笔按钮，然后更改规则参数。
   - 若要删除该规则，请点击**更多**，然后点击**删除**。

联络点随即更改或删除。

在不重新安装Kaspersky Next XDR Expert的情况下，将SMTP服务器连接参数添加到配置文件

若要在不重新安装Kaspersky Next XDR Expert的情况下，将SMTP服务器连接参数添加到配置文件：

1. 在管理员主机上，导出当前配置文件。
2. 在导出的配置文件中，在 `parameters` 部分添加并指定以下参数：`grafana_smtp_host`、`grafana_smtp_user`、`grafana_smtp_password`、`grafana_smtp_bundle`、`grafana_smtp_skip_verify`、`grafana_smtp_from_address`、`grafana_smtp_from_name`、`grafana_smtp_ehlo_identity`、`grafana_starttls_policy`、`grafana_smtp_enable_tracing`。
3. 使用以下命令应用参数更改：

   ```
   ./kdt apply -i '< 更新后的配置文件的完整路径 >'
   ```

SMTP服务器连接参数随即添加到配置文件中。

查看 Longhorn 指标

Kaspersky Next XDR Expert 包含一个控制板，用于显示集群数据存储系统（Longhorn）的关键指标。Longhorn 控制板可以监控数据存储的运行状况和性能。

默认情况下，控制板显示过去三小时的数据。您可以更改此时间段。控制板每 15 秒刷新一次。

要查看 Longhorn 控制板：

1. 转到 `<monitoring_host>.<smp_domain>`。

   `<monitoring_host>`表示主机名，`<smp_domain>`表示域名。它们共同构成了Kaspersky Next XDR Expert监控服务的FQDN，并在Kaspersky Next XDR Expert部署期间在配置文件中指定。
2. 输入您在 配置文件 中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password`）。
3. 在菜单中，转到 **首页 → 控制板 → Longhorn 控制板**。

Longhorn 控制板显示出来。

Longhorn 控制板指标描述如下。

节点

- **节点** – 系统中的节点总数。
- **可调度节点** – 可用于分发卷副本的节点数量。
- **已禁用节点** – 用户禁用的节点。
- **故障节点** – 无响应、离线或无法使用的节点。

卷

- **附加卷** – 当前附加到节点的卷。
- **分离卷** – 未附加到节点的卷。
- **降级卷** – 副本数量不足的卷。
- **故障卷** – 没有正常工作的副本的卷。

容量

- **节点容量** – 每个节点上的总存储容量。
- **磁盘容量** – 每个磁盘上的存储容量。
- **卷容量** – 每个卷的容量。

资源使用率

- **节点存储使用率/容量** – 每个节点上存储容量的百分比。
- **磁盘空间使用率** – 每个磁盘容量的百分比。
- **每个节点的卷数** – 每个节点上挂载的卷数。
- **卷大小/容量**–当前容量/最大容量比。
- **卷写入吞吐量** – 系统每秒写入的数据量 (bps)。
- **卷读取吞吐量** – 系统每秒读取的数据量 (bps)。
- **卷写入 IOPS** – 写入输入/输出操作数 (IOPS)，即操作员每秒执行的写入操作次数。
- **卷读取 IOPS** – 读取输入/输出操作数 (IOPS)，即操作员每秒执行的读取操作次数。
- **卷写入延迟** – 完成单次写入操作所需的时间（纳秒）。
- **卷读取延迟** – 完成单次读取操作所需的时间（纳秒）。
- **节点CPU使用率/容量** – 每个节点的CPU利用率百分比。
- **节点内存使用率/容量** – 每个节点的内存利用率百分比。

- **Longhorn 管理器 CPU 使用率** — Longhorn 管理器的 CPU 负载（milliCPU）。
- **Longhorn 管理器内存使用率** — Longhorn 管理器的内存负载。
- **实例管理器 CPU 使用率** — Longhorn 实例的 CPU 负载（毫 CPU）。
- **实例内存使用率** — Longhorn实例使用的内存。

磁盘使用

磁盘使用率面板上的指标显示磁盘读取和写入时间的百分比。这些指标基于以下指标：

- `longhorn_volume_read_iops`
- `longhorn_volume_read_latency_seconds`
- `longhorn_volume_write_iops`
- `longhorn_volume_write_latency_seconds`

查看EDR控制板和指标

Kaspersky Next XDR Expert包含EDR控制板，可显示负责处理端点代理程序对象的组件的关键指标。监控这些指标有助于确保组件平稳安全地运行，从而采取主动措施来预防潜在问题。

下列控制板可用：

- EDR代理程序服务器
- EDR KSB
- EDR KSN代理
- EDR沙盒
- EDR扫描程序

若要查看EDR控制板：

1. 转到 `<monitoring_host>.<smp_domain>`。

   `<monitoring_host>`表示主机名，`<smp_domain>`表示域名。这些参数构成了Kaspersky Next XDR Expert监控服务的FQDN，并在部署 Kaspersky Next XDR Expert时在配置文件中设置。

2. 输入您在 配置文件 中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password`）。
3. 在菜单中，转到**主页→控制板**。
4. 在标签筛选下拉菜单（**按标签筛选**）中，选择**edr**标签。

   可用的EDR控制板列表随即显示。

5. 点击要查看的控制板名称。

选定的控制板随即打开。

每个EDR控制板中可用的小部件和指标如下所述。

EDR代理服务器

默认情况下，控制板显示最近2天的数据。您可以点击页面顶部的**最近2天**并选择其他时间段来更改时间段。

EDR代理服务器小部件和指标

小部件名称	指标名称	描述
任务数	xdr_agentserver_tasks_total	从事故响应平台收到的任务总数。
设置	xdr_agentserver_settings_total	从事故响应平台收到的配置总数。
活动任务数	xdr_agentserver_tasks_active	正在进行的任务总数。
活动设置数	xdr_agentserver_settings_active	正在进行的配置申请总数。
任务错误数	xdr_agentserver_tasks_errors_total	完成任务时出错的任务总数。
设置错误数	xdr_agentserver_settings_errors_total	配置应用程序错误总数。
对象存储	xdr_agentserver_objectstorage_upload_errors_total	对象存储中的文件上传错误总数。
对象存储数	xdr_agentserver_objectstorage_download_errors_total	对象存储中的文件下载错误总数。
代理程序信息更新数	xdr_agentserver_agentinfo_updates_total	端点代理程序信息更新并发送到资产管理器的总次数。
资产解决错误数	xdr_agentserver_assets_resolve_errors_total	在OSMP和端点代理之间映射ID时的错误总数。
资产数	xdr_agentserver_assets_resolve_total	解决方案总数。
代理服务器速率超限	xdr_agentserver_rate_limit_exceeded_total	超过限速的案例总数。
代理程序验证	xdr_agentserver_agent_auth_total	端点代理程序身份验证尝试总数。
代理程序验证数	xdr_agentserver_agent_auth_errors_total	端点代理程序身份验证错误总数。
Vtproxy会话数	xdr_agentserver_vtproxy_sessions_total	创建的会话总数。
Vtproxy验证错误数	xdr_agentserver_vtproxy_auth_errors_total	会话身份验证错误总数。
Vtproxy验证成功数	xdr_agentserver_vtproxy_successful_auths_total	成功会话认证总数。
Vtproxy传感器活动会话数	xdr_agentserver_vtproxy_sensor_session_active	传感器的活动会话数。
Vtproxy活动会话数	xdr_agentserver_vtproxy_sessions_active	活动会话的数量。
Vtproxy会话持续时间	xdr_agentserver_vtproxy_session_duration_seconds	会话持续时间（以秒为单位）。
Vtproxy传输字节数	xdr_agentserver_vtproxy_bytes_transferred_total	传输的总字节数。

EDR KSB

默认情况下，控制板显示最近2天的数据。您可以点击页面顶部的**最近2天**并选择其他时间段来更改时间段。

EDR KSB小部件和指标

小部件名称	指标名称	描述
多任务数	xdr_ksb_multitasks_total	扫描任务总数。
活动多任务数	xdr_ksb_multitasks_active	活动扫描任务数。
多任务重复数	xdr_ksb_multitask_duplicates_total	重复扫描任务数。

小部件名称	指标名称	描述
多任务文件重复数	xdr_ksb_multitask_file_duplicates_total	扫描任务中的重复文件数量。
多任务文件大小	xdr_ksb_multitask_files_size_bytes_total	多任务文件的大小（以字节为单位）。
代理程序验证失败数	xdr_ksb_agent_auth_failures_total	端点代理程序验证失败的数量。
速率超限	xdr_ksb_rate_limit_exceeded_total	超过限速的案例总数。

EDR KSN代理

默认情况下，控制板显示最近6小时的数据。您可以点击页面顶部的**最近6小时**，并选择其他时间段来更改时间段。

EDR KSN代理小部件和指标

小部件名称	指标名称	描述
统计信息消息	xdr_scanner_ksnproxyfacade_stats_messages_total	统计信息的消息总数。
集成模式变更数	xdr_scanner_ksnproxyfacade_integration_mode_changes_total	集成类型变更总数。
KSN代理启动数	xdr_scanner_ksnproxysupervisor_ksnproxy_starts_total	KSN代理启动总数。
KSN代理启动错误数	xdr_scanner_ksnproxysupervisor_ksnproxy_start_errors_total	KSN代理启动错误总数。
KSN可用性	xdr_scanner_ksnproxy_ksn_proxy_ksn_available	KSN可用性。
KSN心跳请求失败数	xdr_scanner_ksnproxy_ksn_proxy_ksn_heartbeat_failed_requests_total	失败的心跳请求总数。
KSN心跳请求数	xdr_scanner_ksnproxy_ksn_proxy_ksn_heartbeat_requests_total	同步请求总数

EDR沙盒

默认情况下，控制板显示最近6小时的数据。您可以点击页面顶部的**最近6小时**，并选择其他时间段来更改时间段。

要查看特定沙盒的指标，请在顶部的**沙盒**菜单中选择其IP地址。

EDR沙盒小部件和指标

小部件名称	指标名称	描述
开始时间 正常运行时间	xdr_scanner_sb_process_start_time_seconds	沙盒进程启动时间及其正常运行时间，以秒为单位。
沙盒上次运行状况检查 沙盒运行状况检查错误数	xdr_scanner_sb_health_check_errors_current	上次运行状况检查的时间和当前检测到的错误数量。
沙盒数据库年龄	xdr_scanner_sb_health_bases_age_seconds	沙盒中病毒数据库的年龄，以秒为单位
CPU数	xdr_scanner_sb_process_cpu_seconds_total	使用的CPU内核数量。
内存：使用情况	xdr_scanner_sb_go_memstats_sys_bytes	向系统请求的内存大小（以字节为单位）。
内存使用率	xdr_scanner_sb_go_memstats_heap_inuse_bytes	堆内存使用量（以字节为单位）。
内存使用率	xdr_scanner_sb_go_memstats_stack_inuse_bytes	使用的栈内存量（以字节为单位）。
内存使用率	xdr_scanner_sb_process_resident_memory_bytes	常驻内存（RSS），以字节为单位。
磁盘写入/读取数	xdr_scanner_sb_node_disk_read_bytes_total	从磁盘读取的总字节数。
磁盘写入/读取数	xdr_scanner_sb_node_disk_written_bytes_total	写入磁盘的总字节数。

小部件名称	指标名称	描述
网络使用情况	xdr_scanner_sb_process_network_receive_bytes_total	入站的流量。
网络使用情况	xdr_scanner_sb_process_network_transmit_bytes_total	出站的流量。
恶意软件渠道可用性	xdr_scanner_sbscanapi_sb_malware_channel_availability	特定沙盒的恶意软件通道可用性。
沙盒镜像状态	xdr_scanner_sb_vm_images_status	沙盒中虚拟机的当前状态，指示是否安装了操作系统。
沙盒镜像版本状态	xdr_scanner_sb_vm_image_version_status	虚拟机上使用的镜像版本的状态，指示每个版本是否正确。

EDR扫描程序

默认情况下，控制板显示最近2天的数据。您可以点击页面顶部的**最近2天**并选择其他时间段来更改时间段。

在顶部的**"扫描引擎"**菜单中，选择扫描引擎以查看其指标：

- **AM**：反恶意软件引擎指标
- **YARA**：YARA指标
- **SB**：沙盒指标

EDR扫描程序小部件和指标

小部件名称	指标名称	描述
上次数据库更新时间	xdr_scanner_updater_updater_bases_age	更新程序数据库的年龄。
上次数据库更新时间	xdr_scanner_updater_updater_retranslation_age	更新程序重译的年龄。
上次数据库更新时间	xdr_scanner_internalscanner_am_bases_age	反恶意软件引擎的防病毒数据库的年龄。
上次数据库更新时间	xdr_scanner_sb_health_bases_age_seconds	沙箱中防病毒数据库上次更新至今所经过的时间，以秒为单位）。
AM扫描引擎完成 SB扫描引擎完成 YARA扫描引擎完成	xdr_scanner_internalscanner_scan_engine_complete_total	每个扫描引擎的已完成扫描任务总数及对象扫描结果。
扫描运行状况	xdr_scanner_internalscanner_total_scans	扫描的数量。
扫描运行状况	xdr_scanner_internalscanner_failed_scans	扫描的失败次数。
恶意软件扫描任务数	xdr_scanner_internalscanner_am_queue_len	反恶意软件引擎队列中的作业数。
恶意软件扫描任务数	xdr_scanner_internalscanner_am_queue_total_items	所有反恶意软件软件引擎队列中的任务总数。
恶意软件扫描任务数	xdr_scanner_internalscanner_am_queue_failed_items_total	反恶意软件引擎队列中失败任务的总数。
AM队列大小	xdr_scanner_internalscanner_am_queue_size	反恶意软件引擎队列使用的文件系统大小。
反恶意软件队列大小	xdr_scanner_internalscanner_am_storage_size_limit	反恶意软件引擎队列允许的最大大小。
恶意软件扫描任务数	xdr_scanner_internalscanner_sb_wait_queue_len	OSMP扫描程序中沙盒队列中的作业数。
SB扫描任务数	xdr_scanner_internalscanner_sb_queue_total_items	沙盒队列中所有任务的总数。
SB扫描任务数	xdr_scanner_internalscanner_sb_queue_failed_items_total	沙盒队列中任务失败的总数。

小部件名称	指标名称	描述
SB扫描任务数	xdr_scanner_internalscanner_sb_queue_len	沙盒队列中的任务数。
SB队列大小	xdr_scanner_internalscanner_sb_queue_size	沙盒队列中数据（样本）的大约大小。
SB队列大小	xdr_scanner_internalscanner_sb_storage_size_limit	沙盒队列允许的最大大小。
沙盒平均扫描时间	xdr_scanner_sbscanapi_sb_scan_time_total	沙盒扫描总时间。
沙盒平均扫描时间	xdr_scanner_sbscanapi_sb_scan_count_total	沙盒上的扫描总数。
YARA扫描任务数	xdr_scanner_internalscanner_yr_queue_len	YARA队列中的作业数。
YARA队列大小	xdr_scanner_internalscanner_yr_queue_size	YARA队列使用的文件系统大小。
YARA队列大小	xdr_scanner_internalscanner_yr_storage_size_limit	最大YARA队列大小。
YARA扫描任务数	xdr_scanner_internalscanner_yr_queue_total_items	所有YARA队列中的任务总数。
YARA扫描任务数	xdr_scanner_internalscanner_yr_queue_failed_items_total	YARA队列中任务失败的总数。
上次数据库更新时间	xdr_scanner_internalscanner_am_bases_age	反恶意软件引擎的防病毒数据库的年龄。

查看Node Exporter完整版控制板

Node Exporter完整版控制板显示集群节点性能的关键指标。

若要查看Node Exporter完整版控制板：

1. 转到 `<monitoring_host>.<smp_domain>`。

   `<monitoring_host>`表示主机名，`<smp_domain>`表示域名。这些参数构成了Kaspersky Next XDR Expert监控服务的FQDN，并在部署 Kaspersky Next XDR Expert时在配置文件中设置。

2. 输入您在 配置文件 中指定的 Grafana 凭据（`grafana_admin_user` 和 `grafana_admin_password`）。

3. 在菜单中，转到**主页→控制板**。

4. 点击**Node Exporter完整版**。

   控制板随即打开。

默认情况下，控制板显示最近24小时的数据。您可以点击页面顶部的**“最近24小时”**并选择其他时间段来更改时间段。

下表描述了控制板中可用的面板。

Node Exporter完整版面板

面板	描述
CPU/内存/磁盘概览	主要资源的概览：CPU负载、内存使用情况和磁盘使用情况。
压力	压力阻塞信息（PSI）：CPU、内存和输入/输出。显示系统负载情况。
CPU繁忙情况	处理器忙于计算的时间百分比（用户时间 + 系统时间）。
系统负载	1分钟、5分钟和15分钟内的平均系统负载（平均负载）。
RAM使用情况	已使用的RAM，包括缓冲区和缓存。
交换空间使用情况	已使用的交换空间。
根文件系统使用情况	根文件系统 (/) 上使用的空间。

面板	描述
CPU内核数	节点上的核心数（vCPU）。
正常运行时间	自上次系统启动以来经过的时间。
RootFS总大小	根文件系统总大小。
RAM总量	RAM总量。
交换空间总量	可用交换内存总量。
CPU/内存/网络/磁盘概览	CPU、内存、网络和磁盘关键指标概览。
CPU概览	基本CPU负载面板，包括用户/系统/空闲/iowait指标。
内存：概览	主内存和交换空间使用情况指标。
网络流量：概览	按接口统计的网络总流量（入站/出站）。
磁盘空间使用情况概览	磁盘空间使用情况和分区情况。
CPU	详细的CPU使用率指标（按核心统计，以百分比表示）。
内存：栈内存	内存层使用情况图（已用、缓存、缓冲区、可用）。
网络流量	按接口统计的总网络流量（字节/秒）。
磁盘空间使用情况	按分区统计的详细磁盘空间使用情况。
磁盘操作次数	每秒输入/输出操作次数（每秒输入/输出数）。
输入/输出使用情况：读/写	磁盘数据读写速度（字节/秒）。
输入/输出使用率	存储设备的使用率：磁盘忙于输入/输出的时间百分比。
来宾（虚拟机）中的CPU耗时（秒）：	CPU运行来宾虚拟机（来宾时间）所花费的时间。
内存：活动/非活动	活动和非活动内存页（已用和潜在可回收）。
内存：提交情况	分配给进程的内存量（包括超额提交）。
内存：活动/非活动详情	活动和非活动分页的详细信息，包括匿名页/文件页。
内存回写页数和脏页数	等待写入磁盘的分页数（脏页、回写页）。
内存：共享和映射	共享和映射的内存。
内存：Slab	分配给内核对象的内存（Slab，可回收/不可回收）。
内存：Vmalloc	内核虚拟内存分配情况。
内存：跳出率	弹出页的数量（很少见，适用于旧硬件）。
内存：匿名	匿名内存（不支持文件）。
内核/CPU内存	内核和CPU结构使用的内存。
内存：大页计数器	已使用的大页（HugePages）数量。
内存：大页大小	大内存页的大小和状态。
内存：直接映射	物理内存的直接映射（DirectMap）。
内存：不可驱逐和锁定	RAM中锁定的内存（锁定，不可驱逐）。
内存：NFS	NFS子系统使用的内存。
内存：Meminfo	proc/meminfo的摘要信息。
内存：分页输入/输出数	加载/卸载到内存中的分页数。
内存：分页交换输入/输出数	在RAM和交换空间之间移动的页数。
内存：分页错误数	分页错误（次要错误/主要错误）的数量。
OOM Killer	系统因内存不足而终止进程的事件。
内存：Vmstat	扩展虚拟内存统计信息（/proc/vmstat）。
时间同步漂移	系统时间与同步源之间的差异。
时间PLL调整	时间调整参数（PLL、偏移量）。

面板	描述
时间同步状态	时间同步状态（例如，chrony/ntpd）。
时间其他指标	其他与时间相关的指标（偏移量、抖动）。
系统时间同步	节点上的整体时间同步状态。
进程状态	按状态统计的进程统计信息（运行、睡眠、僵尸进程）。
进程状态直方图	进程状态的分布图。
进程分支数	创建的进程数（分支）。
内存：进程	进程的内存使用情况。
PID数量和限制	系统中当前和最大的PID数量。
进程调度统计信息：运行/等待	按"运行"和"等待"状态进行进程分布。
线程数量和限制	线程数和系统限制。
上下文切换/中断数	上下文切换和硬件中断数量。
系统负载	1分钟、5分钟和15分钟的平均负载。
CPU频率调节	当前CPU频率和调节设置（调速器、最小值/最大值）。
压力阻塞信息	CPU、内存和输入/输出压力 - 显示任务延迟数。
中断详情	中断类型的详细分类。
每个CPU执行的调度时间片	每个核心执行的时间片数量。
熵	可用熵（随机数生成质量）。
CPU在用户和系统上下文中花费的时间	CPU在用户和系统模式下花费的总时间。
文件描述符数	打开的文件描述符数量。
硬件温度监控	系统组件（CPU、磁盘、传感器）的温度。
节流阀冷却装置	冷却系统状态和节流情况。
电源	电源数据（电压、电流、电池）。
Systemd套接字数	活动systemd套接字的数量。
系统单元状态	systemd单元的状态（活动、失败、非活动）。
磁盘操作完成数	完成的输入/输出操作数。
磁盘读/写数据	读取/写入的数据量。
磁盘平均等待时间	输入/输出平均等待时间。
队列平均大小	输入/输出队列的平均长度。
合并的磁盘读/写数	合并的读/写操作次数。
输入/输出操作耗时	输入/输出操作所花费的时间。
瞬时队列大小	当前输入/输出队列的长度。
完成/合并的磁盘输入/输出操作丢弃数	完成/合并的丢弃（TRIM）操作数。
可用文件系统空间	文件系统上的可用空间。
文件节点空闲数	空闲inode的数量。
文件描述符数	文件描述符的数量。
文件节点大小	inode表的大小。
文件系统：只读/错误状态	文件系统状态（错误、只读挂载）。
网络流量：数据包	各接口接收/发送数据包的数量。
网络流量：错误数	传输和接收错误的数量。
网络流量：丢包率	丢包率。
网络流量：压缩	压缩的流量

面板	描述
组播的网络流量	组播的流量。
网络流量：Fifo	接口上的FIFO错误数。
网络流量：帧	帧的错误数。
网络流量：载波	链路级错误数（载波）。
网络流量：冲突	网络冲突。
NF连接跟踪数	跟踪的网络连接数（conntrack）。
ARP条目	ARP表（条目数）。
MTU	最大数据包大小（MTU）。
速度	网络接口速度（比特/秒）。
队列长度	接口数据包队列长度。
Softnet数据包	Softnet数据包处理（内核）。
Softnet超出配额	由于Softnet络溢出而丢包。
网络运行状态	当前接口状态（开启/关闭）。
Sockstat TCP / UDP / FRAG / RAW	TCP、UDP和其他协议套接字的统计信息。
内存：Sockstat大小/已使用	按套接字划分的内存使用情况和活动套接字数量。
Netstat IP：输入/输出字节数	传入/传出的IP数据包数量（以字节为单位）。
Netstat IP：转发	IP转发状态。
ICMP：输入/输出/错误数	ICMP数据包和错误统计信息。
UDP：输入/输出/错误数	UDP数据包和错误统计信息。
TCP：连接/输出/错误数	TCP流量和错误数。
TCP：连接数	按状态统计的TCP活动连接数。
TCP：SynCookie/直接转换/状态	SYN cookie保护、TCP状态直接转换和TCP统计信息。
Node Exporter：抓取时间/抓取	Node Exporter的性能，重点关注抓取持续时间和目标状态。

