kaspersky

Kaspersky Next XDR Expert

© 2026 AO Kaspersky Lab

目錄

Kaspersky Next XDR Expert
版本更新摘要
修正的錯誤
關於Kaspersky Next XDR Expert
  硬體及軟體需求
    Kaspersky Deployment Toolkit
    具有KUMA服務的主機需求
    OSMP主控台需求
    網路代理要求
    虛擬化組態
    常見需求與注意事項
  Kaspersky Next XDR Expert元件
  相容的卡巴斯基應用程式和解決方案
  基本概念
    管理伺服器
    管理伺服器階層
    網頁伺服器
    網路代理
    管理群組
    受管理裝置
    未配置的裝置
    管理員工作站
    管理 Web 外掛程式
    政策
    政策設定檔
    工作
    關聯器
    事件
    警示
    事件
    資源
    工作範圍
    本機應用程式設定與政策的關係
    發佈點
    連線閘道
    核心
    儲存庫
    收集器
    服務
    KUMA代理程式
    關於嚴重程度
Open Single Management Platform架構
  SIEM元件架構

OSMP主控台介面
變更OSMP主控台介面的語言
變更OSMP主控台首頁
新增和移除書籤
產品授權
關於《最終使用者產品授權協議》
關於產品授權金鑰
關於啟動碼
關於金鑰檔案
產品授權限制
Kaspersky Next XDR Expert產品授權功能
啟動Kaspersky Next XDR Expert
為SIEM元件新增產品授權金鑰
檢視使用中產品授權金鑰的相關資訊
撤銷最終使用者產品授權協議的許可
續約 Kaspersky 應用程式的產品授權
移除SIEM組件的產品授權金鑰
使用卡巴斯基市場選擇卡巴斯基商業解決方案
關於資料提供
關於資料提供
Kaspersky Unified Monitoring and Analysis Platform中的資料提供
沙盒中的資料提供
正在啟動
Kaspersky Next XDR Expert的部署和初始設定
驗證Kaspersky Next XDR Expert組態的正確性
使用威脅監控、偵測和搜尋功能
使用Kaspersky Next XDR Expert進行事件調查的範例
Kaspersky Next XDR Expert的部署
硬化指南
管理Kaspersky Next XDR Expert的基礎設施
連線安全
帳戶和身分驗證
管理Kaspersky Next XDR Expert的防護
管理用戶端裝置防護
事件傳輸到第三方系統
配置受管理應用程式的防護
部署方案
多節點部署結構
單節點部署方案
Kaspersky Next XDR Expert使用的連接埠
變更用於連線至 OSMP Console 伺服器的連接埠
變更 Endpoint Agent 用來連線至 agentserver 元件的連接埠
準備工作和部署
多節點佈署：準備管理員主機和目標主機
單節點部署：準備管理員主機和目標主機
準備主機以安裝KUMA服務
安裝資料庫管理系統

- 設定 PostgreSQL 或 Postgres Pro 伺服器以搭配 Kaspersky Next XDR Expert 使用
- 準備KUMA清查文件，以便在Kubernetes叢集外部安裝KUMA服務
- 多節點部署：指定安裝參數
- 單節點部署：指定安裝參數
- 透過代理節點連線 Endpoint Agent
- Kaspersky Next XDR Expert 部署精靈
- 安裝 Kaspersky Next XDR Expert
- 設定目標主機的網際網路存取
- 同步裝置時間
- 在Kubernetes叢集內安裝KUMA服務
- 在Kubernetes叢集外部安裝KUMA服務
- 部署多個Kubernetes叢集和Kaspersky Next XDR Expert實例
- 在實體隔離環境中安裝或升級 Kaspersky Next XDR Expert
- 部署前的基礎設施就緒狀況預檢
- Kaspersky Next XDR Expert元件的安裝前完整性檢查
- 將資料匯入 Kaspersky Next XDR Expert

與端點代理程式的整合

沙盒的準備與安裝程式

- 為沙盒安裝程式準備IT基礎設施
- 準備用於安裝沙盒的虛擬機器
- 準備安裝程式磁碟映像
- 安裝沙盒
  - 步驟 1。檢視最終使用者產品授權協議和隱私權政策
  - 步驟 2。選擇用於安裝沙盒的磁碟
  - 步驟 3。設定沙盒管理員密碼的最小密碼長度
  - 步驟 4。建立沙盒管理員帳戶
  - 步驟 5。設定管理網路介面
  - 步驟 6。指派主機名稱並新增DNS伺服器位址
  - 步驟 7。設定靜態網路路由

與沙盒整合

Kaspersky Next XDR Expert的高可用性部署

- Kaspersky Next XDR Expert的高可用性組態
- 恢復Kubernetes叢集中的故障節點

Kaspersky Next XDR Expert 的高可用性多站台部署

- 多站台部署：準備管理員主機和目標主機
- 多站台部署：指定安裝參數
- 在標準 Ubuntu Server 24.04 LTS 虛擬機器上進行跨資料中心多站台部署

Kaspersky Next XDR Expert的維護

- 更新Kaspersky Next XDR Expert元件
- 檢查Kaspersky Next XDR Expert元件的完整性
- 無需重新安裝即可變更Kaspersky Next XDR Expert的參數
- 新增和刪除Kubernetes叢集的主節點和工作線程節點
- 對組態檔進行版本管理。
- 解除安裝Kaspersky Next XDR Expert
- 手動取消安裝Kaspersky Next XDR Expert元件
- 安裝失敗後重新安裝Kaspersky Next XDR Expert
- 重新安裝Kaspersky Next XDR Expert元件

Kaspersky Next XDR Expert資料的備份複製和還原
設定Kaspersky Next XDR Expert備份副本的儲存
設定和管理備份排程
手動建立Kaspersky Next XDR Expert資料的備份副本
檢視Kaspersky Next XDR Expert資料的備份
從備份副本還原Kaspersky Next XDR Expert資料
停止Kubernetes叢集節點
使用Kaspersky Next XDR Expert公共服務的憑證
計算和變更用於儲存管理伺服器資料的磁碟空間
檢視和變更KUMA Core和指標服務的磁碟空間
檢視和更改物件儲存體容量
增加可觀測性儲存體容量
輪換Kubernetes叢集憑證
輪換登錄檔存取憑據
輪換DBMS憑據和憑證
新增主機以安裝附加的KUMA服務
取代使用KUMA儲存體的主機
使用部署在虛擬機器上的Kaspersky Next XDR Expert
Kaspersky Next XDR Expert部署的演示
準備管理員和目標主機
指定安裝參數
將 Kaspersky Next XDR Expert 從 2.2 版升級至 2.3 版
遷移到 Kaspersky Next XDR Expert
關於從卡巴斯基安全管理中心Windows遷移
從卡巴斯基安全管理中心 Windows 匯出群組物件
將匯出檔案匯入Kaspersky Next XDR Expert
將受管理裝置切換到Kaspersky Next XDR Expert的管理之下
關於從KEDR 7.1遷移
設定和使用SIEM元件
KUMA服務
服務工具
獲取服務識別碼
停止、啟動和檢查服務狀態
重新啟動服務。
刪除服務
檢視活動查詢表
分割區視窗
搜尋相關事件
服務資源集
建立儲存體
ClickHouse叢集結構
ClickHouse叢集節點設定
事件的冷存儲
移除冷儲存磁碟
中斷連接、封存及連接分割區
為儲存空間建立資源集
在OSMP中建立儲存服務

- 在OSMP網路基礎架構中安裝儲存體
- 備份、恢復和匯入分割區
  - 排定分割區備份
  - 手動備份分割區
  - 從外部 OSMP 實例匯入分割區
  - 從備份中還原分割區
- 建立關聯器
  - 啟動關聯器安裝精靈
    - 步驟1：一般關聯器設定
    - 步驟 2。全域變數
    - 步驟3。關聯
    - 步驟4。擴充
    - 步驟 5。回應
    - 步驟 6：路由
    - 步驟 7。設定驗證
  - 在 OSMP 網路基礎設施中安裝關聯器
  - 驗證關聯器安裝
  - 建立 correlator-ng 關聯器
    - 建立關聯器correlator-ng
    - correlator-ng 支援的資料類型
    - 關聯規則選擇器和運算式
    - 標準關聯規則的屬性
    - correlator-ng中的資料函式
- 建立事件路由器
  - 啟動事件路由器安裝精靈
    - 步驟 1。事件路由器的一般設定
    - 步驟 2：路由
    - 步驟 3。設定驗證
  - 在伺服器上安裝事件路由器
- 建立收集器
  - 啟動收集器安裝精靈
    - 步驟 1。連線事件來源
    - 步驟 2。傳輸
    - 步驟 3。事件解析
    - 步驟 4。事件篩選
    - 步驟 5。事件彙總
    - 步驟 6。事件擴充
    - 步驟 7：路由
    - 步驟 8。設定驗證
  - 在KUMA網路基礎架構中安裝收集器
  - 驗證收集器安裝
  - 確保收集器運作不間斷
    - 使用rsyslog控制事件流
    - 使用nginx控制事件流
  - 預定義收集器

- 建立代理程式
  - 為代理程式建立資源集
  - 在OSMP中建立代理程式服務
  - 在OSMP網路基礎架構中安裝代理程式
    - 在Linux資產上安裝KUMA代理程式
    - 在 Windows 資產上安裝 KUMA 代理程式
  - 自動建立的代理程式
  - 更新代理程式
  - 將事件從隔離網段傳輸到KUMA
    - 二極體代理程式組態檔
    - 密鑰欄位說明
    - 在隔離網段中安裝Linux代理程式
    - 在隔離網段中安裝Windows代理程式
  - 將事件從 Windows 裝置傳輸到 OSMP
  - 設定代理以接收來自隔離網路區段的 Netflow 事件
- AI服務
  - 使用KIRA分析警示和事件
    - 使用LLM提供者設定與KIRA的整合
    - 使用KIRA進行分析
    - 「使用KIRA進行分析」工作可能發生的錯誤
  - 使用KIRA以自然語言建立搜尋查詢
    - 使用KIRA建立自然語言搜尋查詢並將其轉換為SQL查詢
    - 使用自然語言建構查詢時可能出現的錯誤
  - 設定偵測DLL劫持
  - AI資產分數和狀態。
    - 安裝AI資產分數和狀態服務
    - 重新簽發AI服務憑證
    - AI資產分數和狀態服務的設定
- 設定事件來源
  - 設定接收Auditd事件
    - 安裝KUMA收集器以接收Auditd事件
    - 設定事件來源伺服器
  - 設定接收KATA/EDR事件
    - 設定將KATA/EDR事件匯出至KUMA
    - 建立KUMA收集器以接收KATA/EDR事件
    - 安裝KUMA收集器以接收KATA/EDR事件
  - 配置Open Single Management Platform以將事件匯出至KUMA SIEM系統
    - 設定KUMA收集器以收集Open Single Management Platform事件
    - 安裝KUMA收集器以收集Open Single Management Platform事件
  - 設定從MS SQL接收Open Single Management Platform事件
    - 在MS SQL資料庫中建立帳戶
    - 配置SQL Server瀏覽器服務
    - 在KUMA中建立密鑰
    - 設定連接器
    - 配置KUMA收集器以從MS SQL資料庫接收卡巴斯基安全管理中心事件
    - 安裝KUMA收集器以從MS SQL資料庫接收卡巴斯基安全管理中心事件

設定使用KUMA代理程式 (WEC) 從Windows裝置接收事件
設定稽核來自Windows裝置的事件
在Windows裝置上設定稽核政策
使用群組政策設定稽核
使用Windows事件收集器服務設定集中接收來自Windows裝置的事件
設定從事件來源伺服器傳輸資料
設定Windows事件收集器服務
授予檢視Windows事件的權限
授予作為服務登入的權限
設定KUMA收集器以接收來自Windows裝置的事件
安裝KUMA收集器以從Windows裝置接收事件
設定使用KUMA代理程式（WEC）將事件從Windows裝置轉送至KUMA
設定使用KUMA代理程式 (WMI)從Windows裝置接收事件。
設定用於管理KUMA的審核設定
使用本機政策設定稽核
使用群組政策設定稽核
設定從事件來源伺服器傳輸資料
授予檢視Windows事件的權限
授予作為服務登入的權限
設定接收PostgreSQL事件
安裝pgAudit外掛程式
設定Syslog伺服器以傳送事件
設定接收IVK Kolchuga-K事件
設定將IVK Kolchuga-K事件匯出至KUMA
設定接收CryptoPro NGate事件
設定將CryptoPro NGate事件匯出到KUMA
設定接收Ideco UTM事件
設定將Ideco UTM事件匯出到KUMA
設定接收KWTS事件
設定將KWTS事件匯出到KUMA
設定接收KLMS事件
設定將KLMS事件匯出到KUMA
設定接收KSMG事件
設定將KSMG事件匯出至KUMA
設定接收PT NAD事件
設定將PT NAD事件匯出到KUMA
設定使用MariaDB稽核外掛程式接收事件
設定MariaDB稽核外掛程式以傳送MySQL事件
設定MariaDB稽核外掛程式以傳送MariaDB事件
設定Syslog伺服器以傳送事件
設定接收Apache Cassandra事件
在KUMA中設定Apache Cassandra事件日誌記錄
設定接收FreeIPA事件
設定將FreeIPA事件匯出至KUMA
設定接收VipNet TIAS事件
設定將ViPNet TIAS事件匯出至KUMA

- 設定接收Nextcloud事件
  - 設定Nextcloud事件稽核
  - 設定Syslog伺服器以傳送Nextcloud事件
- 設定接收Snort事件
  - 設定Snort事件的日誌記錄
- 設定接收Suricata事件
  - 設定Suricata事件日誌記錄。
- 設定接收FreeRADIUS事件
  - 設定FreeRADIUS事件稽核
  - 設定Syslog伺服器以傳送FreeRADIUS事件
- 設定接收VMware vCenter事件
  - 設定與VMware vCenter的連線
- 設定接收zVirt事件
  - 設定zVirt事件的匯出
- 設定接收Zeek IDS事件
  - Zeek IDS事件日誌格式的轉換
- 使用ETW連接器設定接收DNS伺服器事件
  - Windows端的設定
- 使用Kaspersky Endpoint Security for Windows設定接收Windows事件
- Codemaster Mirada
  - 設定接收Codemaster Mirada事件
- 設定接收Postfix事件
  - 設定Postfix以傳送事件
  - 設定KUMA收集器以接收和處理Postfix事件
- 設定接收CommuniGate Pro事件
  - 設定CommuniGate Pro以傳送事件
  - 設定KUMA收集器以接收和處理CommuniGate Pro事件
- 設定接收Yandex Cloud事件
  - 設定稽核Yandex Cloud事件
  - 設定匯出Yandex Cloud事件
- 設定接收Microsoft 365事件
- 設定接收Kontinent加密系統事件
  - 準備接收Kontinent事件
  - 設定kuma-kont公用程式
  - 啟動和管理kuma-kont服務
  - kuma-kont-config.yaml組態檔中的設定

與其他解決方案整合

- 與卡巴斯基安全管理中心整合
  - 設定卡巴斯基安全管理中心資產的資料重新整理間隔
  - 排程匯入卡巴斯基安全管理中心資產
  - 手動匯入卡巴斯基安全管理中心資產
  - 檢視卡巴斯基安全管理中心伺服器的層次結構
  - 匯入卡巴斯基安全管理中心資料庫事件
- Kaspersky Endpoint Detection and Response整合
  - 使用kafka連接器匯入Kaspersky Endpoint Detection and Response事件
  - 使用kata/edr連接器匯入Kaspersky Endpoint Detection and Response事件
  - 設定在KUMA警示中顯示Kaspersky Endpoint Detection and Response偵測的連結

與Kaspersky CyberTrace整合
整合CyberTrace指標搜尋
設定CyberTrace接收和處理請求
建立事件擴充規則
整合CyberTrace介面
透過LDAP連線
啟用和停用LDAP整合
將租用戶新增至LDAP伺服器整合清單
建立LDAP伺服器連線
建立LDAP伺服器連線的副本
變更LDAP伺服器連線
變更資料更新頻率
變更資料儲存週期
啟動帳號資料更新工作
刪除LDAP伺服器連線
Kaspersky Industrial CyberSecurity for Networks整合
在KICS for Networks中設定整合
在KUMA中設定整合
啟用和停用與KICS for Networks的整合
變更資料更新頻率
匯入KICS for Networks資產資訊時的特殊注意事項
變更KICS for Networks資產的狀態
與Neurodat SIEM IM整合
Kaspersky Automated Security Awareness Platform
在KASAP中建立權杖並取得API請求的連結
在KUMA中設定整合
檢視KASAP使用者資訊並變更學習群組
向Telegram傳送通知
建立和設定Telegram機器人
建立傳送通知的指令碼
在KUMA中設定通知
UserGate整合
在UserGate中設定整合
準備與UserGate整合的指令碼
設定與UserGate整合的回應規則
與Kaspersky Web Traffic Security整合
在KWTS中設定整合
準備用於與KWTS整合的指令碼
設定用於與KWTS整合的回應規則
與Kaspersky Secure Mail Gateway整合
在KSMG中設定整合
準備用於與KSMG整合的指令碼
從RedCheck匯入資產資訊
設定接收Sendmail事件
設定Sendmail日誌記錄
設定匯出Sendmail事件
設定與外部SIEM系統的集成

- 管理KUMA
  - 設定KUMA Core
  - 代理
  - 連線到SMTP伺服器
  - 處理卡巴斯基安全管理中心工作
    - 在卡巴斯基安全管理中心中建立KUMA工作
    - 手動啟動卡巴斯基安全管理中心工作
    - 自動啟動卡巴斯基安全管理中心工作
    - 檢查卡巴斯基安全管理中心工作的狀態
  - KUMA日誌
  - KUMA通知
  - 編輯KUMA使用者設定檔
  - 管理租用戶
- 管理憑證
  - 下載憑證
  - 修改自我簽署的 Web 介面憑證
  - 重新簽發內部 CA 憑證
  - 重新簽發特定服務的憑證
- 使用地理資料
  - 地理資料格式
  - 將地理資料從MaxMind轉換為IP2Location
  - 匯入和匯出地理資料
  - 地理資料的預設對應
- 使用知識庫
  - 檢視套件詳細資料
  - 檢視資源詳細資料
  - 安裝和更新套件與資源
- KUMA資源
  - 資源操作
    - 建立、重新命名、移動和刪除資源資料夾
    - 建立、複製、移動、編輯和刪除資源
    - 將資源關聯到服務
    - 更新資源
      - 使用Kaspersky Update Utility設定自訂來源
    - 匯出資源
    - 匯入資源
    - 標籤管理
  - 標準化器
    - 事件解析設定
    - 擴充事件結構描述
      - 新增擴充事件結構欄位
      - 編輯擴充事件結構欄位
      - 匯入和匯出擴充事件結構欄位
      - 刪除擴充事件結構欄位
      - 在規範化器中使用擴充事件結構欄位
    - 使用 KIRA 產生正規表示式
    - 標準化器中的擴充功能

- 將資料傳送到額外標準化器的條件
- 支援的事件來源
- 連接器
  - 檢視連接器設定
  - 新增連接器
  - 連接器設定
    - Tcp類型
    - Udp類型
    - Netflow類型
    - Sflow類型
    - Nats-jetstream 類型
    - 連接器，Kafka類型
    - kata/edr類型
    - 連接器，http類型
    - SQL類型
    - 檔案類型
    - 1c-xml類型
    - 1c-log類型
    - 二極體類型
    - Ftp類型
    - Sftp類型
    - smb類型
    - Nfs類型
    - vmware類型
    - Wmi類型
    - Wec類型
    - SNMP 類型
    - SNMP 陷阱類型
      - 設定Windows的SNMP陷阱訊息來源
        - 設定和啟動SNMP和SNMP陷阱服務
        - 設定事件到陷阱轉換器服務
    - elastic類型
    - etw類型
    - universalAPI類型
    - promtail類型
    - http-streaming 類型
    - 預定義連接器
- 目標
  - 目標，內部類型
  - Nats-jetstream 類型
  - Tcp類型
  - Udp類型
  - Http類型
  - 二極體類型
  - Kafka類型
  - 檔案類型
  - 儲存體類型：

- 關聯器類型
- 目標，事件路由器類型
- 預定義目標

篩選器

活動清單

- 檢視活動清單表
- 新增活動清單
- 檢視活動清單的設定
- 變更活動清單的設定
- 複製活動清單的設定
- 刪除活動清單
- 檢視活動清單中的記錄
- 搜尋活動清單中的記錄
- 將記錄新增至活動清單
- 複製活動清單中的記錄
- 變更活動清單中的記錄
- 刪除活動清單中的記錄
- 將資料匯入活動清單
- 匯出活動清單資料
- 預定義活動清單

字典

密鑰

快顯表單

- 檢視快顯表單清單
- 新增快顯表單
- 檢視快顯表單設定
- 編輯快顯表單設定
- 複製快顯表單設定
- 刪除快顯表單
- 檢視快顯表單記錄
- 搜尋快顯表單記錄
- 新增快顯表單
- 編輯快顯表單記錄
- 刪除快顯表單記錄
- 將資料匯入快顯表單
- 從快顯表單匯出資料

關聯規則

- 標準關聯規則
- 簡單關聯規則
- 操作關聯規則
- 關聯器中的變數
  - 相同和唯一欄位中的局部變數
  - 選擇器中的局部變數
  - 事件擴充中的局部變數
  - 活動清單擴充中的局部變數
  - 變數的內容
  - 變數的需求

變數的函式
宣告變數
預定義關聯規則
為關聯規則新增暫時排除清單
Sigma 規則轉換器
準備 Sigma 規則
支援的 Sigma 規則轉換範例
MITRE ATT&CK框架涵蓋範圍
彙總規則
擴充規則
回應規則
卡巴斯基安全管理中心的回應規則
自訂指令碼的回應規則
KICS for Networks的回應規則
Kaspersky Endpoint Detection and Response的回應規則
Active Directory的回應規則
資料收集和分析規則
虛擬管理伺服器
建構OSMP實例的層次結構
將子實例連線到父實例
在 OSMP 實例階層中指派從屬管理伺服器
將子實例與父實例斷開連線
層級結構中關聯規則的分發
將全域關聯器組態與全域關聯規則一起分發
分發全域關聯規則供本機使用
複製繼承的關聯規則供本機使用
查看在 OSMP 子實例中建立的資源和服務
在階層中分發資源時的資料夾行為
將 OSMP 實例組合成階層
憑證輪替後修復實例層次結構
與其他解決方案整合
Kaspersky Automated Security Awareness Platform
Создание токена в KASAP и получение URL для API-запросов
與Kaspersky Threat Intelligence Portal整合
設定與KATA/KEDR的整合
設定Kaspersky Next XDR Expert與指令碼啟動服務的整合
威脅偵測
搭配警示一起使用
關於警示
警示資料模型
檢視警示表
檢視警示詳情
將警示指派給分析師
變更警示狀態
手動建立警示
將警示連結到事件中
取消警示與事件的連結

- 將事件連結到警示中
- 取消事件與警示的連結
- 在調查圖表上使用警示
- 將IOA規則新增至排除清單
- 管理聚合規則
  - 建立彙總規則
  - 編輯彙總規則
  - 將彙總規則複製到另一個租用戶
  - 刪除彙總規則

處理事件

- 關於事件
- 事件資料模型
- 建立事件
- 建立子事件
- 檢視事件表
- 檢視事件詳細資料
- 將事件指派給分析師
- 變更事件狀態
- 變更事件優先順序
- 合併事件
- 匯出事件到檔案
- 從XDR事件建立「受管理偵測和回應」事件
- 調查圖表
  - 進程樹狀圖
    - 建構進程樹狀圖
    - 刪除進程樹狀圖
    - 在進程樹狀圖上備注
- 區隔規則
- 將分段規則複製到另一個租用戶
- 管理服務等級協定（SLA）
  - 建立服務等級協議（SLA）事項
  - 刪除服務等級協定（SLA）事項
- 管理事件類型
  - 檢視事件類型表
  - 建立事件類型
  - 編輯事件類型
  - 刪除事件類型
- 管理事件工作流程
  - 檢視事件工作流程表
  - 預先定義的事件工作流程
  - 建立事件工作流程
  - 編輯事件工作流程與狀態
  - 刪除事件工作流程
- 管理事件工作量
  - 新增事件工作量
  - 編輯事件工作量

- 刪除事件工作量
- 產生和匯出事件報告
- 設定警示和事件的保存週期
- 設定警示和事件的自動指派
- 檢視資產詳細資訊
- 透過遠端終端進行調查和回應
  - 管理遠端終端連線
  - 透過遠端終端執行回應操作
- 威脅搜尋
- 處理事件
  - 事件資料模型
    - Process
    - Registry Create
    - File Create
    - File Modify
    - File Rename
    - File Read
    - File Delete
    - File Attributes Modify
    - File Creation Time Modify
    - File Hardlink Created
    - File Symlink Created
    - Module
    - Registry Create
    - Registry Delete
    - Registry Modify
    - Registry Rename
    - Registry Query
    - Registry Save
    - Connection
    - Port Listen
    - AMSI Scan
    - Process Console Input
    - Driver
    - Process Interpreted File Run
    - DNS
    - Pipe Create
    - Pipe Connect
    - LDAP
    - WMI Activity
    - WMI Consumer Register
    - Code Injection
    - Process Access
    - Threat Detect
    - Threat Detect Processing Result
    - Linux Event Log
    - Windows Event Log

Blocked Document
Applock
Process Terminated
Device
File System Mount
File System Unmount
Bits Job Create
Bits Job Complete
Bits Job Start
Bits Job Stop
Bits Job Add File
Bits Job Error
Service Create
Service Modify
Service Delete
Scheduled Task Create
Scheduled Task Modify
Scheduled Task Delete
File Owner Change
File ACL Change
Registry Owner Change
Registry ACL Change
Executable Memory Mapped
Agent Start
Agent Stop
Agent Install
Agent Uninstall
Agent Action
System Startup
System Shutdown
Connection Close
事件的細粒度存取
檢視事件表
搜尋和篩選事件
手動建立SQL查詢
使用建構器產生SQL查詢
使用 KUMA SQL 函數產生 SQL 查詢
在 SQL 查詢中使用「enrich」函數集
在 SQL 查詢中使用「lookup」函數集
檢視事件詳情
儲存和選取事件篩選器組態
依期間篩選事件
匯出事件
查看稽核事件和設定通知
稽核事件
回溯掃瞄
獲取事件表統計資訊

威脅回應
回應操作
終止進程
將裝置移動至管理群組
更新資料庫
變更裝置的授權狀態
將檔案移至隔離區
從隔離區還原檔案
從隔離區取得檔案
從隔離區刪除檔案
檢視KASAP使用者的資訊並變更學習群組
啟用和停用網路隔離
執行「新增阻止規則」和「刪除阻止規則」回應操作
執行程式
管理服務
透過Kaspersky NGFW阻止IP位址
取得文件以進行進一步分析
取得檔案
取得登錄檔金鑰
取得NTFS元檔案
取得鑑識資訊
若要取得磁碟映像
取得記憶體轉儲
取得進程記憶體轉儲
掃描裝置來偵測威脅
執行惡意軟體掃描
YARA 掃描
IOC 掃描
掃描從裝置取得的文件
刪除檔案
透過Active Directory進行回應
使用協力廠商程式碼進行回應
透過UserGate進行回應
透過Ideco NGFW進行回應
透過Ideco UTM進行回應
透過Redmine進行回應
透過Check Point NGFW進行回應
透過Sophos防火牆進行回應
透過Continent 4進行回應
透過SKDPU NT進行回應
透過FortiGate進行回應
透過Palo Alto NGFW回應
透過 Jira 進行回應
從警示或事件詳細資訊中檢視回應歷史記錄
檢視惡意軟體掃描結果
處理回應操作取得的檔案

使用阻止規則表
建立阻止規則。
匯入阻止規則
使用IOC規則表
使用YARA規則表
常規程式
檢視常規程式表
建立常規程式
在視覺化編輯器中設定常規程式執行步驟
編輯常規程式
自訂常規程式
檢視常規程式內容
終止常規程式
刪除常規程式
管理常規程式版本
比較常規程式版本
還原常規程式版本
以測試模式啟動常規程式
啟動常規程式和回應操作
手動啟動常規程式
為使用者指定的物件啟動常規程式
以訓練操作模式啟動常規程式
設定回應操作的手動核准
核准常規程式或回應操作
從常規程式擴充
檢視回應歷史記錄
預定義常規程式
[KL] P001「辦公室應用程式建立可執行檔」
[KL] P002「Windows事件日誌已清除」
[KL] P003「來自wmiprvse.exe的可疑子程序」
[KL] P004「沙盒中等偵測」
[KL] P005「沙盒高等偵測」
[KL]「檢查外部IP位址的常規程式」
[KL]「檢測到受感染文件時隔離裝置的常規程式」
[KL][EDR]「從警示中刪除已傳輸至主機的惡意檔案」
[KL][EDR] "刪除從事件傳輸至主機的惡意檔案"
[KL][EDR]「從警報中偵測到探索活動時隔離主機」
[KL][EDR]「從事件中偵測到探索活動時隔離主機」
[KL][EDR]「偵測到資料外洩活動時隔離主機」
[KL][EDR] 從警示偵測到反向 Shell 活動時隔離主機
[KL][EDR]「在事件中偵測到反向 Shell 活動時隔離主機」
[KL][EDR]「從警示緩解電子郵件附件的惡意活動」
[KL][EDR]「緩解事件中電子郵件附件的惡意活動」
[KL][EDR]「從警示緩解記憶體傾印活動」
[KL][EDR]「緩解事件中的記憶體傾印活動」
常規程式觸發器

- 常規程式演算法
  - 常規程式參數
  - 執行步驟參數
    - 迴圈
    - 並行
    - 決定
    - UpdateData
  - 回應函式參數
- 使用常規程式編輯事件
- 使用常規程式編輯警示

管理沙盒

- 初始社會設定
  - 為沙盒設定資料庫更新
  - 沙盒網路介面
    - 配置DNS設定
    - 設定管理網路介面
    - 設定已處理物件的網際網路存取
    - 新增靜態網路路由
  - 變更沙盒管理員帳戶密碼
  - 沙盒身分驗證政策
    - 終止不活躍的沙盒會話
    - 關於沙盒身分驗證嘗試失敗的通知
  - 設定將偵測到的物件傳送到KPSN拒絕清單
- 準備虛擬機器
  - 將映像上傳到儲存體
  - 匯入範本
  - 建立自訂虛擬機器範本
  - 設定作業系統和軟體
  - 建立虛擬機器
  - 安裝虛擬機器
  - 下載偵錯符號

設定OSMP以使用偵測技術

- 更新沙盒和反惡意軟體引擎的防病毒資料庫
- 建立受密碼保護的封存檔案的密碼清單
- 選擇用於掃描沙盒中物件的作業系統
- 建立自訂沙盒規則
- 設定將檔案從端點代理程式傳送到沙盒
- 關於入侵指標、IOC檔案和IOC規則
- 匯入IOC規則
- 匯入YARA規則

Kaspersky Next XDR Expert API

- 建立權杖
- 授權API請求

使用Open Single Management Platform

- 設定管理伺服器
  - 配置管理伺服器連線位址
  - 設定 OSMP 主控台與管理伺服器的連線

- 設定網際網路存取設定
- Open Single Management Platform工作憑證
  - 關於Open Single Management Platform憑證
  - Open Single Management Platform中使用的自訂憑證的要求
  - 為OSMP主控台重新簽發憑證
  - 取代OSMP主控台的憑證
  - 將 PFX 憑證轉換為 PEM 格式
  - 情境：指定自訂管理伺服器憑證
  - 使用 klsetsrvcert 公用程式替換管理伺服器憑證
  - 使用 klmover 公用程式將網路代理連線到管理伺服器
- 管理伺服器階層
- 建立管理伺服器階層：新增次要管理伺服器
- 檢視從屬管理伺服器清單
- 管理虛擬管理伺服器
  - 建立虛擬管理伺服器
  - 啓用和停用虛擬管理伺服器
  - 為虛擬管理伺服器指派管理員
  - 變更用戶端裝置的管理伺服器
  - 刪除虛擬管理伺服器
- 配置管理伺服器連線事件記錄
- 設定事件儲存區中的最大事件數量
- 變更 DBMS 憑證
- 管理伺服器資料的備份與還原
  - 配置管理伺服器備份工作
  - 使用KDT公用程式恢復管理伺服器資料
- 刪除管理伺服器階層
- 存取公用 DNS 伺服器
- 設定介面
- 使用 TLS 的加密通信

發現網路裝置

- 情境：發現網路裝置
- Windows 網路輪詢
- IP 範圍輪詢
- 網域控制器輪詢
- 配置 Samba 網域控制器
- 在用戶端裝置上使用 VDI 動態模式
  - 在網路代理安裝套件的內容中啟用 VDI 動態模式
  - 將啟用 VDI 的裝置移至管理群組

管理用戶端裝置

- 受管理裝置設定
- 檢查用戶端裝置與管理伺服器之間的連線。klnagchk 公用程式
- 建立管理群組
- 裝置移動規則
  - 建立裝置移動規則
  - 複製裝置移動規則
  - 裝置移動規則的條件
- 將裝置手動新增至管理群組

將裝置或者叢集手動移動至管理群組
關於叢集和伺服器陣列
叢集或伺服器陣列的屬性
發佈點和連線閘道的調整
發佈點的標準配置：單一辦公室
發佈點的標準配置：多個小遠端辦公室
計算發佈點的數量和配置
自動分配發佈點
手動分配發佈點
修改管理群組的發佈點清單
啟用推送伺服器
關於裝置狀態
設定裝置狀態轉換
裝置分類
從裝置分類中檢視裝置清單
建立裝置分類
配置裝置分類
從裝置分類中匯出裝置清單
在分類中從管理群組中刪除裝置
裝置標籤
裝置標籤
建立裝置標籤
重命名裝置標籤
刪除裝置標籤
檢視分配了標籤的裝置
檢視分配到裝置的標籤
手動標記裝置
從裝置上刪除分配的標籤
檢視自動標記裝置規則
編輯自動標記裝置規則
建立自動標記裝置規則
為自動標記裝置執行規則
刪除自動標記裝置規則
資料加密與防護
檢視加密磁碟機的清單
檢視加密事件清單
建立和檢視加密報告
以離線模式授予加密磁碟機的存取權限
在管理伺服器之間傳輸加密金鑰
變更用戶端裝置的管理伺服器
當裝置顯示不活動時檢視和配置操作
遠端存取受管理裝置
從安裝有OSMP主控台的Linux裝置遠端存取受管理的Linux裝置
從安裝有OSMP主控台的Linux裝置遠端存取受管理的Windows裝置
從安裝有OSMP主控台的Windows裝置遠端存取受管理的Linux裝置
從安裝有OSMP主控台的Windows裝置遠端存取受管理的Windows裝置

管理資產
新增資產類別
設定資產表
搜尋資產
匯出資產資料
檢視資產詳細資訊
新增資產
在OSMP中新增資產資訊
從卡巴斯基安全管理中心匯入資產資訊
從MaxPatrol匯入資產資訊
從MaxPatrol VM匯入資產資訊
kuma–ptvm–config.yaml 組態檔的設定
從KICS for Networks匯入資產資訊
匯入過程中資產欄位比較的範例
kuma-ptvm-config.yaml組態檔的設定
為資產指派類別
編輯資產參數
歸檔資產
移除資產
刪除資產類別
批次刪除資產
更新協力廠商應用程式並修復卡巴斯基安全管理中心資產上的弱點
將資產移至選定管理群組
資產稽核
設定資產稽核
儲存和搜尋資產稽核事件
啟用和停用資產稽核
自訂資產欄位
緊急資訊基礎架構資產
佈署 Kaspersky 應用程式
情境：卡巴斯基應用程式部署
防護佈署精靈
步驟 1。開始防護佈署精靈
步驟 2。選取安裝套件
步驟 3。選取金鑰檔案或啟動碼的發佈方式
步驟 4。選取網路代理版本
步驟 5。選取裝置
步驟 6。指定遠端安裝工作設定
步驟 7。重新啟動管理
步驟 8。安裝前移除不相容的應用程式
步驟 9。移動裝置到受管理裝置
步驟 10。選取存取裝置的帳戶
步驟 11。啟動安裝
新增卡巴斯基應用程式的管理外掛程式
移除管理Web外掛程式
檢視整合在Open Single Management Platform中的元件清單
檢視卡巴斯基Next XDR Expert元件的名稱、參數和自訂操作

- 下載和建立 Kaspersky 應用程式的安裝套件
- 從檔案建立安裝套件
- 建立獨立安裝套件
- 變更自訂安裝套件資料大小限制
- 準備 Linux 裝置以安裝網路代理
- 準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理
- 準備好用於遠端安裝的 Windows 裝置
- 準備在封閉軟體環境模式下執行 Astra Linux 的裝置以安裝網路代理
- 以靜默模式安裝適用於 Linux 的網路代理（搭配回應檔案）
- 檢視獨立安裝套件清單
- 分發安裝套件至從屬管理伺服器
- 同時部署 Kaspersky Next XDR Expert 與 Kaspersky Endpoint Security for Linux
- 使用遠端軟體安裝工作安裝應用程式
  - 遠端安裝應用程式
  - 在從屬管理伺服器上安裝應用程式
- 指定在 Unix 裝置上進行遠端安裝的設定
- 啟動和停止卡巴斯基應用程式
- 取代協力廠商安全應用程式
- 遠端移除應用程式或軟體更新

配置卡巴斯基應用程式

- 情境：配置網路防護
- 關於以裝置為中心和以使用者為中心的安全管理方法
- 政策設定和傳播：以裝置為中心的方法
- 政策設定和傳播：以使用者為中心的方法
- 關於將網路代理切換到其他管理伺服器
- 為漫遊使用者建立連線設定檔
- 政策和政策設定檔
  - 關於政策和政策設定檔
  - 關於鎖定和已鎖定的設定
  - 政策繼承和政策設定檔
    - 政策層次結構
    - 政策層次結構中的政策設定檔
    - 如何在受管理裝置上實作設定
  - 管理政策
    - 檢視政策清單
    - 建立新政策
    - 一般政策設定
    - 修改政策
    - 啟用和停用政策繼承選項
    - 複製政策
    - 移動政策
    - 匯出政策
    - 匯入政策
    - 強制同步
    - 檢視政策發佈狀態圖表
    - 在出現病毒爆發事件時自動啟用政策
    - 刪除政策

- 管理政策設定檔
  - 檢視政策設定檔
  - 變更政策設定檔優先順序
  - 建立政策設定檔
  - 複製政策設定檔
  - 建立政策設定檔啟動規則
  - 刪除政策設定檔
  - 匯出和匯入政策設定檔
- 網路代理政策設定
- Windows、Linux 和 macOS 網路代理的使用：比較
- 按作業系統比較網路代理設定
- 配置受管理應用程式的防護設定
- Kaspersky Endpoint Security 更新群組工作的手動設定
- 卡巴斯基安全網路和卡巴斯基私人安全網路
  - 關於 KSN
  - 設定對 KSN 的存取
  - 啟用和停用 KSN 的使用
  - 設定與KPSN本機信譽資料庫的連線
  - 檢視接受的 KSN 聲明
  - 接受更新的 KSN 聲明
  - 檢查發佈點是否作為 KSN 代理伺服器運作
  - 檢視 KSN 代理伺服器統計
- 管理端點防護工作
  - 關於工作
  - 關於工作範圍
  - 建立工作
  - 手動啟動工作
  - 為選取的裝置啟動工作
  - 檢視工作清單
  - 一般工作設定
  - 匯出工作
  - 匯入工作
  - 啟動變更工作密碼精靈
    - 步驟 1。指定憑證
    - 步驟 2。選取要採取的動作
    - 步驟 3。檢視結果
  - 檢視儲存在管理伺服器中的工作執行結果
  - Kaspersky Endpoint Security 裝置掃描群組工作的手動設定
- 管理偵測和回應工作
  - 檢視工作表
  - 檢視工作執行結果
  - 重新啟動工作
- 應用程式標籤
  - 建立應用程式標籤
  - 重命名應用程式標籤
  - 分配標籤到應用程式

- 從應用程式上刪除分配的標籤
- 刪除應用程式標籤
- 在OSMP主控台中註冊卡巴斯基Industrial CyberSecurity for Networks應用程式

管理使用者和使用者角色

- 關於使用者帳戶
- 關於用於角色
- 設定應用程式功能的存取權限。角色型存取控制
  - 應用程式功能的存取權
  - 預先定義的使用者角色
  - 為特定物件分配存取權限
  - 分配權限到使用者和群組
- 新增內部使用者帳戶
- 建立安全群組
- 編輯內部使用者帳戶
- 變更使用者工作狀態
- 編輯安全群組
- 為使用者或安全群組分配角色
- 新增使用者帳戶到內部安全群組
- 指派使用者作為裝置所有者
- 設定雙步驟驗證
  - 關於帳戶的雙因素驗證
  - 在OSMP主控台登入時設定雙因素驗證密鑰
  - 允許使用者配置雙因素驗證
  - 重置和刪除雙因素驗證秘密金鑰
  - 從雙因素驗證中排除帳戶
  - 編輯安全碼簽發者的名稱
- 允許的密碼輸入嘗試次數
- 設定使用者 SSO 工作階段和身分驗證權杖的存留期
- 刪除使用者或安全群組
- 變更使用者帳戶密碼
- 在登入頁面新增自訂消息區塊
- 建立使用者角色
- 編輯使用者角色
- 編輯使用者角色範圍
- 刪除使用者角色
- 關聯政策設定檔到角色
- 設定 Kerberos 網域身分驗證

更新 Kaspersky 資料庫和應用程式

- 情境：定期更新 Kaspersky 資料庫與應用程式
- 關於更新 Kaspersky 資料庫、軟體模組和應用程式
- 建立「將更新下載至管理伺服器儲存區」工作
- 瀏覽已下載的更新
- 驗證已下載的更新
- 建立「將更新下載至發佈點儲存區」工作
- 為將更新下載到管理伺服器儲存區工作新增更新來源
- 批准和拒絕軟體更新
- 自動安裝 Kaspersky Endpoint Security for Windows 的更新

關於使用 diff 檔案更新 Kaspersky 資料庫和軟體模組
啟用下載 diff 檔案功能
透過發佈點下載更新
在離線裝置上更新 Kaspersky 資料庫和軟體模組
用戶端裝置的遠端診斷
開啟遠端診斷視窗
啟用與停用應用程式偵錯
下載應用程式偵錯檔案
刪除偵錯檔案
下載應用程式設定
從用戶端裝置下載系統資訊
下載事件記錄
啟動、停止、重新啟動應用程式
執行卡巴斯基安全管理中心網路代理的遠端診斷並下載結果
在用戶端裝置執行應用程式
為應用程式建立記憶體傾印檔案
在基於 Linux 的用戶端裝置上執行遠端診斷
管理用戶端裝置上的協力廠商應用程式和可執行檔
使用「應用程式控制」來管理可執行檔
應用程式控制模式和類別
取得並檢視安裝在用戶端裝置的應用程式清單
取得並檢視儲存在用戶端裝置上的可執行檔清單
建立含有手動新增內容的應用程式類別
建立應用程式類別以包含來自所選裝置的可執行檔
建立應用程式類別以包含來自所選資料夾的可執行檔
檢視應用程式類別清單
在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制
新增事件相關的可執行檔到應用程式類別
建立「安裝必要更新並修復弱點」工作
「弱點掃描和所需更新」工作設定
關於產品授權
OPENAPI 參考手冊
監控和報告
方案：監控和報告
關於監控和報告的類型
智慧培訓模式中的規則觸發
檢視並確認使用自適應異常控制規則執行的偵測
從適應性異常控制規則新增排除
儀表板和小部件
使用儀表板
管理和防護小部件
新增小部件到儀表板
從儀表板隱藏小部件
移動儀表板上的小部件
變更部件尺寸或樣子
變更部件設定

偵測和回應小工具
管理小工具的基礎知識
在小工具中顯示資料的特殊注意事項
建立小部件
新增小部件
刪除小部件
小工具設定
事件小工具
活動清單小工具
快線表單小工具
資產自訂小工具
其他小工具
篩選小工具資料
在單一小工具上篩選資料
在多個小工具中篩選資料
深層探究到相關儀表板
在活動清單類型小工具中顯示租用戶名稱
偵測和回應儀表板
建立儀表板佈局
選擇儀表板佈局
選擇儀表板佈局作為預設佈局
編輯儀表板佈局
刪除儀表板佈局
啟用和禁用TV模式
預先設定的儀表板佈局
關於“僅儀表板”模式
配置“僅儀表板”模式
管理和防護報告
使用報告
報告範本
建立報告範本
檢視和編輯報告範本內容
刪除報告範本
通用報告範本
匯出報告到檔案
生成和瀏覽報告
建立報告傳送工作
偵測和回應報告
報告範本
建立報告範本
設定報告排程
編輯報告範本
複製報告範本
刪除報告範本
匯出或匯入報告範本
通用報告範本

- 產生的報告
  - 檢視報告
  - 產生報告
  - 儲存報告
  - 更新報告
  - 刪除報告
- 事件和事件分類
  - 關於 Kaspersky Next XDR Expert 中的事件
  - Kaspersky Next XDR Expert 元件事件
    - 事件類型描述的資料結構
    - 管理伺服器事件
      - 管理伺服器緊急事件
      - 管理伺服器功能失效事件
      - 管理伺服器警告事件
      - 管理伺服器資訊事件
    - 網路代理事件
      - 網路代理警告事件
      - 網路代理資訊事件
  - 使用事件分類
  - 建立事件分類
  - 編輯事件分類
  - 檢視事件分類清單
  - 匯出事件分類
  - 匯入事件分類
  - 檢視事件詳細資訊區域
  - 匯出事件到檔案
  - 從事件檢視物件歷程
  - 刪除事件
  - 刪除事件分類
  - 設定事件儲存期限
  - 封鎖頻繁事件
    - 關於封鎖頻發事件
    - 管理頻發事件封鎖
    - 移除對頻發事件的封鎖
  - 在管理伺服器上的事件處理和儲存
- 回溯掃瞄
- 通知和裝置狀態
  - 使用通知
  - 檢視螢幕通知
  - 關於裝置狀態
  - 設定裝置狀態轉換
  - 配置通知傳送
  - 測試通知
  - 用於描述事件的參數和環境變數

監控事件來源
來源狀態
事件來源清單
監控政策
卡巴斯基公告
關於卡巴斯基公告
停用卡巴斯基公告
Cloud Discovery
使用小工具啟用 Cloud Discovery
在儀表板中新增 Cloud Discovery 小工具
檢視雲端服務使用情況資訊
雲端服務的風險等級
封鎖對不需要的雲端服務進行的存取活動
匯出到 SIEM 系統的事件
設定事件匯出到 SIEM 系統
先決條件
關於事件匯出
配置在 SIEM 系統中的事件匯出
標記事件，將其以 Syslog 格式匯出到 SIEM 系統
關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統
將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出
標記一般事件，將其以 Syslog 格式匯出
關於使用 Syslog 格式匯出事件
使用 CEF 和 LEEF 格式匯出事件
將事件轉換為 CEF 或 LEEF 格式
設定 Kaspersky Next XDR Expert 以將事件匯出至 SIEM 系統
監控政策與政策設定檔變更
直接從資料庫匯出事件
使用 klsql2 實用程式執行 SQL 查詢
klsql2 實用程式中的 SQL 查詢例子
檢視 Kaspersky Next XDR Expert 資料庫名稱
檢視匯出結果
將事件從OSMP收集器傳送到外部SIEM系統收集器
管理物件修訂
檢視並儲存政策修訂
比較政策版本
回溯物件到先前修訂
物件刪除
從隔離區和檔案備份下載和刪除檔案
從隔離區和檔案備份區下載檔案
關於從隔離區、檔案備份區或主動威脅儲存路中刪除物件
上傳檔案以進行掃描
手動掃描檔案儲存庫中的檔案
檢視掃描狀態和掃描結果

- Kaspersky Next XDR Expert元件的運行診斷
  - 取得Kaspersky Next XDR Expert元件的日誌檔案
  - 查看OSMP指標
    - 監控Kaspersky Next XDR Expert元件的狀態
    - 設定有關Kubernetes叢集運行狀況事件的電子郵件通知
    - 管理Kubernetes叢集運行狀況事件的電子郵件通知收件者
    - 無需重新安裝Kaspersky Next XDR Expert即可將SMTP伺服器連線參數新增到組態檔中
    - 檢視Longhorn指標
    - 檢視EDR儀表板和指標
    - 檢視Node Exporter完整版儀表板
  - 服務監控
    - 查看KUMA指標
    - KUMA指標警示觸發條件
  - 儲存有關Kaspersky Next XDR Expert元件的診斷資訊
  - 取得追蹤檔案
  - 記錄自訂操作的啟動
- 多租用戶
  - 關於將管理伺服器連結到租用戶
  - 設定與Open Single Management Platform的整合
  - 檢視和編輯租用戶
  - 新增租用戶
  - 為租用戶中的使用者和群組指派角色
  - 刪除租用戶
  - 設定電子郵件通知
  - 建立通知範本
  - 編輯並刪除通知範本
  - 設定儲存用於存取共用網路資源的憑證
  - 設定排定的IOC掃描
  - 在檔案儲存庫中設定檔案自動輪換功能
- 聯絡技術支援
  - 如何取得技術支援
  - 透過 Kaspersky CompanyAccount 獲取技術支援
- 已知問題與限制
- 故障排除
- 附錄
  - 元件手動啟動和安裝命令
  - KUMA檔案的完整性檢查
  - 標準化事件資料模型
  - 設定來自KATA EDR的標準化事件資料模型
  - 資產資料模型
  - 使用者帳戶資料模型
  - 稽核事件
    - 使用者已編輯欄位集設定以定義來源
    - 密鑰檔案已新增
    - 備用產品授權金鑰已新增
    - 備用產品授權金鑰已刪除
    - 使用啟動碼啟動的應用程式

產品授權已續期
無效的啟動碼
啟動碼已封鎖
啟動碼或金鑰檔案已刪除
EPS已超限
產品授權已到期，寬限期已開始
寬限期結束
已新增過期的啟動碼或金鑰檔案
更改了用於區分事件存取權限的空間集
服務監控閾值已更改
KUMA Core設定已修改
GeoIP資料庫已匯入
服務已建立
服務已刪除
服務已重新載入
服務已重新啟動
服務已啟動
服務已配對
工作狀態已變更
分割區已被使用者刪除
資料分割區會在保留期限過後自動刪除
分割區已按絕對保留期刪除
分割區已按相對保留期刪除
分割區已移至冷儲存體
將分割區移到冷儲存體時發生錯誤
活動清單清除成功或操作失敗
活動清單項目變更成功或操作失敗
活動清單項目刪除成功或操作失敗
活動清單匯入成功或操作失敗
活動清單已匯出
快顯表單已匯出
快顯表單匯入成功或操作失敗
快顯表單項目修改成功或操作失敗
內容相關資料表項目已修改或操作失敗
快顯表單刪除成功或操作失敗
資源已新增
資源已刪除
資源已更新
匯入資源
設定已更新
服務上的字典更新成功或操作失敗
字典項目已新增
字典項目成功刪除或操作失敗
擴充事件結構欄位已建立
擴充事件結構欄位已編輯
擴充事件結構欄位已匯入
包含擴充事件結果欄位的規範化器已匯入

擴充事件結構欄位已刪除
將請求傳送至KIRA
KICS/KATA回應
Kaspersky Automated Security Awareness Platform回應
KEDR回應
匯入MITRE ATT&CK技術與策略
指標警示已註冊服務或操作失敗
Active Directory中的回應
備份分割區、從備份中還原、從外部安裝的KUMA匯入分割區
使用KIRA將自然語言查詢轉換為SQL查詢。
事件讀取嘗試
搜尋請求已取消
KEDR資源已更新
KEDR資源更新工作已完成
KEDR事件欄位已更新
檔案localizations.json已匯入
規則已連結至收集器
規則已取消與收集器的連結
規則已連結至關聯器
規則已與關聯器取消連結
從 KUMA 匯出的資源
從隔離網路區段接收事件相關服務資料
關聯規則
時間格式
對應預定義標準化器的欄位
詞彙表
Bootstrap
EPP應用程式
IOA 規則
IOC檔案
Kaspersky Deployment Toolkit
Kubernetes叢集
KUMA 服務
KUMA清查檔案
上下文
事件
事件
事件路由器
代理程式
傳輸封存檔案
儲存體
分段規則
分發套件
可觀察部分
回應操作
多租用戶
威脅發展鏈

- 常規程式
- 常規程式演算法
- 收集器
- 標準化事件
- 登錄檔
- 目標主機
- 租用戶
- 節點
- 管理員裝置
- 組態檔
- 網路代理
- 網路位置辨識 (NLA)
- 自訂操作
- 調查圖表
- 警示
- 資產
- 輕量級 Nagent（LWNGT）
- 鑑證資料
- 關聯器
- 關聯規則

第三方程式碼相關資訊

商標聲明

The MITRE Corporation Terms of Use

Kaspersky Next XDR Expert

新功能

- Kaspersky Next XDR Expert的新增功能

主要功能

- 管理警示和安全事件
- 搜尋威脅工具
- 調查圖表
- 預定義和自訂常規程式
- 手動威脅回應操作
- 儀表板和小工具

相容性以及硬體和軟體需求

- 硬體和軟體需求
- 相容的卡巴斯基應用程式和解決方案
- 與其他解決方案和協力廠商系統整合

正在啟動

- Kaspersky Next XDR Expert的部署、啟動和初始設定的演示情境
- Kaspersky Next XDR Expert的部署
- 遷移到 Kaspersky Next XDR Expert
- 使用威脅監控、偵測和搜尋功能
- 使用Kaspersky Next XDR Expert進行事件調查的範例

使用 Open Single Management Platform

- 在企業網路裝置上安裝卡巴斯基安全應用程式
- 遠端執行掃描和更新工作
- 管理受管理應用程式的安全政策

新增內容

Kaspersky Next XDR Expert 2.3

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 在包含警示詳情和事件詳情的視窗中，於**可觀測項**區段，您可以依據**值**欄中的資料搜尋可觀察物件表格。
- 當警示新增至**新增**狀態的事件或從中移除時，系統會自動重新評估事件優先順序。優先順序會設為**事件嚴重性**值。
- 現已提供新的預先定義常規程式：
  - [KL][EDR]「根據警示緩解電子郵件附件引發的惡意活動」常規程式
  - [KL][EDR]「根據事件緩解電子郵件附件引發的惡意活動」常規程式
  - [KL][EDR]「根據警示緩解記憶體傾印活動」常規程式
  - [KL][EDR]「根據事件緩解記憶體傾印活動」常規程式
  - [KL][EDR]「根據警示，在偵測到探索活動時隔離主機」常規程式
  - [KL][EDR]「根據事件，在偵測到探索活動時隔離主機」常規程式
  - [KL][EDR]「偵測到資料外洩活動時隔離主機」常規程式
  - [KL][EDR]「根據警示刪除已傳輸至主機的惡意檔案」常規程式
  - [KL][EDR]「根據事件刪除已傳輸至主機的惡意檔案」常規程式
  - [KL][EDR]「根據警示，在偵測到反向 Shell 活動時隔離主機」常規程式
  - [KL][EDR]「根據事件，在偵測到反向 Shell 活動時隔離主機」常規程式

Kaspersky Next XDR Expert 2.2

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 可在首次登入後強制使用者帳戶變更密碼，或在指定天數後強制其變更密碼。
- 分段和彙總規則的改善事項：
  - 現在支援繼承。
  - 現在可在 **監控 → 資源與服務** 區段中設定規則。
- 新增兩個連接器，用於透過 SMB 和 SFTP 通訊協定接收記錄檔。
- 新的選用參數 `--pair.fingerprint` 有助於提升服務連線至 KUMA Core 的安全性。從 Kaspersky Next XDR Expert 2.2 起，當您建立服務時，安裝精靈預設會在安裝命令中包含 CA 憑證指紋。例如：`/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:7210 --pair.fingerprint XXXX --id YYYY --api.port ZZZZ --install`。如果您不想使用指紋驗證，可以輸入 `insecure` 作為該選項的值。從 Kaspersky Next XDR Expert 2.1 升級到 2.2 時，不需要執行任何額外動作。在 Kaspersky Next XDR Expert 2.2 之前安裝的服務，升級後預設使用 `insecure` 值。如果將 CA 憑證指紋 ID 用於 `--pair.fingerprint` 選項，則在重新簽發 CA 憑證後，您需要從網頁介面複製新的指紋 ID，並在 systemd 組態中以新值更新該選項，然後重新啟動服務。
- 新增了**新的轉換類型 unicodeUnescape**，可在將原始事件欄位的值寫入 OSMP 事件欄位之前，將其從 Unicode 字串轉換為人類可讀的文字。

  轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

  可用轉換類型：
  - **小寫** — 用於將值的所有字元變為小寫
  - **大寫** — 用於將值的所有字元變為大寫
  - **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
  - **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。
  - **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
    - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
    - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
  - **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
  - **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
  - **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。

- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。
  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。
  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。
- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

- 您現在可以使用安裝在該網路區段內的代理，將隔離網路區段中事件的服務資料傳送至收集器。
- XDR 功能區域現在提供更精細的租用戶存取權限。
- Kaspersky Deployment Toolkit 改善事項和新增功能：
  - 推出 **XDR Deployer**，這是一個逐步互動式精靈，可自動執行作業系統準備、預先檢查和應用程式部署。
  - 您現在可以設定存取權杖、重新整理權杖和 SSO 工作階段的存留期。可在部署前透過設定檔參數進行設定，也可在部署後使用自訂動作進行設定。

- 除了記錄檔外，緊急部署錯誤現在也會直接顯示在主控台視窗中。
- 新增 `./kdt metrics export` 命令，可讓您取得主要 OSMP 指標的壓縮檔案，以便進一步匯入及分析。

- 使用者體驗改善：
  - 在資產詳細資料中，您現在可以搜尋已安裝軟體清單。
  - 您現在可以變更 EDR 代理連線至代理伺服器所用的預設連接埠，以及透過瀏覽器存取 OSMP Console 伺服器所用的預設連接埠。
  - 改善了不包含 `ProcessUniqueId` 欄位之事件的調查圖節點之間的連結。
  - 新增從事件詳情和警示詳情導覽至 Kaspersky TIP 的功能，以檢視 MITRE ATT&CK 戰術與技術的詳細資訊。
  - 警示和事件表格現在包含 **外部參考** 欄。
  - 新增編輯和刪除警示及事件註解的時間限制。現在可設定在警示或事件建立後經過指定期間後，這些動作不再可用。

- 以下功能繼承自Kaspersky Security Center for Linux：
  - 已增強**工作**和**政策**表格的篩選功能。現在您可以使用 OR 邏輯新增多個條件，也可以使用新的運算符，該運算符允許您為單一屬性選擇多個值，並顯示至少符合一個指定條件的記錄。
  - 發佈點功能已改進：清單現在僅顯示未指派的分發點。
  - 現在，您可以一次為多個虛擬管理伺服器指派管理員。
  - 在主功能表中：
    - 提供了新的**軟體管理**區段。下列區段現在已移至**軟體管理**：**安裝套件**、**卡巴斯基應用程式**、**第三方應用程式**、**最新應用程式版本**，以及 **修補程式管理**。
    - **未指派的裝置**和**硬體**部分現已移至**資產管理**。
    - **工作** 和 **儲存區** 區段已移至功能表的第一層級。
    - 「Web 外掛程式備份」區段已不再使用，並已從網頁主控台中移除。

- Kaspersky Deployment Toolkit現支援以下作業系統版本：
  - Ubuntu Server 26.04 LTS
  - Astra Linux特別版 RUSB.10015-01（操作更新 1.8.5）

- Kaspersky Next XDR Expert現支援以下作業系統版本：
  - Ubuntu Server 26.04 LTS
  - Astra Linux特別版 RUSB.10015-01（操作更新 1.8.5）

- 現支援以下虛擬化平台：
  - Microsoft Hyper-V Server 2022
  - Nutanix 7.3
- Kaspersky Next XDR Expert現支援搭配使用以下DBMS：
  - PostgreSQL 18.4 64位元
  - Postgres Pro 18 Enterprise 64 位元（叢集內建高可用）
- 新增了針對 `DeviceCustom*` 和 `Flex*` 事件卡欄位使用精簡顯示模式的功能，其中 `Label*` 欄位值會顯示為欄位名稱。
- 新增了專為使用 KUMA 套件和資源而設計的新知識庫區段。此區段可讓使用者搜尋和篩選套件與資源、檢視其相關資訊、安裝整個套件或個別資源、更新資源，以及檢視它們之間的相依性。
- 新增了新的 hexToDecimal 轉換類型，用於在將來源事件欄位值儲存至 KUMA 事件欄位前，將其從十六進位轉換為十進位。
- 使用 **regexp** 剖析方法的正規化程式現在可讓您使用 KIRA，根據新增的範例產生規則運算式。在此情況下，產生的規則運算式會自動新增至 **正規化** 欄位。
- 新增了建立 SQL 查詢時的函數建議。當您在 SQL 查詢欄位中輸入函數名稱時，會顯示可用函數清單，並顯示所選函數的使用範例。
- 現在可對以 sFlow 格式接收的事件使用額外正規化。
- 降低 DNS 豐富化期間 DNS 伺服器的負載：事件發生時，解決方案會進行兩次豐富化嘗試。聯絡 DNS 伺服器後，收集器會將 IP 位址和主機名稱的相關資訊快取至磁碟。此資料會在快取記錄的整個保留期間內使用。事件記錄會儲存在磁碟上，直到快取或記錄從 DNS 伺服器刪除為止。
- 若要從隔離的網路區段接收 NetFlow 事件，會使用安裝在此區段內的專用代理。代理會作為中繼節點：在本機接收 NetFlow 事件，並將其轉送至已設定 NetFlow 連接器的收集器。
- 新增了用於測試與 SMTP 伺服器連線的按鈕。若要測試連線，Kaspersky Next XDR Expert 會將測試訊息傳送到目前使用者設定檔中指定的電子郵件地址。
- 從儲存庫匯入資源時，會使用在 KUMA Core 設定區段的 KUMA 資源本地化設定中指定的語言。
- 在 Kaspersky Next XDR Expert 2.1 中以 Beta 版本新增的兩項功能 — 週期類型的關聯規則，以及帳戶未經授權使用偵測 — 在 Kaspersky Next XDR Expert 2.2 中無法使用。這些功能預計會在 Kaspersky Next XDR Expert 的下一個版本中重新設計並發行。
- 已新增對使用 ODBC 驅動程式的SQL 連接器的支援。
- 新增用於透過 HTTP 接收串流事件的http-streaming 類型連接器。

Kaspersky Next XDR Expert 2.1

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 使用者活動稽核事件現在可以在**威脅搜尋**部分找到。這些事件提供有關使用者操作的詳細資訊，並在**EventType** 欄位中以 `Audit` 值標記。
- 在威脅搜尋**威脅搜尋執行事件搜尋**時，對於手動執行的查詢，會產生一個稽核事件。
- [OOTB] Kaspersky OSMP 收集器用於從 OSMP 元件接收稽核事件（稽核事件、稽核事件）。此收集器會在 OSMP 部署期間自動安裝。稽核事件會被傳送到稽核空間，該空間在儲存中自動建立。
- 資產篩選選項包括：**僅顯示子實例**和**僅顯示父實例**。這些選項可讓您根據資產屬於子執行個體還是父執行個體來篩選資產。所選篩選條件將直接套用於資產表，並立即更新顯示結果。
- 刪除資產類別分為兩個階段：歸檔和永久刪除。歸檔階段允許您在將類別從系統中永久移除之前，請驗證該類別是否仍被任何資源引用。
- 新增調查和回應功能：
  - 在您指定延遲原因之前，針對違反SLA的事件的操作將被阻止。
  - 現在，警示和事件詳情的載入速度更快。
  - 現在可以透過API匯出和匯入常規程式。您可以使用它在租用戶和實例之間輕鬆傳輸常規程式。
  - 增加了比較常規程式不同版本的功能來跟蹤更改並簡化版本管理。
  - 現在可以查看常規程式和回應操作執行的詳細結果。您可以在**回應歷史**部分查看這些結果，方法是按一下**常規程式狀態**或**動作狀態**值以開啟執行詳情窗格。
  - 現在，您可以在Kaspersky TIP中檢視IOA規則的詳細資訊。為此，在警示或事件詳情或IOA規則詳情中，按一下**在 Kaspersky TIP 中尋找**按鈕。
  - 新的預定義常規程式現已可用：
    - 檢查外部IP位址的常規程式。
    - 用於隔離檢測到受感染文件的裝置的常規程式。
- 現在開啟運作狀況監控儀表板更方便。您無需再輸入URL，只需在Kaspersky Next XDR Expert中按一下按鈕。
- 檔案管理功能改進：
  - 檔案上傳進度現在會顯示在檔案區段中。您可以將檔案直接上傳到**檔案**部分，也可以將其附加到警示或事件。上傳進度只能在**檔案**部分跟踪，所有已上傳檔案都會自動顯示在此處。
  - 現在，您可以在**檔案**部分檔案。啟用此功能後，系統會刪除最舊的檔案以釋放空間，方便上傳新檔案。與偵測到的威脅關聯的檔案不會被刪除，並會繼續連結到相應的警示。

- 對OSMP實例層級結構的改進：
  - 現在您可以將阻止規則分發到整個層級結構中。
  - 現在您可以將YARA和IOC規則分發到整個層級結構中。
- 改進了進程樹狀圖可視化功能。現在，進程樹狀圖資料是按需載入的，而不是一次檢索所有相關事件。
- 改進了沙盒環境中的使用者活動日誌記錄：
  - 沙盒環境中已記錄的使用者操作集已得到擴展。
  - 沙盒使用者活動日誌現已可供查看。
- OSMP可以使用Syslog協定將應用程式網頁介面中的使用者操作資訊以及警示匯出到外部SIEM系統。SIEM 系統可以是 KUMA（獨立解決方案）或協力廠商 SIEM 系統。
- OSMP分發套件包含一個預定義關聯規則，該規則會在三次身分驗證失敗後產生關聯事件。
- 當分區因相對保留期而被刪除時，會將 `DeviceEventCategory` 參數新增至產生的稽核事件。
- 現在可以指定最大EPS值，以確定回溯掃描中的最大負載。
- 現在支援在 extract_from_timestamp 函數中使用 `$timezone` 變數。時區可以動態設定，包括透過關聯規則局部變數中定義的基於字典的變數。
- 您現在可以使用**自訂**模式，透過 Kaspersky Investigation and Response Assistant 分析警示和事件。在**自訂**模式下，請求將直接傳送到指定的第三方LLM提供者的API。
- 以下功能繼承自Kaspersky Security Center for Linux：
  - 您可以比較政策修訂版本。此選項目前適用於管理伺服器、網路代理程式、 Kaspersky Endpoint Security for Windows（從14.0網頁外掛程式版本開始）和Kaspersky Endpoint Security for Mac（從12.2.1 Patch A網頁外掛程式版本開始）。在未來版本中，支援此功能的卡巴斯基應用程式清單將會擴展。
  - 您可以將事件以CEF或LEEF格式匯出至SIEM系統。
  - 改進了在 Linux 裝置上保留網路代理裝置識別碼（`Device ID` 參數）的演算法。如果裝置的BIOS序列號、主機板序列號、儲存磁碟ID或MAC位址與之前已知的值匹配，則管理伺服器會在作業系統更新或MAC位址更改後正確識別裝置。
  - 網路代理現支援 Windows ARM 64 位元架構。您可以在對應的說明文件中驗證與受管應用程式管理的相容性。
  - 現在提供適用於Linux的網路代理程式的單一安裝程式套件。此安裝程式包含適用於不同軟體套件管理器和CPU架構的版本。在安裝程式過程中，系統會自動偵測環境並安裝對應的網路代理程式軟體套件。
  - 在隔離網路中，為 Windows 裝置建立安裝套件現在需要從卡巴斯基網站下載其他模組。
  - 適用於Linux的網路代理程式現支援無法解析localhost的環境。
  - 現在您可以一次刪除事件分類和裝置事件清單中的所有事件。

    事件分類和裝置事件清單中均有**全選**和**全部選取目前頁面**選項。

    - 現在，您可以手動指定移動規則的優先順序。
      選擇移動規則後， **變更優先順序**按鈕將變為可用狀態，讓您指定新的優先順序。

- Kaspersky Deployment Toolkit現支援以下作業系統版本：
    - Astra Linux特別版RUSB.10015-01（操作更新1.8.2）
    - Oracle Linux 9.7
- 網路代理現在支援搭配使用以下新作業系統版本：
    - Microsoft Windows 11家用版/專業版/工作站專業版/企業版/教育版ARM
    - Platform V SberLinux OS Server (SLO) 9.6
- Kaspersky Next XDR Expert現支援以下作業系統版本：
    - Astra Linux特別版RUSB.10015-01（操作更新1.8.2）
- 現支援以下虛擬化平台：
    - VMWare vSphere 9
- Kaspersky Next XDR Expert現支援搭配使用以下DBMS：
    - PostgreSQL 17.9 64位元
    - PostgreSQL 18.3 64位元
    - Postgres Pro 17.7.1企業版64 位元（叢集內建高可用性）

Kaspersky Next XDR Expert 2.0

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 統一的OSMP主控台：您現在可以在Kaspersky Next XDR Expert中管理Kaspersky Unified Monitoring and Analysis Platform和Kaspersky Endpoint Detection and Response的情景。
- 現支援KasperskyKaspersky Endpoint Detection and Response新增回應操作：
    - 管理服務
    - 刪除檔案
    - 取得檔案
    - 從隔離區取得檔案
    - 掃描從裝置獲取或使用者上傳的檔案
    - 取得記憶體轉儲

    - 取得進程記憶體傾印檔案
    - 若要取得磁碟映像
    - 取得鑑識資訊
    - 取得登錄檔金鑰
    - 取得NTFS元檔案
    - YARA 掃描
    - IOC 掃描
    - 從隔離區還原檔案
    - 從隔離區刪除檔案
- 新增AI功能：
    - 使用KIRA產生警示和事件的簡要報告，以提高分析效率。
    - AI會分析帳戶行為，並在偵測到可疑活動或帳戶被盜用跡象時產生警示。
    - AI可以偵測合法應用程式載入惡意的DLL並替換原始DLL的攻擊。
    - AI 現在可以協助您在 **威脅搜尋**區段中產生 SQL 查詢。
- 現在所有帳戶都需要雙步驟身分驗證以增強安全性。
- 現在您可以在測試模式下啟動常規程式，以便在執行前檢查其功能。
- 您現在可以從**資產（裝置）**和**回應歷史**部分以及**事件詳細資訊**中啟動回應操作。
- 現在可以使用更新的參數重新執行回應操作。
- 新增遠端終端存取功能，用於直接進行裝置調查和回應操作。
- 調查圖的改進：
    - 您現在可以根據時間線在調查圖表上放置事件。較早發生的事件顯示在左側，較晚發生的事件顯示在右側。
    - 事件樹現在顯示在專門的窗格中，而不是直接顯示在圖表上。
    - 圖表上的事件現在沿著時間線排列：早期事件顯示在左側，後期事件顯示在右側。
    - 現在您可以為整個流程樹和單一節點新增備注。
    - 縮放圖表時，節點可以分組到叢集中，您可以延伸叢集以在最佳化比例下檢視底層節點。
- 我們實行了新的事件資料模型。

- 新增了以下警示類型：
  - 基於檔案掃描結果產生的警示。
  - 當檔案在先前的警示中未被分析後再次掃描時，系統會建立重新掃描警示；
  - 由TAA（IOA）偵測技術產生的警示；
  - 由IOC偵測技術產生的警示；
  - 由YARA偵測技術產生的警示。
- IOA規則排除項設定現在可以在Kaspersky Endpoint Security for Windows策略中配置，可以直接在策略中或從警示或事件詳情中配置。
- 現在您可以設定使用者身分驗證政策，包括密碼有效期限和使用者會話終止前允許的非活動期。
- 新增了對分層多租用戶的支援。安裝程式可以組織成父實例和子實例，並且能夠從父實例連接到子實例。
- 「**資產（裝置）**」部分現在包含兩個頁籤：
  - 「**資產（裝置）**」，您可以在這裡管理和分類裝置。
  - 「**分析與回應**」，您可以在這裡對列出的資產啟動回應操作，並透過遠端終端連線到這些資產。
- 現在您可以建立和管理以下自訂規則：
  - 阻止規則
  - IOC 規則
  - YARA 規則
  - 沙盒規則
- 啟用與卡巴斯基沙盒的整合後，Kaspersky Endpoint Security for Windows和Kaspersky Endpoint Security for Linux現在支援自動和手動向沙盒傳送檔案。
- 現在支援物理隔離部署：
  - 在具有網際網路存取權限的管理主機上準備一個軟體套件存檔。
  - 將該軟體套件存檔傳輸到隔離環境。
  - 在無法存取網際網路的目標主機上安裝Kaspersky Next XDR Expert。
- 增加了對上傳伺服器和端點代理憑證的支援，以便在它們之間建立安全連線。
- 新增了對上傳憑證以連線到沙盒的支援。
- 現支援FreeIPA和ALD Pro網域控制器。
- 您的帳戶選單現在已從主選單移至頂部窗格。
- 新增語言支援：Kaspersky Next XDR Expert現已支援簡體中文和繁體中文。

- SIEM組件 (KUMA) 中引入的新功能和改進：
  - Metrics服務可以安裝在任意主機上。必須只存在一個Metrica服務。從頭開始安裝KUMA時，您必須在清查檔案的`kuma_metrics`部分指定安裝Metrics服務的主機。將KUMA升級到4.2版本時，您必須在清查檔案的`kuma_metrics`部分中指定作用中Metrics服務安裝所在的主機。例如，如果在KUMA 4.0中，Metrics服務安裝在kuma-core.example.com主機上，在升級到4.2版本之前，您需要在清查檔案的kuma_metrics部分指定kuma-core.example.com主機。如果您想將Metrics服務遷移到另一個主機，您可以使用expand.sh安裝程式和expand.inventory.yml清查檔案進行遷移。

    將KUMA Core遷移到Kubernetes叢集時，您必須首先使用expand.sh安裝程式和expand.inventory.yml清查檔案將Metrics服務遷移到與KUMA Core相同的主機。將KUMA Core遷移到Kubernetes叢集時，會檢查Metrics服務是否在此主機上執行。如果找不到Metrics服務，則會傳回錯誤並停止遷移。當您將KUMA Core遷移到Kubernetes叢集時，指標資料會遷移到叢集中。
  - 您可以按排程備份分割區、手動備份分割區、從備份中還原分割區，或從外部安裝的KUMA匯入分割區。
  - 現在您可以使用網頁介面備份和還原KUMA Core。
  - 對於冷儲存，ClickHouse叢集中的資料現在可以傳輸到S3雲端儲存服務。
  - Kafka連接器現在使用SCRAM-SHA-256和SCRAM-SHA-512安全連線機制進行授權。
  - 新增了universalAPI連接器，用於從任意REST API取得資料，支援JSON、依ID篩選和迭代模式。
  - 現在您可以在背景執行SQL請求，執行時採用較低的優先順序，並在執行完成後檢視結果。
  - 使用主管理員帳戶時，您現在可以檢視及管理其他使用者的作用中請求。
  - 引入定期關聯規則類型，該類型用於透過偵測可能表明帳戶被盜的異常使用者活動來偵測未經授權的帳戶使用。只有在使用correlator-ng關聯器時才能建立此規則。
  - 現在您可以在使用者帳戶中設定時區和ISO 8601格式，以及為整個KUMA實例自訂一週的第一天（僅主管理員可用）。
  - 現在您可以將資源（關聯規則、擴充規則、回應規則、彙總規則和目標）關聯到收集器、關聯器和事件路由器等服務。可用的服務取決於所選資源的型別。
  - 新增了一種目標類型：udp，允許透過UDP從收集器和關聯器傳輸規範化事件。
  - 現在，您可以在快顯表單中以CSV和TSV格式匯出資料。
- 卡巴斯基安全管理中心 Linux 16.1 中引入的新功能和改進。

Kaspersky Next XDR Expert 1.4

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 升級Kaspersky Next XDR Expert 時，您可能需要根據要升級的版本更新 Bootstrap。

  - **需要Bootstrap更新的升級**

    請為以下Kaspersky Next XDR Expert升級更新Bootstrap：

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

    若要更新Bootstrap，請執行以下命令：

    ```
    ./kdt apply -k <path_to_XDR_updates_archive> -i <path_to_configuration_file> --force-bootstrap
    ```

    之後，執行以下命令更新Kaspersky Next XDR Expert：

    ```
    ./kdt apply -k <path_to_XDR_updates_archive>
    ```

  - **無需Bootstrap更新的升級**

    對於以下Kaspersky Next XDR Expert更新版本，請勿更新Bootstrap：

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

    若要更新Kaspersky Next XDR Expert，請執行下列命令：

    ```
    ./kdt apply -k <path_to_XDR_updates_archive>
    ```

- 現在您可以為事件處理設定固定回應時間（SLA）。SLA指標包括徹底解決事件所需的時間、首次回應時間以及確認事件所需的時間。
- 現支援Postgres Pro內建高可用性叢集。安裝Kaspersky Next XDR Expert時，此DBMS叢集的節點會在連線字串中指定。
- 您現在可以儲存 Kaspersky Next XDR Expert 資料的備份副本，然後從建立的副本還原資料。
- 現在，您可以新增或刪除Kubernetes叢集包含的工作線程節點，而無需重新啟動叢集節點。
- 現支援將常規程式儲存為草稿。常規程式無法啟動，但可以在常規程式所屬的租用戶中進行編輯。若要啟動常規程式草稿，您需要先將其發布。
- 您可以為任何圖表節點或連結留下備注。

- 現支援將事件匯出為PDF。
- 現在您可以將受警示或事件影響或涉及的資產資訊，以及與當前事件相關的警示的可觀察物件資訊匯出為CSV檔案。
- 您可以手動或使用常規程式將警示和事件指派給使用者群組。如果您希望根據使用者群組的工作負載和可用性狀態自動將警示和事件指派給使用者群組，可以啟用自動指派功能。
- 現在可以使用常規程式視覺化編輯器建立常規程式。常規程式視覺化編輯器可讓您建立和視覺化常規程式執行流程以及常規程式演算法步驟之間的關係。
- 將警示連結到事件時，會顯示警示和事件的名稱。這樣可以依名稱篩選警示和事件。
- 警示和事件的篩選功能隨即改善。
- 如果警示套用了多個彙總規則，這些規則現在會根據指定的優先順序依順序處理，而不僅僅是處理找到的第一個規則。
- 現在可以使用 Linux 裝置漫遊使用者的連線設定檔。透過使用連線設定檔，您可以為 Linux 裝置上的網絡代理配置連線到相同或不同管理伺服器的規則，具體取決於裝置位置。
- 現在可以在管理伺服器之間傳輸加密金鑰。
- **掃描**按鈕被從**隔離**部分刪除。

Kaspersky Next XDR Expert 1.3

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 應用程式中使用了更新版本的Bootstrap。在安裝新版本的Kaspersky Next XDR Expert之前，請執行以下命令更新Bootstrap：

  ```
  ./kdt apply -k <path_to_XDR_updates_archive> -i <path_to_configuration_file> --force-bootstrap
  ```

- 現在您可以建立子事件。子事件可讓您調查和回應不同租用戶中的事件。
- Kaspersky NGFW現支援事件回應情景。您可以使用KUMA清查檔案為Kaspersky NGFW建立服務。Kaspersky NGFW包含以下功能：
  - 透過Kaspersky NGFW阻止IP位址。
  - Kaspersky NGFW的全新儀表板。
- 現在，您無需重新安裝即可使用Kaspersky Deployment Toolkit變更Kubernetes叢集的IP位址和服務的FQDN。
- 組態檔參數預驗證。Kaspersky Deployment Toolkit會在安裝或更新Kaspersky Next XDR Expert之前，先驗證組態檔中參數的存在及其值。此功能適用於單節點和多節點部署。
- 現在您可以在Kaspersky Next XDR Expert的使用者介面中管理彙總規則。
- 新小工具，**依類型分類的事件**，隨即新增。

- 以下儀表板小工具現在會顯示未關閉事件的資訊：
  - 活動事件
  - 依租用戶分類的活動事件
  - 依嚴重程度分類的事件
  - 事件中受影響的資產
  - 事件中受影響的資產類別
  - 最新事件
- 可合併的事件關聯警示數量上限已提高。可合併的事件關聯警示最大數量為1000個。合併事件時， 在**合併事件**視窗中會顯示與這些事件相關的警示數量。
- 卡巴斯基IP位址不再包含在與警示或事件相關的可觀察物件中。
- Kaspersky Next XDR Expert現支援新版本的EPP應用程式。

Kaspersky Next XDR Expert 1.2

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 應用程式中使用了更新版本的Bootstrap。在安裝新版Kaspersky Next XDR Expert之前，請執行下列命令更新Bootstrap：

  ```
  ./kdt apply -k <path_to_XDR_updates_archive> -i <path_to_configuration_file> --force-bootstrap
  ```

- Kaspersky Next XDR Expert從版本1.1升級到版本1.2。
- Kaspersky Next XDR Expert 部署經過最佳化：改良的設定檔和快速啟動精靈可協助輸入安裝參數。
- 部署前檢查。在部署Kaspersky Next XDR Expert之前，您現在可以檢查系統是否符合需求。Kaspersky Deployment Toolkit（KDT）會檢查您的硬體、作業系統、軟體和網路環境。如果至少一項需求未滿足，KDT將中斷部署並提供詳細報告。
- 靈活的事件工作流程。您可以設定事件工作流程並在視覺化編輯器中檢視。
- 現在您可以將檔案附加到警示或事件。根據需要，您可以刪除或下載附加檔案。
- 使用事件類型來自訂事件處理流程。
- 建立常規程式時，您可以設定常規程式演算法來編輯事件內容或警示內容。
- 您可以將事件表中顯示的所有事件的資訊匯出到JSON檔案。當您必須向協力廠商提供此資訊時，可能需要此資訊。
- 基於AI的資產評分。基於機器學習的引擎可協助您評估資產上執行的進程，並確定特定進程是否正常，或是否異常並需要SOC分析師關注。

- 改進了Kaspersky Next XDR Expert中發生的事件的電子郵件通知範本的配置流程。
- 您可以根據需要縮短或延長警示和事件的保存期間。預設情況下，警示和事件的保存期間為360天。
- 解除安裝 Kaspersky Next XDR Expert。所有已建立的資料也將被刪除。
- 現在，您可以從警示詳情視窗或事件詳情視窗的快速選單中，在新瀏覽器頁籤中開啟**威脅搜尋**頁面。
- 在警示詳情視窗或事件詳情視窗中，您現在可以搜尋受影響的資產和可觀察物件。
- 此外，您也可以透過REST API設定警示彙總規則。
- 當您從警示詳情視窗或事件詳情視窗開啟**威脅搜尋**頁面時，搜尋範圍現在為警示或事件的第一個事件和最後一個事件之間的時間段，而不是過去24小時。
- 部署預檢。在部署Kaspersky Next XDR Expert之前，您現在可以檢查系統是否符合需求。Kaspersky Deployment Toolkit（KDT）會檢查您的硬體、作業系統、軟體和網路環境。如果至少一項需求未滿足，KDT將中斷部署並提供詳細報告。
- Kaspersky Next XDR Expert 現在可以安裝在 Nutanix AHV 虛擬化平台上。
- OSMP主控台最佳化：主控台視窗、登入頁面和儀表板的載入速度更快。
- 現在您可以從事件詳情視窗切換到**威脅搜尋**頁面上的事件關聯事件。
- Kaspersky Next XDR Expert現支援以下EPP應用程式：
  - Kaspersky Endpoint Security for Windows，版本12.5、12.6 和 12.7
  - Kaspersky Endpoint Security 12.1 for Linux
  - Kaspersky Endpoint Security 12.1 for Mac
  - Kaspersky Industrial CyberSecurity for Nodes 4.0
  - Kaspersky Endpoint Agent 4.0
- Kaspersky Next XDR Expert現與Kaspersky Anti Targeted Attack Platform 7.0相容。
- 現在，您可以點擊重新整理圖示來重新整理警示詳情視窗和事件詳情視窗中的資訊。

Kaspersky Next XDR Expert 1.1

Kaspersky Next XDR Expert有幾項新功能和改善事項：

- 應用程式中使用了更新版本的Bootstrap。在安裝新版Kaspersky Next XDR Expert之前，請執行下列命令更新Bootstrap：

  ```
  ./kdt apply -k <path_to_XDR_updates_archive> -i <path_to_configuration_file> --force-bootstrap
  ```

- 全新的使用者介面設計。

- 更低的硬體和軟體需求。
- 更高的應用程式穩定性。
- 新增部署精靈，用於簡化安裝參數的設定。
- 新增預定義常規程式。
- Kaspersky Next XDR Expert現支援以下EPP應用程式：
  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Industrial CyberSecurity for Nodes 3.2
  - Kaspersky Endpoint Agent 3.16
- 新增儀表板小工具，用於監控透過常規程式執行的回應。
- 從卡巴斯基安全管理中心遷移到Kaspersky Next XDR Expert ，包含使用者和租用戶的遷移，以及將租用戶綁定到卡巴斯基安全管理中心的管理伺服器。
- Kaspersky Next XDR Expert現與Kaspersky Anti Targeted Attack Platform 6.0相容。
- Kaspersky Unified Monitoring and Analysis Platform於2024年8月更新中引入了新功能與改進。

修正的錯誤

下表列出了在Kaspersky Next XDR Expert先前版本中發現並在目前版本中修復的所有問題。

Kaspersky Next XDR Expert 2.3中已修復問題清單

受影響的第一個版本	問題ID	問題描述
2.2	10682804	選取某些區段（例如 **來源狀態**）作為首頁，並重新登入 OSMP 主控台後，顯示空白頁面。
2.1	10699357	登入 OSMP 主控台時，可能會顯示訊息 Kaspersky Next XDR Expert 組態不正確。
2.1	10684421	從事件卡片向下鑽取至相關警示和其他事件的警示詳情後，卡片便停止載入。
2.1	10664845	將裝置新增至 Kaspersky Endpoint Security for Windows 政策的信任區域時，顯示的可用裝置清單可能會包含已新增至信任區域的裝置。
2.2	10644898	如果在 **遠端網路位址** 索引標籤上指定 IP 位址範圍，則在政策內容（**應用程式設定** → **防火牆**）中新增的網路封包規則不會儲存。
2.1	10563335	Kaspersky Endpoint Security for Windows 政策的安裝作業會在 MDR 設定步驟之後停止。
2.1	10563321	修正了在 Kaspersky Endpoint Security for Windows 政策內容（**應用程式設定** → **一般設定** → **遙測設定**）中編輯排除規則時發生的問題：如果排除規則包含格式為「EventType = *value*」的條件，將「=」運算子取代為「等於」會導致「已存在具有該名稱的規則」錯誤。
1.4	9934440	安裝 OSMP 期間，不會在安裝主機上檢查是否能透過 `resolv.conf` 檔案中指定的 DNS 伺服器正確解析平台元件（OSMP 主控台、管理伺服器、DBMS）的 FQDN。

Kaspersky Next XDR Expert 2.2.1 中已修正的問題清單

受影響的第一個版本	問題ID	問題描述
2.2	10563365	新增 HTTP 串流連接器。
2.1	10624497 10634081	Kaspersky Next XDR Expert 資料的備份副本已正確建立。

Kaspersky Next XDR Expert 2.2中已修復問題清單

受影響的第一個版本	問題ID	問題描述
2.1	10355947	URL 未顯示在警示或事件詳細資料的 **可觀測項** 區段中。
2.1	10137933	`/api/v1/alerts` 端點傳回文字格式而非 JSON 格式的錯誤回應。
2.0	10135653	如果金鑰放置在中繼憑證檔案的開頭，套用設定檔會失敗並出現 `intermediate_bundle: parameter is not PEM encoded` 錯誤。
2.1	10014033	在 **回應歷史** 區段中，套用「**常規程式名稱** != <playbook name>」篩選器時，手動回應項目被錯誤地包含在搜尋結果中。

2.1	10091214	再次按一下目前使用中的主選單區段會導致出現空白頁面。
2.1	9726211	比較兩個常規程式版本時，先選擇最新版本，然後再選擇較早版本後，比較檢視會顯示為顛倒狀態：較新的版本顯示在左側，變更以紅色醒目提示；較舊的版本顯示在右側，變更以綠色醒目提示。

Kaspersky Next XDR Expert 2.1.3 中已修復問題清單

受影響的第一個版本	問題ID	問題描述
2.1	10119212	將 Kaspersky Next XDR Expert 2.0.1 HF4 升級到 2.1 HF2 時，如果使用超過五個工作節點，則遷移至 NATS 會失敗。
2.1	10129716	無法從警示詳情導覽至關聯的 CEF 事件，且無法使用 CEF 事件匯出。
2.1	10132483	無法設定警示和事件清單的自動重新整理間隔。
2.1	10132891	匯出特定租用戶的事件時，匯出的檔案包含所有租用戶的事件，而非僅包含所選租用戶的事件。
2.1	10133000	內部連接器的 Auditd 參數運作不正確。
2.1	10133396	在 SQL 查詢中使用 EDR 和 CEF 欄位時，欄位別名處理不正確，導致 countIf 函式和巢狀查詢失敗。
2.1	10133457	存在大量作用中服務時，**資源和服務**區段載入緩慢。
2.1	10135956	存在大量警示或事件時，無法依警示或事件 ID 搜尋表格。
2.1	10145872	無法透過 OSMP 主控台介面或 API 刪除 SMTP 設定中包含的金鑰。此外，即使在不需要金鑰的情況下，也必須在SMTP設定中指定金鑰。
2.1	10146680	當本機使用者瀏覽至**監控 → CyberTrace**區段時，即使 CyberTrace 整合已正確設定，仍發生 `bad token response` 錯誤。
2.1	10152245	KUMA 資源資料夾載入緩慢。
2.1	10159009	租用戶內容中未顯示包含警示和事件設定的區段。
2.1	10084426	輪詢 Active Directory 網域後，重新啟動卡巴斯基安全管理中心元件時，所有資訊都會重新發佈至 NATS，而不是僅傳送新增或修改的資料。
2.1	10091301	輪詢 Active Directory 網域後，卡巴斯基安全管理中心元件將 `tenant_id` 參數的錯誤值傳送至 NATS。

Kaspersky Next XDR Expert2.1.2中已修復問題清單

受影響的第一個版本	問題ID	問題描述
2.1	9987559	在**開啟遠端終端**部分的**「分析與回應」**分頁中，未顯示**資產（裝置）**按鈕。
2.1	9987778	在虛擬介面上安裝 Bootstrap 失敗，並出現 `ssh_verify_known_hosts failed` 錯誤，原因是 k0s 檔案傳輸期間發生 `MSCP` 錯誤。
2.1	9986780	由於事件時間戳記的時區不正確，事件時間線不完整。
2.1	9818418	當根租用戶設定的**憑證**部分中不存在任何憑證時，「憑證匯入」按鈕無法使用。
2.1	9952850	9952850：如果調查圖表包含舊版（2.0 版本之前）EDR 事件，則調查圖表顯示為空白（500 錯誤，“無法反序列化圖表”）。
2.1	9970495	如果檔案先前已透過**移動到隔離區**回應被隔離，則還原後檔案仍處於隔離狀態。
2.1	9973357	在建立或變更密碼時，密碼驗證僅允許使用 3 個必需類別的字元，而不是 4 個。
2.1	9989267	從**威脅搜尋**事件手動建立的警示錯誤地觸發了「**建立事件：相同主機資產**」和「連結到**現有事件：相同主機資產**」分段規則。
2.1	9989284	將警報與事件取消連結後，無法更改警報中的分析員。

2.1	9996452	如果在沙盒規則中指定了最小和最大檔案大小，**獲取檔案**和**檔案掃描**回應無法啟動。
2.1	9992321	警示中資產卡的「**連結至類別**按鈕無法使用。
2.1	10037395	事件卡中的「**在威脅狩獵中搜尋**」按鈕會傳回空事件清單。
2.1	10042351	取得進程記憶體轉儲」回應未能完成，並一直卡在「已啟動」狀態。**取得處理程序記憶體傾印已啟動**
2.1	10026313	根租用戶產品授權的活動裝置數錯誤地顯示為 0。
2.1	10055774	在時間線模式下，調查圖中未顯示垂直時間戳記。
2.1	9986186	XDR 從 2.0.1 升級至 2.1 時，在卡巴斯基安全管理中心安裝階段失敗（`invocation image launch is completed with an error`）。
2.1	9997088	XDR 從 2.0.1 升級至 2.1 時，在 irp-licensing-policy 遷移階段因 `create storage: check migrations: missing migration` 錯誤而失敗。

Kaspersky Next XDR Expert已修正問題清單

受影響的第一個版本	問題ID	問題描述
2.1	9940726	未收到觸發的關聯規則的統計資料。
2.1	9961307	新增Kaspersky Endpoint Detection and Response產品授權金鑰時，無法透過遠端終端連線到資產。
2.1	9995015	無法重新接受更新後的KSN聲明。
2.1	9935812	**目錄的完整路徑**回應操作的**執行 YARA 掃描**欄位不接受帶有遮罩的路徑。
2.1	9942685	無法從IOC規則產生的警示開啟IOC報告。
2.1	9942527, 9942530	在OSMP關聯器事件中，從`ThreatVerdictname`欄位導覽到Kaspersky Threats時，開啟了錯誤的URL。
2.1	9941545, 9941548	從事件、警示或事件中的`DeviceAdress`欄位導覽到Kaspersky Threat Intelligence Portal時，開啟了錯誤的URL。
2.1	9942427	從遙測事件中的雜湊值欄位導航到VirusTotal服務時，開啟了錯誤的URL。
2.1	9951714	由於預設時間篩選器設定錯誤，並非所有與事件相關的事件都顯示在**威脅搜尋**部分。
2.1	9959926	AMSI掃描事件中的`AmsiContentData`欄位顯示不正確，且不支援右鍵功能表操作。
2.1	9960056	在具有EDR模組的產品授權下，在**更新設定**區段中變更更新來源未儲存。
2.1	9964882	從報告編輯視圖傳回報告範本清單無法運作，導致頁面空白。
2.1	9967180	點選**監控政策**頁籤上的**顯示**（**來源**欄位）後，頁面顯示為空白。
2.1	9959327	資源2.0值出現在資源與服務**資源和服務資源類型**篩選下拉式功能表中。

Kaspersky Next XDR Expert 2.1中已修復問題清單

受影響的第一個版本	問題ID	問題描述
2.0	9662328	刷新警示或事件詳細資料後，可觀察物件的擴充結果會被清除。
2.0	9714816	同一IOA規則產生的警示未彙總完整的24小時週期。
2.0	9652409 9636329	在新增從屬管理伺服器到管理群組後，裝置未顯示在管理群組層次結構的**受管理裝置**下。
2.0	9696104	匯出和匯入IOA排除項時，引號未轉義，導致SQL剖析器發生錯誤，並使某些排除項無法在KES政策中正常運作。

2.0	9544457	**威脅搜尋**區段中使用的預設設定不適用於EDR事件。
2.0	9757637	無法匯卡巴斯基安全管理中心資產。
2.0	9702974	將主控台語言切換為中文後， **Detection and Response**頁籤（ **資產管理→資產（裝置）→Detection and Response** ）的內容仍顯示為英文。
2.0	9708837 9474866	在單一節點部署期間，內部DBMS帳戶密碼中的特殊字元導致無法安裝 OSMP掃描程式和設定沙盒。
2.0	9577657	無法使用組態檔自訂代理伺服器和更新程式。
2.0	9499714	由於記憶體使用過多， **事件**區段無法打開，並顯示 取得事件類型清單失敗 錯誤。
2.0	9660585	將OSMP主控台語言切換為簡體中文後， Kaspersky Managed Detection and Response外掛程式的本地化未正確套用。
1.4	8773796	在某些情況下，調查圖表上的**撤銷**和**重做**按鈕無法正常運作。
1.3	8452910	如果將Kaspersky Next XDR Expert從1.2版本升級到1.3版本時，某些元件的設定步驟是自動執行而不是手動執行，則可能會導致資源溢位和Kaspersky Next XDR Expert運作異常。
1.2	7323982	在支援版本管理的物件內容視窗中， **網頁主控台 IP 位址**區段的**變更歷史**欄位顯示了錯誤的IP位址。

關於Kaspersky Next XDR Expert

Kaspersky Next XDR Expert（XDR）是一款強大的網路安全解決方案，可保護您的企業IT基礎設施免受複雜的網路威脅，包括安裝在企業資產上的EPP應用程式無法偵測到的威脅。它提供了完整的可見性、關聯和自動化；並利用各種回應工具和資料來源，包括端點資產以及網路和雲端資料。為了有效地保護您的IT基礎設施，Kaspersky Next XDR Expert分析來自這些來源的資料，以識別威脅，為潛在事件建立警示，並提供應對這些事件的工具。Kaspersky XDR擁有先進的分析功能和豐富的安全專業知識。

該解決方案透過整合元件和單一介面中的整體情境提供統一的偵測和回應流程，從而提高安全專業人員的效率。Kaspersky Next XDR Expert的所有元件都部署在名為Open Single Management Platform的單一平台上。

偵測工具包括：

- 威脅搜尋工具，用於透過分析事件主動搜尋威脅和漏洞。
- 進階威脅偵測和相互關聯：來自不同來源的事件的即時關聯，使用MITRE ATT&CK矩陣對應為不同情境提供350多個開箱即用關聯規則，能夠建立新規則和自訂現有規則，以及用於偵測零日弱點的回顧性掃描。
- 調查圖表，用於可視化和促進事件調查並確定警示的根本原因。
- Kaspersky Threat Intelligence Portal的使用 取得最新的詳細威脅情報，例如網址、網域名稱、IP 位址、檔案雜湊值、統計和行為資料以及WHOIS和DNS資料。

回應工具包括：

- 手動回應操作：資產隔離、執行命令、新增和刪除阻止規則、在資產上啟動任務、Kaspersky Threat Intelligence Portal信譽擴充以及對使用者的培訓指派。
- 預先定義和使用者建立的常規程式，用於自動執行典型的回應操作。
- 協力廠商應用程式回應操作和跨應用程式回應情境。

Kaspersky Next XDR Expert包含端點威脅偵測和回應功能（來自Kaspersky Endpoint Detection and Response）：

- 整個企業基礎設施中端點的全面檢視。
- 基於入侵指標（IOC）、YARA規則和唯一攻擊指標（IOA）來檢測威脅。
- 保護郵件伺服器以及傳入和傳出電子郵件訊息，防範有害物件、垃圾郵件和網路釣魚。
- 沙盒用於安全分析可疑檔案和程式，提供有關隔離環境中物件行為的資訊。

Kaspersky Next XDR Expert也利用Open Single Management Platform元件進行資產管理以及集中運作安全管理和維護工作：

- 在公司網路中的資產上部署卡巴斯基應用程式。
- 遠端執行掃描和更新工作；
- 獲取有關資產防護的詳細資訊。
- 使用卡巴斯基應用程式配置所有安全元件。

Kaspersky Next XDR Expert支援租用戶層次結構。

Kaspersky Next XDR Expert與Active Directory整合，包括API，並支援與Kaspersky應用程式和協力廠商解決方案的廣泛整合，用於資料獲取和回應。有關Kaspersky Next XDR Expert支援的應用程式和解決方案的信息，請參閱相容的卡巴斯基應用程式和與其他解決方案的整合部分。

Kaspersky Next XDR Expert元件

	Open Single Management Platform		Kaspersky Industrial CyberSecurity for Networks
	Kaspersky Anti Targeted Attack Platform		Kaspersky Industrial CyberSecurity for Nodes
	Kaspersky Security for Linux Mail Server		Kaspersky CyberTrace
	Kaspersky Endpoint Security for Business		Kaspersky Automated Security Awareness Platform
	Kaspersky Hybrid Cloud Security		

在美國使用的軟體將無法提供更新功能（包括防毒軟體簽章更新和程式碼庫更新）和 KSN 功能。

硬體和軟體需求

本文說明單節點部署方案和多節點部署方案的硬體需求、Kaspersky Next XDR Expert 的軟體需求，以及 Kaspersky Deployment Toolkit 和 Open Single Management Platform 元件的硬體及軟體需求。

由於Kaspersky Next XDR Expert及其元件需要快速資料傳輸，我們強烈建議您使用直接連線儲存體。首選以下儲存體介面：SAS v3.5及更高版本，SATA Express。

單節點部署：硬體需求

單節點部署需要較少的資源（請參閱下表），但應考慮以下因素:

- 單節點方案僅支援網路中多達10,000台裝置。
- 資料庫位於叢集外的主要工作節點上。

  在單節點部署的情況下，強烈建議您先在將充當主要節點的主機上手動安裝DBMS。之後，您可以在同一台主機上部署Kaspersky Next XDR Expert。

- 為了正確部署解決方案，請確保目標主機的CPU支援BMI、AVX和SSE 4.2指令集。

最小硬體條件

單節點部署方案的硬體需求

解決方案	250台裝置	1,000台裝置	3,000台裝置	5,000台裝置	10,000台裝置
包含以下應用程式的解決方案： • Open Single Management Platform • Kaspersky Unified Monitoring and Analysis Platform • 沙盒	1個XDR主要工作節點： • CPU：10核心，運作頻率：2.5GHz。 • RAM：44 GB • 可用固態硬碟空間： • 主要磁碟子系統：400GB • 從屬磁碟子系統：500GB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。	1個XDR主要工作節點： • CPU：16核心，運作頻率：2.5GHz。 • RAM：48 GB • 可用固態硬碟空間： • 主要磁碟子系統：400GB • 從屬磁碟子系統：600GB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。	1個XDR主要工作節點： • CPU：22核心，運作頻率：2.5GHz。 • RAM：54 GB • 可用固態硬碟空間： • 主要磁碟子系統：600GB • 從屬磁碟子系統：1TB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。	1個XDR主要工作節點： • CPU：32核心，運作頻率：2.5GHz。 • RAM：62 GB • 可用固態硬碟空間： • 主要磁碟子系統：800GB • 次要磁碟子系統：1.4 TB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。	1個XDR主要工作節點： • CPU：38核心，運作頻率：2.5GHz。 • RAM：74 GB • 可用固態硬碟空間： • 主要磁碟子系統：1.5TB • 從屬磁碟子系統：2.4TB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。

多節點部署：硬體需求

多節點部署需要更多資源（請參閱下表），對於此方案，需要考慮以下因素：

- 超過10,000台裝置的網路建議使用多節點叢集方案。
- 資料庫位於叢集外的單獨主機上。
- 為了正確部署解決方案，請確保目標主機的CPU支援BMI、AVX和SSE 4.2指令集。

最小硬體需求

多節點部署方案的硬體需求

解決方案	20,000台裝置	30,000台裝置	50,000台裝置
包含以下應用程式的解決方案： • Open Single Management Platform • Kaspersky Unified Monitoring and Analysis Platform • 沙盒	12個節點： • 1個XDR主要節點 • 3個XDR工作節點 • 1個XDR資料庫節點 • 1個KUMA收集器 • 1個KUMA關聯器 • 3個KUMA keeper • 2個KUMA儲存體	12個節點： • 1個XDR主要節點 • 3個XDR工作節點 • 1個XDR資料庫節點 • 1個KUMA收集器 • 1個KUMA關聯器 • 3個KUMA keeper • 2個KUMA儲存體	12個節點： • 1個XDR主要節點 • 3個XDR工作節點 • 1個XDR資料庫節點 • 1個KUMA收集器 • 1個KUMA關聯器 • 3個KUMA keeper • 2個KUMA儲存體
	1個XDR主要節點： • CPU：4核心 • RAM：8 GB • 可用固態硬碟空間：500GB 3個XDR工作線程節點： • CPU：+10核心。 • RAM：20 GB • 可用SSD磁碟空間：1 TB 1個XDR資料庫節點： • CPU：+10核心。 • RAM：22 GB • 可用SSD磁碟空間：1,6 TB 1個KUMA收集器節點： • CPU：+8核心。 • RAM：16 GB • 可用固態硬碟空間：500GB 1個KUMA關聯器節點： • CPU：+8核心。 • RAM：32 GB • 可用固態硬碟空間：500GB 3個KUMA keeper節點： • CPU：+6核心。 • RAM：12 GB • 可用固態硬碟空間：200GB 2個KUMA儲存體節點： • CPU：24核心 • RAM：64 GB • 可用SSD磁碟空間：4.7 TB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。 網路頻寬：每個節點10Gbps	1個XDR主要節點： • CPU：4核心 • RAM：8 GB • 可用固態硬碟空間：500GB 3個XDR工作線程節點： • CPU：+12核心。 • RAM：24 GB • 可用SSD磁碟空間：1 TB 1個XDR資料庫節點： • CPU：+12核心。 • RAM：24 GB • 可用SSD磁碟空間：2,7 TB 1個KUMA收集器節點： • CPU：+8核心。 • RAM：16 GB • 可用固態硬碟空間：500GB 1個KUMA關聯器節點： • CPU：+8核心。 • RAM：32 GB • 可用固態硬碟空間：500GB 3個KUMA keeper節點： • CPU：+6核心。 • RAM：12 GB • 可用固態硬碟空間：200GB 2個KUMA儲存體節點： • CPU：24核心 • RAM：64 GB • 可用SSD磁碟空間：7 TB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。 網路頻寬：每個節點10Gbps	XDR主節點： • CPU：4核心 • RAM：8 GB • 可用固態硬碟空間：500GB 3個XDR工作線程節點： • CPU：+14核心。 • RAM：30 GB • 可用SSD磁碟空間：1 TB 1個XDR資料庫節點： • CPU：+16核心。 • RAM：32 GB • 可用SSD磁碟空間：4,3 TB 1個KUMA收集器節點： • CPU：+8核心。 • RAM：16 GB • 可用固態硬碟空間：500GB 1個KUMA關聯器節點： • CPU：+8核心。 • RAM：32 GB • 可用固態硬碟空間：500GB 3個KUMA keeper節點： • CPU：+6核心。 • RAM：12 GB • 可用固態硬碟空間：200GB 2個KUMA儲存體節點： • CPU：24核心 • RAM：64 GB • 可用SSD磁碟空間：12 TB 1個沙盒節點： • CPU：+32核心。 • RAM：80 GB • 磁碟子系統：2個硬碟，每個600GB，10,000RPM。 網路頻寬：每個節點10Gbps

Kaspersky Next XDR Expert：軟體需求

軟體需求以及支援的系統和平台

作業系統	支援以下64位元版本的作業系統： Ubuntu Server 24.04 LTS Ubuntu Server 26.04 LTS Astra Linux® Special Edition RUSB.10015-01（作業更新 1.8.5）
套件	Python® 3.8 或更新版本

<table>
<tr><td>虛擬化平台</td><td>Kaspersky Next XDR Expert 支援此處列出的所有虛擬化平台。然而，Kaspersky Next XDR Expert 元件有一些限制。差異如下表所示。
<table>
<tr><th>虛擬化平台名稱</th><th>Kaspersky Next XDR Expert</th><th>KUMA</th><th>沙盒</th></tr>
<tr><td>VMware ESXi 7.0.3</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Microsoft Hyper-V® Server 2022</td><td>✓</td><td>✓</td><td>—</td></tr>
<tr><td>基於核心的虛擬機（KVM）</td><td>✓</td><td>✓</td><td>—</td></tr>
<tr><td>Brest 3.3虛擬化軟體</td><td>✓</td><td>—</td><td>✓</td></tr>
<tr><td>RED Virtualization 7.3</td><td>✓</td><td>—</td><td>✓</td></tr>
<tr><td>Proxmox Virtual Environment 9.1、9.2</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Nutanix 7.5</td><td>✓</td><td>✓</td><td>—</td></tr>
<tr><td>zVirt Node 4.5</td><td>✓</td><td>—</td><td>✓</td></tr>
</table></td></tr>
<tr><td>資料庫管理系統（DBMS）</td><td>PostgreSQL 17.9 64位元
PostgreSQL 18.4 64位元
Postgres Pro 18 Enterprise 64 位元（叢集內建高可用）
所有列出的PostgreSQL版本都支援Corosync/Pacemaker</td></tr>
<tr><td>叢集節點（控制器和工作線程）上的檔案系統</td><td>ext4
XFS</td></tr>
</table>

Kaspersky Next XDR Expert元件

若要檢視 Kaspersky Next XDR Expert 元件的硬體和軟體需求，請按一下其名稱：

- OSMP主控台
- Kaspersky Unified Monitoring and Analysis Platform（以下簡稱KUMA）
- 從屬卡巴斯基安全管理中心管理伺服器
- 卡巴斯基安全管理中心網路代理
- Kaspersky Endpoint Security for Windows
- Kaspersky Anti Targeted Attack Platform (以下簡稱KATA)
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky CyberTrace
- Kaspersky Threat Intelligence Portal
- Kaspersky Automated Security Awareness Platform (以下簡稱KASAP)

Kaspersky Deployment Toolkit

所有 Kaspersky Next XDR Expert 元件均使用 Kaspersky Deployment Toolkit 公用程式（以下簡稱 KDT）安裝。

KDT的硬體和軟體需求如下：

規格	系統需求
硬體	CPU：4 核心，作業頻率 2.5 GHz RAM：8 GB 可用磁碟空間：至少100GB，包括： • Docker資料儲存目錄（預設：`/var/lib/docker`）：至少60GB • KDT的臨時檔案目錄（預設：`/tmp`）：至少15GB
系統	支援以下64位元版本的作業系統： • Astra Linux特別版 RUSB.10015-01（操作更新 1.8.5） • Ubuntu Server 24.04 LTS • Ubuntu Server 26.04 LTS

具有KUMA服務的主機需求

KUMA服務（收集器、關聯器和儲存體）可以安裝在Kubernetes叢集外部的專用主機上，也可以作為Kaspersky Next XDR Expert部署的一部分，以工作負載形式安裝在Kubernetes®叢集內部。

當KUMA服務部署在Kubernetes叢集外部時，本文定義的硬體、軟體和安裝需求可直接套用至安裝這些服務的主機。

當KUMA服務部署在Kubernetes叢集內部時，它們會在Kubernetes工作線程節點上執行，並根據本文中定義的KUMA硬體、軟體和安裝需求耗用叢集資源。在這種情況下，Kubernetes工作節點必須提供足夠的容量來滿足這些需求。

一般應用程式安裝需求

您可以在以下作業系統上安裝該應用程式：

- Oracle Linux
- Astra Linux
- Ubuntu

  支援的作業系統版本列於「硬體和軟體需求」部分。

  支援的組態有伺服器版和支援GUI的伺服器版。在支援GUI的伺服器組態中，您無需安裝額外的報告軟體套件。

在部署應用程式之前，請確保滿足以下條件：

- 您要安裝元件的伺服器符合硬體和軟體需求。
- 已安裝的 KUMA 實例所使用的連接埠可用。
- KUMA元件使用主機的完全限定網域名稱（FQDN）進行定址，格式為hostname.example.com。在安裝應用程式之前，請確保在執行以下命令時返回正確的主機FQDN：

  ```
  hostname -f
  ```

- 執行安裝程式的伺服器名稱不是 `localhost` 或 `localhost.<` 網域 `>`。

- 您要安裝KUMA Core的伺服器名稱不以數字開頭。
- 在所有具有KUMA服務的伺服器上設定了網路時間協定（NTP）的時間同步。

安裝 Sigma 規則轉換器的需求

此轉換器支援下列作業系統：

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

建議的硬體和軟體需求

本部分列出了處理高達40,000個每秒事件數（EPS）的資料流的硬體和軟體要求。KUMA負載值取決於正在解析的事件類型和標準化器的效率。

對於事件處理效率而言，CPU核心數量比時脈頻率更重要。例如，在處理事件時，8個中等時脈頻率的CPU核心比4個高時脈頻率的CPU核心更有效率。下表列出了KUMA元件的硬體和軟體需求。

收集器使用的RAM量取決於設定的擴充方法（DNS、RAM、資產、使用Kaspersky CyberTrace資料進行擴充）以及是否使用彙總。RAM消耗受資料彙總視窗設定、用於彙總資料的欄位數量以及被彙總欄位中的資料量的影響。

例如，在事件流為1000 EPS且停用事件擴充功能（停用事件擴充功能和停用事件彙總功能、5000個帳戶和每個租用戶5000個資產）的情況下，一個收集器需要以下資源：

- 1個CPU核心或1個虛擬CPU
- 512MB RAM
- 1GB磁碟空間（不包括事件快取)

例如，要支援5個不執行事件擴充的收集器，您必須分配以下資源：5個CPU核心、2.5GB RAM和5GB可用磁碟空間。

	收集器	關聯器	儲存庫
CPU	支援SSE 4.2的Intel或AMD™： 至少4核心/8執行緒或8個虛擬CPU。	支援SSE 4.2的Intel或AMD： 至少4核心/8執行緒或8個虛擬CPU。	支援SSE 4.2的Intel或AMD： 至少12核心/24執行緒或24個虛擬CPU。
RAM	16 GB	16 GB	48 GB
剩餘磁碟空間	/opt目錄大小：至少500 GB。	/opt目錄大小：至少500 GB。	/opt目錄大小：至少500 GB。
作業系統	• Ubuntu Server 24.04 LTS • Oracle Linux 8.6, 8.7, 9.2, 9.4. • Astra Linux特別版RUSB.10015-01（操作更新1.8.2）		
網路頻寬	100 Mbps	100 Mbps	如果資料流超過20,000個EPS， ClickHouse節點之間的傳輸速率必須至少為10Gbps。

以下虛擬環境支援安裝KUMA：

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

卡巴斯基對儲存體伺服器的建議

對於儲存體伺服器，卡巴斯基專家建議如下：

- 將ClickHouse放在固態硬碟（SSD）上。SSD有助於提高資料存取速度。硬碟可用於透過HDFS技術儲存資料。
- 若要將資料儲存系統連線到儲存體伺服器，請使用高速協議，例如光纖通道或iSCSI 10G。我們不建議使用NFS和SMB等應用程式級協定來連線資料儲存系統。
- 在ClickHouse叢集伺服器上使用ext4檔案系統。
- 如果您使用RAID陣列，請使用RAID 0以獲得高效能，或使用RAID 10以獲得高效能和容錯能力。
- 為確保資料儲存子系統的容錯能力與效能，請確保ClickHouse節點嚴格部署在不同的磁碟陣列上。
- 如果您使用虛擬化基礎設施來託管系統元件，請在不同的虛擬機器管理程式上部署ClickHouse叢集節點。在這種情況下，有必要防止兩個具有ClickHouse的虛擬機在同一個虛擬機管理程式上運作。
- 對於高負載KUMA安裝，請在實體伺服器上安裝ClickHouse 。

代理裝置需求

要將資料傳送到KUMA收集器，必須在網路基礎設施裝置上安裝代理程式。下表列出了硬體和軟體需求。

安裝代理程式的建議硬體和軟體需求

	Windows裝置	Linux裝置
CPU	單核，1.4GHz或更高	單核，1.4GHz或更高
RAM	512 MB	512 MB
剩餘磁碟空間	1 GB	1 GB
作業系統	• Microsoft Windows® 2012 • Microsoft Windows Server® 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows 10 20H2, 21H1	• Astra Linux特別版RUSB.10015-01（2023-0426SE17更新1.7.4） • Ubuntu 22.04 LTS (Jammy Jellyfish) • Debian 11.7 (Bullseye)

Oracle Linux、Astra Linux、Ubuntu 22.04 LTS作業系統的安裝需求

	Oracle Linux	Astra Linux	Ubuntu 22.04 LTS
Python版本	從3.6到3.11。不支援3.12及更高版本。	從3.6到3.11。不支援3.12及更高版本。	從3.6到3.11。不支援3.12及更高版本。
SELinux模組	已停用	已停用	已停用

	Oracle Linux	Astra Linux	Ubuntu 22.04 LTS
套件管理器	pip3	pip3	pip3

基本套件	• netaddr
	• firewalld
	• compat-openssl11
	您需要在KUMA Core將部署在叢集外部的Oracle Linux 9主機上安裝此軟體套件。
	關於從Oracle Linux 8.x升級到Oracle Linux 9.x的更多資訊。
	若要安裝這些軟體套件，請執行以下命令：
	`pip3 install netaddr`
	`yum install firewalld`
	`yum install compat-openssl11`
		• python3-apt
		• curl
		• libcurl4
		若要安裝軟體套件，請執行以下命令：
		`apt install python3-apt curl libcurl4`
			• python3-apt
			• curl
			• libcurl4
			• openssl 1.1.1
			• acl
			若要安裝軟體套件，請執行以下命令：
			`apt install python3-apt curl libcurl4 acl`
			您可以從Ubuntu官方網站下載openssl1.1.1套件，並使用以下命令進行安裝：
			`dpkg -i libssl1.1_1.1.1f-1ubuntu2_amd64.deb`

依賴套件	沒有值。	• netaddr • python3-cffi-backend 若要安裝軟體套件，請執行以下命令： `apt install python3-netaddr python3-cffi-backend` 如果您打算從KUMA查詢Oracle DB資料庫，您必須安裝Astra Linux libio1軟體套件。	• netaddr • python3-cffi-backend 若要安裝軟體套件，請執行以下命令： `apt install python3-netaddr python3-cffi-backend`
為了正確產生和下載報告，必須在安裝了KUMA Core的裝置上安裝以下軟體套件。	• nss • gtk2 • atk • libnss3.so • libatk-1.0.so.0 • libxkbcommon • libdrm • at-spi2-atk • mesa-libgbm • alsa-lib • cups-libs • libXcomposite • libXdamage • libXrandr 若要安裝軟體套件，請執行以下命令： `yum install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr`	• libgtk2.0.0 • libnss3 • libatk-adapter • libdrm-common • libgbm1 • libxkbcommon0 • libasound2 若要安裝軟體套件，請執行以下命令： `apt install libgtk2.0.0 libnss3 libatk-adaptor libdrm-common libgbm1 libxkbcommon0 libasound2`	• libatk1.0-0 • libgtk2.0-0 • libatk-bridge2.0-0 • libcups2 • libxcomposite-dev • libxdamage1 • libxrandr2 • libgbm-dev • libxkbcommon-x11-0 • libpangocairo-1.0-0 • libasound2 若要安裝軟體套件，請執行以下命令： `apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2 libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2`
安裝應用程式所需的使用者權限	沒有值。	您需要為將要安裝該應用程式的使用者指派必要的權限： `sudo pdpl-user -i 63 <` 將要安裝該應用程式的使用者 `>`	沒有值。

OSMP主控台需求

OSMP主控台伺服器

有關硬體和軟體需求，請參閱工作節點的需求。

用戶端裝置

對於用戶端裝置，OSMP主控台的使用僅需要一個瀏覽器。

最小螢幕解析度為1366x768像素。

裝置的硬體和軟體需求與用於存取OSMP主控台的瀏覽器需求相同。

瀏覽器：

- Google Chrome™ 149.0.7827.115 或更新版本（正式版本）
- Microsoft Edge® 149.0.4022.62 或更新版本
- macOS Safari 18.6（20621.3.11.11.3版本）
- Yandex Browser 26.4.4.799 或更高版本
- Mozilla Firefox™ 延伸支援版本 140.11.0 或更新版本

網路代理要求

最小硬體條件：

- 執行頻率為 1 GHz 或更高的 CPU。64 位元作業系統，CPU 最低頻率 1.4 GHz。
- RAM：512MB。
- 可用磁碟空間：1 GB。

針對基於 Linux 的裝置的軟體要求：必須安裝 Perl 語言解譯器 5.10 或更高版本。

網路代理。支援的平台

作業系統。Microsoft Windows® 工作站	Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32 位元 Microsoft Windows Embedded 7 Standard (Service Pack 1) 32 位元/64 位元 Microsoft Windows Embedded 8.1 Industry Pro 32 位元/64 位元 Microsoft Windows 10 Enterprise 2015 LTSB 32 位元 /64 位元 Microsoft Windows 10 Enterprise 2016 LTSB 32 位元 /64 位元 Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 位元 /64 位元 Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 位元 /64 位元 Microsoft Windows 10 Enterprise 2019 LTSC 32 位元 /64 位元 Microsoft Windows 10 IoT 企業版 1703、1709、1803、1809 32 位元/64 位元 Microsoft Windows 10 20H2、21H2 IoT 企業版 32 位元/64 位元 Microsoft Windows 10 IoT 企業版 32 位元/64 位元 Microsoft Windows 10 IoT 企業版 1909 32 位元 / 64 位元 Microsoft Windows 10 IoT 企業版 LTSC 2021 32 位元/64 位元 Microsoft Windows 10 IoT 企業版 1607 32 位元 / 64 位元 Microsoft Windows 10 TH1（2015 年 7 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 TH2（2015 年 11 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS1（2016 年 8 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS2（2017 年 4 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS3（秋季創作者更新，v1709）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS4（2018 年 4 月更新，17134）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS5（2018 年 10 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS6（2019 年 5 月）家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 10 19H1、19H2 家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 20H1（2020 年 5 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 20H2（2020 年 10 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 21H1（2021 年 5 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 21H2（2021 年 10 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 22H2（2023 年 10 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 11 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 IoT企業版25H2 64位元 Microsoft Windows 11 22H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 23H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 24H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 25H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 8.1 專業版/企業版 32 位元/64 位元 Microsoft Windows 8 專業版/企業版 32 位元/64 位元 Microsoft Windows 7 專業版/企業版/旗艦版/家用基本版/進階版（Service Pack 1 和更高版本）32 位元/64 位元 Microsoft Windows XP Professional（Service Pack 2）32 位元/64 位元（僅受網路代理版本 10.5.1781 支援） Microsoft Windows XP Professional Service Pack 3及更高的32位元版本（受網路代理版本14.0.0.20023支援，需要Windows XP的安全更新KB2868626） 適用於嵌入式系統的 Microsoft Windows XP Professional Service Pack 3 32 位元（受網路代理版本 14.0.0.20023 支援）

作業系統。Microsoft Windows 伺服器	Microsoft Windows MultiPoint® Server 2011 標準版/進階版 64 位元 Microsoft Windows Server® 2003 SP1 32 位元/64 位元（僅受網路代理版本 10.5.1781 支援，您可透過技術支援申請此版本） Microsoft Windows Server 2003 SP2 標準版/企業版 32 位元/64 位元（僅受網路代理版本 10.5.1781 支援） Microsoft Windows Server 2003 R2 標準版/企業版 SP2 32 位元/64 位元（僅受網路代理版本 10.5.1781 支援） Microsoft Windows Server 2008 Foundation (Service Pack 2) 32 位元/64 位元 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter (Service Pack 2) 32 位元/64 位元 Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Core Mode/Standard（Service Pack 1 和更高版本）64 位元 Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 位元 Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 位元 Microsoft Windows Server 2016 Datacenter/Standard/Server Core（安裝選項）(LTSB) 64 位元 Microsoft Windows Server 2019 Standard/Datacenter/Core 64 位元 Microsoft Windows Server 2019 RS5 Essentials/Standard 64 位元 Microsoft Windows Server 2022 Standard/Datacenter/Core 64 位元 Microsoft Windows Server 2025 Standard/Datacenter/Core 64 位元 Microsoft Windows Server 2022 21H2 Standard/Datacenter 64 位元 Microsoft Windows Storage Server 2019 64 位元 Microsoft Windows Small Business Server 2011 Standard 64 位元 Microsoft Windows Small Business Server 2011 Essentials 64 位元 Microsoft Windows Small Business Server 2011 Premium Add-on 64 位元

作業系統。Linux	Debian GNU/Linux 10.x (Buster) 32 位元 / 64 位元 Debian GNU/Linux 11.x (Bullseye) 32 位元/64 位元 Debian GNU/Linux 12 (Bookworm) 32 位元 / 64 位元 Debian GNU/Linux 13 (Trixie) 64位元 Ubuntu Server 10.04 LTS (Lucid Lynx) 32 位元/64 位元 Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位元 / 64 位元 Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位元 Ubuntu Server 20.04 LTS (Focal Fossa) 64 位元 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位元 Ubuntu Server 22.04 LTS ARM® 64 位元 Ubuntu Server 24.04 LTS (Noble Numbat) 64 位元 Ubuntu Server 26.04 LTS (Resolute Raccoon) 64 位元 Ubuntu Server 26.04 LTS ARM 64 位元 Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32 位元/64 位元 Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位元 / 64 位元 CentOS 5.2 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 5.4 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 6.4 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 6.6 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 7.2 及更高版本 64 位元 CentOS Stream 8 64 位元 CentOS Stream 9 64 位元 CentOS Stream 9 ARM 64 位元 CentOS Stream 10 64位元 Red Hat Enterprise Linux Server 6.x 32 位元/64 位元 Red Hat Enterprise Linux Server 7.2 和更高版本 64 位元 Red Hat Enterprise Linux Server 8.x 64 位元 Red Hat Enterprise Linux Server 9.x 64 位元 Red Hat Enterprise Linux Server 10.x 64位元 SUSE Linux Enterprise Server 12.5 和更高版本（所有服務套件）64 位元 SUSE Linux Enterprise Server 15（所有服務套件）64 位元 SUSE Linux Enterprise Server 15（所有服務套件）ARM 64 位元 openSUSE Leap 15 64 位元 EulerOS 2.0 SP10 64 位元 EulerOS 2.0 SP10 ARM 64 位元 Astra Linux Special Edition RUSB.10015-01（操作更新 1.4）32 位元 Astra Linux Special Edition RUSB.10015-01（操作更新 1.4）64 位元（僅受 Linux Legacy 版網路代理支援，您可以使用網頁主控台介面或從卡巴斯基網站下載此網路代理） Astra Linux 特別版 RUSB.10015-01（操作更新 1.5）64 位元 Astra Linux 特別版 RUSB.10015-01（操作更新 1.6）64 位元 Astra Linux 特別版 RUSB.10015-16（版本 1）（操作更新 1.6）64 位元 Astra Linux 特別版 RUSB.10015-17（操作更新 1.7.3）64 位元 Astra Linux 特別版 RUSB.10015-01（操作更新 1.7）64 位元 Astra Linux 特別版 RUSB.10015-01（操作更新 1.8）64 位元 Astra Linux 特別版 RUSB.10015-03（操作更新 7.6）64 位元 Astra Linux 特別版 RUSB.10015-37（操作更新 7.7）64 位元 Astra Linux 特別版 RUSB.10152-02（操作更新 4.7）ARM 64 位元 Astra Linux 通用版（操作更新 2.12）64 位元 ALT Workstation 11 64位元 ALT Server 11 64位元 ALT Education 11 64位元 ALT Workstation 10.1 64 位元 ALT Server 10.1 64 位元

ALT Education 10.1 64 位元
ALT SP Server 10 32 位元/64 位元
ALT SP Server 10 ARM 64 位元
ALT SP Workstation 10 32 位元/64 位元
ALT SP Workstation 10 ARM 64 位元
ALT 8 SP Server (LKNV.11100-01) 32 位元/64 位元
ALT 8 SP Server (LKNV.11100-02) 32 位元/64 位元
ALT 8 SP Server (LKNV.11100-03) 32 位元/64 位元
ALT 8 SP Workstation (LKNV.11100-01) 32 位元/64 位元
ALT 8 SP Workstation (LKNV.11100-02) 32 位元/64 位元
ALT 8 SP Workstation (LKNV.11100-03) 32 位元/64 位元
Oracle Linux 7 64 位元
Oracle Linux 8 64 位元
Oracle Linux 9 64 位元
Linux Mint 21.1 及更高版本 64 位元
Linux Mint 22.x 64 位元
AlterOS 7.5 及更高版本 64 位元
AlterOS 2025 64位元
GosLinux IC6/7.17 64 位元
GosLinux IC6/7.2 64 位元
SberOS 3.4.0 64位元
SberOS 3.5.0 64位元
SberOS 3.6.1 64 位元
Platform V SberLinux OS Server (SLO) 8.10.1 64 位元
Platform V SberLinux OS Server (SLO) 9.1 64 位元
Platform V SberLinux OS Server (SLO) 9.5.1 64 位元
Platform V SberLinux OS Server (SLO) 9.6 64 位元
Platform V SberLinux OS Server (SLO) 9.7 64 位元
RED OS 7.3 Server 64 位元
RED OS 7.3 Certified Edition 64 位元
RED OS 8 64 位元
RED OS 8 ARM 64 位元
ROSA Enterprise Linux Server 7.9 64 位元
ROSA Enterprise Linux Desktop 7.9 64 位元
ROSA COBALT 7.9 64 位元
ROSA CHROME 12 64 位元
AlmaLinux 8 及更高版本 64 位元
AlmaLinux 9 及更高版本 64 位元
Rocky Linux™ 8 及更高版本 64 位元
Rocky Linux 9 及更高版本 64 位元
Atlant · Alcyone build · 版本 2022.02 64 位元
MSVSPHERE 9.2 伺服器 64 位元
MSVSPHERE 9.2 ARM 64 位元
MSVSPHERE 9.4 伺服器 64 位元
MSVSPHERE 9.4 ARM 64 位元
SynthesisM 伺服器 8.6 64 位元
SynthesisM 用戶端 8.6 64 位元
OSnova 2.* 64 位元
OSnova 3.* 64位元
TeNIX WS 64 位元
Kylin 10 64 位元
EMIAS 1.0 64 位元
Amazon Linux 2 64 位元
MosOS 15.5 Arbat 64 位元
OS MES (Moscow Electronic School) 12（適用於電腦和膝上型電腦）64 位
OS MES (Moscow Electronic School) 12 Server （適用於互動平板電腦） 64 位元

	M OS (Moscow Electronic School) 12 Server 64 位元 Mostech 64 位元 Mostech Server 64 位元 Fedora® Linux Server 41 64 位元 Fedora Linux Workstation 41 64 位元
作業系統。macOS	有關受支援的作業系統清單，請參閱Kaspersky Endpoint Security for Mac 說明。 ™
虛擬化平台	如需支援的虛擬化平台相關資訊，請參閱Kaspersky Security for Virtualization Light Agent線上說明。

在早於Microsoft Windows Server 2008 R2（伺服器版本）和Microsoft Windows 7（桌面版）的Windows版本上，網路代理程式不支援下列功能：

- 更新重譯（發佈點使用）
- KSN代理程式（發佈點使用）
- 弱點掃描工作

在執行 Microsoft Windows 10 RS4 或 RS5 版本的裝置上，卡巴斯基安全管理中心可能無法在啟用了大小寫敏感的資料夾中偵測到一些弱點。

在執行 Windows 7、Windows Server 2008、Windows Server 2008 R2 或 Windows MultiPoint Server 2011 的裝置上安裝網路代理之前，請先確保已安裝適用於 Windows 作業系統的安全性更新 KB3063858（適用於 Windows 7 的安全性更新 (KB3063858)，適用於 x64 型系統的 Windows 7 安全性更新 (KB3063858)，適用於 Windows Server 2008 的安全性更新 (KB3063858)，適用於 Windows Server 2008 x64 版的安全性更新 (KB3063858)，適用於 Windows Server 2008 R2 x64 版的安全性更新 (KB3063858)。

在 Microsoft Windows XP，網路代理可能錯誤執行一些操作。

您只能在 Microsoft Windows XP 中安裝或更新適用於 Windows XP 的網路代理。支援的作業系統清單中列出了受支援的 Microsoft Windows XP 版本及其對應的網路代理版本。您可以從此頁面下載適用於 Microsoft Windows XP 的網路代理所需版本。

我們建議您安裝與Open Single Management Platform相同版本的Linux網路代理。

Open Single Management Platform完全支援相同或更新版本的網路代理。

適用於 macOS 的網路代理與適用於此作業系統的卡巴斯基安全應用程式一起提供。

虛擬化組態

在hypervisor主機上，必須停用BIOS/UEFI中的所有節能最佳化（C-States、P-States、Turbo-Boost和類似功能）。

如果hypervisor主機上的BIOS/UEFI支援CPU效能設定，則必須將其設定為最高效能。請參考硬體供應商文件以獲取詳情。

在hypervisor程式主機上，必須在BIOS/UEFI中啟用虛擬化支援（Intel VTx/VTd、 AMD-V/AMD-Vi等）。

必須啟用透明大頁（THP）。

I/O 排程器必須設定為「noop」。

我們建議您增加「max_io_threads」參數。

NUMA（非統一記憶體存取）

對於單通道或低記憶體的主機，應停用NUMA。

在多通道系統中，應啟用NUMA（建議在XDR建議規格的基礎上至少增加20%的額外內存，以應對NUMA開銷）。

VMware組態

啟用「Reserve all guest memory」選項。

設定共用資源參數（例如CPU和記憶體份額）的最小值，以確保每個虛擬機器都能獲得專用資源。

將VMXNET3網路介面卡用於虛擬機器，以取得最佳網路效能。

Kernel 型虛擬機器、Proxmox、Nutanix、RED Virtualization、zVirt 節點組態

將hypervisor設定為host模式或host-passthrough模式。

儲存子系統應使用SCSI驅動程式，而不是區塊（blk）驅動程式。

不要使用共用資源，以確保分配專用資源。

HYPER-V組態

vCPU-to-pCore比率應設定為1:1。

請遵循文章中列出的建議：

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

常見需求與注意事項

如果使用虛擬化，則需要100%的vCPU分配。

對於超過40,000台裝置的網絡，請使用從屬管理伺服器。

確保 DNS 伺服器在網路上可用。

單節點部署無法升級到多節點部署。如果預期需要擴展基礎設施，則最好採用多節點安裝。

有效裝置和EPS運算

硬體需求可能會因端點裝置上執行的作業系統而異。使用下列公式估算網路中的有效裝置：

```
< 裝置數量 > = < Windows 端點 > + 3* < Linux 和 macOS 端點 > + 20 * < 伺服器 >
```

在預設設定下，有效裝置預計貢獻0.5EPS（每秒事件數）。總EPS使用以下公式計算：

```
< 總EPS > = < 有效裝置EPS > + < 協力廠商EPS >
```

您可以使用以下公式將總EPS轉換為有效裝置：

```
< 有效裝置總數 > = < 總EPS > *2
```

節點組態

如果BIOS/UEFI支援IOMMU（輸入輸出記憶體管理單元），則必須啟用它。

BIOS/UEFI中的所有節能最佳化都必須停用，例如C-States、P-States、Turbo-Boost。

如果BIOS/UEFI支援CPU效能設定，則必須對其進行最大效能配置。有關更多資訊，請參考硬體供應商提供的文件。

磁碟/儲存體需求

最低輸入/輸出效能：

- 對於單節點部署： 12,000 IOPS（循序讀取/寫入，8 KB 區塊大小）。
- 對於多節點部署： 8,000 IOPS（循序讀取/寫入，8 KB 區塊大小）。

RAID陣列的條帶大小必須至少為16KB。

SSD/NVMe驅動程式必須支援TRIM。

不建議丟棄掛載選項。相反，必須設定定期清理未使用的資料區塊以保持效能。

fsync延遲不得超過最佳值：

- 單節點部署與控制平面節點為2毫秒；
- EPS高於1000的運算節點為3毫秒；
- EPS低於1000的運算節點為10毫秒。

NUMA（非統一記憶體存取）

對於單通道或低記憶體的主機，應停用NUMA。

在多通道系統中，應啟用NUMA。我們建議您在XDR建議規格的基礎上至少增加20%的額外內存，以應對NUMA開銷。

Kaspersky Next XDR Expert元件

下表列出了Kaspersky Next XDR Expert包含的元件。

Kaspersky Next XDR Expert元件

元件名稱	描述
agentserver	此元件允許透過代理程式整合對資產執行回應操作。
asset-manager	此元件用於集中式資產管理。
backup-operator	此自動化工具透過自訂資源和標籤管理資料備份和復原。
bootstrap	基本的執行環境，包括Kaspersky Next XDR Expert功能的Kubernetes叢集和基礎設施元件。
cp	此通訊平台可實現系統元件間資料交換和互動。
openbao-csi-provider	透過容器儲存介面（CSI）實現叢集對外部儲存的存取的元件。
database-cluster	一組資料庫伺服器，協同工作以實現高可用性和可擴充性。
database-operator	CloudNativePG Kubernetes控制器，用於管理內部資料庫連線設定、資料庫資源、密鑰和憑證輪替。
gateway	Kubernetes叢集閘道。
hierman	此元件管理層級操作。
iam	此OSMP平台元件提供身分驗證和授權。
irp	此元件用於自動處理警示和事件並執行回應操作。
istio	此服務網格用於管理Kubernetes叢集中服務通訊。
keswin_web_plugin_xdr	此 Web 外掛程式用於在 Kaspersky Next XDR Expert 中管理 Kaspersky Endpoint Security for Windows，支援安全性政策配置、事件監控和平台元件整合。
ksb-facade	此元件使用mixin和部署模板執行操作。
ksc	卡巴斯基安全管理中心管理伺服器
ksn-proxy-facade	此元件透過Porter、外部KSN服務整合和統計處理管理KSN代理部署。
kuma-migrator	此元件可自動在KUMA版本之間遷移設定、資料和設定。

元件名稱	描述
loadbalancer	此元件將請求路由到叢集中的容器或進程，並提供跨節點的稽核、身分驗證和會話同步。
nsqlookupd	此服務可發現NSQ產生者並引導叢集內用戶端。
nwc	OSMP主控台。
objectstorage	此元件用於儲存臨時常規程式資料、警示和事件檔案，並支援S3 API以進行外部整合。
observability	此元件提供對事件、威脅和資產的集中式可見性，並透過與KUMA平台整合來支援回應自動化。
orchestra	自動化平台。此通用元件用於協調工作流程和執行常規程式，以支援自動事件回應和簡化安全操作。
osmp-ksn-proxy	此元件透過KSN代理API和路由資料將偵測和警示統計資料傳輸到KSN或KPSN。
osmp-scanner	此元件使用反惡意軟體、YARA和沙盒掃描檔案、傳送檔案進行分析並產生報告。
plugin-admin-agent	此元件管理網路代理策略。
plugin-admin-server	此元件管理管理伺服器。
plugin-agent-server	此元件管理Kaspersky Endpoint Detection and Response的各項功能。
plugin-asset-management	此元件管理資產，包括裝置、使用者和其他資源。
plugin-enterprise	該元件與其他卡巴斯基解決方案集成，並透過網頁介面和API提供資產管理、監控、回應管理自動化和多租用戶支援。
plugin-kata	該元件與KATA/EDR集成，以執行回應操作、擴充事件資料，並提供高可用性和可擴充性支援。
plugin-kuma	此元件將 KUMA 功能整合到 Kaspersky Next XDR Expert 中。
plugin-osmp-scanner	該元件提供掃描互動，與反惡意軟體、YARA和沙盒整合，將結果傳送到ObjectStorage、Proxy和Disaster Recovery，並支援自動和手動回應操作。
plugin-public-api-token-settings	此元件透過公共 API 管理 API 權杖設定，以支援 Kaspersky Next XDR Expert 元件和外部系統的身分驗證和授權。
plugin-tenant-roles	此元件管理租用戶內使用者和群組角色指派，並與IAM整合，以實現角色模型和支援多租用戶。
spp_web_plugin_xdr	此元件與卡巴斯基單一產品外掛程式整合，透過OSMP主控台管理其他卡巴斯基產品。
secrets-manager	此元件用於管理金鑰，確保其在服務部署和設定期間的安全儲存和正確使用。
tenant-registry	此元件用於管理租用戶生命週期、身分資料，並與卡巴斯基安全管理中心伺服器和外部系統整合。
plugin-kessw	此元件用於在Kaspersky Next XDR Expert中管理Kaspersky Embedded Systems Security for Windows（KESS）。
plugin-kes-linux	管理Kaspersky Endpoint Security for Linux的元件。
plugin-kesw	管理Kaspersky Endpoint Security forWindows的元件。
plugin-spp	卡巴斯基單一產品外掛程式，用於透過OSMP主控台管理其他卡巴斯基產品。