服务监控

您可以使用以下功能来监控除冷存储和代理程序之外的所有服务的状态：

- 查看VictoriaMetrics警报
  具有主管理员角色的用户可以为 KUMA 服务配置阈值；如果超过指定阈值，则会发生以下变化：
  - KUMA记录了一条审计事件：VictoriaMetrics警报已注册为服务。
  - KUMA 会向主管理员发送通知电子邮件。
  - 服务会在**活动服务**部分显示为黄色状态。将鼠标悬停在状态图标上，即可显示错误信息。
    可能的服务状态
    - 绿色表示服务正在运行，并且可以从Core服务器访问。
    - 红色表示服务未运行，或无法从Core服务器访问。

- 黄色是适用于所有服务（代理除外）的状态。黄色状态表示服务正在运行，但服务日志中存在错误，或者有来自VictoriaMetrics的服务警报。您可以通过将鼠标光标悬停在**活动服务**部分的服务状态上来查看错误消息。

- 紫色是适用于正在运行服务的状态，这些服务在数据库中的配置文件已被更改，但不存在其他错误。若服务的配置文件不正确并且存在错误（例如来自 Victoria Metrics 的错误），则该服务的状态为黄色。

- 灰色表示，若已删除的租户中存在仍在运行的服务，则该服务在"活动服务"页面上将显示为灰色状态。当您删除租户时，灰色状态的服务会保留，以便您复制ID并删除服务器上的服务。只有主管理员可以删除灰色状态的服务。删除租户后，该租户的服务将分配给主租户。

- 如果用户拥有具备指标访问权限的角色，则可查看 VictoriaMetrics 指标。

以下示例展示了如何监控服务状态。

1. 如果收集器服务在**活动服务**部分中显示为黄色状态，并且看到**增强错误增加**的消息，您可以：

   - 前往**监控→指标→**<服务类型>→<服务名称>→**增强 → 错误**部分，找到状态为黄色的服务，找出导致错误的增强功能，并查看图表，了解问题是何时开始和怎么演变的。

   - 增强错误的可能原因可能是DNS服务器不可用或CyberTrace增强错误，因此您可以检查您的DNS或CyberTrace连接设置。

2. 如果收集器服务在**活动服务**部分中显示为黄色状态，并且您看到**输出事件丢失不断增加**消息，您可以：

   - 前往**监控→指标→**<服务类型>→<服务名称>→**输入/输出→输出事件丢失**部分，找到显示为黄色状态的服务，并查看图表，了解问题是何时开始和如何演变的。

   - 导致数据增强错误的可能原因是缓冲区溢出或目标不可用，因此您可以检查目标的可用性和连接情况，或者找出缓冲区容量超出限制的原因。

配置服务监控

若要配置服务监控：

1. 在应用程序主窗口中，转到**设置→KUMA→ 打开 KUMA 设置**部分。

   这将打开 KUMA 设置窗口。

2. 在"其他"下，点击**服务监控**。

   这将打开**服务监控**窗口。

3. 指定各项服务的监控参数值。

   服务监控不适用于冷存储。

   如果指定了不符合范围或格式的无效值，则该值将重置为先前配置的值。

4. 单击"**保存**"。

   保存参数后，KUMA会记录一个审计事件：监控服务更改的阈值。

KUMA根据指定的参数监控服务状态。

在**活动服务**部分，您可以按状态筛选服务，或者在搜索字段中输入错误文本中的单词，例如“QPS”或“缓冲区”，然后按回车键。这将生成一个包含错误服务的列表。请勿在搜索字段中使用特殊字符 "、}、{。这会导致搜索结果错误。

禁用服务监控

若要禁用服务监控：

1. 在应用程序主窗口中，转到**设置**→KUMA→ **打开** KUMA **设置**部分。

   这将打开 KUMA 设置窗口。

2. 在“其他”下，点击**服务监控**。

   这将打开**服务监控**窗口。

3. 如果您想仅针对收集器禁用服务监控，请在**服务监控。阈值设置**设置窗口的**收集器**下，选中**停用连接器错误**复选框。

   这将仅禁用对收集器的**连接器错误**指标的分析。

4. 如果您想禁用所有服务的监控，请在“**服务监控。阈值设置**设置中选中**禁用**复选框。

KUMA服务监控随即禁用，服务不会显示黄色状态。

查看 KUMA 指标

为了监控其组件、事件流和关联上下文的性能，KUMA 收集并存储了大量参数。VictoriaMetrics 时间序列数据库用于收集、存储和分析这些参数。收集到的指标通过 Grafana 进行可视化。用于可视化各种 KUMA 组件关键性能参数的仪表板位于 **监控** → **指标** 部分。
KUMA Core 服务会自动配置 VictoriaMetrics 和 Grafana，无需用户操作。

或者，您可以在**控制板**部分查看KUMA指标：

1. 在主菜单中，转到“**监控**”部分。→ **控制板**，然后选择**检测和响应**选项卡。

2. 点击省略号（ ⋮ ）图标。

3. 单击**前往KUMA指标**按钮。

收集到的指标使用 Grafana 解决方案进行可视化。“kuma-core”服务的 RPM 包会生成 Grafana 配置，并创建一个单独的仪表板来对每个服务的指标进行可视化展示。“**指标**”部分中的图大约会延迟 1.5 分钟显示。

有关指标的完整信息，请参阅 OSMP Console 的“**指标**”部分。选择此部分将打开随 KUMA Core 一同部署并自动更新的 Grafana 门户。如果“**Metrics**”部分显示 core: <端口号>，则表示 KUMA 部署在高可用性配置中，并且指标是从**安装 Core** 的主机接收的。在其他配置中，将显示 KUMA 接收指标的主机名称。

要确定 Core 在哪个主机上运行，请在其中一个控制器的终端中运行以下命令：

```
k0s kubectl get pod -n kuma -o wide
```

收集器指标

指标名称	描述
IO – 与服务输入和输出相关的指标。	
处理 EPS	每秒处理的事件数量。
输出 EPS	每秒发送至目标位置的事件数。
输出延迟	发送事件包和从目标位置接收响应所经过的时间（以毫秒为单位）。显示中值。
输出错误	事件包发送到目标位置时每秒发生的错误数。网络错误和写入目标位置磁盘缓冲区的错误分别显示。
输出事件丢失	每秒丢失的事件数量。事件可能由于网络错误或写入目标位置磁盘缓冲区的错误而丢失。如果目标位置响应错误代码（例如，在出现无效请求的情况下），事件也会丢失。
输出磁盘缓冲区大小	与目标位置关联的收集器的磁盘缓冲区大小（以字节为单位）。如果显示零值，则表示收集器的磁盘缓冲区中没有放置事件包，且服务运行正常。
写入网络 BPS	每秒接收到网络的字节数。
连接器错误	连接器日志中的错误数量。

规范化 – 与规范化器相关的指标。	
原始事件和规范化事件的大小	原始事件的大小和规范化事件的大小。显示中值。
错误	每秒规范化错误的数量。

过滤––与过滤器相关的指标。	
EPS	每秒内匹配过滤条件并被发送至处理流程的事件数量。仅当用户已将过滤器添加到收集器服务配置中时，收集器才会处理符合过滤条件的事件。

聚合––与聚合规则相关的指标。	
EPS	聚合规则每秒接收和生成的事件数。此指标有助于确定聚合规则的有效性。
存储桶	聚合规则中的存储桶数量。

增强 – 与增强规则相关的指标。	
缓存 RPS	每秒向本地缓存发送的请求数。
源 RPS	每秒向增强数据源（如字典）发送的请求数。
源延迟	向增强数据源发送请求并从其接收响应所经过的时间（以毫秒为单位）。显示中值。

队列	增强请求队列的大小。此指标有助于查找瓶颈增强规则。
错误	向增强数据源发送请求时每秒出现的错误数。

关联器指标

指标名称	描述
IO – 与服务输入和输出相关的指标。	
处理 EPS	每秒处理的事件数量。
输出 EPS	每秒发送至目标位置的事件数。
输出延迟	发送事件包和从目标位置接收响应所经过的时间（以毫秒为单位）。显示中值。
输出错误	事件包发送到目标位置时每秒发生的错误数。网络错误和写入目标位置磁盘缓冲区的错误分别显示。
输出事件丢失	每秒丢失的事件数量。事件可能由于网络错误或写入目标位置磁盘缓冲区的错误而丢失。如果目标位置响应错误代码（例如，在出现无效请求的情况下），事件也会丢失。
输出磁盘缓冲区大小	与目标位置关联的收集器的磁盘缓冲区大小（以字节为单位）。如果显示零值，则表示收集器的磁盘缓冲区中没有放置事件包，且服务运行正常。

关联 – 与关联规则相关的指标。	
EPS	关联规则每秒生成的关联事件数量。
存储桶	标准类型关联规则中的存储桶数量。
限流触发次数	每秒关联规则超过速率限制的次数。
活动列表 OPS	每秒发送到活动列表的操作请求数及其操作。
活动列表记录	活动列表中的记录数。
活动列表的磁盘大小	磁盘上活动列表的大小（以字节为单位）。

丰富 – 与丰富规则相关的指标。	
缓存 RPS	每秒向本地缓存发送的请求数。
源 RPS	每秒向增强数据源（如字典）发送的请求数。
源延迟	向增强数据源发送请求并从其接收响应所经过的时间（以毫秒为单位）。显示中值。
队列	增强请求队列的大小。此指标有助于查找瓶颈增强规则。
错误	向增强数据源发送请求时每秒出现的错误数。

响应 – 与响应规则相关的指标。	
RPS	每秒激活响应规则的次数。

存储指标

指标名称	描述
ClickHouse/常规 — 与 ClickHouse 集群的常规设置相关的指标。	
活动查询	发送到 ClickHouse 集群的活动查询数。每个 ClickHouse 实例都会显示此指标。
QPS	每秒发送到 ClickHouse 集群的查询数。
失败的 QPS	每秒发送到 ClickHouse 集群的失败查询数。
分配的内存	分配给 ClickHouse 进程的 RAM 量（以 GB 为单位）。

ClickHouse/插入 — 与将事件插入 ClickHouse 实例相关的指标。	
插入 EPS	每秒插入 ClickHouse 实例的事件数。
插入 QPS	每秒发送到 ClickHouse 集群的 ClickHouse 实例插入查询数。 如果“**插入 QPS**”指标显示查询队列不断增长且该指标大于 1，建议同时查看“**批量大小**”指标值，以便在存储服务配置的设置中调整存储缓冲设置。 例如： “**插入 QPS**”指标大于 1，等于 8。 “**批量大小**”指标为 1.2 GB（以字节为单位）。 在这种情况下，您可以通过将“**插入 QPS**”乘以“**批量大小**”来计算缓冲区大小： 8 * 1.2 = 9.6 GB。 将结果值9.6四舍五入，并在存储服务配置的**高级设置**选项卡中将其指定为字节数（例如，10000000000字节），作为**缓冲区大小**设置。同时，将“**缓冲区刷新间隔**”指定为 2 秒。增加缓冲区大小和缓冲区刷新间隔将有助于缓解查询队列的压力。 通常情况下，“**插入 QPS**”指标应小于 1。
失败的插入 QPS	每秒发送到 ClickHouse 集群的失败 ClickHouse 实例插入查询数量。
延迟的插入 QPS	每秒发送到 ClickHouse 集群的延迟 ClickHouse 实例插入查询数量。由于超出活动合并的软限制，查询被 ClickHouse 节点延迟。
拒绝的插入 QPS	每秒发送到 ClickHouse 集群遭到拒绝的 ClickHouse 实例插入查询数量。由于超出活动合并的硬限制，查询被 ClickHouse 节点拒绝。
活动合并	活动合并的数量。
分发队列	由于 ClickHouse 实例不可用而无法插入的事件临时文件数量。无法使用搜索找到这些事件。

ClickHouse/选择 — 与 ClickHouse 实例的事件分类相关的指标。	
选择 QPS	每秒发送到 ClickHouse 集群的 ClickHouse 实例事件分类查询的数量。
失败的选择 QPS	每秒发送到 ClickHouse 集群的失败的 ClickHouse 实例事件选择查询的数量。

ClickHouse/复制 — 与 ClickHouse 节点副本相关的指标。	
活跃的 Zookeeper 连接	Zookeeper 集群节点的活动连接数。正常运行时，该数量应等于 Zookeeper 集群中的节点数。

只读副本	ClickHouse 节点的只读副本数量。正常运行时，ClickHouse 节点的只读副本不应存在。
活跃的复制获取	数据复制期间从 ClickHouse 节点下载数据的活动进程数量。
活跃的复制发送	数据复制期间向 ClickHouse 节点发送数据的活动进程数量。
活跃的复制一致性检查	数据复制期间对 ClickHouse 节点副本进行活动数据一致性检查的次数。

ClickHouse/网络 — 与 ClickHouse 集群网络相关的指标。	
活动 HTTP 连接	ClickHouse 集群 HTTP 服务器的活动连接数量。
活动 TCP 连接	ClickHouse 集群 TCP 服务器的活动连接数量。
活动服务器间的连接	ClickHouse 节点之间的活动服务连接数量。

Core 指标

指标名称	描述
Raft — 与读取和更新 Core 状态相关的指标。	
查找 RPS	每秒发送到 Core 的查找过程请求数量及过程本身。
查找延迟	运行查找过程和过程本身所花费的时间（以毫秒为单位）。显示查找过程的第 99 个百分位数的时间。1% 的查找过程可能需要更长时间才能运行。
建议 RPS	每秒发送到 Core 的 Raft (SQLite) 建议过程请求数量及过程本身。
建议延迟	运行 Raft (SQLite) 建议过程和过程本身所花费的时间（以毫秒为单位）。显示建议过程的第 99 个百分位数的时间。1% 的建议过程可能需要更长时间才能运行。
数据挖掘 — 与数据收集和分析相关的指标	
执行规则	用于执行数据收集和分析请求的正在运行的调度程序数。
排队规则	用于执行排队的数据收集和分析请求的调度程序数。
执行错误	运行数据收集和分析调度程序时发生的错误数量。
执行延迟	调度程序执行请求所需的时间。
任务 — 与监控 KUMA Core 上任务运行相关的指标	
活动任务	单位时间内运行的任务数量。
任务执行延迟	任务运行的持续时间（秒）。
错误	运行任务时的错误数。

API — 与 API 请求相关的指标。	
RPS	每秒向 Core 发出的 API 请求数。
延迟	处理单个 API 请求到 Core 所花费的时间（以毫秒为单位）。显示中值。
错误	向 Core 发送 API 请求时每秒发生的错误数。

通知源 – 与用户活动相关的指标。	
订阅	通过 SSE 连接到 Core 以实时接收服务器消息的客户端数量。此数量通常等于使用 KUMA Web 界面的客户端数量。
错误	向用户发送通知时每秒发生的错误数量。

调度程序 – 与 Core 任务相关的指标。	
活动	重复的活动系统任务数量。用户创建的任务将被忽略。
延迟	运行任务所花费的时间（以毫秒为单位）。显示中值。
错误	执行任务时每秒发生的错误数量。

KUMA 代理指标

指标名称	描述
IO – 与服务输入和输出相关的指标。	
处理 EPS	每秒处理的事件数量。
输出 EPS	每秒发送至目标位置的事件数。
输出延迟	发送事件包和从目标位置接收响应所经过的时间（以毫秒为单位）。显示中值。
输出错误	事件包发送到目标位置时每秒发生的错误数。网络错误和写入目标位置磁盘缓冲区的错误分别显示。
输出事件丢失	每秒丢失的事件数量。事件可能由于网络错误或写入目标位置磁盘缓冲区的错误而丢失。如果目标位置响应错误代码（例如，在出现无效请求的情况下），事件也会丢失。
输出磁盘缓冲区大小	与目标位置关联的收集器的磁盘缓冲区大小（以字节为单位）。如果显示零值，则表示收集器的磁盘缓冲区中没有放置事件包，且服务运行正常。
写入网络 BPS	每秒接收到网络的字节数。

事件路由器指标

指标名称	描述
IO – 与服务输入和输出相关的指标。	
处理 EPS	每秒处理的事件数量。
输出 EPS	每秒发送至目标位置的事件数。
输出延迟	发送事件包和从目标位置接收响应所经过的时间（以毫秒为单位）。显示中值。
输出错误	事件包发送到目标位置时每秒发生的错误数。网络错误和写入目标位置磁盘缓冲区的错误分别显示。
输出事件丢失	每秒丢失的事件数量。事件可能由于网络错误或写入目标位置磁盘缓冲区的错误而丢失。如果目标位置响应错误代码（例如，在出现无效请求的情况下），事件也会丢失。
输出磁盘缓冲区大小	与目标位置关联的收集器的磁盘缓冲区大小（以字节为单位）。如果显示零值，则表示收集器的磁盘缓冲区中没有放置事件包，且服务运行正常。

指标名称	描述
写入网络 BPS	每秒接收到网络的字节数。
连接器错误	连接器日志中的错误数量。

所有服务通用的常规指标

指标名称	描述
进程 – 一般进程指标。	
内存	RAM 使用量 (RSS)，以兆字节为单位。
磁盘 BPS	每秒从磁盘读取或写入磁盘的字节数。
网络 BPS	每秒通过网络接收/传输的字节数。
网络数据包丢失	每秒丢失的网络数据包数量。
GC 延迟	执行 GO 垃圾回收周期所花费的时间（以毫秒为单位）。显示中值。
Goroutines	活动 goroutine 的数量。此数量与操作系统的线程数量不同。

OS – 与操作系统相关的指标。	
加载	平均负载。
CPU	CPU 负载百分比。
内存	RAM 使用率 (RSS) 百分比。
Disk	磁盘空间使用率百分比。

指标存储期限

KUMA 操作数据默认保存 3 个月。此存储期限可以更改。

要更改 KUMA 指标的存储期限：

1. 登录安装 KUMA Core 的服务器的操作系统。
2. 在文件 /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service 的 ExecStart 参数中，编辑 `--retentionPeriod=<metrics storage period, in months>` 标志，插入所需期限。例如，`--retentionPeriod=4` 表示指标将存储 4 个月。
3. 依次运行以下命令以重启 KUMA：

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-victoria-metrics`

   指标的存储期限已更改。

KUMA指标警报触发条件

如果某项服务的 KUMA 指标值超过 KUMA 的**服务监控**部分中配置的相应参数阈值，VictoriaMetrics 会发送警报，并在该服务的状态中显示错误消息。

VictoriaMetrics的警报接收间隔时间如下：

- VictoriaMetrics 每 15 秒从 KUMA 服务获取一次信息。
- VictoriaMetrics每分钟更新一次KUMA服务的警报。
- KUMA Core 服务每 15 秒从 VictoriaMetrics 获取一次信息。

因此，服务状态更新的总延迟小于2-3分钟。

如果您禁用了接收来自VictoriaMetrics的警报，某些KUMA服务的状态可能仍会显示为黄色。这可能发生在以下情况：

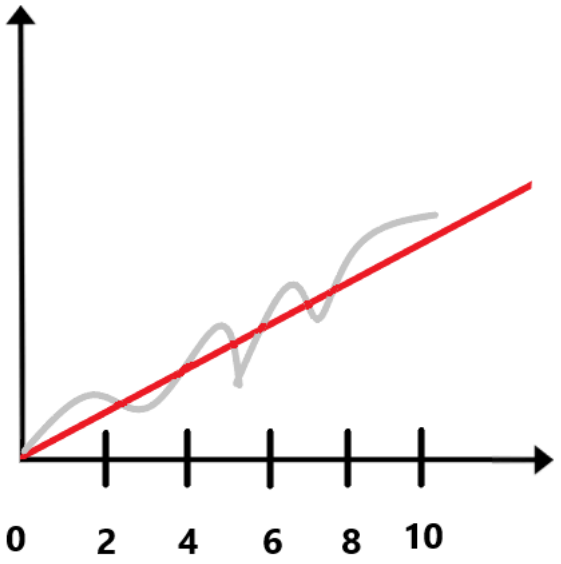
- 对于存储服务：
  - 如果在ClickHouse的/status参数中收到响应API请求的警报
  - 如果存储服务的冷存储未被监控
- 对于收集器服务：如果在/status参数中收到响应API请求的警报。
- 对于关联器服务：如果存在需要高级响应模块的响应规则，但当前授权许可不涵盖此模块，或者涵盖此模块的授权许可已过期。

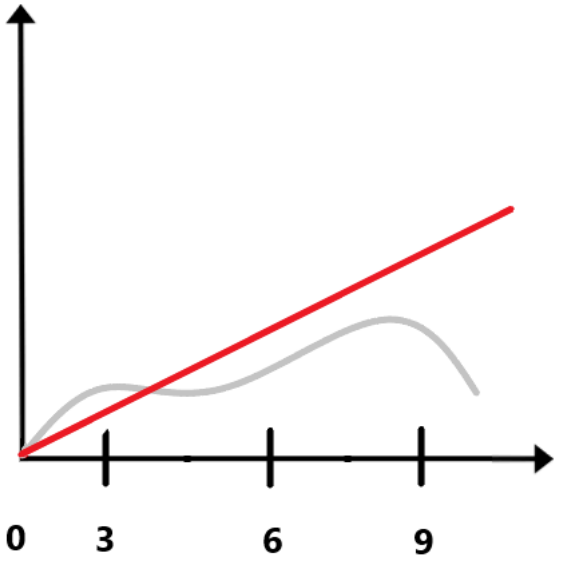
下表提供了当收到VictoriaMetrics警报时，服务状态中可能出现的错误消息，以及这些错误消息基于哪些指标和参数以及依据。有关可用于创建 VictoriaMetrics 警报的 KUMA 指标的详细信息，请参阅查看 KUMA 指标。

例如，如果某项服务的**活动服务**表显示黄色状态和`High distribution queue`错误消息（下表中的"错误消息"列），您可以在**增强**小部件的**分发队列**指标（下表中的"KUMA指标"列）中查看相关信息。

关于KUMA服务错误消息的描述

错误消息	可配置的警报参数	KUMA指标	Description
`QPS threshold reached`	**QPS时间间隔/窗口（分钟）** **QPS阈值**	Clickhouse / 一般 → 失败的QPS	如果"失败的QPS"指标在**QPS时间间隔/窗口（分钟）**参数指定的持续时间内超过指定的**QPS阈值**，则会显示错误消息。 例如，如果VictoriaMetrics对服务的100个请求中有25个不成功，并且**QPS阈值**为0.2，则警报的计算方式如下： (25 / 100) * 100 > 0.2 * 100 25% > 20% 由于失败请求的百分比大于指定的阈值，因此该服务会显示一条错误信息。
`Failed Insert QPS threshold reached`	**失败的插入QPS计算时间间隔/窗口（分钟）** **插入QPS阈值**	Clickhouse / 插入 → 失败的插入QPS	如果"失败的插入QPS"指标在**失败的插入QPS计算时间间隔/窗口（分钟）**参数指定的持续时间内超过指定的**QPS插入阈值**，则会显示错误消息。 例如，如果VictoriaMetrics向服务发出的100个请求中有25个不成功，且**插入QPS阈值**为0.2，则警报的计算方式如下： (25 / 100) * 100 > 0.2 * 100 25% > 20% 由于失败请求的百分比大于指定的阈值，因此该服务会显示一条错误信息。

错误消息	可配置的警报参数	KUMA指标	Description
`High distribution queue`	**分发队列阈值** **分发队列计算时间间隔/窗口（分钟）**	Clickhouse / 插入 → 分发队列	如果"分发队列"指标在**分发队列计算时间间隔/窗口（分钟）**参数指定的时间段内超过指定的**分发队列阈值**，则会显示错误消息。
`Low disk space`	**磁盘可用空间阈值**	操作系统 → 磁盘	如果"磁盘"指标值指示的可用磁盘空间量（以百分比表示）小于**磁盘可用空间阈值**参数中指定的值，则会显示错误消息。 例如，如果安装KUMA的分区占用了所有磁盘空间，则会显示错误消息。
`Low disk partition space`	**分区可用空间阈值**	操作系统 → 磁盘	如果KUMA使用的磁盘分区上的可用空间（以百分比表示）小于**分区可用空间阈值**参数中指定的值，则会显示错误消息。 例如，在以下情况下会显示错误消息： • 如果KUMA以高可用性配置安装，并且磁盘以卷的形式挂载时。 • 如果磁盘挂载在/opt目录下。
`Output Event Loss increasing`	**输出事件丢失**	输入/输出 → 输出事件丢失数	则当"输出事件丢失数"指标持续增加一分钟时，会显示错误消息。您可以使用**输出事件丢失数**参数启用或禁用显示此错误消息。
`Disk buffer size increasing`	**磁盘缓冲区递增时间间隔/窗口（分钟）**	输入/输出 → 输出磁盘缓冲区大小	如果"输出磁盘缓冲区大小"指标在**磁盘缓冲区增加时间间隔/窗口（分钟）**参数指定的采样时间间隔下连续10分钟单调递增，则会显示错误消息。 例如，如果**磁盘缓冲区递增时间间隔/窗口（分钟）**设置为2分钟，则当磁盘缓冲区大小在2分钟的采样时间间隔下连续10分钟单调递增时，会显示错误消息（参见下图）。 

错误消息	可配置的警报参数	KUMA指标	Description
`High enrichment queue`	**递增的数据增强队列时间间隔/窗口（分钟）**	数据增强 → 队列数	如果"队列数"指标在**递增的增强队列时间间隔/窗口（分钟）**参数指定的采样时间间隔下连续10分钟单调递增，则会显示错误消息。 例如，如果**递增的增强队列时间间隔/窗口（分钟）**的值为3，则当数据增强队列数每10分钟单调递增一次（采样时间间隔为3分钟）时，会显示错误消息。 在下图所示的情况下，错误信息不会显示，因为在第九分钟，指标的值减少，并没有单调递增。 
`Enrichment errors increasing`	**数据增强错误数**	数据增强 → 错误数	如果"错误数"指标在一分钟内持续增加，则会显示错误消息。您可以使用**数据增强错误数**参数启用或禁用显示此错误消息。
`Connector log errors increasing`	**停用连接器错误**	输入/输出 → 连接器错误数	如果VictoriaMetrics在一分钟内连续两次轮询"连接器错误数"指标，并且该指标持续增加，则会显示错误消息。您可以使用**停用连接器错误**参数启用或禁用显示此错误消息。

存储有关 Kaspersky Next XDR Expert 组件的诊断信息

有关 Kaspersky Next XDR Expert 组件的诊断信息存储在 Kubernetes 集群的工作节点上。在部署 Kaspersky Next XDR Expert之前，在配置文件中指定存储此信息所需的磁盘空间量（`loki_size` 参数）。

要检查用于存储有关 Kaspersky Next XDR Expert 组件的诊断信息的磁盘空间：

在 KDT 实用程序所在的管理员主机上，运行以下命令：

```
./kdt invoke observability --action getPvSize
```

显示已分配的可用磁盘空间量（以 GB 为单位）。

您还可以在部署 Kaspersky Next XDR Expert 后增加用于存储有关 Kaspersky Next XDR Expert 组件的诊断信息的磁盘空间量。您不能将磁盘空间量设置为小于之前指定的量。

要增加用于存储有关 Kaspersky Next XDR Expert 组件的诊断信息的磁盘空间量：

在 KDT 实用程序所在的管理员主机上，运行以下命令并指定所需的可用磁盘空间量（以 GB 为单位）（例如“50Gi”）：

```
./kdt invoke observability --action setPvSize --param
loki_size='<new_disk_space_amount>Gi'
```

已更改分配用于存储有关 Kaspersky Next XDR Expert 组件的诊断信息的可用磁盘空间量。

获取跟踪文件

通过 KDT 可获取 Kaspersky Next XDR Expert 和 OSMP 组件的跟踪文件，以便您自行或在卡巴斯基技术支持的帮助下排查基础设施故障。

以 OpenTelemetry 格式下载跟踪文件。

要获取 Kaspersky Next XDR Expert 或 OSMP 组件的跟踪文件：

1. 在 KDT 实用程序所在的管理员主机上，运行以下命令并指定要保存跟踪文件列表的文件路径：

   ```
   ./kdt traces find -o <output_file_path>
   ```

   跟踪文件及其 ID 的列表将输出至指定文件。

2. 要输出特定的跟踪文件，请运行以下命令并指定输出文件路径和跟踪文件 ID：

   ```
   ./kdt traces get -o <output_file_path> --trace-id=<trace_ID>
   ```

   指定的跟踪文件已保存。

记录自定义操作的启动

可通过 KDT 获取特定 Kaspersky Next XDR Expert 组件的自定义操作启动历史记录，以及特定自定义操作的启动日志。获取的日志可以帮助您自行调查 Kaspersky Next XDR Expert 组件运行的问题，或者在卡巴斯基技术支持的帮助下进行调查。

要获取特定 Kaspersky Next XDR Expert 组件的自定义操作启动历史记录：

请在 KDT 实用程序所在的管理员主机上运行以下命令，然后指定组件名称：

```
./kdt state -H <component_name>
```

将显示已执行的自定义操作及其 ID 的列表。

要获取自定义操作启动的日志：

请在 KDT 实用程序所在的管理员主机上运行以下命令，然后指定自定义操作启动的组件名称和 ID：

```
./kdt state -l <component_name> -m <custom_action_launch_ID>
```

将显示指定自定义操作启动的日志。

多租户

Kaspersky Next XDR Expert 支持多租户模式。此模式支持主管理员为多个客户端独立提供 Kaspersky Next XDR Expert 功能，或者针对不同分支机构进行资产、应用程序设置及对象的隔离。每个客户端或分支机构相互隔离，被称为一个租户。

通常，多租户模式用于以下情况：

- 服务提供商拥有多个客户端组织，并希望为每个客户端组织独立提供 Kaspersky Next XDR Expert 功能。为此，服务提供商管理员可以为每个客户端组织创建一个租户。
- 大型企业的管理员可能希望隔离分支机构或组织单位的资产、应用程序设置和对象，并独立管理分支机构或组织单位。为此，管理员可以为每个分支机构或组织单位创建一个租户。

多租户模式具有以下特点：

- 租户隔离
- 跨租户场景

租户隔离

租户之间相互隔离且独立管理。只有拥有租户访问权限的用户才能操作和管理该租户。除非主管理员明确授予其他租户的管理员相关访问权限，否则该管理员无法访问该租户的数据、资源和资产。

针对每个租户，您可以定义多个对象，包括：

- 资产

  每个租户的资产列表都是唯一的。单个资产只能归属于一个租户。
- 用户及其访问权限
- 事件、警报和事故
- 行动手册
- 与其他卡巴斯基应用程序、服务和第三方解决方案的集成

跨租户场景

所有租户都按层级结构排列。默认情况下，租户层级结构顶端包含一个预先创建的根租户。不能在根租户所在层级创建其他租户。新建租户时，需将其作为现有租户（包括根租户）的子租户创建。租户层级结构可包含任意数量的嵌套层级。

租户层级结构用于提供跨租户场景，包括以下场景：

- 继承和复制

  子租户从父租户接收以下对象：

  - 用户及其访问权限

    访问权限沿层级结构下行继承，且无法在较低层级撤销。

  - 租户设置，包括集成设置

    租户设置从父租户复制到其子租户。子租户创建后，可重新配置复制的设置以满足新租户需求。

  > 聚合和分段规则仅在租户层级结构中向下继承一级。例如，在根租户中创建的规则会被第一级子租户继承，但不会被这些子租户的子租户继承。

- 授权许可

  Kaspersky Next XDR Expert 的授权许可密钥需应用于与根租户绑定的主管理服务器层级。随后，该授权许可密钥会自动应用于层级结构中的所有租户。

用户角色

Kaspersky Next XDR Expert 为您提供了一组预定义的用户角色。您可以通过为用户分配用户角色来授予用户管理租户的权限。

用户角色	用户角色权限		
	读取	写入	删除
常规管理员	✓	✓	✓
租户管理员	✓	✓	✓
SOC 管理员	✓	✓	—
1级分析师	✓	—	—
2 级分析师	✓	—	—
初级分析师	✓	—	—
SOC 经理	✓	—	—
审批人	✓	—	—
审计员	✓	—	—
与子事故交互	✓	—	—

SLA 管理角色允许用户在事故详情页面中编辑 SLA 指标（**分类时间**、**响应所花的时间**、**解决时间**）。

租户和管理服务器

您只能将物理管理服务器与租户进行绑定。租户和管理服务器建立关联后，可实现两个解决方案（Kaspersky Next XDR Expert 和 Open Single Management Platform）的功能集成。

应用程序界面中的租户过滤器

在 Kaspersky Next XDR Expert 界面中，您可以配置对象列表，仅显示与所选租户相关的对象。租户过滤器适用于以下对象：

- **警报**部分中的警报
- **事故**部分中的事故
- **威胁搜索**部分中的事件
- **行动手册**部分中的行动手册

应用租户过滤器后，新设置将应用于您使用的控制台界面（OSMP 控制台或 KUMA 控制台）中的所有对象类型。

关于将管理服务器绑定到租户

您可以将管理服务器绑定到租户。租户和管理服务器之间进行关联后，您可将该管理服务器所管理的资产与租户之间进行关联。

虚拟管理服务器无法绑定到租户，仅支持物理管理服务器绑定。

租户可包含子租户，因此形成了租户层级结构。管理服务器可包含从属管理服务器，因此形成了服务器层级结构。您不能将任意服务器与任意租户绑定，因为可能导致非法绑定。例如，用户可能不具备对租户层级结构中某个租户的访问权限，但同一用户可能拥有对该租户下设备的访问权限。如果该用户拥有管理服务器 2 的访问权限，而该服务器是与租户绑定的管理服务器 1 的主要服务器，则可能发生这种情况。因此，默认情况下，该用户继承了对管理服务器 1 及其受管理设备的访问权限。为了避免这种情况，租户和管理服务器只能根据绑定规则相互绑定。

绑定有两种类型：

- 显式绑定

  手动选择希望绑定至租户的管理服务器，即可建立该绑定类型。

- 继承绑定

  为拥有从属管理服务器的管理服务器创建显式绑定后，从属管理服务器将通过继承绑定的方式绑定至租户。因此，多个管理服务器可能绑定到一个租户。

绑定规则：

- 根管理服务器始终绑定到根租户。您无法解除其绑定。
- 租户可能未绑定任何管理服务器。此类租户可拥有子租户，且管理服务器可绑定至子租户。
- 处于层级关系的两台管理服务器，只能绑定到同样处于层级关系的两个租户，且管理服务器层级必须与租户层级匹配。
- 一台管理服务器仅能通过显式绑定或继承绑定类型绑定至一个租户。

- 通过显式绑定将管理服务器绑定至租户时：
  - 如果该管理服务器已通过显式方式绑定至其他租户，则原绑定将被自动解除。
  - 如果管理服务器拥有从属管理服务器，则从属管理服务器将通过继承绑定方式绑定至新租户，但通过显式方式绑定至租户的管理服务器除外。在执行此操作之前，Kaspersky Next XDR Expert 会检查所有新绑定是否符合规则。若违反规则，则无法建立绑定。
- 删除租户和管理服务器之间的显式绑定（解除管理服务器绑定）时，管理服务器及其所有从属管理服务器（如有）将通过继承绑定方式自动绑定至所选管理服务器的主管理服务器所绑定的租户。如果某些从属管理服务器已通过显式方式绑定至租户，则将为这些从属管理服务器保留其绑定。
- 向层次结构中添加新的管理服务器时，该管理服务器将通过继承绑定方式自动绑定至其主管理服务器所绑定的租户。
- 从层次结构中删除管理服务器时，若该管理服务器与租户存在显式绑定，则此绑定将被解除。

配置与 Open Single Management Platform 的集成

您可以将管理服务器绑定到租户。管理服务器和租户创建关联后，可将该管理服务器所管理的资产与租户进行关联。

虚拟管理服务器无法绑定到租户，仅支持物理管理服务器绑定。

先决条件：

- 确保您熟悉绑定规则。
- 已创建待绑定管理服务器的目标租户。
- 如有需要，确保已添加待绑定至租户的从属管理服务器。

要将管理服务器绑定到租户或将其与租户解除绑定，您必须拥有授予租户和集成功能区域**写入**权限的角色。

将管理服务器绑定到租户

要将管理服务器绑定到租户：

1. 在主菜单中，转到“**Settings**” → “**Tenants**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡的“**卡巴斯基集成**”部分中，选择“**KSC**”。

4. 单击“**绑定管理服务器**”按钮，然后在打开的窗口中选择要绑定到租户的管理服务器。
   如果想在层次结构中添加新服务器或删除现有服务器，可以在管理服务器属性中进行操作。
5. 单击“**绑定**”按钮。

绑定过程可能需要一段时间。您可以在租户属性窗口中的管理服务器列表的“**绑定状态**”列追踪该过程。

解除管理服务器与租户的绑定

要解除管理服务器与租户的绑定：

1. 在主菜单中，转到“**Settings**” → “**Tenants**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   该租户的属性窗口将打开。
3. 在“**设置**”选项卡中，选中要与租户解除绑定的管理服务器旁边的复选框，然后单击“**解除绑定**”按钮。

查看和编辑租户

您可以使用租户为客户端组织独立提供 Kaspersky Next XDR Expert 功能，或者为不同分支机构隔离资产、应用程序设置和对象。

要查看或编辑租户属性：

1. 在应用程序主窗口中，转到**设置→租户**部分。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   将打开该租户的属性窗口。如果您仅拥有对该租户的**读取**权限，则属性窗口将以只读模式打开。如果您拥有**写入**权限，则可修改租户属性。
3. 修改租户属性，然后单击“**保存**”按钮。
   您可以点击**“保存并关闭”**按钮保存更改并关闭租户属性窗口。

租户属性被修改并保存。

普通

“**常规**”选项卡中包含有关租户的常规信息。您可以修改租户的名称和描述。

设置

“**设置**”选项卡包含以下部分：

- **卡巴斯基集成**

  通过此部分，您可以为当前租户配置要集成到 Kaspersky Next XDR Expert 中的卡巴斯基应用程序的集成设置。

- **第三方集成**

  通过此部分，您可以为当前租户配置要集成到 Kaspersky Next XDR Expert 中的第三方应用程序的集成设置。

- **检测和响应**

  通过此部分，您可以配置与威胁检测和响应相关的设置和对象：

  - 分段规则
  - 聚合规则
  - 邮件服务器连接
  - 资产审计
  - 网络共享凭证
  - 电子邮件模板
  - 扫描设置
  - 资产设置

    - 存档资产的保留期限
    - 自定义资产字段
    - **KSC资源导入**

      受此程序保护的所有资产均已在 Kaspersky Security Center 中注册。受 Kaspersky Security Center 保护的资产的相关信息可以导入 KUMA。为此，您需要提前配置应用程序之间的集成。

      KUMA导入从卡巴斯基安全管理中心网络代理程序收到的以下设备信息：

      - 资产的基本信息：名称、地址、连接到 Kaspersky Security Center 的时间、硬件信息、保护状态、反病毒数据库版本
      - 资产属性信息：漏洞；软件，包括操作系统；资产所有者

若要导入卡巴斯基安全管理中心资产信息：

1. 在主菜单中，前往**资产管理→资产(设备)→检测和响应**。
2. 点击**导入**，然后选择以下操作之一：
   - 如要导入资产基本属性信息，请点击**导入KSC资产**。
     这将打开**导入KSC资产**窗口。
   - 若要导入资产其他属性信息，请点击**导入KSC资产属性**。
     这将打开**导入KSC资产属性**窗口。
3. 在下拉列表中，选择要为其执行导入操作的租户。
   在这种情况下，程序将下载已配置为连接到所选租户的所有 Kaspersky Security Center 服务器全部资产的信息。
   如果要导入所有租户的所有卡巴斯基安全管理中心服务器全部资产的信息，请选择**所有**。
4. 单击"**导入**"按钮。

将导入资产信息。

此外，在租户属性窗口中，您可以安排定期导入资产信息或手动运行导入。

- KICS/KATA资产导入

- KPSN信誉数据库
- 保留期限
  警报和事故的保留期限取决于所使用的 Kaspersky Next XDR Expert 授权许可。
- 事故管理

无需配置共享租户的设置。

角色

角色选项卡列出了对该租户拥有访问权限的用户。您可以更改此列表，并为用户分配用户角色。

添加租户

开始之前，请阅读有关租户的常规信息。

要添加子租户，您必须在父租户或租户层级结构中更高级别租户的"**租户**"功能区域中，拥有**读取**和**写入**权限。

要添加新租户：

1. 在应用程序主窗口中，转到**设置→租户**部分。
2. 选中目标父租户旁边的复选框。新租户将作为所选租户的子租户创建。
3. 单击“**添加**”。
4. 在打开的“**添加租户**”窗口中，输入新租户的名称。
5. 如有必要，可添加新租户的描述。
6. 单击“**添加**”。

   新租户将显示在租户列表中。

子租户将从父租户继承以下对象：

- 用户及其访问权限
- 集成设置

创建租户后，您可以重新配置继承的对象以满足新租户需求。

为租户中的用户和用户组分配角色

您可以向 Kaspersky Next XDR Expert 用户和域组分配 XDR 角色，为其提供租户中的一组访问权限。

为此，您必须在要向用户分配角色的租户中拥有以下 XDR 角色之一：主管理员、SOC 管理员或租户管理员。

由于租户与其他租户隔离并独立管理，因此只有向租户分配了访问权限的用户才能在此租户内操作并进行租户管理。

访问权限在层次结构中向下继承，且无法在层次结构的下级节点中撤销。

OSMP 控制台中的新内部用户账户在账户创建后五分钟内，即可在租户中添加和分配角色。

用户的权限是用户自身权限和用户所属域组（如果有）权限的总和。当用户直接包含在某个组中或通过嵌套组成员身份间接包含在组中时，情况亦是如此。例如，如果用户是组 A 的成员，而该组嵌套在组 B 中，则该用户的权限是分配给该用户的权限以及分配给组 A 和组 B 的权限之和。这意味着，如果您向组 B 分配权限，其嵌套组和属于组 B 的用户将继承这些权限。

但是，在循环组嵌套的情况下，循环中的成员及其子组不会继承分配给其父组的权限。

要将角色分配给租户中的用户或域组：

1. 在主菜单中，转到“**设置**” → “**租户**”。

   屏幕上将显示租户列表。

2. 单击所需租户的名称。
   这将打开“租户属性”窗口。
3. 转到“**访问权限**”选项卡，然后根据要分配角色的对象选择用“**用户**”或“**组**”。
   将显示用户表或域组表。
4. 如果必要，配置表格：
   - 单击过滤图标（ ），然后在调用的菜单中指定并应用过滤条件。
     您无法将过滤器应用于“**组角色**”和“**父组角色**”列。
   - 单击设置图标（ ）来配置列显示。
5. 单击“**添加用户**”按钮或“**添加组**”按钮，具体取决于您在步骤 3 中选择的选项卡。
6. 在打开的窗口中，执行以下操作之一：
   a. 如果您在步骤 3 中选择了“**用户**”选项卡，则在“**用户**”字段中，输入用户名或电子邮件地址。如果在步骤 3 中选择了“**组**”选项卡，则在“**组**”字段中指定组名。
   b. 选中要分配给用户或域组的角色旁边的复选框。
      如有必要，可以选择多个角色。
   c. 单击**添加**。

   窗口将关闭，用户或域组显示在列表中。
7. 单击“**保存**”按钮。

用户或域组将添加到租户并分配角色。如有必要，您可以通过单击用户或域组名称来编辑角色，然后执行步骤 6-7 中描述的操作。

删除租户

一次只能删除一个租户。但是，如果所选租户拥有子租户，则他们也将被删除。与租户相关的行动手册将被删除，有关该租户的警报和事故信息将无法访问。

在 OSMP 控制台中删除租户时，KUMA 控制台中将发生以下变更：

- 租户及其资源将被删除。当存档资产的事件保留期（TTL）到期时，已删除租户的资产将被存档并删除。
- 与租户关联的存储分区被删除。
- 原始事件无法访问。
- 已删除租户的服务状态变为**灰色**。

要删除租户，您必须在所选租户的“**租户**”功能区中拥有“**读取**”和“**写入**”权限。

您无法删除根租户以及从 Kaspersky Unified Monitoring and Analysis Platform 迁移的共享租户。

要删除租户：

1. 在应用程序主窗口中，转到**设置→租户**部分。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 选中要删除租户旁边的复选框。若所选租户拥有子租户，则它们将被自动选中且无法取消选择。
3. 单击“**删除**”按钮。
4. 输入待删除租户名称，以确认删除操作。若租户拥有子租户，则它们也会被列为待删除租户。

所选租户、其子租户（如有）以及相关对象将被删除。

配置邮件通知

您可以通过管理服务器和外部 SMTP 服务器配置有关 Kaspersky Next XDR Expert 中所发生事件的邮件通知。为此，您必须配置与 SMTP 服务器的连接设置。

要配置 SMTP 服务器连接：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   屏幕上将显示租户列表。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。
3. 转到“**设置**”选项卡，然后在“**Detection and response**”部分中，单击“**邮件服务器连接**”。
4. 在右侧窗格中，单击“**查看属性**”按钮。
   管理服务器属性窗口打开，**常规**选项卡被选中。

   > 无论租户绑定到哪个管理服务器，该窗口都会显示主管理服务器的属性以及主管理服务器的 SMTP 设置。

5. 按照“配置通知传递”中步骤 2 所述配置参数。

配置与 SMTP 服务器的连接后，用户将开始接收来自 Kaspersky Next XDR Expert 的电子邮件。

您可以创建电子邮件通知模板，以便在触发您选择的警报、事故或事件时发送给指定用户。这些模板也可以编辑和删除。

创建通知模板

在Kaspersky Next XDR Expert中配置事件电子邮件通知后，您可以为这些电子邮件通知创建自定义模板。

要创建通知模板，您必须具有以下XDR角色之一：主管理员、租户管理员或SOC管理员。

部署 Kaspersky Next XDR Expert 时，根租户中会包含电子邮件通知模板。如果您创建子租户，它会自动从父租户复制设置。由于子设置和父设置不相关，因此您在子租户设置中所做的更改不会影响父租户中的设置，反之亦然。