相容的卡巴斯基應用程式和解決方案

本文列出了應用程式已在其上測試並保證可正常運作的軟體版本。該應用程式也可能相容於其他軟體版本，但這些配置尚未經過完整的測試流程，因此未包含在保證支援的版本清單中。

Kaspersky Next XDR Expert可與以下版本的應用程式和解決方案整合：

- 卡巴斯基安全管理中心 Linux 16.3（作為從屬管理伺服器）
- Kaspersky Security Center Windows 15.1或更高版本（作為從屬管理伺服器）

- Kaspersky Anti Targeted Attack Platform 7.1

  強烈建議過渡至 Open Single Management Platform (OSMP) 架構。在此架構中，Kaspersky Endpoint Security 應用程式會直接連線至 OSMP，無須透過中央節點伺服器。
  如果尚未在所有受管理裝置上將安全應用程式升級至新版本，則在升級完成之前，威脅回應仍會透過與 Kaspersky Anti Targeted Attack Platform (KATA) 的整合進行管理。這表示事件回應平台會向 KATA 傳送要求，接著 KATA 會向安全應用程式傳送要求。
  只有在因故無法過渡至 OSMP 架構的例外情況下，才允許使用此方案。

- Kaspersky Endpoint Security for Windows 14.0、14.1（支援檔案伺服器）
- Kaspersky Endpoint Security for Linux 12.4、12.5
- Kaspersky Endpoint Security for Mac 12.2.1、12.2.1 修補程式 A
- Kaspersky CyberTrace 5.0（只能在KUMA主控台中設定)
- Kaspersky Industrial CyberSecurity for Nodes 5.0
- Kaspersky Industrial CyberSecurity for Networks 4.0（只能在KUMA主控台中設定）
- Kaspersky Secure Mail Gateway 2.0或更高版本（整合只能在KUMA主控台中設定）
- Kaspersky Security for Linux Mail Server 10或更高版本（整合只能在KUMA主控台中設定）
- Kaspersky Web Traffic Security 6.0或更高版本（整合只能在KUMA主控台中設定）
- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal
- Kaspersky NGFW 1.2
- Kaspersky Managed Detection and Response
- Kaspersky SIEM 4.2、4.6
- Kaspersky Security for Virtualization Light Agent 6.3.1、6.4

  Kaspersky Security for Virtualization Light Agent 支援 Kaspersky Next XDR Expert，但有一些限制。Web 外掛程式、安全虛擬機器 (SVM) 和整合伺服器只能從作為從屬管理伺服器的卡巴斯基安全管理中心進行管理。

如需支援的應用程式版本的最新資訊，請參閱 應用程式支援生命週期網頁。

已知問題與限制

Kaspersky Next XDR Expert 支援管理 Kaspersky Endpoint Security for Windows，但有以下限制：

- 自適應異常控制元件不受支援。Kaspersky Next XDR Expert 不支援自適應異常控制規則。
- Kaspersky Sandbox元件不受支援。

基本概念

本節說明與 Kaspersky Next XDR Expert 相關的基本概念。

管理伺服器

Kaspersky Next XDR Expert 元件可對安裝在用戶端裝置上的 Kaspersky 應用程式進行遠端管理。

安裝了管理伺服器元件的裝置將被稱作*管理伺服器*（也稱作*伺服器*）。管理伺服器必須被防護，包括實體防護，以防範非授權的存取。

管理伺服器在安裝的裝置上為系統服務，且擁有以下內容：

- 名稱為 `kladminserver_srv`
- 設定隨作業系統啟動而自動啟動
- 具有 `ksc` 帳戶或在安裝管理伺服器過程中所選取的使用者帳戶

有關安裝設定的完整清單，請參閱以下文章：安裝Open Single Management Platform。

管理伺服器會執行下列功能：

- 儲存管理群組結構
- 儲存關於用戶端裝置設定的資訊
- 應用程式分發套件的儲存結構
- 將應用程式遠端安裝至用戶端裝置和遠端移除應用程式
- 更新 Kaspersky 應用程式的程式資料庫和軟體模組
- 管理用戶端裝置上的政策和工作
- 儲存有關用戶端裝置上已發生事件的資訊
- 產生有關 Kaspersky 應用程式操作的報告

- 向用戶端裝置佈署授權金鑰並儲存授權金鑰資訊
- 有關工作處理程序的通知轉發（例如在用戶端裝置上偵測到病毒）

在應用程式介面命名管理伺服器

在OSMP主控台介面中，管理伺服器可以擁有以下名稱：

- 管理伺服器的裝置名稱，例如："*裝置名稱*"或"管理伺服器：*裝置名稱*"。
- 管理伺服器裝置的 IP 位址，例如："*IP 位址*"或"管理伺服器：*IP 位址*"。
- 從屬管理伺服器和虛擬管理伺服器具有在將虛擬或從屬管理伺服器連線到主管理伺服器時指定的自訂名稱。
- 如果您使用安裝在Linux裝置上的OSMP主控台，則該應用程式將顯示您在回應檔案中指定為受信任的管理伺服器名稱。

您可以使用OSMP主控台連線到管理伺服器。

管理伺服器階層

您可以按照階層架構排列管理伺服器。在該層次結構的不同階層等級上，每個管理伺服器都可以擁有多個次要管理伺服器（稱為*次要伺服器*）。根管理伺服器只能作為主要伺服器運行。次要伺服器的階層等級不受限制。主要管理伺服器的管理群組將會包括所有次要管理伺服器的用戶端裝置。因而，實體隔離的區域網路或不同網段，可使用不同台的管理伺服器進行管理，最後再由一台主要伺服器去管理其他管理伺服器。

在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。

*虛擬管理伺服器*是次要管理伺服器的一個特例。

要做到管理伺服器的樹狀結構，請做到以下幾點：

- 降低管理伺服器的負載（與為整個網路安裝單一的管理伺服器比較）。
- 安裝多台的好處還可以減少內網的流量以及簡化遠端辦公室的工作流量。您不必在主要管理伺服器和所有網路裝置（例如，它們可能位於不同地區）之間建立連線。只需在每個地區或網段中安裝次要管理伺服器，由次要伺服器管理各自的裝置，再由次要伺服器和主要伺服器之間建立專屬連線來同步資訊。
- 可由各地區或網段的管理員管理各自的從屬伺服器以分擔工作量。用於集中管理和監控用戶端防護安全狀態的所有功能仍然可正常使用。
- 服務提供商使用 Kaspersky Next XDR Expert。服務提供商只需安裝 Kaspersky Next XDR Expert 和 OSMP Console。為了管理各種組織的大量用戶端裝置，服務提供商向管理伺服器階級新增從屬管理伺服器（包括虛擬伺服器）。

管理群組階層架構中所包括的用戶端裝置都只能連線到一個管理伺服器。您必須獨立監控裝置到管理伺服器的連線。使用這些功能可以在不同伺服器的管理群組中搜尋裝置。

網頁伺服器

Kaspersky Next XDR Expert *網頁伺服器*（以下亦稱為 *網頁伺服器*）是 Kaspersky Next XDR Expert 的元件，會與管理伺服器一起安裝。「網頁伺服器」專用於透過網路傳輸獨立安裝套件。

當您建立獨立安裝套件時，它會自動發佈在網頁伺服器上。已建立獨立安裝套件清單中將會顯示獨立安裝套件的下載連結。必要時，您可以取消發佈獨立安裝套件或在網頁伺服器上重新發佈。您可以透過任何方便的方式將連結傳送給使用者，例如透過電子郵件。透過點擊連結，使用者可將安裝套件下載至本機裝置。

網路代理

管理伺服器與裝置之間的互動，是透過 Kaspersky Next XDR Expert 的 *網路代理*元件進行。所有使用 Kaspersky Next XDR Expert 管理 Kaspersky 應用程式的裝置都必須安裝網路代理。

安裝了網路代理的裝置被稱為*受管理裝置*或*裝置*。

Linux 網路代理作為系統服務安裝在裝置上，且具有以下內容：

- 名稱“卡巴斯基網路代理”
- 設定隨作業系統啟動而自動啟動
- 使用根帳戶

Windows 網路代理作為系統服務安裝在裝置上，且具有以下內容：

- 名稱“卡巴斯基安全管理中心網路代理”
- 設定隨作業系統啟動而自動啟動
- 使用 LocalSystem 帳戶

macOS的網路代理程式作為服務安裝在裝置上，且具有以下屬性：

- 名稱“com.kaspersky.klnagent.core”
- 設定隨作業系統啟動而自動啟動
- 使用根帳戶

服務處理程序的名稱：

- 對於 Linux：
  - klnagent64.service（對於 64 位元作業系統）
  - klnagent.service（對於 32 位元作業系統）

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

預設情況下，網路代理安裝在以下位置：

- 對於 Linux：
  - 32位元系統：/opt/kaspersky/klnagent/
  - 64 位元系統：/opt/kaspersky/klnagent64/
- 對於 Windows：
  - 32 位元系統：C:\Program Files\Kaspersky Lab\NetworkAgent
  - 64 位元系統：C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- 對於 macOS：
  - 64位元系統：/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

對於 Windows 裝置，您可以在安裝套件的設定中為網路代理的安裝指定不同的資料夾。但是對於 Linux 裝置，網路代理只能安裝在預設目錄中。

網路代理安裝資料夾還包含用於管理和診斷網路代理操作的公用程式，例如 klmover 和 klnagchk 公用程式。

安裝管理伺服器時，網路代理的伺服器版本會與管理伺服器一起自動安裝。儘管如此，若要像管理任何其他受管理裝置一樣管理管理伺服器裝置，請安裝 Network Agent for Linux在管理伺服器裝置上。在這種情況下，Linux 網路代理已安裝，並獨立於您與管理伺服器一起安裝的網路代理伺服器版本。

網路代理同步管理伺服器的受管理裝置。我們建議您設定同步間隔（也叫*心跳*）為每 10,000 台受管理裝置 15 分鐘。

管理群組

管理群組（以下亦稱為*群組*）是依據特定特徵組成的受管理裝置邏輯集合，目的是在 Kaspersky Next XDR Expert 中將群組內的裝置視為單一單位進行管理。

管理群組內的所有受管理裝置都被配置以做如下事情：

- 使用共同的應用程式設定（您可以在群組政策中指定）。
- 透過建立具有指定設定的群組工作，為所有應用程式使用共同的操作模式。群組工作的例子包括建立和安裝公用安裝套件、更新程式資料庫和模組、自訂掃描裝置和啟用即時防護。

受管理裝置只能屬於一個管理群組。

您可以建立管理伺服器和群組的層級。單個層次結構等級可以包括次要和虛擬管理伺服器、群組和受管理裝置。您可以從一個群組移動裝置到其他群組，而不做實體移動。例如，如果企業員工的職位從會計變更為開發者，您可以將該員工的裝置從會計管理群組移動到開發者管理群組。然後，該裝置將自動接收開發者所需的應用程式設定。

受管理裝置

*受管理裝置*是執行 Linux、Windows 或 macOS 並安裝了網路代理的裝置。您可以透過裝置上安裝的應用程式的工作和政策來管理此類裝置。您也可以從受管理裝置接收報告。

您可以讓受管理的裝置作為發佈點和連線閘道執行。

裝置僅可以被一個管理伺服器管理。一台管理伺服器能夠管理的裝置數量取決於託管管理伺服器的裝置的配置和DBMS限制。

未配置的裝置

*未配置的裝置*是網路中未被包含在任何管理群組中的裝置。您可以在未配置裝置上執行一些操作，例如，移動它們到管理群組或在其上安裝應用程式。

當在您的網路中發現新裝置時，該裝置轉到"**未指派的裝置**"管理群組。您可以設定規則以便裝置在被發現後被自動移動到其他管理群組。

管理員工作站

安裝了OSMP主控台伺服器的裝置被稱為*管理員工作站*。管理員可以使用這些裝置來遠端集中管理用戶端裝置上安裝的 Kaspersky 應用程式。

管理主控台的數量不受限制。在任何管理員的工作站電腦上，都可以同時管理網路中多台管理伺服器。您可以使用管理主控台連線至網路中任何層級（實體或虛擬）的管理伺服器。

您可以將管理員的工作站移動至管理群組節點中的用戶端裝置。

在任何管理伺服器的管理群組中，單一裝置可以當做用戶端裝置、管理伺服器或管理主控台。

管理 Web 外掛程式

透過OSMP主控台遠端管理卡巴斯基軟體時，需使用一種特殊元件，即*管理Web外掛程式*。以下，管理Web外掛程式又稱為*管理外掛程式*。管理外掛程式是一種讓OSMP主控台與特定卡巴斯基應用程式相互銜接的介面。使用管理外掛程式，您可以配置應用程式工作和政策。

管理外掛程式提供以下：

- 建立並編輯應用程式工作和設定的介面
- 建立和編輯政策和政策設定檔以便遠端和集中配置 Kaspersky 應用程式和裝置的介面

- 應用程式事件傳輸
- OSMP主控台中用於顯示應用程式的操作資料與事件以及用戶端裝置所提供統計資訊的功能

政策

*政策*是一組應用於管理群組及其子群組的卡巴斯基應用程式設定。您可以在管理群組的裝置上安裝多個 Kaspersky 應用程式。Kaspersky Next XDR Expert 為管理群組中的每個 Kaspersky 應用程式提供單一政策。政策會有下列其中一種狀態：

政策狀態

州	敘述
活動	套用至裝置的目前政策。每個管理群組中的 Kaspersky 應用程式只能啟用一個政策。裝置將為卡巴斯基應用程式套用活動政策的設定值。
不啟用	目前未將政策套用至裝置。
漫遊	如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

政策會根據以下規則執行：

- 您可以為單個應用程式配置擁有不同值的多個政策。
- 對於目前應用程式只有一個政策可以處於啟用狀態。
- 政策可以有子政策。

通常，您可以將政策作為緊急情況 (例如病毒攻擊) 的準備。例如，如果有透過快閃記憶體磁碟機的攻擊，則可以啟動阻止存取快閃記憶體磁碟機的政策。在這種情況下，目前的啟用政策將自動變為非啟用狀態。

為了防止維護多個政策，例如，當不同場合僅假設變更多個設定時，您可以使用政策設定檔。

*政策設定檔*是政策設定值的已命名子集，用於替換政策的設定值。政策設定檔會影響受管理裝置上有效的設定形式。*有效設定*是目前應用於裝置的一組政策設定，政策設定檔設定和本機應用程式設定。

政策設定檔會根據以下規則執行：

- 當特定的啟動條件發生時，政策設定檔會生效。
- 政策設定檔包含與政策設定不同的設定值。
- 政策設定檔的啟動會變更受管理裝置的有效設定。
- 政策可以包含最多 100 個設定檔。

政策設定檔

有時候有必要為不同的管理群組建立單一政策的若干實例；您也可能想要集中修改這些政策的設定。這些實例實例可能僅有一兩處設定不同。例如，企業中所有的會計工作在相同政策下 — 但是進階會計被允許使用快閃記憶體磁碟機，而初級會計不被允許。此種情況下，僅透過管理群組層級套用政策到裝置可能不方便。

為協助您避免建立單一政策的多個實例，Kaspersky Next XDR Expert 可讓您建立*政策設定檔*。政策設定檔用於在單一管理群組中的裝置在不同政策設定下執行時。

政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在受管理裝置上活動。設定檔的啟動將修改在裝置上最初活動的"基本"政策的設定。修改的設定將使用已在設定檔中指定的值。

工作

Kaspersky Next XDR Expert 透過建立及執行*工作*，管理安裝在裝置上的 Kaspersky 安全應用程式。安裝、啟用和停用應用程式、掃描檔案、更新病毒資料庫和軟體模組以及應用程式的其他行為均需要使用工作來完成。

特定應用程式的工作僅在安裝了該應用程式的管理外掛程式時可以被建立。

工作可以在管理伺服器和裝置上執行。

以下工作管理伺服器上執行：

- 自動發佈報告
- 將更新下載至管理伺服器儲存區
- 備份管理伺服器資料
- 資料庫維護

以下類型的工作在裝置上執行：

- *本機工作* — 在特定裝置上執行的工作。

  本機工作可以被管理員透過管理主控台工具修改，或者被遠端裝置使用者修改（例如，透過安全應用程式介面）。如果本機工作同時被管理員和受管理裝置使用者修改，管理員的修改將生效，因為其具有更高優先順序。

- *群組工作* — 在特定裝置上執行的工作。

  除非在工作內容中指定了其他項目，群組工作也影響所選群組的所有子群組。群組工作也影響（可選）佈署在其群組或子群組的連線到從屬和虛擬管理伺服器的裝置。

- *全域工作* — 選取指定裝置來執行的工作，與裝置屬於哪個管理群組無關。

您可以為每個應用程式建立任意數量群組工作、全域工作或本機工作。

您可以修改工作設定、檢視工作進度、複製、匯出、匯入和刪除工作。

只有當裝置上應用程式被執行，建立之工作才會執行。

工作結果會儲存在 Syslog 事件記錄和 Kaspersky Next XDR Expert 事件記錄中，並集中儲存在管理伺服器上及各裝置本機。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

關聯器

*關聯器*是一個用於分析標準化事件的程式元件。在關聯程序中，事件可與來自活動清單和/或字典的資訊進行關聯。

分析所獲得的資料用於執行以下工作：

- 活動清單內容管理。
- 將關聯事件傳送到設定的目標

事件會即時進行關聯。

關聯器的運作原理是以事件的特徵碼分析為基礎。這表示每個事件都會依照使用者設定的關聯規則進行處理。當程式偵測到滿足關聯規則條件的事件序列時，它會建立一個關聯事件並將其傳送到儲存體。關聯事件也可以傳送到關聯器進行重新分析，這允許您自訂關聯規則，以便它們由先前分析的結果觸發。一個關聯規則的結果可以被其他關聯規則使用。

您可以將關聯規則及其使用的活動清單分配給各個關聯器，藉此平衡服務的負載。在此配置下，收集器會將正規化事件傳送至所有可用的關聯器。

關聯器會反覆執行下列步驟：

1. **取得事件**

   關聯器會從收集器或其他服務接收正規化的事件。

2. **套用關聯規則**

   您可以設定關聯規則，使其在發生單一事件或一連串事件時觸發。如果關聯規則未偵測到警示，事件處理會在此結束。

3. **回應警示**

   您可以指定程式在偵測到警示時必須執行的操作。程式中提供以下操作：

   - 事件擴充
   - 活動清單的操作
   - 傳送通知
   - 儲存關聯事件

4. **傳送關聯事件**

   當程式偵測到符合關聯規則條件的事件序列時，它會建立關聯事件並將其傳送到儲存體。至此，關聯器已完成事件處理。

事件

*事件*是在組織IT基礎設施的受監控元素上註冊的資訊安全事件。例如，事件包括登入嘗試、與資料庫的互動以及感應器資訊廣播。每個單獨的事件可能看起來毫無意義，但綜合考慮時，它們會構成網路活動的更大圖景，以幫助辨識安全威脅。這是KUMA的核心功能。

KUMA 從日誌接收事件，並將異質來源的資料轉換為統一格式，以重新建構事件（此程序稱為正規化）。接著，事件會經過篩選及彙總，並傳送至關聯器服務進行分析，以及傳送至儲存服務加以保留。當 KUMA 辨識出特定事件或事件序列時，會建立*關聯事件*，並同樣對其進行分析及保留。如果某個事件或事件序列顯示存在潛在的安全威脅，KUMA會建立警示。此警示包含有關威脅的警告以及安全官應調查的所有相關資料。

在整個生命週期中，事件會經歷轉換，並且可能會獲得不同的名稱。以下是典型事件生命週期的描述：

第一步在收集器中執行。

1. 原始事件。KUMA使用連接器從事件來源接收到的原始訊息稱為*原始事件*。這是一條未經處理的訊息，KUMA尚無法使用它。若要使其可用，必須將其標準化，以符合 KUMA 資料模型。這會在下一階段進行。

2. 標準化事件。規範化器根據KUMA資料模型轉換「原始」事件資料。經此轉換後，原始訊息即成為*標準化事件*，可供 KUMA 進行分析。從此時起，KUMA 僅處理標準化事件。原始事件不再使用，但可作為標準化事件的一部分保留於 `Raw` 欄位內。

   此程式具有以下標準化器：

   - JSON
   - CEF
   - Regexp
   - Syslog（依據RFC3164和RFC5424）
   - CSV/TSV
   - 鍵值
   - XML
   - Netflow v5、v9、IPFIX（v10）、sFlow v5
   - SQL

   此時標準化事件已可用於分析。

3. 事件目標。收集器服務處理完事件後，此事件即可供其他KUMA服務使用，並傳送至KUMA關聯器和/或儲存體。

事件生命週期的後續步驟在關聯器中完成。

事件分為以下類型：

1. 基礎事件。已標準化的事件。

2. 已彙總的事件。處理大量類似事件時，可以將它們「合併」為單一事件，以節省處理時間和資源。這些事件會作為基礎事件，並以相同方式處理；但除了父事件（已「合併」的事件）的所有參數外，已彙總的事件還有一個計數器，用來指出其代表的父事件數量。彙總事件也儲存收到第一個和最後一個父事件的時間。

3. 關聯事件。當偵測到滿足關聯規則條件的事件序列時，程式將建立*關聯事件*。這些事件可以被篩選、擴充和彙總。它們也可以傳送至儲存體，或重新送入關聯器管線。

4. 稽核事件。在卡巴斯基安全管理中心執行特定的安全性相關動作時，便會建立稽核事件（稽核事件、稽核事件）。這些事件用於確保系統完整性。這些事件會自動放入獨立的儲存空間，並儲存至少365天。

5. 監控事件。這些事件用於追蹤KUMA接收的資料量變化。

警示

在KUMA中，當收到觸發關聯規則的一系列事件時，就會建立警示。KUMA 分析師會建立關聯規則，以檢查傳入的事件是否存在潛在安全威脅。因此，觸發關聯規則時，系統會顯示可能存在惡意活動的警告。負責資料保護的安全官必須調查這些警示，並在必要時採取因應措施。

KUMA 會自動為每個警示指派嚴重等級。此參數顯示觸發關聯規則的處理程序之重要性或數量。應先處理嚴重等級較高的警示。收到新的關聯事件時，嚴重等級值會自動更新，但安全官也可以手動設定。在這種情況下，警示嚴重等級不再自動更新。

相關事件會連結至警示，因此可使用這些事件中的資料來補充警示內容。KUMA還提供了用於警示調查的向下切入功能。

您可以基於警示建立事件。

本章節介紹了KUMA中的警示管理。

事件

如果KUMA收到的資料的性質或產生的關聯事件和警示表明可能存在攻擊或弱點，則可以將此類事件的症狀組合成一個*事件*。這使安全專家能夠全面分析威脅表現並促進回應。

您可以為事件指派類別、類型和事件嚴重等級，並將事件指派給資料保護官進行處理。

事件可以匯出到NCIRCC和MDR。

資源

*資源*是KUMA元件，包含用於實現各種功能的參數：例如，與給定的網址建立連線或依據某些規則轉換資料。這些模組化元件會組成服務資源集，進而用於建立 KUMA 服務。

工作範圍

*工作範圍*是執行工作的裝置集合。範圍的類型包括以下：

- 對於*本機工作*，範圍是裝置本身。
- 對於*管理伺服器工作*，範圍是管理伺服器。
- 對於*群組工作*，範圍是包含在群組中的裝置清單。

當建立*全域工作*時，您可以使用以下方法指定範圍：

- 手動指定特定裝置。

  您可以使用 IP 位址（或 IP 範圍）或 DNS 名稱作為該裝置的位址。您還可以選擇由管理伺服器偵測到的聯網裝置。

- 從包含有要新增的裝置位址的 .txt 檔案來匯入裝置清單（每一個電腦位址必須單獨一行）。

  如果透過檔案匯入裝置清單或手動建立裝置清單，且如果裝置是以名稱定義，則清單可以只包含其資訊已被輸入到管理伺服器資料庫中的裝置。而且，資訊必須在裝置被連線或裝置發現中輸入。

- 指定裝置分類。

  後續，工作範圍隨著包含在分類中的裝置集的變更而變更。裝置分類可以基於裝置內容（包含安裝在裝置上的軟體）建立，也可以基於分配到裝置的標籤來建立。裝置分類是指定工作範圍的最靈活的方法。

  裝置分類的工作總是按管理伺服器排程執行。這些工作無法執行在缺少管理伺服器連線的裝置上。使用其他方法指定範圍的工作直接執行在裝置上，且因此不取決於到管理伺服器的裝置連線。

  裝置分類的工作不會按裝置本機時間執行；相反，它們將按照管理伺服器本機時間執行。使用其他方法指定範圍的工作以裝置本機時間執行。

本機應用程式設定與政策的關係

您可以使用政策為群組中的所有裝置設定完全相同的應用程式設定值。

政策指定的設定值可針對群組中的個別裝置使用本機應用程式設定重新定義。但本機只能調整政策中允許修改的設定項目，即為解鎖的項目。

應用程式在用戶端裝置上使用的設定值，是由政策中該設定的鎖定位置 (🔒) 所定義：

- 如果政策內容項目被鎖定，則所有用戶端裝置的設定值與政策中定義設定相同。
- 如果政策內容項目被「解鎖」，則應用程式將使用用戶端裝置的本機設定值，而不是政策中指定的值。您可以在本機應用程式設定中自行調整設定值。

用戶端裝置上執行工作時，應用程式以兩種不同的方式決定使用的設定：

- 如果沒有將設定項目鎖定以避免政策變更，則使用本機應用程式設定。
- 如果鎖定設定項目以避免修改，則使用群組政策設定。

需統一本機應用程式設定但又需要“解鎖”，需先“鎖定”並確定用戶端接收後再“解鎖”。

發佈點

發佈點（先前叫做更新代理）是安裝了網路代理的裝置，用於更新發佈、應用程式遠端安裝和網路裝置資訊檢索。

安裝在作為發佈點的裝置上的網路代理的功能和用例因作業系統而異。

發佈點可執行以下功能：

- 透過將從管理伺服器接收到的更新和安裝套件發佈到群組中的用戶端裝置（包括透過 UDP 進行多點傳送進行發佈）。更新可以從管理伺服器接收，或者從 Kaspersky 更新伺服器獲取。如果後者，必須為發佈點建立更新工作。

  發佈點加速更新發佈並釋放管理伺服器資源。

- 使用 UDP 透過多點傳送發佈政策和群組工作。

- 用作管理群組中的裝置與管理伺服器的連線閘道。

  如果群組中的受管理裝置與管理伺服器之間的直接連線無法建立，則發佈點可用作此群組的管理伺服器連線閘道。在這種情況下，受管理裝置將連線到閘道，連線閘道又連線到管理伺服器。

  用作連線閘道的發佈點的可用性不會封鎖受管理裝置與管理伺服器之間的直接連線。如果連線閘道不可用，但在技術上可與管理伺服器進行直接連線，則受管理裝置將直接連線到管理伺服器。

- 輪詢網路以偵測新裝置並更新現有裝置的資訊。發佈點套用與管理伺服器相同的裝置發現方法。

- 執行卡巴斯基和其他軟體供應商的應用程式遠端安裝，包括在沒有網路代理的用戶端裝置上安裝。

  此功能允許將網路代理的安裝套件遠端傳輸到位於管理伺服器無直接存取權限的網路上的用戶端裝置。

- 作為代理伺服器參與卡巴斯基安全網路 (KSN)。

  您可以在發佈點端啟用 KSN 代理伺服器以使裝置作為 KSN 代理伺服器。此種情況下，KSN 代理服務會在裝置上執行。

檔案透過 HTTP（如果啟用了 SSL 連線，則透過 HTTPS）從管理伺服器傳輸到發佈點。使用 HTTP 或 HTTPS 促成更高效能，相比透過流量的 SOAP。

安裝有網路代理的裝置可以被手動（透過管理員）或自動（透過管理伺服器）分配發佈點。指定管理群組的發佈點完整清單顯示在發佈點清單的報告中。

發佈點的範圍是管理員將其分配到其中的管理群組，以及其所有階層等級的子群組。如果已在管理群組的階層中分配幾個發佈點，則受管理裝置的網路代理會連線在階層上最近的發佈點。

如果發佈點被管理伺服器自動分配，它透過廣播網域分配，而不是透過管理群組。此情況發生在所有廣播網域已知時。網路代理在相同的子網路與其他網路代理交換資訊並傳送給管理伺服器它的其他網路代理的資訊。管理伺服器可以用此資訊透過廣播網域分組網路代理。在管理群組中超過 70% 的網路代理被輪詢後，廣播網域對管理伺服器已知。管理伺服器每兩小時輪詢一次廣播網域。發佈點透過廣播網域分配後，就無法透過管理群組重新分配。

若管理員會手動指派發佈點，則可將其指派至管理群組或網路位置。

帶有活動連線設定檔的網路代理不參與廣播網域偵測。

Kaspersky Next XDR Expert 會為每個網路代理指派一個與其他所有位址皆不同的唯一 IP 多點傳送位址。這允許您避免由於 IP 重疊引起的網路超載。應用程式先前版本分配的 IP 多點傳送位址將不被變更。

當兩個或更多發佈點分配在單獨的網路區域或單獨的管理群組，其中一個會變成活動發佈點，其餘的變成備用發佈點。活動發佈點直接從管理伺服器下載更新和安裝套件，備用發佈點只從活動發佈點接收更新。此種情況下，檔案從管理伺服器下載一次，然後在發佈點之間發佈。如果因為任何原因活動發佈點不可用，其中一個備用發佈點將變成活動的。管理伺服器自動分配發佈點作為備用。

發佈點狀態（*活動* / *備用*）會連帶核取方塊一起顯示在 klnagchk 報告中。

一個發佈點需要至少 4 GB 的可用磁碟空間。如果發佈點的可用磁碟空間少於 2 GB，Kaspersky Next XDR Expert 會建立重要性等級為*警告*的安全問題。安全問題將被發佈在裝置內容中，在**安全問題**區域。

在分配為發佈點的裝置上執行遠端安裝工作需要更多可用磁碟空間。剩餘磁碟空間磁區必須超過安裝套件的總大小。

在分配為發佈點的裝置上執行任何更新（修補）工作和修復弱點工作需要另外的可用磁碟空間。剩餘磁碟空間磁區必須是至少兩倍的要安裝修補程式的總大小。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

連線閘道

*連線閘道*是一種以特殊模式執行的網路代理。連線閘道接受來自其他網路代理的連線，並透過其自身與伺服器的連線將它們透過通道傳送到管理伺服器。與普通的網路代理不同，連線閘道會等待來自管理伺服器的連線，而不是建立與管理伺服器的連線。

連線閘道最多可以接收來自 10,000 台裝置的連線。

您可以使用兩個選項來使用連線閘道：

- 我們建議您在非警戒區 (DMZ) 中安裝連線閘道。對於在辦公室外的裝置上安裝的其他網路代理，您需要透過連線閘道專門設定與管理伺服器的連線。

  連線閘道不以任何方式修改或處理從網路代理傳輸到管理伺服器的資料。此外，它不會將此資料寫入任何緩衝區，因此不能接受來自網路代理的資料，以後再將其轉發給管理伺服器。如果網路代理嘗試透過連線閘道連線到管理伺服器，但是連線閘道無法連線到管理伺服器，則網路代理會認為這是無法存取的管理伺服器。所有資料均保留在網路代理上（不在連線閘道上）。

  連線閘道無法透過另一個連線閘道連線到管理伺服器。這意味著網路代理不能同時作為連線閘道，且不能使用連線閘道連線到管理伺服器。

  所有連線閘道都包含在管理伺服器內容的發佈點清單中。

- 您也可以在網路內使用連線閘道。例如，自動分配的發佈點也將成為其自身範圍內的連線閘道。但是，在內部網路中，連線閘道無法提供可觀的效益。它們減少了管理伺服器接收到的網路連線數量，但是沒有減少傳入資料的數量。即使沒有連線閘道，所有裝置仍可以連線到管理伺服器。

核心

*核心*是KUMA的核心元件，它是所有其他服務和元件的基礎。核心的主控台提供了一個圖形使用者介面，供操作員/分析師日常使用以及設定整個系統。

核心可讓您：

- 建立和設定程式的服務或元件，以及將必要的軟體整合到系統中；
- 集中管理程式服務和使用者帳戶；
- 視覺化程式的統計資料；
- 根據接收到的事件調查安全威脅。

儲存體

KUMA *儲存體*用於儲存正規化事件，並確保 KUMA 能夠快速且可靠地存取這些事件，以擷取分析資料。ClickHouse 技術可實現快速存取和高可用性。這意味著*儲存體*是綁定到KUMA儲存體服務的ClickHouse叢集。ClickHouse叢集可以補充冷儲存磁碟。

選擇ClickHouse叢集組態時，請考慮組織的特定事件儲存需求。如需更多資訊，請參閱ClickHouse 文件。

在儲存庫中，您可以建立*空間*。空間可讓您組織叢集中的資料，例如，將特定類型的事件儲存在一起。

收集器

*收集器*是一個應用程式元件，它從事件來源接收訊息，處理它們，並將它們傳輸到儲存體、關聯器和/或協力廠商服務以識別警示。

對於每個收集器，您需要配置一個連接器和一個標準化器。您也可以配置無限數量的附加標準化器、篩選器、擴充規則和彙總規則。若要讓收集器將標準化事件傳送至其他服務，您必須新增目的地。通常會使用兩個目的地：儲存體和關聯器。

收集器會重複執行下列步驟：

1. **從事件來源接收訊息**

   若要接收訊息，您必須設定主動或被動連接器。被動連接器只會接聽來自事件來源的訊息，而主動連接器則會主動輪詢事件來源，例如資料庫管理系統。

   連接器可以有不同的類型。連接器類型的選擇取決於訊息傳遞所使用的傳輸通訊協定。例如，如果您的事件來源透過 TCP 傳送訊息，則必須安裝 TCP 類型的連接器。

   有以下類型的連接器可用：

   - internal
   - tcp
   - udp

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

2 **事件解析與標準化**

連接器接收的事件會使用由使用者設定的標準化器與標準化規則進行處理。標準化器的選擇取決於事件來源所傳送的訊息格式。例如，如果您的事件來源以 CEF 格式傳送訊息，則必須選擇 CEF 類型的標準化器。

以下標準化器可供使用：

- JSON
- CEF
- Regexp
- Syslog（依據RFC3164和RFC5424）
- CSV
- 鍵值
- XML
- NetFlow v5
- NetFlow v9
- IPFIX (v10)
- SQL

3 標準化事件的篩選

您可以設定篩選器，以便選擇符合指定條件的事件進行進一步處理。

4 標準化事件的擴充和轉換

擴充規則可讓您將來自內部和外部來源的補充資訊新增至事件。

以下擴充來源可供使用：

- 常數
- cybertrace
- 字典
- dns
- 事件
- ldap
- 範本
- 時區資料
- 地理資料

轉換規則可讓您根據特定條件轉換事件欄位的值。

以下轉換方式可供使用：

- lower：將所有字元轉換為小寫。
- upper：將所有字元轉換為大寫。
- regexp：使用 RE2 規則運算式擷取子字串。
- substring：指定第一個和最後一個字元以擷取子字串。
- replace：以字串取代部分文字。
- trim：刪除指定的字元。
- append：在欄位值的結尾新增字元。
- prepend：在欄位值的開頭新增字元。

5 彙總正規化事件

您可以設定彙總規則以減少傳輸到儲存體和/或關聯器的類似事件數。彙總規則可讓您將多個事件合併為一個事件。這有助於降低負責進一步處理事件之服務的負載、節省儲存空間，並減少授權的每秒事件數 (EPS) 配額用量。例如，如果有許多事件涉及兩個 IP 位址之間使用相同傳輸層和應用程式層通訊協定的網路連線，您可以將特定期間內的這類事件彙總為一個大型事件。

6 傳輸正規化事件

完成所有處理階段後，事件將會傳送到設定的目標。

服務

*服務*是KUMA 的主要元件，可接收、處理、分析及儲存事件。每個服務由兩個協同工作的部分組成：

- 服務的一部分是在KUMA主控台內基於服務資源集建立的。
- 服務的另一部分會做為 KUMA 元件之一，安裝在部署 KUMA 的網路基礎架構中。服務的伺服器端部分可由多個實例組成，例如，可同時在多個裝置上安裝相同代理或儲存的服務。

服務的兩個部分會透過服務 ID彼此連結。

KUMA代理程式

KUMA *代理*是將伺服器和工作站的原始事件轉送至 KUMA 目的地的服務。

提供下列類型的代理：

- WMI代理程式用於使用Windows管理規格從遠端Windows裝置接收資料。它們安裝在Windows資產中。
- wec代理程式用於使用Windows事件收集器從本機裝置接收Windows日誌。它們安裝在Windows資產中。
- tcp代理程式用於透過TCP協定接收資料。它們安裝到Linux和Windows資產。
- udp代理程式用於透過UDP協定接收資料。它們安裝到Linux和Windows資產。
- nats代理程式用於NATS通訊。它們安裝到Linux和Windows資產。
- kafka代理程式用於Kafka通訊。它們安裝到Linux和Windows資產。
- http代理程式用於透過HTTP協定進行通訊。它們安裝到Linux和Windows資產。
- 檔案代理程式用於從檔案獲取資料。它們安裝到Linux資產。
- ftp代理程式用於透過檔案傳輸協定接收資料。它們安裝到Linux和Windows資產。
- nfs代理程式用於透過網路檔案系統協定接收資料。它們安裝到Linux和Windows資產。
- snmp代理程式用於透過簡易網路管理通訊協定接收資料。它們安裝到Linux和Windows資產。
- 二極體代理程式與資料二極體一起使用，以接收來自隔離網段的事件。它們安裝到Linux和Windows資產。
- etw代理程式用於接收Windows事件偵錯資料。它們安裝在Windows資產中。

關於嚴重程度

*嚴重等級*反映了KUMA關聯器偵測到的安全敏感活動的相對重要性。它顯示了多個警示的處理順序，並指示是否應讓高級安全官參與。

關聯器會根據關聯規則設定，自動為關聯事件和警示指派嚴重程度值。警示的嚴重等級也取決於與已處理事件相關的資產，因為關聯規則會考慮相關資產類別的嚴重等級。如果警示或關聯事件沒有任何具嚴重程度值的連結資產，或完全沒有任何連結資產，則該警示或關聯事件會繼承產生該警示或事件的關聯規則之嚴重程度。警示或關聯事件的嚴重程度一律等於或高於產生該警示或關聯事件之關聯規則的嚴重程度。

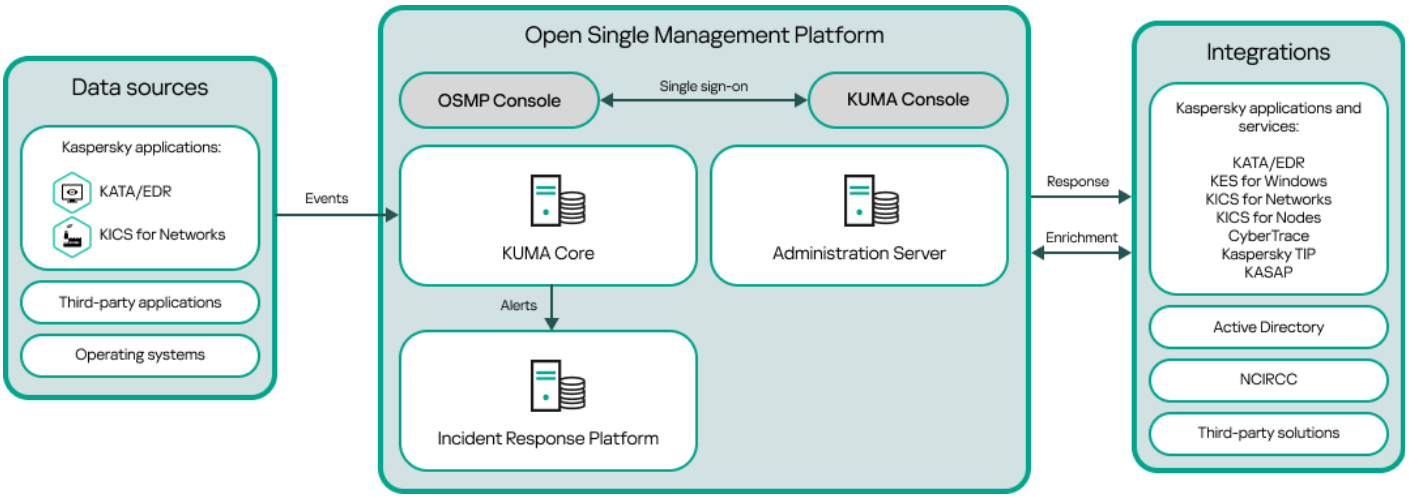
可手動變更警示的嚴重程度。手動修改的嚴重程度不再由關聯規則自動更新。

可能的嚴重等級值：

- 低
- 中
- 高
- 嚴重

Open Single Management Platform架構

本章節介紹了Open Single Management Platform元件及其互動。



Open Single Management Platform架構

Open Single Management Platform包含以下主要元件：

- **Open Single Management Platform** (OSMP)。Kaspersky Next XDR Expert所基於的技術基礎。OSMP 會整合解決方案的所有元件，提供元件之間的互動管道。OSMP 具備可擴充性，並支援與 Kaspersky 應用程式和協力廠商解決方案整合。
- **OSMP主控台**。為OSMP提供網頁介面。
- **KUMA Core**。KUMA的核心元件。KUMA接收、處理和儲存資訊安全事件，然後使用關聯規則分析事件。分析結果顯示，如果滿足關聯規則的條件，KUMA會建立警示並將其傳送到事件回應平台。
- **事件回應平台**Open Single Management Platform元件可讓您自動或手動建立事件、管理警示和事件生命週期、將警示和事件指派給SOC分析師，以及自動或手動回應事件，包括透過常規程式進行回應。
- **管理伺服器**（也稱為*伺服器*）。用戶端組織端點防護的關鍵元件。管理伺服器透過EPP應用程式提供端點防護的集中佈署和管理，並讓您監控端點防護狀態。
- **資料來源**。產生事件的資訊安全硬體和軟體。將Kaspersky Next XDR Expert與所需資料來源整合後，KUMA會接收事件以進行儲存和分析。
- **整合**。卡巴斯基應用程式和協力廠商解決方案與OSMP整合。透過整合解決方案， SOC分析師可以富集事件調查所需的資料，然後對事件做出回應。

SIEM元件架構

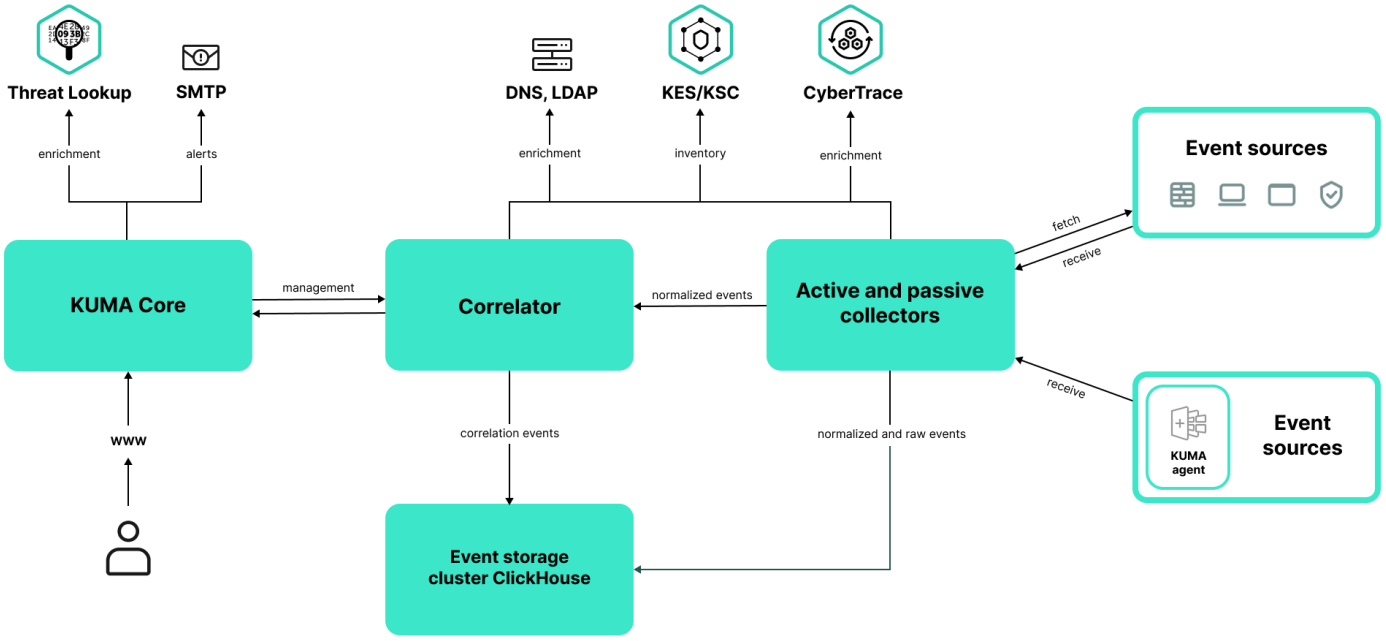
標準程式安裝包含以下元件：

- *核心*，包含用於監控和管理系統元件設定的圖形介面。
- 一個或多個*收集器*，用於接收來自事件來源的訊息，並對其進行解析、標準化以及（如果需要）篩選和/或彙總。

- *關聯器*，用於分析從收集器接收到的標準化事件，使用活動清單執行必要的操作，並根據關聯規則建立警示。

- *儲存區*，用於儲存標準化事件和已登錄的警示。

事件透過可選加密的可靠傳輸協定在元件之間傳輸。您可以設定負載平衡，以在服務實例之間分配負載；如果主要元件無法使用，也可以啟用自動切換至備份元件的功能。如果所有元件都無法使用，事件會儲存至硬碟緩衝區，以便稍後傳送。檔案系統中用於暫存事件的緩衝區大小可以變更。



KUMA架構

OSMP主控台介面

Kaspersky Next XDR Expert透過OSMP主控台介面進行管理。

OSMP主控台視窗中會包含以下項目：

- 視窗左側的主功能表
- 視窗上部的上部窗格
- 視窗右側的工作區

主功能表

主功能表會包含以下區段：

- **管理伺服器**。顯示您目前所連管理伺服器的名稱。您可以透過按一下管理伺服器名稱來開啟管理伺服器屬性。
- **主控台導覽**。顯示主功能表地圖。大部分顯示的部分都可以加入書籤或設定為首頁。預設**主控台導覽**被設定為首頁。您可以變更這些設定。
- **監控**。提供基礎設施、防護狀態和統計資訊的概覽，包括威脅搜尋、警示和事件以及常規程式。此外，本部分還允許您新增和設定KUMA資源和服務。
- **資產管理**。包含資產和硬體管理工具，以及卡巴斯基應用程式政策。
- **工作**。包含用於建立和執行工作的工具。
- **使用者和角色**。可讓您管理使用者和角色、透過向使用者分配角色來設定使用者權限，以及為角色設定關聯的政策設定檔。
- **儲存區**。可讓您存取應用程式儲存庫。
- **軟體管理**。可讓您管理卡巴斯基和協力廠商應用程式，以及安裝套件和修補程式。
- **操作**。包含多種操作，包括應用程式產品授權、檢視和管理加密磁碟機和加密事件。
- **發現和佈署**。可讓您輪詢網路來發現用戶端裝置，以及手動或自動將裝置分發到管理群組。此部分還包含防護佈署精靈。
- **市場**。包含完整卡巴斯基業務解決方案系列的資訊，可讓您選取所需的解決方案，然後繼續在卡巴斯基網站購買這些解決方案。
- **設定**。包含將Kaspersky Next XDR Expert與其他卡巴斯基應用程式整合的設定，可讓您建立API權杖。它還包含與根據正在使用的功能顯示介面元素以及介面語言相關的設定。此外，您也可以從此區段開啟 KUMA 設定視窗，其中包含 KUMA 組態的參數，包括 KUMA 組態設定、KUMA 整合設定、產品授權金鑰管理和存取選項。

如有必要，您可以透過點擊位於螢幕底部的 V 形符號 (‹‹) 來將主選單最小化為圖示。

上方窗格

上方窗格始終顯示在所有主控台部分中，且無法隱藏。

窗格左側包含應用程式名稱和徽標。如果點擊應用程式名稱或標誌，OSMP主控台主頁將開啟。

窗格右側顯示以下設定：

- 通知圖示 (🔔)。如果點擊該圖示，一個包含通知的窗格將開啟。
- 您的帳戶選單。包含指向Kaspersky Next XDR Expert幫助的連結。它還允許您登出Kaspersky Next XDR Expert並檢視OSMP主控台版本和已安裝的管理網頁外掛程式清單。

工作區

工作區會顯示您在OSMP主控台介面視窗的各個部分中所選擇檢視的資訊。其中還會包含供您設定資訊顯示方式的控制元素。

變更OSMP主控台介面的語言

您可以選擇OSMP主控台介面的語言。

要變更介面語言：

1. 在主功能表中，轉至**設定** → **語言**。
2. 選擇一種受支援的當地語係化語言。

變更OSMP主控台首頁

登入OSMP主控台後，將顯示首頁。

預設**主控台導覽區域**被設定為首頁。如果需要的話，您可以變更首頁。

變更首頁：

1. 在**主控台導覽**部分，將滑鼠遊標懸停在您想要設定為首頁的項目上。
2. 在首頁 (⌂) 圖示顯示後，點擊圖示。

   首頁已變更。螢幕上會顯示對應的訊息。選為首頁的項目會以房屋 (⌂) 圖示標示。

市場和**設定**區域不能設定為首頁。

新增和移除書籤

您可以將OSMP主控台的常用部分新增到書籤中，以便從主功能表中的**書籤**部分快速存取它們。

如果您未將任何部分新增至書籤，則**書籤**區域不會顯示在主功能表中。

您只能將顯示頁面的區域新增至書籤。例如，如果您前往**資產管理 → 資產（裝置）**，則會開啟包含裝置表的頁面，這表示您可以將該部分新增到書籤。若在主功能表中選擇該部分後出現視窗或未出現任何元素，則您無法將此類區域新增至書籤。

若要將一個區域新增至書籤：

1. 在主功能表中，將滑鼠遊標停留在要釘選的區段上。
2. 在書籤 (🔖) 圖示顯示後，點擊圖示。

   該區域顯示在**書籤**區域中。

要將區域從書籤中移除：

1. 在主功能表中，轉至**書籤**區域。
2. 將滑鼠遊標停留在要移除的區域上，然後點擊書籤 (🔖) 圖示。

   該區段已從書籤中刪除。

您也可以在 **主控台導覽** 區域中，將滑鼠遊標停留在區域上，然後點擊書籤 (🔖) 圖示，以新增區域至書籤或從書籤中移除區域。所選項目將以書籤 (🔖) 圖示標記，並顯示在主功能表的 **書籤** 區域中。如果您想要從書籤中移除該項目，請點擊書籤 (🔖) 圖示。

書籤 區域僅顯示在主功能表中。它從來不顯示在 **主控台導覽** 頁面上。

產品授權

本節涵蓋 Kaspersky Next XDR Expert 產品授權的主要面向。

關於最終使用者產品授權協議

最終使用者產品授權協議（產品授權協議）是您和AO Kaspersky Lab之間具有約束力的合作協議，其中規定了您使用該程式應遵守的條款。

在您開始使用應用程式之前請仔細閱讀產品授權協議。

您可透過以下方式，檢視最終使用者產品授權協議的條款：

- Open Single Management Platform安裝期間
- 透過讀取license.txt文件。本文件包含在應用程式分發套件中。

當您安裝程式時同意最終使用者產品授權協議，表示您接受最終使用者產品授權協議的條款。如果您不接受產品授權協議中的條款，將取消應用程式安裝且不再使用應用程式。

關於產品授權金鑰

*產品授權金鑰*由一系列字母數字組成，您可以依據最終使是用者產品授權協議的條款使用它們啟動並使用程式。產品授權金鑰由 Kaspersky 專家產生。

您可以使用下面的方法新增一個產品授權金鑰到應用程式：透過套用*金鑰檔案*或輸入*啟動碼*。為程式新增金鑰後，將在程式介面中顯示該產品授權金鑰的唯一字母數字序列。

如果違反產品授權協議的條款，Kaspersky 可能會封鎖產品授權金鑰。如果金鑰已被封鎖，要使用程式，您需要新增另外一個金鑰。

產品授權金鑰可以是啟用或備用的金鑰（或預留）。

*啟動產品授權金鑰*是應用程式目前使用的產品授權金鑰。啟動產品授權金鑰可以被新增為正式產品授權。應用程式只能擁有一個啟動產品授權金鑰。

*備用（或預留）產品授權金鑰*是允許使用者使用應用程式，但是目前未使用的產品授權金鑰。與目前產品授權金鑰相關聯的產品授權到期時，備用產品授權金鑰將自動成為目前產品授權金鑰。只有在新增啟動產品授權金鑰之後，才可以新增備用產品授權金鑰。

試用產品授權金鑰僅可以被當作啟動產品授權金鑰新增。試用產品授權金鑰不可以被當作備用產品授權金鑰新增。

關於啟動碼

*啟動碼*是由 20 個拉丁字母和數字組成的唯一序列。若要新增產品授權金鑰以啟動Open Single Management Platform，您必須輸入啟動碼。您將在購買Open Single Management Platform或申請Open Single Management Platform試用版時提供的電子郵件地址收到啟動碼。

若要使用啟動碼啟動應用程式，您需要網際網路來建立與卡巴斯基啟動伺服器的連線。

如果您在安裝應用程式後遺失了啟動碼，請聯絡您購買產品授權的卡巴斯基合作夥伴。

關於金鑰檔案

*金鑰檔案*是 Kaspersky 提供的 .key 副檔名的檔案。金鑰檔案設計用於透過新增產品授權金鑰啟動應用程式。

您在購買Open Single Management Platform或訂購Open Single Management Platform試用版時提供的電子郵件地址會收到一個金鑰檔案。

您不需要連線到 Kaspersky 啟動伺服器以使用金鑰檔案啟動應用程式。

如果金鑰檔案被意外刪除，您可以還原它。您可能需要金鑰檔案來註冊 Kaspersky CompanyAccount。

若要還原您的金鑰檔案，執行下面任何的操作：

- 聯絡產品授權銷售商。
- 使用您有效的啟動碼，透過卡巴斯基網站接收金鑰檔案。

產品授權限制

購買Kaspersky Next XDR Expert產品授權時，您可以確定要保護的使用者數量。您不能超過產品授權限制的5%。如果超過產品授權限制的5%以上，則額外的裝置和額外的帳戶將添加到**受限制的資產**清單中。

如果超過產品授權限制，OSMP主控台頂部會出現通知。

無法啟動受限資產的回應操作或常規程式。

若要檢視受限資產清單：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 在**租用戶**部分中，按一下根租用戶。
   根租用戶的內容視窗將會開啟。

3. 選取**產品授權**頁籤。

4. 點擊包含受限資產數量的連結。

受限制的資產視窗隨即開啟。

清單最多顯示2000個受限資產（前1000個裝置和前1000個帳戶）。

Kaspersky Next XDR Expert產品授權功能

Kaspersky Next XDR Expert產品授權擴充了Kaspersky EDR Expert產品授權的功能，增加了用於自動化回應和事件管理的進階工具。

Kaspersky Next XDR Expert授權包含的其他功能包括：

- **進階回應**— 透過自訂指令碼或UserGate自動回應警示和事件；
- **XDR回應**— 擴充的XDR回應操作目錄。
- **高階案例管理**— 服務等級協定（SLA）、設定警示和事件的自動指派，以及跨租用戶子事件支援。

Kaspersky Next XDR Expert產品授權提供更靈活、可擴展的事件管理，能夠整合到複雜的基礎設施中，並實現回應流程的進階自動化。

啟動Kaspersky Next XDR Expert

安裝Kaspersky Next XDR Expert後，您必須在管理伺服器內容中啟動應用程式。

若要啟動Kaspersky Next XDR Expert：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選取**產品授權金鑰**區段。

3. 在**目前產品授權**下，按一下**選擇**按鈕。

4. 在開啟的視窗中，選擇要用於啟動Kaspersky Next XDR Expert的產品授權金鑰。如果產品授權金鑰未列出，請按一下**新增新的產品授權金鑰**按鈕，然後指定新的產品授權金鑰。

5. 如有必要，您也可以新增備用產品授權金鑰。為此，請在**備用產品授權金鑰**下，按一下**選擇**按鈕，然後選擇現有產品授權金鑰或新增產品授權金鑰。請注意，如果沒有啟動的產品授權金鑰，則無法新增備用產品授權金鑰。

6. 點擊**儲存**按鈕。

為SIEM元件新增產品授權金鑰

您可以在 OSMP 主控台中新增應用程式產品授權金鑰。如果您使用金鑰檔案啟動應用程式，則可能同時存在兩個產品授權金鑰：一個活動金鑰和一個備用金鑰。如果您使用啟動碼，則只有一組產品授權金鑰。在KUMA中，由一個活動產品授權金鑰、一個備用產品授權金鑰或一個啟動碼組成的群組稱為*產品授權群組*。因此，您可以使用兩個金鑰檔案或一個啟動碼來新增產品授權群組。

如果在KUMA實例中新增了多個產品授權群組，則所有產品授權群組的活動產品授權金鑰將自動合併。這會建立一個*合併產品授權*。此類產品授權的產品授權金鑰將按照以下規則合併：

- 所有活動產品授權金鑰的**EPS可用**值將相加。合併後的EPS值將在合併產品授權中指定，並對所有租用戶可用。

  如果合併產品授權中的任何產品授權金鑰將到期，則該產品授權金鑰的EPS定額值將自動從合併產品授權的總EPS定額中減去。相應地，當將新的活動產品授權金鑰新增至合併授權時，該產品授權金鑰的EPS定額值將自動新增至總EPS定額。

- 租用戶產品授權中可用的模組集必須相同。如果某個產品授權包含其他產品授權中不存在的模組，則該模組在合併產品授權中也不可用。因此，任何租用戶都無法使用該模組。

  向合併產品授權新增產品授權金鑰時，也適用相同的規則。如果某個模組在新產品授權金鑰中可用，但在合併許可證中不可用，則該模組不會在合併許可證下可用。如果某個模組在合併產品授權中可用，但在新產品授權金鑰中不可用，則該模組在合併產品授權下將不可用。當新增包含不符合模組集的產品授權金鑰時，KUMA會顯示警告訊息，並且僅在您確認後才會新增此類產品授權金鑰。

- 合併產品授權最多可包含50個啟動金鑰。

只有具有主管理員角色的使用者才能新增產品授權金鑰。

新增產品授權群組

若要新增產品授權群組：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**其他**下，按一下**產品授權**。

3. 按一下**新增產品授權金鑰**。

4. 這將開啟一個視窗；在該視窗中，輸入新產品授權群組的名稱。

5. 按一下**新增**。

6. 點擊新增的產品授權群組的名稱。

7. 在開啟的視窗中， 選擇要新增產品授權金鑰的方式：

   - 使用啟動碼：

     1. 輸入啟動碼。

     2. 如果您的企業使用代理伺服器連接到網際網路，請輸入代理伺服器資訊。啟動應用程式需要網際網路連線。

   - 使用金鑰檔案。

     1. 在**有效產品授權金鑰**部分，按一下**上傳**按鈕，然後選擇金鑰檔案（副檔名為.KEY的檔案）。

     2. 在**備用產品授權金鑰**部分，以相同方式新增備用產品授權金鑰。

8. 按一下**新增**。

產品授權群組隨即新增到清單中，應用程式將啟動。

新增備用產品授權金鑰

若要將備用產品授權金鑰新增至產品授權群組：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。

2. 在**其他**下，按一下**產品授權**。

3. 按一下要新增備用產品授權金鑰的產品授權群組的名稱。

4. 這將開啟一個視窗；在該視窗的**備用產品授權金鑰**部分，按一下**上傳**按鈕，然後選擇金鑰檔案（副檔名為.KEY的檔案）。

5. 按一下**新增**。

替換活動產品授權金鑰

如果要新增一個活動產品授權金鑰來替換已新增的密鑰，請先刪除當前產品授權密鑰。然後新增產品授權金鑰。

檢視使用中產品授權金鑰的相關資訊

若要檢視有效和備用產品授權金鑰：

1. 在主功能表中，轉至**設定 → 租用戶**。

2. 在**租用戶**部分中，按一下根租用戶。
   根租用戶的內容視窗將會開啟。

3. 選取**產品授權**頁籤。

   有效和備用產品授權金鑰隨即顯示。

顯示的產品授權金鑰將應用於根租用戶的所有子租用戶。無法為子租用戶指定單獨的產品授權金鑰。子租用戶的內容視窗不包含**產品授權**頁籤。

如果超出產品授權金鑰限制，則會顯示通知，並且有關產品授權金鑰的資訊會顯示警告。

您可以點選**移至管理伺服器**按鈕來管理Kaspersky Next XDR Expert產品授權金鑰。

在**產品授權**頁籤上，您也可以檢視已授權物件的清單。為此，請點選 ⓘ 按鈕。

已授權物件的可用性取決於購買的產品授權類型。

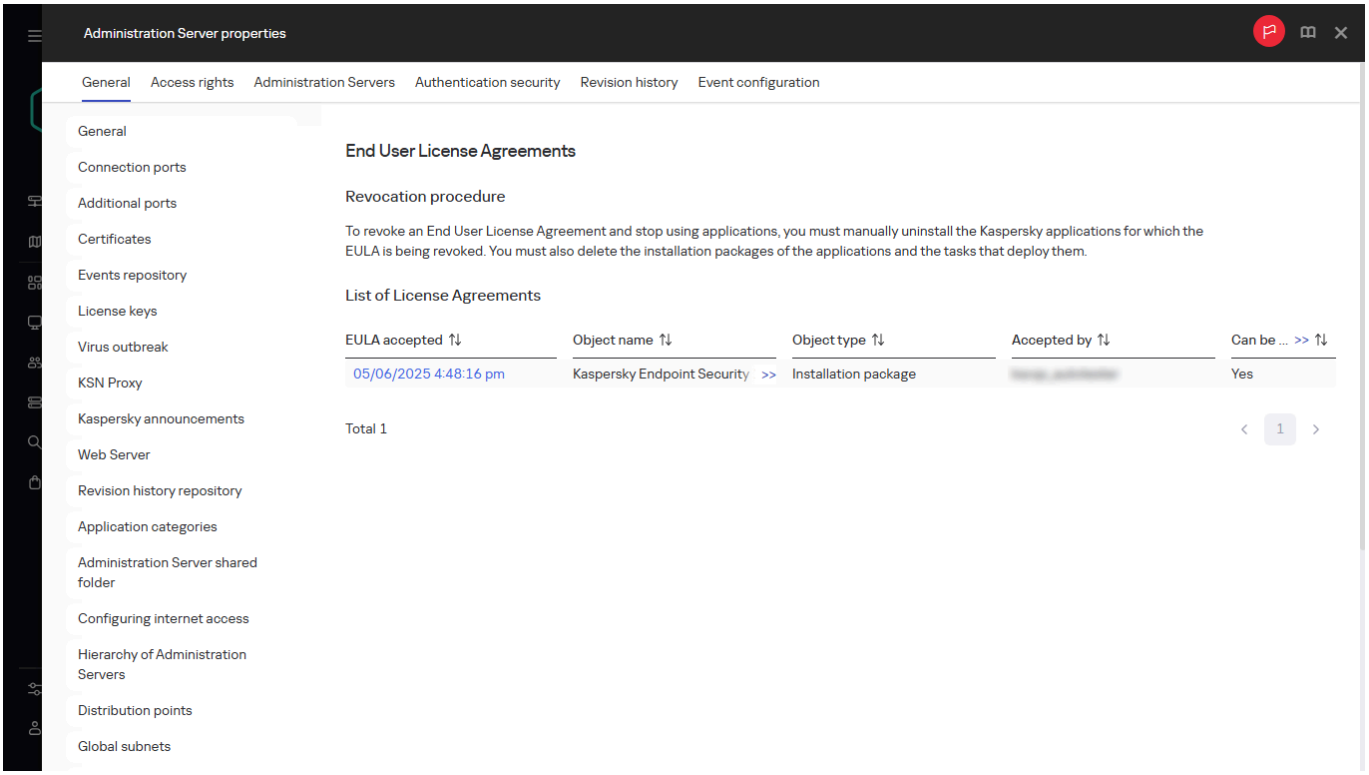
撤銷最終使用者產品授權協議的許可

若您決定停止防護您的一些用戶端裝置，您可針對任何受管理的 Kaspersky 應用程式撤銷最終使用者產品授權協議 (EULA)。您必須先解除安裝所選的應用程式在撤銷其 EULA。

若要撤銷 Kaspersky 受管理應用程式的 EULA：

1. 開啟管理伺服器內容視窗，然後在 **一般** 頁籤上選取 **最終使用者產品授權協議** 區段。

   會顯示在建立安裝套件時、在無縫安裝更新時或在佈署 Kaspersky Security for Mobile 時接受的 EULA 清單。



EULA 清單

2. 在清單中，選取您要撤銷協議的 EULA。

   您可以檢視 EULA 的下列內容：

   - 接受 EULA 的日期
   - 接受 EULA 的使用者名稱

3. 點擊任何 EULA 的接受日期以開啟其顯示以下資料的內容視窗：

   - 接受 EULA 的使用者名稱
   - 接受 EULA 的日期
   - EULA 的唯一識別碼 (UID)
   - EULA 的完整內容
   - EULA 連結的物件清單（安裝套件、無縫更新、行動應用程式），以及其各自的名稱與類型

4. 在 EULA 內容視窗的下部，點擊**撤銷產品授權協議**按鈕。

   若存在任何物件（安裝套件與其各自工作）防止撤銷 EULA，則會顯示對應的通知。刪除這些物件前，您無法處理撤銷。

   在開啟的視窗中，系統會告知您必須先解除安裝對應至 EULA 的 Kaspersky 應用程式。

5. 按一下按鈕以確認撤銷。

EULA 已撤銷。這不會在顯示於 **最終使用者產品授權協議** 區段的產品授權協議清單中。EULA 內容視窗關閉；應用程式將不再繼續安裝。

續約 Kaspersky 應用程式的產品授權

您可以續約 Kaspersky Next XDR Expert 及其中所含 Kaspersky 應用程式（例如 Kaspersky Unified Monitoring and Analysis Platform）的產品授權。您可以續訂已過期或將在30天內過期的許可證。

購買新的Kaspersky Next XDR Expert產品授權後，將向您的電子郵件地址發送一封包含新產品授權金鑰的存檔電子郵件。

若要續約Kaspersky Next XDR Expert的產品授權：

1. 從傳送到您電子郵件地址的檔案中提取新的產品授權金鑰。
2. 請依照啟動Kaspersky Next XDR Expert中所述的步驟操作。

   產品授權隨即續訂。

如果您需要續訂隨附的卡巴斯基應用程式的產品授權，則必須將新的產品授權金鑰新增至這些解決方案的網頁介面。

如需瞭解如何續約 Kaspersky Unified Monitoring and Analysis Platform 的產品授權，請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明中的將產品授權金鑰新增至程式網頁介面一節。

在OSMP主控台中，產品授權即將到期的通知會依以下排程顯示：

- 到期前 30 天
- 到期前 7 天
- 到期前 3 天
- 到期前 24 小時
- 產品授權過期時

移除SIEM組件的產品授權金鑰

在 OSMP 主控台中，您可以從程式中移除已新增的產品授權金鑰（例如，需要以其他產品授權金鑰取代目前的產品授權金鑰時）。產品授權金鑰移除後，收集器立即停止接收和處理事件。舊事件仍然可用。創建和修改資源不可用，創建和執行服務也將不可用。新增產品授權金鑰後，此功能將重新啟動。

只有具備主管理員角色的使用者才能刪除產品授權金鑰。

若要刪除新增的產品授權金鑰：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**其他**下，按一下**產品授權**。
3. 選取要刪除的產品授權金鑰對應的核取方塊，然後按一下垃圾桶圖示（ ）。
4. 這將開啟一個確認視窗；在該視窗中，按一下**刪除**。

   產品授權金鑰將從應用程式中移除。

使用卡巴斯基市場選擇卡巴斯基商業解決方案

市場是主功能表中的一個區段，可讓您檢視整個 Kaspersky 業務解決方案範圍，選擇您需要的解決方案，然後在 Kaspersky 網站上進行購買。您可以使用篩選器僅檢視適合您的組織和資訊安全系統要求的那些解決方案。選擇解決方案後，Kaspersky Next XDR Expert會將您重新導向到卡巴斯基網站上的相關網頁，以了解有關該解決方案的更多資訊。每個網頁都可讓您繼續購買或包含有關購買流程的指示。

在 **市場** 區段，您可以使用以下條件篩選 Kaspersky 解決方案：

- 您想要防護的裝置（端點、伺服器和其他類型的資產）數量：
  - 50–250
  - 250–1000
  - 大於 1000

- 貴組織資訊安全團隊的成熟度：

  - **基金會**

    此級別對於只有一個 IT 團隊的企業來說很典型。自動封鎖最大可能數量的威脅。

  - **最佳**

    此級別對於在 IT 團隊內具有特定 IT 安全功能的企業很典型。在此級別，公司需要能夠讓他們應對商品威脅和繞過現有預防機制的威脅的解決方案。

  - **專家**

    此級別對於具有復雜和分佈式 IT 環境的企業來說很典型。IT 安全團隊成熟或公司有 SOC（安全運營中心）團隊。所需解決方案使公司能夠應對複雜的威脅和有針對性的攻擊。

- 您想要防護的資產類型：

  - **端點**：員工工作站、實體和虛擬機、內嵌系統
  - **伺服器**: 實體和虛擬伺服器
  - **雲端**：公有、私有或混合雲端環境；雲端服務
  - **網路**：區域網路，IT 基礎結構
  - **服務**：Kaspersky 提供的安全相關服務

若要查找和購買 Kaspersky 業務解決方案：

1. 在主功能表中，轉至 **市場**。

   預設情況下，該區段顯示所有可用的 Kaspersky 業務解決方案。

2. 要僅檢視適合您組織的解決方案，請在篩選器中選擇所需的值。

3. 點擊您想要購買或了解更多資訊的解決方案。

您將被重新導向到解決方案網頁。您可以按照熒幕上的指示進行購買。

關於資料提供

Kaspersky Next XDR Expert處理以下資料：

- Open Single Management Platform
- Kaspersky Unified Monitoring and Analysis Platform
- 卡巴斯基安全管理中心 Linux
- 沙盒
- 端點代理程式
  有關端點代理程式傳輸的資料的詳細資訊，請參閱相應應用程式的線上說明：
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Mac

關於資料提供

本機處理的資料

Kaspersky Next XDR Expert旨在即時優化威脅偵測、事件調查、威脅回應（包括自動回應）和主動威脅搜尋。

Kaspersky Next XDR Expert 執行下列主要功能：

- 接收、處理及儲存資訊安全事件
- 分析傳入資料並建立關聯
- 事件和警示調查，手動響應。
- 使用預訂和自訂常規程式自動回應。
- 基於事件的即時威脅搜尋。

為執行其主要功能，Kaspersky Next XDR Expert 可接收、儲存及處理以下資訊：

- 有關安裝了所有Kaspersky Next XDR Expert元件的裝置的資訊：
  - 裝置名稱、MAC 位址、作業系統供應商、作業系統組建編號、作業系統核心版本、所需的已安裝套件、帳戶權限、服務管理工具類型及連接埠狀態。這些資料由Kaspersky Deployment Toolkit在安裝過程中取得。
  - IPv4 位址。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。

- 用於存取安裝了 Kaspersky Next XDR Expert 元件之裝置的帳號名稱和 SSH 金鑰。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。
- Kaspersky Next XDR Expert帳號名稱和密碼。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。
- 資料庫存取資料：IP/DNS名稱、連接埠、使用者名稱和密碼。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。
- KUMA清查檔案和產品授權金鑰。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。
- DNS區域。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。
- 用於受管理裝置安全連線至 Open Single Management Platform 元件的憑證。這些資料由使用者在Kaspersky Deployment Toolkit組態檔中指定。
- 資訊保存在安裝日誌中，該日誌儲存在Kaspersky Deployment Toolkit資料庫中。初始基礎設施的安裝日誌會儲存到使用者裝置上的檔案。初始基礎設施的安裝日誌會儲存到使用者裝置上的檔案。儲存期限沒有限制；解除安裝解決方案時，安裝日誌檔案將被刪除。使用者名稱和密碼以加密格式儲存。
- 有關事件狀態模型的資訊，包括預定義模型。
- 有關事件類型的資訊：事件類型名稱、描述和其他一般資訊。
- 有關使用者帳戶的資訊：全名和電子郵件地址。使用者在OSMP主控台中輸入資料。資料儲存在資料庫中，直到使用者將其刪除。
- 整合權杖資料。
- 有關租用戶的資訊：租用戶名稱、父租用戶名稱、描述。使用者在OSMP主控台中輸入資料。資料儲存在資料庫中，直到使用者將其刪除。
- 憑證資訊：作為端點代理的應用程式的用戶端憑證、OSMP伺服器憑證、KUMA收集器伺服器憑證。
- 組織網路中裝置的資訊。
  - 相關整合設定完成後，OSMP將接收資料。您可以透過以下方式新增資產：
    - 匯入資產：
      - 按需從 MaxPatrol VM 匯入。
      - 依排程從Kaspersky Security Center Core和Kaspersky Industrial CyberSecurity for Networks匯入。
    - 透過OSMP主控台或API手動建立資產。
  - OSMP儲存以下裝置資訊：
    - 技術特性（一般內容、作業系統、硬體詳情和已安裝的卡巴斯基應用程式）。
    - 偵測到的弱點和裝置防護狀態。
    - 特定來源資料。

- 裝置類別及其緊急等級；
- AI評分和狀態。

- 警示和事件資料：
  - 警示資訊：觸發的規則、與 MITRE 矩陣的對應關係、警示狀態、處理結果、指派的操作員或群組、受影響的資產（裝置和帳戶）、可觀察項目（IP 位址、MD5、SHA256、URL、DNS 網域或 DNS 名稱、使用者名稱、主機名稱）、CII 裝置在警示中的涉及情況、註解和變更記錄、檔案。這些資訊是根據從Kaspersky Unified Monitoring and Analysis Platform取得的關聯事件，在OSMP主控台中自動產生的。
    - 根據警示類型，也會儲存其他資料：
      - 對於根據檔案掃描結果產生的警示：掃描檔案的名稱和雜湊值；反惡意軟體防護和沙盒判定結果；有關沙盒分析期間檔案觸發的本機檔案操作和網路活動的資訊；包含掃描檔案物件的受密碼保護的容器；
      - 對於卡巴斯基TAA（IOA）規則產生的警示：有關觸發的IOA規則、IOA規則描述、回應建議以及誤報的可能原因的資訊（規則資訊不是由使用者提供的，而是由卡巴斯基分發的）；
      - 對於IOC偵測技術產生的警示：觸發的IOC規則的名稱和嚴重等級；IOC裝置掃描期間偵測到的物件，包括IP位址、DNS記錄、登錄檔金鑰和值、路由表事項、進程和檔案資訊、服務詳情以及用戶名和ID；
      - 對於YARA偵測技術產生的警示：觸發的YARA規則的名稱和嚴重等級；在裝置YARA掃描期間偵測到的物件，包括檔案和進程資訊。
  - 事件資訊：關聯的警示、子事件、觸發的規則、與 MITRE 矩陣的對應關係、事件狀態、處理結果、指派的操作員或群組、受影響的資產（裝置和帳戶）、可觀察項目（來自警示）、CII 裝置在事件中的涉及情況（包括調查圖譜上的註解）、變更記錄、檔案、事件類型、用於事件排序、回應及解決的指標，以及觸發的 IOA 規則的詳細資訊，包括規則名稱、描述、回應建議和可能造成誤報的原因。這些資訊依據規則在OSMP主控台中自動產生，或由使用者手動產生。
  - 用於從警示產生事件的分段規則設定資料：名稱和規則觸發條件、新事件名稱範本、規則描述、規則啟動優先順序、繼承選項和繼承範圍。使用者在OSMP主控台中輸入資料。
  - 通知範本資訊：範本名稱、訊息主旨、訊息本文範本、範本描述、觸發時會傳送通知的偵測規則、選定要通知使用者的偵測技術，以及警示和事件的嚴重程度。使用者在OSMP主控台中輸入資料。
- 警示和事件的到期日期設定。
- 事件調查圖表和進程樹。OSMP儲存有關為事件建置的進程樹的下列使用者定義資訊：已建立的進程樹的名稱和備注。
- 常規程式資料：
  - 常規程式操作資料，包括回應操作參數資料：名稱、描述、標籤、觸發器和演算法。使用者在OSMP主控台中輸入資料。
  - 常規程式中執行回應操作的資料：來自整合系統的資料、來自裝置的資料。
  - 所有警示和事件的完整回應歷程記錄，包括未與警示或事件相關聯的回應操作。

上面列出的資料將在資料庫中儲存三天，然後刪除。解除安裝Kaspersky Next XDR Expert時，資料將會完全刪除。

- 存取共用資源的憑證。這些憑證以加密形式儲存，並分發到裝置以支援回應操作，例如獲取記憶體轉儲和磁碟映像。

- 透過回應操作從裝置取得或由使用者手動上傳的檔案資訊，包括檔案名稱或檔案完整路徑、大小、雜湊值、租用戶、來源裝置或上傳檔案的使用者、描述、掃描狀態（防毒、YARA、沙箱）和掃描結果。

- 關於套用至裝置的預防規則的資訊。這包括規則名稱、雜湊值、租用戶、規則套用的裝置、規則狀態（啟用或停用）以及執行與預防規則相符的檔案時通知終端使用者的選項。

- 關於用於掃描裝置的YARA規則的資訊。這包括規則名稱、租戶、描述和檔案掃描選項（啟用或停用），該選項決定在伺服器端掃描從裝置取得或使用者上傳的檔案時是否套用該規則。這些規則以檔案的形式儲存在OSMP物件儲存體中，並在執行YARA掃描回應操作時傳遞給端點。

- 關於用於掃描裝置的IOC規則的資訊。這包括規則名稱、嚴重等級、租用戶和排定掃描選項（啟用或停用）。這些規則以檔案的形式儲存在OSMP物件儲存體中，並在執行IOC掃描回應操作時傳遞給端點。對於排定的掃描，掃描排程也會傳遞給端點，其中包括啟用和停用選項、掃描開始時間和最大掃描持續時間。

- 檔案物件掃描設定，包括用於存檔解密的常用用戶端密碼目錄以及資產管理和沙盒資料庫的更新來源。這些設定由使用者在OSMP主控台中配置。

- 在OSMP中使用KPSN時，將處理下列資料：部署KPSN API的伺服器名稱或IP位址，以及用於連線API的憑證。

- 整合設定資料（卡巴斯基解決方案或服務，以及參與Kaspersky Next XDR Expert場景的協力廠商解決方案）：

  - Kaspersky Threat Intelligence Portal整合：用於連接到Kaspersky Threat Intelligence Portal的API存取權杖、快取保存週期、連線是否透過代理程式或服務類型。使用者在OSMP主控台中輸入資料。

  - KATA和KEDR整合：KATA和KEDR伺服器位址：IP位址或主機名稱、連接埠、用於連線到KATA和KEDR的唯一ID、憑證檔案以及用於連線到KATA和KEDR的私鑰。使用者在OSMP主控台中輸入資料。

  - 連線到將執行自訂指令碼的主機：IP位址或主機名稱、連接埠、使用者名稱和SSH金鑰以及密碼或金鑰。使用者在OSMP主控台中輸入資料。

  - OSMP管理伺服器整合：管理伺服器名稱，以及層次結構中管理伺服器的完整路徑。使用者在OSMP主控台中輸入資料。

  - Kaspersky CyberTrace整合： Kaspersky CyberTrace可用的IPv4位址或主機名稱和連接埠、名稱和密碼。使用者在OSMP主控台中輸入資料。

  - Kaspersky Automated Security Awareness Platform（KASAP）整合：用於連線KASAP的API存取權杖、KASAP入口網站URL、KASAP管理員電子郵件以及連線是否透過代理程式。使用者在OSMP主控台中輸入資料。

  - Active Directory整合：網域控制器的位址、用於連線網域控制器的使用者名稱和密碼以及憑證。使用者在OSMP主控台中輸入資料。

  - 外部系統整合（例如UserGate）：用於遠端存取用戶端裝置的帳戶名稱和SSH金鑰或密碼。

  - 卡巴斯基沙盒的整合：部署沙盒的虛擬機器作業系統的參考組態、沙盒伺服器IP位址、沙盒伺服器憑證、OSMP主控台中顯示的伺服器名稱以及用於檔案分析的沙盒規則。使用者在OSMP主控台中輸入資料。

- 使用者連線至OSMP主控台時使用的IP位址會由主控台自動記錄，並儲存至使用者所編輯物件的修訂版本保留期屆滿為止。

- 有關OSMP安裝程式層次結構組態的資訊。

有關為執行Kaspersky Next XDR Expert的主要功能而接收、儲存及處理的其他資料的詳細資訊，請參閱應用程式說明：

- 卡巴斯基安全管理中心 15.4 Linux
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky EDR Expert

上述資料儲存在資料庫中，直到使用者將其刪除。與警示或事件相關的資料將儲存至警示或事件的整個保留期結束。所有其他資料將無限期存儲，直到用戶刪除資料或刪除與資料關聯的租用戶為止。解除安裝Kaspersky Next XDR Expert時，資料將會完全刪除。

上述所有資料只能透過Kaspersky Next XDR Expert元件的傾印檔案、偵錯檔案或記錄檔案傳送給卡巴斯基，包括安裝程式和公用程式建立的記錄檔案。Kaspersky Next XDR Expert元件的傾印文件、偵錯檔案或日誌文件包含個人或機密資料。傾印檔案、偵錯檔案或記錄檔案以非加密形式儲存在裝置上。傾印檔案、偵錯檔案或記錄檔案不會自動傳輸到卡巴斯基；但是管理員可以在技術支援要求下手動傳輸資料到卡巴斯基以便解決Kaspersky Next XDR Expert效能相關問題。卡巴斯基根據適用法律和卡巴斯基政策保護所有收到的資料。資料會透過安全的通訊通道傳輸。此類資訊的預設儲存週期（輪換期）為7天。

傳輸至 AO Kaspersky Lab 的資料

透過 OSMP 主控台的連結前往 Kaspersky Next XDR Expert 說明時，使用者即同意自動將下列資料傳輸至卡巴斯基：Kaspersky Next XDR Expert 代碼、Kaspersky Next XDR Expert 版本及 Kaspersky Next XDR Expert 當地語系。

若要為員工指派訓練課程，Kaspersky Next XDR Expert 會將下列資料傳輸至 Kaspersky Automated Security Awareness Platform：使用者電子郵件地址、Kaspersky Automated Security Awareness Platform ID、訓練群組 ID。

為了獲取其他警示資料， Kaspersky Next XDR Expert會將與警示、事件和事件相關的可觀察物件的類型和值傳輸到Kaspersky Threat Intelligence Portal。

為了獲取有關透過警示、事件或事件卡中的連結存取偵測到的威脅的評估資訊，Kaspersky Next XDR Expert會將以下資料傳輸到 Kaspersky Threats服務：名稱。

為了接收事件偵測和回應服務，Kaspersky Next XDR Expert會將以下資料傳輸至Kaspersky Managed Detection and Response 服務：

- 啟用與Kaspersky Managed Detection and Response的整合後，OSMP會臨時儲存以下資料，直到成功傳輸，並將其傳輸到Kaspersky Managed Detection and Response的基礎設施：接收規則觸發事件的裝置識別碼、使用者識別碼以及Kaspersky Managed Detection and Response客戶識別碼。
- 使用OSMP的Kaspersky Managed Detection and Response解決方案時，警示中的以下附加資訊將被傳輸到Kaspersky Managed Detection and Response的基礎設施：掃描檔案的名稱和雜湊值；反惡意軟體和沙盒偵測結果；有關檔案在沙盒分析期間生成的本機檔案操作和網路活動的資訊；包含掃描檔案物件的受密碼保護的封存檔案；以及觸發IOA規則的事件，其中可能包括裝置上的檔案和應用程式名稱、登錄檔密鑰和值以及使用者名稱。

- 使用OSMP的Kaspersky Managed Detection and Response solution解決方案時，應使用者要求將以下事件相關資訊傳輸到Kaspersky Managed Detection and Response solution的基礎設施：事件名稱；建立和上次更新的日期和時間；有關觸發規則和相關MITRE策略和技術的資訊；指派給事件的運算子的名稱；受影響裝置的名稱和識別號；以及警示中包含的事件。這些事件可能包括用戶端裝置上的檔案名稱、登錄檔密鑰名稱、應用程式名稱和使用者名稱。

  只有在使用者接受Kaspersky Managed Detection and Response資料處理協定（DPA）後，所有這些資料才會傳輸到Kaspersky Managed Detection and Response，當在其介面中啟動Kaspersky Managed Detection and Response時，該協定即被確認。

為了增強資訊保護能力， Kaspersky Next XDR Expert會將OSMP運行期間產生的KSN統計資料傳輸到Kaspersky Security Network服務。傳輸資料的範圍載明於 KSN 聲明中，該聲明包含在應用程式分發套件中。加入KSN是可選的，由OSMP使用者自行控制。傳輸前，KSN統計資料會暫時快取在託管OSMP元件的伺服器上。

使用Kaspersky Private Security Network時，KSN統計資料會快取在託管OSMP元件的伺服器上，其範圍與使用Kaspersky Security Network時相同。如果Kaspersky Private Security Network伺服器位於組織外部，則快取的KSN統計資料可能會傳送到組織外部。Kaspersky Private Security Network管理員負責確保這些資料的安全。

傳輸至協力廠商的資料

透過追蹤警示或事件詳細資訊中的連結以接收有關MITRE政策或技術的信息，以下有關MITRE政策或技術的資訊將傳輸到MITRE網站：ID和類型。

為了透過在遠端用戶端裝置上執行協力廠商指令碼，利用外部系統（例如 UserGate）執行回應操作，Kaspersky Next XDR Expert會將以下資訊傳輸到外部系統：警示和事件中觀察到的物件類型和值。

為了在點選事件卡的連結時檢查檔案和URL的聲譽，Kaspersky Next XDR Expert將以下資訊傳輸到VirusTotal服務：檔案雜湊值（FileMd5和FileSha256）；遠端主機名（NetUrlHostname）；HTTP請求的目標URI（NetUri）；目標IPv4或IPv6地址（NetDstIp）；DNS查詢中請求的URL（DnsResourceName）；以及請求的DNS伺服器（DnsServerIp）。

Kaspersky Unified Monitoring and Analysis Platform中的資料提供

傳輸至協力廠商的資料

KUMA功能不涉及自動向協力廠商提供使用者資料。

本機處理的資料

Kaspersky Unified Monitoring and Analysis Platform（以下簡稱KUMA或「程式」）是一個整合軟體解決方案，包括以下主要功能：

- 接收、處理及儲存資訊安全事件
- 分析傳入資料並建立關聯
- 搜尋已接收的事件
- 偵測到資訊安全威脅的症狀時建立通知。
- 為處理資訊安全威脅建立警示和事件。
- 在儀表板和報告中顯示有關用戶端基礎架構狀態的資訊。
- 監控事件來源。
- 裝置（資產）管理 — 檢視資產資訊、搜尋、新增、編輯及刪除資產，以及將資產資訊匯出至 CSV 檔案。

若要執行其主要功能，KUMA可能會接收、儲存和處理以下資訊：

- 企業網路上的裝置資訊。
  如果設定了相應的整合，KUMA Core伺服器將接收資料。您可以透過以下方式將資產新增至KUMA：
  - 匯入資產：
    - 按需從 MaxPatrol VM 匯入。
    - 按排程從Open Single Management Platform和KICS for Networks匯入。
  - 透過網頁介面或API手動建立資產。

  KUMA儲存以下裝置資訊：
  - 裝置的技術特性。
  - 在資產上偵測到的弱點。
  - 特定於資產來源的資訊。
- 使用者為將事件傳送至 NCIRCC 而指定的企業網路裝置其他技術屬性：IP 位址、網域名稱、URI、受監控物件的電子郵件地址、遭受攻擊的網路服務，以及連接埠/通訊協定。
- 組織資訊：名稱、稅號、地址、用於傳送通知的電子郵件地址。
- 透過查詢Active Directory網路而獲得的有關組織單位、網域、使用者和群組的Active Directory資訊。
  如果設定了相應的整合，KUMA Core伺服器將收到此資訊。為確保與LDAP伺服器連線的安全性，使用者必須在KUMA主控台中輸入伺服器URL、Base DN、連線憑證和憑證。

- KUMA中使用者網域驗證的資訊：用於在Active Directory目錄服務中搜尋存取群組的根DN、網域控制器的URL、憑證（用於簽署AD憑證的根公開金鑰）、AD中使用者存取群組的完整路徑（可分辨名稱）。

- 來自已設定來源的事件中所包含的資訊。

  在收集器中，設定事件來源，產生KUMA事件並將其傳送到其他KUMA服務。有時事件可能首先到達代理服務，該服務將事件從來源中繼到收集器。此外，您也可以設定儲存彙總事件的伺服器的位址或主機名稱。

  此外，端點代理程式會根據事件資料模型向OSMP發送有關事件的資訊。

- KUMA與其他應用程式（Kaspersky Threat Lookup，Kaspersky CyberTrace，Open Single Management Platform，Kaspersky Industrial CyberSecurity for Networks，Kaspersky Automated Security Awareness Platform，Kaspersky Endpoint Detection and Response，Security Orchestration，Automation and Response，AI服務: AI asset score and status，Kaspersky Investigation and Response Assistant）整合所需的資訊。

  它可以包括憑證、令牌、URL或用於與其他應用程式建立連線的憑證，或KUMA基本功能所需的其他資料，例如電子郵件。使用者在KUMA主控台中輸入此資料

- 有關設定事件接收的來源的資訊。

  它可以包括來源名稱、主機名稱、IP 位址、指派給來源的監控政策。監控政策指定負責人的電子郵件地址，如果違反政策，將向其傳送通知。

- 使用者帳戶：姓名、使用者名稱、電子郵件地址。使用者可以在KUMA主控台中檢視其描述檔。

- 使用者描述檔設定：

  - KUMA中的使用者角色。使用者可以看到自己被指派的角色。

  - 在地化語言、通知設定、非列印字元的顯示。

    使用者在KUMA介面中輸入此資料。

  - **資產**部分中的資產類別清單、預設儀表板、儀表板的TV模式旗標、預設事件的SQL查詢、預設設定。

    使用者在KUMA主控台的相應部分中指定這些設定。

- KUMA中使用者網域驗證的資料：

  - Active Directory：用於在Active Directory目錄服務中搜尋存取群組的根DN、網域控制站的URL、憑證（AD憑證簽署的根公開金鑰）、AD 中使用者存取群組的完整路徑（可分辨名稱）。

  - Active Directory聯合驗證服務：可信任方ID（AD FS中的KUMA ID）、用於取得Connect元資料的URI、用於從AD FS重新導向的URL以及AD FS伺服器憑證。

  - FreeIPA：Base DN、URL、憑證（用於簽署FreeIPA憑證的公鑰根金鑰）、自訂整合憑證、連線憑證。

- 稽核事件

  KUMA自動記錄稽核事件。

- KUMA日誌

  使用者可以在KUMA主控台中啟用延伸日誌記錄。日誌條目儲存在使用者的裝置上，不會自動傳輸任何資料。

- 有關使用者接受與卡巴斯基法律協議的條款和條件的資訊。

- 使用者在KUMA介面中輸入的任何資訊。

以上列出的資訊可以透過以下方式進入KUMA：

- 使用者在KUMA主控台中輸入資訊。
- 如果使用者設定了與事件來源的連線，KUMA服務（代理或收集器）將接收資料。
- 透過KUMA REST API。
- 可以使用 MaxPatrol VM 的公用程式獲取裝置信息。

列出的資訊儲存在KUMA資料庫（MongoDB、 ClickHouse、SQLite）中。密碼以加密形式儲存（儲存密碼的雜湊值）。

上列所有資料只能透過KUMA元件的傾印檔案、偵錯檔案或記錄檔案傳輸至卡巴斯基，包含安裝程式和公用程式建立的記錄檔案。

KUMA元件的傾印檔案、偵錯檔案和日誌文檔可能包含個人和機密資訊。傾印檔案、偵錯檔案和記錄檔案以非加密形式儲存在裝置。傾印檔案、偵錯檔案和日誌文檔不會自動提交給卡巴斯基，但管理員可以根據技術支援部門的請求手動將這些資訊提交給卡巴斯基，以有助於解決KUMA問題。

卡巴斯基會以匿名形式使用所收集的資料，且僅用於一般統計目的。系統會根據接收到的原始資料自動產生彙總統計資料，其中不包含任何個人資訊或其他機密資訊。當新資料彙總時，舊資料會被刪除（每年一次）。彙總統計資料會無限期儲存。

卡巴斯基根據適用法律和卡巴斯基政策保護所有收到的資料。資料會透過安全的通訊通道傳輸。

沙盒中的資料提供

透過沙盒元件儲存在伺服器上的資料：

- 已掃描檔案：`/var/opt/kaspersky/sandbox/library/`。
- 檔案掃描結果：`/var/opt/kaspersky/sandbox/library/` 以及 `/tmp/`。
- 任務設定：`/var/opt/kaspersky/sandbox/library/` 以及沙盒元件資料庫。
- 偵錯檔案：`/var/log/kaspersky/sandbox/`。
- 更新來源設定：`/var/opt/kaspersky/apt-updater`。
- 密碼最小長度設定：`/var/opt/kaspersky/apt-config-ram-common/validator.conf`。
- 虛擬機器：`/vm`。
- 已下載的 iso 格式作業系統與應用程式映像：`/var/opt/kaspersky/sandbox/custom_images/iso`。

正在啟動

以下場景是從購買Kaspersky Next XDR Expert到事件調查和威脅搜尋的逐步指南。

首先安裝並初步設定Kaspersky Next XDR Expert ，然後探索Kaspersky Next XDR Expert威脅偵測與搜尋功能，最後查看事件調查工作流程的範例。

Kaspersky Next XDR Expert的部署和初始設定

依照此場景，您可以部署Open Single Management Platform以及執行Kaspersky Next XDR Expert解決方案所需的所有元件，然後執行所需的初步組態和整合。

先決條件

在開始之前，請確保：

- 您擁有Kaspersky Next XDR Expert和相容EPP應用程式的授權金鑰。
- 您的基礎架構滿足硬體和軟體需求。

階段

主要安裝和初始設定情境分階段進行：

1. **部署**

   準備好部署Open Single Management Platform和Kaspersky Next XDR Expert所需的所有元件的基礎架構，然後使用Kaspersky Deployment Toolkit公用程式佈署該解決方案。

2. **啟動**

   在您的產品授權下啟動Kaspersky Next XDR Expert解決方案。

3. **多租戶設定**

   如果需要，您可以使用多租用戶功能：

   1. 規劃並建立所需的租用戶層級結構。
   2. 在Open Single Management Platform中建立相符的管理伺服器層級結構。
   3. 將租用戶綁定到相應的管理伺服器。
   4. 為所有Kaspersky Next XDR Expert使用者建立使用者帳戶，然後指派角色。

4 新增資產

您的基礎架構中必須保護的裝置在Kaspersky Next XDR Expert中表示為資產。Open Single Management Platform可讓您發現網路中的裝置並管理其防護。您也可以在第8階段手動新增資產或從其他來源匯入資產。

使用者帳號在Kaspersky Next XDR Expert中也表示為資產。確保在第9階段配置與Active Directory的整合，以便在相關事件、警示和事件中顯示受影響的使用者帳戶。

5 新增使用者和指派角色

為使用者帳戶指派角色，根據他們的工作定義他們對各項Kaspersky Next XDR Expert功能的存取權限。

6 連線到SMTP伺服器

設定與SMTP伺服器的連線，以便透過電子郵件通知有關Kaspersky Next XDR Expert中發生的事件。

7 安裝端點防護應用程式和解決方案

Kaspersky Next XDR Expert處理從您資產上安裝的安全應用程式接收到的事件。檢查相容的卡巴斯基應用程式和解決方案清單。您可以使用Open Single Management Platform在您基礎架構的裝置上部署卡巴斯基應用程式。

確保端點保護應用程式與Kaspersky Anti Targeted Attack Platform整合。例如，如果您在資產上使用Kaspersky Endpoint Security，請參閱以下說明文件之一，了解如何設定與KATA的整合：

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

8 設定事件來源、儲存和關聯

指定事件的接收來源，以及事件的儲存和處理方式：

1. 登入KUMA主控台。
2. 設定Kaspersky Unified Monitoring and Analysis Platform與卡巴斯基安全管理中心的整合。
3. **從Open Single Management Platform匯入資產**。

   受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

   KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

   - 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
   - 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

   若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

   1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
   2. 按一下**匯入**，然後選擇以下操作之一：

      - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。

        這將開啟**匯入KSC資產**視窗。

- 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。

  這將開啟**匯入KSC資產屬性**視窗。

3. 在下拉清單，選取要為其執行匯入的租用戶。

   在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。

   如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。

4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

4. 手動新增資產，或從其他來源匯入資產（選用）。

5. 設定事件來源以指定您想要從中接收事件的位置。

6. 建立儲存區以儲存事件。

7. 建立收集器以接收、處理（正規化）及傳輸事件。

8. 建立關聯器，以對正規化事件進行初步分析及進一步處理。

   在建立關聯器期間，您可以建立關聯規則來定義處理和回應事件的規則。您也可以匯入先前儲存的關聯規則或使用Kaspersky Next XDR Expert解決方案提供的現成關聯規則集。建立相關器後，您可以根據需要將關聯規則連結到相關器。

   > 建議在此階段設定排除項目，以避免誤報和無關資料。

9 設定整合

設定Kaspersky Next XDR Expert與Active Directory以及其他卡巴斯基解決方案的整合，以擴展其潛力並擴充可用於事件調查的資料。

1. 與Active Directory整合（強烈推薦）。

2. 與KATA/EDR整合（需要產品授權）。

3. 與Kaspersky CyberTrace整合（可選整合；需要產品授權）。

4. 與Kaspersky TIP整合（可選整合；需要產品授權）或Kaspersky Open TIP整合。

5. 與Kaspersky Automated Security Awareness Platform整合（可選整合；需要產品授權）。

10 設定更新

建立下載更新到管理伺服器儲存庫工作

11 驗證組態的正確性

在其中一個資產上使用EICAR測試檔案。如果初始設定正確執行並且設定了必要的關聯規則，則此事件將觸發在警示清單中建立警示。

初始設定完成後，Kaspersky Next XDR Expert將接收並處理來自受保護資產的事件，並在觸發關聯規則時建立警示。

驗證Kaspersky Next XDR Expert組態的正確性

您可以在其中一項資產上使用EICAR 測試病毒，以確保 Kaspersky Next XDR Expert 已正確部署和設定。如果初始設定正確執行並且設定了必要的關聯規則，則此事件將觸發在警示清單中建立警示。

若要驗證Kaspersky Next XDR Expert組態的正確性

1. 在OSMP主控台的KUMA部分中建立新關聯器。

   建立關聯器時，請勿在**關聯**部分指定參數。

2. 從SOC內容包匯入關聯規則，以取得用於檢測EICAR測試病毒的預定義關聯規則。

3. 為建立的關聯器指定關聯規則。

   您可以使用下列方法之一來指定關聯規則：

   - 將預定義關聯規則連結到已建立的關聯器：

     a. 轉至**資源** ，按一下**關聯規則**，然後選擇要套用關聯規則的租用戶。

     b. 在預定義關聯規則清單中，選擇**R077_02_KSC.Malware偵測**規則，以偵測來自卡巴斯基安全管理中心的事件。

     c. 按一下**連結至關聯器**，然後選擇已建立的關聯器，將所選關聯規則連結至該關聯器。

   - 手動建立具有預定義篩選器的關聯規則：

     a. 開啟建立的關聯器設定，轉至**關聯部分**，然後按一下**新增**。

     b. 在**建立關聯規則**視窗的**一般**頁籤上，設定以下參數以及其他規則參數：

        - **型別**：簡單。
        - **已傳播欄位**：DestinationAddress、DestinationHostName、DestinationAccountID、DestinationAssetID、DestinationNtDomain、DestinationProcessName、DestinationUserName、DestinationUserID、SourceAccountID、SourceUserName。

     c. 轉至**選擇器 → 設定** ，然後指定用於篩選所需事件的運算式：

        - 在建構器模式下，新增**f: KSC事件**、**f: KSC病毒發現**和**f: 基本事件**篩選器，並使用AND運算子。
        - 或者，您也可以在原始碼模式下按以下方式指定此運算式：

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

     d. 在關聯規則設定的**操作**部分，僅選取**輸出**核取方塊（必須取消選取**循環至關聯器**和**無警示**核取方塊）。在這種情況下，當偵測到EICAR測試病毒時，將建立一個關聯事件，並在Kaspersky Next XDR Expert的警示清單中建立警報。

     e. 按一下**新建**以儲存連結到關聯器的關聯規則設定。

4. 在OSMP主控台的KUMA部分建立並設定一個收集器，用於從MS SQL資料庫接收有關管理伺服器事件的資訊。

   或者，您可以使用預定義的[OOTB] KSC SQL收集器。

5. 在收集器設定的**路由**部分，將**類型**設為**關聯器**，然後在**URL**欄位中指定建立的關聯器，以便將處理後的事件轉發至該關聯器。

6. 在組織網路的某個資產上安裝網路代理程式和端點保護應用程式（例如，Kaspersky Endpoint Security）。確保該資產已連線到管理伺服器。

7. 將EICAR測試檔案放置在該資產上，然後使用端點保護應用程式偵測測試病毒。

之後，管理伺服器將收到有關資產事件的通知。此事件將被轉發至KUMA元件，轉換為關聯事件，然後事件將觸發在 Kaspersky Next XDR Expert的警示清單中建立警示。如果警示已建立，則表示Kaspersky Next XDR Expert運作正常。

使用威脅監控、偵測和搜尋功能

安裝和設定Kaspersky Next XDR Expert後，您可以使用Kaspersky Next XDR Expert功能監控基礎架構的安全性、調查安全事件、自動化工作流程和主動搜尋威脅：

- **使用儀表板和自訂小部件**

  儀表板的偵測和回應頁籤可以包含小工具，這些小工具顯示有關偵測到和已註冊的警示和事件的資訊，以及對它們的回應操作。您可以為您的儀表板使用和自訂預設的小工具佈局，或建立新的佈局和小工具。

  Open Single Management Platform也提供各種安全監控和報告工具。

- **使用報告**

  您可以在Kaspersky Unified Monitoring and Analysis Platform中設定生成報告，以便根據指定的排程接收所需的摘要資料。

- **使用威脅搜尋**

  您可以使用威脅搜尋工具分析事件，以搜尋尚未自動偵測到的威脅和漏洞。威脅搜尋既可用於警示和事件調查，也可用於主動搜尋威脅。

- **使用常規程式**

  您可以使用常規程式根據指定的演算法自動回應警示和事件。您可以在各種運作模式下啟動許多預定義常規程式。您可以建立自訂常規程式。

使用Kaspersky Next XDR Expert進行事件調查的範例

此場景代表事件調查的範例工作流程。

事件調查分階段進行：

1. **向使用者指派警示**

   您可以將警示指派給自己或其他使用者。

2. **檢查觸發的關聯規則是否與警示事件的資料匹配**

   檢視有關警示的資訊，並確保警示事件資料與觸發的關聯規則相符。如果警示是誤報，請編輯關聯規則。

3. **分析警示資訊**

   分析有關警示的資訊以確定進一步分析警示所需的資料。

4. **手動擴充**

   啟動可用的解決方案，以進一步擴充事件（例如，Kaspersky TIP ）。

5. **誤報檢查**

   確保觸發關聯規則的活動對於組織IT基礎架構來說是異常的。

6. **事件建立**

   如果步驟 3 到 5 顯示警示需要調查，您可以建立事件或將警示連結至現有事件。

   您也可以合併事件。

7. **事件管理**

   您可以透過變更事件狀態和優先順序，以及將事件指派給其他分析師來管理事件。

   您還可以管理事件的SLA、類型和工作流程。此外，您還可以追蹤事件相關工作所花費的精力。

8. **調查**

   此步驟包括檢視有關與事件相關的資產、使用者帳戶和警示的資訊。您可以使用調查圖表和威脅搜尋工具來獲取更多資訊。

9. **搜尋相關資產**

   您可以檢視與事件相關的資產上發生的警示。

10. **搜尋相關事件**

    您可以透過搜尋相關警示的事件來伸調查範圍。

11. **查看事件歷史記錄**

    您可以查看事件的變更日誌和回應記錄。

12. **備注**

    您可以留下備注，提供事件調查所需的資訊。

13. **回應**

    您可以手動執行回應操作。

14. **使用常規程式進行回應**

    您可以透過手動啟動常規程式來回應事件。

15. **關閉事件**

    在採取措施清除組織IT基礎架構中攻擊者存在的痕跡後，您可以關閉事件。

Kaspersky Next XDR Expert的部署

依照此情境，您可以準備基礎設施以部署Open Single Management Platform和Kaspersky Next XDR Expert（包含Kaspersky Endpoint Detection and Response功能）所需的所有元件，準備包含安裝參數的組態檔，並使用Kaspersky Deployment Toolkit公用程式（以下簡稱KDT）部署解決方案。

在部署Open Single Management Platform和Kaspersky Next XDR Expert元件之前，建議您閱讀硬化指南 。

此部署情境分幾個階段進行：

1. **選擇部署Kaspersky Next XDR Expert的選項**

   選擇最適合您組織的Kaspersky Next XDR Expert配置。有多節點部署和單節點部署可供選擇。

2. **下載包含Kaspersky Next XDR Expert元件的分發套件**

   分發套件包含以下元件：

   - 包含Kaspersky Next XDR Expert元件和Kaspersky Next XDR Expert和KDT最終使用者產品授權協議的傳輸存檔

     這些元件使用RSA金鑰和GOST R 34.11-2012金鑰進行簽署。您可以驗證Kaspersky Next XDR Expert元件的真實性和完整性。

   - 使用KDT公用程式進行歸檔，以及組態檔和KUMA清單檔案的範本。

3. **安裝資料庫管理系統 (DBMS)**

   對於多節點部署，請在Kubernetes叢集以外的獨立伺服器上手動安裝DBMS。

   對於單節點部署，請在部署Kaspersky Next XDR Expert之前在目標主機上手動安裝DBMS。在這種情況下，DBMS和Kaspersky Next XDR Expert元件會安裝在相同目標主機上，但DBMS不包含在Kubernetes叢集中。

4. **準備管理員和目標主機**

   根據所選的部署方案，定義將在其上部署Kubernetes叢集以及該叢集中包含的Kaspersky Next XDR Expert元件的目標主機數量。準備所選的管理員和目標主機以部署Kaspersky Next XDR Expert。

   操作說明：

   - 多節點佈署：準備管理員主機和目標主機
   - 單節點部署：準備管理員主機和目標主機

5. **準備KUMA主機以在Kubernetes叢集外部安裝KUMA服務（可選）**

   KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部，也可以完全安裝在叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在叢集外部。

   如果您希望將KUMA服務完全安裝在Kubernetes叢集外部的獨立主機上，或部分安裝在叢集內部，部分安裝在叢集外部，請準備KUMA目標主機以安裝KUMA服務。

   操作說明：準備KUMA主機以在Kubernetes叢集外部安裝KUMA服務

6 準備KUMA清查檔案以在Kubernetes叢集外部安裝KUMA服務（可選）

如果您希望將KUMA服務完全安裝在Kubernetes叢集外部的獨立主機上，或部分安裝在叢集內部，部分安裝在叢集外部，請準備YAML格式的KUMA清查檔案。KUMA清查檔案包含在Kubernetes叢集之外安裝KUMA服務的參數。

操作說明：準備KUMA清查檔案以在Kubernetes叢集外部安裝KUMA服務

7 準備組態檔

準備YAML格式的組態檔。組態檔包含部署目標主機列表和Kaspersky Next XDR Expert元件的安裝參數集。

如果您在單一節點上部署Kaspersky Next XDR Expert，請使用包含特定於單節點部署的安裝參數的組態檔。

說明：

- 多節點部署：指定安裝參數
- 單節點部署：指定安裝參數

您可以手動填寫組態檔範本；或使用部署精靈指定Kaspersky Next XDR Expert部署所需的安裝參數，然後產生組態檔。

操作說明：使用部署精靈指定安裝參數

8 Kaspersky Next XDR Expert的部署

使用KDT部署Kaspersky Next XDR Expert。Kaspersky Deployment Toolkit會自動部署Kubernetes叢集，並在該叢集內安裝OSMP元件和其他基礎設施元件。

操作說明：安裝Kaspersky Next XDR Expert

9 安裝KUMA服務

安裝KUMA服務（收集器、關聯器和儲存體）。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部，也可以完全安裝在叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在叢集外部。

操作說明：在Kubernetes叢集外部安裝KUMA服務

操作說明：在Kubernetes叢集內安裝KUMA服務

10 新增從屬管理伺服器

從屬管理伺服器是進一步整合端點代理程式所必需的。

操作說明：新增從屬管理伺服器

11 安裝和整合端點代理程式

根據端點代理程式說明文件安裝端點代理程式：

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

設定與端點代理程式的整合。

12 安裝和整合沙盒

安裝沙盒，進行設定，然後在其中使用安裝程式安裝虛擬機器。

設定與沙盒的整合。

硬化指南

強化指南適用於部署和管理 Kaspersky Next XDR Expert 的專業人士，以及為使用 Kaspersky Next XDR Expert 的組織提供技術支援的人員。

硬化指南描述了配置Kaspersky Next XDR Expert及其元件的建議和功能，旨在降低其危害的風險。

硬化指南包含以下資訊：

- 準備Kaspersky Next XDR Expert部署的基礎設施
- 設定與Kaspersky Next XDR Expert的安全連線
- 設定帳戶以存取Kaspersky Next XDR Expert
- 管理Kaspersky Next XDR Expert的防護
- 管理用戶端裝置防護
- 配置受管理應用程式的防護
- 將資訊傳輸到協力廠商應用程式

在開始部署Kaspersky Next XDR Expert之前，建議您閱讀硬化指南。

管理Kaspersky Next XDR Expert的基礎設施

本章節介紹使用作業系統和Kaspersky Next XDR Expert正常運作所需的最小應用程式數量的一般原則。本章節也介紹最小權限原則，該原則歸根結底是零信任的概念。

管理作業系統帳戶

要使用KDT操作Kubernetes叢集，我們建議建立一個權限最低的獨立使用者。最佳方案是使用LDAP管理作業系統使用者帳戶，並具備透過LDAP撤銷使用者權限的功能。有關使用者撤銷和封鎖的具體實現，請參閱LDAP解決方案中的使用者/管理員說明。我們建議使用至少18個字元的密碼或至少包含4個單字且包含任意分隔符號的密碼短語進行使用者驗證。您也可以使用實體身份身分驗證方式（例如，權杖）。

如需更多資訊，請參閱OpenLDAP 軟體說明文件。

範例

分發套件	使用者建立命令	最少的群組/權限集
Ubuntu / Debian / Astra / Atlant	`useradd "$1" --shell /bin/bash --create-home --password "$(openssl passwd -1 "$2")"`	`usermod -aG sudo,root "$1"` 將使用者新增至 sudo 群組後，使用者無需密碼即可執行 sudo。

我們還建議保護使用者主目錄及其所有巢狀目錄，確保只有該使用者才能存取。其他使用者和使用者群組不得擁有主目錄的存取權限。

範例

在此範例中，`example_user`使用者的文件目錄位於`~/Documents`。預設（透過`useradd/adduser`和`umask 022`命令建立使用者時），目錄會以`755`權限建立。為確保只有該使用者可以存取根資料夾和所有子資料夾，`umask`會變更為`077`，且權限會明確設定為`700`。以下是命令範例，可用於驗證權限是否已正確設定（只有擁有者才有存取權限）。

```
若要顯示目錄的權限、擁有者和群組：
stat -c "%A %U %G" /home/example_user/Documents
如果權限授予正確，則預期命令輸出如下：
drwx------ example_user example_user
如果權限不符合要求，請將根目錄及其所有子目錄的權限設為700：
chmod -R 700 /home/example_user/Documents
請確保所有者是正確的用戶：
chown -R example_user:example_user /home/example_user/Documents
```

我們建議不要授予使用者主目錄中的.ssh、.kube、.config和.kdt目錄及其所有檔案的執行權限。

範例

顯示最敏感目錄的權限 - 顯示每個指定目錄的權限、擁有者和路徑：

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

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

預期命令輸出：

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

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

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

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

`drwx------` 表示權限 `700`：只有擁有者才能讀取、寫入和執行（對於目錄而言，「執行」是指進入目錄的權限，而不是執行軟體的權限）。

如果偵測到多餘的執行位，請將其從檔案中刪除：

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

如有必要，請設定更嚴格的權限（例如，`600`）：

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

作業系統的套件管理

我們建議僅安裝KDT和Kaspersky Next XDR Expert運行所需的最低限度應用程式。例如，您在Kubernetes叢集工作並不需要使用圖形使用者介面，因此我們建議不要安裝圖形軟體套件。如果已安裝，我們建議解除安裝這些軟體套件，包括Xorg或 Wayland等圖形伺服器。

我們建議您定期安裝系統軟體和Linux核心的安全性更新。我們也建議您啟用自動更新，具體操作如下：

- 對於安裝了apt套件管理器的作業系統：

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

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

- 對於使用 rpm、dnf 和 yum 套件管理器的作業系統：

  /etc/dnf/automatic.conf

  ```
  [commands]
  #  要執行的升級類型：
  # default                            = 所有可用的升級
  # security                           = 僅限安全性升級
  upgrade_type = default
  # 是否應在更新可用時下載更新，由
  # dnf-automatic.timer 執行。notifyonly.timer、download.timer 以及
  # install.timer 會覆寫此設定。
  download_updates = yes
  # 是否應在更新可用時套用更新，由
  # dnf-automatic.timer 執行。notifyonly.timer、download.timer 以及
  # install.timer 會覆寫此設定。
  apply_updates = no
  ```

作業系統安全性設定

Linux 核心安全性設定可在 `/etc/sysctl.conf` 檔案中啟用，或使用 `sysctl` 命令啟用。建議的 Linux 核心安全性設定列於 `/etc/sysctl.conf` 檔案片段中：

/etc/sysctl.conf

```
# 停用 execshield
kernel.randomize_va_space=2
# 啟用 IP 位址欺騙防護
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
# 忽略廣播網路請求
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_responses=1
# 啟用網路欺騙封包的記錄
net.ipv4.conf.all.log_martians=1
# 隱藏核心指標
kernel.kptr_restrict=1
# 限制對核心記錄的存取
kernel.dmesg_restrict = 1
# 禁止非特權使用者進行核心效能分析
kernel.perf_event_paranoid=3
# 增加 ASLR 熵位元
```

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

建議限制對 PID 的存取。這將降低一位使用者追蹤另一位使用者的處理程序的可能性。您可以在掛載 `/proc` 檔案系統時限制對 PID 的存取，例如，將以下行新增至 `/etc/fstab` 檔案：

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

若作業系統處理程序是透過 `systemd` 系統管理，`systemd-logind` 服務仍可監控其他使用者的處理程序。為了讓使用者工作階段在 `systemd` 系統中正常運作，您需要建立 `/etc/systemd/system/systemd-logind.service.d/hidepid.conf` 檔案，然後將以下幾行新增至該檔案：

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

由於某些系統可能沒有 `proc` 群組，建議預先新增 `proc` 群組。

建議停用 **`ctrl`** + **`alt`** + **`del`** 按鍵組合，以防透過 `systemctl mask ctrl-alt-del.target` 命令意外重新啟動作業系統。

我們建議您禁止特權使用者（根使用者）身分驗證以建立遠端使用者連線。

範例

下面這組指令可以同時阻止root使用者透過網路登入並將其排除在LDAP身分驗證之外。

```
# 1&period; SSH

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

sudo systemctl restart sshd

# 2&period; Local account

sudo passwd -l root

sudo usermod -s /usr/sbin/nologin root

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

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

if [ -f "$LDAP_CONF" ]; then

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

sudo systemctl restart ksc-orchestrator

fi

# 4&period; Sudo without NOPASSWD
```

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

我們建議您使用防火牆來限制網路活動。有關所用連接埠和協定的更多資訊，請參閱Kaspersky Next XDR Expert所使用的連接埠。

範例

操作	ufw (Ubuntu/Debian)	firewalld (RHEL/CentOS)	iptables
檢查狀態	ufw status	firewall-cmd --list-all	iptables -L -n
檢查連接埠	ss -tuln | grep 443	ss -tuln | grep 443	ss -tuln | grep 443
外部稽核	nc -zv IP 443	nc -zv IP 443	nc -zv IP 443
開啟連接埠	ufw allow 443/tcp	firewall-cmd --add-port=443/tcp --permanent + --reload	iptables -A INPUT -p tcp --dport 443 -j ACCEPT
關閉連接埠	ufw deny 443/tcp	firewall-cmd --remove-port=443/tcp --permanent + --reload	iptables -A INPUT -p tcp --dport 443 -j DROP
儲存規則	Auto	自動	iptables-save > /etc/iptables/rules.v4

建議啟用 `auditd`，以簡化安全事件的調查。有關啟用遙測重定向的更多資訊，請參閱設定接收Auditd事件。

我們建議您定期備份以下組態和資料目錄：

- 管理主機：`~/kdt`
- 目標主機：`/etc/k0s/`、`/var/lib/k0s`

此外，我們也建議您對這些備份進行加密。

各種作業系統和DBMS的硬化指南

若要配置作業系統和軟體的安全性設定，您可以參考網路安全中心（CIS）提供的建議。

如果您使用Astra Linux作業系統，請參閱可套用至您的Astra Linux版本的安全建議。

若要配置PostgreSQL的安全性設定，請參考PostgreSQL官方說明文件中的伺服器管理建議。

連線安全

嚴格的 TLS 設定

建議使用 1.2 及以後版本的 TLS 協定，限製或禁止不安全的加密演算法。

您可以設定管理伺服器使用的加密協定（TLS）。請注意，在發佈Kaspersky Next XDR Expert版本時，加密協定設定預設設定，以確保資料傳輸安全。

限制對Kaspersky Next XDR Expert資料庫的存取

我們建議限制對Kaspersky Next XDR Expert資料庫的存取。例如，僅授予部署了Kaspersky Next XDR Expert的裝置的存取權限。這會降低Kaspersky Next XDR Expert資料庫因已知漏洞而受損的可能性。

您可以根據所用資料庫的操作說明設定參數，也可以在防火牆上提供關閉的連接埠。

帳戶和身分驗證

使用Kaspersky Next XDR Expert的雙步驟驗證

Kaspersky Next XDR Expert 提供以 RFC 6238 標準（以時間為基礎的一次性密碼 (TOTP) 演算法）為基礎的使用者**雙因素驗證**功能。

為您自己的帳戶啟用雙因素驗證後，每次透過瀏覽器登入 Kaspersky Next XDR Expert 時，都必須輸入使用者名稱、密碼和額外的一次性安全碼。若要接收一次性使用的安全碼，您必須在電腦或行動裝置上安裝身份驗證器應用程式。

有支援 RFC 6238 標準的軟體和硬體驗證器（權杖）。例如，軟體驗證器包括 Google Authenticator、Microsoft Authenticator、FreeOTP。

我們強烈建議不要在與Kaspersky Next XDR Expert建立連線的同一台裝置上安裝驗證器應用程式。您可以在行動裝置上安裝驗證器應用程式。

對作業系統使用雙重身分驗證

我們建議在部署了Kaspersky Next XDR Expert的裝置上，透過使用權杖、智慧卡或其他方法（如果可能）進行多重身份驗證（MFA）。

禁止儲存管理員密碼

如果您透過瀏覽器使用Kaspersky Next XDR Expert，我們建議不要將管理員密碼儲存在使用者裝置上安裝的瀏覽器中。

內部使用者帳戶的身分驗證

預設情況下，Kaspersky Next XDR Expert內部使用者帳戶的密碼必須遵守以下規則：

- 密碼必須是 10 到 256 位字元長度。

- 密碼必須包含以下組中三組的字元：
  - 大寫字母（A-Z）
  - 小寫字母 (a-z)
  - 數字（0-9）
  - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密碼不可以包含任何空白、Unicode 字元或 "." 和「@」的組合，並且「@」前不可有「.」。

預設下，允許的最大密碼輸入嘗試次數是 3。此數字是固定的，無法更改。

使用者可以輸入無效密碼的次數有限。達到限制後，使用者帳戶被鎖定一小時。

限制指派主管理員角色

使用者在 Kaspersky Next XDR Expert 的存取控制清單（ACL）中獲指派主管理員角色。我們不建議將主管理員角色指派給大量使用者。

設定應用程式功能的存取權限

我們建議為每個使用者或使用者組使用Kaspersky Next XDR Expert功能的存取權限的靈活組態。

基於角色的存取控制可讓您使用一群組預先定義的權限建立標準使用者角色並根據使用者的職責範圍將這些角色分配給使用者。

角色型存取控制模型的主要優點：

- 易於管理
- 角色層次結構
- 最少特權方法
- 職責分離

您可以根據職位為某些員工分配內建角色，或建立全新的角色。

設定角色時，需要注意與變更Kaspersky Next XDR Expert裝置的防護狀態以及遠端安裝協力廠商軟體相關聯的權限：

- 對管理群組進行管理。
- 管理伺服器操作
- 遠端安裝

- 變更用於儲存事件和傳送通知的參數。

  此權限允許您設定當事件發生時在OSMP裝置上執行指令碼或可執行模組的通知。

為遠端安裝應用程式使用單獨的帳戶

除了基本的存取權限區分之外，我們建議限制所有帳戶（主管理員或其他專用帳戶除外）遠端安裝應用程式。

我們建議為遠端安裝應用程式使用單獨的帳戶。你可以分配角色或者權限給單獨帳戶。

定期稽核所有使用者和使用者的操作

我們建議對部署了Kaspersky Next XDR Expert的裝置上的所有使用者進行定期稽核。這使您能夠應對與裝置可能受到危害相關的某些類型的安全威脅。

另外，您還可以追蹤使用者的操作，例如連線到管理伺服器和斷開連線、連線到管理伺服器時發生錯誤以及物件修改（適用於支援修訂管理的物件）。

管理Kaspersky Next XDR Expert的防護

選擇Kaspersky Next XDR Expert的防護軟體

根據Kaspersky Next XDR Expert的部署類型和一般防護政策，選擇應用程式來防護佈署了Kaspersky Next XDR Expert的裝置和管理員。

如果您在專用裝置上部署Kaspersky Next XDR Expert，我們建議選擇Kaspersky Endpoint Security應用程式來防護部署了Kaspersky Next XDR Expert和管理員主機的裝置。這可讓您套用所有可用技術來防護這些裝置，包括行為分析模組。

如果Kaspersky Next XDR Expert安裝在基礎結構的裝置上並且之前曾用於其他工作，我們建議考慮以下防護軟體：

- Kaspersky Industrial CyberSecurity for Nodes。我們建議在包含在產業網路中的裝置上安裝此應用程式。Kaspersky Industrial CyberSecurity for Nodes 是一個應用程式，具有與各種工業軟體製造商的相容性憑證。
- 推薦的安全應用程式。如果Kaspersky Next XDR Expert部署在帶有其他軟體的裝置上，我們建議考慮該軟體供應商關於安全應用程式相容性的建議（可能已經有選擇安全解決方案的建議，您可能需要配置可信區域）。

防護模組

如果與Kaspersky Next XDR Expert在同一裝置上安裝的協力廠商軟體的供應商沒有特別建議，我們建議啟動和配置所有可用的防護模組（在檢查這些防護模組的執行一段時間後）。

設定Kaspersky Next XDR Expert裝置的防火牆

在部署了Kaspersky Next XDR Expert的裝置上，我們建議設定防火牆以限制管理員可以透過瀏覽器連線至Kaspersky Next XDR Expert的裝置數量。

預設情況下，

Kaspersky Next XDR Expert使用連接埠443透過瀏覽器登入。我們建議限制使用此連接埠可以管理Kaspersky Next XDR Expert的裝置數量。

管理用戶端裝置防護

限制將產品授權金鑰新增到安裝套件

安裝套件可以透過包含在Kaspersky Next XDR Expert中的網頁伺服器來發布。如果您將產品授權金鑰新增到網頁伺服器上發佈的安裝套件中，則所有使用者都可以讀取產品授權金鑰。

為避免洩露產品授權金鑰，我們不建議將產品授權金鑰新增到安裝套件中。

我們推薦使用將產品授權金鑰自動發佈到受管理裝置，通過受管理應用程式的*新增產品授權金鑰*工作進行佈署，並手動將啟動碼或金鑰檔案新增到裝置。

在管理群組之間移動裝置的自動規則

我們建議限制使用自動規則在管理群組之間行動裝置。

如果您使用自動規則移動裝置，這可能會導致政策的傳播，這些政策為移動的裝置提供比重新定位前的裝置更多的權限。

此外，將用戶端裝置移動到另一個管理群組可能會導致政策設定的傳播。這些政策設定可能不適合發佈給訪客和不受信任的裝置。

此建議不適用於將裝置一次性初始分配給管理群組。

發佈點和連線閘道的安全要求

安裝了網路代理的裝置可以充當發佈點並執行以下函式：

- 將從Kaspersky Next XDR Expert收到的更新和安裝套件發佈到群組內的用戶端裝置。
- 在用戶端裝置上執行協力廠商軟體和卡巴斯基應用程式的遠端安裝。
- 輪詢網路以偵測新裝置並更新現有裝置的資訊。發佈點可以使用與Kaspersky Next XDR Expert相同的裝置偵測方法。

在組織的網路上放置發佈點用於：

- 減少Kaspersky Next XDR Expert的負載
- 流量最佳化
- 為Kaspersky Next XDR Expert提供對網路中難以到達部分的裝置的存取

考慮到可用功能，我們建議防護充當發佈點的裝置免受任何類型的未經授權存取（包括物理存取）。

限制自動分配發佈點

為了簡化管理並保持網路的可操作性，我們建議使用自動分配發佈點。但是，對於產業網路和小型網路，我們建議您避免自動分配發佈點，因為（例如）用於推送遠端安裝工作的帳戶的私人資訊可以被通過作業系統轉移到發佈點。

對於產業網路和小型網路，您可以手動分配裝置作為發佈點。

您還可以檢視發佈點活動報告。

事件傳輸到第三方系統

本部分介紹將用戶端裝置上發現的安全問題傳輸到協力廠商系統的具體方法。

監控和報告

為了及時回應安全問題，我們建議配置監控和報告功能。

匯出到 SIEM 系統的事件

為了在重大損害發生之前快速偵測安全問題，我們建議使用 SIEM 系統中的事件匯出。

稽核事件的電子郵件通知

為了及時回應緊急情況，我們建議配置管理伺服器以傳送有關其發布的稽核事件、關鍵事件、故障事件和警告的通知。

由於這些事件是系統內事件，因此可以預期它們的數量很少，這非常適用於郵件。

配置受管理應用程式的防護

受管理應用程式政策

我們建議為使用的每種類型的應用程式和Kaspersky Next XDR Expert元件（網路代理程式、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Agent 等）建立一個政策。此政策必須套用於所有受管理裝置（根管理群組）或根據配置的移動規則受管理裝置將自動移動到其中的單獨群組。

指定用於停用防護和解除安裝應用程式的密碼

我們強烈建議啟用密碼防護，以防止入侵者停用或解除安裝卡巴斯基安全應用程式。在支援密碼防護的平台上，您可以為 Kaspersky Endpoint Security、網路代理和其他卡巴斯基應用程式設定密碼。啟用密碼防護後，我們建議通過關閉"鎖"來鎖定相應的設定。

使用卡巴斯基安全網路

不允許使用 KSN，因為這會導致應用程式失去認證狀態。

定期掃描受管理裝置

對於所有裝置群組，我們建議建立一個定期執行完整裝置掃描的工作。

發現新裝置

我們建議正確配置裝置發現設定：設定與網域控制器的整合，並指定用於發現新裝置的 IP 位址範圍。

出於安全目的，您可以使用包含所有新裝置的預設管理群組和影響該群組的預設政策。

部署方案

部署Kaspersky Next XDR Expert（包含Kaspersky Endpoint Detection and Response功能）有兩種選擇：在Kubernetes叢集內的多個節點上部署，或在單一節點上部署。在開始之前，我們建議您熟悉可用的部署方案，然後選擇最符合您組織需求的方案。您還可以參考容量大小指南，其中概述了硬體要求，並根據您企業中的裝置數量建議部署選項。

根據您選擇的部署選項，Kaspersky Next XDR Expert可能需要下列主機才能正常運作：

- **管理員裝置**

  管理員主機是一台實體機或虛擬機，用於部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。由於KDT在管理員主機上運行，因此該主機必須滿足KDT的需求。

  如果管理員主機不包含在叢集中，它將僅用於部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。在這種情況下，主機必須滿足目標主機的需求。

- **目標主機**

  目標主機是用於部署Kaspersky Next XDR Expert的實體機器或虛擬機器。使用的目標主機如下：

  - 在叢集中安裝Kaspersky Next XDR Expert元件的目標主機

    Kubernetes叢集中包含的主機，工作負載在這些主機之間分配。目標主機必須滿足所選部署選項（多節點部署或單節點部署）的需求。

    KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部，也可以完全安裝在叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在叢集外部。在這種情況下，主機必須滿足安裝KUMA服務所需的硬體、軟體和安裝需求。

    您可以將其中一個目標主機用作管理員主機來執行Kaspersky Next XDR Expert部署。在這種情況下，該主機還必須滿足KDT的需求。

  - 用於安裝KUMA服務的KUMA目標主機（可選）

    KUMA服務（收集器、關聯器和儲存體）可以安裝在叢集外部獨立主機的目標主機上。KUMA目標主機的數量取決於Kaspersky Next XDR Expert必須處理的事件數量。

    KUMA目標主機必須滿足安裝KUMA服務所需的硬體、軟體和安裝需求。

- **DBMS主機（僅限多節點部署）。**

  用於安裝DBMS的主機是位於Kubernetes叢集之外的獨立伺服器。此主機必須滿足資料庫節點的需求。

多節點部署

在多節點部署中，Kaspersky Next XDR Expert元件會安裝在Kubernetes叢集的多個工作線程節點上。如果一個節點發生故障，叢集可以在另一個節點上恢復元件運作。

在此組態中，您至少需要五個主機：

- 一個用於DBMS的主機
- 用於運行Kubernetes叢集和Kaspersky Next XDR Expert元件的四個目標主機：
  - 一個主機同時充當管理員主機和目標主機
  - 三個目標主機

  如果您想使用位於群集之外的管理員主機，則需要額外分配一個主機進行部署。

  要在叢集之外安裝KUMA服務，您必須至少額外分配一個KUMA目標主機。

單節點部署

在單節點部署中，所有Kaspersky Next XDR Expert元件都安裝在Kubernetes叢集的單一節點上。此選項適用於計算資源需求較低的解決方案。

在此組態中，至少需要一個目標主機來安裝Kubernetes叢集、Kaspersky Next XDR Expert元件和DBMS。該主機同時充當管理員主機和目標主機。若要使用位於群集之外的管理員主機，則必須額外分配一個主機進行部署。

如果您想在群集之外安裝KUMA服務，必須額外分配至少一個KUMA目標主機。

在此組態中，DBMS不需要單獨的節點。但是，在部署Kaspersky Next XDR Expert之前，應將其手動安裝在目標主機上。

單節點分層部署

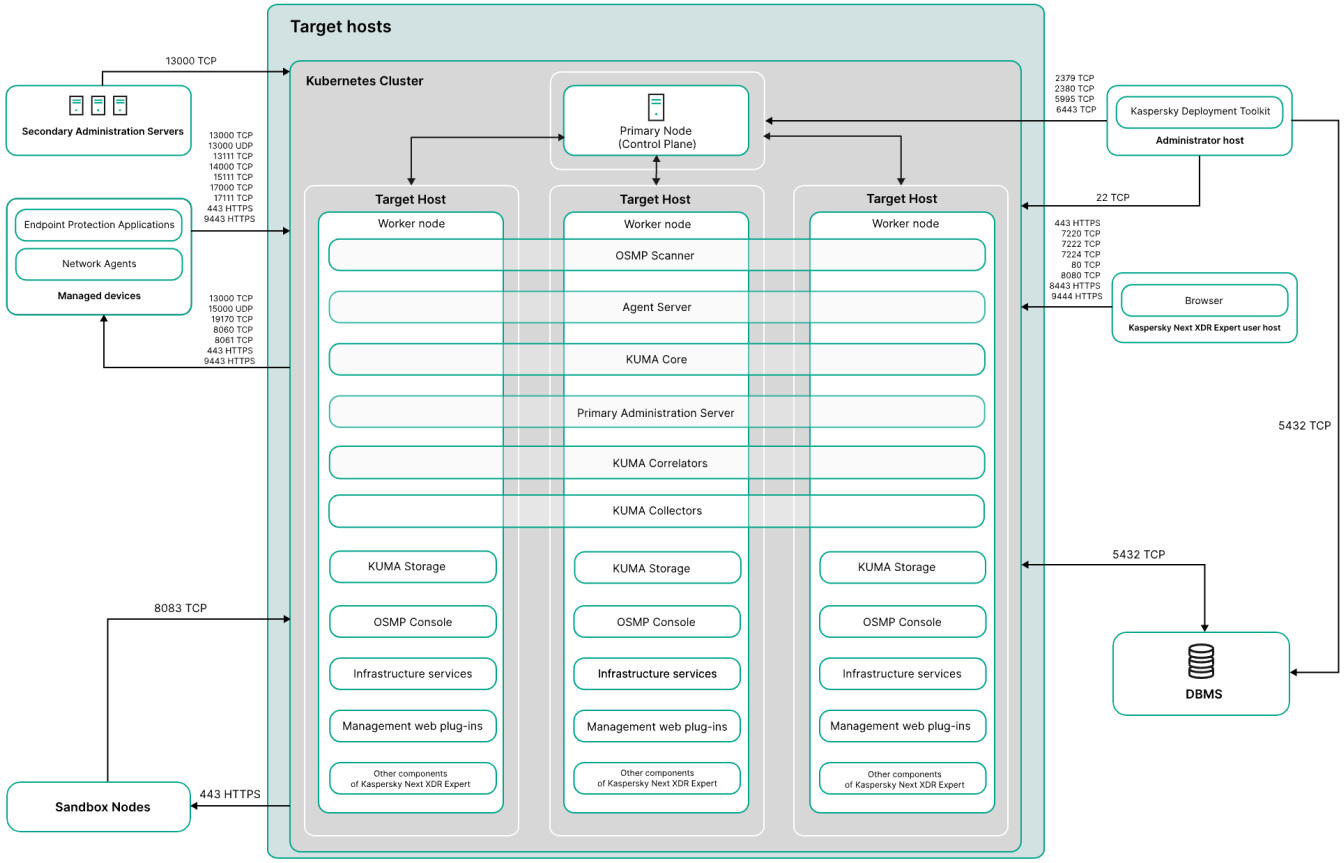
在分層部署中，會部署多個單節點。所有單節點部署完畢後，選擇一個節點為父實例。通常情況下，效能最強的節點會根據計算結果成為父實例。其餘節點隨後連線到該父實例。

如果您需要協助計算部署所需的資源，請聯絡技術支援。

多節點部署方案

下圖顯示了Kaspersky Next XDR Expert在多個節點上的部署方案。

在方案中，以範例形式展示了Kaspersky Next XDR Expert元件在工作線程節點上的分佈。實際的元件分佈可能會有所不同。



Kaspersky Next XDR Expert的多節點部署方案

Kaspersky Next XDR Expert的多節點部署結構包含以下主要元件：

- **管理員主機**。在該主機上，管理員使用Kaspersky Deployment Toolkit來部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。管理員主機可以位於Kubernetes叢集外部，也可以位於叢集內部。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。

- **DBMS伺服器**。Kaspersky Next XDR Expert元件的正常運作需要一台安裝了資料庫管理系統的伺服器。DBMS伺服器不包含在Kubernetes叢集中。管理員需要在Kubernetes叢集之外的獨立伺服器上手動安裝DBMS。

- **Kubernetes叢集**。Kubernetes叢集包含一個控制器節點（在部署過程中也稱為主要節點）以及至少三個工作線程節點。主節點和工作線程節點的數量可能會有所不同。Kaspersky Next XDR Expert的所有元件都部署在工作線程節點上：