要创建电子邮件通知模板：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   显示租户列表。
2. 单击所需租户的名称。
   这将打开“租户属性”窗口。
3. 转到“**设置**”选项卡，然后在“**Detection and response**”部分中，单击“**电子邮件模板**”。
   将显示您可以为其配置通知模板的事件类型表。
4. 如果在步骤 2 中选择了根租户，请在“**管理服务器显示名称**”字段中输入要在电子邮件里警报和事故链接中使用的地址。
5. 单击**创建**按钮，然后在打开的下拉列表中选择要为其创建电子邮件通知模板的事件类型。
6. 在打开的**创建电子邮件模板**面板中，指定以下设置：

   可用字段会根据所选事件类型而有所不同。

   - 在**名称**字段中，指定电子邮件通知的主题。
   - 如果要更改电子邮件通知模板的事件类型，请在**事件类型**字段中选择新的事件类型。
   - 如果要为选定的事件类型启用电子邮件通知，请将切换按钮移动到**状态**字段中的**已启用**位置。
     您还可以从事件类型表中启用电子邮件通知。默认情况下，电子邮件通知处于禁用状态。
   - 在“**主题**”字段中，指定电子邮件通知的主题。必填字段。
     您还可以在 **主题** 字段中使用警报字段、事故字段和 KUMA 规范化事件字段，例如 `New incident in OSMP: {{ .InternalID }}, {{ .Name }}`。
   - 在**模板**字段中，编写电子邮件通知消息。
     电子邮件通知消息示例

     ```
     您好，<br>
     <br>
     ```

```
警报 {{ .InternalID }}{{ with escapeHTML .Rules.Names }} "{{ . }}"{{ else }}{{ end }} 已于 {{ .CreatedAt }}
注册。<br>
<br>
警报详细信息：<br>
<br>
租户：{{ .TenantID }}<br>
警报严重性：{{ .Severity }}<br>
警报首次出现时间：{{ .FirstEventTime }}<br>
警报最后出现时间：{{ .LastEventTime }}<br>
警报的完整信息可在 OSMP Web 界面中找到：{{ link_alert . }}<br>
<br>
Open Single Management Platform
```

您可以访问警报字段、事故字段和KUMA规范化事件字段，并使用HTML标签。

编写模板时，您可以使用以下函数：

- `date` — 定义日期和时间格式。该函数将以毫秒为单位的时间（UNIX 时间）作为第一个参数。第二个参数可用于传递 RFC 标准格式的时间。时区无法更改。

  ```
  {{range .Events }}
  Service name: {{.Event.ServiceName}}
  Device host name:  {{.Event.DeviceHostName}}
  Message: {{.Event.Message}}
  {{end}}
  ```

  嵌套对象可以有自己特定的嵌套对象。您可以使用嵌套范围函数访问这些嵌套对象。

- `limit` — 限制 `range` 函数返回的对象数量。
- `link_alert` — 生成指向警报的链接，URL 在**管理服务器显示名称**字段中指定。
- `link_incident` — 生成指向事故的链接，URL 在**管理服务器显示名称**字段中指定。
- `link` — 采用链接的形式，用户收到通知电子邮件时可以打开该链接。

- 在**收件人**字段中，指定一个或多个用于发送通知的电子邮件地址。
- 在**相关规则**下拉列表中，选择一个或多个关联规则，电子邮件通知将根据这些规则发送。
- 在**根据严重级别通知**字段中，选择触发电子邮件通知的警报的最低严重级别。严重级别低于指定级别的警报将不会触发电子邮件通知。
- 在**检测技术**下拉列表中，选择一个或多个将触发电子邮件通知的检测技术。
- 如有必要，在“**描述**”字段中输入通知模板的描述。

7. 单击“**创建**”按钮。

   创建电子邮件模板窗口随即关闭。

8. 在租户属性窗口中，保存更改。

电子邮件通知模板随即创建并保存。当Kaspersky Next XDR Expert中发生所选类型的事件时，模板通知将发送到您指定的电子邮件地址。

编辑和删除通知模板

您可以编辑或删除有关Kaspersky Next XDR Expert中发生的事件的电子邮件通知模板。

要编辑或删除通知模板，您需要具备以下 XDR 角色之一：主管理员、租户管理员或 SOC 管理员。

部署 Kaspersky Next XDR Expert 时，根租户中会包含电子邮件通知模板。如果您创建子租户，它会自动从父租户复制设置。由于子设置和父设置不相关，因此您在子租户设置中所做的更改不会影响父租户中的设置，反之亦然。

若要编辑电子邮件通知模板：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   显示租户列表。
2. 单击所需租户的名称。
   这将打开“租户属性”窗口。
3. 转到“**设置**”选项卡，然后单击“**电子邮件模板**”。
4. 在表格的**事件类型**列中，单击要编辑的通知模板的事件类型。
5. 在打开的**编辑电子邮件模板**窗口中，更改必要的设置：
6. 保存更改。
   编辑电子邮件模板窗口随即关闭。
7. 保存更改。

邮件通知模板随即编辑并保存。当Kaspersky Next XDR Expert中发生所选类型的事件时，模板通知将发送到您指定的电子邮件地址。

若要删除电子邮件通知模板：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   显示租户列表。
2. 单击所需租户的名称。
   这将打开“租户属性”窗口。
3. 转到“**设置**”选项卡，然后单击“**电子邮件模板**”。
4. 选中要删除通知模板旁边的复选框。

5. 单击“**删除**”按钮。

6. 在打开的窗口中，确认删除：

   邮件通知模板随即删除。

配置用于访问共享网络资源的凭证存储

执行“获取磁盘映像”和“获取内存转储”响应操作后获得的文件需要占用大量可用空间。因此，这些文件会被保存到共享网络资源中。

如果使用多个共享网络资源，则必须为每个资源指定凭证。

为此，您必须拥有以下 XDR 角色之一：主管理员、SOC 管理员、租户管理员。

要配置访问共享网络资源的凭证：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   屏幕上将显示租户列表。

2. 单击所需租户的名称。
   这将打开“租户属性”窗口。

3. 转到“**设置**”选项卡，然后选择“**网络共享凭证**”部分。

4. 然后单击“**添加**”按钮。
   将打开“**添加凭证**”窗格。

5. 请在相应的字段中指定用于访问共享网络资源的账户的登录名和密码。

   > 保存设置后，密码无法删除。

   如有必要，您可以在**“描述”**栏中填写任何评论。

6. 单击“**保存**”按钮。

   窗格已关闭，设置已保存并显示在表格中。

如有必要，您可以通过单击表格中带有其名称的链接来编辑设置，或者通过选中表格中设置名称旁边的复选框，然后单击**删除**来删除设置。

配置定期IOC扫描

您可以在安装了端点代理组件的设备上配置IOC扫描的时间表。如果设置了扫描计划，端点代理将根据已启用定期扫描的IOC规则，每天在设备上搜索入侵指标（IOC）。

默认情况下，IOC 扫描每天执行一次。您可以更改扫描的开始时间和持续时间，或者禁用每日扫描。

若要配置定期IOC扫描：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   租户过滤器将打开。该列表仅包含您对其至少拥有“**读取**”权限的租户。
2. 点击目标租户的名称。
   这将打开“租户属性”窗口。
3. 选择**设置**选项卡。
4. 在“**扫描设置**”部分，选择“**IOC 扫描计划**”选项卡。
5. 打开“**每日扫描**”切换开关，然后指定扫描计划的设置：
   - **开始时间 (UTC)**。IOC扫描的开始时间。此时间以执行配置的OSMP服务器的时区为准。
     如果端点代理在“**开始时间 (UTC)**”中指定的时间之后收到新的扫描计划，则下一次扫描将在第二天“**开始时间 (UTC)**”中指定的时间启动。
   - **最大扫描时长(小时)**。IOC扫描的时间限制（以小时为单位）。达到此限制后，端点代理将结束扫描过程，无论扫描是否完成。
6. 单击**保存**或**保存并关闭**以保存设置。

新的IOC扫描时间表将在保存更改后立即生效。如果扫描检测到威胁，则会创建 IOC 警报。

Kaspersky Endpoint Security for Windows的限制

如果IOC规则中定义的IOC搜索范围包含RegistryItem数据类型，则Kaspersky Endpoint Security for Windows将扫描有限的注册表项集。

配置文件存储库中文件的自动轮换

通过限制**文件**存储库的空间来确保文件的自动轮换：一旦达到限制，存储库中最旧的文件将被删除。如果您没有指定限制，在部署Kaspersky Next XDR Expert时，在为存储库分配的空间用完后，您将无法将新文件上传到**文件**存储库。

例如，在部署过程中，为**文件**存储库分配了 20 GB 磁盘空间。然后，您在租户设置中指定了 10 GB 作为限制；达到该限制时，将删除**文件**存储库中最旧的文件。如果您未指定任何限制，当**文件**存储库达到 20 GB 时，您将无法再向其中上传文件。

若要在文件存储库中配置文件的自动轮换：

1. 在主菜单中，转到“**设置**” → “**租户**”。
   屏幕上将显示租户列表。
2. 单击所需租户的名称。
   该租户的属性窗口将打开。

3. 前往**设置**标签，然后在**文件轮换**部分中，完成以下操作：

   a. 在**自动文件轮换**字段中，将切换按钮切换到**已启用**位置。

   b. 在“最大存储限制”字段中，指定将从**文件**存储库中删除最旧文件的文件卷。
   最小值为1GB。

   c. 单击**保存**或**保存并关闭**以保存设置。

自动文件轮换随即启用并配置。

联系技术支持

该部分描述如何获取技术支持和其可用条款。

如果获得技术支持

如果您在 Kaspersky Next XDR Expert 文档或任何 Kaspersky Next XDR Expert 信息源中都找不到问题的解决方案，请联系卡巴斯基客户服务团队。技术支持专家将回答关于安装和使用 Kaspersky Next XDR Expert 的所有问题。

卡巴斯基在 Kaspersky Next XDR Expert 的生命周期内提供支持（请参见应用程序支持生命周期页面）。与技术支持部门联系之前，请阅读支持规则。

您可以通过以下任一方式联系技术支持：

- 访问技术支持网站
- 从 Kaspersky CompanyAccount 门户向技术支持团队发送请求

通过 Kaspersky CompanyAccount 获得技术支持

Kaspersky CompanyAccount 是面向使用卡巴斯基应用程序的公司的门户。Kaspersky CompanyAccount 门户旨在通过在线请求促进用户和卡巴斯基专家之间的互动。您可以使用 Kaspersky CompanyAccount 来跟踪在线请求状态，并存储它们的历史记录。

您可以将贵组织的所有员工注册到一个 Kaspersky CompanyAccount 账户下。您可以通过一个账户集中管理已注册员工向卡巴斯基发出的电子请求，还可以通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户支持以下语言：

- 英语
- 西班牙语
- 意大利语
- 德语
- 波兰语
- 葡萄牙语
- 俄语

- 法语
- 日语

要了解有关 Kaspersky CompanyAccount 的更多信息，请访问技术支持网站。

已知问题和限制

Kaspersky Next XDR Expert 存在一些对应用程序运行并不重要的限制：

- 10721464：禁用 EDR 并将资产移至 KATA 后，该资产在资产表（**资产(设备)** → **Detection and response**）的**资产来源** 列中仍显示“EDR”值。这可能导致无法执行 KATA 响应。
- 10079501：使用实例层次结构时，在 Kaspersky Security Center 中分配的权限不会从父实例复制到子实例。为确保正确运行，请在每个子实例上手动为已复制的用户分配所需权限。
- 10112300：如果证书信任链断开，Web 界面不会显示通知。只能通过间接迹象识别该问题，例如资源继承缺失。当从父 OSMP 实例打开继承自父 OSMP 实例或最初属于子 OSMP 实例的资源时，会显示以下消息：“SIEM 组件连接错误。”

  解决方法：替换证书并修复实例层次结构。
- 10111236：在条形图小部件中，表示接近0%的小值的条形不会显示在图表上。
- 9302142：“**使用网络代理作为 DMZ 连接网关**”选项在 Microsoft Windows on Arm 上不受支持。
- 10011047：对于在升级到版本2.1 HF2之前创建的租户，IOC扫描计划功能可能在界面中显示为已启用，而按计划执行的IOC扫描实际上处于禁用状态。
- 10141948：在运行内核版本 6.12.60-1-generic 或更高版本的 Astra Linux 的管理员设备上，KDT 命令会延迟约 6 分钟执行。作为解决方法，请以 root 身份运行以下命令：

  ```
  echo "N" > /sys/module/nfs/parameters/localio_enabled
  ```
- 10042351：当您获取内存占用量为3GB或更大的进程的内存转储时，响应操作会启动但无法完成。
- 9957846：如果KICS/KATA资产在导入到第一个租户后又导入到第二个租户，则这些资产将从第一个租户移除并移动到第二个租户。如果配置了计划导入，则资产可能会在租户之间持续移动。
- 9823258：如果将集成到Kaspersky Next XDR Expert中的管理服务器添加为另一个集成XDR的管理服务器的从属管理服务器，则无法通过**添加从属管理服务器向导**自动上传管理服务器证书。在这种情况下，您必须手动上传从属服务器的证书。
- 9495472: 如果您计划在基础设施中使用多个租户，请为每个租户创建一个单独的收集器。
- 9218282: Kaspersky Next XDR Expert 2.0使用更新的事件数据模型。基于之前数据模型的行动手册可能无法按预期工作。您必须更新在Kaspersky Next XDR Expert 1.4及更早版本中创建的行动手册，以确保它们与新的事件数据模型正常工作。
- 9365692: 当使用自签名证书时，从在Kaspersky Endpoint Security for Windows中启用了**加密连接扫描**选项的设备到另一个设备的远程终端连接会被阻止。若要允许远程终端连接到目标设备，请执行以下操作之一：
  - 在连接设备上使用受信任的证书。
  - 从加密连接扫描中排除连接设备的网址。
  - 允许访问具有不受信任证书的域。

- 9117520: 使用不同的数据库名称和不同的证书从备份恢复Kaspersky Next XDR Expert时，部署会在`klnagchk -fullwait`验证步骤停止。
- 8690777: 只有 Linux 设备支持使用行动手册启动第三方自定义脚本。
- 8428740: 指定聚合或分段规则的触发器时，带有相互依赖参数的函数的 jq 表达式被视为无效。例如：`any(.Observables[]; .Type == "ip" and .Value == "1.1.1.1")`
- 7143556: 关闭 Kubernetes 集群的基础架构服务器并重新启动后，尝试登录 OSMP 控制台将返回错误。
- 7268335: 如果在受管理设备管理组属性的"**访问权限**"选项卡上启用"**使用自定义权限**"选项，则无法将客户端设备从 Open Single Management Platform 导出到 KUMA。
- 6704698: 即使在 Kaspersky Next XDR Expert 中未安装 Kaspersky Endpoint Security for Windows Web 插件，包含通过 Kaspersky Endpoint Security for Windows 执行响应操作的行动手册仍会在行动手册列表中显示为可用。
- 7208621: 当您导入*将更新下载到分发点存储库*或*更新验证*任务时，**选择任务将被分配到的设备**选项将启用。这些任务不能分配给设备分类或特定设备。如果将*下载更新分配到分发点存储库*或将*更新验证*任务分配到特定设备，则任务将无法正确导入。
- 6646913: 在调查图中，重新排列节点的操作不正确。
- 6962370: 将数据从 Kaspersky Security Center Windows 的从属管理服务器迁移到 Kaspersky Next XDR Expert 的主管理服务器时，迁移向导无法完成"**导入数据**"步骤。如果您在从属管理服务器上创建全局任务（例如，*远程卸载应用程序*任务），并在"迁移向导"的"**要导出的受管理应用程序**"参数中仅选择了 **Kaspersky Security Center 管理服务器**这一值，则会出现此问题。
- 6983311: 无法接收卡巴斯基公告。
- 6810101: 尽管 Kaspersky Next XDR Expert 不支持移动设备管理，但管理服务器属性窗口包含移动设备的设置。
- 6822204: 有关新版本 Web 插件可供下载的通知已被禁用。您可以使用 Kaspersky 部署工具包更新插件。
- 6919635: 创建新租户后，与该租户相关的警报将发送到服务器，但不会显示在警报表中。您可能需要刷新网页以更新表格数据。
- 9763104: 在管理服务器属性窗口中，**双重身份验证**选项卡会显示**允许生成 Secret 密钥的用户**表。由于所有用户都可以生成密钥，因此表格是不合理的。
- 10412424: Kaspersky Next XDR Expert 从版本 2.1 升级到版本 2.2 后，**监控 → 资源**区域无法打开。在浏览器设置中删除 Cookie 后，该区域即可正常打开。
- 10456232: 如果您正在升级到版本 2.3，并且配置了多个 OSMP 实例的层次结构，则子实例继承的资源以及在子实例中创建的资源可能不会显示在父实例中。如果出现这种情况，请在升级后重新保存子实例上的资源。或者，您可以导出这些资源（机密类型的资源除外），然后将其导入同一租户。
- 10751535: 如果您使用的是低于 2.3.224 版本的 Kaspersky Next XDR Expert，并且配置了多个 OSMP 实例的层次结构，则对于在子实例上创建或由子实例继承的资源，父实例上的资源列表不会在**资源类型**列中显示值。

有关 OSMP 的已知问题列表，请参阅Kaspersky Security Center 文档。

故障解决

本节提供在使用 Kaspersky Next XDR Expert 时可能遇到的常见问题的解决方案。

使用自签名证书时，远程终端连接会被阻止

当使用自签名证书时，从在Kaspersky Endpoint Security for Windows中启用了**加密连接扫描**选项的设备到另一个设备的远程终端连接会被阻止。

若要允许远程终端连接到目标设备，请执行以下操作之一：

- 在连接设备上使用受信任的证书。
- 从加密连接扫描中排除连接设备的网址。
- 允许访问具有不受信任证书的域。

附录

本部分提供的信息是对文档正文的补充，其中包含参考信息。

组件手动启动和安装命令

本部分包含 KUMA 可执行文件 /opt/kaspersky/kuma/kuma 的参数，可用于手动启动或安装 KUMA 服务。当您需要查看服务器操作系统控制台中的输出时，这一功能可能会很有用。

命令参数

命令	描述
`tools`	启动 KUMA 管理工具。
`collector`	安装、启动或删除收集器服务。
`core`	安装、启动或卸载核心服务。
`correlator`	安装、启动或删除关联器服务。
`agent`	安装、启动或删除代理服务。
`help`	获取有关可用命令和参数的信息。
`license`	获取有关授权许可的信息。
`storage`	启动或安装存储。
`version`	获取有关程序版本的信息。

标志：

`-h`、`--h` 用于获取有关任何 kuma 命令的帮助。例如，`kuma <component> --help`。

示例：

- `kuma version` 用于获取 KUMA 安装程序的版本。
- `kuma core -h` 用于获取有关 KUMA 安装程序核心命令的帮助。
- `kuma collector --core <收集器应从中获取其设置的服务器地址> --id <已安装服务的 ID> --api.port <端口>` 用于启动收集器服务的安装。

KUMA 文件的完整性检查

在KUMA 目标主机上，如果 KUMA 服务（收集器、关联器、存储、事件路由器）安装在 Kubernetes 集群之外，则使用位于 `/opt/kaspersky/kuma/integrity/bin/ directory` 中的脚本执行完整性验证。此目录包含特定于服务的完整性检查脚本（`check_collector.sh`、`check_correlator.sh`、`check_storage.sh`、`check_event_router.sh`），以及用于验证 Windows 版 KUMA 代理的脚本（`check_kuma_exe.sh`）。其中还包括完整性检查机制内部使用的验证实用程序（`integrity_checker` 和 `integrity_checker.sh`）。

已在运行服务的机器上添加了完整性检查脚本，并将日志记录到dmsg：

- `manual_integrity_check.sh`—允许手动对所需的 KUMA 服务执行完整性检查（与标志 `collector`、`correlator`、`storage`、`eventRouter` 配合使用）。
- `systemd_integrity_check.sh`—在 KUMA 服务启动或重启时运行完整性检查。

要检查组件文件的完整性：

1. 在安装了KUMA服务的KUMA目标主机上，运行以下命令导航到包含该脚本集的目录：

   ```
   cd /opt/kaspersky/kuma/integrity/bin
   ```

2. 运行所需的脚本（例如，`check_collector.sh`）。

   将检查组件文件的完整性。

   检查每个组件的结果将按以下格式显示：

- “`Summary`”部分描述了扫描对象的数量以及扫描状态：完整性未确认/对象已跳过/完整性已确认：
  - `Manifests` - 已处理的清单文件数量。
  - `Files` - 执行 KUMA 完整性检查时不使用。
  - `Directories` - 执行 KUMA 完整性检查时不使用。
  - `Registries` - 执行 KUMA 完整性检查时不使用。
  - `Registry values` - 执行 KUMA 完整性检查时不使用。
- 组件完整性检查结果：
  - `SUCCEEDED` - 完整性已确认。
  - `FAILED` - 完整性校验失败。

成功进行完整性检查后的命令输出示例

```
================================================>
Summary( failed / skipped / succeeded ):
Manifests: 0 / 0 / 1
Files: 0 / 0 / 1
Directories: 0 / 0 / 0
Registries: 0 / 0 / 0
Registry values: 0 / 0 / 0
================================================>
SUCCEEDED
```

在输出中，成功验证的清单数量显示在成功列下的 `Manifests`行中。状态`SUCCEEDED`表示所有已验证的组件均与签名清单匹配，未检测到完整性违规。如果发现差异，则检查结果报告为`FAILED`。