  - **主管理伺服器**。用戶端組織端點防護的關鍵元件。管理伺服器透過EPP應用程式提供端點防護的集中部署和管理，並讓您監控端點防護狀態。

    此元件部署在其中一個工作线程節點上，不具節點親和性。Kubernetes調度器會根據可用資源選擇工作線程節點。

  - **OSMP掃描器**。此元件使用反惡意軟體引擎、YARA和沙盒掃描檔案、傳送檔案進行分析並產生報告。

    此元件部署在其中一個工作线程節點上，不具節點親和性。Kubernetes調度器會根據可用資源選擇工作線程節點。

  - **代理程式伺服器**。此元件負責OSMP和端點代理程式之間的互動。

    此元件部署在其中一個工作线程節點上，不具節點親和性。Kubernetes調度器會根據可用資源選擇工作線程節點。

  - **KUMA Core**。SIEM元件的核心組成部分，是所有其他服務和組成部分的基礎。

    此元件部署在其中一個工作线程節點上，不具節點親和性。Kubernetes調度器會根據可用資源選擇工作線程節點。

  - **OSMP主控台**。為OSMP提供網頁介面的元件。

    此元件部署在所有叢集節點上。

  - **管理網頁外掛程式**。此元件用於透過OSMP主控台遠端管理卡巴斯基軟體。

    這些元件部署在所有叢集節點上。

  - **Kaspersky EDR Expert的基礎設施服務和其他元件**。提供集中資產管理、資料交換、層次結構構建、身份驗證和授權的其他元件；以及其他功能，如操作稽核、安全正常管理和更新分發。這些元件部署在所有叢集節點上。

- **KUMA服務**。KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。用於KUMA服務的目標主機數量可能會有所不同。KUMA服務由管理員手動建立。

  在此方案中，KUMA服務完全安裝在叢集內部的工作節點上。在這種情況下，KUMA收集器和KUMA關聯器由管理員手動建立，預設情況下，在沒有節點親和性的情況下部署。每個節點上手動建立多個KUMA儲存體。

- **Kaspersky Next XDR Expert使用者主機**。使用者裝置，用於登入OSMP主控台。

- **從屬管理伺服器**（可選）。輔助管理伺服器用於建立伺服器層次結構，並用於與端點代理程式進一步整合。

- **受管理裝置**。用戶端裝置受Kaspersky Next XDR Expert保護。每個受管理裝置都安裝了網路代理程式和EPP應用程式。

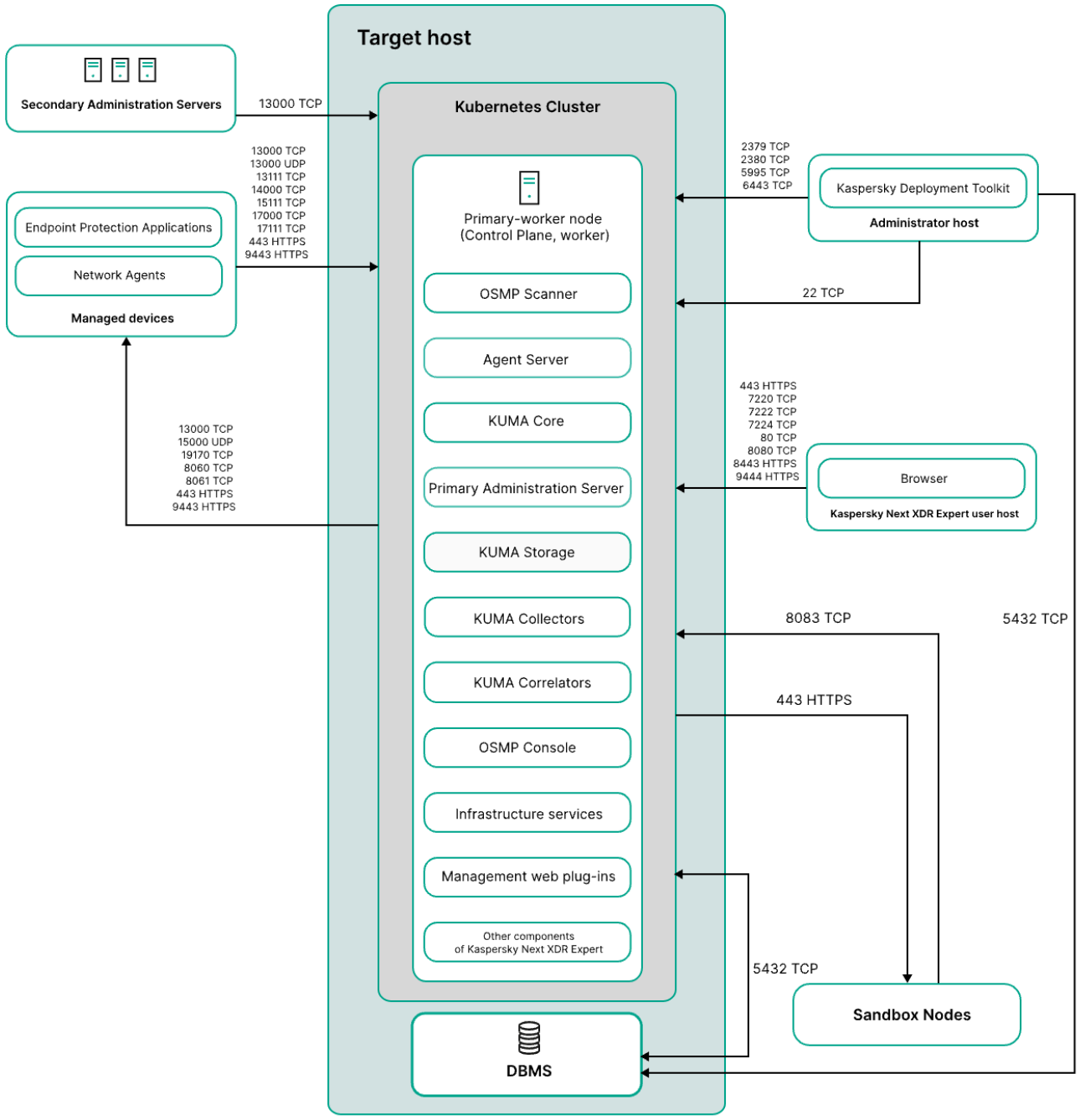
- **沙盒節點**。沙盒節點可包含一或多部執行沙盒元件實例的伺服器。承載隔離執行環境和輔助服務的專用運算資源。此節點負責分析和處理進入受保護系統的檔案、連結、URL和其他物件。沙盒節點獨立於Kubernetes叢集運行。

  沙盒伺服器的數量可能因工作量而異。管理員在每台伺服器上手動安裝沙盒。

此方案不提供成功部署所需的所有連接埠。有關埠的完整清單，請參閱Kaspersky Next XDR Expert使用的連接埠。

單節點部署方案

下圖顯示了Kaspersky Next XDR Expert在單節點上的部署方案。



Kaspersky Next XDR Expert單節點部署方案

Kaspersky Next XDR Expert單節點部署方案包含以下主要元件：

- **管理員主機**。在該主機上，管理員使用Kaspersky Deployment Toolkit來部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。管理員主機可以位於Kubernetes叢集外部，也可以位於叢集內部。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。

- **DBMS伺服器**。Kaspersky Next XDR Expert元件的正常運作需要一台安裝了資料庫管理系統的伺服器。DBMS伺服器不包含在Kubernetes叢集中。在部署Kaspersky Next XDR Expert之前，管理員需要先在將作為主要工作線程節點的目標主機上手動安裝DBMS。

- **Kubernetes叢集**。Kubernetes叢集包含一個主機，該主機既充當控制器節點（在部署過程中也稱為主要節點），又充當工作線程節點。所有Kaspersky Next XDR Expert元件都部署在此主要工作節點上：

  - **主管理伺服器**。用戶端組織端點防護的關鍵元件。管理伺服器透過EPP應用程式提供端點防護的集中部署和管理，並讓您監控端點防護狀態。

  - **OSMP掃描器**。此元件使用反惡意軟體引擎、YARA和沙盒掃描檔案、傳送檔案進行分析並產生報告。

  - **代理程式伺服器**。此元件負責OSMP和端點代理程式之間的互動。

  - **KUMA Core**。SIEM元件的核心組成部分，是所有其他服務和組成部分的基礎。

  - **OSMP主控台**。為OSMP提供網頁介面的元件。

  - **管理網頁外掛程式**。此元件用於透過OSMP主控台遠端管理卡巴斯基軟體。

  - **Kaspersky EDR Expert的基礎設施服務和其他元件**。提供集中資產管理、資料交換、層次結構構建、身份驗證和授權的其他元件；以及其他功能，如操作稽核、安全正常管理和更新分發。

- **KUMA服務**。KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。用於KUMA服務的目標主機數量可能會有所不同。KUMA服務由管理員手動建立。在此方案中，KUMA服務完全安裝在叢集內部的工作節點上。

- **Kaspersky Next XDR Expert使用者主機**。使用者裝置，用於登入OSMP主控台。

- **從屬管理伺服器**（可選）。輔助管理伺服器用於建立伺服器層次結構，並用於與端點代理程式進一步整合。

- **受管理裝置**。用戶端裝置受Kaspersky Next XDR Expert保護。每個受管理裝置都安裝了網路代理程式和EPP應用程式。

- **沙盒節點**。沙盒節點可包含一或多部執行沙盒元件實例的伺服器。承載隔離執行環境和輔助服務的專用運算資源。此節點負責分析和處理進入受保護系統的檔案、連結、URL和其他物件。沙盒節點獨立於Kubernetes叢集運行。

  沙盒伺服器的數量可能因工作量而異。管理員在每台伺服器上手動安裝沙盒。

此方案不提供成功部署所需的所有連接埠。有關埠的完整清單，請參閱Kaspersky Next XDR Expert使用的連接埠。

Kaspersky Next XDR Expert使用的連接埠

為了在管理員主機和目標主機之間進行正確的互動，您必須透過下表中列出的連接埠提供從管理員主機到目標主機的連線存取權限。這些連接埠無法變更。

對於管理員主機和用於安裝KUMA服務且位於Kubernetes叢集之外的主機之間的互動，您必須僅透過TCP 22連接埠提供存取權限。

用於管理員主機與目標主機之間互動的連接埠

連接埠	協定	方向	來源	目的	連接埠目的
22	TCP	入站	管理員裝置	目標主機	提供從管理員主機到目標主機的SSH連線。 提供從管理員主機到用於安裝外部KUMA服務的主機的SSH連線。
2379, 2380	TCP	入站	管理員裝置	目標主機（主要節點）	連線到Kubernetes儲存體（ETCD）。
5995	TCP	入站	管理員裝置	目標主機（主要節點）	連線到Docker登錄檔。
6443	TCP	入站	管理員裝置	目標主機（主要節點）	連線到Kubernetes API。

為了Kaspersky Next XDR Expert元件正常運作，目標主機必須位於同一廣播域中。

下表包含叢集中所有目標主機的防火牆上必須開啟的連接埠。這些連接埠無法變更。

如果您在目標主機上使用firewalld或UFW防火牆，KDT會自動開啟防火牆上的所需連接埠。否則，您可以在部署Kaspersky Next XDR Expert之前手動開啟列出的連接埠。

Kaspersky Next XDR Expert元件使用的必要連接埠

連接埠	協定	方向	來源	目的	連接埠目的
80, 8080	TCP（HTTP）	連入	瀏覽器	叢集的目標主機	從瀏覽器接收連線。重新導向到443 TCP（HTTPS）連接埠。
443, 8443	TCP（HTTPS）	連入	瀏覽器	叢集的目標主機	從瀏覽器接收連線。 透過 OpenAPI™ 接收與管理伺服器的連線。用於自動化與管理伺服器協同工作的情境。
13000	TCP	入站	網路代理程式或從屬管理伺服器	叢集的目標主機	接收來自網路代理和從屬管理伺服器的連線。
13000	UDP	連入	網路代理程式	叢集的目標主機	接收從網路代理關閉的裝置資訊
14000	TCP	入站	網路代理程式	叢集的目標主機	接收來自網路代理的連線
17000	TCP	入站	受管理裝置	叢集的目標主機	接收來自受管理裝置（但不包括行動裝置）的應用程式啟動連線。
19170	TCP（HTTPS）	出站	叢集的目標主機	受管理裝置	使用OSMP主控台遠端存取受管理裝置。
7210	TCP	入站	KUMA目標注記	叢集的目標主機	接收來自KUMA Core伺服器的KUMA組態。
7220	TCP	入站	瀏覽器	叢集的目標主機	從瀏覽器接收連線。
7222	TCP	入站	瀏覽器	叢集的目標主機	CyberTrace系統中的反向代理。
7224	TCP	入站	瀏覽器	叢集的目標主機	身分識別與存取管理器（IAM）的回呼
8429	TCP	入站	KUMA代理程式	叢集的目標主機	記錄KUMA代理程式的績效指標。

下表包含在Kaspersky Next XDR Expert部署期間防火牆上預設未開啟的連接埠。這些連接埠無法變更。

如果您需要執行下表**連接埠用途**直欄中所列的操作，您可以手動開啟所有目標主機防火牆上的對應連接埠。

Kaspersky Next XDR Expert元件所使用的防火牆可選連接埠

連接埠	協定	方向	來源	目的	連接埠目的
8060	TCP	出站	叢集的目標主機	受管理裝置	傳輸發佈的安裝套件到受管理裝置
8061	TCP	出站	叢集的目標主機	受管理裝置	傳輸發佈的安裝套件到受管理裝置
8083	HTTP	連入	沙盒	叢集的目標主機	在沙盒內更新病毒資料庫。

連接埠	協定	方向	來源	目的	連接埠目的
13111	TCP	入站	受管理裝置	叢集的目標主機	接收從受管理裝置到KSN代理伺服器的請求
15111	UDP	連入	受管理裝置	叢集的目標主機	接收從受管理裝置到KSN代理伺服器的請求
17111	TCP	入站	受管理裝置	叢集的目標主機	接收從受管理裝置到KSN代理伺服器的請求
5432	TCP	入站	DBMS (PostgreSQL)	叢集的目標主機	與DBMS（PostgreSQL）的互動。僅當您執行示範部署並在Kubernetes叢集內的目標主機上安裝DBMS時才使用此連接埠。

下表列出了與沙盒互動的主機防火牆上必須開啟的連接埠。

用於與沙盒互動的連接埠

連接埠	協定	方向	來源	目的	連接埠目的
22	TCP	入站	管理員裝置	沙盒節點	透過SSH連線到沙盒伺服器。
443	TCP	入站	OSMP	沙盒節點上的目標元件	來自OSMP元件的入站連線。
8443	TCP	入站	瀏覽器	沙盒節點上的目標元件	存取沙盒網頁介面。
80或443	TCP	出站	沙盒節點上的目標元件	目標更新伺服器	從卡巴斯基更新伺服器取得更新。
任何	任何	出站和相應的入站	沙盒節點上的目標元件	網際網路上的目標資源	存取網際網路以分析已處理物件的網路行為。

下表包含必須開啟的連接埠才能使Kubernetes叢集和基礎設施元件正常運作。這些連接埠無法變更。

如果您在目標主機上使用firewalld或UFW防火牆，KDT會自動開啟防火牆上的所需連接埠。否則，您可以在部署Kaspersky Next XDR Expert之前手動開啟列出的連接埠。

Kubernetes叢集及基礎設施元件所使用的連接埠

連接埠	協定	節點
80	TCP	控制節點
443	TCP	控制節點
10250	TCP	控制節點
9443	TCP	控制節點
6443	TCP	控制節點
8132	TCP	控制節點
5995	TCP	控制節點
80	TCP	工作線程節點
443	TCP	工作線程節點
179	TCP	工作線程節點
10250	TCP	工作線程節點
10255	TCP	工作線程節點
9443	TCP	工作線程節點
6443	TCP	工作線程節點
9500	TCP	工作線程節點
9501	TCP	工作線程節點
9502	TCP	工作線程節點
9503	TCP	工作線程節點
8500	TCP	工作線程節點
8501	TCP	工作線程節點

連接埠	協定	節點
3260	TCP	工作線程節點
8000	TCP	工作線程節點
8002	TCP	工作線程節點
2049	TCP	工作線程節點
3370	TCP	工作線程節點
179	UDP	工作線程節點
51820	UDP	工作線程節點
51821	UDP	工作線程節點

為了讓未包含在Kubernetes叢集中的KUMA服務正常運作，您必須開啟下表中列出的連接埠。下表顯示了預設網路連接埠值。這些連接埠在KUMA安裝期間會自動開啟。

用於與外部KUMA服務互動的連接埠

連接埠	協定	方向	來源	目的	連接埠目的
8123	HTTPS	連入	儲存服務	ClickHouse叢集節點	在ClickHouse集群中寫入和接收標準化事件。
9009	HTTPS	連入/連出	ClickHouse叢集副本	ClickHouse叢集副本	ClickHouse叢集副本之間用於傳輸叢集資料的內部通訊。
2181	TCP	入站	ClickHouse叢集節點	ClickHouse keeper複製協調服務	ClickHouse伺服器副本接收並寫入複製元資料。
2182	TCP	連入/連出	ClickHouse keeper複製協調服務	ClickHouse keeper複製協調服務	複製協調服務之間的內部通訊以達到最小副本數。
8001	TCP	入站	Victoria指標	ClickHouse伺服器	接收ClickHouse伺服器操作指標。
9000	TCP	入站	ClickHouse用戶端	ClickHouse叢集節點	在ClickHouse叢集中寫入和接收資料。

如果您在伺服器上建立了額外的KUMA服務（收集器、關聯器或儲存體），則需要手動開啟與伺服器上建立的服務對應的連接埠。您可以使用TCP 7221連接埠或其他用於服務安裝的連接埠。

如果使用開箱即用的範例服務，則在Kaspersky Next XDR Expert部署期間會自動開啟下列連接埠：

- 7230 TCP
- 7231 TCP
- 7232 TCP
- 7233 TCP
- 7234 TCP
- 7235 TCP
- 7236 TCP
- 5140 TCP
- 5140 UDP
- 5141 TCP
- 5144 UDP

- 5150 UDP

變更用於連線至 OSMP Console 伺服器的連接埠

預設情況下，當管理員透過瀏覽器連線至 OSMP Console 伺服器，以及 Endpoint Agent 連線至 agentserver 元件時，會使用相同的節點和相同的連接埠 (443)，但兩者各自使用不同的 FQDN。如有必要，可在安裝 Kaspersky Next XDR Expert 期間，或在解決方案已安裝後，為這些元件設定兩個不同的連接埠。

若要變更所需的連接埠，您必須有權存取 KDT 公用程式所在的管理員主機。

變更 OSMP Console 連接埠的程序有以下限制：

- 如果將連接埠號碼指定為無效值（超出範圍、包含無效字元或空值），解決方案安裝將會失敗。
- 變更連接埠後，連線至 OSMP Console 時，請務必在瀏覽器的網址列中指定新的連接埠號碼。

若要在安裝 Kaspersky Next XDR Expert 後變更 OSMP Console 連接埠：

1. 選擇 1–65535 範圍內的新連接埠號碼。
2. 如果使用防火牆或其他網路存取限制工具，請設定這些工具，以確保所選連接埠可供存取。
3. 執行下列命令以變更連接埠：

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

   其中，請將 `<port_number>` 替換為您選擇的連接埠號碼。

   如果命令成功完成，目前的 OSMP Console 連線工作階段會終止。

4. 重新連線至 OSMP Console 伺服器。若要這麼做，請在瀏覽器的網址列中，輸入 組態檔 中指定的網頁主控台服務 FQDN 以及新的連接埠號碼。

用於連線至 OSMP Console 的連接埠已變更。預設連接埠 443 不再接受與 OSMP Console 的連線。

若要在安裝 Kaspersky Next XDR Expert 期間變更 OSMP Console 連接埠：

1. 選擇 1–65535 範圍內的新連接埠號碼。
2. 請在組態檔中指定新的連接埠號碼。

   若要這麼做，請在 組態檔 中新增新 OSMP Console 連接埠的安裝參數，然後依下列方式指定選取的連接埠號碼：

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

其中：

- `console_port` 指定新的連接埠號碼。
- `<port_number>` 會被取代為您選取的連接埠號碼。

3. 如果使用防火牆或其他網路存取限制工具，請設定這些工具，以確保所選連接埠可供存取。
4. 安裝 Kaspersky Next XDR Expert。
   如需詳細資訊，請參閱部署 Kaspersky Next XDR Expert一節。
5. 成功安裝後，請連線至 OSMP Console 伺服器。
   若要這樣做，請在瀏覽器的網址列中輸入網頁主控台服務的 FQDN，以及設定檔中指定的新連接埠號碼。

用於連線至 OSMP Console 的連接埠已變更。預設連接埠 (443) 不再用於連線至 OSMP Console。

變更 Endpoint Agent 用來連線至 agentserver 元件的連接埠

預設情況下，當管理員透過瀏覽器連線至 OSMP Console 伺服器，以及 Endpoint Agent 連線至 agentserver 元件時，會使用相同的節點和相同的連接埠 (443)，但兩者各自使用不同的 FQDN。如有必要，可在安裝 Kaspersky Next XDR Expert 期間，或在解決方案已安裝後，為這些元件設定兩個不同的連接埠。

若要變更所需的連接埠，您必須能夠存取 KDT 公用程式所在的管理員主機，並具備修改 Endpoint Agent 政策的權限。

變更 Endpoint Agent 所使用連接埠的程序有一項限制。如果將連接埠號碼指定為無效值（超出範圍、包含無效字元或空值），第一個程序中用於變更連接埠的命令會失敗。在第二個程序中，解決方案的安裝會失敗。

若要在 Kaspersky Next XDR Expert 已安裝後變更 Endpoint Agent 使用的連接埠：

1. 選擇 1–65535 範圍內的新連接埠號碼。
2. 如果使用防火牆或其他網路存取限制工具，請設定這些工具，以確保所選連接埠可供存取。
3. 執行下列命令，以變更 Endpoint Agent 用於連線至 agentserver 元件的連接埠（第一個命令），以及用於傳送遙測資料的連接埠（第二個命令）：

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

   其中，請將 `<port_number>` 替換為您選擇的連接埠號碼。

   如果這些命令成功完成，目前 Endpoint Agent 與 agentserver 元件之間的連線工作階段會終止。agentserver 元件不再接收來自 Endpoint Agent 的資料。
4. 如果來自 Endpoint Agent 的資料透過代理節點路由，請執行以下操作：
   a. 在 Nginx 設定檔中，於字串 `listen <port_number> ssl http2;` 中指定新的連接埠號碼
   b. 執行命令 `nginx -s reload` 以重新啟動 Nginx，套用設定檔中的變更。
5. 在 OSMP Console 的主功能表中，轉至**資產管理→政策**。

6. 在清單中點擊所需的端點安全應用程式政策，然後轉至**應用程式設定 → 內置代理設定 → Endpoint Detection and Response Expert (on-premises)→ 連線至回應伺服器**。

7. 在**連線設定**下，選取伺服器旁的核取方塊，然後點擊**刪除**按鈕。

   使用舊連接埠的所需伺服器已刪除。

8. 在窗格中點擊**新增**按鈕，然後點擊**選擇伺服器**按鈕。

9. 在開啟的視窗中，選取使用新連接埠的伺服器，然後確認動作。

Endpoint Agent 用於連線至 agentserver 元件的連接埠已變更。agentserver 元件開始透過新連接埠接收來自 Endpoint Agent 的資料。將政策套用至 Endpoint Agent 後，Endpoint Agent 會透過新的連接埠重新連線至 OSMP 元件。預設連接埠 (443) 不再用於連線至 agentserver 元件。

若要變更安裝 Kaspersky Next XDR Expert 時 Endpoint Agent 使用的連接埠：

1. 選擇 1–65535 範圍內的新連接埠號碼。

2. 在設定檔中，指定 Endpoint Agent 用於連線至 agentserver 元件的新連接埠，以及用於傳送遙測資料的連接埠。

   若要這麼做，請在設定檔中新增新連接埠的安裝參數，如下所示：

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

   其中：

   - `as_smp_port` 指定 Endpoint Agent 使用的新連接埠號碼。
   - `kuma_gateway_telemetry_listener_port` 指定傳送遙測資料所使用的新連接埠號碼。
   - `<port_number>` 會被取代為您選取的連接埠號碼。

3. 如果使用防火牆或其他網路存取限制工具，請設定這些工具，以確保所選連接埠可供存取。

4. 安裝 Kaspersky Next XDR Expert。

   如需詳細資訊，請參閱部署 Kaspersky Next XDR Expert一節。

5. 如果來自 Endpoint Agent 的資料透過代理節點路由，請執行以下操作：

   a. 在 Nginx 設定檔中，於字串 `listen <port_number> ssl http2;` 中指定新的連接埠號碼

   b. 執行命令 `nginx -s reload` 以重新啟動 Nginx，套用設定檔中的變更。

Endpoint Agent 使用的連接埠已變更。agentserver 元件開始透過新連接埠接收來自 Endpoint Agent 的資料。無法使用預設連接埠 443 連線至 agentserver 元件。

準備工作和部署

本章節介紹如何為Kaspersky Next XDR Expert部署準備基礎設施，設定多節點或單節點部署的特定安裝參數，以及如何使用部署精靈產生組態檔。

您將了解如何根據多節點和單節點部署方案安裝Kaspersky Next XDR Expert。此外，本章節還包含有關如何部署多個包含Kaspersky Next XDR Expert實例的Kubernetes叢集以及如何使用KDT在它們之間切換的資訊。

多節點佈署：準備管理員主機和目標主機

準備多節點部署包括設定管理員和目標主機。準備好主機並指定設定檔後，您將能夠使用KDT在目標主機上部署Kaspersky Next XDR Expert。

準備管理員主機

首先，您需要準備一台裝置作為啟動KDT的管理員主機。該主機可以包含在KDT在部署期間建立的Kubernetes叢集中，也可以不包含在內。如果管理員主機不包含在叢集中，它將僅用於部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。

所有指派給管理員主機的虛擬 CPU 都必須位於單一NUMA 節點上。在 Hypervisor 上設定管理員主機的虛擬機時，請確保 CPU 和記憶體資源配置自同一個 NUMA 節點。這可防止跨節點記憶體存取，以免在安裝期間發生記憶體配置失敗。

若要準備管理員主機：

1. 確保管理員主機上的硬體和軟體符合需求。

   如果管理員主機未包含在Kubernetes叢集，請使用KDT需求。

   如果管理員主機包含在叢集，請使用多節點部署的硬體需求和OSMP的軟體需求。

2. 請在暫存檔案目錄（預設為 `/tmp`）中為 KDT 配置至少 15 GB 的可用空間。若此目錄中的可用空間不足，請執行以下命令以指定另一個目錄的路徑：

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

3. 設定容器執行階段。使用下列其中一個容器執行階段：

   - KDT 內建容器執行階段（以 runc 為基礎）。

     若要安裝此執行階段，請執行以下命令：

     ```
     sudo ./kdt init
     ```

     如果內建容器執行階段不適用於您的環境，您可以改用 Docker 容器執行階段。

   - Docker 容器執行階段。

安裝適用於 Docker 版本 25 的軟體包 或稍後。請勿從作業系統維護者儲存區安裝非官方的Docker軟體套件發行版。

如果無法自動下載 Docker 金鑰環，請手動下載：

a. 在瀏覽器中開啟 https://download.docker.com/linux/ubuntu/gpg 連結，將金鑰儲存為 docker.asc。

b. 執行以下命令：

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

Docker 資料儲存的磁碟分割區（預設為 `/var/lib/docker`）必須至少有 60 GB 可用空間。

執行安裝後步驟，以設定管理主機，使其能夠與Docker正常運作：

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

4. 對於將包含在叢集中的管理主機，請執行其他準備步驟：

a. 由於該裝置將充當管理員和目標主機，請確保它符合多節點部署的需求。

b. 確保cgroup v2 技術在管理員主機上受支援。

a. 由於裝置將作為管理員和目標主機，請確保其滿足單節點佈署的需求（因為演示和單節點部署的部署方案類似）。

b. 確保cgroup v2 技術在管理員主機上受支援。

Linux核心2.6.24或更高版本支援cgroup v2技術。

c. 在管理員主機上安裝uidmap套件。

檢查/etc/subgid 和 /etc/subuid檔案是否包含將用於啟動 KDT 的使用者帳戶。為此，您可以執行以下命令：

```
getsubids USER
```

如果此命令未傳回結果，您必須手動將使用者帳戶新增至 /etc/subgid 和 /etc/subuid 檔案，格式如下：

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

其中：

- `<username>` — 啟動 KDT 時所使用的帳戶使用者名稱。
- `<min_subid>` — 最小 subuid 值。
- `<range_length>` — 分配給使用者 `<username>` 的 subuid 數量。

準備目標主機

目標主機是用於部署Kaspersky Next XDR Expert並包含在Kubernetes叢集中的實體機或虛擬機。Kaspersky Next XDR Expert元件在這些主機上運作。

其中一個目標主機可用作管理員主機。在這種情況下，您必須按照上一步驟所述將此主機準備為管理員主機，然後執行目標主機的準備工作。

多節點部署的最低叢集設定包括四個節點：

- 一個主要節點

  主要節點用於管理叢集、儲存元資料和分配工作負載。

- 三個工作節點

  工作節點用於執行Kaspersky Next XDR Expert元件的工作負載。

叢集集中的主節點和工作線程節點數量可能有所不同。為了在節點之間實現最佳工作負載分配，建議使用效能大致相同的節點。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。

如果您有多個主節點，則需要一個負載平衡器來在主節點之間分配傳入請求，並確保工作負載平衡。如果您想使用外部負載平衡器，請在Kubernetes叢集外部分配一個單獨的主機，並在組態檔中指定其參數。如果您不想使用外部負載平衡器，則工作線程節點將充當負載平衡器。

若要準備目標主機：

1. 確保目標主機上的硬體和軟體符合多節點部署的需求，並且目標主機位於同一廣播域中。

   如果KUMA服務安裝在叢集內，目標主機必須滿足安裝KUMA服務所需的硬體、軟體和安裝需求。

   為了Kaspersky Next XDR Expert正常運作，在裝有Ubuntu系列作業系統的目標主機上，Linux核心版本必須為5.15.0.107或更高版本。

   為了確保 Kubernetes 叢集及其元件正常運作，必須在所有叢集節點上停用交換空間。如果節點已啟用交換空間，KDT 將在部署期間自動將其停用。

   除將用作管理員主機的目標主機外，不得在目標主機上安裝 Docker。KDT將在部署期間安裝所有必要的軟體和依賴項。

2. 確保掛載在 `/var` 的檔案系統在每個目標主機上至少有 700 GB 的可用空間。

   我們建議將 `/opt/lvp/hot` 目錄放置在專用的高效能磁碟子系統上，並將 `/opt/lvp/cold` 目錄放置在獨立的大容量磁碟子系統上。

3. 在每個目標主機上，如果尚未安裝sudo套件，請安裝此套件。對於Debian系列作業系統，在目標主機上安裝UFW軟體套件。

4. 在每個目標主機上，設定/etc/environment檔案。如果您的組織基礎設施使用代理伺服器存取網際網路，請在目標主機上使用代理伺服器設定網際網路存取。

5. 在具有UFW組態的主節點上，允許IP轉送功能。在 `/etc/default/ufw` 檔案中，將 `DEFAULT_FORWARD_POLICY` 設為 `ACCEPT`。

6. 提供對儲存Kaspersky Next XDR Expert所需的以下軟體套件的軟體套件儲存區的存取權限：

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

   KDT將在部署期間嘗試從軟體套件儲存區安裝這些軟體套件。您也可以手動安裝這些安裝套件。

7. 確保滿足以下條件：

   - 在每個目標主機上：python3-apt
   - 在主節點上：curl

   使用KDT從軟體套件儲存區部署期間不會安裝curl和libnfs軟體套件。如果尚未安裝這些安裝套件，則必須手動安裝它們。

8. 針對目標主機，請在Hypervisor、虛擬交換器或網路基礎設施層級停用 ARP/MAC欺騙防護機制。

   對於 VMware，請啟用**偽造傳輸**和**MAC 位址變更**。對於 Hyper-V，請啟用**MAC 位址欺騙**。對於網路設備，請停用**動態 ARP 檢查 (DAI)**，或將連接埠設定為受信任。

   如需範例，請參閱MetalLB 疑難排解指南，瞭解如何檢查 ARP 要求是否到達節點。

9. 為目標主機和Kubernetes叢集閘道保留靜態IP位址。

Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。閘道 IP 位址為 IPv4 位址（例如，10.80.23.182）。其於設定檔中指定（`ingress_ip` 參數）。

確保目標主機、Kubernetes叢集閘道和DBMS主機位於同一個廣播網域。

Kubernetes叢集閘道和目標主機需要IPv4位址。如果您的環境需要IPv6連線，請在目標主機和Kubernetes叢集閘道上設定作業系統，以便透過IPv6閘道（NAT64）或IPv6隧道路由IPv6流量。此組態可使叢集在IPv4上執行，同時提供與IPv6網路的互通性。

10. 在您的DNS伺服器上，註冊服務FQDN以連線到Kaspersky Next XDR Expert服務。

    預設情況下，Kaspersky Next XDR Expert服務在以下位址可用：

    - <console_host>.<smp_domain>—存取OSMP主控台介面。
    - <ksc_host>.<smp_domain>—與管理伺服器互動。
    - <kuma_host>.<smp_domain>—存取SIEM元件。
    - <api_host>.<smp_domain>—存取Kaspersky Next XDR Expert API。
    - <monitoring_host>.<smp_domain>—存取OSMP指標。

      其中<console_host>、<admsrv_host>、<kuma_host>、<api_host>與<monitoring_host>皆為服務主機名稱，<smp_domain>為服務網域名稱。這些參數是服務 FQDN 的組成部分，且可在設定檔中指定。如果您未指定服務主機名稱的自訂值，則會使用預設值：`console_host`—「`console`」、`ksc_host`—「`admsrv`」、`kuma_host`—「`kuma`」、`api_host`—「`api`」、`monitoring_host`—「`monitoring`」。

    所列的服務FQDN必須解析為Kubernetes叢集的IP位址。例如，如果Kubernetes叢集位址為10.80.23.182，則服務FQDN將如下解析為IP位址：

    - <console_host>.<smp_domain>—10.80.23.182
    - <ksc_host>.<smp_domain>—10.80.23.182
    - <kuma_host>.<smp_domain>—10.80.23.182
    - <api_host>.<smp_domain>—10.80.23.182
    - <monitoring_host>.<smp_domain>—10.80.23.182

11. 在目標主機上，建立將用於部署Kaspersky Next XDR Expert的帳戶。

    這些帳戶用於 SSH 連線，且必須能夠在不輸入密碼的情況下提升權限 (sudo)。為此，請將建立的使用者帳戶新增至 `/etc/sudoers` 檔案。

    檢視詳情

    若要將建立的使用者帳戶新增至 `/etc/sudoers` 檔案：

    1. 執行以下指令：

       ```
       sudo useradd -m -s /bin/bash <user_name>
       sudo usermod -aG sudo <user_name>
       ```

2. 使用以下指令開啟 `/etc/sudoers` 檔案：

```
sudo visudo
```

3. 在 `# Allow members of group sudo to execute any command` 區段的結尾新增下列行：

```
<user_name> ALL=(ALL) NOPASSWD: ALL
```

其中 `<user_name>` 是所建立使用者的名稱。

4. 儲存並關閉 `/etc/sudoers` 檔案。

12. 設定管理員和目標主機之間的SSH連線：

a. 在管理員主機上，使用ssh-keygen公用程式產生SSH金鑰（無需密碼）。

b. 使用 ssh-copy-id 公用程式將公開金鑰複製到每個目標主機；如果使用負載平衡器，則也複製到負載平衡器主機（例如，複製到 `/home/<user_name>/.ssh` 目錄）。

如果使用目標主機作為管理員主機，則也必須將公鑰複製到該主機。

13. 為了使Kaspersky Next XDR Expert元件正常運作，請在目標主機之間提供網路存取，並在必要時在管理員和目標主機的防火牆上打開所需的連接埠。

14. 在管理員和目標主機上設定透過網路時間協定（NTP）進行時間同步。

15. 如有必要，請準備自訂憑證以用於Kaspersky Next XDR Expert公共服務。

您可以為每個服務使用一個從組織的根憑證或葉憑證頒發的中間憑證。將使用準備好的自訂憑證取代自簽名憑證。

單節點部署：準備管理員主機和目標主機

準備單節點部署包括設定管理員和目標主機。在單節點組態中，Kubernetes叢集和Kaspersky Next XDR Expert元件安裝在相同目標主機上。準備好主機並指定組態檔後，您將能夠使用KDT在目標主機上部署Kaspersky Next XDR Expert。

準備管理員主機

首先，您需要準備一台裝置作為啟動KDT的管理員主機。該主機可以包含在KDT在部署期間建立的Kubernetes叢集中，也可以不包含在內。如果管理員主機不包含在叢集中，它將僅用於部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。在這種情況下，解決方案的部署和運作只需要一台主機。

所有指派給管理員主機的虛擬 CPU 都必須位於單一NUMA 節點上。在 Hypervisor 上設定管理員主機的虛擬機時，請確保 CPU 和記憶體資源配置自同一個 NUMA 節點。這可防止跨節點記憶體存取，以免在安裝期間發生記憶體配置失敗。

若要準備管理員主機：

1. 確保管理員主機上的硬體和軟體符合需求。

   如果管理員主機未包含在Kubernetes叢集，請使用KDT需求。

   如果管理員主機包含在叢集，請使用多節點部署的硬體需求和OSMP的軟體需求。

2. 請在暫存檔案目錄（預設為 `/tmp`）中為 KDT 配置至少 15 GB 的可用空間。若此目錄中的可用空間不足，請執行以下命令以指定另一個目錄的路徑：

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

3. 設定容器引擎。請使用以下其中一種容器引擎：

   - KDT 內建容器引擎（以 runc 為基礎）

     執行以下命令以安裝內建容器引擎：

     ```
     sudo ./kdt init
     ```

     如果內建容器引擎不適合您的環境，您可以改用 Docker 容器引擎。

   - Docker 容器引擎

     安裝適用於 Docker 版本 25 的軟體包 或稍後。請勿從作業系統維護者儲存區安裝非官方的Docker軟體套件發行版。

     如果無法自動下載 Docker 金鑰環，請手動下載：

     a. 在瀏覽器中開啟 https://download.docker.com/linux/ubuntu/gpg 連結，將金鑰儲存為 docker.asc。

     b. 執行以下命令：

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

     Docker 資料儲存的磁碟分割區（預設為 `/var/lib/docker`）必須至少有 60 GB 可用空間。

     執行安裝後步驟，以設定管理主機，使其能夠與Docker正常運作：

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

4. 對於將包含在叢集中的管理主機，請執行其他準備步驟：

   a. 由於該裝置將充當管理員和目標主機，請確保它符合單節點部署的需求。

   b. 確保管理員主機支援cgroup v2 技術。

      a. 由於裝置將作為管理員和目標主機，請確保其滿足單節點佈署的需求（因為演示和單節點部署的部署方案類似）。

      b. 確保cgroup v2 技術在管理員主機上受支援。

         Linux核心2.6.24或更高版本支援cgroup v2技術。

c. 在管理員主機上安裝uidmap套件。

檢查/etc/subgid 和 /etc/subuid檔案是否包含將用於啟動 KDT 的使用者帳戶。為此，您可以執行以下命令：

```
getsubids USER
```

如果此命令未傳回結果，您必須手動將使用者帳戶新增至 /etc/subgid 和 /etc/subuid 檔案，格式如下：

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

其中：

- `<username>` — 啟動 KDT 時所使用的帳戶使用者名稱。
- `<min_subid>` — 最小 subuid 值。
- `<range_length>` — 為使用者 `<username>` 配置的 subuid 數量。

準備目標主機

目標主機是用於部署Kaspersky Next XDR Expert並包含在Kubernetes叢集中的實體機或虛擬機。目標主機管理Kubernetes叢集以及運行在該主機上的Kaspersky Next XDR Expert元件，並儲存元資料。

單節點部署的最小叢集組態包括一個目標主機，該主機充當主要節點和工作線程節點。在這個主要工作線程節點上，安裝了Kubernetes叢集和Kaspersky Next XDR Expert元件。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部的主要工作線程節點上，也可以完全安裝在Kubernetes叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在Kubernetes叢集外部。

如果要從目標主機執行Kaspersky Next XDR Expert部署，則必須依照前面的步驟將此主機準備為管理員主機，然後再準備目標主機。

若要準備目標主機：

1. 請確保管理員主機上的硬體和軟體符合單節點部署的需求。

   如果KUMA服務安裝在叢集內部，則目標主機必須符合安裝KUMA服務所需的硬體、軟體和安裝需求。

   由於DBMS將安裝在目標主機上，因此您還需要確保目標主機符合DBMS的需求。

   為了Kaspersky Next XDR Expert正常運作，在裝有Ubuntu系列作業系統的目標主機上，Linux核心版本必須為5.15.0.107或更高版本。

   為了確保 Kubernetes 叢集及其元件正常運作，必須在所有叢集節點上停用交換空間。如果節點已啟用交換空間，KDT 將在部署期間自動將其停用。

   除非目標主機將用作管理員主機，否則不要在目標主機上安裝Docker。KDT將在部署期間安裝所有必要的軟體和依賴項。

2. 請確保掛載在`/var`目錄下的檔案系統在目標主機上至少有360GB的可用空間。

   我們建議將`/opt/lvp/hot`目錄置於專用的高效能磁碟子系統，並將`/opt/lvp/cold`目錄置於獨立的高容量磁碟子系統。

3. 在目標主機上安裝DBMS。

   您必須在部署Kaspersky Next XDR Expert之前安裝DBMS，因為在這種情況下，DBMS和Kaspersky Next XDR Expert元件將安裝在相同目標主機上，且DBMS不會包含在Kubernetes叢集中。

4. 如果尚未安裝sudo套件，請安裝此套件。對於Debian系列作業系統，安裝UFW套件。

5. 設定/etc/environment檔案。如果您的組織基礎設施使用代理伺服器存取網際網路，請在目標主機上使用代理伺服器設定網際網路存取。

6. 在具 UFW 設定的主要工作節點上，允許 IP 轉送功能。在`/etc/default/ufw`檔案中，將`DEFAULT_FORWARD_POLICY`設定為`ACCEPT`。

7. 提供對儲存Kaspersky Next XDR Expert所需的以下軟體套件的軟體套件儲存區的存取權限：

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

   KDT將在部署期間嘗試從軟體套件儲存區安裝這些軟體套件。您也可以手動安裝這些安裝套件。

8. 確保以下軟體包已安裝在主工作線程節點上：

   - python3-apt
   - curl

使用KDT從軟體套件儲存區部署期間不會安裝curl和libnfs軟體套件。如果尚未安裝這些安裝套件，則必須手動安裝它們。

9. 對於目標主機，請停用虛擬機器管理程式、虛擬交換器或網路基礎設施上的ARP/MAC欺騙防護機制。

   對於 VMware，請啟用**偽造傳輸**和**MAC 位址變更**。對於 Hyper-V，請啟用**MAC 位址欺騙**。對於網路設備，請停用**動態 ARP 檢查 (DAI)**，或將連接埠設定為受信任。

   如需範例，請參閱MetalLB 疑難排解指南，瞭解如何檢查 ARP 要求是否到達節點。

10. 為目標主機和Kubernetes叢集閘道保留靜態IP位址。

    Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。閘道 IP 位址為 IPv4 位址（例如，10.80.23.182）。其於設定檔中指定（`ingress_ip` 參數）。

    確保目標主機和Kubernetes叢集閘道位於同一個廣播網域。

    > Kubernetes叢集閘道和目標主機需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。

11. 在您的DNS伺服器上，註冊服務FQDN以連線到Kaspersky Next XDR Expert服務。

    預設情況下，Kaspersky Next XDR Expert服務在以下位址可用：

    - <console_host>.<smp_domain>—存取OSMP主控台介面。
    - <ksc_host>.<smp_domain>—與管理伺服器互動。
    - <kuma_host>.<smp_domain>—存取SIEM元件。
    - <api_host>.<smp_domain>—存取Kaspersky Next XDR Expert API。
    - <monitoring_host>.<smp_domain>—存取OSMP指標。

      其中<console_host>、<admsrv_host>、<kuma_host>、<api_host>與<monitoring_host>皆為服務主機名稱，<smp_domain>為服務網域名稱。這些參數是服務 FQDN 的組成部分，且可在設定檔中指定。如果您未指定服務主機名稱的自訂值，則會使用預設值：`console_host`—「`console`」、`ksc_host`—「`admsrv`」、`kuma_host`—「`kuma`」、`api_host`—「`api`」、`monitoring_host`—「`monitoring`」。

    所列的服務FQDN必須解析為Kubernetes叢集的IP位址。例如，如果Kubernetes叢集位址為10.80.23.182，則服務FQDN將如下解析為IP位址：

    - <console_host>.<smp_domain>—10.80.23.182
    - <ksc_host>.<smp_domain>—10.80.23.182
    - <kuma_host>.<smp_domain>—10.80.23.182
    - <api_host>.<smp_domain>—10.80.23.182
    - <monitoring_host>.<smp_domain>—10.80.23.182

12. 建立將用於部署Kaspersky Next XDR Expert的使用者帳戶。

    這些帳戶用於 SSH 連線，且必須能夠在不輸入密碼的情況下提升權限 (sudo)。為此，請將建立的使用者帳戶新增至 `/etc/sudoers` 檔案。

    檢視詳情

若要將建立的使用者帳戶新增至 `/etc/sudoers` 檔案：

1. 執行以下指令：

```
sudo useradd -m -s /bin/bash <user_name>
sudo usermod -aG sudo <user_name>
```

2. 使用以下指令開啟 `/etc/sudoers` 檔案：

```
sudo visudo
```

3. 在 `# Allow members of group sudo to execute any command` 區段的結尾新增下列行：

```
<user_name> ALL=(ALL) NOPASSWD: ALL
```

其中 `<user_name>` 是所建立使用者的名稱。

4. 儲存並關閉 `/etc/sudoers` 檔案。

13. 設定管理員和目標主機之間的SSH連線：

a. 在管理員主機上，使用ssh-keygen公用程式產生SSH金鑰（無需密碼）。

b. 使用 ssh-copy-id 公用程式將公開金鑰複製至目標主機（例如，複製至 `/home/<user_name>/.ssh` 目錄）。

如果使用目標主機作為管理員主機，則也必須將公鑰複製到該主機。

14. 為了使Kaspersky Next XDR Expert元件正常運作，根據需要，請在管理員和目標主機的防火牆上開啟所需的連接埠。

15. 在管理員和目標主機上設定透過網路時間協定（NTP）進行時間同步。

16. 如有必要，請準備自訂憑證以用於Kaspersky Next XDR Expert公共服務。

您可以為每個服務使用一個從組織的根憑證或葉憑證頒發的中間憑證。將使用準備好的自訂憑證取代自簽名憑證。

準備主機以安裝KUMA服務

KUMA服務（收集器、關聯器和儲存體）安裝在Kubernetes叢集外部的KUMA目標主機上。

使用KUMA目標主機的FQDN存取KUMA服務。管理員主機必須能夠透過其FQDN存取KUMA目標主機。

如果您打算在基礎設施中使用多個租用戶，請為每個租用戶建立一個單獨的收集器。

若要準備用於安裝KUMA服務的KUMA目標主機：

1. 確保滿足硬體、軟體和安裝需求。
2. 指定主機名稱。

   必須指定FQDN，例如：kuma1.example.com。

   我們不建議在安裝後更改KUMA主機名稱。這將導致無法驗證憑證的真實性，並會中斷應用程式元件之間的網路通訊。
3. 執行以下指令：

   ```
   hostname -f
   ```

   ```
   hostnamectl status
   ```

   比較 `hostname -f` 指令的輸出與 `hostnamectl status` 指令輸出中 `Static hostname` 欄位的值。這些值必須與裝置的FQDN相符。
4. 設定管理員主機和KUMA目標主機之間的SSH連線。

   使用為目標主機建立的SSH金鑰。使用ssh-copy-id公用程式將公鑰複製到KUMA目標主機。
5. 在您組織的DNS區域中註冊KUMA目標主機，以允許將主機名稱轉換為IP位址。
6. 確保在所有KUMA目標主機上設定了透過網路時間協定（NTP）的時間同步。KUMA服務（收集器、關聯器和儲存體）安裝在Kubernetes叢集外部的KUMA目標主機上。

主機已準備好安裝KUMA服務。

安裝資料庫管理系統

卡巴斯基Next XDR Expert支援PostgreSQL或Postgres Pro資料庫管理系統 (DBMS)。有關支援的DBMS的完整列表，請參閱硬體和軟體要求。

以下每個卡巴斯基Next XDR Expert元件都需要一個資料庫：

- 管理伺服器
- 自動化平台
- 事件回應平台 (IRP)
- 身分識別與存取管理器 (IAM)

每個元件都必須在同一個DBMS實例中有一個單獨的資料庫。DBMS實例必須安裝在Kubernetes叢集之外的獨立伺服器上。我們建議您在Kubernetes叢集之外安裝DBMS實例。

對於DBMS的安裝， KDT需要一個具有建立資料庫和其他DBMS帳戶權限的特權DBMS帳戶。KDT使用具有超級使用者權限的預設DBMS帳戶，或具有相同權限的其他DBMS帳戶，來建立Kaspersky Next XDR Expert元件所需的資料庫和其他DBMS帳戶。

對於多節點部署，您必須在不包含在Kubernetes叢集的獨立伺服器上手動安裝DBMS 。

對於單節點部署，您必須在部署Kaspersky Next XDR Expert之前在目標主機上手動安裝DBMS。在這種情況下，DBMS和Kaspersky Next XDR Expert元件會安裝在相同目標主機上，但DBMS不包含在Kubernetes叢集中。

對於如何安裝所選 DBMS 的資訊，請參考其文件。

PostgreSQL安裝命令範例

若要安裝PostgreSQL，請執行以下命令：

```
sudo apt install -y postgresql-<版本>
sudo systemctl start postgresql
sudo systemctl enable postgresql
```

其中 <版本> 是支援的 PostgreSQL 版本之一。

安裝DBMS後，您需要設定DBMS伺服器參數，以確保DBMS與Open Single Management Platform的正常運作。

設定 PostgreSQL 或 Postgres Pro 伺服器以搭配 Kaspersky Next XDR Expert 使用

若要成功設定PostgreSQL或Postgres Pro伺服器以與Open Single Management Platform搭配使用，您必須使用本文中指定的伺服器參數之外的預設伺服器參數。

Kaspersky Next XDR Expert支援PostgreSQL或Postgres Pro資料庫管理系統 (DBMS)。有關支援的DBMS的完整列表，請參閱硬體和軟體要求。考慮配置DBMS伺服器參數以最佳化DBMS與管理伺服器的協同工作。DBMS 伺服器參數符合建議值，是安裝 Kaspersky Next XDR Expert 的先決條件之一。參數的符合性會使用 KDT 驗證。

找到DBMS組態檔：

- PostgreSQL 組態檔的預設路徑為：`/etc/postgresql/< VERSION >/main/postgresql.conf`
- Postgres Pro 組態檔的預設路徑為：`/var/lib/pgpro/std-< VERSION >/data/postgresql.conf`

如果預設路徑上沒有組態檔，請執行以下命令以找到正確的路徑：

```
sudo su - postgres
psql -c 'SHOW config_file'
```

命令回應將包含組態檔的路徑。

然後執行以下命令登出`postgres`使用者：

```
exit
```

用於管理伺服器的PostgreSQL和Postgres Pro DBMS的建議參數：

- `listen_addresses = '*'`
  指定管理伺服器將監聽的IP介面。出於安全考慮，請設定防火牆，僅允許受信任的IP位址存取連接埠 5432。

- `max_connections = 512`

  這是建議的最小值，您可以指定更大的值。如果您使用叢集 Postgres DBMS，請在所有 DBMS 伺服器及叢集設定中指定 `max_connections` 參數。

- `shared_buffers = N`

  N = 安裝DBMS的裝置RAM值的25%–40%，但不得少於3GB。

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth = N`

  若 DBMS 安裝在 Linux 裝置上，則 N 等於最大堆疊大小減去 1 MB 安全裕度。若要取得最大堆疊大小值（以 KB 為單位），請執行 '`ulimit -s`' 命令。

  如果DBMS安裝在Windows裝置上，則保留預設值2MB。

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = on

如果您使用 Postgres Pro 15.7 或 Postgres Pro 15.7.1，請停用 `enable_compound_index_stats` 參數：

`enable_compound_index_stats = off`

更新組態檔後，重新載入配置或重新啟動DBMS伺服器。

有關 PostgreSQL 和 Postgres Pro 伺服器參數以及如何指定參數的詳細資訊，請參閱相應的 DBMS 文件。

在pg_hba.conf組態檔中指定節點的身分驗證條目。您可以在postgresql.conf所在的同一路徑中找到它。

- 在 `"# "local" is for Unix domain socket connections only"` 區段中，針對 `local`，在 `METHOD` 欄中，將值變更為 `trust`
- 在 `"IPv4 local connections"` 區段中，針對 `host`，在 `ADDRESS` 欄中，將值變更為 `0.0.0.0/0`
- 執行以下命令以套用更改，而無需重新啟動資料庫伺服器：

  ```
  sudo -u postgres psql -c "SELECT pg_reload_conf();"
  ```

為 `postgres` 使用者指定密碼：

1. 執行以下指令：

   ```
   sudo su - postgres
   psql
   ```

   命令輸出應如下所示：

   ```
   psql (15.12)
   Type "help" for help.
   postgres=#
   ```

2. 在 `postgres=#` 後，輸入 `\password`：

   ```
   postgres=# \password
   ```

3. 輸入並再次輸入密碼：

   ```
   Enter new password for user "postgres"
   Enter it again:
   ```

4. 若要登出使用者 `postgres`：

   ```
   postgres=# exit
   ```

Kaspersky Next XDR Expert 元件需要在 `parameters.psql_dsn` 中將 PostgreSQL 超級使用者憑證指定為 `value`。在部署組態檔中指定postgres憑據。如需更多資訊，請參閱單節點佈署：指定安裝參數或多節點佈署：指定安裝參數章節，視您的部署方案而定。

檢查資料庫連線

要檢查資料庫連線：

1. 確保Postgres服務正在執行：

   ```
   systemctl list-unit-files | grep postgres
   ```

   範例輸出：

   ```
   postgrespro-std-17.service                                    enabled         enabled
   ```

2. 重新啟動Postgres服務：

   ```
   systemctl restart <Postgres_service>
   ```

   其中，`<Postgres_service>`是在此程序的步驟1中取得的Postgres服務名稱。

3. 執行`psql`檢查連線：

   ```
   psql -h <fqdn> -U postgres -d postgres
   ```

   請輸入之前指定的密碼：

   ```
   Password for user postgres:
   ```

   範例輸出：

   ```
   psql (17.4)
   Type "help" for help.
   ```

4. 輸入`exit`：

```
postgres=# exit
```

高可用叢集支援

高可用性MariaDB和PostgreSQL叢集支援以下設定：

- 複製類型：同步。
- 最少節點數：3。
- 最大節點數：15。

將`psql_dsn`參數設定如下：`postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`

當使用 Postgres 高可用性叢集（版本 14 或更高版本）作為資料庫時，資料庫使用者必須具有 `pg_read_all_stats` 權限。您可以透過執行以下命令授予此權限：

```
GRANT pg_read_all_stats TO "dbms_username";
```

其中 `dbms_username` 是具權限的內部 DBMS 帳戶名稱。

在設定檔 (`/etc/postgresql/<VERSION>/main/postgresql.conf`) 中指定以下參數：

```
log_hostname = 1
```

支援Corosync/Pacemaker

若要使用 Corosync/Pacemaker，請使用 DBMS 叢集的虛擬 IP 位址設定 `psql_dsn` 參數，如下所示：

```
psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>
```

準備KUMA清查文件，以便在Kubernetes叢集外部安裝KUMA服務

KUMA清查檔案是YAML格式的檔案，其中包含用於部署Kubernetes叢集中未包含的KUMA服務的安裝參數。KUMA清查檔案的路徑包含在卡巴斯基佈署套件用於Kaspersky Next XDR Expert部署的組態檔中。

KUMA清查檔案的範本位於分發套件中。如果要在一個主機上安裝KUMA服務（儲存體、收集器和關聯器），請使用single.inventory.yaml檔案。若要在網路基礎架構中的多個主機上安裝服務，請使用distributed.inventory.yaml檔案。

我們建議您備份用於安裝KUMA服務的KUMA清查檔案。您可以使用它來刪除KUMA。

若要準備KUMA清單文件，

請開啟分發套件中的KUMA清查檔案範本，然後編輯清查檔案中的變數。

KUMA清查檔案包含以下區塊：

- `all` 區塊

  `all` 區塊包含套用至清查檔案中指定之所有主機的變數。變數位於 `vars` 區段。

- `kuma` 區塊

  `kuma` 區塊包含套用至將安裝 KUMA 服務之主機的變數。這些主機列於 `children` 區段中的 `kuma` 區塊。變數位於 `vars` 區段。

下表列出了可能的變數、它們的描述、可能的值以及這些變數所在的KUMA清查檔案區塊。

vars部分中可能的變數清單

變數	敘述	可能的值	封鎖
位於 `all` 與 `kuma` 區塊的 `vars` 區段中的變數			
`ansible_connection`	用於連線KUMA服務主機的方法。	• `ssh` — 透過 SSH 建立與目標主機的連線。 • `local` — 未與目標主機建立連線。 若要確保 KUMA 服務正確安裝，請在 `all` 區塊中，將 `ansible_connection` 變數設定為 `local`。 在 `kuma` 區塊中，必須指定 `ansible_connection` 變數並將 `ansible_connection` 設定為 `ssh`，以便透過 SSH 與安裝了 KUMA 服務的主機建立連線。	• `all` • `kuma`
`ansible_user`	用於連線到KUMA服務主機以安裝外部KUMA服務的使用者名稱。	如果目標主機上的根使用者被封鎖，請指定有權建立SSH連線並使用su或sudo提升權限的使用者名稱。 若要確保 KUMA 服務正確安裝，請在 `all` 區塊中，將 `ansible_user` 變數設定為 `nonroot`。 在 `kuma` 區塊中，必須覆寫 `ansible_user` 變數，並將 `ansible_user` 設定為可透過 SSH 連線至遠端主機的帳戶使用者名稱，以便為安裝 KUMA 服務做好準備。	• `all` • `kuma`
`ansible_become`	用於指示需要提升用於安裝KUMA元件的使用者帳戶權限的變數。	• `false` — 如果 `ansible_user` 的值為 `root`。 • `true` — 如果 `ansible_user` 的值不是 `root`。	`kuma`
`ansible_become_method`	用於提升用於安裝KUMA元件的使用者帳戶權限的方法。	`su` 或 `sudo` — 如果 `ansible_user` 的值不是 `root`。	`kuma`
位於 `kuma` 區塊的 `children` 區段中的變數			

kuma_utils	用於儲存KUMA服務檔案和公用程式的主機群組。 主機可以同時包含在 kuma_utils 群組，以及 kuma_collector 、 kuma_correlator 或 kuma_storage 群組中。 kuma_utils 群組可以包含多個主機。 在 Kaspersky Next XDR Expert 部署期間，對於隸屬於 kuma_utils 的主機，以下檔案將被複製至 /opt/kaspersky/kuma/utils/ 目錄： • kuma是用於安裝KUMA服務的可執行檔。 • kuma.exe是用於在基於Windows的主機上安裝KUMA代理程式的可執行檔。 • LEGAL_NOTICES是包含協力廠商程式碼資訊的檔案。 • kuma-ptvm.tar.gz 是用於與 MaxPatrol 整合的公用程式。 • ootb-content是一個包含KUMA服務開箱即用資源的存檔。	主機群組包含 ansible_host 變數，該變數會指定主機的唯一 FQDN 與 IP 位址。	kuma
kuma_collector	KUMA收集器主機群組。該群組可以包含多個主機。	KUMA 收集器主機群組包含 ansible_host 變數，該變數會指定主機的唯一 FQDN 與 IP 位址。	kuma
kuma_correlator	KUMA關聯器主機群組。該群組可以包含多個主機。	KUMA 關聯器主機群組包含 ansible_host 變數，該變數會指定主機的唯一 FQDN 與 IP 位址。	kuma
kuma_storage	KUMA儲存體主機群組。該群組可以包含多個主機。	KUMA 儲存體主機群組包含 ansible_host 變數，該變數會指定主機的唯一 FQDN 與 IP 位址。	kuma

用於在單一主機上安裝KUMA服務的KUMA清查檔案範本範例（single.inventory.yaml檔案）

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 1
```

用於在多個主機上安裝KUMA服務的KUMA清查檔案範本範例（distributed.inventory.yaml檔案）

```
all:
  vars:
```

```
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
  children:
    kuma_utils:
      hosts:
        kuma-utils.example.com:
        ansible_host: 0.0.0.0
    kuma_collector:
      hosts:
        kuma-collector-1.example.com:
        ansible_host: 0.0.0.0
    kuma_correlator:
      hosts:
        kuma-correlator-1.example.com:
        ansible_host: 0.0.0.0
    kuma_storage:
      hosts:
        kuma-storage-1.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 1
            keeper: 1
        kuma-storage-2.example.com:
            ansible_host: 0.0.0.0
            shard: 1
            replica: 2
            keeper: 2
        kuma-storage-3.example.com:
            ansible_host: 0.0.0.0
            shard: 2
            replica: 1
            keeper: 3
        kuma-storage-4.example.com:
            ansible_host: 0.0.0.0
            shard: 2
            replica: 2
```

多節點部署：指定安裝參數

組態檔是YAML格式的檔案，包含Kaspersky Next XDR Expert元件的安裝參數集。

下表列出的安裝參數是Kaspersky Next XDR Expert多節點部署所必需的。若要在單一節點上部署Kaspersky Next XDR Expert，請使用包含特定於單節點部署的安裝參數的設定檔。

組態檔的範本（multinode.smp_param.yaml.template）位於KDT公用程式檔案中的分發套件中。您可以手動填寫組態檔範本；或使用部署精靈指定Kaspersky Next XDR Expert部署所需的安裝參數，然後產生組態檔。

組態檔模板中並未包含下面列出的所有參數。此範本僅包含部署Kaspersky Next XDR Expert之前必須指定的參數。其餘參數設定為預設值，不包含在範本中。您可以手動將這些參數新增至組態檔以覆蓋其值。參數值必須遵循下面所述的規則。在Kaspersky Next XDR Expert 部署期間，KDT會檢查是否正確指定了所需的安裝參數。如果組態檔中必需的參數缺失或無效，部署將會中斷。

Kaspersky Next XDR Expert多節點部署組態檔範例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Nodes on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
  # Control node settings.
    # 節點名稱。 此值長度必須為 1 到 63 個字元。
    # The node name can contain only ASCII characters: letters (a-z; A-Z), numbers (0-9),
    and hyphen (-).
  - desc: cdt-primary1
    # The node type.
    # Possible node types: control, worker.
    # The primary node is intended for managing the cluster, storing metadata, and
    distributing the workload.
    type: primary
    # The IP address of the node.
    # Primary and worker nodes must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.42
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
        # A user name can contain only ASCII characters: letters (a-z; A-Z), numbers (0-
        9), and hyphen (-).
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
  # Worker node settings.
    # 節點名稱。 此值長度必須為 1 到 63 個字元。
    # The node name can contain only ASCII characters: letters (a-z; A-Z), numbers (0-9),
    and hyphen (-).
  - desc: cdt-w1
    # The node type.
    # Possible node types: control, worker.
    # The workload of Kaspersky XDR components is distributed between worker nodes.
    type: worker
    # KUMA 服務安裝在工作節點上。 可以指定一個、多個或不指定 KUMA 服務。
    kuma_roles: ["core","metrics","collector"]
    # The IP address of the node.
    # Primary and worker nodes must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.141
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
```

```
      # The user name must be 1 to 31 characters long.
      # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
      9), and hyphen (-).
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
  # Worker node settings.
    # 節點名稱。 此值長度必須為 1 到 63 個字元。
    # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
    and hyphen (-).
  - desc: cdt-w2
    # The node type.
    # Possible node types: control, worker.
    # The workload of Kaspersky XDR components is distributed between worker nodes.
    type: worker
    # The IP address of the node.
    # Primary and worker nodes must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.45
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
        # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
        9), and hyphen (-).
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
  # Worker node settings.
    # 節點名稱。 此值長度必須為 1 到 63 個字元。
    # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
    and hyphen (-).
  - desc: cdt-w3
    # The node type.
    # Possible node types: control, worker.
    # The workload of Kaspersky XDR components is distributed between worker nodes.
    type: worker
    # The IP address of the node.
    # Primary and worker nodes must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.30
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
        # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
        9), and hyphen (-).
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
# Parameters for the Kaspersky XDR deployment
parameters:
  # The connection string for access to the DBMS that is installed and configured on a
  separate server.
```

```
# user_db – 具權限的內部 DBMS 帳戶的使用者名稱。 此帳戶被授予建立資料庫及其他 DBMS 帳戶的權限。
# password_db—The password of the privileged internal DBMS account.
# fqdn_db:port_db is the fully qualified domain name and connection port of the separate server on which the DBMS is installed.
# 'psql_dsn' 參數值必須符合 URI 格式。 如果連線 URI 的任何部分包含具有特殊意義的符號，則必須使用百分比編碼進行編碼。
- name: psql_dsn
  source:
    value: "postgres://postgres:password@dbms.example.com:1234"
# IP address of the Kubernetes cluster gateway
# The Kubernetes cluster gateway is intended for connecting to the Kaspersky XDR components installed inside the Kubernetes cluster.
# The gateway must be included in the same subnet as all cluster nodes.
- name: ingress_ip
  source:
    value: 10.80.23.182
# 使用 KDT 連線至控制節點和工作節點所需的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: ssh_pk
  source:
    path: /root/.ssh/id_rsa
# Password of the Kaspersky XDR user account that will be created during the installation.
# The password must be 10 to 256 characters long.
# It can contain only ASCII characters: upper or lower case letters (A–Z, a–z), numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
# The password must not contain either whitespaces or ".@".
- name: admin_password
  source:
    value: "password"
# Disk space for the KUMA Core, in gigabytes.
# 指定為「<amount>Gi」。 預設值為 512Gi。
# If the 'low_resources' setting is set to true, the 'core_disk_request' setting is ignored and 4Gi is allocated.
- name: core_disk_request
  source:
    value: 512Gi
# 包含 KUMA 服務部署安裝設定的 KUMA 清單檔案路徑。 此檔案位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Kaspersky Endpoint Detection and Response 產品授權金鑰的路徑。 此檔案位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: license
  source:
    value: "/home/user/license.key"
# 網域名稱。 參數值必須符合最高至第四層網域的命名要求。
# The service host name and domain name are parts of FQDNs of the Kaspersky XDR services.
# Default values of service host names: nwc_host—"console", flow_host—"console", hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host—"console", api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom device names can be specified in the configuration file.
# 範例：console.smp.local 是提供 OSMP 主控台存取權限的服務的 FQDN。 此 FQDN 由「console_host」和「smp_domain」設定的值組成。
```

```
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom
certificate must be generated.
# 參數值必須是以空格分隔的主機名稱清單。 如果未指定自訂主機名稱，則會使用下列預設主機名稱：
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring"
- name: autodeploy_plan
  source:
    value: "edr"
# The user name of the account used to view OSMP metrics through the Grafana tool.
# The user name must be 1 to 30 characters long.
# A user name can contain lowercase letters ('a' to 'z'), numerals ('0' to '9') and
special characters (_ -.)&period;
# A user name must begin with a letter and may not contain spaces or the "@" character.
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# The password of the account used to view OSMP metrics through the Grafana tool.
# The password must be 8 to 256 characters long.
# It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' ,
&period; ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

為了確保KDT與設定檔正確配合使用，請在檔案末端新增一個空白行。

設定檔的 `nodes` 區段包含 Kubernetes 叢集每個 目標主機 的安裝參數。這些參數列於下表。

節點部分

參數名稱	必要	描述
`desc`	是	節點名稱。 值必須符合以下規則： • 節點名稱長度必須為1到63個字元。 • 節點名稱可以包含以下字元： • 大寫ASCII字母（A-Z） • 小寫ASCII字母（a-z） • 數字（0-9） • 連字符（-） 所有叢集節點必須具有唯一名稱。此要求安裝Kaspersky Next XDR Expert的先決條件之一，並已通過KDT驗證。
`type`	是	節點類型。 可能的參數值： • `primary` • `worker` • `loadbalancer`

參數名稱	必要	描述
`host`	是	節點的IP位址。 所有節點必須與Kubernetes叢集閘道位於同一子網路中。 節點需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。 如果您有多個主節點，則需要一個負載平衡器來在主節點之間分配傳入請求，並確保工作負載平衡。如果您想使用外部負載平衡器，請在叢集外部分配一個單獨的主機，並在組態檔中指定其參數。如果您不想使用外部負載平衡器，則工作線程節點將充當負載平衡器。
`kuma_role`	否	您可以指定要在工作線程節點上安裝的KUMA服務。您可以指定一個、多個或不指定任何KUMA服務。 當使用OSMP主控台將KUMA服務安裝在Kubernetes叢集內時，會考慮 `kuma_roles` 參數。如果您打算安裝KUMA服務的節點過載，叢集將選擇另一個負載較低的節點進行服務安裝。 KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。如果所有KUMA服務都將安裝在叢集內部，請將 `inventory` 參數設為 `/dev/null`。 不允許將由同一KUMA資源建立的儲存體放在同一工作線程節點上。此規則確保了所需的容錯性。 如果儲存體叢集包含多個儲存體實例，則所有實例必須部署在叢集內部或叢集外部。 可能的參數值： • `core`—KUMA Core • `metrics`—KUMA指標 • `collector`—收集器 • `eventrouter`—事件路由器 • `correlator`—關聯器 • `storage`—儲存體 參數值指定為包含KUMA角色的字串清單。例如： `kuma_roles: ["core","metrics","collector"]`
`user`	是	在目標主機上建立的帳戶的使用者名，用於透過KDT連線到節點。 值必須符合以下規則： • 使用者名稱長度必須為1到31個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 底線(_)、連字號（-）
`password`	否	用於連接節點的密碼。可以代替由 `ssh_pk` 參數指定的 SSH 金鑰。

其他安裝參數列於設定檔的 `parameters` 區段，如下表所述。

參數部分

參數名稱	必要	描述

psql_dsn	是	用於存取在Kubernetes叢集外部安裝和設定的DBMS的連接字串。
		如下指定此參數：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`
		其中：
		• `dbms_username` — 具權限的內部 DBMS 帳戶的使用者名稱。此帳戶被授予建立資料庫及其他 DBMS 帳戶的權限。透過使用此具權限的 DBMS 帳戶，部署期間將建立 Kaspersky Next XDR Expert 元件所需的資料庫及其他 DBMS 帳戶。
		• `password` — 具權限的內部 DBMS 帳戶的密碼。
		• `fqdn:port` — 安裝有 DBMS 的目標主機的 FQDN 與連接埠。
		若要使用高可用性叢集，請如下指定此參數：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`
		若要使用Corosync/Pacemaker，請以下列方式使用虛擬IP指定此參數：
		`psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>`
		`psql_dsn` 參數值必須符合 URI 格式。若連線 URI 的任一部分包含具有特殊意義的符號，則必須以百分比編碼進行編碼。
		`psql_dsn` 參數值中必須替換的符號：
		• 空白字元 → `%20`
		• ! → `%21`
		• # → `%23`
		• % → `%25`
		• & → `%26`
		• / → `%2F`
		• : → `%3A`
		• = → `%3D`
		• ? → `%3F`
		• @ → `%40`
		• [→ `%5B`
		•] → `%5D`
		請參閱PostgreSQL 連線字串一文以瞭解詳細資訊。

nwc-language	是	預設指定OSMP主控台介面的語言。安裝後，您可以變更OSMP主控台語言。 可能的參數值： • `enUS`（預設值） • `ruRu` 如果未在組態檔中指定此參數，則使用預設值。
ingress_ip	是	Kubernetes叢集閘道的保留靜態IPv4位址。 Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。閘道必須包含在與主節點和工作線程節點相同的子網中。
ssh_pk	是	位於管理主機上 SSH 金鑰私鑰部分的路徑，該金鑰用於透過 KDT 連線至主要工作節點及具有 KUMA 服務的節點（收集器、關聯器與儲存體）。參數值必須為Linux檔案路徑或Base64編碼的檔案內容。

參數名稱	必要	描述
admin_password	是	admin_password 參數指定安裝過程中 KDT 所建立之 Kaspersky Next XDR Expert 使用者帳戶的密碼。該帳戶的預設使用者名稱為「admin」。 主管理員角色已指派給此使用者帳戶。 密碼必須符合以下規則： • 使用者密碼不能少於10個或多於256個字元。 • 密碼必須包含以下組中三組的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密碼不得包含任何空格或".@"組合。 手動指定 admin_password 參數值（而非透過部署精靈指定）時，請確保此值符合 YAML 標準對字串值的要求： • 包含特殊字元的參數值必須用單引號引起來。 • 參數值中的任何單引號'都必須重複以轉義此單引號。 範例：使用者帳戶密碼 Any_pass%1234'5678"90 必須指定為 admin_password 參數的值 'Any_pass%1234''5678"90'。
low_resources	否	此參數表示 Kaspersky Next XDR Expert 已安裝在運算資源有限的目標主機上。若要進行多節點部署，請將 low_resources 參數設定為 false。 可能的參數值： • true — 使用有限計算資源進行安裝（用於單節點部署） • false — 標準安裝（預設值）
core_disk_request	是	指定KUMA Core運行所需磁碟空間量的參數。 若未指定 core_disk_request 參數，且 low_resources 參數設定為 false 或未指定，KUMA Core 運行所需的預設磁碟空間量為 100 GB。 若未指定 core_disk_request 參數，且 low_resources 參數設定為 true，KUMA Core 運行所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 core_disk_request 參數。
metrics_disk_request	是	指定Metrics服務運作所需磁碟空間量的參數。 若未指定 metrics_disk_request 參數，且 low_resources 參數設定為 false 或未指定，Metrics 服務運作所需的預設磁碟空間量為 80 GB。 若未指定 metrics_disk_request 參數，且 low_resources 參數設定為 true，Metrics 服務運作所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 metrics_disk_request 參數。
inventory	是	位於管理員主機上的KUMA清查檔案的路徑。此清查檔案包含用於部署Kubernetes叢集中未包含的KUMA服務的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。如果所有 KUMA 服務都將安裝在叢集內部，請將 inventory 參數設為 /dev/null。
host_inventory	否	位於管理員主機上的附加KUMA清查檔案的路徑。此檔案包含用於部分新增或刪除具有KUMA服務的主機的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若執行 Kaspersky Next XDR Expert 的初始部署或執行需要設定檔的自訂動作，請保留預設參數值 (/dev/null)。
license	否	位於管理員主機上的KUMA產品授權金鑰的路徑。 參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 部署完成並登入OSMP後，您可以上傳產品授權金鑰或指定啟動碼。

參數名稱	必要	描述

`nwc_host`
`flow_host`
`hydra_host`
`login_host`
`ksc_host`
`console_host`
`api_host`
`kuma_host`
`monitoring_host`
`xdr_edr_ingress_host`
	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的主機名稱。服務主機名稱與網域名稱（ `smp_domain` 參數值）皆為服務 FQDN 的組成部分。
		如果未指定自訂主機名稱，則使用下列預設主機名稱：
		• `nwc_host—"console"`
		• `flow_host—"console"`
		• `hydra_host—"console"`
		• `login_host—"console"`
		• `ksc_host—"admsrv"`
		• `console_host—"console"`
		• `api_host—"api"`
		• `kuma_host—"kuma"`
		• `monitoring_host—"monitoring"`
		• `xdr_edr_ingress_host—"agentserver"`

`smp_domain`	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的網域名稱。參數值必須符合最高四級網域的命名要求。 服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 `console_host` 變數的值為 `console`，而 `smp_domain` 變數的值為 `smp.local`，則提供 OSMP 主控台存取權的服務完整名稱為 `console.smp.local`。
`pki_host_list`	是	將生成自簽名或自訂憑證的公共Kaspersky Next XDR Expert服務的主機名稱列表。參數值必須是主機名稱列表，以空格分隔。
`intermediate_enabled`	否	該參數用於指示是否對 Kaspersky Next XDR Expert 公開服務使用自訂中間憑證而非自我簽署憑證。 可能的參數值： • `true` — 使用自訂中間憑證。 • `false` — 使用自我簽署憑證（預設值）。
`intermediate_bundle`	否	用於與 Kaspersky Next XDR Expert 公開服務協作之自訂中間憑證的路徑。若 `intermediate_enabled` 參數設定為 `true`，則指定此參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。自訂中級憑證的有效期限必須至少為399天。

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	否	用於與對應的公開 Kaspersky Next XDR Expert 服務搭配運作的自訂葉憑證路徑：`<admsrv_host>.<smp_domain>`、`<api_host>.<smp_domain>`、`<kuma_host>.<smp_domain>`、`<monitoring_host>.<smp_domain>` 和 `<console_host>.<smp_domain>`。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。
		如果要指定自訂葉憑證，請將 `intermediate_enabled` 參數設定為 `false`，且不要指定 `intermediate_bundle` 參數和 `pki_host_list` 參數。

`ksc_state_size`	是	分配用於儲存管理伺服器資料（更新、安裝套件和其他內部服務資料）的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。所需的可用磁碟空間量取決於受管理裝置的數量和其他參數，並且可以計算。 預設值為 30 GB。如果未在設定檔中指定此參數，則使用此值。
`prometheus_size`	是	分配給儲存指標的可用磁碟空間量。以GB為單位，指定為「<amount>GB」。 最小值與預設值皆為5GB。如果未在組態檔中指定此參數，則使用預設值。
`grafana_admin_user`	否	用於透過Grafana工具檢視OSMP指標的帳戶的使用者名稱。 值必須符合以下規則： • 使用者名稱長度必須為1到30個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 特殊字元（_ - .） • 使用者名稱必須以字母開頭。 • 使用者名稱不能包含空格或"@"符號。

參數名稱	必要	描述
`grafana_admin_password`	否	用於透過Grafana工具檢視OSMP指標的帳戶的密碼。 密碼必須符合以下規則： • 使用者密碼不能少於8個或多於256個字元。 • 密碼必須包含下列群組中的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配給儲存OSMP日誌的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。 最低建議值和預設值為 40 GB。如果未在組態檔中指定此參數，則使用預設值。
`loki_retention_period`	是	OSMP日誌的儲存週期，超過此週期後日誌將自動刪除。預設值為72小時（將設定檔中的參數值設定為「<time in hours>h」。例如：「72h」）。如果未在組態檔中指定此參數，則使用預設值。
`file_storage_cp`	否	指派給元件用於儲存資料以處理回應操作的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。最小推薦值為20 GB。
`psql_tls_off`	否	指示是否使用 TLS 協定對 Kaspersky Next XDR Expert 元件與 DBMS 之間的流量進行加密的參數。若 DBMS 安裝在叢集外部，則預設停用 TLS 加密（預設值為 `true`）。 可能的參數值： • `true` — 不加密流量（預設值）。 • `false` — 加密流量。
`psql_trusted_cas`	否	可以包含DBMS伺服器的TLS憑證或可以簽發TLS伺服器憑證的根憑證的PEM檔案的路徑。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若將在單獨的伺服器上安裝與設定 DBMS，並且已啟用流量加密（`psql_tls_off` 設定為 `false`），則請指定 `psql_trusted_cas` 參數。
`proxy_enabled`	否	指示是否使用代理伺服器將 Kaspersky Next XDR Expert 元件連線至網際網路的參數。若安裝 Kaspersky Next XDR Expert 的主機具有網際網路存取權限，亦可為 Kaspersky Next XDR Expert 元件（例如管理伺服器）的運作以及特定整合（包括卡巴斯基與第三方）提供網際網路存取權限。若要建立代理連線，還須在管理伺服器內容中指定代理伺服器參數。 可能的參數值： • `true` — 使用代理伺服器。 • `false` — 不使用代理伺服器（預設值）。
`proxy_addresses`	否	代理伺服器的IP位址。若代理伺服器使用多個 IP 位址，請指定這些位址，並以空格分隔（例如，`"0.0.0.0 0.0.0.1 0.0.0.2"`）。若 `proxy_enabled` 參數設定為 `true`，則指定此參數。
`proxy_port`	否	用於建立代理連線的連接埠號碼。若 `proxy_enabled` 參數設定為 `true`，則指定此參數。
`console_port`	否	用於指定連線至 OSMP 主控台伺服器所用的自訂連接埠號碼的參數。預設值是443。
`as_smp_port`	否	用於指定 Endpoint Agent 連線至 agentserver 元件所用的自訂連接埠號碼的參數。預設值是443。
`kuma_gateway_telemetry_listener_port`	否	用於指定傳送遙測資料所用的自訂連接埠號碼的參數。預設值是443。
`trace_level`	否	管理伺服器追蹤檔案的詳盡程度。追蹤在管理伺服器運作期間寫入。 預設值為0，不寫入任何追蹤。 可能的參數值：0–5。 參數值越高，追蹤詳細資訊越詳盡。

參數名稱	必要	描述
ansible_extra_flags	否	KDT執行的KUMA Core和KUMA服務部署日誌的詳盡程度。 可能的參數值： • -v • -vv • -vvv • -vvvv 隨著旗標中「v」字母數量的增加，日誌將變得更詳盡。如果組態檔中未指定此參數，則將儲存標準元件安裝日誌。
incident_attachments_max_count_limit	否	可附加到事件的檔案數量。預設值是 100。
incident_attachments_max_size_limit	否	已附加到事件的檔案總大小。以位元組為單位。指定時不指明測量單位。預設值是 26214400。
ignore_precheck	否	該參數用於指示是否在部署前檢查Kubernetes叢集節點的硬體、軟體及網路設定，以確認是否符合解決方案的安裝先決條件。 可能的參數值： • true — 略過預檢查。 • false — 執行預檢查（預設值）。
airgap_mode	否	此參數指示是否執行APT軟體套件管理器預檢查並更新軟體套件快取。這可讓您在實體隔離環境中部署Kaspersky Next XDR Expert。 可能的參數值： • true — 略過預檢查和軟體套件快取更新。 • false — 執行預檢查並更新軟體套件快取（預設值）。
grafana_smtp_host	否	Grafana的SMTP伺服器位址，用於發送有關Kubernetes叢集運行狀況事件的電子郵件通知。請以 <host>:<port> 格式指定此參數，例如 localhost:25。
grafana_smtp_user	否	在SMTP伺服器上進行身份驗證的使用者名稱。
grafana_smtp_password	否	在SMTP伺服器上進行身份驗證的密碼。
grafana_smtp_bundle	否	包含X.509憑證鏈的檔案，用於驗證與SMTP伺服器的TLS連線。
grafana_smtp_skip_verify	否	此參數指示是否跳過SMTP伺服器的TLS憑證驗證。 可能的參數值： • true—跳過TLS憑證驗證。 • false—執行TLS憑證驗證（預設值）。
grafana_smtp_from_address	否	寄件者的電子郵件地址，該地址將顯示在發送電子郵件通知時的「寄件者」欄位中。
grafana_smtp_from_name	否	電子郵件通知中顯示的寄件者名稱。
grafana_smtp_ehlo_identity	否	連線到SMTP伺服器時，EHLO命令中使用的識別碼。
grafana_starttls_policy	否	連線SMTP伺服器時使用STARTTLS的政策。 可能的參數值： • OpportunisticStartTLS—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器。 • MandatoryStartTLS—需要STARTTLS；如果SMTP伺服器不支援STARTTLS，則失敗。 • NoStartTLS—不使用STARTTLS；以不加密的方式連線到SMTP伺服器。 • empty—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器（預設值）。
grafana_smtp_enable_tracing	否	此參數指示是否啟用SMTP連線偵錯以偵錯電子郵件發送。 可能的參數值： • true—啟用SMTP連線偵錯。 • false—停用SMTP連線偵錯（預設值）。

參數名稱	必要	描述
autodeploy_plan	否	此參數指示是為Kaspersky EDR部署還是為Kaspersky NGFW部署KUMA服務。 可能的參數值： • edr—在 Kubernetes 叢集內為 OSMP 和 Kaspersky EDR 部署 KUMA 服務（預設值）。 • ngfw—在 Kubernetes 叢集內為 OSMP 和 Kaspersky NGFW 部署 KUMA 服務。此外，預先定義的收集器 **[OOTB] Kaspersky NGFW** 將安裝在 KUMA 清單檔案中 kuma_collector 參數指定的主機清單中的第一個主機上。 • none—不為 Kaspersky EDR 或 Kaspersky NGFW 部署 KUMA 服務。在未部署 Kaspersky EDR 和 Kaspersky NGFW 的 KUMA 服務情況下部署 Kaspersky Next XDR Expert，或從備份還原 Kaspersky Next XDR Expert 時，請指定此值。還原 Kaspersky Next XDR Expert 時，指定 edr 或 ngfw 可能會導致已部署的服務與備份副本中的服務發生衝突。
tokenhub_access_token	否	存取權杖的存留期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可用值為 5m，最大值為 2h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 您可以在應用程式部署後再變更 tokenhub_access_token 參數。
tokenhub_refresh_token	否	用於取得新存取權杖的重新整理權杖有效期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可用值為 12h，最大值為 4320h。 預設值是 24h。如果未在設定檔中指定此參數，則使用此值。 應用程式部署後，您可以再變更 tokenhub_refresh_token 參數。
credentials_session_ttl	否	單一登入工作階段的最大閒置時間。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可用值為 5m，最大值為 96h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 應用程式部署後，您可以再變更 credentials_session_ttl 參數。

單節點部署：指定安裝參數

用於在單一節點上部署Kaspersky Next XDR Expert的組態檔，包含多節點部署與單節點部署都需要的安裝參數。此外，此組態檔包含僅適用於單節點部署的參數：openbao_ha_mode、openbao_standalone 和 default_class_replica_count)。

組態檔範本（singlenode.smp_param.yaml.template）位於具有KDT公用程式的存檔的分發套件中。您可以手動填寫組態檔範本；或使用部署精靈指定Kaspersky Next XDR Expert部署所需的安裝參數，然後產生組態檔。

組態檔模板中並未包含下面列出的所有參數。此範本僅包含部署Kaspersky Next XDR Expert之前必須指定的參數。其餘參數設定為預設值，不包含在範本中。您可以手動將這些參數新增至組態檔以覆蓋其值。參數值必須遵循下面所述的規則。在Kaspersky Next XDR Expert 部署期間，KDT會檢查是否正確指定了所需的安裝參數。如果組態檔中必需的參數缺失或無效，部署將會中斷。

Kaspersky Next XDR Expert多節點部署組態檔範例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Node on which the Kubernetes cluster and Kaspersky XDR will be deployed
```

```
nodes:
  # Primary/worker node settings.
    # 節點名稱。 此值長度必須為 1 到 63 個字元。
    # The node name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–9),
    and hyphen (-).
  - desc: cdt-1
    # The node type.
    # 若為單一節點部署，請將「type」設定為「primary-worker」。 在此情況下，目標主機將充當主要節
    點與工作節點。
    type: primary-worker
    # The IP address of the node.
    # The primary worker node must be included in the same subnet as the Kubernetes
    cluster gateway.
    host: 10.80.23.42
    access:
      ssh:
        # User account name.
        # A user account is created on the target device and is used by KDT for connection
        to the node.
        # The user name must be 1 to 31 characters long.
        # A user name can contain only ASCII characters: letters (a–z; A–Z), numbers (0–
        9), and hyphen (-).
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
# Parameters for the Kaspersky XDR deployment
parameters:
  # The connection string for access to the DBMS that is installed and configured on a
  separate server.
  # user_db — 具權限的內部 DBMS 帳戶的使用者名稱。 此帳戶被授予建立資料庫及其他 DBMS 帳戶的權
  限。
  # password_db—The password of the privileged internal DBMS account.
  # fqdn_db:port_db is the fully qualified domain name and connection port of the
  separate server on which the DBMS is installed.
  # 'psql_dsn' 參數值必須符合 URI 格式。 如果連線 URI 的任何部分包含具有特殊意義的符號，則必須使
  用百分比編碼進行編碼。
  - name: psql_dsn
    source:
      value: "postgres://postgres:password@dbms.example.com:1234"
  # IP address of the Kubernetes cluster gateway
  # The Kubernetes cluster gateway is intended for connecting to the Kaspersky XDR
  components installed inside the Kubernetes cluster.
  # The gateway must be included in the same subnet as the primary worker node.
  - name: ingress_ip
    source:
      value: 10.80.23.182
  # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
  # The parameter value must be a Linux file path or Base64-encoded file content.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky XDR user account that will be created during the
  installation.
  # The password must be 10 to 256 characters long.
  # It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
  numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \
  ` ~ " ( ) ;).
  # The password must not contain either whitespaces or ".@".
```

```
- name: admin_password
  source:
    value: ""
# The parameter indicating that Kaspersky XDR is installed on the target host with
limited computing resources.
# For the single-node deployment, set the 'low_resources' parameter to "true" so that
Kaspersky Next XDR Expert components will require less memory and CPU resources.
# Also, if you enable this parameter, 4 GB of free disk space will be allocated to
install KUMA Core on the target host.
- name: low_resources
  source:
    value: "true"
# The number of disk volumes that are used to store the service data of Kaspersky XDR
components and KDT.
# For the single-node deployment, set the parameter value to "1".
- name: default_class_replica_count
  source:
    value: "1"
# The parameter that indicates whether to run the secret storage in the High
Availability (HA) mode.
# For the single-node deployment, set the parameter value to "false".
- name: openbao_ha_mode
  source:
    value: "false"
# The parameter that indicates whether to run the secret storage in the standalone
mode.
# For the single-node deployment, set the parameter value to "true"&period;
- name: openbao_standalone
  source:
    value: "true"
# 包含 KUMA 服務部署安裝設定之 KUMA 清單檔案的路徑。 此檔案位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Kaspersky Endpoint Detection and Response 產品授權金鑰的路徑。 此檔案位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: license
  source:
    value: "/home/user/license.key"
# 網域名稱。 參數值必須符合第二層網域名稱的命名要求。
# The service host name and domain name are parts of FQDNs of the Kaspersky XDR
services.
# Default values of service host names: nwc_host—"console", flow_host—"console",
hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host—"console",
api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom device names can be specified in the configuration file.
# 範例：console.smp.local 是提供 OSMP 主控台存取權限的服務的 FQDN。 此 FQDN 由
「console_host」和「smp_domain」設定的值組成。
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom
certificate must be generated.
# 參數值必須是以空格分隔的主機名稱清單。 如果未指定自訂主機名稱，則會使用下列預設主機名稱：
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring"
```

```
- name: autodeploy_plan
  source:
    value: "edr"
# The user name of the account used to view OSMP metrics through the Grafana tool.
# The user name must be 1 to 30 characters long.
# A user name can contain lowercase letters ('a' to 'z'), numerals ('0' to '9') and
special characters (_ -.)&period;
# A user name must begin with a letter and may not contain spaces or the "@" character.
- name: grafana_admin_user
  source:
    value: "grafana_admin_user"
# The password of the account used to view OSMP metrics through the Grafana tool.
# The password must be 8 to 256 characters long.
# It can contain only ASCII characters: upper or lower case letters (A–Z, a–z),
numerals (0–9), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' ,
&period; ? / \ ` ~ " ( ) ;).
- name: grafana_admin_password
  source:
    value: "grafana_admin_password"
```

為了確保KDT與設定檔正確配合使用，請在檔案末端新增一個空白行。

設定檔的 `nodes` 區段包含下表所列的目標主機參數。

節點部分

參數名稱	必要	描述
`desc`	是	節點名稱。 值必須符合以下規則： • 節點名稱長度必須為1到63個字元。 • 節點名稱可以包含以下字元： • 大寫ASCII字母（A-Z） • 小寫ASCII字母（a-z） • 數字（0-9） • 連字符（-） 所有叢集節點必須具有唯一名稱。此要求安裝Kaspersky Next XDR Expert的先決條件之一，並已通過KDT驗證。
`type`	是	節點類型。 對於目標主機，請將 `type` 參數設定為 `primary-worker`，以啟用**單節點部署**。此種情況下，目標主機將充當主要節點與工作節點。
`host`	是	節點的IP位址。 主要工作線程節點必須與Kubernetes叢集閘道位於同一子網路中。 該節點需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。
`kuma_role`	否	您可以指定要在工作線程節點上安裝的KUMA服務。 KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。如果所有KUMA服務都將安裝在叢集內部，請將 `inventory` 參數設為 `/dev/null`。 對於**單節點部署**，請將此參數留空，因為所有服務都會安裝在單一節點上。

參數名稱	必要	描述
`user`	是	在目標主機上建立的帳戶的使用者名，用於透過KDT連線到節點。 值必須符合以下規則： • 使用者名稱長度必須為1到31個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 底線(_)、連字號（-）
`password`	否	用於連接節點的密碼。可以代替由 `ssh_pk` 參數指定的 SSH 金鑰。

其他安裝參數列於設定檔的 `parameters` 區段，如下表所述。

參數部分

參數名稱	必要	描述

`psql_dsn`	是	用於存取在Kubernetes叢集外部安裝和設定的DBMS的連接字串。
		如下指定此參數：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`
		其中：
		• `dbms_username` — 具權限的內部 DBMS 帳戶的使用者名稱。此帳戶被授予建立資料庫及其他 DBMS 帳戶的權限。透過使用此具權限的 DBMS 帳戶，部署期間將建立 Kaspersky Next XDR Expert 元件所需的資料庫及其他 DBMS 帳戶。
		• `password` — 具權限的內部 DBMS 帳戶的密碼。
		• `fqdn:port` — 安裝有 DBMS 的目標主機的 FQDN 與連接埠。
		如果您的 DBMS 與 Kubernetes 叢集節點安裝在相同主機上，請勿在 `psql_dsn` 參數中使用 `localhost` 或 `127.0.0.1` 作為 DBMS 位址。請使用可透過叢集網路存取的主機IP位址（而非環回位址）。
		若要使用高可用性叢集，請如下指定此參數：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`
		若要使用Corosync/Pacemaker，請以下列方式使用虛擬IP指定此參數：
		`psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>`
		`psql_dsn` 參數值必須符合 URI 格式。若連線 URI 的任一部分包含具有特殊意義的符號，則必須以百分比編碼進行編碼。
		`psql_dsn` 參數值中必須替換的符號：
		• 空白字元 → `%20`
		• ! → `%21`
		• # → `%23`
		• % → `%25`
		• & → `%26`
		• / → `%2F`
		• : → `%3A`
		• = → `%3D`
		• ? → `%3F`
		• @ → `%40`
		• [→ `%5B`
		•] → `%5D`
		請參閱PostgreSQL 連線字串文章以取得詳細資訊。

`nwc-language`	是	預設指定OSMP主控台介面的語言。安裝後，您可以變更OSMP主控台語言。 可能的參數值： • `enUS`（預設值） • `ruRu` 如果未在組態檔中指定此參數，則使用預設值。
`ingress_ip`	是	Kubernetes叢集閘道的保留靜態IPv4位址。 Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。閘道必須與主要工作線程節點位於同一子網路中。 Kubernetes叢集閘道需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。 此參數的值不能是執行部署的同一主機的IP地址。

參數名稱	必要	描述
`ssh_pk`	是	位於管理主機上 SSH 金鑰私鑰部分的路徑，該金鑰用於透過 KDT 連線至主要工作節點及具有 KUMA 服務的節點（收集器、關聯器與儲存體）。參數值必須為Linux檔案路徑或Base64編碼的檔案內容。
`admin_password`	是	`admin_password` 參數指定安裝過程中 KDT 所建立之 Kaspersky Next XDR Expert 使用者帳戶的密碼。該帳戶的預設使用者名稱為「admin」。 主管理員角色已指派給此使用者帳戶。 密碼必須符合以下規則： • 使用者密碼不能少於10個或多於256個字元。 • 密碼必須包含以下組中三組的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密碼不得包含任何空格或".@"組合。 手動指定 `admin_password` 參數值（而非透過部署精靈指定）時，請確保此值符合 YAML 標準對字串值的要求： • 包含特殊字元的參數值必須用單引號引起來。 • 參數值中的任何單引號'都必須重複以轉義此單引號。 範例：使用者帳戶密碼 `Any_pass%1234'5678"90` 必須指定為 `admin_password` 參數的值 `'Any_pass%1234''5678"90'`。
`low_resources`	是	表示Kaspersky Next XDR Expert安裝在計算資源有限的目標主機上的參數。 可能的參數值： • `true` — 使用有限計算資源進行安裝（用於單節點部署） • `false` — 標準安裝 對於**單節點部署**，請將 `low_resources` 參數設定為 `true`，使 Kaspersky Next XDR Expert 元件佔用更少的記憶體與 CPU 資源。此外，若啟用此參數，系統將配置 4 GB 的可用磁碟空間，以便在目標主機上安裝 KUMA Core。
`openbao_ha_mode`	是	指示是否在高可用性（HA）模式下執行密鑰儲存的參數。 可能的參數值： • `true` • `false` 對於**單節點部署**，請將 `openbao_ha_mode` 參數設定為 `false`。
`openbao_standalone`	是	指示是否在獨立模式下執行密鑰儲存的參數。 可能的參數值： • `true` • `false` 對於**單節點部署**，請將 `openbao_standalone` 參數值設定為 `true`。
`default_class_replica_count`	是	用於儲存 Kaspersky Next XDR Expert 元件與 KDT 的服務資料的磁碟區數量。 預設值是 `3`。 對於**單節點部署**，請將 `default_class_replica_count` 參數值設定為 `1`。
`core_disk_request`	是	指定KUMA Core運行所需磁碟空間量的參數。 若未指定 `core_disk_request` 參數，且 `low_resources` 參數設定為 `false` 或未指定，KUMA Core 運行所需的預設磁碟空間量為 100 GB。 若未指定 `core_disk_request` 參數，且 `low_resources` 參數設定為 `true`，KUMA Core 運行所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 `core_disk_request` 參數。
`metrics_disk_request`	是	指定Metrics服務運作所需磁碟空間量的參數。 若未指定 `metrics_disk_request` 參數，且 `low_resources` 參數設定為 `false` 或未指定，Metrics 服務運作所需的預設磁碟空間量為 80 GB。 若未指定 `metrics_disk_request` 參數，且 `low_resources` 參數設定為 `true`，Metrics 服務運作所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 `metrics_disk_request` 參數。
`inventory`	是	位於管理員主機上的KUMA清查檔案的路徑。此清查檔案包含用於部署Kubernetes叢集中未包含的KUMA服務的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。如果所有 KUMA 服務都將安裝在叢集內部，請將 `inventory` 參數設為 `/dev/null`。

參數名稱	必要	描述
host_inventory	否	位於管理員主機上的附加KUMA清查檔案的路徑。此檔案包含用於部分新增或刪除具有KUMA服務的主機的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若執行 Kaspersky Next XDR Expert 的初始部署或執行需要設定檔的自訂動作，請保留預設參數值 (/dev/null)。
license	否	位於管理員主機上的KUMA產品授權金鑰的路徑。 參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 部署完成並登入OSMP後，您可以上傳產品授權金鑰或指定啟動碼。
nwc_host flow_host hydra_host login_host ksc_host console_host api_host kuma_host monitoring_host xdr_edr_ingress_host	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的主機名稱。服務主機名稱與網域名稱（ smp_domain 參數值 ）皆為服務 FQDN 的組成部分。 如果未指定自訂主機名稱，則使用下列預設主機名稱： • nwc_host—"console" • flow_host—"console" • hydra_host—"console" • login_host—"console" • ksc_host—"admsrv" • console_host—"console" • api_host—"api" • kuma_host—"kuma" • monitoring_host—"monitoring" • xdr_edr_ingress_host—"agentserver"
smp_domain	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的網域名稱。參數值必須符合最高四級網域的命名要求。 服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 console_host 變數的值為 console，而 smp_domain 變數的值為 smp.local，則提供 OSMP 主控台存取權的服務完整名稱為 console.smp.local。
pki_host_list	是	將生成自簽名或自訂憑證的公共Kaspersky Next XDR Expert服務的主機名稱列表。參數值必須是主機名稱列表，以空格分隔。
intermediate_enabled	否	該參數用於指示是否對 Kaspersky Next XDR Expert 公開服務使用自訂中間憑證而非自我簽署憑證。 可能的參數值： • true — 使用自訂中間憑證。 • false — 使用自我簽署憑證（預設值）。
intermediate_bundle	否	用於與 Kaspersky Next XDR Expert 公開服務協作之自訂中間憑證的路徑。若 intermediate_enabled 參數設定為 true，則指定此參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。自訂中級憑證的有效期限必須至少為399天。
admsrv_bundle api_bundle console_bundle kuma_bundle monitoring_bundle	否	用於與對應的公開 Kaspersky Next XDR Expert 服務搭配運作的自訂葉憑證路徑：<admsrv_host>.<smp_domain> 、<api_host>.<smp_domain> 、<kuma_host>.<smp_domain> 、<monitoring_host>.<smp_domain> 和 <console_host>.<smp_domain>。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 如果要指定自訂葉憑證，請將 intermediate_enabled 參數設定為 false，且不要指定 intermediate_bundle 參數和 pki_host_list 參數。
ksc_state_size	是	分配用於儲存管理伺服器資料（更新、安裝套件和其他內部服務資料）的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。所需的可用磁碟空間量取決於受管理裝置的數量和其他參數，並且可以計算。 預設值為 30 GB。如果未在設定檔中指定此參數，則使用此值。
prometheus_size	是	分配給儲存指標的可用磁碟空間量。以GB為單位，指定為「<amount>GB」。 最小值與預設值皆為5GB。如果未在組態檔中指定此參數，則使用預設值。

參數名稱	必要	描述
`grafana_admin_user`	否	用於透過Grafana工具檢視OSMP指標的帳戶的使用者名稱。 值必須符合以下規則： • 使用者名稱長度必須為1到30個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 特殊字元（_ - .） • 使用者名稱必須以字母開頭。 • 使用者名稱不能包含空格或"@"符號。
`grafana_admin_password`	否	用於透過Grafana工具檢視OSMP指標的帳戶的密碼。 密碼必須符合以下規則： • 使用者密碼不能少於8個或多於256個字元。 • 密碼必須包含下列群組中的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配給儲存OSMP日誌的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。 最低建議值和預設值為 40 GB。如果未在組態檔中指定此參數，則使用預設值。
`loki_retention_period`	是	OSMP日誌的儲存週期，超過此週期後日誌將自動刪除。預設值為72小時（將設定檔中的參數值設定為「<time in hours>h」。例如：「72h」）。如果未在組態檔中指定此參數，則使用預設值。
`file_storage_cp`	否	指派給元件用於儲存資料以處理回應操作的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。最小推薦值為20 GB。
`psql_tls_off`	否	指示是否使用 TLS 協定對 Kaspersky Next XDR Expert 元件與 DBMS 之間的流量進行加密的參數。若 DBMS 安裝在叢集外部，則預設停用 TLS 加密（預設值為 `true`）。 可能的參數值： • `true` — 不加密流量（預設值）。 • `false` — 加密流量。
`psql_trusted_cas`	否	可以包含DBMS伺服器的TLS憑證或可以簽發TLS伺服器憑證的根憑證的PEM檔案的路徑。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若將在單獨的伺服器上安裝與設定 DBMS，並且已啟用流量加密（`psql_tls_off` 設定為 `false`），則請指定 `psql_trusted_cas` 參數。
`proxy_enabled`	否	指示是否使用代理伺服器將 Kaspersky Next XDR Expert 元件連線至網際網路的參數。若安裝 Kaspersky Next XDR Expert 的主機具有網際網路存取權限，亦可為 Kaspersky Next XDR Expert 元件（例如管理伺服器）的運作以及特定整合（包括卡巴斯基與第三方）提供網際網路存取權限。若要建立代理連線，還須在管理伺服器內容中指定代理伺服器參數。 可能的參數值： • `true` — 使用代理伺服器。 • `false` — 不使用代理伺服器（預設值）。
`proxy_addresses`	否	代理伺服器的IP位址。若代理伺服器使用多個 IP 位址，請指定這些位址，並以空格分隔（例如，`"0.0.0.0 0.0.0.1 0.0.0.2"`）。若 `proxy_enabled` 參數設定為 `true`，則指定此參數。
`proxy_port`	否	用於建立代理連線的連接埠號碼。若 `proxy_enabled` 參數設定為 `true`，則指定此參數。
`console_port`	否	用於指定連線至 OSMP 主控台伺服器所用的自訂連接埠號碼的參數。預設值是443。
`as_smp_port`	否	用於指定 Endpoint Agent 連線至 agentserver 元件所用的自訂連接埠號碼的參數。預設值是443。

參數名稱	必要	描述
kuma_gateway_telemetry_listener_port	否	用於指定傳送遙測資料所用的自訂連接埠號碼的參數。預設值是443。
trace_level	否	管理伺服器追蹤檔案的詳盡程度。追蹤在管理伺服器運作期間寫入。 預設值為0，不寫入任何追蹤。 可能的參數值：0–5。 參數值越高，追蹤詳細資訊越詳盡。
ansible_extra_flags	否	KDT執行的KUMA Core和KUMA服務部署日誌的詳盡程度。 可能的參數值： • -v • -vv • -vvv • -vvvv 隨著旗標中「v」字母數量的增加，日誌將變得更詳盡。如果組態檔中未指定此參數，則將儲存標準元件安裝日誌。
incident_attachments_max_count_limit	否	可附加到事件的檔案數量。預設值是 100。
incident_attachments_max_size_limit	否	已附加到事件的檔案總大小。以位元組為單位。指定時不指明測量單位。預設值是 26214400。
ignore_precheck	否	該參數用於指示是否在部署前檢查Kubernetes叢集節點的硬體、軟體及網路設定，以確認是否符合解決方案的安裝先決條件。 可能的參數值： • true — 略過預檢查。 • false — 執行預檢查（預設值）。
airgap_mode	否	此參數指示是否執行APT軟體套件管理器預檢查並更新軟體套件快取。這可讓您在實體隔離環境中部署Kaspersky Next XDR Expert。 可能的參數值： • true — 略過預檢查和軟體套件快取更新。 • false — 執行預檢查並更新軟體套件快取（預設值）。
grafana_smtp_host	否	Grafana的SMTP伺服器位址，用於發送有關Kubernetes叢集運行狀況事件的電子郵件通知。請以 <host>:<port> 格式指定此參數，例如 localhost:25。
grafana_smtp_user	否	在SMTP伺服器上進行身份驗證的使用者名稱。
grafana_smtp_password	否	在SMTP伺服器上進行身份驗證的密碼。
grafana_smtp_bundle	否	包含X.509憑證鏈的檔案，用於驗證與SMTP伺服器的TLS連線。
grafana_smtp_skip_verify	否	此參數指示是否跳過SMTP伺服器的TLS憑證驗證。 可能的參數值： • true—跳過TLS憑證驗證。 • false—執行TLS憑證驗證（預設值）。
grafana_smtp_from_address	否	寄件者的電子郵件地址，該地址將顯示在發送電子郵件通知時的「寄件者」欄位中。
grafana_smtp_from_name	否	電子郵件通知中顯示的寄件者名稱。
grafana_smtp_ehlo_identity	否	連線到SMTP伺服器時，EHLO命令中使用的識別碼。
grafana_starttls_policy	否	連線SMTP伺服器時使用STARTTLS的政策。 可能的參數值： • OpportunisticStartTLS—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器。 • MandatoryStartTLS—需要STARTTLS；如果SMTP伺服器不支援STARTTLS，則失敗。 • NoStartTLS—不使用STARTTLS；以不加密的方式連線到SMTP伺服器。 • empty—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器（預設值）。
grafana_smtp_enable_tracing	否	此參數指示是否啟用SMTP連線偵錯以偵錯電子郵件發送。 可能的參數值： • true—啟用SMTP連線偵錯。 • false—停用SMTP連線偵錯（預設值）。

參數名稱	必要	描述
autodeploy_plan	否	此參數指示是為Kaspersky EDR部署還是為Kaspersky NGFW部署KUMA服務。 可能的參數值： • edr—在 Kubernetes 叢集內為 OSMP 和 Kaspersky EDR 部署 KUMA 服務（預設值）。 • ngfw—在 Kubernetes 叢集內為 OSMP 和 Kaspersky NGFW 部署 KUMA 服務。此外，預先定義的收集器 **[OOTB] Kaspersky NGFW** 將安裝在 KUMA 清單檔案中 kuma_collector 參數指定的主機清單中的第一個主機上。 • none—不為 Kaspersky EDR 或 Kaspersky NGFW 部署 KUMA 服務。此值適用於在不為Kaspersky EDR 和Kaspersky NGFW部署KUMA服務的情況下部署Kaspersky Next XDR Expert，或用於從備份還原Kaspersky Next XDR Expert。如果您將 edr 或 ngfw 值用於還原 Kaspersky Next XDR Expert，可能會導致已部署的服務與備份中儲存的服務之間發生衝突。
tokenhub_access_token	否	存取權杖的存留期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可用值為 5m，最大值為 2h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 您可以在應用程式部署後再變更 tokenhub_access_token 參數。
tokenhub_refresh_token	否	用於取得新存取權杖的重新整理權杖有效期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可用值為 12h，最大值為 4320h。 預設值是 24h。如果未在設定檔中指定此參數，則使用此值。 應用程式部署後，您可以再變更 tokenhub_refresh_token 參數。
credentials_session_ttl	否	單一登入工作階段的最大閒置時間。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可用值為 5m，最大值為 96h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 應用程式部署後，您可以再變更 credentials_session_ttl 參數。

透過代理節點連線 Endpoint Agent

本節描述了Kaspersky Next XDR Expert端點代理程式的部署場景，以及當它們位於不同網路時向哪些伺服器傳輸資料。這種方法簡化了網路配置，同時確保了終端代理程式和伺服器之間的可靠連線。

在此應用場景中，來自端點代理程式的資料將透過中間代理節點進行路由。這樣，代理節點和解決方案之間只需建立一條網路連線，而無需每個端點代理程式都與解決方案建立多個連線。此方法適用於 Kaspersky Next XDR Expert 的單節點和多節點部署。

本節介紹如何在Linux裝置上設定Nginx代理伺服器。如有需要，您可以使用支援 mTLS Passthrough 的其他代理伺服器，以及不同的作業系統。

此場景使用在解決方案部署期間指定的公用 Kaspersky Next XDR Expert 服務的 FQDN範例（<agentserver>.<smp_domain>、<ksc_host>.<smp_domain> 和 <kuma_host>.<smp_domain>）、檔案路徑和目錄路徑。您應該將這些項目替換為符合您基礎架構的值。

如果您變更了Endpoint Agent 用於連線至 agentserver 元件的連接埠，也應在 Nginx 設定檔中指定新的連接埠號碼。

部署步驟

透過中間代理節點設定端點代理程式資料的部署涉及幾個步驟：

1 安裝和設定 Nginx

在與端點代理程式位於相同網路（子網路）的伺服器上安裝Nginx代理伺服器。

1. 執行以下指令：

```
sudo apt update
sudo apt install nginx-full
```

2. 請確保 Nginx 中包含並載入 `stream`、`stream_ssl` 和 `stream_ssl_preread` 模組：

```
nginx -V 2>&1 | grep -E 'stream|stream_ssl|stream_ssl_preread
```

指令輸出必須包含 `stream`、`stream_ssl` 和 `stream_ssl_preread` 模組。

已在伺服器上安裝包含 `stream`、`stream_ssl` 和 `stream_ssl_preread` 模組的 Nginx 代理伺服器。

3. 請確保 Nginx 設定檔（預設為 /etc/nginx/nginx.conf）包含 `stream {}` 區塊，並已在此區塊中設定 `stream.d` 目錄連線。如果缺少 `stream` 區塊，請在與 `http {}` 區塊相同的層級新增此區塊：

```
/etc/nginx/nginx.conf
...
http {
    ...
}
stream {
    include /etc/nginx/stream.d/*.conf;
}
```

4. 根據以下範本，在 /etc/nginx/stream.d/ 目錄中建立或編輯 CONF 格式的 Nginx 設定檔。

如果 /etc/nginx/stream.d/ 目錄不存在，請建立該目錄。

Nginx 設定檔的路徑和名稱：/etc/nginx/stream.d/asproxy.conf。

範本變數（使用與您的基礎架構相對應的值）：

Endpoint Agent 會與其通訊的公開 Kaspersky Next XDR Expert 服務的 FQDN 主機名稱：

- `<agentserver>.<smp_domain>` – 可透過代理整合對資產執行回應動作之元件的 FQDN。
- `in.<some_symbols>.<kuma_host>.<smp_domain>` – 遙測目標後端伺服器的 FQDN。

  如何取得伺服器位址

  1. 在主功能表中，**轉至監控→資源與服務→服務管理與操作→有效服務**。
  2. 在服務清單中，找到**[OOTB] 卡巴斯基 EDR**服務，選取它，然後在選單中按一下**「部署」**。

3. 在開啟的視窗中，複製**API閘道URL**欄位中的伺服器位址。

   伺服器名稱應採用以下格式：`in.blh4zjhm4edckdt8qyprkpm2b.kuma_host.smp_domain`。

- `<ksc_host>.<smp_domain>` – 用於代理管理的目標後端伺服器 FQDN。它可以是用於 Endpoint Agent 管理的 OSMP 元件 FQDN，或次要 KSC 伺服器的 FQDN。

IP 位址：

- `<ingress_ip>` – OSMP 叢集入口的 IP 位址。
- `<ksc_ip>` – 次要 OSMP 或 KSC 伺服器的 IP 位址（如果使用）。

連線 Endpoint Agent 的方式有三種：

- 透過政策。在此情況下，請在 Nginx 代理伺服器上設定 Endpoint Agent 與伺服器之間通訊的代理：指定 `<ksc_host>.<smp_domain>` 以及 TCP 13000、TCP 14000 和 TCP 13292 連接埠。

  範例

```
# ----- SNI → upstream ------------------------------------------------
map_hash_bucket_size 256;
map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    <ksc_host>.<smp_domain>          ksc_ingress;
    default                           deny-backend;
}
# ----- Backends------------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream ksc-ingress {
    server <ingress_ip>:13000;
    server <ingress_ip>:14000;
    server <ingress_ip>:13292;
}
upstream deny-backend {
    server 127.0.0.1:1;
}
# ----- Logging-------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;
# ----- Timeouts-----------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;
# ----- Server (port 443) --------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    listen 13000;
    listen 14000;
    listen 13292;
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

- 透過次要 OSMP 或 KSC 伺服器中的政策。在此情況下，請在 Nginx 代理伺服器上設定 Endpoint Agent 與伺服器之間通訊的代理：指定 `<ksc_host>.<smp_domain>` 以及 TCP 13000、TCP 14000 和 TCP 13292 連接埠。

  範例

```
# ----- SNI → upstream ------------------------------------------------
map_hash_bucket_size 256;
```

```
map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    <ksc_host>.<smp_domain>          ksc_ingress;
    default                           deny-backend;
}
# ----- Backends-----------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream ksc-ingress {
    server <ksc_ip>:13000;
    server <ksc_ip>:14000;
    server <ksc_ip>:13292;
}
upstream deny-backend {
    server 127.0.0.1:1;
}
# ----- Logging------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;
# ----- Timeouts----------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;
# ----- Server (port 443) ------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    listen 13000;
    listen 14000;
    listen 13292;
    ssl_preread on;              # reads only ClientHello
    proxy_pass $upstream_osmp;   # var from map
}
```

- 在本機。在此情況下，不需要設定 Nginx 代理伺服器上的 `<ksc_host>.<smp_domain>` 和 TCP 連接埠。如需更多資訊，請參閱此情境的步驟 3。

範例

```
# ----- SNI → upstream ---------------------------------------------
map_hash_bucket_size 256;
map $ssl_preread_server_name $upstream_osmp {
    hostnames;
    <agentserver>.<smp_domain>        osmp-ingress;
    in.<some_symbols>.<kuma_host>.<smp_domain>        osmp-ingress;
    default                           deny-backend;
}
# ----- Backends-----------------------------------------------------
upstream osmp-ingress {
    server <ingress_ip>:443;
}
upstream deny-backend {
    server 127.0.0.1:1;
}
# ----- Logging------------------------------------------------------
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 'sni="$ssl_preread_server_name" '
                 '"$upstream_connect_time"';
access_log /var/log/nginx/passthrough_access.log  basic;
error_log  /var/log/nginx/passthrough_error.log notice;
# ----- Timeouts----------------------------------------
preread_timeout       10s;
proxy_connect_timeout 5s;
proxy_timeout         30s;
# ----- Server (port 443) ------------------------------------------
server {
    listen 443;                  # regular TCP-port, no  TLS termination
    ssl_preread on;              # reads only ClientHello
```

```
    proxy_pass $upstream_osmp;   # var from map
}
```

5. 檢查 Nginx 設定：

```
nginx -t
```

測試成功時的指令輸出：

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

6. 重新啟動 Nginx，以套用設定檔中的變更：

```
nginx -s reload
```

已安裝的Nginx代理伺服器隨即設定為端點代理程式資料代理。

2 設定 Nginx 代理節點與 Kaspersky Next XDR Expert 之間的網路連線

1. 設定網路連線。確保網路設定（防火牆、路由）允許代理節點透過 TCP 13000、TCP 14000、TCP 13292 和 TCP 443 連接埠，對 OSMP 平台和次要 OSMP 或 KSC 伺服器建立傳出連線。
2. 設定網路，使 Endpoint Agent 節點傳送至 `<smp_domain>` 的請求路由到代理節點。

3 設定Kaspersky Endpoint Security for Windows端點代理程式使用代理節點

1. 設定網路連線。確保網路設定（防火牆、路由）允許 Endpoint Agent 透過 TCP 13000、TCP 14000、TCP 13292 和 TCP 443 連接埠，對代理節點建立傳出連線。
2. 下載下列 OSMP 憑證：
   - certificate.pem – 回應伺服器憑證
   - certificate.pfx – Endpoint Agent 憑證
   - [OOTB] Kaspersky EDR – 遙測伺服器憑證
3. 將憑證檔案複製到安裝 Endpoint Agent 的伺服器（本節範例中為 C:\Users\TestUser\）。
4. 以管理員權限開啟命令提示字元 `cmd.exe`。

5. 前往包含 Endpoint Agent 可執行檔的目錄，並執行下列命令：

```
./avp.com EDREXPERTONPREM `
/SET /mode=EDRExpertOnPrem `
/servers=<agentserver>.<smp_domain>:443 `
/server-certificate=C:\Users\TestUser\certificate.pem `
/client-certificate=C:\Users\TestUser\certificate.pfx `
/client-certificate-password=client certificate password`
/telemetry-servers=in.blh4zjhm4edckdt8qyprkpm2b.<kuma_host>.<smp_domain>:443 `
/telemetry-server-certificate='C:\Users\TestUser\[OOTB] Kaspersky EDR' `
/telemetry-client-certificate=C:\Users\TestUser\certificate.pfx `
/telemetry-client-certificate-password=client certificate password
```

6. 啟動 Kaspersky Next XDR Expert (如果尚未啟動)：

```
./avp.com start EDREXPERTONPREM
```

如需有關使用命令列設定 Endpoint Agent 的詳細資訊，請參閱 Kaspersky Endpoint Security 說明文件。

Kaspersky Next XDR Expert 部署精靈

準備 Kaspersky Next XDR Expert 部署環境涉及多個手動步驟，例如：設定安裝參數、準備目標主機，以及確認系統需求。部署精靈可讓您指定部署 Kaspersky Next XDR Expert 所需的安裝參數，然後產生組態檔。選用安裝參數會使用預設值，且無法在部署精靈中使用。您可以手動將這些參數新增至組態檔以覆蓋其預設值。

部署精靈會自動檢查目標主機是否已準備好進行部署，包括 SSH 連線能力、所需連接埠的可用性、IP 位址唯一性、叢集節點上的 DNS 名稱解析，以及時間同步。如果偵測到任何問題，精靈會顯示描述該問題的錯誤訊息。所有檢查都成功完成後，您可以儲存產生的組態檔，或直接繼續部署 Kaspersky Next XDR Expert。

部署精靈目前僅支援單一節點部署。

先決條件

- 安裝資料庫管理系統

  以單一節點組態部署 Kaspersky Next XDR Expert 之前，您必須在目標主機上手動安裝 DBMS。DBMS 和 Kaspersky Next XDR Expert 元件會安裝在同一部主機上，但 DBMS 會部署在 Kubernetes 叢集之外。

- 執行管理員、目標主機和KUMA 主機所需的所有準備步驟（如果 KUMA 服務將安裝在叢集外部的獨立伺服器上）。

Process

若要使用部署精靈指定安裝參數：

1. 在 KDT 公用程式所在的管理員主機上，使用以下命令執行部署精靈：

```
./kdt wizard -k <path_to_transport_archive> -o <path_to_configuration_file>
```

其中：

- `<path_to_transport_archive>` 是 傳輸壓縮檔案的路徑。這是選用參數，您可以稍後指定。
- `<path_to_configuration_file>` 是要儲存設定檔的路徑與設定檔名稱。這是選用參數，您可以稍後指定。

部署精靈會提示您指定安裝參數。

如果您沒有指定目錄的寫入權限，或者目錄中存在同名檔案，則會發生錯誤，精靈將會終止。

2. 輸入傳輸壓縮檔案的路徑。

   如果您在啟動部署精靈時指定了此參數，則會自動填入。

3. 輸入設定檔路徑。

   參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。如果您在啟動部署精靈時指定了此參數，則會自動填入。

4. 輸入主要工作節點的 IPv4 位址（ 設定檔的 `host` 參數）。

   此節點必須與叢集閘道 IP 位址位於相同子網路中。

5. 輸入供 KDT 用於連線至主要工作節點的帳戶使用者名稱（設定檔中的 `user` 參數）。

   值必須符合以下規則：

   - 使用者名稱長度必須為1到31個字元。
   - 使用者名稱可以包含以下字元：
     - 小寫字母（a-z）
     - 數字（0-9）
     - 底線 (_)、連字號（-）

6. 輸入連線至節點的密碼（設定檔中的 `password` 參數）。

   可以使用密碼取代 SSH金鑰。

7. 輸入私密 SSH金鑰的路徑（設定檔中的 `key` 參數）。

   私密 SSH金鑰位於管理員主機上，KDT 會使用此金鑰連線至主要工作節點。預設值是 `/root/.ssh/id_rsa`。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。

   可以使用 SSH金鑰取代密碼來連線至節點。我們建議使用SSH金鑰與節點建立連線。

8. 輸入用於存取 DBMS 的連線字串（設定檔中的 `psql_dsn` 參數）。

   如下指定此參數：`postgres://<dbms_username>:<password>@<fqdn>:<port>`

   其中：

   - `dbms_username` — 具權限的內部 DBMS 帳戶的使用者名稱。此帳戶被授予建立資料庫及其他 DBMS 帳戶的權限。透過使用此具權限的 DBMS 帳戶，部署期間將建立 Kaspersky Next XDR Expert 元件所需的資料庫及其他 DBMS 帳戶。
   - `password` — 具權限的內部 DBMS 帳戶的密碼。

- `fqdn:port` — 安裝有 DBMS 的目標主機的 FQDN 與連接埠。

  對於單節點部署，如果您的 DBMS 與 Kubernetes 叢集節點安裝在同一台主機上，請勿在連線字串中使用 `localhost` 或 `127.0.0.1` 作為 DBMS 位址。應使用主機的FQDN或IP位址。

部署精靈只會針對將 DBMS 安裝在 Kubernetes 叢集外部的部署選項指定安裝參數。

9. 請輸入位於管理員主機上的 KUMA 清查檔案的路徑（即設定檔中的 `inventory` 參數）。

   KUMA 清查檔案包含用於部署未包含在 Kubernetes 叢集中的 KUMA 服務的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。

   如果 KUMA 服務安裝在 Kubernetes 叢集中，請指定路徑 `/dev/null`。

10. 選擇 OSMP主控台介面的語言。安裝後，您可以變更 OSMP主控台語言（即設定檔中的 `nwc-language` 參數）。

    可能的值：

    - enUS
    - ruRu

11. 請輸入安裝期間 KDT 將建立的 Kaspersky Next XDR Expert 使用者帳戶的密碼（即設定檔中的 `admin_password` 參數）。

    該帳戶的預設使用者名稱為「admin」。主管理員角色已指派給此使用者帳戶。

    密碼必須符合以下規則：

    - 使用者密碼不能少於10個或多於256個字元。
    - 密碼必須包含以下組中三組的字元：
      - 大寫字母（A-Z）
      - 小寫字母（a-z）
      - 數字（0-9）
      - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
    - 密碼不得包含任何空格或".@"組合。

12. 請輸入 Kubernetes 叢集閘道的 IPv4 位址（設定檔中的 `ingress_ip` 參數）。

    閘道必須與主要工作節點位於同一子網路中。

13. 請輸入用於透過 Grafana 工具檢視 OSMP 指標的帳戶使用者名稱（設定檔中的 `grafana_admin_user` 參數）。

值必須符合以下規則：

- 使用者名稱長度必須為1到30個字元。
- 使用者名稱可以包含以下字元：
  - 小寫字母（a-z）
  - 數字（0-9）
  - 特殊字元（_ - .）
- 使用者名稱必須以字母開頭。
- 使用者名稱不能包含空格或“@”符號。

14. 請輸入用於透過 Grafana 工具檢視 OSMP 指標的帳戶密碼（組態檔的 `grafana_admin_password` 參數）。
密碼必須符合以下規則：
    - 使用者密碼不能少於10個或多於256個字元。
    - 密碼必須包含以下組中三組的字元：
      - 大寫字母（A-Z）
      - 小寫字母（a-z）
      - 數字（0-9）
      - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
    - 密碼不能包含空格或“.@”。
15. 略過指定 `extended_incident_lifecycle` 參數的步驟。這是一個服務參數。預設情況下，`extended_incident_lifecycle` 參數已停用，請勿變更。
16. 請輸入 Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的網域名稱（組態檔的 `smp_domain` 參數）。
參數值必須符合第二層網域名稱的命名要求。
17. 請輸入 Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的主機名稱（組態檔的 `nwc_host`、`flow_host`、`hydra_host`、`login_host`、`ksc_host`、`console_host`、`api_host`、`kuma_host`、`monitoring_host`、`xdr_edr_ingress_host` 參數）。
如果未指定自訂主機名稱，則使用下列預設主機名稱：
    - `nwc_host—"console"`
    - `flow_host—"console"`
    - `hydra_host—"console"`
    - `login_host—"console"`
    - `ksc_host—"admsrv"`

- `console_host–"console"`
- `api_host–"api"`
- `kuma_host–"kuma"`
- `monitoring_host–"monitoring"`
- `xdr_edr_ingress_host–"agentserver"`

服務主機名稱與網域名稱（`smp_domain` 參數值）皆為服務 FQDN 的組成部分。

18. 選擇 `Validate` 以驗證產生的組態檔，或選擇 `Skip` 不進行驗證而繼續。
19. 選擇 `Save and exit` 以使用指定的參數將產生的組態檔儲存為 YAML 格式。組態檔中包含其他安裝參數，並具有預設值。您可以在部署Kaspersky Next XDR Expert之前手動編輯組態檔。選擇 `Install` 以使用此組態檔開始部署 Kaspersky Next XDR Expert。

部署精靈會以 YAML 格式儲存包含指定參數的組態檔，並開始部署 Kaspersky Next XDR Expert。

安裝 Kaspersky Next XDR Expert

Kaspersky Next XDR Expert使用KDT進行部署。Kaspersky Deployment Toolkit會自動部署Kubernetes叢集，並在該叢集內安裝OSMP元件和其他基礎設施元件。Kaspersky Next XDR Expert安裝過程的步驟不取決於所選的部署選項。

如果需要使用Kaspersky Next XDR Expert實例安裝多個Kubernetes集群，則可以使用所需數量的上下文。

若要安裝Kaspersky Next XDR Expert

1. 在管理員主機上使用KDT解壓縮下載的分發套件。
2. 請閱讀Kaspersky Next XDR Expert元件分發包中的KDT最終使用者產品授權協議（EULA）。

   開始使用KDT即表示您接受KDT最終使用者授權協議的條款。

   您可以在部署 Kaspersky Next XDR Expert 後閱讀 KDT 的 EULA。`license_kdt.txt` 檔案位於執行 Kaspersky Next XDR Expert 部署之使用者的 `~/kaspersky_eula` 目錄。
3. 安裝過程中，KDT會從作業系統儲存體下載缺少的軟體套件。安裝Kaspersky Next XDR Expert之前，請在目標主機上執行以下命令，以確保apt/yum快取是最新的。

   ```
   apt update
   ```
4. 重啟目標主機。
5. 在管理員主機上，執行以下命令，使用KDT開始部署Kaspersky Next XDR Expert。使用Kaspersky Next XDR Expert元件指定傳輸存檔的路徑和您之前填寫的設定檔的路徑（多節點和單節點部署的安裝參數集不同）。

   ```
   chmod +x kdt
   ./kdt apply -k <傳輸存檔的完整路徑> -i <設定檔的完整路徑>
   ```

   若使用 `--accept-eula` 旗標，即可在不提示閱讀 OSMP 的 EULA 與「隱私權政策」條款的情況下安裝 Kaspersky Next XDR Expert。此種情況下，您必須在部署 Kaspersky Next XDR Expert 之前閱讀 OSMP 的 EULA 與「隱私權政策」。這些檔案位於包含 Kaspersky Next XDR Expert 元件的分發套件中。

若想在部署期間閱讀並接受 EULA 與「隱私權政策」的條款，請勿使用 `--accept-eula` 旗標。

若使用 KDT 部署 Kaspersky Next XDR Expert 時發生錯誤，請指定設定檔的路徑但不使用 `-i` 旗標，以重新啟動部署。

6. 若未在前一步驟中使用 `--accept-eula` 旗標，請閱讀 OSMP 的 EULA 與「隱私權政策」。文字顯示在命令行視窗中。按空格鍵檢視下一個文字段。然後，當出現提示時，輸入以下值：

   a. 如果您瞭解並接受 EULA 的條款，請輸入 `y`。

   如果您不接受 EULA 的條款，請輸入 `n`。

   b. 若您瞭解並接受「隱私權政策」的條款，並且同意您的資料將依照「隱私權政策」所述進行處理和傳輸（包括傳輸到第三國），請輸入 `y`。

   如果您不接受「隱私權政策」的條款，請輸入 `n`。

   > 若要使用Kaspersky Next XDR Expert，您必須接受EULA和隱私權政策的條款。

   啟動部署後，KDT 會檢查 Kubernetes 叢集節點的硬體、軟體及網路設定是否符合解決方案安裝的先決條件。若所有嚴格的預檢查都成功完成，KDT 會在目標主機上的 Kubernetes 叢集內部署 Kaspersky Next XDR Expert 元件。否則，部署將會中斷。若需要，您可以略過部署前的預檢查（將 `ignore_precheck` 安裝參數設定為 `true`）。

   此外，KDT也會檢查所需的安裝參數是否正確指定。如果組態檔中所需的參數缺失或無效，部署將中斷。安裝參數值所遵循的規則在組態檔範本（multinode.smp_param.yaml.template和singlenode.smp_param.yaml.template）中指定。

   > 在Kaspersky Next XDR Expert部署期間，會在主管理伺服器上建立一個新使用者。若要開始設定OSMP主控台，此使用者會被指派下列角色：根租用戶中主管理員的XDR角色和主管理員的卡巴斯基安全管理中心角色。

7. 使用KDT公用程式檢視目錄中Bootstrap元件的安裝日誌，並取得有關Kaspersky Next XDR Expert元件的診斷資訊（如果需要）。

8. 登入OSMP主控台。

   OSMP 主控台位址為 `https://<console_host>.<smp_domain>:443`。

   位址由 組態檔 中指定的 `console_host` 和 `smp_domain` 參數值組成。

Kaspersky Next XDR Expert已部署在目標主機上。安裝KUMA服務以開始使用該解決方案。

設定目標主機的網際網路存取

若組織的基礎架構使用代理伺服器存取網際網路，且需讓目標主機連線至網際網路，則必須在部署 Kaspersky Next XDR Expert 前，將每個目標主機的 IP 位址新增至 /etc/environment 檔案中的 `no_proxy` 變數。如此可讓目標主機與網際網路建立直接連線，並正確部署 Kaspersky Next XDR Expert。

若要為目標主機設定網際網路存取：

1. 在目標主機上，使用文字編輯器開啟/etc/environment檔案。例如，以下命令使用GNU nano文字編輯器開啟檔案：

   ```
   sudo nano /etc/environment
   ```

2. 在 /etc/environment 檔案中，將目標主機的 IP 位址新增至 no_proxy 變數，以逗號分隔，且不加空格。

   例如，no_proxy 變數的初始設定可如下所示：

   ```
   no_proxy=localhost,127.0.0.1
   ```

   您可以將目標主機的 IP 位址 (192.168.0.1) 新增至 no_proxy 變數：

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.1
   ```

   或者，您可以指定包含目標主機的子網路（採用CIDR標記法）：

   ```
   no_proxy=localhost,127.0.0.1,192.168.0.0/24
   ```

3. 儲存/etc/environment檔案。

4. 重啟目標主機：

   ```
   reboot
   ```

將/etc/environment檔案中的IP位址新增到每個目標主機並重新啟動後，您可以繼續準備目標主機和進一步的Kaspersky Next XDR Expert部署。

同步裝置時間

若要在裝置上設定時間同步：

1. 執行下列命令安裝chrony：

   ```
   sudo apt install chrony
   ```

2. 設定系統時間與NTP伺服器同步：

   a. 確保虛擬機可以存取網際網路。

      如果可以存取網際網路，請轉到步驟b。

      如果無法存取網際網路，請將 /etc/chrony.conf 檔案中目前的公用來源（以 pool 開頭）取代為您組織內部 NTP 伺服器的名稱或 IP 位址。

   b. 透過執行以下命令啟動系統時間同步服務：

      ```
      sudo systemctl enable --now chrony
      ```

   c. 等待幾秒鐘，然後執行以下命令：

      ```
      sudo timedatectl | grep 'System clock synchronized'
      ```

      如果系統時間已正確同步，輸出將包含 System clock synchronized: yes 這一行。

同步隨即設定。

在Kubernetes叢集內安裝KUMA服務

*服務*是KUMA SIEM系統的主要元件，可協助系統管理事件。服務可讓您從事件來源接收事件，然後將它們轉換為公用格式，以便於找尋關聯規則、儲存體和手動分析資料。

服務類型：

- 儲存體用於保存事件。
- 收集器用於接收事件並將其轉換為KUMA格式。

  如果您打算在基礎設施中使用多個租用戶，請為每個租用戶建立一個單獨的收集器。

- 關聯器用於分析事件並搜尋定義的模式。
- 代理程式用於接收遠端裝置上的事件並將其轉發到KUMA收集器。

您必須在部署Kaspersky Next XDR Expert後才能安裝KUMA服務。在Kaspersky Next XDR Expert部署期間，將準備所需的基礎設施：在準備好的主機上建立服務目錄，並將服務安裝所需的檔案新增至這些目錄。我們建議按以下順序安裝服務：儲存體、收集器、關聯器和代理程式。

限制

在Kubernetes叢集集中安裝KUMA服務時，請注意下列限制：

- 每個安裝程式只能部署一個KUMA Core實例。
- 被動式收集器只能在使用啟用了TLS的HTTP或TCP連接器時部署。
- 對於被動式HTTP和TCP連接器，設定的伺服器位址和連接埠將自動替換為`0.0.0.0:7310`。
- 儲存體叢集必須完全部署在Kubernetes內部或完全部署在Kubernetes外部。不支援混合部署。
- 如果部署在Kubernetes外部的收集器或關聯器向部署在Kubernetes內部的儲存服務傳送事件，則事件傳遞將透過單一入口URL進行。Kubernetes在TCP層級執行儲存體節點之間的負載平衡。
- 如果流量必須路由到不同的儲存體節點群組，則需要部署單獨的eventRouter服務並透過它們路由流量。
- 當您變更部署在Kubernetes叢集內收集器的設定時，KUMA不會驗證修改後的設定。不正確的設定可能會導致收集器無法接收事件。
- 使用相同的**儲存體節點FQDN**值，不能在單個Kubernetes叢集中部署由同一儲存資源建立的多個儲存服務。

若在Kubernetes叢集中安裝和設定KUMA服務：

1. 請依照下列說明之一，確保已根據所選部署方案準備好Kaspersky Next XDR Expert的管理員主機和目標主機：
   - 多節點佈署：準備管理員主機和目標主機
   - 單節點部署：準備管理員主機和目標主機
2. 在OSMP控制台中，為每個KUMA服務（儲存體、收集器和關聯器）建立一個資源集。
3. 為儲存體、收集器和關聯器建立服務。

4. **將每個服務部署到Kubernetes叢集**。

    1. 在主應用程式視窗中，轉至**監控→資源和服務→活動服務**區段。

    2. 選擇要部署的服務，然後按一下**部署**按鈕。

    3. 在**將服務新增至Kubernetes**視窗中，填入下列欄位：

        - **儲存體節點FQDN**：指定儲存體資源中定義的儲存體叢集節點的名稱。此參數僅適用於儲存服務，且在服務部署後無法變更。

        - **儲存類別**：選擇用於儲存服務狀態的儲存子系統。此參數的值在部署後無法變更。可用值：

            - **Longhorn**— 此儲存類別提供支援複製的網路儲存體。預設情況下，服務狀態會複製到三個網路磁碟機。建議將此儲存類別用於收集器、事件路由器、關聯器、指標和Core服務，因為它允許Kubernetes在當前節點發生故障時將服務Pod遷移到另一個工作線程節點。它還可以用於為部署為單一實例的儲存服務提供高可用性。

            - **local-path**—此儲存類別使用掛載在`/opt/lvp/hot`目錄下的Kubernetes工作線程節點的本機磁碟陣列，並提供最高效能。建議將此儲存類別用於儲存服務，因為儲存體支援原生集群，並且不依賴Kubernetes機制來實現高可用性。它還可以用於使用HTTP或TCP連接器的收集器服務，以及從單一KUMA資源建立的多個執行個體部署的eventRouter服務。在單節點部署中，建議所有KUMA服務類型都使用**Local-Path**。

        - **冷儲存類別**：選擇用於長期資料儲存的儲存子系統。此參數僅適用於儲存服務，部署後無法變更。**local-path-cold**儲存類別與**local-path**類似，但專用於在掛載於/opt/lvp/cold目錄下的低速磁碟陣列上進行長期儲存。