使用此机制验证安装在Kubernetes集群之外的KUMA服务的完整性。

您还可以检查已安装的Kaspersky Next XDR Expert组件的完整性。

规范化事件数据模型

本部分介绍 KUMA 规范化事件数据模型。KUMA 关联器处理的所有用于检测警报的事件都必须符合此模型。

不符合此数据模型的事件必须使用收集器导入此格式（或进行规范化）。

规范化事件数据模型

字段名称	数据类型	字段大小	描述
			字段名称反映其用途。字段可修改。
ApplicationProtocol	字符串	31个字符	应用程序层协议的名称。例如，HTTPS、SSH、Telnet。
BytesIn	数字	从 -9223372036854775808 到 9223372036854775807	已接收的字节数。
BytesOut	数字	从 -9223372036854775808 到 9223372036854775807	已发送的字节数。
DestinationAddress	字符串	45个字符	将对其执行操作的资产的 IPv4 或 IPv6 地址。例如，0.0.0.0 或 xxx:
DestinationCity	字符串	1023个字符	与"目标地址"字段中的 IP 地址对应的城市。
DestinationCountry	字符串	1023个字符	与"目标地址"字段中的 IP 地址对应的国家/地区。
DestinationDnsDomain	字符串	255个字符	目标位置的完全限定域名的 DNS 部分。
DestinationHostName	字符串	1023个字符	目标的主机名。目标的 FQDN（如果可用）。
DestinationLatitude	浮点数	+/- 1.7E-308 至 1.7E+308	与"目标地址"字段中的 IP 地址对应的经度。
DestinationLongitude	浮点数	+/- 1.7E-308 至 1.7E+308	与"目标地址"字段中的 IP 地址对应的纬度。
DestinationMacAddress	字符串	17个字符	目标的 MAC 地址。例如，aa:bb:cc:dd:ee:00
DestinationNtDomain	字符串	255个字符	目标的 Windows 域名。
DestinationPort	数字	从 -9223372036854775808 到 9223372036854775807	目标的端口号。
DestinationProcessID	数字	从 -9223372036854775808 到 9223372036854775807	在目标上注册的系统进程 ID。
DestinationProcessName	字符串	1023个字符	在目标上注册的系统进程名称。例如，sshd、telnet。
DestinationRegion	字符串	1023个字符	与 DestinationAddress 字段中的 IP 地址对应的区域。
DestinationServiceName	字符串	1023个字符	目标端服务的名称。例如，sshd。
DestinationTranslatedAddress	字符串	45个字符	转换后的目标 IPv4 或 IPv6 地址。例如，0.0.0.0 或 xxxx:xxxx:xxxx:x
DestinationTranslatedPort	数字	从 -9223372036854775808 到 9223372036854775807	转换后的目标端口号。
DestinationUserID	字符串	1023个字符	目标的用户 ID。
DestinationUserName	字符串	1023个字符	目标的用户名。
DestinationUserPrivileges	字符串	1023个字符	用于标识目标端用户权限的角色名称。例如，用户、访客、管理员
DeviceAction	字符串	63个字符	事件源采取的操作。例如，已阻止、检测到。
DeviceAddress	字符串	45个字符	发送事件的设备的 IPv4 或 IPv6 地址。例如，0.0.0.0 或 xxxx:xxxx:x

DeviceCity	字符串	1023个字符	与 DeviceAddress 字段中的 IP 地址对应的城市。
DeviceCountry	字符串	1023个字符	与 DeviceAddress 字段中的 IP 地址对应的国家/地区。
DeviceDnsDomain	字符串	255个字符	发送事件的设备的完全限定域名的 DNS 部分。
DeviceEventClassID	字符串	1023个字符	事件源分配的事件类型 ID。
DeviceExternalID	字符串	255个字符	事件源分配的设备或应用程序 ID。
DeviceFacility	字符串	1023个字符	事件源设置的设备参数值。
DeviceHostName	字符串	100个字符	发送事件的设备的名称。设备的 FQDN（如果有）。
DeviceInboundinterface	字符串	128个字符	传入连接接口的名称。
DeviceLatitude	浮点数	+/- 1.7E-308 至 1.7E+308	与 DeviceAddress 字段中的 IP 地址对应的经度。
DeviceLongitude	浮点数	+/- 1.7E-308 至 1.7E+308	与 DeviceAddress 字段中的 IP 地址对应的纬度。
DeviceMacAddress	字符串	17个字符	发送事件的资产的 MAC 地址。例如，aa:bb:cc:dd:ee:00
DeviceNtDomain	字符串	255个字符	设备的 Windows 域名。
DeviceOutboundinterface	字符串	128个字符	传出连接接口的名称。
DevicePayloadID	字符串	128个字符	与原始事件关联的有效负载唯一 ID。
DeviceProcessID	数字	从 -9223372036854775808 到 9223372036854775807	生成事件的设备上的系统进程 ID。
DeviceProcessName	字符串	1023个字符	进程名称。
DeviceProduct	字符串	63个字符	生成事件的应用程序名称。DeviceVendor、DeviceProduct 和 Dev
DeviceReceiptTime	数字	从 -9223372036854775808 到 9223372036854775807	设备接收事件的时间。
DeviceRegion	字符串	1023个字符	与 DeviceAddress 字段中的 IP 地址对应的区域。
DeviceTimeZone	字符串	255个字符	生成事件的设备的时区。
DeviceTranslatedAddress	字符串	45个字符	发送事件的设备的重新转换后的 IPv4 或 IPv6 地址。例如，0.0.0.0
DeviceVendor	字符串	63个字符	事件源的厂商名称。DeviceVendor、DeviceProduct 和 DeviceVer
DeviceVersion	字符串	31个字符	事件源的应用程序版本。DeviceVendor、DeviceProduct 和 Devic
EndTime	数字	从 -9223372036854775808 到 9223372036854775807	事件结束的日期和时间（时间戳）。
EventOutcome	字符串	63个字符	操作结果。例如，成功、失败。
ExternalID	字符串	40个字符	可以保存 ID 的字段。
FileCreateTime	数字	从 -9223372036854775808 到 9223372036854775807	文件创建时间。
FileHash	字符串	255个字符	文件的哈希值。示例：CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C49401
FileID	字符串	1023个字符	文件的 ID。
FileModificationTime	数字	从 -9223372036854775808 到 9223372036854775807	文件最后修改时间。
FileName	字符串	1023个字符	文件名，未指定文件路径。
FilePath	字符串	1023个字符	文件路径，包括文件名。
FilePermission	字符串	1023个字符	文件权限列表。

FileSize	数字	从 -9223372036854775808 到 9223372036854775807	文件大小。
FileType	字符串	1023个字符	文件类型。
消息	字符串	1023个字符	事件的简要描述。
名称	字符串	512个字符	事件的名称。
OldFileCreateTime	数字	从 -9223372036854775808 到 9223372036854775807	从事件创建 OLD 文件的时间。以 UTC0 指定时间。在 KUMA 控制
OldFileHash	字符串	255个字符	旧文件的哈希值。示例：CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C49401
OldFileID	字符串	1023个字符	旧文件的 ID。
OldFileModificationTime	数字	从 -9223372036854775808 到 9223372036854775807	旧文件最后修改的时间。
OldFileName	字符串	1023个字符	旧文件的名称（不含文件路径）。
OldFilePath	字符串	1023个字符	旧文件的路径，包含文件名。
OldFilePermission	字符串	1023个字符	旧文件的权限列表。
OldFileSize	数字	从 -9223372036854775808 到 9223372036854775807	旧文件的大小。
OldFileType	字符串	1023个字符	旧文件的类型。
原因	字符串	1023个字符	事件原因信息。
RequestClientApplication	字符串	1023个字符	http 请求的"用户-代理"参数的值。
RequestContext	字符串	2048个字符	http 请求上下文的描述。
RequestCookies	字符串	1023个字符	与 http 请求关联的 Cookie。
RequestMethod	字符串	1023个字符	发出 http 请求时使用的方法。
RequestUrl	字符串	1023个字符	请求的 URL。
严重级别	字符串	1023个字符	严重级别。这可以是原始事件的"严重级别"字段或"级别"字段。
SourceAddress	字符串	45个字符	源的 IPv4 或 IPv6 地址。示例格式：0.0.0.0 或 xxxx:xxxx:xxxx:xxxx:x
SourceCity	字符串	1023个字符	与 SourceAddress 字段中的 IP 地址对应的城市。
SourceCountry	字符串	1023个字符	与 SourceAddress 字段中的 IP 地址对应的国家/地区。
SourceDnsDomain	字符串	255个字符	源的完全限定域名的 DNS 部分。
SourceHostName	字符串	1023个字符	事件源设备的 Windows 域名。
SourceLatitude	浮点数	+/- 1.7E-308 至 1.7E+308	与 SourceAddress 字段中的 IP 地址对应的经度。
SourceLongitude	浮点数	+/- 1.7E-308 至 1.7E+308	与 SourceAddress 字段中的 IP 地址对应的纬度。
SourceMacAddress	字符串	17个字符	源的 MAC 地址。格式示例：aa:bb:cc:dd:ee:00
SourceNtDomain	字符串	255个字符	源的 Windows 域名。
SourcePort	数字	从 -9223372036854775808 到 9223372036854775807	源端口号。
SourceProcessID	数字	从 -9223372036854775808 到 9223372036854775807	系统进程 ID。
SourceProcessName	字符串	1023个字符	源端系统进程名称。例如 sshd、telnet 等。

SourceRegion	字符串	1023个字符	SourceAddress 字段 IP 地址对应的地区。
SourceServiceName	字符串	1023个字符	源端服务名称。例如，sshd。
SourceTranslatedAddress	字符串	15个字符	源端转换后的 IPv4 或 IPv6 地址。示例格式：0.0.0.0 或 xxxx:xxxx:x
SourceTranslatedPort	数字	从 -9223372036854775808 到 9223372036854775807	转换后的源端口号。
SourceUserID	字符串	1023个字符	源的用户 ID。
SourceUserName	字符串	1023个字符	源的用户名。
SourceUserPrivileges	字符串	1023个字符	标识源的用户权限的角色名称。例如，用户、访客、管理员等。
StartTime	数字	从 -9223372036854775808 到 9223372036854775807	与事件关联的活动开始的日期和时间（时间戳）。
Tactic	字符串	128个字符	来自 MITRE ATT&CK 矩阵的战术名称。
Technique	字符串	128个字符	来自 MITRE ATT&CK 矩阵的技术名称。
TransportProtocol	字符串	31个字符	OSI 模型的传输层协议名称（TCP、UDP 等）。
类型	数字	从 -9223372036854775808 到 9223372036854775807	事件类型：1 - 基本，2 - 聚合，3 - 关联，4 - 审计，5 - 监控。
用户可以定义其用途的字段。字段可修改。			
DeviceCustomDate1	数字、时间戳	从 -9223372036854775808 到 9223372036854775807	用于映射日期和时间值（时间戳）的字段。以 UTC0 指定时间。在
DeviceCustomDate1Label	字符串	1023个字符	用于描述 DeviceCustomDate1 字段用途的字段。
DeviceCustomDate2	数字、时间戳	从 -9223372036854775808 到 9223372036854775807	用于映射日期和时间值（时间戳）的字段。以 UTC0 指定时间。在
DeviceCustomDate2Label	字符串	1023个字符	用于描述 DeviceCustomDate2 字段用途的字段。
DeviceCustomFloatingPoint1	浮点数	+/- 1.7E-308 至 1.7E+308	用于映射浮点数的字段。
DeviceCustomFloatingPoint1Label	字符串	1023个字符	用于描述 DeviceCustomFloatingPoint1 字段用途的字段。
DeviceCustomFloatingPoint2	浮点数	+/- 1.7E-308 至 1.7E+308	用于映射浮点数的字段。
DeviceCustomFloatingPoint2Label	字符串	1023个字符	用于描述 DeviceCustomFloatingPoint2 字段用途的字段。
DeviceCustomFloatingPoint3	浮点数	+/- 1.7E-308 至 1.7E+308	用于映射浮点数的字段。
DeviceCustomFloatingPoint3Label	字符串	1023个字符	用于描述 DeviceCustomFloatingPoint3 字段用途的字段。
DeviceCustomFloatingPoint4	浮点数	+/- 1.7E-308 至 1.7E+308	用于映射浮点数的字段。
DeviceCustomFloatingPoint4Label	字符串	1023个字符	用于描述 DeviceCustomFloatingPoint4 字段用途的字段。
DeviceCustomIPv6Address1	字符串	45个字符	用于映射 IPv6 地址值的字段。格式示例：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address1Label	字符串	1023个字符	用于描述 DeviceCustomIPv6Address1 字段用途的字段。
DeviceCustomIPv6Address2	字符串	45个字符	用于映射 IPv6 地址值的字段。格式示例：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address2Label	字符串	1023个字符	用于描述 DeviceCustomIPv6Address2 字段用途的字段。
DeviceCustomIPv6Address3	字符串	45个字符	用于映射 IPv6 地址值的字段。格式示例：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address3Label	字符串	1023个字符	用于描述 DeviceCustomIPv6Address3 字段用途的字段。
DeviceCustomIPv6Address4	字符串	45个字符	用于映射 IPv6 地址值的字段。例如，y:y:y:y:y:y:y:y
DeviceCustomIPv6Address4Label	字符串	1023个字符	用于描述 DeviceCustomIPv6Address4 字段用途的字段。

DeviceCustomNumber1	数字	从 -9223372036854775808 到 9223372036854775807	用于映射整数值的字段。
DeviceCustomNumber1Label	字符串	1023个字符	用于描述 DeviceCustomNumber1 字段用途的字段。
DeviceCustomNumber2	数字	从 -9223372036854775808 到 9223372036854775807	用于映射整数值的字段。
DeviceCustomNumber2Label	字符串	1023个字符	用于描述 DeviceCustomNumber2 字段用途的字段。
DeviceCustomNumber3	数字	从 -9223372036854775808 到 9223372036854775807	用于映射整数值的字段。
DeviceCustomNumber3Label	字符串	1023个字符	用于描述 DeviceCustomNumber3 字段用途的字段。
DeviceCustomString1	字符串	4,000个字符	用于映射字符串值的字段。
DeviceCustomString1Label	字符串	1023个字符	用于描述 DeviceCustomString1 字段用途的字段。
DeviceCustomString2	字符串	4,000个字符	用于映射字符串值的字段。
DeviceCustomString2Label	字符串	1023个字符	用于描述 DeviceCustomString2 字段用途的字段。
DeviceCustomString3	字符串	4,000个字符	用于映射字符串值的字段。
DeviceCustomString3Label	字符串	1023个字符	用于描述 DeviceCustomString3 字段用途的字段。
DeviceCustomString4	字符串	4,000个字符	用于映射字符串值的字段。
DeviceCustomString4Label	字符串	1023个字符	用于描述 DeviceCustomString4 字段用途的字段。
DeviceCustomString5	字符串	4,000个字符	用于映射字符串值的字段。
DeviceCustomString5Label	字符串	1023个字符	用于描述 DeviceCustomString5 字段用途的字段。
DeviceCustomString6	字符串	4,000个字符	用于映射字符串值的字段。
DeviceCustomString6Label	字符串	1023个字符	用于描述 DeviceCustomString6 字段用途的字段。
DeviceDirection	数字	从 -9223372036854775808 到 9223372036854775807	用于描述事件连接方向的字段。“0”- 传入连接，“1”- 传出连接。
DeviceEventCategory	字符串	1023个字符	由向 SIEM 发送事件的设备分配的事件类别。
FlexDate1	数字、时间戳	从 -9223372036854775808 到 9223372036854775807	用于映射日期和时间值（时间戳）的字段。以 UTC0 指定时间。在
FlexDate1Label	字符串	128个字符	用于描述 FlexDate1Label 字段用途的字段。
FlexNumber1	数字	从 -9223372036854775808 到 9223372036854775807	用于映射整数值的字段。
FlexNumber1Label	字符串	128个字符	用于描述 FlexNumber1Label 字段用途的字段。
FlexNumber2	数字	从 -9223372036854775808 到 9223372036854775807	用于映射整数值的字段。
FlexNumber2Label	字符串	128个字符	用于描述 FlexNumber2Label 字段用途的字段。
FlexString1	字符串	1023个字符	用于映射字符串值的字段。
FlexString1Label	字符串	128个字符	用于描述 FlexString1Label 字段用途的字段。
FlexString2	字符串	1023个字符	用于映射字符串值的字段。
FlexString2Label	字符串	128个字符	用于描述 FlexString2Label 字段用途的字段。
			服务字段。无法编辑。

AffectedAssets	嵌套的 [Affected] 结构	-	嵌套结构，您可以从中查询与警报相关的资产和用户账户，并找出
AggregationRuleID	字符串	-	聚合规则的 ID。
AggregationRuleName	字符串	-	处理事件的聚合规则的名称。
BaseEventCount	数字	-	对于聚合基础事件，这是聚合规则处理的基础事件数量。对于关联 数量。
BaseEvents	嵌套的 [Event] 列表	-	包含基础事件列表的嵌套结构。关联事件可以填写此字段。
代码	字符串	-	在基础事件中，这是从源返回的流程、函数或操作的代码。
CorrelationRuleID	字符串	-	关联规则的 ID。
CorrelationRuleName	字符串	-	触发关联事件创建的关联规则的名称。仅关联事件需要填写。
DestinationAccountID	字符串	-	此字段存储用户 ID。
DestinationAssetID	字符串	-	此字段存储目标的资产 ID。
设备资产 ID	字符串	-	此字段存储将事件发送到 SIEM 的资产的 ID。
额外	嵌套的 [string:string] 字典	-	在原始事件的规范化过程中，此字段可用于放置尚未映射到 KUMA 段的最大大小为 4 MB。
GroupedBy	字符串	-	关联规则中用于分组的字段名称列表。仅关联事件需要填写此字段
ID	字符串	-	UUID 类型的唯一事件 ID。对于在收集器上生成的基础事件，ID 由 改变。
Raw	字符串	-	原始"raw"事件的非规范化文本。字段最大容量是 16,384 字节。
ReplayID	字符串	-	生成事件的回溯扫描 ID。
ServiceID	字符串	-	服务实例（关联器、收集器、存储）的 ID。
ServiceName	字符串	-	KUMA 管理员在创建微服务时分配的微服务实例的名称。
SourceAccountID	字符串	-	此字段存储用户 ID。
SourceAssetID	字符串	-	此字段存储事件源的资产 ID。
SpaceID	字符串	-	空间 ID。
TenantID	字符串	-	此字段存储租户的 ID。
TI	嵌套的 [string:string] 字典	-	此字段包含外部威胁情报源基于事件中的指标、以字典格式返回的
TICategories	map[String]	-	此字段包含外部威胁情报提供商基于事件中所含指标返回的类别信
时间戳	数字	-	收集器中创建的基础事件的时间戳。收集器创建关联事件的时间。 户浏览器的时区显示。

嵌套的 `Affected` 结构

字段	数据类型	描述
`Assets`	嵌套的 `[AffectedRecord]` 列表	与警报关联的资产列表和数量。
`Accounts`	嵌套的 `[AffectedRecord]` 列表	与警报关联的用户账户列表和数量。

嵌套的 `AffectedRecord` 结构

字段	数据类型	描述
`Value`	字符串	资产或用户账户的 ID。
`Count`	数字	资产或用户账户在警报相关事件中出现的次数。

KUMA 生成的字段

KUMA 生成以下无法修改的字段：BranchID、BranchName、DestinationAccountName、DestinationAssetName、DeviceAssetName、SourceAccountName、SourceAssetName、TenantName。

配置来自 KATA EDR 的规范化事件的数据模型

要调查信息，事件和 KATA/EDR 进程的 ID 必须填入规范化事件的特定字段中。要为来自 KATA/EDR 的事件构建进程树，必须在 KUMA 规范化器中按以下方式，将原始事件字段中的数据复制到规范化事件的对应字段：

1. 对于任何 KATA/EDR 事件，您必须通过复制以下字段来配置规范化：
   - KATA/EDR 事件的 `EventType` 字段必须复制到规范化 KUMA 事件的 `DeviceEventCategory` 字段。
   - KATA/EDR 事件的 `HostName` 字段必须复制到规范化 KUMA 事件的 `DeviceHostName` 字段。
2. 对于 DeviceProduct = 'KATA' 的任何事件，必须根据下表配置规范化。

KATA/EDR 事件字段的规范化

KATA/EDR 事件字段	规范化事件字段
IOATag	DeviceCustomIPv6Address2
	IOATag
IOAImportance	DeviceCustomIPv6Address1
	IOAImportance
FilePath	FilePath
FileName	FileName
MD5	FileHash
FileSize	FileSize

3. 对于下表列出的事件，必须根据表格配置带有字段复制的额外规范化。

通过复制 KATA/EDR 事件字段进行额外规范化

事件	原始事件字段	规范化事件字段
Process	UniqueParentPid	FlexString1
	UniquePid	FlexString2
	hostName	DeviceHostName
	FileName	FileName

事件	原始事件字段	规范化事件字段
Applock	UniquePid	FlexString2
	hostName	DeviceHostName
	FileName	FileName
BlockedDocument	UniquePid	FlexString2
	hostName	DeviceHostName
	FileName	FileName
Module	UniquePid	FlexString2
	hostName	DeviceHostName
	FileName	FileName
FileChange	UniquePid	FlexString2
	hostName	DeviceHostName
	FileName	FileName
驱动程序	hostName	DeviceHostName
	FileName	FileName
	ProductName	DeviceCustomString5
		ProductName
	ProductVendor	DeviceCustomString6
		ProductVendor
连接	UniquePid	FlexString2
	hostName	DeviceHostName
	URl	RequestUrl
	RemoteIP	DestinationAddress
	RemotePort	DestinationPort
PortListen	UniquePid	FlexString2
	hostName	DeviceHostName
	LocalIP	SourceAddress
	LocalPort	SourcePort

事件	原始事件字段	规范化事件字段
注册表	UniquePid	FlexString2
	hostName	DeviceHostName
	ValueName	DeviceCustomString5
		新值名称
	KeyName	DeviceCustomString4
		新密钥名称
	PreviousKeyName	FlexString2
		旧密钥名称
	ValueData	DeviceCustomString6
		新值数据
	PreviousValueData	FlexString1
		旧值数据
	ValueType	FlexNumber1
		值类型
	PreviousValueType	FlexNumber2
		旧值类型
SystemEventLog	UniquePid	FlexString2
	hostName	DeviceHostName
	OperationResult	EventOutcome
	EventId	DeviceCustomNumber3
		EventId
	EventRecordId	DeviceCustomNumber2
		EventRecordId
	Channel	DeviceCustomString6
		Channel
	ProviderName	SourceUserID
ThreatDetect	UniquePid	FlexString2
	hostName	DeviceHostName
	VerdictName	EventOutcome
	DetectedObjectType	OldFileType
	isSilent	FlexString1
		是否静默
	RecordId	DeviceCustomString5
		记录 ID
	DatabaseTimestamp	DeviceCustomDate2
		数据库时间戳
ThreatDetectProcessingResult	UniquePid	FlexString2
	hostName	DeviceHostName
	威胁状态	DeviceCustomString5
		威胁状态

事件	原始事件字段	规范化事件字段
PROCESS_INTERPRET_FILE_RUN	UniquePid	FlexString2
	hostName	DeviceHostName
	FileName	FileName
	InterpretedFilePath	OldFilePath
	InterpretedFileSize	OldFileSize
	InterpretedFileHash	OldFileHash
PROCESS_CONSOLE_INTERACTIVE_INPUT	UniquePid	FlexString2
	hostName	DeviceHostName
	InteractiveInputText	DeviceCustomString4
		命令行
AMSI SCAN	UniquePid	FlexString2
	hostName	DeviceHostName
	ObjectContent	DeviceCustomString5
		对象内容

资产数据模型

资产的结构用包含值的字段表示。字段还可以包含嵌套结构。

资产字段	值类型	描述
`ID`	字符串	资产 ID。
`TenantName`	字符串	租户名称。
`DeletedAt`	数字	资产删除日期。
`CreatedAt`	数字	资产创建日期。
`TenantID`	字符串	租户 ID。
`DirectCategories`	嵌套的字符串列表	资产类别。
`CategoryModels`	嵌套的 `[Category]` 结构	更改资产类别。
`AffectedByIncidents`	嵌套字典： `[string:string TRUE/FALSE]`	事故 ID。
`IPAddress`	嵌套的字符串列表	资产 IP 地址。
`FQDN`	字符串	资产 FQDN。
`Weight`	数字	资产重要性。
`Deleted`	包含 `TRUE/FALSE` 值的字符串	指示该资产是否已标记为从 KUMA 中删除的标志。
`UpdatedAt`	数字	资产的最后更新日期。
`MACAddress`	嵌套的字符串列表	资产 MAC 地址。
`IPAddressInt`	嵌套的数字列表	数字格式的 IP 地址。
`Owner`	嵌套的 [OwnerInfo] 结构	资产所有者信息。
`OS`	嵌套的 [OS] 结构	资产操作系统信息。
`displayName`	字符串	资产名称。
`APISoft`	嵌套的 [Software] 结构	资产上安装的软件。

APIVulns	嵌套的 [Vulnerability] 结构	资产漏洞。
KICSServerIp	字符串	KICS for Networks 服务器 IP 地址。
KICSConnectorID	数字	KICS for Networks 连接器 ID。
KICSDeviceID	数字	KICS for Networks 资产 ID。
KICSStatus	字符串	KICS for Networks 资产状态。
KICSHardware	嵌套的 [KICSSystemInfo] 结构	从 KICS for Networks 接收的资产硬件信息。
KICSSoft	嵌套的 [KICSSystemInfo] 结构	从 KICS for Networks 接收的资产软件信息。
KICSRisks	嵌套的 [KICSRisk] 结构	从 KICS for Networks 接收的资产漏洞信息。
Sources	嵌套的 [Sources] 结构	来自各种来源的资产基本信息。
FromKSC	包含 TRUE/FALSE 值的字符串	指示已从 Kaspersky Security Center 导入资产详细信息的标志。
NAgentID	字符串	接收资产信息的 Kaspersky Security Center 网络代理的 ID。
KSCServerFQDN	字符串	Kaspersky Security Center 服务器的 FQDN。
KSCInstanceID	字符串	Kaspersky Security Center 实例 ID。
KSCMasterHostname	字符串	Kaspersky Security Center 服务器主机名。
KSCGroupID	数字	Kaspersky Security Center 组 ID。
KSCGroupName	字符串	Kaspersky Security Center 组名。
LastVisible	数字	从 Kaspersky Security Center 上次收到资产相关信息的日期。
Products	嵌套字典： [string:nested [ProductInfo] structure]	从 Kaspersky Security Center 接收的有关安装在资产上的卡巴斯基应用程序的信息。
Hardware	嵌套的 [Hardware] 结构	从 Kaspersky Security Center 接收的资产硬件信息。
KSCSoft	嵌套 [软件] 结构	从 Kaspersky Security Center 接收的资产软件信息。
KSCVulns	嵌套 [漏洞] 结构	从 Kaspersky Security Center 接收的资产漏洞信息。

嵌套的类别结构

字段	值类型	描述
ID	字符串	类别 ID。
TenantID	字符串	租户 ID。
TenantName	字符串	租户名称。
Parent	字符串	父类别。
Path	嵌套字符串列表	类别结构。
Name	字符串	类别名称。
UpdatedAt	数字	类别的上次更新。
CreatedAt	数字	类别创建日期。
Description	字符串	类别描述。
Weight	数字	类别重要性。
CategorizationKind	字符串	资产类别分配类型。
CategorizationAt	数字	分类日期。
CategorizationInterval	字符串	类别分配间隔。

嵌套的所有者信息结构

字段	值类型	描述
displayName	字符串	资产所有者的名称。

嵌套的操作系统结构

字段	值类型	描述
Name	字符串	操作系统名称。
BuildNumber	数字	操作系统版本。

嵌套的软件结构

字段	值类型	描述
displayName	字符串	软件名称。
DisplayVersion	字符串	软件版本。
Publisher	字符串	软件发布者。
InstallDate	字符串	安装日期。
HasMSIInstaller	TRUE/FALSE 字符串	指示软件是否包含 MSI 安装程序。

嵌套的漏洞结构

字段	值类型	描述
KasperskyID	字符串	卡巴斯基分配的漏洞 ID。
ProductName	字符串	软件名称。
DescriptionURL	字符串	包含漏洞描述的 URL。
RecommendedMajorPatch	字符串	建议更新。
RecommendedMinorPatch	字符串	建议更新。
SeverityStr	字符串	漏洞严重级别。
Severity	数字	漏洞严重级别。
CVE	嵌套的字符串列表	CVE 漏洞 ID。
ExploitExists	TRUE/FALSE 字符串	指示是否存在漏洞利用。
MalwareExists	TRUE/FALSE 字符串	指示是否存在恶意软件。

嵌套的 KICS 系统信息结构

字段	值类型	描述
Model	字符串	设备模型。
Version	字符串	设备版本。
Vendor	字符串	供应商。

嵌套的 KICS 风险结构

字段	值类型	描述
ID	数字	KICS for Networks 风险 ID。
Name	字符串	风险名称。
Category	字符串	风险类型。
Description	字符串	风险描述。
DescriptionURL	字符串	风险描述链接。
Severity	数字	风险严重级别。
Cvss	数字	CVSS 分数。

嵌套的源结构

字段	值类型	描述
KSC	嵌套的 [SourceInfo] 结构	从 Kaspersky Security Center 接收的资产信息。
API	嵌套的 [SourceInfo] 结构	通过 REST API 接收的资产信息。
Manual	嵌套的 [SourceInfo] 结构	手动输入的资产相关信息。
KICS	嵌套的 [SourceInfo] 结构	从 KICS for Networks 接收的资产信息。

嵌套的源结构

字段	值类型	描述
MACAddress	嵌套的字符串列表	资产 MAC 地址。
IPAddressInt	嵌套的数字列表	数字格式的 IP 地址。
Owner	嵌套的 [OwnerInfo] 结构	资产所有者信息。
OS	嵌套的 [OS] 结构	资产操作系统信息。
displayName	字符串	资产名称。
IPAddress	嵌套的字符串列表	资产 IP 地址。

FQDN	字符串	资产 FQDN。
Weight	数字	资产重要性。
Deleted	包含 TRUE/FALSE 值的字符串	指示该资产是否已标记为从 KUMA 中删除的标志。
UpdatedAt	数字	资产的最后更新日期。

嵌套的产品信息结构

字段	值类型	描述
ProductVersion	字符串	软件版本。
ProductName	字符串	软件名称。

嵌套的硬件结构

字段	值类型	描述
NetCards	嵌套的 [NetCard] 结构	资产网卡列表。
CPU	嵌套的 [CPU] 结构	资产处理器列表。
RAM	嵌套的 [RAM] 结构	资产 RAM 列表。
Disk	嵌套的 [Disk] 结构	资产驱动器列表。

嵌套的 Netcard 结构

字段	值类型	描述
ID	字符串	网卡 ID。
MACAddresses	嵌套的字符串列表	网卡的 MAC 地址。
Name	字符串	网卡名称。
Manufacture	字符串	网卡制造商。
DriverVersion	字符串	驱动程序版本。

嵌套的 RAM 结构

字段	值类型	描述
Frequency	字符串	RAM 频率。
TotalBytes	数字	RAM 数量（以字节为单位）。

嵌套的 CPU 结构

字段	值类型	描述
ID	字符串	CPU ID。
Name	字符串	CPU 名称。
CoreCount	字符串	核心数。
CoreSpeed	字符串	频率。

嵌套的磁盘结构

字段	值类型	描述
FreeBytes	数字	可用磁盘空间。
TotalBytes	数字	总磁盘空间。

用户账户数据模型

用户账户字段可在电子邮件模板中引用，也可在事件关联过程中调用。

字段	值类型	描述
ID	字符串	用户账户 ID。
ObjectGUID	字符串	Active Directory 属性。Active Directory 中的用户账户 ID。
TenantID	字符串	租户 ID。
TenantName	字符串	租户名称。
UpdatedAt	数字	用户账户的上次更新。
Domain	字符串	域。
CN	字符串	Active Directory 属性。用户名。
displayName	字符串	Active Directory 属性。显示的用户名。
DistinguishedName	字符串	Active Directory 属性。LDAP 对象名称。
employeeID	字符串	Active Directory 属性。员工 ID。
Mail	字符串	Active Directory 属性。用户电子邮件地址。
mailNickname	字符串	Active Directory 属性。备用电子邮件地址。
Mobile	字符串	Active Directory 属性。手机号码。
ObjectSID	字符串	Active Directory 属性。安全 ID。
SAMAccountName	字符串	Active Directory 属性。登录名。
TelephoneNumber	字符串	Active Directory 属性。电话号码。
UserPrincipalName	字符串	Active Directory 属性。用户主体名称 (UPN)。
Archived	TRUE/FALSE string	判定用户账户是否已废弃的标志。

MemberOf	字符串列表	Active Directory 属性。用户加入的 Active Directory 组。 此属性可用于关联期间的事件搜索。
PreliminarilyArchived	TRUE/FALSE string	判定用户账户是否应标记为废弃状态的标志。
CreatedAt	数字	用户账户创建日期。
SN	字符串	Active Directory 属性。用户的姓氏。
SAMAccountType	字符串	Active Directory 属性。用户账户类型。
Title	字符串	Active Directory 属性。用户的职务。
Division	字符串	Active Directory 属性。用户所在部门。
Department	字符串	Active Directory 属性。用户所在事业部。
Manager	字符串	Active Directory 属性。用户的主管。
Location	字符串	Active Directory 属性。用户位置。
Company	字符串	Active Directory 属性。用户所在公司。
StreetAddress	字符串	Active Directory 属性。公司地址。
PhysicalDeliveryOfficeName	字符串	Active Directory 属性。配送地址。
managedObjects	字符串列表	Active Directory 属性。用户控制的对象。
UserAccountControl	数字	Active Directory 属性。Active Directory 账户类型。
WhenCreated	数字	Active Directory 属性。用户账户创建日期。
WhenChanged	数字	Active Directory 属性。用户账户修改日期。
AccountExpires	数字	Active Directory 属性。用户账户到期日期。
BadPasswordTime	数字	Active Directory 属性。上次登录尝试失败的日期。

审计事件

在OSMP中完成某些与安全相关的操作时，会创建审计事件。这些事件用于确保系统完整性。

审计事件在KUMA Core服务器上创建，并发送到主租户的存储（主租户关联器）。因此，必须在主租户中至少创建一个存储来存储审计事件。如果不存在存储，您需要创建一个。审计事件发送到审计空间，该空间在存储中自动创建。

[OOTB] Kaspersky OSMP收集器在OSMP安装期间自动部署，用于接收来自OSMP组件的审计事件。[OOTB] Kaspersky OSMP收集器无法删除。

要查看审计事件，您需要转到**威胁搜索**区域，并将`SELECT * FROM 'events' WHERE Type=4`添加到查询中。

执行查询后，如果用户和角色允许查看审计事件，则会显示审计事件。

包含一般信息的事件字段

每个审计事件都具有下表描述的事件字段。

事件字段名称	字段值
Timestamp	事件时间。

DeviceHostName	事件源主机。对于审计事件，主机名是安装了kuma-core服务的主机名，因为该服务是事件来源。
DeviceTimeZone	托管 KUMA Core 的服务器的系统时间时区，格式为 +-hh:mm。
Type	审计事件类型：Audit或Base。
TenantID	租户 ID。
DeviceVendor	"Kaspersky"
DeviceProduct	KUMA
EndTime	事件创建时间。
SpaceID	KUMA Audit
DeviceAction	审计事件中捕获的操作。

用户已编辑字段集设置来定义来源

事件字段名称	字段值
DeviceAction	settings updated
DeviceFacility	eventSourceIdentity
EventOutcome	succeeded
SourceUserName	进行更改的用户的帐户名。
SourceUserID	进行更改的用户ID。
DeviceCustomString5	已更新字段集，| 用作分隔符。

密钥文件已添加

事件字段名称	字段值
DeviceAction	license key installed
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	添加密钥文件的用户ID。
SourceUserName	添加密钥文件的用户的帐户名。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

备用授权许可密钥已添加

事件字段名称	字段值
DeviceAction	reserve license key installed
DeviceAddress	添加备用授权许可密钥的设备的IP地址。
EventOutcome	succeeded

Message	授权许可名称。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserID	添加备用授权许可密钥的用户ID。
SourceUserName	添加备用授权许可密钥的用户的帐户名。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

备用授权许可密钥已删除

事件字段名称	字段值
DeviceAction	reserve license key uninstalled
DeviceAddress	删除备用授权许可密钥的设备的IP地址。
EventOutcome	succeeded
Message	授权许可名称。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserID	删除备用授权许可密钥的用户ID。
SourceUserName	删除备用授权许可密钥的用户帐户名。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

应用程序已使用激活码激活。

事件字段名称	字段值
DeviceAction	license activated
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	输入激活码的用户ID。
SourceUserName	输入激活码的用户账号名称。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

授权许可已续期。

事件字段名称	字段值
DeviceAction	license reactivated
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	添加密钥文件的用户ID。
SourceUserName	添加密钥文件的用户的帐户名。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

无效的激活码

事件字段名称	字段值
DeviceAction	activation code license activated
EventOutcome	failed
Message	错误文本。
SourceUserID	输入激活码的用户ID。
SourceUserName	输入激活码的用户账号名称。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

激活码已被阻止

事件字段名称	字段值
DeviceAction	license blocked
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	输入激活码的用户ID。
SourceUserName	输入激活码的用户账号名称。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

激活码或密钥文件已删除

事件字段名称	字段值
DeviceAction	license uninstalled
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	删除密钥文件的用户ID。
SourceUserName	删除密钥文件的用户的帐户名。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

EPS已超限

事件字段名称	字段值
DeviceAction	license limit for EPS exceeded
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	添加密钥文件或输入激活码的用户ID。
SourceUserName	添加密钥文件或输入激活码的用户帐户名。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

授权许可已到期，宽限期已开始

事件字段名称	字段值
DeviceAction	license expired
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	添加密钥文件或输入激活码的用户ID。
SourceUserName	添加密钥文件或输入激活码的用户帐户名。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

宽限期结束

事件字段名称	字段值
DeviceAction	license ended
EventOutcome	succeeded
Message	授权许可名称。
SourceUserID	添加密钥文件或输入激活码的用户ID。
SourceUserName	添加密钥文件或输入激活码的用户帐户名。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

已添加过期的激活码或密钥文件

事件字段名称	字段值
DeviceAction	license key installed
IP	添加密钥文件或输入激活码的IP地址。
EventOutcome	failed
Message	错误文本。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserID	添加密钥文件或输入激活码的用户ID。
SourceUserName	添加密钥文件或输入激活码的用户帐户名。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

用于区分事件访问权限的空间集已更改

事件字段名称	字段值
DeviceAction	• space set was created • space set was deleted • space set was updated（包括授予和撤销访问权限）
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。

SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改设置的用户的帐户名。
SourceUserID	修改设置的用户ID。
DeviceCustomString5	空间集ID。
DeviceCustomString5Label	set ID
DeviceCustomString3	空间集名称。
DeviceCustomString3Label	space name

服务监控阈值已更改

事件字段名称	字段值
DeviceAction	settings updated
DeviceFacility	serviceAlertSettings
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改设置的用户的帐户名。
SourceUserID	修改设置的用户ID。
DeviceCustomString1	数据库中记录的阈值的JSON。
DeviceCustomString1Label	thresholds
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

KUMA Core设置已修改

事件字段名称	字段值
DeviceAction	settings updated
DeviceFacility	coreProperties
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改设置的用户的帐户名。
SourceUserID	修改设置的用户ID。
DeviceCustomString1	包含数据库中记录的KUMA Core设置值的JSON。
DeviceCustomString1Label	properties

GeoIP数据库已导入

事件字段名称	字段值
DeviceAction	new geobase imported
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	导入数据库的用户的帐户名。
SourceUserID	导入数据库的用户ID。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

服务已创建

事件字段名称	字段值
DeviceAction	service created
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	创建该服务的用户的帐户名。
SourceUserID	创建服务的用户ID。
DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

服务已删除

事件字段名称	字段值
DeviceAction	service deleted

EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	删除该服务的用户的帐户名。
SourceUserID	删除服务的用户ID。
DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DestinationAddress	用于启动服务的设备的地址。如果服务之前从未启动过，则该字段将为空。
DestinationHostName	用于启动服务的计算机的 FQDN。如果服务之前从未启动过，则该字段将为空。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

服务已重新加载

事件字段名称	字段值
DeviceAction	service reloaded
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	重启服务的用户的帐户名。
SourceUserID	重启服务的用户ID。
DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

服务已重新启动

事件字段名称	字段值
DeviceAction	service restarted
EventOutcome	succeeded

SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	重启服务的用户的帐户名。
SourceUserID	重启服务的用户ID。
DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

服务已启动

事件字段名称	字段值
DeviceAction	service started
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DestinationAddress	启动服务的设备的地址。
DestinationHostName	启动服务的设备的 FQDN。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

服务已配对

事件字段名称	字段值
DeviceAction	service paired
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。

DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

任务状态已更改

事件字段名称	字段值
DeviceAction	service status changed
DeviceExternalID	服务 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DestinationAddress	启动服务的设备的地址。
DestinationHostName	启动服务的设备的 FQDN。
DeviceCustomString1	green、yellow 或 red
DeviceCustomString1Label	new status
DeviceCustomString2	green、yellow 或 red
DeviceCustomString2Label	old status
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

分区已被用户删除

事件字段名称	字段值
DeviceAction	partition deleted
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	删除分区的用户的帐户名。
SourceUserID	删除分区的用户ID。
Name	存储名称|移动或删除分区的租户| 分区所属空间的名称。
DeviceCustomDate1	数据修改时间（UTC）。存储分区中 date 列显示的日期。

DeviceCustomDate1Label	date of event
Message	deleted by user

分区将在保留期结束后自动删除

事件字段名称	字段值
DeviceAction	applied retention policy by days
EventOutcome	succeeded
Name	行动手册所属的租户名。
DeviceCustomDate1	数据修改时间（UTC）。“日期”列中存储分区中显示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分区的大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件数量。
DeviceCustomNumber2Label	events
SourceServiceName	scheduler
Message	deleted partition data
DeviceEventCategory	event log 仅在删除审计分区时才会显示 DeviceEventCategory 字段。

分区已按绝对保留期删除

事件字段名称	字段值
Name	行动手册所属的租户名。
Message	deleted partition data
DeviceAction	applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	数据修改时间（UTC）。“日期”列中存储分区中显示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分区大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件数量。
DeviceCustomNumber2Label	events
EventOutcome	succeeded

分区已按相对保留期删除

事件字段名称	字段值
Name	行动手册所属的租户名。
Message	deleted partition data
DeviceAction	applied retention policy by percent
SourceServiceName	scheduler
DeviceCustomDate1	数据修改时间（UTC）。“日期”列中存储分区中显示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分区大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件数量。
DeviceCustomNumber2Label	events
EventOutcome	succeeded

分区已移至冷存储

事件字段名称	字段值
Name	行动手册所属的租户名。
Message	moved partition data to cold storage
DeviceAction	可用值如下： • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	数据修改时间（UTC）。“日期”列中存储分区中显示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分区大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件数量。
DeviceCustomNumber2Label	events
EventOutcome	succeeded
DeviceCustomString1	空间 ID。
DeviceCustomString1Label	nodeID

将分区移至冷存储时出错

事件字段名称	字段值
Name	行动手册所属的租户名。
Message	move partition data to cold storage failed: {"error":"Code: 243. DB::Exception: Move is not possible.Not enough space on 'cold_volume'. (NOT_ENOUGH_SPACE) (version 23.8.8.207)\n"}
DeviceAction	可用值如下： • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	数据修改时间（UTC）。“日期”列中存储分区中显示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分区大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件数量。
DeviceCustomNumber2Label	events
EventOutcome	failed
DeviceCustomString1	空间 ID。
DeviceCustomString1Label	nodeID

活动列表清除成功或操作失败

仅针对用户执行的操作创建活动列表的审计事件。使用关联规则修改活动列表时不会生成审计事件。**如果您需要跟踪此类更改，可以使用警报进行跟踪**。

如果使用定义了 **输出**和**循环**操作的**简单**类型关联规则修改活动列表，则每次触发该规则时都会创建活动列表修改警报。

该事件可被分配 `succeeded` 或 `failed` 状态。

由于清除活动列表的请求是通过远程连接发出的，因此数据传输错误可能在删除之前和删除之后随时发生。

这意味着活动列表可能已成功清除，但事件被分配了 `failed` 状态，因为 EventOutcome 返回请求的 TCP/IP 连接状态，但不返回活动列表清除的成功或失败状态。

审计事件“活动列表清除成功或操作失败”的字段值

事件字段名称	字段值
DeviceAction	active list cleared
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。

SourceUserName	用于清除活动列表的用户登录名。
SourceUserID	用于清除活动列表的用户 ID。
DeviceExternalID	已清除活动列表的服务 ID。
ExternalID	活动列表 ID。
Name	活动列表名称。
Message	如果 EventOutcome = failed，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	租户 ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

活动列表项更改成功或操作失败

仅针对用户执行的操作创建活动列表的审计事件。使用关联规则修改活动列表时不会生成审计事件。**如果您需要跟踪此类更改，可以使用警报进行跟踪**。

如果使用定义了 **输出**和**循环**操作的**简单**类型关联规则修改活动列表，则每次触发该规则时都会创建活动列表修改警报。

该事件可被分配 succeeded 或 failed 状态。

由于更改活动列表项的请求是通过远程连接发出的，因此数据传输错误可能在更改之前和之后随时发生。

这意味着活动列表项可能已成功更改，但事件被分配了 failed 状态，因为 EventOutcome 返回的是请求的 TCP/IP 连接状态，而不是活动列表项更改的成功或失败状态。

审计事件"活动列表项更改成功或操作失败"的字段值

事件字段名称	字段值
DeviceAction	active list item changed
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于更改活动列表项的用户登录名。
SourceUserID	用于更改活动列表项的用户 ID。
DeviceExternalID	已更改活动列表的服务 ID。
ExternalID	活动列表 ID。
Name	活动列表名称。
DeviceCustomString1	键名。
DeviceCustomString1Label	key
Message	如果 EventOutcome = failed，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	tenant ID

DeviceCustomString6	租户名称
DeviceCustomString6Label	tenant name

活动列表项删除成功或操作失败

仅针对用户执行的操作创建活动列表的审计事件。使用关联规则修改活动列表时不会生成审计事件。**如果您需要跟踪此类更改，可以使用警报进行跟踪**。

如果使用定义了 **输出**和**循环**操作的**简单**类型关联规则修改活动列表，则每次触发该规则时都会创建活动列表修改警报。

该事件可被分配 `succeeded` 或 `failed` 状态。

由于删除活动列表项的请求是通过远程连接发出的，因此数据传输错误可能在删除之前和删除之后随时发生。

这意味着活动列表项可能已成功删除，但事件被分配了 `failed` 状态，因为 EventOutcome 返回的是请求的 TCP/IP 连接状态，而不是活动列表项删除的成功或失败状态。

审计事件"活动列表项删除成功或操作失败"的字段值

事件字段名称	字段值
DeviceAction	active list item deleted
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于删除活动列表项的用户登录名。
SourceUserID	用于删除活动列表项的用户 ID。
DeviceExternalID	已清除活动列表的服务 ID。
ExternalID	活动列表 ID。
Name	活动列表名称。
DeviceCustomString1	键名。
DeviceCustomString1Label	key
Message	如果 EventOutcome = failed，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