        - **最小CPU**：指定為該服務保留的CPU核心數（執行緒數）。該值必須為正整數。預設值為`0`。

        - **最大CPU** ：指定服務可用的最大CPU核心數（執行緒數）。該值必須為正整數，且不能小於**最小CPU**值。預設值為`0`。

        - **最小RAM**：指定為該服務保留的RAM體量（以GB為單位）。該值必須為正整數。預設值為`0`。

        - **最大RAM**：指定服務可用的最大RAM體量（以GB為單位）。該值必須為正整數，且不能小於**最小RAM**值。預設值為`0`。

        - **儲存請求**：指定分配給服務的磁碟空間大小（以GB為單位）。只有在使用**longhorn**儲存類別時，此參數才可用。

        - **冷儲存請求**：指定分配給長期資料儲存的磁碟空間大小（以GB為單位）。此參數僅適用於使用**longhorn**儲存類別的儲存服務。

    4. 點擊**建立服務**按鈕。

5. 如有必要，請驗證收集器和關聯器是否已準備好接收事件。

6. 如有必要，請在KUMA網路基礎設施中安裝代理程式。

    代理安裝所需的檔案位於 `/opt/kaspersky/kuma/utils` 目錄。

Kaspersky Next XDR Expert功能所需的KUMA服務安裝在Kubernetes叢集中。

在Kubernetes叢集外部安裝KUMA服務

*服務*是KUMA元件的主要元件，可協助系統管理事件。服務可讓您從事件來源接收事件，然後將它們轉換為公用格式，以便於找尋關聯規則、儲存體和手動分析資料。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。

服務類型：

- 儲存體用於保存事件。
- 收集器用於接收事件並將其轉換為KUMA格式。

  如果您打算在基礎設施中使用多個租用戶，請為每個租用戶建立一個單獨的收集器。

- 關聯器用於分析事件並搜尋定義的模式。
- 代理程式用於接收遠端裝置上的事件並將其轉發到KUMA收集器。

您必須在部署Kaspersky Next XDR Expert後才能安裝KUMA服務。在Kaspersky Next XDR Expert部署期間，將準備所需的基礎設施：在準備好的主機上建立服務目錄，並將服務安裝所需的檔案新增至這些目錄。我們建議按以下順序安裝服務：儲存體、收集器、關聯器和代理程式。

若要在Kubernetes叢集外部安裝和設定KUMA服務：

1. 在OSMP主控台的主功能表中，轉至**設定→ KUMA** 。
2. 在OSMP主控台的KUMA部分，為要在網路基礎設施中準備好的主機上安裝的每個KUMA服務（儲存體、收集器和關聯器）建立一個資源集。
3. 為儲存體、收集器和關聯器建立服務。
4. 取得服務識別碼以綁定建立的資源集和KUMA服務：
   a. 在 OSMP 解決方案中，前往**資源 → 作用中服務**。
   b. 選擇所需的KUMA服務，然後按一下**複製ID**按鈕。
5. 在網路基礎設施中準備好的主機上，執行對應的命令來安裝KUMA服務。使用先前取得的服務識別碼：
   - 儲存體的安裝命令：

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
     ```

   - 收集器的安裝命令：

     ```
     sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port>
     ```

- 相關器的安裝命令：

  ```
  sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
  ```

  其中：

  - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
  - <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

    `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

    您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

    為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
  - <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
  - <API port> 是用於與已安裝元件通訊的連接埠。

  預設情況下，KUMA Core 的 FQDN 為 `<kuma_host>.<smp_domain>`。

  用於連接到KUMA Core的連接埠無法變更。預設埠號為 7210。

  開啟伺服器上已安裝之收集器和關聯器所對應的連接埠（TCP 7221，以及安裝服務時用作 `--api.port <port>` 參數值的其他連接埠）。

6. 在安裝KUMA服務期間，請參閱KUMA的最終使用者產品授權協議（EULA）。文字顯示在命令列視窗中。按空格鍵檢視下一個文字段。然後，當出現提示時，輸入以下值：

   - 如果您瞭解並接受 EULA 的條款，請輸入 `y`。
   - 輸入 `n`（如果您不接受 EULA 的條款）。若要使用 KUMA 服務，您必須接受 EULA 的條款。

   在安裝KUMA服務後，您可以透過以下其中一種方式閱讀KUMA的最終使用者許可協議：

   - 在主機上，其包含於 KUMA 清查檔案中的 `kuma_utils` 群組：請開啟位於 `/opt/kaspersky/kuma/utils` 目錄中的 LICENSE 檔案。
   - 在主機上，其包含於 KUMA 清查檔案中的其他群組（`kuma_storage`, `kuma_collector` 或 `kuma_correlator`）：請開啟位於 `/opt/kaspersky/kuma` 目錄中的 LICENSE 檔案。
   - 執行以下命令：

     ```
     /opt/kaspersky/kuma/kuma license --show
     ```

   接受EULA後，KUMA服務將安裝在網路基礎設施中準備好的裝置上。

7. 如有必要，請驗證收集器和關聯器是否已準備好接收事件。

8. 如有必要，請在KUMA網路基礎設施中安裝代理程式。

   代理安裝所需的檔案位於 `/opt/kaspersky/kuma/utils` 目錄。

Kaspersky Next XDR Expert功能所需的KUMA服務已安裝。

部署多個Kubernetes叢集和Kaspersky Next XDR Expert實例

KDT可讓您部署多個帶有Kaspersky Next XDR Expert實例的Kubernetes集群，並使用上下文在它們之間切換。*上下文*是一組存取參數，用於定義使用者可以選擇與之互動的Kubernetes叢集。上下文還包括使用KDT連線到叢集的資料。

先決條件

在建立上下文和安裝具有Kaspersky Next XDR Expert實例的Kubernetes叢集之前，您必須執行下列操作：

1. 準備好管理員主機和目標主機。

   對於安裝多個叢集和Kaspersky Next XDR Expert實例，您需要為所有叢集準備一個管理主機，並為每個叢集準備單獨的目標主機集。不應在目標主機上安裝Kubernetes元件。

2. 準備用於安裝KUMA服務的主機。

   要安裝KUMA服務，您需要為每個Kaspersky Next XDR Expert實例準備好單獨的主機集。

3. 準備KUMA清查檔案。

   要安裝KUMA服務，您需要為每個Kaspersky Next XDR Expert實例準備單獨的清查檔案。

4. 準備組態檔。

   若要安裝多個叢集和Kaspersky Next XDR Expert實例，您需要為每個Kaspersky Next XDR Expert實例準備組態檔。在這些組態檔中，指定對應的管理和目標主機，以及特定叢集和Kaspersky Next XDR Expert實例特有的其他參數。

Process

若要建立具有Kubernetes叢集和Kaspersky Next XDR Expert實例的上下文：

1. 在KDT公用程式所在的管理員主機上，執行下列命令並指定上下文名稱：

   ```
   ./kdt ctx --create <context_name>
   ```

   已建立具有指定名稱的上下文。

2. 安裝Kubernetes叢集和Kaspersky Next XDR Expert。

具有Kaspersky Next XDR Expert實例的叢集已部署在上下文中。上下文的建立隨即完成。當取得Kaspersky Next XDR Expert元件的日誌檔案時，日誌檔案包含您目前的上下文名稱。

您可以重複此程序以建立所需數量的具有已安裝叢集和卡巴斯基 Next XDR Expert 實例的上下文。

建立上下文後，必須部署Kubernetes叢集和Kaspersky Next XDR Expert實例才能完成上下文建立。如果您不在上下文中執行部署，然後建立另一個上下文，則第一個上下文將被刪除。

若要查看已建立上下文清單和活動上下文名稱，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt ctx
```

若要切換至所需上下文，

在KDT公用程式所在的管理員主機上，執行下列命令並指定上下文名稱：

```
./kdt ctx <context_name>
```

選擇上下文後，KDT將連線到對應的Kubernetes叢集。現在，您可以使用此叢集和Kaspersky Next XDR Expert實例。KDT命令將套用至選定的叢集。

當使用KDT刪除Kubernetes叢集中安裝的Kaspersky Next XDR Expert元件以及叢集本身時，對應的上下文也會被刪除。不會刪除其他上下文及其包含Kaspersky Next XDR Expert實例的叢集。

在實體隔離環境中安裝和更新 Kaspersky Next XDR Expert

Kaspersky Next XDR Expert 可以在實體隔離環境中安裝或升級。在實體隔離環境中進行安裝和更新時，使用kdt-airgap-preparation公用程序，包括以下階段：

1. 準備管理員主機和目標主機，以及組態檔。
2. 取得安裝在位於實體隔離環境中的目標主機上的安裝套件的資訊

   將此資訊與所需軟體套件清單進行比較，並將目標主機上缺少的內容資訊儲存到YAML清單檔案中。
3. 從開放環境中的公共網際網路儲存庫或企業映像儲存庫下載庫存檔案中指定的所需軟體套件及其依賴項。

   下載的軟體套件將儲存到本機TAR軟體套件存檔。
4. 從本地TAR歸檔檔案中安裝或更新軟體套件及其對實體隔離環境中目標主機的依賴項。
5. 在實體隔離環境中安裝或升級 Kaspersky Next XDR Expert

準備管理員和目標主機

您需要根據所選的部署方案，確定要部署 Kubernetes 叢集及此叢集所包含之 Kaspersky Next XDR Expert 元件的目標裝置數量。請遵循下列其中一份指南，準備管理員主機和目標主機以部署 Kaspersky Next XDR Expert（忽略涉及下載和安裝軟體套件的步驟）：

- 多節點佈署：準備管理員主機和目標主機
- 單節點部署：準備管理員主機和目標主機

準備YAML格式的組態檔。組態檔包含部署目標主機列表和Kaspersky Next XDR Expert元件的安裝參數集。

使用包含特定於所選部署方案的安裝參數的組態檔：

- 多節點部署：指定安裝參數
- 單節點部署：指定安裝參數

在實體隔離環境中部署Kaspersky Next XDR Expert時，請將`airgap_mode`安裝參數設定為`true`。

取得安裝在位於實體隔離環境中的目標主機上的安裝套件的資訊

若要取得目標主機的作業系統和已安裝軟體套件的資訊：

1. 在管理員主機上，執行下列命令：指定位於管理員主機上的SSH私鑰的路徑，用於連線到目標主機，您之前填寫的組態檔路徑，以及將儲存資訊的清查檔案路徑：

   ```
   kdt-airgap-preparation scan -k <full_path_to_ssh_key> -c
   <full_path_to_configuration_file> --airgap -i <full_path_to_inventory_file>
   ```

   kdt-airgap-preparation公用程式會將目標主機上的資訊與所需軟體套件清單進行比較，並將目標主機上缺少的軟體包資訊儲存到YAML清單檔案中。YAML清單檔案會以指定的名稱儲存到指定的目錄。

如果需要檢查目標主機上的其他軟體套件（例如Docker），請執行以下命令：

```
kdt-airgap-preparation scan -k <full_path_to_ssh_key> -c
<full_path_to_configuration_file> --airgap -i <full_path_to_inventory_file> --add-pkgs
<package_name>
```

目標主機上未安裝的其他軟體套件資訊將會加入YAML清單檔案。

建立的清單檔案將用於從公共網際網路儲存庫或開放環境中的企業映像儲存庫下載目標主機缺少的軟體套件。如果發生錯誤，kdt-airgap-prepare 公用程式會結束，並將對應的錯誤訊息傳送至記錄檔和 stdout。

在開放環境中下載所需軟體套件

若要下載清單檔案中指定的所需軟體套件：

1. 將YAML清單檔案複製到卸除式磁碟機，然後將該檔案移至開放環境中的管理員主機。
2. 在管理員主機上，執行下列命令：指定清單檔案的路徑以及要儲存所需缺少軟體套件的軟體套件存檔的路徑：

   `kdt-airgap-preparation pull -n <清單檔案的完整路徑> -a <軟體套件存檔的完整路徑>`

   kdt-airgap-preparation公用程式會下載清單檔案中列出的軟體套件及其依賴項，並將軟體套件儲存到TAR軟體套件存檔中。此軟體套件存檔將儲存到指定的目錄，並使用指定的名稱。
3. 將清單檔案新增至軟體套件存檔。

   建立的軟體套件存檔將用於在隔離環境中的目標主機上使用安裝程式安裝缺少的必要軟體套件。如果發生錯誤，kdt-airgap-preparation公用程式將終止並將相應的錯誤訊息輸出到日誌檔案和stdout。

在實體隔離環境中的目標主機上安裝或更新軟體套件

若要在目標主機上安裝或更新軟體套件及其依賴項：

1. 將TAR軟體套件存檔複製到卸除式磁碟機，然後將該存檔移至實體隔離環境中的管理員主機。
2. 在管理員主機上，執行下列命令：指定TAR軟體套件存檔的路徑以及位於管理員主機上並用於連線到目標主機的SSH私鑰路徑：

   `kdt-airgap-preparation install -a <軟體套件存檔的完整路徑> -k <SSH私鑰的完整路徑>`

   kdt-airgap-preparation公用程式使用清單檔案和軟體套件存檔在目標主機上安裝或更新所需的軟體套件。

準備好目標主機後，安裝或升級Kaspersky Next XDR Expert。

部署前的基礎設施就緒狀況預檢

開始部署Kaspersky Next XDR Expert後，KDT會檢查Kubernetes叢集節點的硬體、軟體和網路設定是否滿足安裝解決方案的先決條件。對叢集中的每個節點執行預檢。

所有檢查分為兩類：

- 嚴格檢查

  檢查對Kaspersky Next XDR Expert的運作緊急的參數。如果此檢查失敗，則部署會中斷。
- 非嚴格檢查

  檢查對Kaspersky Next XDR Expert的運作並非緊急的參數。如果此檢查失敗，則部署會繼續進行。

執行以下預檢：

- 硬體：
  - 磁碟上的可用空間足以滿足部署需求。
  - CPU組態符合需求。
  - 剩餘RAM空間足以滿足部署需求。
  - CPU支援AVX、SSE 4.2和BMI指令集。
  - `/tmp`目錄中的可用磁碟空間必須至少等於傳輸壓縮檔案的大小（對於管理員主機，嚴格檢查）。
- 軟體：
  - 作業系統及其版本符合需求。
  - 核心版本符合需求。
  - Systemctl已安裝且可用（嚴格檢查）。
  - 軟體套件管理器快取的更新可用（嚴格檢查）。
  - 節點上已安裝正確版本的必需軟體套件（嚴格檢查）。
  - 節點上未安裝禁止使用的軟體套件（docker和podman）（嚴格檢查）。
  - 缺少過時的k0s二進位（嚴格檢查）。
  - 缺少過時的k0s組態檔（嚴格檢查）。
  - PostgreSQL或Postgres Pro DBMS伺服器參數必須符合需求（嚴格檢查）。
- 網路：
  - 所有叢集節點都位於同一個廣播域中。
  - 所有叢集節點都有唯一名稱（組態檔的`desc`參數）（嚴格檢查）。
  - 自訂憑證檔案對指定網域有效，並包含加密後的私鑰（嚴格檢查）。
  - 自訂中級憑證的有效期限必須至少為399天。
  - 自訂葉證書的有效期限至少為399天（嚴格檢查）。
  - 節點上的DNS名稱解析可用（嚴格檢查）。
  - 叢集節點上的時間同步已設定（嚴格檢查）。
  - 所有節點的本機時間相差不超過5秒（嚴格檢查）。
  - 所需連接埠可用。

若所有嚴格的預檢查都成功完成，KDT 會在目標主機上的 Kubernetes 叢集內部署 Kaspersky Next XDR Expert 元件。所有通過與未通過檢查的結果，均會儲存於各節點的 /tmp/k0s_report.txt 檔案中。若需要，您可以略過部署前的預檢查（將 `ignore_precheck` 安裝參數設定為 `true`）。

Kaspersky Next XDR Expert元件的安裝前完整性檢查

收到包含Kaspersky Next XDR Expert元件的傳輸歸檔後，您可以驗證其真實性和完整性。傳輸歸檔中的每個元件（CNAB）都包含一個XML格式的清單檔案。此清單檔案包含元件核對總和，並使用GOST R 34.11-2012的256位元演算法進行數位簽章。此數位簽章既確保元件檔案核對總和的有效性，也確保清單中的核對總和未被變更。

您可以驗證元件的核對總和是否與清單檔案中指定的核對總和相符。這確認組件未被修改，並且來自可信任來源。

要檢查已安裝的Kaspersky Next XDR Expert元件的完整性：

1. 解壓縮傳輸歸檔。
2. 請在提取的元件及其清單檔案所在的目錄中執行以下命令之一。

   - 驗證單一元件

     指定清單檔案名稱以驗證對應的元件。`integrity_checker` 公用程式會驗證指定清單檔案的數位簽章：

     ```
     ./integrity_checker --signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
     <CNAB_manifest_file.xml>
     ```

   - 驗證所有元件

     `integrity_checker` 公用程式會驗證所有清單檔案的數位簽章：

     ```
     find . -type f -iname "*.xml" -print0 | xargs -0 -I {} echo --manifest {} | xargs ./integrity_checker --
     signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
     ```

完整性檢查成功後的命令輸出範例

成功透過驗證的清單檔案數量顯示在`Manifests`行的`succeeded`欄中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 0 / 0 / 38
        Files: 0 / 0 / 38
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
SUCCEEDED
```

完整性檢查失敗後的命令輸出範例

在本例中，清單檔案在簽名後被修改，或簽名有問題。跳過的清單檔案或驗證失敗的清單檔案數量顯示在`Manifests`行的`failed`直欄中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 2 / 0 / 36
        Files: 0 / 0 / 0
        Directories: 0 / 0 / 0
```

```
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
==============================================>
FAILED
ERR 無法驗證檔案「/home/xdr_user/integrity_check.xml」的數位簽章。 標誌：無：0x80000106（物件不受信任）
清單檔案 /home/xdr_user/integrity_check.xml 驗證失敗。原因：無法驗證檔案「/home/xdr_user/integrity_check.xml」的數位簽章。 標誌：無：0x80000106（物件不受信任）
```

Kaspersky Next XDR Expert元件的真實性和完整性已驗證。

將資料匯入 Kaspersky Next XDR Expert

若要登入 Kaspersky Next XDR Expert，您必須知道 OSMP 主控台的網址。在您的瀏覽器中，JavaScript 必須被啟用。

若要登入 OSMP 主控台：

1. 在您的瀏覽器中，前往 `https://<console_host>.<smp_domain>:443`。

   OSMP 主控台位址由 設定檔中指定的 `console_host` 和 `smp_domain` 參數值組成。

   登入頁面顯示。

2. 執行以下操作之一：

   - 若要使用網域使用者帳戶登入 OSMP 主控台，請輸入網域使用者的使用者名稱和密碼。

     您可以採用以下格式之一輸入網域使用者的使用者名稱：

     - 使用者名稱@ `dns.domain`
     - NTDOMAIN\使用者名稱

   - 輸入內部使用者的使用者名稱和密碼。

3. 點擊**登入**按鈕。

4. 指定身分驗證器應用程式在行動裝置上產生的一次性安全碼。

   首次登入時，請為您的帳戶配置雙步驟身分驗證。如果您無法設定雙因素驗證，請聯絡在一般功能：使用者權限功能區域中擁有**修改物件ACL**權限且已設定雙因素驗證的使用者，將您的帳戶新增至雙因素驗證允許清單中。

5. 如果您的帳戶啟用了強制修改密碼或您的密碼已過期，則會彈出密碼修改視窗。設定用於登入 OSMP 主控台的新密碼。

登入後，會顯示儀表板，其中包含您上次登入時使用的語言和主題。

登入嘗試次數超出允許範圍

OSMP分發套件包含一個關聯規則*[OOTB]：使用相同帳戶多次嘗試登入OSMP主控台*。此規則已新增至關聯器中，該關聯器會在OSMP部署期間安裝。此規則會在使用者登入OSMP控制台失敗三次後建立一個關聯事件。

產生的關聯事件將作為超出允許登入嘗試次數警示的依據。

您可以修改允許的密碼輸入嘗試次數。有關詳細信息，請參閱以下文章：更改允許的密碼輸入嘗試次數。

網域身分驗證

Kaspersky Next XDR Expert 可讓您透過 Kerberos 通訊協定使用網域身分驗證。有關詳細信息，請參閱以下文章：設定Kerberos網域身分驗證。

若要登出 OSMP 主控台，

在上方窗格中，按一下您的帳戶名稱以開啟帳戶選單，然後選取 **登出**。

OSMP 主控台將關閉，並顯示登入頁面。

與端點代理程式的整合

若要整合端點代理程式，您需要取得所需的憑證，以便在OSMP和端點代理程式之間建立*可信任連線*。

要取得從端點代理程式接收遙測資料的憑證：

1. 在主功能表中，轉至**監控→資源和服務→活動服務**。
2. 在服務清單中，以滑鼠右鍵按一下要用於收集端點代理程式所傳送的遙測資料的收集器，然後從快線表單中選擇**下載憑證**。

   您的瀏覽器會將伺服器TLS憑證下載到下載資料夾。

要取得向端點代理程式傳送回應的憑證：

1. 在主功能表中，轉至**設定** → **租用戶** → 按一下租用戶名稱 → **設定** 索引標籤 → **憑證**。
2. 在**伺服器憑證**部分，按一下**匯出**。

   您的瀏覽器會將伺服器TLS憑證下載到下載資料夾。

若要取得端點代理程式TLS憑證：

1. 在主功能表中，轉至**設定** → **租用戶** → 按一下租用戶名稱 → **設定** 索引標籤 → **憑證**。
2. 在**端點代理程式**部分，選擇目前的TLS憑證，然後按一下**匯出**。
3. 為包含端點代理程式TLS憑證的受密碼保護的PFX封存檔案指定密碼，然後按一下**匯出**。

   您的瀏覽器會將PFX封存檔案（加密容器）下載到下載資料夾。

   在向端點代理程式發送回應和從端點代理程式接收遙測資料時，需要使用所獲得的憑證進行雙向TLS身分驗證。

下載所有必要的憑證後，即可建立用於整合端點代理程式的政策。有關如何建立政策和新增憑證的詳細說明，請參閱端點代理程式說明文件：

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

沙盒的準備與安裝程式

若要準備安裝程式和安裝沙盒：

1. 為沙盒安裝準備好您的IT基礎設施。
2. 準備一台虛擬機器。
3. 準備安裝程式磁碟映像。
4. 安裝沙盒。

為沙盒安裝程式準備IT基礎設施

若要為沙盒安裝程式準備IT基礎設施：

1. 禁止沙盒伺服器的管理網路介面和用於處理物件存取網際網路的網路介面存取本機網路。
2. 依下列方式指定與其他元件互動的連接埠：
   - 入站方向（管理介面）：
     - TCP 22
       透過SSH連線到伺服器。
     - TCP 443
       與OSMP的通訊
     - TCP 8443
       存取應用程式的網頁介面
   - 出站方向（管理介面）：
     - TCP 80或TCP 443
       與卡巴斯基更新伺服器通訊。
   - 出站和對應的入站方向（用於存取已處理物件的協助工具介面）：
     任意連接埠。
     存取網際網路以分析已處理物件的網路行為。

     > 拒絕存取公司區域網，以保護網路免受被分析物件的侵害。

準備用於安裝沙盒的虛擬機器

若要準備用於安裝沙盒元件的虛擬機器：

1. 執行VMware ESXi Hypervisor。
2. 開啟虛擬機器管理主控台。
3. 在要安裝沙盒元件的虛擬機器的快顯選單中，選擇**編輯設定**。
   虛擬機器內容視窗隨即開啟。
4. 在**虛擬硬體**頁籤上，延伸「CPU設定」群組，然後選取**向客體作業系統公開硬體輔助虛擬化**核取方塊。
5. 在**虛擬機器選項**頁籤的**延遲敏感度**下拉清單中，選擇**高**。
6. 點擊**確定**。

虛擬機器隨即準備用於安裝沙盒元件。

準備安裝程式磁碟映像

在安裝沙盒之前，您必須準備一個基於Astra Linux作業系統的安裝程式磁碟iso映像。

用於建立iso映像的裝置的最低硬體需求：

- CPU：4核，時脈頻率2500 MHz或更高。
- RAM：8 GB
- 可用磁碟空間：100 GB。

軟體需求：

- 基於最新Linux核心的作業系統。
- Docker 20或更高版本。
- Astra Linux特別版1.8.2.8的ISO映像（以下簡稱astra-installation.iso）。

Kaspersky Next XDR Expert不支援其他版本的Astra Linux作業系統。

要掛載基於Astra Linux作業系統的沙盒元件的ISO映像：

1. 從分發套件下載以下檔案：
   - 來自沙盒分發套件的tar.gz封存檔案
   - 用於建立ISO映像的工具

2. 建立一個名為iso_builder.sh的檔案，內容如下：

```
#!/bin/bash
usage="Builds the KEDR install ISO.
Usage:
$(basename "$0") [-h] source_iso distribution iso_builder_image build target_iso_name
where:
    -h, --help        - show this text and exit
    source_iso        - absolute path to the source OS ISO file
    distribution      - absolute path to the KEDR distribution archive
    iso_builder_image - absolute path to the iso_builder docker image
    build             - absolute path to a temporary build directory
    target_iso_name   - absolute path to the resulting ISO file
"
if [ "$#" -eq 0 ] || [ "$1" == "-h" ] || [ "$1" == "--help" ]
then
    echo "$usage"; exit 10;
fi
if [ "$#" -lt 5 ]
then
    echo "錯誤：參數不足。 請參閱說明文字。"; exit 11;
fi
docker load -i $3
docker run -v $1:$1 -v $2:$2 -v $4:/build kaspersky/kata/deployment/iso_builder:6.0 --source-iso-uri file://$1
--kata-distribution-uri file://$2 --target-iso-name $5
```

3. 執行以下命令：

```
mkdir /var/kedr_builder
```

4. 將步驟1中列出的檔案和astra-installation.iso映像放在新建立的/var/kedr_builder目錄中。

5. 執行以下命令：

```
sudo ./iso_builder.sh \
 /var/kedr_builder/astra-installation.iso \
 /var/kedr_builder/kata-sb-distribution-<version>-x86_64_en-ru-zh.tar.gz \
 /var/kedr_builder/iso-builder-<version>-x86_64_en-ru-zh.tar \
 /var/kedr_builder buildSandboxAstra.iso
```

其中，<版本>是沙盒分發版本。

安裝磁碟映像buildSandboxAstra.iso在/var/kedr_builder目錄中建立。

如果您將檔案儲存在不同的目錄中，可以執行下列指令：

```
sudo ./iso_builder.sh <source_iso_host_path> <distribution_host_path> <iso_builder_image_host_path>
<build_host_path> <target_iso_name>
```

在上述指令中：

- source_iso_host_path是Astra Linux特別版1.8.2.8分發套件的路徑。
- distribution_host_path是沙盒分發套件的路徑。
- iso_builder_image_host_path是ISO builder工具的路徑。
- build_host_path是已掛載ISO映像的存放路徑，無需指定ISO映像的名稱。
- target_iso_name是指派給ISO映像的名稱。

安裝沙盒

若要開始安裝沙盒元件：

1. 執行包含沙盒元件的磁碟映像。
   安裝精靈隨即啟動。
2. 選擇**繼續**並按下**回車鍵**。

步驟 1。檢視最終使用者產品授權協議和隱私權政策

若要繼續安裝，您必須閱讀並接受AO Kaspersky Lab的最終使用者產品授權協定和隱私權政策的條款與條件（以下分別稱為「 EULA」和「隱私權政策」）。您必須接受EULA和隱私權政策的條款，安裝程式才能繼續。

在Astra Linux作業系統上，您還需要接受Astra Linux作業系統的最終使用者產品授權協定。

若要接受EULA和隱私權政策的條款和條件：

1. 在清單中選擇要閱讀EULA和隱私權政策文字的語言，然後按下**回車鍵**。
2. 在Astra Linux作業系統上，您必須先接受Astra Linux作業系統的最終使用者產品授權協定。閱讀EULA。如果您接受其條款和條件，請選擇**我接受**並按下**回車鍵**。
3. 閱讀卡巴斯基的EULA。如果您接受其條款和條件，請選擇**我接受**並按下**回車鍵**。
4. 閱讀隱私政策。如果您接受其條款和條件，請選擇**我接受**並按下**回車鍵**。

安裝精靈隨即繼續執行下一步。

步驟 2。選擇用於安裝沙盒的磁碟

若要選擇用於安裝元件的磁碟：

1. 選擇建議的磁碟機之一來安裝程式，然後按**回車鍵**。
2. 在確認視窗中，選擇**是**並按下**回車鍵**。

安裝精靈隨即繼續執行下一步。

步驟 3。設定沙盒管理員密碼的最小密碼長度

若要設定沙盒元件管理員密碼的最小長度：

1. 在**最小密碼長度**中，輸入字元長度。
   建議密碼長度為12個字元或以上。
2. 選擇**確定**並按下**回車鍵**。

安裝精靈隨即繼續執行下一步。

步驟 4。建立沙盒管理員帳戶

若要建立沙盒管理員帳戶：

1. 在**新使用者名稱**欄位中，輸入管理員帳戶的名稱。預設情況下，使用「admin」帳戶。
2. 在**新建密碼**欄位中，輸入管理員帳戶的網域密碼。
   密碼必須符合以下規則：
   - 此密碼必須至少包含8個字元。
   - 密碼必須包含至少三種類型的字元：
     - 大寫字母 (A-Z)
     - 小寫字母 (a-z)
     - 數字。
     - 特殊字元。
   - 密碼不得與使用者名稱完全或實質上相同。
   - 密碼不得包含三個或更多連續的相同字元。
3. 在**確認密碼**欄位中再次輸入密碼。
4. 選擇**確定**並按下**回車鍵**。

安裝精靈隨即繼續執行下一步。

步驟 5。設定管理網路介面

為確保沙盒元件正常運行，您必須連接至少兩張網卡並設定以下網路介面：

- 管理網路介面。此介面旨在提供對沙盒伺服器的SSH存取；沙盒伺服器也使用此介面接收要掃描的物件。
- 用於透過網際網路存取已處理物件的網路介面。沙盒處理的物件可以使用此介面嘗試在網路上進行活動，沙盒可以分析它們的行為。如果您阻止網際網路存取，沙盒將無法分析網際網路上物件的行為，因此只會分析沒有網際網路存取的物件的行為。

> 用於透過網際網路存取已處理物件的網路介面必須與貴組織的本地網路隔離。

選擇要用作管理介面的網路介面並進行設定。

若要選擇管理網路介面並進行設定：

1. 在網路清單中，選擇要用作管理介面的網路介面。
2. 按一下**Enter**。
3. 在**位址**欄位中，輸入要指派給此網路介面的IP位址。
4. 在**子網路遮罩**欄位中，輸入您希望使用此網路介面的網路遮罩。
5. 選擇**確定**並按下**回車鍵**。
6. 選擇**繼續**並按下**回車鍵**。

安裝精靈繼續執行下一步。

步驟 6。指派主機名稱並新增DNS伺服器位址

為DNS伺服器指派伺服器主機名，並新增DNS伺服器位址。

若要指派伺服器主機名稱並新增DNS伺服器位址：

1. 在**DNS設定**視窗中，選擇**主機名稱**。
2. 請在**主機名稱**欄位中輸入伺服器的完整網域名稱。
   請以FQDN格式指定伺服器名稱（例如：host.domain.com或host.domain.subdomain.com）。
3. 選擇**確定**並按下**回車鍵**。
4. 在**DNS設定**視窗中，選擇**DNS伺服器**。
5. 選擇**新建**並按下**回車鍵**。
   DNS伺服器位址事項視窗隨即開啟。
6. 在**DNS伺服器**文字方塊中，以IPv4格式輸入主要DNS伺服器的IP位址。
7. 選擇**確定**並按下**回車鍵**。
   DNS伺服器位址事項視窗關閉。
8. 如果要新增其他DNS伺服器的IP位址，請對要新增的每個伺服器重複這些說明中的步驟5到7。
9. 新增完所有DNS伺服器後，選擇**返回**並按**回車鍵**。
10. 在DNS伺服器視窗中，選擇**繼續**並按下**回車鍵**。

安裝精靈隨即繼續執行下一步。

步驟 7。設定靜態網路路由

若要設定靜態網路路由：

1. 在**IPv4路由器**視窗中，選擇**新建**並按下**回車鍵**。
   IPv4 靜態路由視窗隨即開啟。
2. 在**位址/遮罩**欄位中，輸入要為其設定網路路由的子網路的IP位址和遮罩。
3. 如果要使用預設網路路由，請輸入`0.0.0.0/0`。
4. 在**閘道**欄位中，輸入閘道的IP位址。
5. 選擇**確定**並按下**回車鍵**。
6. 如果您想要新增其他網路路由，請對要新增的每個網路路由重複這些說明中的步驟1到5。
7. 新增完網路路由後，請按一下**繼續**。

設定過程可能需要一些時間。至此，安裝完成。

與沙盒整合

與沙盒整合涉及兩個步驟：

1. 在OSMP介面中建立連線到沙盒伺服器的請求。
2. 在沙盒網頁介面中接受請求。

若要透過OSMP介面建立到沙盒伺服器的連線請求：

1. 在主功能表中，轉至**設定** → **租用戶**。
   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。
2. 按一下所需政策的名稱。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤中，轉到**沙盒伺服器**部分。
   記下*OSMP憑證指紋*。稍後您需要此指紋與沙盒網頁介面中顯示的指紋進行比對。
4. 按一下**新增**按鈕。
   新增沙盒伺服器窗格將顯示在網頁介面視窗的右側。
5. 在**IP**欄位中，指定沙盒伺服器的IP位址。
6. 點選**取得憑證指紋**。Kaspersky Next XDR Expert顯示*沙盒憑證指紋*。稍後您需要此指紋與沙盒網頁介面中顯示的指紋進行比對。

7. 在**沙盒名稱**欄位中，指定要在OSMP介面中顯示的沙盒元件名稱。

8. 按一下**儲存**按鈕。

OSMP向沙盒傳送連線請求。現在您需要接受請求。

若要接受來自OSMP的連線請求：

1. 在沙盒網頁介面中，轉至**授權**部分。

2. 比較憑證指紋：

   - 沙盒IP下顯示的沙盒憑證指紋應與您先前在OSMP介面中取得的沙盒憑證指紋相符。
   - 在OSMP傳送的連線請求清單中，找到來自OSMP的連線請求。**憑證指紋**直欄包含傳送連線請求的伺服器的憑證指紋。請確保此憑證指紋與您先前在OSMP介面中取得的憑證指紋相符。

3. 若要接受連線請求，請按一下**同意**。之後，您可以點擊**撤銷**按鈕來撤銷先前接受的連線請求。

4. 點擊**"套用"**。

與沙盒的整合隨即完成。

Kaspersky Next XDR Expert的高可用性部署

Kaspersky Next XDR Expert的高可用性組態確保了連續正常運作，即使部署解決方案的任何Kubernetes叢集節點出現故障或失去網路連線。

在此應用情境之後，您可以準備基礎設施，以部署Open Single Management Platform和Kaspersky Next XDR Expert在高可用性組態（包括Kaspersky Endpoint Detection and Response功能）的所有必要元件，準備包含安裝參數的組態檔，並使用Kaspersky Deployment Toolkit公用程式（以下簡稱KDT）部署解決方案。

在部署Open Single Management Platform和Kaspersky Next XDR Expert元件之前，建議您閱讀硬化指南 。

此部署情境分幾個階段進行：

1. **下載包含Kaspersky Next XDR Expert元件的分發套件**

   分發套件包含以下元件：

   - 包含Kaspersky Next XDR Expert元件、Kaspersky Next XDR Expert的終端使用者許可協議和KDT的終端使用者許可協議的傳輸檔案。

     這些元件使用RSA金鑰和GOST R 34.11-2012金鑰進行簽署。

   - 包含KDT公用程式的存檔，以及組態檔和KUMA清查檔案的範本

2. **安裝資料庫管理系統 (DBMS)**

   手動將DBMS安裝在不會包含在Kubernetes叢集內的獨立伺服器上。

   使用受支援的高可用性資料庫組態之一：Kaspersky Next XDR Expert的高可用性組態。

3. **準備管理員和目標主機**

定義將部署Kubernetes叢集和Kaspersky Next XDR Expert元件的目標主機數量。Kaspersky Next XDR Expert的高可用性組態必須至少有7個目標主機。

準備管理員主機和目標主機以部署Kaspersky Next XDR Expert。

操作說明：多節點部署：準備管理員主機和目標主機

4. **準備組態檔**

準備YAML格式的組態檔。組態檔包含部署目標主機列表和Kaspersky Next XDR Expert元件的安裝參數集。

操作說明：多節點部署：指定安裝參數

您可以手動填寫組態檔範本；或使用部署精靈指定Kaspersky Next XDR Expert部署所需的安裝參數，然後產生組態檔。

操作說明：使用設定精靈指定安裝參數

5. **Kaspersky Next XDR Expert的部署**

使用KDT部署Kaspersky Next XDR Expert。Kaspersky Deployment Toolkit會自動部署Kubernetes叢集，並在該叢集內安裝OSMP元件和其他基礎設施元件。

操作說明：安裝Kaspersky Next XDR Expert

6. **在Kubernetes叢集內安裝KUMA服務**

安裝KUMA服務（收集器、關聯器和儲存體）。

操作說明：在Kubernetes叢集內安裝KUMA服務

7. **新增從屬管理伺服器（可選）**

從屬管理伺服器是進一步整合端點代理程式所必需的。

操作說明：新增從屬管理伺服器

8. **安裝和整合端點代理程式**

根據端點代理程式說明文件安裝端點代理程式：

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

設定與端點代理程式的整合。

9. **安裝和整合沙盒**

安裝沙盒，進行設定，然後在其中安裝虛擬機器。之後，設定與沙盒的整合。

說明：

- 安裝沙盒元件
- 初始社會設定
- 準備虛擬機器
- 與沙盒整合

Kaspersky Next XDR Expert的高可用性組態

Kaspersky Next XDR Expert的高可用性組態可確保即使部署該解決方案的任何Kubernetes叢集節點發生故障或失去網路連線，也能確保連續正常運行和資料可用。

在高可用性組態中，您至少需要7個Kubernetes叢集節點：

- 三個主節點（控制平面節點）
- 四個工作線程節點

如果您打算在虛擬化環境中部署 Kaspersky Next XDR Expert，其中叢集節點作為虛擬機器執行，我們建議將虛擬機器分佈在不同的實體目標主機上。這種方法確保單一實體主機的故障不會影響解決方案中的多個虛擬節點。虛擬機器在實體主機上的放置和分佈由Hypervisor程式管理。

支援以下高可用性資料庫組態：

- Postgres Pro企業版BiHA叢集
  - 版本：Postgres Pro企業版16或更高版本
  - 叢集類型：BiHA
  - 節點數：3到15
  - 複製類型：同步。
  - 用於存取DBMS的連線字串包括叢集節點清單（由`psql_dsn`參數指定）：

    ```
    psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>
    ```

- 包含虛擬IP的PostgreSQL叢集（Corosync/Pacemaker）
  - 叢集類型：包含虛擬IP的PostgreSQL叢集（Corosync/Pacemaker）
  - 節點數：3 個或更多
  - 用於存取DBMS的連線字串包括DBMS叢集的虛擬IP地址（由`psql_dsn`參數指定）：

    ```
    psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>
    ```

支援以下安裝在Kubernetes叢集內的KUMA服務的高可用性組態：

- KUMA儲存體
  - 工作線程節點數：3個或更多
  - KUMA儲存體綁定到這些節點，不得遷移到其他節點。

- KUMA儲存體直接使用這些節點的磁碟，不使用Longhorn。
- 不允許將由同一KUMA資源建立的儲存體放在同一工作線程節點上。此規則確保了所需的容錯性。

- KUMA Core
  - 工作線程節點數：1個
    高可用性由Kubernetes機制保證；節點出現故障時，停機時間約為6分鐘。
- KUMA收集器
  有兩種高可用性組態：
  - 工作線程節點數：2個
    節點出現故障時，停機時間最短。
  - 工作線程節點數：1個
    高可用性由Kubernetes機制保證；停機時間約6分鐘。
- KUMA關聯器
  - 工作線程節點數：1個
    Kubernetes機制保證了高可用性。節點故障時，停機時間約6分鐘。
- KUMA事件路由器
  有兩種高可用性組態：
  - 工作線程節點數：2個
    節點出現故障時，停機時間最短。
  - 工作線程節點數：1個
    Kubernetes機制保證了高可用性。節點故障時，停機時間約6分鐘。
- KUMA指標
  - 工作線程節點數：1個
    Kubernetes機制保證了高可用性。節點故障時，停機時間約6分鐘。

恢復Kubernetes叢集中的故障節點

如果Kubernetes叢集節點發生電源或網路故障，但其磁碟資料完好無損且網路名稱未更改，管理員應恢復電源和網路連線。節點恢復運作後，約5-6分鐘內會自動重新加入叢集。

如果節點的磁碟資料損壞或遺失，或者由於故障導致主機名稱更改，則必須重新配置節點並使其再次準備作為Kubernetes叢集的一部分運行，然後再將其重新新增至叢集。

要準備並將節點新增到Kubernetes叢集中：

1. 準備將充當主節點和工作線程節點的目標主機。
2. 在管理員主機上，使用以下命令匯出目前的組態檔：

   ```
   ./kdt ec -e '<configuration_file_name_with_path>'
   ```

   目前版本的組態檔將以指定的名稱儲存到指定的目錄中。
3. 在匯出的組態檔的 `nodes` 區段中，刪除故障節點參數，並新增已恢復節點的參數（`desc`、`type`、`host`、`kind`、`user` 和 `key`）。儲存更新的組態檔。
4. 使用 ssh-copy-id 公用程式將公開金鑰複製至每個新節點（例如，複製至 `~/.ssh` 目錄）。
5. 在管理員主機上，執行以下命令將修改後的設定檔套用到Kubernetes叢集，並指定設定檔的完整路徑：

   ```
   ./kdt apply -i '<設定檔的完整路徑>'
   ```

   執行後，KDT將驗證設定檔。隨後KDT會檢查Kubernetes叢集節點的硬體、軟體及網路設定是否符合安裝先決條件。如果所有嚴格的預檢查都成功完成，KDT會向stdout和KDT日誌輸出驗證成功的通知。否則，系統將儲存包含驗證失敗資訊的日誌，並中止新增主機的進程。如有需要，可以透過將`ignore_precheck`安裝參數設定為`true`，跳過執行命令前的預檢查。

已復原的節點已新增至Kubernetes叢集。然後，KDT將有關恢復節點的資訊輸出到stdout和KDT日誌中。

Kaspersky Next XDR Expert 的高可用性多站台部署

Kaspersky Next XDR Expert 的高可用性多站台部署透過將 Kubernetes 叢集節點分散在多個資料中心，提供容錯能力。如果某個資料中心無法使用，工作負載會自動轉移到另一個資料中心的叢集節點，讓 Kaspersky Next XDR Expert 能夠在將中斷降至最低的情況下持續運作。

多站台組態至少需要三個資料中心。在至少三個資料中心部署 Kaspersky Next XDR Expert，可確保在某個資料中心無法使用時，仍能維持 Kubernetes 仲裁。在每個資料中心中，您必須部署至少四個叢集節點：一個主要節點和三個工作節點。每個資料中心都會使用自己的 Kubernetes 叢集閘道，並具有專用 IP 位址。目標主機和 Kubernetes 叢集閘道必須位於資料中心內的相同子網路中。

每個資料中心至少需要一台 Sandbox 主機。必須使用由客戶管理的高可用性負載平衡器，將流量分散到不同資料中心的叢集節點。您也必須在支援的高可用性組態中安裝 DBMS。

例如，在包含三個資料中心的多站台組態中，必須至少有 15 台主機：

- Kubernetes 叢集中包含的 12 台目標主機：
  - 一個主要節點，3 個主要節點（每個資料中心至少 1 個節點）
  - 9 個工作節點（每個資料中心至少 3 個節點）
- 3 台 Sandbox 主機（每個資料中心至少 1 個節點）

此外，部署需要由客戶管理的高可用性負載平衡器，以及以支援的高可用性組態部署的 DBMS。

多站台部署限制

- 位於不同資料中心的節點之間的頻寬必須至少為 10 Gbps，且延遲不得超過 20 毫秒。
- 任兩個資料中心之間的最大距離為 1200 公里（根據同步複寫的 20 毫秒延遲要求）。
- 位於不同資料中心的 Kubernetes 叢集節點必須能透過 Kaspersky Next XDR Expert 使用的所有連接埠進行網路連線。
- 同一資料中心內的所有 Kubernetes 叢集節點必須位於同一廣播網域。
- 資料庫必須以具備同步複寫的高可用性組態部署，且仲裁節點必須位於與資料庫節點不同的可用區域。

資料中心故障期間的已知問題

- 如果資料中心宕機，惡意軟體防護引擎傳送至資料中心中 Sandbox 進行掃描的檔案可能會丟失。此外，Sandbox 中的自動掃描也可能經歷延遲。
- 停電時正在資料中心中執行的 IRP 工作（包括掃描工作）也可能丟失。這些工作的偵測結果將不會收到。
- 當資料中心宕機時，由於外部系統中佇列堆積，剩餘資料中心的 Sandbox 可能超載。結果，隨著 Sandbox 負載上升，可能發生工作遺失的情況。
- 如果傳送至資料中心進行掃描的檔案由於資料中心故障而未得到處理，這些檔案的掃描結果（偵測）將會丟失，並且檔案可能會被預設標記為「乾淨」。如果 Sandbox 符合大小要求，檔案和偵測丟失可能持續達 15 分鐘，否則最長 1 小時。
- 還原資料中心或新增資料中心以建立多站台部署後，在同步叢集資料期間，解決方案可能需要 30–60 分鐘才能具備容錯能力。在此期間，解決方案會正常運作，但如果其中一個資料中心離線，解決方案可能會無法使用。如果資料量大於預設大小，同步可能需要更長時間。資料中心之間的低頻寬或高延遲也可能延長同步時間。

階段

依照此情境，您可以準備基礎設施，以在多個資料中心部署 Open Single Management Platform 以及 Kaspersky Next XDR Expert 所需的所有元件，準備包含安裝參數的組態檔，並使用 Kaspersky Deployment Toolkit 公用程式（以下簡稱 KDT）部署解決方案。

在部署Open Single Management Platform和Kaspersky Next XDR Expert元件之前，建議您閱讀硬化指南 。

此部署情境分幾個階段進行：

1. **下載包含Kaspersky Next XDR Expert元件的分發套件**

分發套件包含以下元件：

- 包含Kaspersky Next XDR Expert元件和Kaspersky Next XDR Expert和KDT最終使用者產品授權協議的傳輸存檔

  這些元件使用RSA金鑰和GOST R 34.11-2012金鑰進行簽署。您可以驗證Kaspersky Next XDR Expert元件的真實性和完整性。

- 使用KDT公用程式進行歸檔，以及組態檔和KUMA清單檔案的範本。

2 安裝資料庫管理系統 (DBMS)

在支援的其中一種高可用性資料庫組態中，於獨立伺服器上手動安裝 DBMS：Kaspersky Next XDR Expert 的高可用性組態。

DBMS 由客戶提供並設定。

3 設定高可用性負載平衡器

設定高可用性負載平衡器，以在位於多個資料中心的叢集節點之間分配傳入流量。

負載平衡器由客戶提供並設定。

組態檔範例

例如，您可以使用開放原始碼 HAProxy 作為負載平衡器。在負載平衡器組態中，為每個資料中心指定 Kubernetes 叢集閘道 IP 位址（組態檔中的 `ingress_ip` 參數）。

```
global
  log /dev/log  local0
  log /dev/log  local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin
  stats timeout 30s
  user haproxy
  group haproxy
  daemon
defaults
  log  global
  mode  http
  option  httplog
  option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
  errorfile 400 /etc/haproxy/errors/400.http
  errorfile 403 /etc/haproxy/errors/403.http
  errorfile 408 /etc/haproxy/errors/408.http
  errorfile 500 /etc/haproxy/errors/500.http
  errorfile 502 /etc/haproxy/errors/502.http
  errorfile 503 /etc/haproxy/errors/503.http
  errorfile 504 /etc/haproxy/errors/504.http
listen stats
    mode http
    bind *:8080
    stats enable
    stats uri /stats
    stats refresh 10s
#    stats admin if LOCALHOST
frontend http
  mode tcp
  bind :80
  default_backend http_servers
backend http_servers
  mode tcp
  balance first
  option tcp-check
```

```
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:80 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:80 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:80 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend https
  mode tcp
  bind :443
  default_backend https_servers
backend https_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend https9
  mode tcp
  bind :9443
  default_backend https9_servers
backend https9_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:9443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:9443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:9443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend https4
  mode tcp
  bind :4443
  default_backend https4_servers
backend https4_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:4443 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:4443 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:4443 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
frontend ksc13000
  mode tcp
  bind :13000
  default_backend ksc13000
backend ksc13000
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <ingress_ip_1>:13000 check inter 5s # first data center - IP address of the Kubernetes
cluster gateway
  server proxmox2 <ingress_ip_2>:13000 check inter 5s # second data center - IP address of the Kubernetes
cluster gateway
  server proxmox3 <ingress_ip_3>:13000 check inter 5s # third data center - IP address of the Kubernetes
cluster gateway
```

4 準備管理員和目標主機

定義每個資料中心中將部署 Kubernetes 叢集和 Kaspersky Next XDR Expert 元件的目標主機數量，然後準備管理員主機和目標主機以部署 Kaspersky Next XDR Expert。

如果您要執行多站台部署，您還必須設定 DNS 記錄，讓服務 FQDN 解析為客戶管理的負載平衡器 IP 位址。

操作說明：多站台部署：準備管理員主機和目標主機

5. **準備KUMA主機以在Kubernetes叢集外部安裝KUMA服務（可選）**

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部，也可以完全安裝在叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在叢集外部。

如果您希望將KUMA服務完全安裝在Kubernetes叢集外部的獨立主機上，或部分安裝在叢集內部，部分安裝在叢集外部，請準備KUMA目標主機以安裝KUMA服務。

操作說明：準備KUMA主機以在Kubernetes叢集外部安裝KUMA服務

6. **準備KUMA清查檔案以在Kubernetes叢集外部安裝KUMA服務（可選）**

如果您希望將KUMA服務完全安裝在Kubernetes叢集外部的獨立主機上，或部分安裝在叢集內部，部分安裝在叢集外部，請準備YAML格式的KUMA清查檔案。KUMA清查檔案包含在Kubernetes叢集之外安裝KUMA服務的參數。

操作說明：準備KUMA清查檔案以在Kubernetes叢集外部安裝KUMA服務

7. **準備組態檔**

準備YAML格式的組態檔。組態檔包含部署目標主機列表和Kaspersky Next XDR Expert元件的安裝參數集。

如果您正在執行多站台部署，則也必須指定基礎架構區域和資料中心的參數。

操作說明：多站台部署：指定安裝參數

8. **Kaspersky Next XDR Expert的部署**

使用KDT部署Kaspersky Next XDR Expert。Kaspersky Deployment Toolkit會自動部署Kubernetes叢集，並在該叢集內安裝OSMP元件和其他基礎設施元件。

操作說明：安裝Kaspersky Next XDR Expert

9. **安裝KUMA服務**

安裝KUMA服務（收集器、關聯器和儲存體）。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部，也可以完全安裝在叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在叢集外部。

操作說明：在Kubernetes叢集外部安裝KUMA服務

操作說明：在Kubernetes叢集內安裝KUMA服務

10. **新增從屬管理伺服器**

從屬管理伺服器是進一步整合端點代理程式所必需的。

操作說明：新增從屬管理伺服器

11. **安裝和整合端點代理程式**

根據端點代理程式說明文件安裝端點代理程式：

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

設定與端點代理程式的整合。

12. **安裝和整合沙盒**

    安裝沙盒，進行設定，然後在其中使用安裝程式安裝虛擬機器。

    設定與沙盒的整合。

多站台部署：準備管理員主機和目標主機

多站台部署的準備工作包括設定管理員主機和目標主機。準備好主機並指定設定檔後，您將能夠使用KDT在目標主機上部署Kaspersky Next XDR Expert。

準備管理員主機

首先，您需要準備一台裝置作為啟動KDT的管理員主機。該主機可以包含在KDT在部署期間建立的Kubernetes叢集中，也可以不包含在內。如果管理員主機不包含在叢集中，它將僅用於部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。

若要準備管理員主機：

1. 確保管理員主機上的硬體和軟體符合需求。

   如果管理員主機未包含在Kubernetes叢集，請使用KDT需求。

   如果管理員主機包含在叢集，請使用多節點部署的硬體需求和OSMP的軟體需求。

2. 請在暫存檔案目錄（預設為 `/tmp`）中為 KDT 配置至少 15 GB 的可用空間。若此目錄中的可用空間不足，請執行以下命令以指定另一個目錄的路徑：

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

3. 設定容器執行階段。使用下列其中一個容器執行階段：

   - KDT 內建容器執行階段（以 runc 為基礎）。

     執行下列命令以安裝內建容器執行階段：

     ```
     sudo ./kdt init
     ```

     如果內建容器執行階段不符合您的需求，可以改用 Docker 容器執行階段。

   - Docker 容器執行階段。

     安裝 Docker 25 版本的套件或更新版本，然後執行安裝後步驟，設定管理主機以確保 Docker 正常運作。

     Docker 資料儲存的磁碟分割區（預設為 `/var/lib/docker`）必須至少有 60 GB 可用空間。

     請勿從作業系統維護者儲存區安裝非官方的Docker軟體套件發行版。

4. 對於將包含在叢集中的管理主機，請執行其他準備步驟：

   a. 由於該裝置將充當管理員和目標主機，請確保它符合多節點部署的需求。

   b. 確保cgroup v2 技術在管理員主機上受支援。

準備目標主機

目標主機是用於部署Kaspersky Next XDR Expert並包含在Kubernetes叢集中的實體機或虛擬機。Kaspersky Next XDR Expert元件在這些主機上運作。

其中一個目標主機可用作管理員主機。在這種情況下，您必須按照上一步驟所述將此主機準備為管理員主機，然後執行目標主機的準備工作。

若為包含三個資料中心的多站台組態，則必須至少有 12 個叢集節點：

- 一個主要節點，3 個主要節點（每個資料中心至少 1 個節點）

  主要節點用於管理叢集、儲存元資料和分配工作負載。

- 9 個工作節點（每個資料中心至少 3 個節點）

  工作節點用於執行Kaspersky Next XDR Expert元件的工作負載。

叢集集中的主節點和工作線程節點數量可能有所不同。為了在節點之間實現最佳工作負載分配，建議使用效能大致相同的節點。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。

若要準備目標主機：

1. 確保目標主機上的硬體和軟體符合多節點部署的需求，並且目標主機位於同一廣播域中。

   如果KUMA服務安裝在叢集內，目標主機必須滿足安裝KUMA服務所需的硬體、軟體和安裝需求。

   為了Kaspersky Next XDR Expert正常運作，在裝有Ubuntu系列作業系統的目標主機上，Linux核心版本必須為5.15.0.107或更高版本。

   除將用作管理員主機的目標主機外，不得在目標主機上安裝 Docker。KDT將在部署期間安裝所有必要的軟體和依賴項。

2. 確保掛載在 `/var` 的檔案系統在每個目標主機上至少有 700 GB 的可用空間。

3. 在每個目標主機上，如果尚未安裝sudo套件，請安裝此套件。對於Debian系列作業系統，在目標主機上安裝UFW軟體套件。

4. 在每個目標主機上，設定/etc/environment檔案。如果您的組織基礎設施使用代理伺服器存取網際網路，請在目標主機上使用代理伺服器設定網際網路存取。

5. 在具有UFW組態的主節點上，允許IP轉送功能。在 `/etc/default/ufw` 檔案中，將 `DEFAULT_FORWARD_POLICY` 設為 `ACCEPT`。

6. 提供對儲存Kaspersky Next XDR Expert所需的以下軟體套件的軟體套件儲存區的存取權限：

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

   KDT將在部署期間嘗試從軟體套件儲存區安裝這些軟體套件。您也可以手動安裝這些安裝套件。

7. 確保滿足以下條件：

   - 在每個目標主機上：python3-apt
   - 在主節點上：curl

   使用KDT從軟體套件儲存區部署期間不會安裝curl和libnfs軟體套件。如果尚未安裝這些安裝套件，則必須手動安裝它們。

8. 針對目標主機，請在Hypervisor、虛擬交換器或網路基礎設施層級停用 ARP/MAC欺騙防護機制。

   對於 VMware，請啟用**偽造傳輸**和**MAC 位址變更**。對於 Hyper-V，請啟用**MAC 位址欺騙**。對於網路設備，請停用**動態 ARP 檢查 (DAI)**，或將連接埠設定為受信任。

   如需範例，請參閱MetalLB 疑難排解指南，瞭解如何檢查 ARP 要求是否到達節點。

9. 為目標主機和Kubernetes叢集閘道保留靜態IP位址。

   Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。閘道 IP 位址為 IPv4 位址（例如，10.80.23.182）。

   在多站台組態中，每個資料中心都會使用自己的Kubernetes叢集閘道，並具有專用IP位址。這會在每個資料中心的設定檔中指定（ `zones` 區段中的 `ingress_ip` 參數）。

目標主機和 Kubernetes 叢集閘道必須位於資料中心內的相同子網路中。

Kubernetes叢集閘道和目標主機需要IPv4位址。如果您的環境需要IPv6連線，請在目標主機和Kubernetes叢集閘道上設定作業系統，以便透過IPv6閘道（NAT64）或IPv6隧道路由IPv6流量。此組態可使叢集在IPv4上執行，同時提供與IPv6網路的互通性。

10. 在您的DNS伺服器上，註冊服務FQDN以連線到Kaspersky Next XDR Expert服務。

    預設情況下，Kaspersky Next XDR Expert服務在以下位址可用：

    - <console_host>.<smp_domain>
    - <ksc_host>.<smp_domain>
    - <kuma_host>.<smp_domain>
    - <api_host>.<smp_domain>
    - <monitoring_host>.<smp_domain>
    - <xdr_edr_ingress_host>.<smp_domain>
    - <updater>.<smp_domain>

      其中，<console_host>、<ksc_host>、<kuma_host>、<api_host>、<monitoring_host>、<xdr_edr_ingress_host>和<updater>皆為服務主機名稱，<smp_domain>為服務網域名稱。這些參數是服務FQDN 的組成部分，且可在設定檔中指定。如果您未指定服務主機名稱的自訂值，將使用預設值：`console_host—"console"`，`ksc_host—"admsrv"`，`kuma_host—"kuma"`，`api_host—"api"`，`monitoring_host—"monitoring"`，`xdr_edr_ingress_host—"agentserver"`，`updater—"updater"`。

    所列的服務FQDN必須解析為客戶管理的負載平衡器的IP位址。

    例如：

    - <load_balancer_host_ip>—admsrv.<smp_domain>
    - <load_balancer_host_ip>—api.<smp_domain>
    - <load_balancer_host_ip>—console.<smp_domain>
    - <load_balancer_host_ip>—kuma.<smp_domain>
    - <load_balancer_host_ip>—*.kuma.<smp_domain>
    - <load_balancer_host_ip>—monitoring.<smp_domain>
    - <load_balancer_host_ip>—agentserver.<smp_domain>
    - <load_balancer_host_ip>—updater.<smp_domain>

11. 在目標主機上，建立將用於部署Kaspersky Next XDR Expert的帳戶。

    這些帳戶用於 SSH 連線，且必須能夠在不輸入密碼的情況下提升權限 (sudo)。為此，請將建立的使用者帳戶新增至 `/etc/sudoers` 檔案。

    檢視詳情

若要將建立的使用者帳戶新增至 `/etc/sudoers` 檔案：

1. 執行以下指令：

```
sudo useradd -m -s /bin/bash <user_name>
sudo usermod -aG sudo <user_name>
```

2. 使用以下指令開啟 `/etc/sudoers` 檔案：

```
sudo visudo
```

3. 在 `# Allow members of group sudo to execute any command` 區段的結尾新增下列行：

```
<user_name> ALL=(ALL) NOPASSWD: ALL
```

其中 `<user_name>` 是所建立使用者的名稱。

4. 儲存並關閉 `/etc/sudoers` 檔案。

12. 設定管理員和目標主機之間的SSH連線：

a. 在管理員主機上，使用ssh-keygen公用程式產生SSH金鑰（無需密碼）。

b. 使用 ssh-copy-id 公用程式將公開金鑰複製到每個目標主機；如果使用負載平衡器，則也複製到負載平衡器主機（例如，複製到 `/home/<user_name>/.ssh` 目錄）。

如果使用目標主機作為管理員主機，則也必須將公鑰複製到該主機。

13. 為了使Kaspersky Next XDR Expert元件正常運作，請在目標主機之間提供網路存取，並在必要時在管理員和目標主機的防火牆上打開所需的連接埠。

14. 在管理員和目標主機上設定透過網路時間協定（NTP）進行時間同步。

15. 如有必要，請準備自訂憑證以用於Kaspersky Next XDR Expert公共服務。

您可以為每個服務使用一個從組織的根憑證或葉憑證頒發的中間憑證。將使用準備好的自訂憑證取代自簽名憑證。

多站台部署：指定安裝參數

組態檔是YAML格式的檔案，包含Kaspersky Next XDR Expert元件的安裝參數集。

組態檔模板中並未包含下面列出的所有參數。此範本僅包含部署Kaspersky Next XDR Expert之前必須指定的參數。其餘參數設定為預設值，不包含在範本中。您可以手動將這些參數新增至組態檔以覆蓋其值。參數值必須遵循下面所述的規則。在Kaspersky Next XDR Expert 部署期間，KDT會檢查是否正確指定了所需的安裝參數。如果組態檔中必需的參數缺失或無效，部署將會中斷。

Kaspersky Next XDR Expert多站台部署組態檔範例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
```

```
#Infrastructure regions that contain data centers
regions:
  # Infrastrusture region 1
  prox1:
    # Name of the infrastructure region.
    description: Proxmox1
  # Infrastructure region 2
  prox2:
    # Name of the infrastructure region.
    description: Proxmox2
  # Infrastructure region 3
  prox3:
    # Name of the infrastructure region.
    description: Proxmox3
# Data centers where the Kubernetes cluster nodes are distributed
zones:
  # Data center 1
  proxmox1:
    # Name of the infrastructure region that the data center belongs to.
    region: prox1
    # Kubernetes cluster gateway IP address of the data center 1.
    ingress_ip: 10.0.0.200
  # Data center 2
  proxmox2:
    # Name of the infrastructure region that the data center belongs to.
    region: prox2
    # Kubernetes cluster gateway IP address of the data center 2.
    ingress_ip: 10.10.20.100
  # Data center 3
  proxmox3:
    # Name of the infrastructure region that the data center belongs to.
    region: prox3
    # Kubernetes cluster gateway IP address of the data center 3.
    ingress_ip: 10.65.20.100
# Nodes on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
  # Data center 1 - primary node
  - desc: cdt-primary1
    # Node type.
    type: primary
    # Name of the data center that the node belongs to.
    zone: proxmox1
    # IP address of the node.
    host: 10.0.0.100
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
        # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
        key: /root/.ssh/id_rsa
  # Data center 2 - primary node
  - desc: cdt-primary2
    # Node type.
    type: primary
    # Name of the data center that the node belongs to.
    zone: proxmox2
```

```
  # IP address of the node.
  host: 10.10.20.18
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
# Data center 3 - primary node
- desc: cdt-primary3
  # Node type.
  type: primary
  # Name of the data center that the node belongs to.
  zone: proxmox3
  # IP address of the node.
  host: 10.65.20.100
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 1
- desc: cdt-w1
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.101
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
# Data center 1 - worker node 2
- desc: cdt-w2
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.102
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
```

```
# Data center 1 - worker node 3
- desc: cdt-w3
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox1
  # IP address of the node.
  host: 10.0.0.103
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 1
- desc: cdt-w4
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.20
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 2
- desc: cdt-w5
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.21
  access:
    ssh:
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
# Data center 2 - worker node 3
- desc: cdt-w6
  # Node type.
  type: worker
  # Name of the data center that the node belongs to.
  zone: proxmox2
  # IP address of the node.
  host: 10.10.20.22
  access:
    ssh:
```

```
      # User name of the account&period;
      user: root
      # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
      # password: pass
      # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
      key: /root/.ssh/id_rsa
  # Data center 3 - worker node 1
  - desc: cdt-w7
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.11
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
        # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
        key: /root/.ssh/id_rsa
  # Data center 3 - worker node 2
  - desc: cdt-w8
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.12
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
        # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
        key: /root/.ssh/id_rsa
  # Data center 3 - worker node 3
  - desc: cdt-w9
    # Node type.
    type: worker
    # Name of the data center that the node belongs to.
    zone: proxmox3
    # IP address of the node.
    host: 10.65.20.13
    access:
      ssh:
        # User name of the account&period;
        user: root
        # 用於連線至節點的密碼。 可以用來取代由 ssh_pk 參數指定的 SSH 金鑰。
        # password: pass
        # KDT 用於連線到主要工作節點的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
        key: /root/.ssh/id_rsa
# Parameters for the Kaspersky XDR deployment
parameters:
  # Connection string for accessing the DBMS installed and configured on a separate
  server.
```

```
# user_db – 具權限的內部 DBMS 帳戶的使用者名稱。 此帳戶被授予建立資料庫及其他 DBMS 帳戶的權限。
# password_db—The password of the privileged internal DBMS account.
# fqdn_db:port_db—The FQDN and connection port of a separate server on which the DBMS is installed.
# 'psql_dsn' 參數值必須符合 URI 格式。 如果連線 URI 的任何部分包含具有特殊意義的符號，則必須使用百分比編碼進行編碼。
- name: psql_dsn
  source:
    value: "postgres://postgres:password@dbms.example.com:1234"
# KDT 連線至主要節點和工作節點所用的 SSH 私密金鑰路徑。SSH 私密金鑰位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: ssh_pk
  source:
    path: /root/.ssh/id_rsa
# Password of the Kaspersky XDR user account that will be created during the installation.
# Password must be 8 to 256 characters long.
# It can contain lowercase or uppercase letters ('a' to 'z'), digits ('0' to '9'), and special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- name: admin_password
  source:
    value: "password"
# 包含 KUMA 服務部署安裝設定的 KUMA 清單檔案路徑。 此檔案位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# Kaspersky Endpoint Detection and Response 產品授權金鑰的路徑。 此檔案位於管理員主機上。
# The parameter value must be a Linux file path or Base64-encoded file content.
- name: license
  source:
    value: "/home/user/license.key"
# 網域名稱。 參數值必須符合最高至第四層網域的命名要求。
# The service host name and domain name are parts of FQDNs of the Kaspersky XDR services.
# Default values of service host names: nwc_host—"console", flow_host—"console", hydra_host—"console", login_host—"console", ksc_host—"admsrv", console_host—"console", api_host—"api", kuma_host—"kuma", monitoring_host—"monitoring".
# Custom host names can be specified in the configuration file.
# 範例：console.smp.local 是提供 OSMP 主控台存取權限的服務的 FQDN。 此 FQDN 由「console_host」和「smp_domain」設定的值組成。
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom certificate must be generated.
# 參數值必須是以空格分隔的主機名稱清單。 如果未指定自訂主機名稱，則會使用下列預設主機名稱：
- name: pki_host_list
  source:
    value: "admsrv api console kuma monitoring agentserver updater"
# The parameter that indicates whether to deploy the KUMA services for Kaspersky EDR or for Kaspersky NGFW.
- name: autodeploy_plan
  source:
    value: "edr"
# User name for authentication on the SMTP server.
- name: grafana_admin_user
```

```
  source:
    value: xdr
# Password for authentication on the SMTP server.
- name: grafana_admin_password
  source:
    value: "password"
```

為了確保KDT與設定檔正確配合使用，請在檔案末端新增一個空白行。

`regions` 區段包含每個邏輯基礎架構區域的安裝參數。區域代表地理區域或部署位置，並將一或多個資料中心（區域）分組在一起。

區域區段

參數名稱	必要	描述
`description`	是	基礎架構區域的名稱。 值必須符合以下規則： • 節點名稱長度必須為1到63個字元。 • 節點名稱可以包含以下字元： • 大寫ASCII字母（A-Z） • 小寫ASCII字母（a-z） • 數字（0-9） • 連字符（-） 所有基礎設施區域的名稱都必須唯一。

`zones` 區段包含每個資料中心的安裝參數。每個可用區都屬於特定的區域。

可用區部分

參數名稱	必要	描述
`region`	是	可用區所屬的基礎設施區域名稱。 值必須符合以下規則： • 節點名稱長度必須為1到63個字元。 • 節點名稱可以包含以下字元： • 大寫ASCII字母（A-Z） • 小寫ASCII字母（a-z） • 數字（0-9） • 連字符（-） `region` 參數的值必須與 `regions` 區段中定義的區域識別碼相符。
`ingress_ip`	是	Kubernetes 叢集閘道的保留靜態 IPv4 位址。 Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。 每個資料中心都必須有其專屬且唯一的叢集閘道 IP 位址。閘道必須與位於同一資料中心的主要節點和工作節點位於同一個子網路中。