活动列表导入成功或操作失败

仅针对用户执行的操作创建活动列表的审计事件。使用关联规则修改活动列表时不会生成审计事件。**如果您需要跟踪此类更改，可以使用警报进行跟踪**。

如果使用定义了 **输出**和**循环**操作的**简单**类型关联规则修改活动列表，则每次触发该规则时都会创建活动列表修改警报。

活动列表项通过远程连接分批导入。

由于导入是通过远程连接执行的，因此数据传输错误可能在数据部分导入或全部导入时随时发生。EventOutcome 返回连接状态，而不是导入状态。

审计事件"活动列表导入成功或操作失败"的字段值

事件字段名称	字段值
DeviceAction	active list imported
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于执行导入的用户登录名。
SourceUserID	用于执行导入的用户 ID。
DeviceExternalID	已执行导入操作的服务 ID。
ExternalID	活动列表 ID。
Name	活动列表名称。
Message	如果 EventOutcome = failed，可以在此处找到错误消息。错误文本可以采用 JSON 格式，例如 {"error":"line 1: header does not contain column IP!"}。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称
DeviceCustomString6Label	tenant name

活动列表已导出

仅针对用户执行的操作创建活动列表的审计事件。使用关联规则修改活动列表时不会生成审计事件。**如果您需要跟踪此类更改，可以使用警报进行跟踪**。

如果使用定义了 **输出**和**循环**操作的**简单**类型关联规则修改活动列表，则每次触发该规则时都会创建活动列表修改警报。

审计事件"活动列表已导出"的字段值

事件字段名称	字段值
DeviceAction	active list exported
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于执行导出的用户登录名。
SourceUserID	用于执行导出的用户 ID。
DeviceExternalID	已执行导出操作的服务 ID。
ExternalID	活动列表 ID。

Name	活动列表名称。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称
DeviceCustomString6Label	tenant name

上下文表已导出

上下文表的审计事件仅为用户执行的操作创建。

审计事件“上下文表已导出”的字段值

事件字段名称	字段值
DeviceAction	context table exported
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于执行导出的用户登录名。
SourceUserID	用于执行导出的用户 ID。
DeviceExternalID	已执行导出操作的服务 ID。
ExternalID	上下文表ID
Name	上下文表的名称。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

上下文表导入成功或操作失败

上下文表的审计事件仅为用户执行的操作创建。

上下文表项目通过远程连接分部分导入。

由于导入是通过远程连接执行的，因此数据传输错误可能在数据部分导入或全部导入时随时发生。EventOutcome 返回连接状态，而不是导入状态。

审计事件“上下文表导入成功或操作失败”的字段值

事件字段名称	字段值
DeviceAction	context table imported
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。

SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于执行导入的用户登录名。
SourceUserID	用于执行导入的用户 ID。
DeviceExternalID	已执行导入操作的服务 ID。
ExternalID	上下文表ID
Name	上下文表的名称。
Message	如果 EventOutcome = `failed`，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	租户名称。
DeviceCustomString6Label	`tenant name`

上下文表项修改成功或操作失败

上下文表的审计事件仅为用户执行的操作创建。

该事件可被分配 `succeeded` 或 `failed` 状态。

审计事件“上下文表项修改成功或操作失败”的字段值

事件字段名称	字段值
DeviceAction	`context table item is set`
EventOutcome	`succeeded` 或 `failed`
SourceTranslatedAddress	此字段包含 HTTP 标头 `x-real-ip` 或 `x-forwarded-for` 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	更改上下文表项的用户的帐户名。
SourceUserID	更改上下文表项的用户ID。
DeviceExternalID	修改了上下文表的服务ID。
ExternalID	上下文表ID
Name	上下文表的名称。
DeviceCustomString1	记录密钥的名称。
DeviceCustomString1Label	`key`
Message	如果 EventOutcome = `failed`，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	租户名称。
DeviceCustomString6Label	`tenant name`

上下文表项删除成功或操作失败

上下文表的审计事件仅为用户执行的操作创建。

该事件可被分配 `succeeded` 或 `failed` 状态。

审计事件“上下文表项已修改或操作失败”的字段值

事件字段名称	字段值
DeviceAction	`context table item deleted`
EventOutcome	`succeeded` 或 `failed`
SourceTranslatedAddress	此字段包含 HTTP 标头 `x-real-ip` 或 `x-forwarded-for` 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	删除上下文表项的用户的帐户名。
SourceUserID	删除上下文表项的用户ID。
DeviceExternalID	上下文表项被删除的服务ID。
ExternalID	上下文表ID
Name	上下文表的名称。
DeviceCustomString1	记录密钥的名称。
DeviceCustomString1Label	`key`
Message	如果 EventOutcome = `failed`，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	租户名称。
DeviceCustomString6Label	`tenant name`

上下文表清除成功或操作失败

上下文表的审计事件仅为用户执行的操作创建。

该事件可被分配 `succeeded` 或 `failed` 状态。

由于清除上下文表的请求是通过远程连接提出的，因此数据传输错误随时都可能发生：删除前和删除后。

这意味着上下文表可能会成功清除，但事件仍会获得 `failed` 状态，因为 EventOutcome 返回的是请求的 TCP/IP 连接状态，而不是上下文表清除的成功或失败状态。

审计事件“上下文表清除成功或操作失败”的字段值

事件字段名称	字段值
DeviceAction	`context table cleared`
EventOutcome	`succeeded` 或 `failed`
SourceTranslatedAddress	此字段包含 HTTP 标头 `x-real-ip` 或 `x-forwarded-for` 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	清除上下文表的用户的帐户名。
SourceUserID	清除上下文表的用户ID。
DeviceExternalID	上下文表被清空的服务ID。
ExternalID	上下文表ID

Name	上下文表的名称。
Message	如果 EventOutcome = failed，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	租户 ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

资源已添加

事件字段名称	字段值
DeviceAction	resource added
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于添加资源的用户登录名。
SourceUserID	用于添加资源的用户 ID。
DeviceExternalID	资源 ID。
DeviceProcessName	资源名称。
DeviceFacility	资源类型： • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

资源已删除

事件字段名称	字段值
DeviceAction	resource deleted
EventOutcome	succeeded

SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于删除资源的用户登录名。
SourceUserID	用于删除资源的用户 ID。
DeviceExternalID	资源 ID。
DeviceProcessName	资源名称。
DeviceFacility	资源类型： • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

资源已更新

事件字段名称	字段值
DeviceAction	resource updated
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于更新资源的用户登录名。
SourceUserID	用于更新资源的用户 ID。
DeviceExternalID	资源 ID。
DeviceProcessName	资源名称。

DeviceFacility	资源类型： • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

导入资源

事件字段名称	字段值
DeviceAction	import resources
EventOutcome	succeeded
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	导入资源的用户的帐户名。
SourceUserID	导入资源的用户ID。
DeviceCustomString5	导入资源的租户ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	导入资源的租户名。
DeviceCustomString6Label	tenant name
FileType	导入源： file 或 repository 。
FileID	如果资源是从存储库导入的，则为软件包ID。 如果资源是从文件导入的，则为该文件的系统ID。
ExternalID	如果资源是从存储库导入的，则需要指定导入软件包的版本。 如果资源是从文件中导入的，则值为空。

设置已更新

事件字段名称	字段值
DeviceAction	settings updated
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。

SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	用于更新设置的用户登录名。
SourceUserID	用于更新设置的用户 ID。
DeviceFacility	设置类型。
DeviceCustomString1	数据库中记录的阈值的JSON。
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

字典已成功在服务上更新或操作失败

事件字段名称	字段值
DeviceAction	dictionary update succeeded
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	用于创建服务的用户登录名。
SourceUserID	用于创建服务的用户 ID。
DeviceExternalID	服务 ID。
ExternalID	字典 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString1	字典类型：表格、字典。
DeviceCustomString1Label	dictionary type
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name
Message	如果 EventOutcome = failed，可以在此处找到错误消息。

字典条目已添加

通过API添加或更新的字典项目。

审计事件"字典条目已添加"的字段值

事件字段名称	字段值
DeviceAction	dictionary item added

EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	添加该项目的用户的帐户名称。
SourceUserID	添加项目的用户ID。
DeviceExternalID	服务 ID。
ExternalID	字典 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString1	字典类型：表格、字典。
DeviceCustomString1Label	dictionary type
DeviceCustomString2	记录密钥。
DeviceCustomString2Label	key
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

字典条目删除成功或操作失败

通过API删除字典项目（类型：表格、字典）。

该事件可被分配 succeeded 或 failed 状态。

审计事件"字典条目删除成功或操作失败"的字段值

事件字段名称	字段值
DeviceAction	dictionary item deleted
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	删除字典项目的用户的帐户名。
SourceUserID	删除字典项目的用户ID。
DeviceExternalID	字典项目被删除的服务ID。
ExternalID	字典 ID。
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceCustomString1	字典类型：表格、字典。
DeviceCustomString1Label	dictionary type
DeviceCustomString2	记录密钥。
DeviceCustomString2Label	key

Message	如果 EventOutcome = failed，可以在此处找到错误消息。
DeviceCustomString5	服务租户 ID。某些错误会阻止将租户信息添加到事件中。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

扩展事件模式字段已创建

事件字段名称	字段值
DeviceAction	extended field created
EventOutcome	succeeded
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	创建扩展事件架构字段的用户的帐户名。
SourceUserID	创建扩展事件模式字段的用户ID。
DeviceCustomString5	字段的全称（SA.sting_array）。

扩展事件模式字段已编辑

事件字段名称	字段值
DeviceAction	extended field edited
EventOutcome	succeeded
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	编辑扩展事件模式字段的用户的帐户名。
SourceUserID	编辑扩展事件模式字段的用户ID。
DeviceCustomString5	字段的全称（SA.sting_array）。

扩展事件模式字段已导入

事件字段名称	字段值
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	导入扩展事件模式字段的用户的帐户名。
SourceUserID	导入扩展事件模式字段的用户ID。
DeviceCustomString5	字段的全称（SA.sting_array）。

带有扩展事件模式字段的规范化器已导入

事件字段名称	字段值
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	导入带有扩展事件架构字段的规范化器的用户帐户名。
SourceUserID	导入带有扩展事件架构字段的规范化器的用户ID。
DeviceCustomString5	字段的全称（SA.sting_array）。

扩展事件模式字段已删除

事件字段名称	字段值
DeviceAction	extended field deleted
EventOutcome	succeeded
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	删除扩展事件模式字段的用户的帐户名。
SourceUserID	删除扩展事件模式字段的用户ID。
DeviceCustomString5	字段的全称（SA.sting_array）。

发送至 KIRA 的请求

事件字段名称	字段值
DeviceAction	KIRA task
EventOutcome	succeeded/failed
SourceUserName	用于发送请求的用户登录信息。
SourceUserID	用于发送请求的用户 IDS。
DeviceCustomString1	发送的结果字符串。
DeviceCustomString1Label	cmd
DeviceCustomString2	发送请求的事件ID。
DeviceCustomString2Label	event
DeviceCustomString3	为发送请求建立的任务ID。
DeviceCustomString3Label	task

KICS/KATA响应

事件字段名称	字段值
DeviceAction	KICS response
DeviceAssetID	asset fqdn
DeviceFacility	manual response 或 automatic response
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	发送请求的用户的登录名。
SourceUserID	发送请求的用户的 ID。
DeviceCustomString3	响应规则名称： Authorized， Not Authorized。
DeviceCustomString3Label	response rule name
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name
DeviceExternalID	资产 ID。
SourceHostName	资产 FQDN。
Name	资产名称。
DeviceCustomString1	资产的 IP 地址列表。
DeviceCustomString1Label	addresses
消息	如果EventOutcome = failed，则会将错误消息写入此字段。
DeviceCustomString2	fdqn
DeviceCustomString2Label	fqdns

Kaspersky Automated Security Awareness Platform 响应

事件字段名称	字段值
DeviceAction	KASAP response
DeviceFacility	manual response
EventOutcome	succeeded 或 failed
Message	如果发生错误，则描述错误，否则该字段为空。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	发送请求的用户的登录名。

SourceUserID	发送请求的用户的 ID。
DeviceCustomString1	被分配课程用户的经理。
DeviceCustomString1Label	manager
DeviceCustomString3	有关用户所属组的信息。不适用于 failed。
DeviceCustomString3Label	manager
DeviceCustomString4	有关用户所加入组的信息。
DeviceCustomString4Label	new kasap group
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name
DestinationUserID	触发响应的 Active Directory 用户账户的 ID。
DestinationUserName	账户名 (sAMAccountName)。
DestinationNtDomain	触发响应的 Active Directory 用户账户的域。

KEDR response

事件字段名称	字段值
DeviceAction	KEDR response
DeviceFacility	manual response 或 automatic response
EventOutcome	succeeded 或 failed
Message	如果发生错误，则描述错误，否则该字段为空。
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	发送请求的用户的登录名。
SourceUserID	发送请求的用户的 ID。
SourceAssetID	触发响应的 KUMA 资产 ID。如果响应基于哈希或针对所有资产，则不指定该值。
DeviceExternalID	在 KEDR 中分配给 KUMA 的外部 ID。如果只有一个外部 ID，则在用户主机上启动时不会填写。
DeviceCustomString1	基于事件卡片中选定哈希的主机防护规则所对应资产的 IP/FQDN 地址列表。
DeviceCustomString1Label	user defined list of ips or hostnames
DeviceCustomString2	KEDR 中的传感器 ID 参数 (UUIDv4 | 'all' | 'custom')。
DeviceCustomString2Label	sensor id of asset in KATA/EDR
ServiceID	触发响应的服务 ID。仅在自动响应的情况下填写。
DeviceCustomString3	任务类型名称：enable_network_isolation、disable_network_isolation、enable_prevention、disable_prevention、run_process。
DeviceCustomString3Label	kedr response kind
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

导入MITRE ATT&CK技术和策略

事件字段名称	字段值
DeviceAction	import MITRE
EventOutcome	succeeded
FileID	要导入的文件名。
SourceUserID	发送导入请求的用户ID。
SourceUserName	发送请求的用户的帐户名称。

指标警报已注册服务或操作失败

事件字段名称	字段值
DeviceProcessName	服务名称。
DeviceFacility	服务类型。
DeviceExternalID	服务 ID。
DeviceCustomString6Label	tenant name
DeviceCustomString6	租户名称。
DeviceCustomString5Label	tenant ID
DeviceCustomString5	租户 ID。
DeviceCustomString2Label	可能值： • QPS threshold reached • Failed Insert QPS threshold reached • High distribution queue • Low disk space • Low disk partition space • Output Event Loss increasing • Disk buffer size increasing • Enrichment errors increasing • High enrichment queue • Connector log errors increasing
DeviceCustomString2	created（服务创建时间）
DeviceCustomString1Label	API port.
DeviceCustomNumber1	工作持续时间（秒）。
DeviceAction	service alert
EventOutcome	succeeded 或 failed

Active Directory 中的响应

事件字段名称	字段值
DeviceAction	ad response
DeviceFacility	manual response 或 automatic response

EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理登录，则会有一个代理地址。
SourcePort	用户登录时使用的端口。如果用户使用代理登录，则会有一个代理端的端口。
SourceUserName	执行响应的用户的帐户名。
SourceUserID	执行响应的用户的 ID。
DeviceCustomString3	响应规则名称：CHANGE_PASSWORD、ADD_TO_GROUP、REMOVE_FROM_GROUP、BLOCK_USER。
DeviceCustomString3Label	response rule name
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name
DestinationUserName	调用响应的 Active Directory 用户账户 (sAMAccountName)。
DestinationNtDomain	调用响应的 Active Directory 用户账户的域。
DestinationUserID	KUMA 中的账户 UUID。
FlexString1	有关添加或删除用户的组的信息。
FlexString1Label	group DN

备份分区、从备份中还原、从外部安装的KUMA导入分区

事件字段名称	字段值
DeviceAction	backup/restore/import
EventOutcome	succeeded 或 failed
SourceUserName	执行分区备份、从备份还原以及从外部 KUMA 实例导入分区的用户的用户名。
SourceUserID	执行分区备份、从备份还原以及从外部 KUMA 实例导入分区的用户 ID。
DeviceExternalID	存储服务的 ID。
Name	存储名称。
FilePath	备份文件保存的完整路径。 要从备份中恢复或导入分区的完整路径。
Message	如果为 EventOutcome = failed，可在此处找到错误消息。

使用KIRA将自然语言查询转换为SQL查询。

事件字段名称	字段值
DeviceAction	KIRA request
EventOutcome	succeeded/failed
SourceUserName	用于发送请求的用户登录信息。
SourceUserID	用于发送请求的用户 IDS。

DeviceCustomString1	发送的结果字符串。
DeviceCustomString1Label	sql text

事件读取尝试

事件字段名称	字段值
DeviceAction	event search
Name	读取日志。
EventOutcome	succeeded 或 failed
SourceUserName	发起搜索查询的用户的账户名称。
SourceUserID	进行搜索查询的用户ID。
DeviceCustomString3	用户在**事件**部分选择的存储空间列表。
DeviceCustomString3Label	space name
DeviceCustomString4	搜索查询文本。
DeviceCustomString4Label	text of the search query

搜索请求已取消。

“消息”字段可能缺失。

事件字段名称	字段值
DeviceAction	canceling a search query
Message	取消请求的原因。
Name	搜索请求已取消。
DeviceCustomString5	服务租户ID（某些错误可能导致租户信息缺失）。
DeviceCustomString3Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name
DeviceExternalID	存储ID。
EventOutcome	succeeded 或 failed
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	发起搜索查询的用户的账户名称。
SourceUserID	进行搜索查询的用户ID。

KEDR资源已更新

事件字段名称	字段值
DeviceAction	resource updated
EventOutcome	succeeded 或 failed
DeviceExternalID	资源 ID。
DeviceProcessName	资源名称。
DeviceFacility	资源类型。
DeviceCustomNumber2	资源版本（编号）。
DeviceCustomNumber2Label	EDR resource version
DeviceCustomString4	KUMA版本。
DeviceCustomString4Label	KUMA version
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenantID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

KEDR资源更新任务已完成

事件字段名称	字段值
DeviceAction	Apply EDR resources task
Message	过时的EDR资源已更新。包含已更新EDR资源的服务已重新加载。
EventOutcome	succeeded 或 failed
DeviceCustomNumber1	资源收集器名称。
DeviceCustomNumber1Label	reloaded collectors
DeviceCustomNumber3	资源关联器名称。
DeviceCustomNumber3Label	reloaded correlators
DeviceCustomString4	KUMA版本。
DeviceCustomString4Label	KUMA version
DeviceCustomString5	资源名称。
DeviceCustomString5Label	imported resources

KEDR事件字段已更新

事件字段名称	字段值
DeviceAction	Apply EDR resources task
Message	新的EDR扩展字段已应用。

EventOutcome	succeeded 或 failed
DeviceCustomNumber1	扩展事件字段的版本。
DeviceCustomNumber1Label	New EDR fields version
DeviceCustomString4	KUMA版本。
DeviceCustomString4Label	KUMA version

文件localizations.json已导入

事件字段名称	字段值
DeviceAction	Import IOA rules localizations
EventOutcome	succeeded 或 failed
DeviceCustomDate1	dd.mm.yyy hh:mm:ss
DeviceCustomDate1Label	Last update IoA rules localizations file content

规则已关联到收集器

事件字段名称	字段值
DeviceAction	link rule to collector
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改数据的用户名称。
SourceUserID	修改数据的用户ID。
ExternalID	规则所关联的服务ID。
Name	规则所关联的服务名称。
DeviceFacility	操作（规则已关联）。
DeviceCustomString1	规则的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	规则名称。
DeviceCustomString2Label	rule name
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

规则已取消与收集器的关联

事件字段名称	字段值
DeviceAction	unlink rule from collector
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改数据的用户名称。
SourceUserID	修改数据的用户ID。
ExternalID	与该规则取消关联的服务 ID。
Name	与该规则取消关联的服务名称。
DeviceFacility	操作（规则已取消关联）。
DeviceCustomString1	规则的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	规则名称。
DeviceCustomString2Label	rule name
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

规则已关联到关联器

事件字段名称	字段值
DeviceAction	link rule to correlator
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改数据的用户名称。
SourceUserID	修改数据的用户ID。
ExternalID	规则所关联的服务ID。
Name	规则所关联的服务名称。
DeviceFacility	操作（规则已关联）。
DeviceCustomString1	规则的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	规则名称。

DeviceCustomString2Label	rule name
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

规则已与关联器解除关联

事件字段名称	字段值
DeviceAction	unlink rule from correlator
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	修改数据的用户名称。
SourceUserID	修改数据的用户ID。
ExternalID	与该规则取消关联的服务 ID。
Name	与该规则取消关联的服务名称。
DeviceFacility	操作（规则已取消关联）。
DeviceCustomString1	规则的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	规则名称。
DeviceCustomString2Label	rule name
DeviceCustomString5	租户 ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租户名称。
DeviceCustomString6Label	tenant name

从 KUMA 导出的资源

每个导出的资源都会生成一个单独的审计事件。

事件字段名称	字段值
DeviceAction	export resources
EventOutcome	succeeded
SourceTranslatedAddress	此字段包含 HTTP 标头 x-real-ip 或 x-forwarded-for 的值。如果这些标头不存在，则该字段为空。
SourceAddress	用户登录时的地址。如果用户使用代理服务器登录，则指定代理服务器的地址。
SourcePort	用户登录时使用的端口。如果用户使用代理服务器登录，则指定代理服务器的端口。
SourceUserName	导出资源的用户的用户名。

SourceUserID	导出资源的用户 ID。
DeviceCustomString5	资源导出来源的租户ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	导出的资源ID。
DeviceCustomString6Label	resource ID
DeviceCustomString4	导出的资源版本。
DeviceCustomString4Label	version

从隔离网段接收有关事件的服务数据

有关事件的服务信息通过“internal”协议传输到收集器。要从隔离网段传输此类数据，可以使用安装在该网段内的专用代理。

要通过“internal”协议将数据从代理传输到收集器，代理和收集器必须使用证书相互进行身份验证。可以在代理的配置文件中创建并保存代理证书，然后使用该文件在隔离网段中安装代理。证书信息以加密形式保存在文件中。

要配置从隔离网段接收有关事件的服务数据：

1. 使用“internal”连接器创建或配置收集器。
2. 创建代理并配置向收集器传输数据：
   a. 在 KUMA Web 界面中，在“**资源和服务**”→“**代理程序**”下，单击“**创建**”。
   b. 在打开的“**创建代理程序**”窗口中，在“**基础设置**”选项卡上，指定“**名称**”和“**租户**”设置。
   c. 在“**配置资源 #{{index}}**”上的“**连接器**”区域中，指定以下设置：
      - 在“**名称**”字段中，指定连接器的名称。
      - 在“**类型**”字段中，指定连接器类型。
      - 在“**URL**”字段中，指定将安装用于接收事件的代理的主机。
   d. 在“**配置资源 #{{index}}**”上的“**目标位置**”区域中，指定以下设置：
      - 在“**名称**”字段中，指定目标的名称。
      - 在“**类型**”字段中，输入将用于发送事件的“**internal**”协议。
      - 在“**URL**”字段中，指定安装了带有“**internal**”连接器的收集器的主机。
   e. 单击“**创建**”。
   f. 从列表中选择已创建的代理资源集，然后在代理属性窗口中单击“**下载包含证书的配置**”。在显示的窗口中，指定用于加密证书的密码；启动代理时也会要求输入该密码。

      代理设置配置根据浏览器的设置，以 JSON 文件形式下载。在隔离网段中安装代理时需要使用此文件。

> 您必须使用访问控制列表 (ACL) 来配置在待安装代理的服务器上访问文件的权限。运行代理的用户账户必须具有文件读取访问权限。

g. 在隔离网段中安装代理。它可以安装到 Linux 和 Windows 设备上。

已配置接收来自隔离网段的事件服务数据。

关联规则

点击链接可下载相关文件，其中介绍了分发包中包含的关联规则。它提供了规则涵盖的场景、使用条件以及必要的事件源。

> 文档中描述的关联规则包含在 OSMP 分发包中的 SOC_package 文件中；该文件的密码是 SOC_package1。一次只能使用一个版本的 SOC 规则集：俄语或英语。

> 您可以将导入的关联规则添加到组织使用的关联器中。有关详细信息，请参阅以下主题："步骤 3：关联"。

要将关联规则包导入 KUMA：

1. 在OSMP控制台的KUMA部分，转到**设置 → 存储库更新**，然后将**更新来源**参数设置为**卡巴斯基更新服务器**。您还可以配置存储库更新。
2. 单击"**运行更新**"以保存更新设置并手动启动"*存储库更新*"任务。
3. 转到"**任务管理器**"以确保"*存储库更新*"任务已完成。
4. 转到"**资源**"，然后单击"**导入资源**"。
5. 在"**资源导入**"窗口中，选择要分配已导入资源的租户。
6. 在"**导入源**"下拉列表中，选择"**存储库**"，选择"SOC 内容包"，然后单击"**导入**"。

SOC 内容包中的资源将导入到 KUMA。有关导入的更多信息，请参阅"导入资源"。

下载 SOC_package.xlsx 文件中包含的关联规则描述。

时间格式

KUMA 支持以如下格式对传递给事件数据模型中时间戳类型字段（EndTime、StartTime、DeviceCustomDate1 等）的信息进行处理：

- "May 8, 2009 5:57:51 PM"、
- "oct 7, 1970"、
- "oct 7, '70"、

- “oct. 7, 1970”、
- “oct. 7, 70”、
- “Mon Jan 2 15:04:05 2006”、
- “Mon Jan 2 15:04:05 MST 2006”、
- “Mon Jan 02 15:04:05 -0700 2006”、
- “Monday, 02-Jan-06 15:04:05 MST”、
- “Mon, 02 Jan 2006 15:04:05 MST”、
- “Tue, 11 Jul 2017 16:28:13 +0200 (CEST)”、
- “Mon, 02 Jan 2006 15:04:05 -0700”、
- “Mon 30 Sep 2018 09:09:09 PM UTC”、
- “Mon Aug 10 15:44:11 UTC+0100 2015”、
- “Thu, 4 Jan 2018 17:53:36 +0000”、
- “Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)”、
- “Sun, 3 Jan 2021 00:12:23 +0800 (GMT+08:00)”、
- “2012年九月17日上午10:09”、
- “2012年九月17日上午10:09 PST-08”、
- “September 17, 2012, 10:10:09”、
- “October 7, 1970”、
- “October 7th, 1970”、
- “12 Feb 2006, 19:17”、
- “12 Feb 2006 19:17”、
- “14 May 2019 19:11:40.164”、
- “7 oct 70”、
- “7 oct 1970”、
- “03 February 2013”、
- “1 July 2013”、
- “2013-Feb-03”。

dd/Mon/yyyy 格式

- “06/01/2008:15:04:05 -0700”、
- “06/01/2008 15:04:05 -0700”。

mm/dd/yyyy 格式

- “3/31/2014”、
- “03/31/2014”、
- “08/21/71”、
- “8/1/71”、
- “4/8/2014 22:05”、
- “04/08/2014 22:05”、
- “4/8/14 22:05”、
- “04/2/2014 03:00:51”、
- “8/8/1965 12:00:00 AM”、
- “8/8/1965 01:00:01 PM”、
- “8/8/1965 01:00 PM”、
- “8/8/1965 1:00 PM”、
- “8/8/1965 12:00 AM”、
- “4/02/2014 03:00:51”、
- “03/19/2012 10:11:59”、
- “03/19/2012 10:11:59.3186369”。

yyyy/mm/dd 格式

- “2014/3/31”、
- “2014/03/31”、
- “2014/4/8 22:05”、

- “2014/04/08 22:05”、
- “2014/04/2 03:00:51”、
- “2014/4/02 03:00:51”、
- “2012/03/19 10:11:59”、
- “2012/03/19 10:11:59.3186369”。

yyyy:mm:dd 格式

- “2014:3:31”、
- “2014:03:31”、
- “2014:4:8 22:05”、
- “2014:04:08 22:05”、
- “2014:04:2 03:00:51”、
- “2014:4:02 03:00:51”、
- “2012:03:19 10:11:59”、
- “2012:03:19 10:11:59.3186369”。

包含中文字符的格式

“2014年04月08日”

yyyy-mm-ddThh 格式

- “2006-01-02T15:04:05+0000”、
- “2009-08-12T22:15:09-07:00”、
- “2009-08-12T22:15:09”、
- “2009-08-12T22:15:09.988”、
- “2009-08-12T22:15:09Z”、

- “2017-07-19T03:21:51:897+0100”、
- “2019-05-29T08:41-04”（不显示秒数，时区为 2 位字符）。

yyyy-mm-dd hh:mm:ss 格式

- “2014-04-26 17:24:37.3186369”、
- “2012-08-03 18:31:59.257000000”、
- “2014-04-26 17:24:37.123”、
- “2013-04-01 22:43”、
- “2013-04-01 22:43:22”、
- “2014-12-16 06:20:00 UTC”、
- “2014-12-16 06:20:00 GMT”、
- “2014-04-26 05:24:37 PM”、
- “2014-04-26 13:13:43 +0800”、
- “2014-04-26 13:13:43 +0800 +08”、
- “2014-04-26 13:13:44 +09:00”、
- “2012-08-03 18:31:59.257000000 +0000 UTC”、
- “2015-09-30 18:48:56.35272715 +0000 UTC”、
- “2015-02-18 00:12:00 +0000 GMT”、
- “2015-02-18 00:12:00 +0000 UTC”、
- “2015-02-08 03:02:00 +0300 MSK m=+0.000000001”、
- “2015-02-08 03:02:00.001 +0300 MSK m=+0.000000001”、
- “2017-07-19 03:21:51+00:00”、
- “2014-04-26”、
- “2014-04”、
- “2014”、
- “2014-05-11 08:20:13,787”。

yyyy-mm-dd-07:00 格式

“2020-07-20+08:00”

mm.dd.yyyy 格式

- “3.31.2014”、
- “03.31.2014”、
- “08.21.71”。

yyyy.mm.dd 格式

“2014.03.30”

yyyymmdd 格式及类似格式

- “20140601”、
- “20140722105203”。

yymmdd hh:mm:yy 格式

“171113 14:14:20”

Unix 时间戳格式

- “1332151919”、
- “1384216367189”、
- “13842163671111222”、
- “138421636711122233 3”。

映射预定义规范化器的字段

可通过下载链接获取的文件包含预设容器的字段映射的描述。

下载预设规范化器的字段映射描述。

词汇表

Bootstrap

基本执行环境，包括 Kubernetes 集群和用于运行 Kaspersky Next XDR Expert 的基础设施组件。Bootstrap 包含在传输存档文件中，并在部署 Kaspersky Next XDR Expert 期间自动安装。

EPP 应用程序

安装在端点设备上的应用程序提供防护，并向管理服务器报告其防护状态以进行集中管理。在Kaspersky Next XDR Expert中，EPP应用程序是Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux和Kaspersky Endpoint Security for Mac。

IOA规则

Kaspersky Next XDR Expert使用攻击指标（IOA）。IOA规则包含对系统中可疑活动的描述，这可能是有针对性攻击的迹象。这些规则从KUMA存储库下载，并由TAA（目标攻击分析器）技术用于威胁搜寻。您可以从相应的警报详情中打开IOA规则详情。此外，OSMP控制台中还预定义了一条IOA规则。预定义规则显示在关联规则表中：**监控→资源和服务→关联规则**。如果触发了预定义的IOA规则，则会创建IOA警报。

IOC 文件

IOC 文件包含一组与事件指标进行比较的指标。如果比较的指标匹配，应用程序将该事件视为检测并创建警报。如果扫描检测到对象数据与多个 IOC 文件之间的精确匹配，则警报的可能性会增加。

Kubernetes 集群

通过 Kubernetes 组合为一个计算资源的一组主机。Kubernetes 集群用于运行 Kaspersky Next XDR Expert 组件（KUMA 服务除外）的功能。Kubernetes 集群可以同时包含目标主机和管理员主机。

KUMA 服务

KUMA 的主要组件，可帮助系统管理事件。服务允许您从事件源接收事件，然后将它们转换为通用格式，以便于查找关联、存储和人工分析。KUMA 服务是安装在 Kubernetes 集群之外的主机上的代理、收集器、关联器、存储和事件路由器。

KUMA 清查文件

一个 YAML 格式的文件，其中包含 Kubernetes 集群中未包含的 KUMA 服务的安装参数。KUMA 清查文件的路径包含在 KDT 用于部署 Kaspersky Next XDR Expert 的配置文件中。

Observables

与警报和事故相关的对象，例如 MD5 和 SHA256 哈希、IP 地址、URL、域名、用户名或主机名。

上下文

一组访问参数，用于定义用户可以选择与之交互的 Kubernetes 集群。上下文还包括使用 KDT 连接到集群的数据。

事件

在组织 IT 基础设施的受监控元素上注册的信息安全事件。例如，事件包括登录尝试、与数据库的交互以及传感器信息广播。每个单独的事件可能看似无关紧要，但综合来看，它们会构成一个更全面的网络活动图景，从而帮助识别安全威胁。

事件路由器

一种 KUMA 服务，用于从收集器和关联器接收事件流，然后根据配置的过滤器将事件分发到指定的目的位置。

事故

警报容器，通常指示组织 IT 基础设施中存在真实的问题。一个事故可能包含一个或多个警报。通过使用事故，分析师可以将多个警报作为单个问题进行调查。

代理

KUMA 服务，用于接收远程设备上的事件并将其转发到 KUMA 收集器。

传输存档文件

存档文件，包含 Kaspersky Next XDR Expert 组件、管理 Web 插件以及 Kaspersky Next XDR Expert 和 KDT 的最终用户授权许可协议。传输存档文件包含在分发包中。

关联器

KUMA 服务，用于分析规范化事件。

关联规则

KUMA 资源用于识别已处理事件的定义序列并在识别后执行特定操作。

分发包

包含 Kaspersky Next XDR Expert 组件以及 Kaspersky Next XDR Expert 和 KDT 最终用户授权许可协议的传输存档文件，以及包含 KDT 实用程序、配置文件与 KUMA 清查文件模板的存档文件。

分段规则

允许您根据指定条件自动将相关警报拆分为不同事故的规则。

卡巴斯基部署工具包

一款实用程序，用于部署和管理 Kubernetes 集群、Kaspersky Next XDR Expert 组件和管理 Web 插件。KDT 在管理员主机上运行，并通过 SSH 连接到目标主机。

取证信息

一套旨在识别、获取和分析数据的方法和技术，这些数据可以作为网络攻击或设备上实施的其他非法活动的数字证据。

响应操作

在行动手册内启动的操作。

多租户

一种模式，允许主管理员为多个客户端独立提供 Kaspersky Next XDR Expert 功能，或为不同分支机构提供资产、应用程序设置和对象的隔离管理服务。此外，多租户模式还可用于从父租户复制和继承租户设置和对象，并自动将 Kaspersky Next XDR Expert 的授权许可密钥应用于层次结构中的所有租户。

威胁发展链

一系列追踪网络攻击各个阶段的步骤。威胁发展链有助于分析威胁的原因。为了创建威胁发展链，受管理应用程序会通过网络代理将数据从设备传输到管理服务器。

存储

KUMA 服务，用于存储规范化事件，以便可以从 KUMA 快速且持续地访问这些事件，从而提取分析数据。

收集器

KUMA 服务从事件源接收消息、进行处理，然后将其传输到存储、关联器和/或第三方服务以识别警报。

注册表

存储应用程序容器的基础设施组件，用于安装和存储 Kaspersky Next XDR Expert 组件。

目标主机

用于部署 Kaspersky Next XDR Expert 的物理机或虚拟机。目标主机包含在 Kubernetes 集群中。Kaspersky Next XDR Expert 组件在这些主机上运行。

租户

一个逻辑实体，对应获得 Kaspersky Next XDR Expert 功能的组织单元（如客户端或分支机构）。每个租户均可以包括资产、用户及其访问权限、事件、警报、事故、行动手册以及与其他卡巴斯基应用程序、服务和第三方解决方案的集成。租户还会界定对所含对象可执行的一组操作。

管理员设备

一个物理机或虚拟机，用于通过 KDT 来部署和管理 Kubernetes 集群和 Kaspersky Next XDR Expert。KDT 在管理员主机上运行。如果管理员主机未包含在 Kubernetes 集群中，则它将仅用于部署。如果管理员主机包含在集群中，它还将充当用于运行 Kaspersky Next XDR Expert 组件的目标主机。

网络代理

Open Single Management Platform 的一个组件，它能够实现管理服务器和特定网络节点（工作站或服务器）上安装的卡巴斯基应用程序之间的交互。该组件是公司内所有 Microsoft® Windows® 应用程序的通用组件。对于为 Unix 和 macOS 之类的平台开发的 Kaspersky 产品，分别有不同版本的网络代理。

网络位置识别 (NLA)

帮助操作系统识别当前网络的 Windows 服务。NLA 可检测网络变化并调整设备的安全配置。

自定义操作

KDT命令可让您执行针对特定Kaspersky Next XDR Expert组件的其他操作。

节点

部署了 Kaspersky Next XDR Expert 的物理机或虚拟机。有主节点和工作节点。主节点用于管理集群、存储元数据和分配工作负载。工作节点用于执行 Kaspersky Next XDR Expert 组件的工作负载。

行动手册

根据指定算法（行动手册算法）响应警报或事故的对象。行动手册可用于工作流自动化并减少处理警报和事故所需的时间。

行动手册算法

一种算法，包含一系列响应操作，有助于分析和处理警报或事故。

规范化事件

根据 KUMA 规范化事件数据模型处理的事件。

警报

组织 IT 基础设施中被 Open Single Management Platform 标记为异常或可疑的事件，可能对组织 IT 基础设施的安全构成威胁。

调查图

一种可视化分析工具，显示事件、警报、事故、可观察对象和资产（设备）之间的关系。此外，调查图还显示事故的详细信息：相应的警报、用户、资产及其共同属性。

资产

基础设施中需要保护的设备或用户。如果在某个资产上检测到警报或事故，您可以针对该资产执行响应操作。

轻量级 Nagent（LWNGT）

用于与移动设备上的 Kaspersky Endpoint Security 进行交互的协议。LWNGT（又称移动协议）起到网络代理的作用，而无需在移动设备上实际安装网络代理。

配置文件

YAML 格式的文件，包含用于部署 Kaspersky Next XDR Expert 的目标主机列表和 Kaspersky Next XDR Expert 组件的一组安装参数。配置文件供 KDT 使用。

有关第三方代码的信息

有关第三方代码的信息包含在充当运算子节点的设备上的以下文件中：

- legal_notices_ksmp.txt；
- legal_notices_kuma.txt；
- legal_notices_kesl.txt；
- legal_notices_kesw.txt；
- legal_notices_spp.txt。

这些文件位于运行 Kaspersky Next XDR Expert 部署的用户的 `~/kaspersky_eula` 目录中。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

Adobe、Flash 和 PostScript 是 Adobe 在美国和/或其他国家/地区的注册商标或商标。

AMD 和 AMD64 是 Advanced Micro Devices, Inc. 的商标或注册商标。

Amazon、Amazon EC2、Amazon Web Services、AWS、和 AWS Marketplace 是 Amazon.com, Inc. 或其附属公司的商标。

Apache 和 Apache Cassandra 是 Apache Software Foundation 在美国和/或其他国家/地区的注册商标或商标。

Apple、App Store、AppleScript、Carbon、FileVault、iPhone、Mac、Mac OS、macOS、OS X、Safari 和 QuickTime 是 Apple Inc. 的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地方的注册商标。

蓝牙词语，标志和标识都为 Bluetooth SIG, Inc. 所有。

LTS 和 Ubuntu 是 Canonical Ltd. 的注册商标。

Check Point NGFW 是 Check Point Software Technologies Ltd. 或其附属公司的商标或注册商标。

Cisco、IOS 和 Snort 是 Cisco Systems, Inc. 和/或其关联公司在美国及某些其他国家/地区的注册商标或商标。

Citrix、XenServer 是 Cloud Software Group, Inc. 和/或其子公司在美国和/或其他国家/地区的注册商标或商标。

Citrix NetScaler 是 Cloud Software Group, Inc. 和/或其子公司在美国和/或其他国家/地区的注册商标或商标。

Cloudflare、Cloudflare 徽标和 Cloudflare Workers 是 Cloudflare, Inc. 在美国和其他司法管辖区的商标和/或注册商标。

Grafana Word Mark 和 Grafana Logo 是 Coding Instinct AB 在美国和其他国家/地区的注册商标/服务标志或商标/服务标志，并经 Coding Instinct 许可使用。我们与 Coding Instinct 或 Grafana 社区无任何关联，亦未获得其认可或赞助。

CorelDRAW 是 Corel Corporation 和/或其附属公司在加拿大、美国和其他国家/地区的商标或注册商标。

Dell Technologies 和其他商标是 Dell Inc. 或其子公司的商标。

Docker 和 Docker 徽标是 Docker, Inc. 在美国和/或其他国家/地区的商标或注册商标。Docker, Inc. 和其他方可能对本文中使用的其他术语拥有商标权。

Elasticsearch 是 Elasticsearch BV 在美国和其他国家/地区的商标。

ESET 是 ESET spol. s r.o. 或相应 ESET 实体的商标或注册商标。

F5 是 F5 Networks, Inc. 在美国和其他某些国家/地区的商标。

Firebird 是 Firebird Foundation 的注册商标。

Fortinet、FortiGate、FortiMail 和 FortiSOAR 是 Fortinet, Inc. 在美国和/或其他国家/地区的注册商标或商标。

FreeBSD 是 FreeBSD foundation 的注册商标。

Google、Android、Chrome、Dalvik、Firebase、Google Chrome、Google Maps、Google Play、Google Public DNS 是 Google LLC 的商标。

HUAWEI、EulerOS 和 Huawei Eudemon 是华为技术有限公司的商标。

ViPNet 是 Infotecs 的注册商标。

IBM、Guardium、InfoSphere、QRadar 是 International Business Machines Corporation 在全球众多司法管辖区的商标。

Intel 和 Insider 是 Intel Corporation 或其子公司的商标。

Node.js 是 Joyent, Inc. 的商标。

Juniper、Juniper Networks 和 JUNOS 是 Juniper Networks, Inc. 在美国和其他国家/地区的商标或注册商标。

Linux 是 Linus Torvalds 在美国和其他国家的注册商标。

Kubernetes 是 The Linux Foundation 在美国和其他国家/地区的注册商标。

Microsoft、Access、Active Directory、ActiveSync、ActiveX、Azure、BitLocker、Excel、Halo、Hyper-V、InfoPath、Internet Explorer、Lync、Microsoft 365、Microsoft Edge、MS-DOS、MultiPoint、Office 365、OneNote、Outlook、PowerPoint、PowerShell、Segoe、SharePoint、Skype、SQL Server、Tahoma、Visio、Win32、Windows、Windows Media、Windows Mobile、Windows Phone、Windows PowerShell、Windows Server 和 Windows Vista 是 Microsoft 集团公司的商标。

CVE 是 The MITRE Corporation 的注册商标。

Mozilla、Firefox 是 Mozilla Foundation 在美国和其他国家/地区的商标。

NetApp 是 NetApp, Inc. 在美国和其他国家/地区的商标或注册商标。

Netskope、Netskope 徽标以及本文提及的其他 Netskope 产品名称均为 Netskope, Inc. 和/或其子公司的商标，且可能已在美国专利商标局和其他国家/地区的专利商标局注册。

NetWare 是 Novell Inc. 在美国和其他国家/地区的注册商标。

Novell 是 Novell Enterprises Inc. 在美国和其他国家/地区的注册商标。

OpenSSL 是 OpenSSL 软件基金会拥有的商标。

Oracle、Java 和 JavaScript 是 Oracle 和/或其关联公司的注册商标。

OpenVPN 是 OpenVPN, Inc. 的注册商标。

Parallels、Parallels 徽标和 Coherence 是 Parallels International GmbH 的商标或注册商标。

PROOFPOINT 是 Proofpoint, Inc. 在美国和其他国家/地区的商标。

Chef 是 Progress Software Corporation 和/或其子公司或附属公司之一在美国和/或其他国家/地区的商标或注册商标。

Puppet 是 Puppet, Inc. 的商标或注册商标。

Python 是 Python Software Foundation 的商标或注册商标。

Ansible 是 Red Hat, Inc. 在美国和其他国家/地区的注册商标。

Red Hat、CentOS、Fedora 和 Red Hat Enterprise Linux 是 Red Hat Inc. 或其子公司在美国和其他国家/地区的商标或注册商标。

BlackBerry 是 Research In Motion Limited 所有的商标，已在美国注册，且可能在其他国家/地区处于申请中或已注册状态。

Samsung 是 SAMSUNG 在美国或其他国家/地区的商标。

Sendmail 以及其他名称和产品名称均为 Sendmail, Inc. 的商标或注册商标。

Debian 是 Public Interest, Inc. 公司的软件的注册商标。

SolarWinds 和 Dameware 商标归 SolarWinds Worldwide, LLC 或其附属公司专有，已在美国专利商标局注册，并且可能在其他国家/地区已注册或正在申请注册。

Splunk 是 Splunk Inc. 在美国和其他国家/地区的商标和注册商标。

CommuniGate Pro 名称是 Stalker Software, Inc. 的商标或注册商标。

SUSE 是 SUSE LLC 在美国和其他国家/地区的注册商标。

Symantec 是 Symantec Corporation 或其附属公司在美国和其他国家/地区的商标或注册商标。

Symbian 是 Symbian Foundation Ltd. 所拥有的商标。

OpenAPI 是 The Linux Foundation 的商标。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商标。

Trend Micro 是 Trend Micro Incorporated 的商标或注册商标。

用于标识 UserGate 产品和服务的名称、图像、徽标和图片是 UserGate 和/或其子公司或附属公司的专有标识，相关产品本身归 UserGate 所有。

VMware、VMware ESXi、VMware Horizon、VMware vCenter、VMware vSphere、VMware Workstation 和 Carbon Black 是 VMware, Inc. 在美国和其他国家/地区的注册商标和/或商标。

UNIX 是在美国和其他国家的注册商标，通过 X/Open Company Limited 授权。

ClickHouse. 是 YANDEX LLC 的商标。

Zabbix 是 Zabbix SIA 的注册商标。

The MITRE Corporation Terms of Use

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes.Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

"© 2025 The MITRE Corporation.This work is reproduced and distributed with the permission of The MITRE Corporation."

DISCLAIMERS

MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques.Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE MITRE CORPORATION, ITS BOARD OF TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.