設定檔的 `nodes` 區段包含 Kubernetes 叢集每個 目標主機 的安裝參數。這些參數列於下表。

參數名稱	必要	描述
`desc`	是	節點名稱。 值必須符合以下規則： • 節點名稱長度必須為1到63個字元。 • 節點名稱可以包含以下字元： • 大寫ASCII字母（A-Z） • 小寫ASCII字母（a-z） • 數字（0-9） • 連字符（-） 所有叢集節點必須具有唯一名稱。此要求安裝Kaspersky Next XDR Expert的先決條件之一，並已通過KDT驗證。
`type`	是	節點類型。 可能的參數值： • `primary` • `worker`
`host`	是	節點的IP位址。 屬於某個資料中心的所有節點，都必須與該資料中心的 Kubernetes 叢集閘道位於同一子網路中。 節點需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。
`zone`	是	節點所屬資料中心的名稱。`zone` 參數的值必須與 `zones` 區段中定義之資料中心的識別碼相符。
`kuma_role`	否	您可以指定要在工作線程節點上安裝的KUMA服務。您可以指定一個、多個或不指定任何KUMA服務。 當使用OSMP主控台將KUMA服務安裝在Kubernetes叢集內時，會考慮 `kuma_roles` 參數。如果您打算安裝KUMA服務的節點過載，叢集將選擇另一個負載較低的節點進行服務安裝。 KUMA服務（收集器、關聯器和儲存體）可以完全安裝在工作線程節點上的叢集內，完全安裝在Kubernetes叢集外的單獨主機上，或部分安裝在Kubernetes叢集內部和部分外部。如果所有KUMA服務都將安裝在叢集內部，請將 `inventory` 參數設為 `/dev/null`。 不允許將由同一KUMA資源建立的儲存體放在同一工作線程節點上。此規則確保了所需的容錯性。 如果儲存體叢集包含多個儲存體實例，則所有實例必須部署在叢集內部或叢集外部。 可能的參數值： • `core`—KUMA Core • `metrics`—KUMA指標 • `collector`—收集器 • `eventrouter`—事件路由器 • `correlator`—關聯器 • `storage`—儲存體 參數值指定為包含KUMA角色的字串清單。例如： `kuma_roles: ["core","metrics","collector"]`
`user`	是	在目標主機上建立的帳戶的使用者名，用於透過KDT連線到節點。 值必須符合以下規則： • 使用者名稱長度必須為1到31個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 底線(_)、連字號（-）
`password`	否	用於連接節點的密碼。可以代替由 `ssh_pk` 參數指定的 SSH 金鑰。

其他安裝參數列於設定檔的 `parameters` 區段，如下表所述。

參數名稱	必要	描述

`psql_dsn`	是	用於存取在Kubernetes叢集外部安裝和設定的DBMS的連接字串。
		如下指定此參數：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn>:<port>`
		其中：
		• `dbms_username` — 具權限的內部 DBMS 帳戶的使用者名稱。此帳戶被授予建立資料庫及其他 DBMS 帳戶的權限。透過使用此具權限的 DBMS 帳戶，部署期間將建立 Kaspersky Next XDR Expert 元件所需的資料庫及其他 DBMS 帳戶。
		• `password` — 具權限的內部 DBMS 帳戶的密碼。
		• `fqdn:port` — 安裝有 DBMS 的目標主機的 FQDN 與連接埠。
		若要使用高可用性叢集，請如下指定此參數：
		`psql_dsn=postgres://<dbms_username>:<password>@<fqdn1>:<port>,<fqdn2>:<port>,<fqdn3>:<port>`
		若要使用Corosync/Pacemaker，請以下列方式使用虛擬IP指定此參數：
		`psql_dsn=postgres://postgres:pass!@<virtual ip>:<port>`
		`psql_dsn` 參數值必須符合 URI 格式。若連線 URI 的任一部分包含具有特殊意義的符號，則必須以百分比編碼進行編碼。
		`psql_dsn` 參數值中必須替換的符號：
		• 空白字元 → `%20`
		• ! → `%21`
		• # → `%23`
		• % → `%25`
		• & → `%26`
		• / → `%2F`
		• : → `%3A`
		• = → `%3D`
		• ? → `%3F`
		• @ → `%40`
		• [→ `%5B`
		•] → `%5D`
		請參閱PostgreSQL 連線字串一文以瞭解詳細資訊。

`nwc-language`	是	預設指定OSMP主控台介面的語言。安裝後，您可以變更OSMP主控台語言。 可能的參數值： • `enUS`（預設值） • `ruRu` 如果未在組態檔中指定此參數，則使用預設值。
`ssh_pk`	是	位於管理主機上 SSH 金鑰私鑰部分的路徑，該金鑰用於透過 KDT 連線至主要工作節點及具有 KUMA 服務的節點（收集器、關聯器與儲存體）。參數值必須為Linux檔案路徑或Base64編碼的檔案內容。
`admin_password`	是	`admin_password` 參數指定安裝過程中 KDT 所建立之 Kaspersky Next XDR Expert 使用者帳戶的密碼。該帳戶的預設使用者名稱為「admin」。 主管理員角色已指派給此使用者帳戶。 密碼必須符合以下規則： • 使用者密碼不能少於10個或多於256個字元。 • 密碼必須包含以下組中三組的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密碼不得包含任何空格或".@"組合。 手動指定 `admin_password` 參數值（而非透過部署精靈指定）時，請確保此值符合 YAML 標準對字串值的要求： • 包含特殊字元的參數值必須用單引號引起來。 • 參數值中的任何單引號'都必須重複以轉義此單引號。 範例：使用者帳戶密碼 `Any_pass%1234'5678"90` 必須指定為 `admin_password` 參數的值 `'Any_pass%1234''5678"90'`。

參數名稱	必要	描述
low_resources	否	此參數表示 Kaspersky Next XDR Expert 已安裝在運算資源有限的目標主機上。若要進行多節點部署，請將 low_resources 參數設定為 false。 可能的參數值： • true — 使用有限計算資源進行安裝（用於單節點部署） • false — 標準安裝（預設值）
core_disk_request	是	指定KUMA Core運行所需磁碟空間量的參數。 若未指定 core_disk_request 參數，且 low_resources 參數設定為 false 或未指定，KUMA Core 運行所需的預設磁碟空間量為 100 GB。 若未指定 core_disk_request 參數，且 low_resources 參數設定為 true，KUMA Core 運行所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 core_disk_request 參數。
metrics_disk_request	是	指定Metrics服務運作所需磁碟空間量的參數。 若未指定 metrics_disk_request 參數，且 low_resources 參數設定為 false 或未指定，Metrics 服務運作所需的預設磁碟空間量為 80 GB。 若未指定 metrics_disk_request 參數，且 low_resources 參數設定為 true，Metrics 服務運作所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 metrics_disk_request 參數。
inventory	是	位於管理員主機上的KUMA清查檔案的路徑。此清查檔案包含用於部署Kubernetes叢集中未包含的KUMA服務的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。如果所有 KUMA 服務都將安裝在叢集內部，請將 inventory 參數設為 /dev/null。
host_inventory	否	位於管理員主機上的附加KUMA清查檔案的路徑。此檔案包含用於部分新增或刪除具有KUMA服務的主機的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若執行 Kaspersky Next XDR Expert 的初始部署或執行需要設定檔的自訂動作，請保留預設參數值 (/dev/null)。
license	否	位於管理員主機上的KUMA產品授權金鑰的路徑。 參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 部署完成並登入OSMP後，您可以上傳產品授權金鑰或指定啟動碼。
nwc_host flow_host hydra_host login_host ksc_host console_host api_host kuma_host monitoring_host xdr_edr_ingress_host	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的主機名稱。服務主機名稱與網域名稱（ smp_domain 參數值）皆為服務 FQDN 的組成部分。 如果未指定自訂主機名稱，則使用下列預設主機名稱： • nwc_host—"console" • flow_host—"console" • hydra_host—"console" • login_host—"console" • ksc_host—"admsrv" • console_host—"console" • api_host—"api" • kuma_host—"kuma" • monitoring_host—"monitoring" • xdr_edr_ingress_host—"agentserver"
smp_domain	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的網域名稱。參數值必須符合最高四級網域的命名要求。 服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 console_host 變數的值為 console，而 smp_domain 變數的值為 smp.local，則提供 OSMP 主控台存取權的服務完整名稱為 console.smp.local。
pki_host_list	是	將生成自簽名或自訂憑證的公共Kaspersky Next XDR Expert服務的主機名稱列表。參數值必須是主機名稱列表，以空格分隔。

參數名稱	必要	描述
`intermediate_enabled`	否	該參數用於指示是否對 Kaspersky Next XDR Expert 公開服務使用自訂中間憑證而非自我簽署憑證。 可能的參數值： • `true` — 使用自訂中間憑證。 • `false` — 使用自我簽署憑證（預設值）。
`intermediate_bundle`	否	用於與 Kaspersky Next XDR Expert 公開服務協作之自訂中間憑證的路徑。若 `intermediate_enabled` 參數設定為 `true`，則指定此參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。自訂中級憑證的有效期限必須至少為399天。

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	否	用於與對應的公開 Kaspersky Next XDR Expert 服務搭配運作的自訂葉憑證路徑：`<admsrv_host>.<smp_domain>`、`<api_host>.<smp_domain>`、`<kuma_host>.<smp_domain>`、`<monitoring_host>.<smp_domain>` 和 `<console_host>.<smp_domain>`。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。
		如果要指定自訂葉憑證，請將 `intermediate_enabled` 參數設定為 `false`，且不要指定 `intermediate_bundle` 參數和 `pki_host_list` 參數。

`ksc_state_size`	是	分配用於儲存管理伺服器資料（更新、安裝套件和其他內部服務資料）的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。所需的可用磁碟空間量取決於受管理裝置的數量和其他參數，並且可以計算。 預設值為 30 GB。如果未在設定檔中指定此參數，則使用此值。
`prometheus_size`	是	分配給儲存指標的可用磁碟空間量。以GB為單位，指定為「<amount>GB」。 最小值與預設值皆為5GB。如果未在組態檔中指定此參數，則使用預設值。
`grafana_admin_user`	否	用於透過Grafana工具檢視OSMP指標的帳戶的使用者名稱。 值必須符合以下規則： • 使用者名稱長度必須為1到30個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 特殊字元（_ - .） • 使用者名稱必須以字母開頭。 • 使用者名稱不能包含空格或"@"符號。
`grafana_admin_password`	否	用於透過Grafana工具檢視OSMP指標的帳戶的密碼。 密碼必須符合以下規則： • 使用者密碼不能少於8個或多於256個字元。 • 密碼必須包含下列群組中的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配給儲存OSMP日誌的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。 最低建議值和預設值為 40 GB。如果未在組態檔中指定此參數，則使用預設值。
`loki_retention_period`	是	OSMP日誌的儲存週期，超過此週期後日誌將自動刪除。預設值為72小時（將設定檔中的參數值設定為「<time in hours>h」。例如：「72h」）。如果未在組態檔中指定此參數，則使用預設值。
`file_storage_cp`	否	指派給元件用於儲存資料以處理回應操作的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。最小推薦值為20 GB。
`psql_tls_off`	否	指示是否使用 TLS 協定對 Kaspersky Next XDR Expert 元件與 DBMS 之間的流量進行加密的參數。若 DBMS 安裝在叢集外部，則預設停用 TLS 加密（預設值為 `true`）。 可能的參數值： • `true` — 不加密流量（預設值）。 • `false` — 加密流量。

參數名稱	必要	描述
psql_trusted_cas	否	可以包含DBMS伺服器的TLS憑證或可以簽發TLS伺服器憑證的根憑證的PEM檔案的路徑。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若將在單獨的伺服器上安裝與設定 DBMS，並且已啟用流量加密（ psql_tls_off 設定為 false ），則請指定 psql_trusted_cas 參數。
proxy_enabled	否	指示是否使用代理伺服器將 Kaspersky Next XDR Expert 元件連線至網際網路的參數。若安裝 Kaspersky Next XDR Expert 的主機具有網際網路存取權限，亦可為 Kaspersky Next XDR Expert 元件（例如管理伺服器）的運作以及特定整合（包括卡巴斯基與第三方）提供網際網路存取權限。若要建立代理連線，還須在管理伺服器內容中指定代理伺服器參數。 可能的參數值： • true — 使用代理伺服器。 • false — 不使用代理伺服器（預設值）。
proxy_addresses	否	代理伺服器的IP位址。若代理伺服器使用多個 IP 位址，請指定這些位址，並以空格分隔（例如，"0.0.0.0 0.0.0.1 0.0.0.2"）。若 proxy_enabled 參數設定為 true，則指定此參數。
proxy_port	否	用於建立代理連線的連接埠號碼。若 proxy_enabled 參數設定為 true，則指定此參數。
trace_level	否	管理伺服器追蹤檔案的詳盡程度。追蹤在管理伺服器運作期間寫入。 預設值為0，不寫入任何追蹤。 可能的參數值：0–5。 參數值越高，追蹤詳細資訊越詳盡。
ansible_extra_flags	否	KDT執行的KUMA Core和KUMA服務部署日誌的詳盡程度。 可能的參數值： • -v • -vv • -vvv • -vvvv 隨著旗標中「v」字母數量的增加，日誌將變得更詳盡。如果組態檔中未指定此參數，則將儲存標準元件安裝日誌。
incident_attachments_max_count_limit	否	可附加到事件的檔案數量。預設值是 100。
incident_attachments_max_size_limit	否	已附加到事件的檔案總大小。以位元組為單位。指定時不指明測量單位。預設值是 26214400。
ignore_precheck	否	該參數用於指示是否在部署前檢查Kubernetes叢集節點的硬體、軟體及網路設定，以確認是否符合解決方案的安裝先決條件。 可能的參數值： • true — 略過預檢查。 • false — 執行預檢查（預設值）。
airgap_mode	否	此參數指示是否執行APT軟體套件管理器預檢查並更新軟體套件快取。這可讓您在實體隔離環境中部署Kaspersky Next XDR Expert。 可能的參數值： • true — 略過預檢查和軟體套件快取更新。 • false — 執行預檢查並更新軟體套件快取（預設值）。
grafana_smtp_host	否	Grafana的SMTP伺服器位址，用於發送有關Kubernetes叢集運行狀況事件的電子郵件通知。請以 <host>:<port> 格式指定此參數，例如 localhost:25。
grafana_smtp_user	否	在SMTP伺服器上進行身份驗證的使用者名稱。
grafana_smtp_password	否	在SMTP伺服器上進行身份驗證的密碼。
grafana_smtp_bundle	否	包含X.509憑證鏈的檔案，用於驗證與SMTP伺服器的TLS連線。
grafana_smtp_skip_verify	否	此參數指示是否跳過SMTP伺服器的TLS憑證驗證。 可能的參數值： • true—跳過TLS憑證驗證。 • false—執行TLS憑證驗證（預設值）。
grafana_smtp_from_address	否	寄件者的電子郵件地址，該地址將顯示在發送電子郵件通知時的「寄件者」欄位中。

參數名稱	必要	描述
grafana_smtp_from_name	否	電子郵件通知中顯示的寄件者名稱。
grafana_smtp_ehlo_identity	否	連線到SMTP伺服器時，EHLO命令中使用的識別碼。
grafana_starttls_policy	否	連線SMTP伺服器時使用STARTTLS的政策。 可能的參數值： • OpportunisticStartTLS—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器。 • MandatoryStartTLS—需要STARTTLS；如果SMTP伺服器不支援STARTTLS，則失敗。 • NoStartTLS—不使用STARTTLS；以不加密的方式連線到SMTP伺服器。 • empty—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器（預設值）。
grafana_smtp_enable_tracing	否	此參數指示是否啟用SMTP連線偵錯以偵錯電子郵件發送。 可能的參數值： • true—啟用SMTP連線偵錯。 • false—停用SMTP連線偵錯（預設值）。
autodeploy_plan	否	此參數指示是為Kaspersky EDR部署還是為Kaspersky NGFW部署KUMA服務。 可能的參數值： • edr—在 Kubernetes 叢集內為 OSMP 和 Kaspersky EDR 部署 KUMA 服務（預設值）。 • ngfw—在 Kubernetes 叢集內為 OSMP 和 Kaspersky NGFW 部署 KUMA 服務。此外，預先定義的收集器 **[OOTB] Kaspersky NGFW** 將安裝在 KUMA 清單檔案中 kuma_collector 參數指定的主機清單中的第一個主機上。 • none—不為 Kaspersky EDR 或 Kaspersky NGFW 部署 KUMA 服務。在未部署 Kaspersky EDR 和 Kaspersky NGFW 的 KUMA 服務情況下部署 Kaspersky Next XDR Expert，或從備份還原 Kaspersky Next XDR Expert 時，請指定此值。還原 Kaspersky Next XDR Expert 時，指定 edr 或 ngfw 可能會導致已部署的服務與備份副本中的服務發生衝突。
tokenhub_access_token	否	存取權杖的存留期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可用值為 5m，最大值為 2h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 您可以在應用程式部署後再變更 tokenhub_access_token 參數。
tokenhub_refresh_token	否	用於取得新存取權杖的重新整理權杖有效期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可用值為 12h，最大值為 4320h。 預設值是 24h。如果未在設定檔中指定此參數，則使用此值。 應用程式部署後，您可以再變更 tokenhub_refresh_token 參數。
credentials_session_ttl	否	單一登入工作階段的最大閒置時間。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可用值為 5m，最大值為 96h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 應用程式部署後，您可以再變更 credentials_session_ttl 參數。

在標準 Ubuntu Server 24.04 LTS 虛擬機器上進行跨資料中心多站台部署

本節說明如何在標準 Ubuntu Server 24.04 LTS 虛擬機器上部署跨資料中心多站台 Kaspersky Next XDR Expert。

❶ 三個主節點、九個工作節點和 HAProxy 的典型組態

在此部署中，會使用三個資料中心，每個資料中心各有一個主節點和三個工作節點。此部署總共需要三個主節點、九個工作節點和一個 HAProxy 節點。節點需求如下：

- 主節點：4個虛擬CPU，8 GB RAM，500 GB固態硬碟*
- 工作節點：10個虛擬CPU，20 GB RAM，1 TB固態硬碟*
- HAProxy 節點：4個虛擬CPU，8 GB RAM，100 GB固態硬碟*

*或任何隨機存取模式下具有8000IOPS（每秒輸入/輸出操作數）的裝置

> 硬體需求必須按照 Sizing Guide 進行計算。

❷ 設定 HAProxy 節點、主節點和工作節點

2.1 設定 HAProxy 主機

若要實作跨資料中心解決方案，主機必須分散在不同的子網路中，並使用來自各個子網路的三個 Kubernetes 叢集閘道，以及位於其中一個子網路中的 HAProxy 主機。

1. 安裝 HAProxy：

```
sudo apt update
sudo apt install haproxy
```

2. 編輯 HAProxy 組態檔：

```
sudo nano /etc/haproxy/haproxy.cfg
```

組態檔範例

```
global
  log /dev/log  local0
  log /dev/log  local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin
  stats timeout 30s
  user haproxy
  group haproxy
  daemon
defaults
  log  global
  mode  http
  option  httplog
  option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
  errorfile 400 /etc/haproxy/errors/400.http
  errorfile 403 /etc/haproxy/errors/403.http
  errorfile 408 /etc/haproxy/errors/408.http
  errorfile 500 /etc/haproxy/errors/500.http
  errorfile 502 /etc/haproxy/errors/502.http
  errorfile 503 /etc/haproxy/errors/503.http
  errorfile 504 /etc/haproxy/errors/504.http
listen stats
    mode http
    bind *:8080
    stats enable
    stats uri /stats
    stats refresh 10s
#    stats admin if LOCALHOST
frontend http
  mode tcp
  bind :80
  default_backend http_servers
backend http_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一個閘道 IP>:80 check inter 5s # ingress_ip number 1
  server proxmox2 <第二個閘道 IP>:80 check inter 5s # ingress_ip number 2
  server proxmox3 <第三個閘道 IP>:80 check inter 5s # ingress_ip number 3
frontend https
  mode tcp
  bind :443
  default_backend https_servers
backend https_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一個閘道 IP>:443 check inter 5s # ingress_ip number 1
  server proxmox2 <第二個閘道 IP>:443 check inter 5s # ingress_ip number 2
  server proxmox3 <第三個閘道 IP>:443 check inter 5s # ingress_ip number 3
frontend https9
  mode tcp
  bind :9443
  default_backend https9_servers
backend https9_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一個閘道 IP>:9443 check inter 5s  # ingress_ip number 1
```

```
    server proxmox2 <第二個閘道 IP>:9443 check inter 5s  # ingress_ip number 2
    server proxmox3 <第三個閘道 IP>:9443 check inter 5s # ingress_ip number 3
frontend https4
  mode tcp
  bind :4443
  default_backend https4_servers
backend https4_servers
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一個閘道 IP>:4443 check inter 5s # ingress_ip number 1
  server proxmox2 <第二個閘道 IP>:4443 check inter 5s # ingress_ip number 2
  server proxmox3 <第三個閘道 IP>:4443 check inter 5s # ingress_ip number 3
frontend ksc13000
  mode tcp
  bind :13000
  default_backend ksc13000
backend ksc13000
  mode tcp
  balance first
  option tcp-check
  timeout queue 2s
  timeout connect 2s
  timeout check 1s
  server proxmox1 <第一個閘道 IP>:13000 check inter 5s # ingress_ip number 1
  server proxmox2 <第二個閘道 IP>:13000 check inter 5s # ingress_ip number 2
  server proxmox3 <第三個閘道 IP>:13000 check inter 5s # ingress_ip number 3
```

3. 儲存（**Ctrl+S**），然後關閉檔案（**Ctrl+X**）。

4. 重新啟動 HAProxy 服務：

```
sudo systemctl restart haproxy
```

2.2 設定主要節點和工作節點

2.2.1 設定用於部署 Kaspersky Next XDR Expert 的使用者帳戶

1. 開啟/etc/sudoers：

```
sudo visudo
```

2. 在檔案末尾新增下列行：

```
{user} ALL=(ALL) NOPASSWD: ALL
```

其中，`{user}` 是用於部署的使用者帳戶。

3. 儲存（**Ctrl+S**），然後關閉檔案（**Ctrl+X**）。

2.2.2 檢查 /var、/opt 和 /tmp 目錄中的可用空間

1. 在主要節點上，執行下列命令：

```
df -h /var
```

至少需要200GB的可用空間。

```
df -h /opt
```

至少需要200GB的可用空間。

```
df -h /tmp
```

至少需要50GB的可用空間。

2. 在 worker1-worker3 節點上，執行下列命令：

```
df -h /var
```

至少需要200GB的可用空間。

```
df -h /opt
```

至少需要700GB的可用空間。

```
df -h /tmp
```

至少需要50GB的可用空間。

2.2.3 確保同步儲存區時沒有錯誤

執行以下命令：

```
sudo apt update
```

該命令不應傳回任何錯誤。

2.2.3 安裝 python3-apt 和 curl

執行以下命令：

```
sudo apt install python3-apt curl -y
```

2.2.4 設定系統時間與NTP伺服器同步

1. 執行以下指令：

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

輸出結果將包含以下行：

```
System clock synchronized: yes
```

2. 若要檢查同步情況，請執行：

```
date
```

輸出結果必須包含當前日期和時間。

❸ 設定DBMS主機

DBMS主機是安裝了DBMS實例的主機。

安裝 DBMS實例的目標主機需求：

- 10個虛擬CPU
- 20 GB RAM
- 1.6 TB 的固態硬碟或任何隨機存取速度達到8000 IOPS（每秒輸入/輸出操作數）的裝置

如需瞭解支援的 PostgreSQL 版本，請參閱硬體和軟體需求一文。

3.1 安裝和設定PostgreSQL

1. 安裝PostgreSQL：

```
sudo apt install -y postgresql-<版本>
```

其中，<版本> 為PostgreSQL版本。

如果連線的儲存庫中無法取得所需的 PostgreSQL 版本，您必須新增 `postgresql` 儲存庫。如需相關指示，請參閱 PostgreSQL 網站。

2. 建立一個獨立的PostgreSQL超級使用者：

```
sudo -u postgres createuser --superuser xdr
```

3. 為使用者設定密碼：

```
sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD '您的密碼';"
```

4. 建立一個與使用者同名的資料庫：

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. 允許任何IP位址存取PostgreSQL：

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/<版本>/main/pg_hba.conf
```

其中，<版本> 為PostgreSQL版本。

6. 在 PostgreSQL 組態檔（ /etc/postgresql/<版本>/main/postgresql.conf ）中編輯以下參數，其中 <版本> 為 PostgreSQL 版本。例如，對於 PostgreSQL 16：/etc/postgresql/16/main/postgresql.conf。

已註解（ # ）的行需要取消註解。

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. 重新啟動PostgreSQL

```
sudo systemctl restart postgresql
```

3.2 設定系統時間與NTP伺服器同步：

1. 執行以下指令：

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

輸出結果將包含以下行：

```
System clock synchronized: yes
```

2. 若要檢查同步情況，請執行：

```
date
```

輸出結果必須包含當前日期和時間。

4 設定管理員主機

管理員主機是執行KDT公用程式的主機。發佈套件中的檔案（包括含有 KDT 公用程式的壓縮檔案）必須位於管理員主機上。該主機可能是KDT公用工具在部署期間建立的Kubernetes叢集的一部分，也可能位於叢集之外。如果管理員主機不包含在叢集內，它將僅用於部署和管理Kubernetes叢集和OSMP。如果管理主機包含在叢集內，則它也可以作為執行OSMP元件的目標主機。

4.1 解壓縮 KDT 公用程式

執行下列指令以建立目錄並解壓縮 KDT 公用程式：

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

4.2 安裝Docker

支援25及更高版本。

4.2.1 安裝在 Ubuntu 24 上：

```
sudo apt update && sudo apt install docker.io
```

4.2.2 **或** *依照官方說明進行安裝：*

1. 安裝所需軟體套件：

   ```
   sudo apt update && sudo apt install ca-certificates curl
   ```

2. 下載Docker金鑰環：

   ```
   sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc && sudo chmod 0755
   /etc/apt/keyrings/docker.asc
   ```

3. 新增Docker apt儲存庫：

   ```
   sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
   Types: deb
   URIs: https://download.docker.com/linux/ubuntu
   Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
   Components: stable
   Architectures: $(dpkg --print-architecture)
   Signed-By: /etc/apt/keyrings/docker.asc
   EOF
   ```

4. 更新儲存庫快取並安裝Docker軟體套件：

   ```
   sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
   plugin
   ```

4.3 設定Docker

1. 將目前使用者新增至 docker 群組：

```
sudo usermod -aG docker $USER
```

2. 在目前工作階段中啟用使用者的 docker 群組成員資格：

```
newgrp docker
```

4.4 設定系統時間與NTP伺服器同步：

1. 執行以下指令：

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

輸出結果將包含以下行：

```
System clock synchronized: yes
```

2. 若要檢查同步情況，請執行：

```
date
```

輸出結果必須包含當前日期和時間。

4.5 檢查/tmp目錄中的可用空間

執行以下命令：

```
df -h /tmp
```

至少需要50GB的可用空間。

如果/tmp目錄中沒有足夠的可用空間，請指定另一個目錄的路徑：

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

或分配所需的可用空間：

```
echo 'tmpfs /tmp tmpfs defaults,size=50G 0 0' | sudo tee -a /etc/fstab
```

分配所需空間後，重新啟動主機或重新掛載分割區。

4.6 設定管理者主機與主節點和工作節點之間的 SSH 連線

1. 建立SSH金鑰：

```
ssh-keygen -t rsa -b 4096 -N ""
```

2. 將密鑰逐一複製到每個目標主機：

```
ssh-copy-id {user}@{primary_ip}
ssh-copy-id {user}@{worker_ip}  # copy the key to each worker node in a subnet
```

其中 `{user}` 是在目標主機設定期間建立、用於部署 Kaspersky Next XDR Expert 的使用者帳戶。

4.7 DNS組態

在您的 DNS 伺服器上，註冊要連線到 OSMP 服務的服務的 FQDN（`<smp_domain>`）。

若要快速開始，請在您的 DNS 伺服器中新增一筆指向 HAProxy IP 位址的萬用字元 A 記錄。HAProxy 會在三個 Kubernetes 叢集閘道（`<ingress_ip>`）之間平衡流量，然後這些閘道會將流量路由到適當的服務。

預設情況下，OSMP服務可透過以下位址存取：

```
<haproxy_host_ip> - admsrv.<smp_domain>
<haproxy_host_ip> - api.<smp_domain>
<haproxy_host_ip> - console.<smp_domain>
<haproxy_host_ip> - kuma.<smp_domain>
<haproxy_host_ip> - *.kuma.<smp_domain>
<haproxy_host_ip> - monitoring.<smp_domain>
<haproxy_host_ip> - agentserver.<smp_domain>
<haproxy_host_ip> - updater.<smp_domain>
```

4.8 建立用於運行安裝程式的組態

顯示圖例

- `10.0.0.100`—第一個子網路中第一個主要節點的 IP 位址 (`<primary1_ip>`)
- `10.10.20.18`—第二個子網路中第二個主要節點的 IP 位址 (`<primary2_ip>`)
- `10.65.20.10`—第三個子網路中第三個主要節點的 IP 位址 (`<primary3_ip>`)
- `10.0.0.101`—第一個子網路中第一個工作節點的 IP 位址 (`<worker1_ip>`)
- `10.0.0.102`—第一個子網路中第二個工作節點的 IP 位址 (`<worker2_ip>`)
- `10.0.0.103`—第一個子網路中第三個工作節點的 IP 位址 (`<worker3_ip>`)
- `10.10.20.20`—第二個子網路中第一個工作節點的 IP 位址 (`<worker4_ip>`)
- `10.10.20.21`—第二個子網路中第二個工作節點的 IP 位址 (`<worker5_ip>`)
- `10.10.20.22`—第二個子網路中第三個工作節點的 IP 位址 (`<worker6ip>`)
- `10.65.20.11`—第三個子網路中第一個工作節點的 IP 位址 (`<worker7_ip>`)

- `10.65.20.12`—第三個子網路中第二個工作節點的 IP 位址 (`<worker8_ip>`)
- `10.65.20.13`—第三個子網路中第三個工作節點的 IP 位址 (`<worker9_ip>`)
- `10.0.0.150`—DBMS 主機的 IP 位址 (`<DB_ip>`)
- `10.0.0.200`—第一個 Kubernetes 叢集閘道的 IP 位址
- `10.10.20.100`—第二個 Kubernetes 叢集閘道的 IP 位址
- `10.65.20.100`—第三個 Kubernetes 叢集閘道的 IP 位址
- `10.0.0.111`—HAProxy 主機的 IP 位址
- `user`—部署的使用者帳戶 (`<user_name>`)
- `/home/user/.ssh/id_rsa`—在管理員主機上設定 SSH 連線期間建立的 SSH 金鑰路徑 (`<ssh_key_path>`)
- `xdr.mydomain.com`—Ingress 的網域 (`<smp_domain>`)

4.8.1 使用組態檔指定安裝參數

組態檔的範本（multinode.smp_param.yaml.template）位於KDT公用程式檔案中的分發套件中。

`psql_dsn` 參數值必須符合 URI 格式。若連線 URI 的任一部分包含具有特殊意義的符號，則必須以百分比編碼進行編碼。

`psql_dsn` 參數值中必須替換的符號：

- 空白字元 → `%20`
- ! → `%21`
- # → `%23`
- % → `%25`
- & → `%26`
- / → `%2F`
- : → `%3A`
- = → `%3D`
- ? → `%3F`
- @ → `%40`
- [→ `%5B`
-] → `%5D`

請參閱PostgreSQL 連線字串文章以取得詳細資訊。

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
regions:
    prox1:
        description: Proxmox1
    prox2:
        description: Proxmox2
    prox3:
        description: Proxmox3
zones:
    proxmox1:
        region: prox1
        ingress_ip: 10.0.0.200
    proxmox2:
        region: prox2
        ingress_ip: 10.10.20.100
    proxmox3:
```

```
        region: prox3
        ingress_ip: 10.65.20.100
nodes:
  - desc: cdt-primary1
    type: primary
    zone: proxmox1
    host: 10.0.0.100
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary2
    type: primary
    zone: proxmox2
    host: 10.10.20.18
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-primary3
    type: primary
    zone: proxmox3
    host: 10.65.20.100
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w1
    type: worker
    zone: proxmox1
    host: 10.0.0.101
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w2
    type: worker
    zone: proxmox1
    host: 10.0.0.102
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w3
    type: worker
    zone: proxmox1
    host: 10.0.0.103
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w4
    type: worker
    zone: proxmox2
    host: 10.10.20.20
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w5
    type: worker
    zone: proxmox2
    host: 10.10.20.21
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w6
    type: worker
    zone: proxmox2
    host: 10.10.20.22
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w7
    type: worker
    zone: proxmox3
    host: 10.65.20.11
    access:
      ssh:
        user: <user_name>
```

```
        key: <ssh_key_path>
  - desc: cdt-w8
    type: worker
    zone: proxmox3
    host: 10.65.20.12
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
  - desc: cdt-w9
    type: worker
    zone: proxmox3
    host: 10.65.20.13
    access:
      ssh:
        user: <user_name>
        key: <ssh_key_path>
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<your_password>@<DB_ip>:5432
  - name: ssh_pk
    source:
      path: <ssh_key_path>
  - name: admin_password
    source:
      value: "your_password"
  - name: inventory
    source:
      value: /dev/null
  - name: license
    source:
      value: /dev/null
  - name: smp_domain
    source:
      value: "<domain_smp>"
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr
  - name: grafana_admin_password
    source:
      value: "your_password"
```

5 安裝 Kaspersky Next XDR Expert

執行以下命令：

```
./kdt/bin/kdt apply --accept-eula -k xdr-<program_version>.tar -i params.yaml
```

如果安裝成功，終端將顯示以下資訊：

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<ver>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

若要檢查安裝情況，您需要前往授權頁面。為此，請在瀏覽器的搜尋欄中輸入以下內容：

```
console.<smp_domain>
```

其中 `<smp_domain>` 是此程序步驟 4.7 中的 FQDN。

Kaspersky Next XDR Expert的維護

本章節介紹如何使用KDT更新、刪除和重新安裝Kaspersky Next XDR Expert元件。此外，本章節還提供了有關如何停止Kubernetes叢集節點、自訂Kaspersky Next XDR Expert公共服務的自訂憑證、取得目前版本的組態檔以及使用KDT對Kaspersky Next XDR Expert元件執行其他操作的說明。

更新Kaspersky Next XDR Expert元件

KDT可讓您更新Kaspersky Next XDR Expert元件（包含管理網頁外掛程式）和Bootstrap元件。Kaspersky Next XDR Expert元件的新版本包含在分發套件中。

不支援安裝早期版本的元件。

若要更新Kaspersky Next XDR Expert元件：

1. 下載包含新版本Kaspersky Next XDR Expert元件的分發套件。
2. 如有必要，請在管理員主機上匯出目前版本的組態檔。

   如果沒有新增或修改安裝參數，則無需匯出設定檔。
3. 更新Kaspersky Next XDR Expert元件和Bootstrap。

   指定Kaspersky Next XDR Expert元件的傳輸存檔路徑以及組態檔路徑。如果在Bootstrap更新命令中指定了組態檔路徑，或未新增或修改安裝參數，則組態檔路徑是可選的：

   - 執行以下命令對Kaspersky Next XDR Expert元件進行標準更新：

     `./kdt apply -k <XDR 更新存檔的完整路徑> -i <組態檔的完整路徑>`

   - 若安裝的 Kaspersky Next XDR Expert 元件版本與分發套件中的元件版本相符，則略過該元件的更新。執行以下命令，透過 `force` 旗標強制更新此元件：

     `./kdt apply --force -k <XDR 更新存檔的完整路徑> -i <組態檔的完整路徑>`
4. 如果出現新版本的EULA和隱私權政策，請參閱Kaspersky Next XDR Expert元件的最終使用者產品授權協議（EULA）和隱私權政策。文字顯示在命令行視窗中。按空格鍵檢視下一個文字段。然後，當出現提示時，輸入以下值：

   a. 如果您瞭解並接受 EULA 的條款，請輸入 `y`。

      如果您不接受 EULA 的條款，請輸入 `n`。若要使用 Kaspersky Next XDR Expert 元件，您必須接受 EULA 的條款。

b. 若您瞭解並接受「隱私權政策」的條款，並且同意您的資料將依照「隱私權政策」所述進行處理和傳輸（包括傳輸到第三國），請輸入 y。

如果您不接受「隱私權政策」的條款，請輸入 n。

若要使用Kaspersky Next XDR Expert元件，您必須接受EULA和隱私權政策的條款。

在您接受EULA和隱私權政策後，KDT將更新Kaspersky Next XDR Expert元件。

更新後，您可閱讀 Kaspersky Next XDR Expert 元件的 EULA 與「隱私權政策」。這些檔案位於執行 Kaspersky Next XDR Expert 部署之使用者的 `~/kaspersky_eula` 目錄中。

檢查Kaspersky Next XDR Expert元件的完整性

部署Kaspersky Next XDR Expert後，您可以檢查解決方案元件的真實性和完整性。傳輸歸檔中的每個元件（CNAB）都包含一個XML格式的清單檔案。此清單檔案包含元件核對總和，並使用GOST R 34.11-2012的256位元演算法進行數位簽章。此數位簽章既確保元件檔案核對總和的有效性，也確保清單中的核對總和未被變更。

您可以驗證元件的核對總和是否與清單檔案中指定的核對總和相符。這確認組件未被修改，並且來自可信任來源。

檢查Kubernetes叢集中已安裝的Kaspersky Next XDR Expert元件完整性

若要對已安裝的Kaspersky Next XDR Expert元件執行完整性檢查：

1. 請執行以下命令，將Kaspersky Next XDR Expert元件及其清單檔案從已部署的解決方案中提取到指定目錄。僅從解決方案中提取位於傳輸存檔中的元件：

```
./kdt extract --reference <path to transport archive> -d <path to extracted cnabs>
```

其中：

- `<path to transport archive>` — 傳輸壓縮檔案的路徑
- `<path to extracted cnabs>` — 解決方案元件及其清單檔案將提取到的目錄路徑

2. 從包含已提取元件及其清單檔案的目錄中執行以下命令。`integrity_checker`公用程式會將從已部署的解決方案中提取的元件核對總和，與從傳輸壓縮檔案中提取的清單檔案內的核對總和進行比較：

```
find . -type f -iname "*.xml" -print0 | xargs -0 -I {} echo --manifest {} | xargs ./integrity_checker --
signature-purpose 1.3.6.1.4.1.23668.1800.1.1.15 --signature-type kds-with-filename
```

完整性檢查成功後的命令輸出範例

成功透過驗證的清單檔案數量顯示在`Manifests`行的`succeeded`欄中。

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 0 / 0 / 38
        Files: 0 / 0 / 38
```

```
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
================================================>
SUCCEEDED
```

完整性檢查失敗後的命令輸出範例

在本例中，清單檔案在簽名後被修改，或簽名有問題。跳過的清單檔案或驗證失敗的清單檔案數量顯示在 `Manifests` 行的 `failed` 直欄中。

```
================================================>
Summary( failed / skipped / succeeded ):
        Manifests: 2 / 0 / 36
        Files: 0 / 0 / 0
        Directories: 0 / 0 / 0
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
================================================>
FAILED
ERR 無法驗證檔案「/home/xdr_user/integrity_check.xml」的數位簽章。 標誌：無：0x80000106（物件不受信任）
清單檔案 /home/xdr_user/integrity_check.xml 驗證失敗。原因：無法驗證檔案「/home/xdr_user/integrity_check.xml」的數位簽章。 標誌：無：0x80000106（物件不受信任）
```

驗證了安裝在Kubernetes叢集中的Kaspersky Next XDR Expert元件的完整性。如果叢集內部也安裝了KUMA服務，則也會驗證其完整性。

您也可以檢查安裝在Kubernetes叢集外部的KUMA服務的完整性。

無需重新安裝即可變更Kaspersky Next XDR Expert的參數

若組織的基礎架構已變更，則 Kaspersky Next XDR Expert 可能需要快速變更主要參數值，無需重新安裝解決方案。Kaspersky Next XDR Expert 支援透過 KDT 變更 Kubernetes 叢集 IP 位址（`ingress_ip` 參數）及服務的 FQDN（特別是變更服務網域名稱，即 `smp_domain` 參數）。

若要變更參數值且無需重新安裝Kaspersky Next XDR Expert：

1. 在管理員主機上，匯出目前的組態檔。
2. 在匯出的組態檔中，變更 `smp_domain` 或 `ingress_ip` 參數值。您可以同時變更這兩個參數，也可以分別變更其中任一參數。

   如果您跨多個資料中心部署 Kaspersky Next XDR Expert，請變更組態檔中 `zones` 區段內的 `ingress_ip` 參數值。
3. 使用下列命令套用參數變更：

```
./kdt apply -i '<full_path_to_updated_configuration_file>'
```

`smp_domain` 和 `ingress_ip` 設定的值已變更。Kaspersky Next XDR Expert 使用新設定。

`smp_domain` 參數值變更時，FQDN 服務名稱也會變更。因此，KDT 將重新核發所有憑證，使用 Kaspersky Next XDR Expert 公開服務需要這些憑證。

新增和刪除Kubernetes叢集的主節點和工作線程節點

如果需要擴充Kubernetes叢集以符合目前工作負載、提高其容錯能力或最佳化運算資源，可以使用KDT新增或刪除叢集包含的主節點和工作線程節點。

僅當Kaspersky Next XDR Expert部署在多個節點上時，才能新增或刪除主節點和工作線程節點。

為Kubernetes叢集新增主節點和工作線程節點

若要新增主節點和工作線程節點：

1. 準備將充當主節點和工作線程節點的目標主機。
2. 在管理員主機上，使用以下命令匯出目前的組態檔：

   ```
   ./kdt ec -e '<configuration_file_name_with_path>'
   ```

   目前版本的組態檔將以指定名稱儲存到指定目錄。
3. 請於匯出的組態檔的 `nodes` 區段中，新增一或多個新節點的參數（`desc`、`type`、`host`、`kind`、`user` 與 `key`），隨後儲存該組態檔。
4. 使用 ssh-copy-id 公用程式將公開金鑰複製至每個新節點（例如，複製至 `~/.ssh` 目錄）。
5. 在管理員主機上，執行以下命令將修改後的組態檔套用到Kubernetes叢集。在命令中，指定此組態檔的完整路徑：

   ```
   ./kdt apply -i '< 設定檔的完整路徑 >'
   ```

   啟動命令後，KDT會檢查組態檔是否填寫正確。隨後KDT會檢查Kubernetes叢集節點的硬體、軟體及網路設定是否符合安裝解決方案的先決條件。若所有嚴格預檢查皆成功完成，KDT會輸出驗證成功通知至stdout與 KDT日誌。否則，系統將儲存包含驗證失敗資訊的日誌，並中止新增主機的進程。若需要，您可以略過執行命令前的預檢查（將 `ignore_precheck` 安裝參數設定為 `true`）。

新的主節點和工作線程節點隨即新增至Kubernetes叢集。KDT將新增主節點和工作線程節點的資訊輸出到stdout和KDT日誌。

從Kubernetes叢集刪除主節點和工作線程節點

刪除節點時，請注意叢集主節點的最小數量為1，工作節點的最小數量為3。如果刪除時少於一個主節點和三個工作線程節點，操作將中斷。您可以在匯出後獲得的組態檔中檢視主節點數和工作線程節點數。

若要刪除主節點和工作線程節點：

1. 在管理員主機上，使用以下命令匯出目前的組態檔：

   ```
   ./kdt ec -e '<configuration_file_name_with_path>'
   ```

   目前版本的組態檔將以指定名稱儲存到指定目錄。

2. 請在匯出的組態檔的nodes區段中，刪除一或多個主節點和工作線程節點的參數（ desc 、 type 、 host 、 kind 、 user和key ），然後儲存組態檔。

   確保刪除節點後，叢集中至少還剩下一個主節點和三個工作線程節點。多節點部署的最小叢集組態包括四個節點（一個主要節點和三個工作線程節點）。如果此條件不滿足，則刪除進程將中斷。

   您也可以刪除帶有kind=admsrv的節點，前提是該節點不是叢集中僅存的帶有kind=admsrv的節點。若嘗試從叢集中刪除該節點，刪除過程中會略過該節點。

3. 在管理員主機上，執行以下命令將修改後的組態檔套用到Kubernetes叢集。在命令中，指定此組態檔的完整路徑：

   ```
   ./kdt apply -i '< 設定檔的完整路徑 >'
   ```

指定的節點隨即刪除。KDT將有關已刪除的主節點和工作線程節點的資訊輸出到stdout和KDT日誌。

對組態檔進行版本管理。

使用 Kaspersky Next XDR Expert 時，您可能需要變更於 Kaspersky Next XDR Expert 部署前在設定檔中指定的參數。例如，當變更用於儲存管理伺服器資料的磁碟空間時，`ksc_state_size` 參數會被修改。包含已修改 `ksc_state_size` 參數的組態檔目前版本，已在 Kubernetes 叢集中更新。

如果您嘗試在需要組態檔的KDT自定義操作中使用先前版本的組態檔，則會發生衝突。為避免衝突，您必須僅使用從Kubernetes叢集匯出的目前版本的組態檔。

若要匯出目前版本的組態檔，

在安裝了KDT公用程式的管理員主機上，執行下列自訂操作，然後指定組態檔的路徑及其名稱：

```
./kdt ec -e <configuration_file_name_with_path>
```

目前版本的組態檔將以指定名稱儲存到指定目錄。

例如，在更新 Kaspersky Next XDR Expert 元件或為卡巴斯基應用程式新增管理外掛程式時，您可以使用匯出的組態檔。

如果沒有新增或修改安裝參數，則無需匯出設定檔。

解除安裝Kaspersky Next XDR Expert

KDT可讓您解除安裝Kubernetes叢集中安裝的所有Kaspersky Next XDR Expert元件、叢集本身、叢集外安裝的KUMA服務以及在解決方案部署或執行期間建立的其他工件。

若要解除安裝Kaspersky Next XDR Expert元件和相關資料：

1. 在管理員主機上，執行下列命令：

`./kdt remove --all`

此命令將刪除下列物件和工件：

- Kubernetes叢集中安裝的所有Kaspersky Next XDR Expert元件和叢集本身。
- KDT在部署期間建立的Kaspersky Next XDR Expert使用者帳戶。
- 位於單獨伺服器或叢集內部的資料庫、DBMS方案和KDT在部署期間建立的DBMS帳戶。
- 在清查檔案指定的主機上，叢集外安裝的KUMA服務。
- 目標主機上以下目錄的內容：
  - `/var/spool/ksc/logs`
  - `/var/spool/ksc/backup`
  - `/var/spool/ksc/`
  - `/var/lib/k0s`
  - `/run/k0s`
  - `/etc/k0s/`
  - `/etc/containerd/`
  - `/var/lib/containerd/`
  - `/run/containerd/`
- Kaspersky Next XDR Expert元件安裝和運行期間所取得的日誌。
- 管理員主機上與Kaspersky Next XDR Expert元件相關的資料。

如果管理員主機無法存取目標主機的網絡，則解除安裝元件會中斷。您可以恢復網路存取並重新開始解除安裝Kaspersky Next XDR Expert。或者，您可以手動從目標主機解除安裝卡巴斯基Next XDR Expert 元件。

> 如果您使用依上下文管理的多個Kubernetes叢集，則此命令僅刪除目前Kubernetes上下文、相應的叢集以及叢集中安裝的Kaspersky Next XDR Expert元件。不會刪除其他上下文及其包含Kaspersky Next XDR Expert實例的叢集。

2. 如有需要，請關閉Kaspersky Next XDR Expert在部署期間開啟的使用的連接埠。這些連接埠不會自動關閉。
3. 如果需要，請刪除在部署期間自動安裝的作業系統套件。這些套件不會自動刪除。
4. 移除 KDT 以及 `~/kaspersky_eula` 和 `~/.kdt` 目錄的內容。

Kaspersky Next XDR Expert元件、資料庫和相關資料將被刪除，並且Kaspersky Next XDR Expert所使用的連接埠將會關閉。

安裝在受管理裝置上的卡巴斯基應用程式不會透過 `./kdt remove` 命令移除。有關如何移除卡巴斯基應用程式的資訊，請參閱相應的說明文件。

解除安裝Kaspersky Next XDR Expert後，目標主機不會自動重新啟動。如有需要，您可以手動重新啟動這些主機。

手動取消安裝Kaspersky Next XDR Expert元件

如果管理員主機沒有對目標主機的網路存取權限，則使用KDT解除安裝Kaspersky Next XDR Expert元件會中斷。您可以恢復網路存取權限並重新開始移除該解決方案。或者，您可以手動從目標主機解除安裝Kaspersky Next XDR Expert元件。

若要手動從目標主機解除安裝Kaspersky Next XDR Expert元件：

1. 在目標主機上，執行以下指令來停止k0s服務：

   ```
   /usr/local/bin/k0s stop
   ```

2. 執行以下命令將叢集節點重設為初始狀態：

   ```
   /usr/local/bin/k0s reset
   ```

3. 刪除以下目錄中的所有內容：

   - 所需目錄：
     - `/etc/k0s/`
     - `/var/lib/k0s/`
     - `/usr/libexec/k0s/`
     - `/usr/local/bin/`（僅移除 `k0s` 檔案）
   - 可選目錄：
     - `/var/lib/containerd/`
     - `/var/cache/k0s/`
     - `/var/cache/kubelet/`
     - `/var/cache/containerd/`

     如果 containerd 服務僅供 Kaspersky Next XDR Expert 的功能使用，您可以刪除 `/var/lib/containerd/` 和 `/var/cache/containerd/` 目錄。否則，`/var/lib/containerd/` 和 `/var/cache/containerd/` 目錄中包含的資料可能會遺失。

     重新啟動目標主機後，`/var/cache/k0s/`、`/var/cache/kubelet/` 和 `/var/cache/containerd/` 目錄的內容會自動刪除。您不必手動清除這些資料夾。

4. 重新啟動所有目標主機。

Kaspersky Next XDR Expert元件隨即從目標主機中刪除。

安裝失敗後重新安裝Kaspersky Next XDR Expert

如果Kaspersky Next XDR Expert安裝失敗，您可以重新啟動安裝程式。在安裝Bootstrap或Kaspersky Next XDR Expert元件期間，可能會出現安裝失敗。重新安裝Kaspersky Next XDR Expert所需的步驟取決於出現安裝錯誤時Kubernetes叢集是否已部署。

若要確定安裝失敗的階段，

執行以下命令來檢視所有已安裝的Kaspersky Next XDR Expert元件清單：

```
./kdt state
```

如果出現Bootstrap安裝錯誤，KDT將顯示Bootstrap未安裝的訊息。在這種情況下，您必須手動解除安裝部署期間建立的目錄。

如果 Bootstrap 安裝成功，其會在命令輸出中顯示為 `Success` 狀態。這表示發生 Kaspersky Next XDR Expert 元件安裝錯誤。此種情況下，您必須重新安裝未正確安裝的元件或重新安裝整個解決方案。在命令輸出中，此類元件會顯示為 `Failed` 狀態。

如果未安裝Bootstrap，則重新安裝Kaspersky Next XDR Expert。

若要重新啟動Kaspersky Next XDR Expert元件：

1. 轉至包含KDT公用程式的目錄，然後檢視Bootstrap元件的安裝日誌。

   如果在Bootstrap安裝階段出現錯誤，日誌中將會有記錄。在這種情況下，Bootstrap尚未安裝，Kubernetes叢集也尚未建立。

   執行 `/.kdt/kdt-{date}.log | grep -iE "connect|auth|ident|password"` 命令，以尋找與最常見安裝問題相關的記錄項目：

   - 資料庫連線設定
   - 管理員密碼格式
   - 硬體資源不足
   - 連線至節點時發生授權問題

2. 請手動解除安裝部署期間建立的目錄。

   a. 在管理員主機上，前往 `.kdt` 目錄，然後移除 `cluster.config` 檔案。

   b. 刪除以下目錄中的所有內容：

- 所需目錄：
  - `/etc/k0s/`
  - `/var/lib/k0s/`
  - `/usr/libexec/k0s/`
  - `/usr/local/bin/`（僅移除 `k0s` 檔案）
- 可選目錄：
  - `/var/lib/containerd/`
  - `/var/cache/k0s/`
  - `/var/cache/kubelet/`
  - `/var/cache/containerd/`

  如果 containerd 服務僅供 Kaspersky Next XDR Expert 的功能使用，您可以刪除 `/var/lib/containerd/` 和 `/var/cache/containerd/` 目錄。否則，`/var/lib/containerd/` 和 `/var/cache/containerd/` 目錄中包含的資料可能會遺失。

  重新啟動目標主機後，`/var/cache/k0s/`、`/var/cache/kubelet/` 和 `/var/cache/containerd/` 目錄的內容會自動刪除。您不必手動清除這些資料夾。

c. 重新啟動所有目標主機。

3. 重新啟動Kaspersky Next XDR Expert的安裝程式。

如果Bootstrap已安裝，請重新安裝Kaspersky Next XDR Expert

若要重新安裝錯誤安裝的Kaspersky Next XDR Expert元件：

1. 使用下列命令來檢視錯誤安裝的Kaspersky Next XDR Expert元件的完整安裝日誌：

   `./kdt state -l <component_name>`

   您也可以使用下列命令來輸出Kaspersky Next XDR Expert元件的所有診斷資訊：

   `./kdt logs get --to-archive`

2. 自行或在卡巴斯基技術支援的協助下排查安裝錯誤。
3. 重新安裝錯誤安裝的KasperskyNext XDR Expert元件。
   - 如果您沒有修改組態檔，請執行下列命令，然後指定與Kaspersky Next XDR Expert安裝程式時所使用的相同的傳輸封存檔案：

     `./kdt apply -k <full_path_to_transport_archive>`
   - 若要更改安裝參數，請匯出組態檔，對其進行修改，然後使用傳輸存檔和更新的組態檔執行以下命令：

     `./kdt apply -k <full_path_to_transport_archive> -i <full_path_to_configuration_file>`

KDT僅重新安裝錯誤的Kaspersky Next XDR Expert元件。

4. 使用以下命令來重新啟動Kaspersky Next XDR Expert的安裝程式：

   `./kdt apply --force -k <XDR 更新存檔的完整路徑> -i <組態檔的完整路徑>`

如果重新安裝元件後仍無法解決安裝錯誤，您可以解除安裝整個解決方案。

若要重新啟動Kaspersky Next XDR Expert的安裝程式：

1. 使用以下命令來輸出有關Kaspersky Next XDR Expert元件的所有診斷資訊：

   `./kdt logs get --to-archive`

2. 自行或在卡巴斯基技術支援的協助下排查安裝錯誤。

3. 解除安裝Kaspersky Next XDR Expert。在管理員主機上，執行下列命令：

   `./kdt remove --all`

4. 使用以下命令來重新啟動Kaspersky Next XDR Expert的安裝程式：

   `./kdt apply --force -k <XDR 更新存檔的完整路徑> -i <組態檔的完整路徑>`

重新安裝Kaspersky Next XDR Expert元件

在管理員主機上安裝Kaspersky Next XDR Expert期間，KDT會顯示安裝日誌，以顯示Kaspersky Next XDR Expert元件是否已正確安裝。

安裝Kaspersky Next XDR Expert後，您可以執行下列命令來檢視所有已安裝元件的清單：

```
./kdt state
```

系統會顯示已安裝的元件清單。正確安裝的元件會顯示 `Success` 狀態。若元件安裝失敗，此元件會顯示 `Failed` 狀態。

若要檢視卡巴斯基 Next XDR Expert元件安裝不正確的完整安裝日誌，請執行下列命令：

```
./kdt state -l <component_name>
```

您也可以使用下列命令來輸出有關Kaspersky Next XDR Expert元件的所有診斷資訊：

```
./kdt logs get --to-archive
```

您可以利用取得的日誌自行或在卡巴斯基技術支援的協助下進行錯誤排查。

若要重新安裝錯誤安裝的Kaspersky Next XDR Expert元件：

- 如果您沒有修改組態檔，請執行下列命令，然後指定與Kaspersky Next XDR Expert安裝程式時所使用的相同的傳輸封存檔案：

  `./kdt apply -k <full_path_to_transport_archive>`

- 若要更改安裝參數，請匯出組態檔，對其進行修改，然後使用傳輸存檔和更新的組態檔執行以下命令：

  `./kdt apply -k <full_path_to_transport_archive> -i <full_path_to_configuration_file>`

KDT僅重新安裝錯誤的Kaspersky Next XDR Expert元件。

Kaspersky Next XDR Expert資料的備份複製和還原

資料備份可讓您儲存Kaspersky Next XDR Expert資料的完整副本。在備份過程中，Kaspersky Next XDR Expert元件的運作會暫時中止，以確保資料一致性。備份建立完成後，會將其儲存在單獨伺服器的網路資料夾中，然後解決方案即可恢復運作。您可以手動建立備份，也可以依照指定的排程建立備份。

依照此方案，您可以設定備份儲存、設定排程備份或手動建立備份、管理備份，並從備份中還原Kaspersky Next XDR Expert資料。

限制：

- 在備份過程中，Kaspersky Next XDR Expert元件的運作會暫時中止，以確保資料一致性。
- 備份包含所有Kaspersky Next XDR Expert資料。不支援建立單一元件的備份或還原其資料。
- 從備份中還原Kaspersky Next XDR Expert資料時，必須使用與建立備份時相同版本的Kaspersky Next XDR Expert。
- 僅當DBMS未包含在Kubernetes叢集中時，才支援備份和還原Kaspersky Next XDR Expert資料。將DBMS安裝到 Kubernetes叢集的組態僅用於熟悉解決方案，不用於解決標準工作任務。
- 備份所需的可用空間不會自動檢查。您必須確保網路資料夾中有足夠的可用空間。

階段

Kaspersky Next XDR Expert資料的備份複製和還原分階段進行：

1. **設定備份儲存**

   指定用於儲存備份的網路資料夾路徑。此網路資料夾必須位於單獨的伺服器上，並且必須能夠透過CIFS或NFS協定從Kubernetes叢集存取。

   為避免網路資料夾過載，可儲存於網路資料夾中的備份數量設有上限。預設最多可以建立10個備份。您可在手動建立備份或設定備份排程時，使用`backup_retain`參數來設定備份數量上限。若網路資料夾已包含最大數量的備份檔案，則下一個備份將覆寫最早的備份。

   由於網路資料夾中的可用空間不會自動檢查，我們建議您定期監控此資料夾中的可用空間，以防止備份失敗。

2. **建立Kaspersky Next XDR Expert資料的備份副本**

   您可以使用下列方法之一建立備份：

   - 排程備份

     若要依排程建立備份，則必須使用KDT設定排程。您只能指定一個備份排程。建立新排程將覆蓋現有排程。此外，您可以查看目前排程，並暫停或恢復自動備份。

     在使用自動排程備份之前，我們建議您手動建立備份，以確保用於儲存備份的網路資料夾設定正確且可存取。

   - 手動備份

     如果您需要在不等待下一次自動備份的情況下儲存備份，則可以建立手動備份。

備份將保存到指定的網路資料夾。您可以檢視可用備份清單以及每個備份的詳情。

KDT日誌提供有關備份操作結果的詳情，包括備份成功或失敗、執行日期和時間以及備份副本的名稱和位置。

3. **從備份副本還原Kaspersky Next XDR Expert資料**

   還原備份副本，將Kaspersky Next XDR Expert回滾到已儲存的狀態。

設定Kaspersky Next XDR Expert備份副本的儲存

所有建立的備份都儲存在單獨伺服器上的網路資料夾中。此資料夾必須可透過CIFS或NFS協定從Kubernetes叢集存取。

備份所需的可用空間不會自動檢查。您必須確保網路資源上有足夠的可用空間。

為避免網路資料夾過載，可儲存於網路資料夾中的備份數量設有上限。預設最多可以建立10個備份。您可在手動建立備份或設定備份排程時，使用`backup_retain`參數來設定備份數量上限。若網路資料夾已包含最大數量的備份檔案，則下一個備份將覆寫最早的備份。

指定備份儲存的網路資料夾路徑

若要指定可透過CIFS/SMB協定存取的備份儲存路徑，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a setBackupStore \
  --param backup_target_url="cifs://<主機>/<路徑>" \
  --param cifs_username="<使用者名稱>" \
  --param cifs_password="<密碼>"
```

其中：

- < 主機 > 是網路儲存伺服器的位址。
- < 路徑 > 是備份網路資料夾的路徑。
- < 使用者名稱 > 是存取網路資料夾的使用者名稱。
- < 密碼 > 是存取網路資料夾的密碼。

  若密碼包含雙引號，請使用反斜線對雙引號進行跳脫 (`\"`)。

若要指定可透過NFS協定存取的備份儲存路徑，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a setBackupStore --param backup_target_url="nfs://<主機>:/<路徑>"
```

其中：

- < 主機 > 是網路儲存伺服器的位址。
- < 路徑 > 是備份網路資料夾的路徑。

用於備份儲存的網路資料夾的路徑隨即指定。

檢視備份儲存的網路資料夾路徑

若要檢視目前備份儲存路徑，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a getBackupStore
```

目前備份儲存路徑隨即顯示。

設定和管理備份排程

Kaspersky Next XDR Expert可讓您根據排程建立備份、檢視目前排程、暫停或復原排程備份以及刪除排程。

您只能設定一個備份排程。建立新排程將覆蓋現有排程。

在使用排程備份之前，我們建議您手動建立備份，以確保用於儲存備份的網路資料夾設定正確且可存取。

設定備份排程

若要設定備份排程：

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a updateSchedule \
  --param schedule='<schedule>' \
  --param schedule_paused=<schedule_is_paused> \
  --param backup_retain=<max_number_of_backups>
```

其中：

- <schedule> 是採用 UNIX™ cron 格式的字串，用於指定備份頻率。例如，要在每月1日和15日上午9:30以及每個星期一建立備份，請使用以下命令：

  ```
  ./kdt invoke backup-operator -a updateSchedule --param schedule='30 9 1,15 * 1' --param schedule_paused=false --param backup_retain=5
  ```

系統會驗證格式的正確性：如果您輸入了錯誤的參數，系統將顯示錯誤訊息。

- `<schedule_is_paused>` 是指定排程建立後，排程備份狀態的參數：
  - `<schedule_is_paused>=false`—排程備份已啟用，並會依設定執行。
  - `<schedule_is_paused>=true`—排程備份已暫停，不會執行。
- `<max_number_of_backups>` 是可儲存於網路資料夾中的備份數量上限。預設值是10。若網路資料夾已包含最大數量的備份檔案，則下一個備份將覆寫最早的備份。若調降參數值（例如，在手動建立備份或設定備份排程時，將 `<max_number_of_backups>` 設定為 `3`），KDT 將刪除除最近三份備份外的所有備份。

備份排程隨即設定。

檢視備份排程詳情

若要檢視備份排程詳情，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a getBackupSchedule
```

系統會顯示已設定備份排程的詳細資訊，包含於 `NAME` 欄位中顯示的排程名稱。

暫停排程備份

若要暫停排程備份，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a updateSchedule --param schedule_paused=true
```

排程備份隨即暫停。

恢復排程備份

若要恢復排程備份，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a updateSchedule --param schedule_paused=false
```

排程備份隨即恢復。

手動建立Kaspersky Next XDR Expert資料的備份副本

如果您需要在不等待下一次自動備份的情況下儲存備份，或者確保用於儲存備份的網路資料夾設定正確且可存取，則可以建立手動備份。在備份過程中，Kaspersky Next XDR Expert元件的運作會暫時中止，以確保資料一致性。

若要手動建立備份，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a createBackup --param backup_retain=
<max_number_of_backups>
```

其中 `<max_number_of_backups>` 是可儲存於網路資料夾中的備份數量上限。預設值是10。若網路資料夾已包含最大數量的備份檔案，則下一個備份將覆寫最早的備份。若調降參數值（例如，在手動建立備份或設定備份排程時，將 `<max_number_of_backups>` 設定為 `3`），KDT 將刪除除最近三份備份外的所有備份。

建立的備份副本隨即儲存到設定的網路資料夾。KDT日誌提供有關備份操作結果的詳情，包括備份成功或失敗、執行日期和時間以及備份副本的名稱和位置。

檢視Kaspersky Next XDR Expert資料的備份

檢視備份清單

若要檢視備份清單：

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a listBackups
```

備份清單隨即顯示。清單會顯示備份大小、狀態、備份執行日期和時間，以及顯示於 `NAME` 欄中的備份名稱和顯示於 `BACKUPID` 欄中的唯一備份識別碼。

查看備份詳情

若要查看備份詳情，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a describeBackup --param backup_id='<backup_name>'
```

其中 `<backup_name>` 是備份名稱，該名稱顯示於備份清單中的 `NAME` 欄。

備份詳情隨即顯示。

如有必要，您可以使用自訂操作刪除備份。為此，在KDT公用程式所在的管理員主機上執行以下命令：

```
./kdt invoke backup-operator -a deleteBackup --param
backup_id='01kp2qkprmwaajpd8cgy3zeqbt'
```

從備份副本還原Kaspersky Next XDR Expert資料

在還原資料之前，請確保使用與建立備份時相同版本的Kaspersky Next XDR Expert。

僅當DBMS未包含在Kubernetes叢集中時，才支援備份和還原Kaspersky Next XDR Expert資料。將DBMS安裝到 Kubernetes叢集的組態僅用於熟悉解決方案，不用於解決標準工作任務。

若要從備份副本還原Kaspersky Next XDR Expert資料，

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a restoreFromBackup --param backup_id='<backup_id>'
```

其中 `<backup_id>` 是顯示於已建立備份清單中 `BACKUPID` 欄位的唯一備份識別碼。

Kaspersky Next XDR Expert資料隨即從備份中還原。在日誌檔案中，KDT輸出有關恢復操作成功或失敗及其總持續時間的資訊。

若要檢視從備份副本還原 Kaspersky Next XDR Expert 資料的狀態：

在管理員主機上，執行下列命令：

```
./kdt invoke backup-operator -a restoreStatus
```

停止Kubernetes叢集節點

您可能需要停止整個Kubernetes叢集或暫時分離叢集的一個節點進行維護。

在虛擬環境中，不要關閉託管活動Kubernetes叢集節點的虛擬機器。

如果您沒有超級使用者權限，則必須取得該權限，或在下列每個命令前加上 `sudo` 來提升您的權限，例如：`sudo k0s status`、`sudo k0s stop`。

建議您參閱作業系統的官方文件，以了解要執行之命令的詳細資訊。

停止多節點Kubernetes叢集

若要停止多節點Kubernetes叢集（多節點部署方案）：

1. 登入工作線程節點並啟動優雅關閉：

   a. 執行以下命令停止節點：

   ```
   k0s stop
   ```

   b. 執行以下命令檢查節點是否已停止：

   ```
   k0s status
   ```

   c. 執行以下命令關閉節點：

   ```
   shutdown -now
   ```

   出於安全原因，不建議您使用 `--force` 金鑰。

2. 對所有工作線程節點重複此進程。

3. 登入主要節點，並按照步驟 a-c 所述啟動優雅關閉。

如果 Kubernetes 叢集中的活動節點數少於三個，部分功能可能會喪失，直到節點數恢復到初始數量為止。關閉主要節點時，管理叢集的能力（包括透過 kdt 工具進行管理）將會喪失，直到主要節點重新啟動為止。

停止單節點Kubernetes叢集

若要停止單節點Kubernetes叢集（單節點部署方案）：

登入主要節點，並按照步驟 a-c 所述啟動優雅關閉。

啟動 Kubernetes 叢集

若要啟動 Kubernetes 叢集：

1. 作業系統載入後，執行以下命令：

   ```
   k0s start
   ```

2. 執行以下命令檢查節點是否已啟動：

   ```
   k0s status
   ```

3. 對於多節點部署方案，請對所有節點重複此程序。

使用Kaspersky Next XDR Expert公共服務的憑證

若要使用Kaspersky Next XDR Expert公共服務，您可以使用自簽署憑證或自訂憑證。預設情況下，Kaspersky Next XDR Expert使用自簽署憑證。

以下Kaspersky Next XDR Expert公共服務需要憑證：

- `<console_host>.<smp_domain>`—存取 OSMP 主控台介面。
- `<ksc_host>.<smp_domain>`—與管理伺服器互動。
- `<api_host>.<smp_domain>`—存取 Kaspersky Next XDR Expert API。
- `<monitoring_host>.<smp_domain>`—存取 OSMP 指標。
- `<kuma_host>.<smp_domain>`—存取 SIEM 元件。

Kaspersky Next XDR Expert 公開服務的 FQDN 由設定檔中指定的主機名稱與網域名稱組成。Kaspersky Next XDR Expert 公共服務的位址清單（於部署期間定義自我簽署憑證或自訂憑證者），已在 `pki_host_list` 安裝參數中指定。

自訂憑證必須以PEM格式的檔案形式指定，該檔案包含完整的憑證鏈（或僅一個憑證）和一個未加密的私鑰。

您可以從組織的私鑰基礎設施（PKI）中指定中級憑證。Kaspersky Next XDR Expert公共服務的自訂憑證將由此自訂中級憑證簽發。或者，您可以為每個公共服務指定葉憑證。如果僅為部分公共服務指定葉證書，則會為其他公共服務簽發自簽署憑證。

對於 `<console_host>.<smp_domain>`、`<kuma_host>.<smp_domain>`、`<monitoring_host>.<smp_domain>` 與 `<api_host>.<smp_domain>` 公開服務，您只能在部署前於設定檔中指定自訂憑證。指定 `intermediate_bundle` 與 `intermediate_enabled` 安裝參數，以使用自訂中級憑證。自訂中級憑證的有效期限必須至少為399天。

若想將自訂葉憑證與 Kaspersky Next XDR Expert 公開服務搭配使用，請指定對應的 `console_bundle`、`admsrv_bundle`、`kuma_bundle`、`monitoring_bundle` 與 `api_bundle` 安裝參數。將 `intermediate_enabled` 參數設定為 `false`，且不要指定 `intermediate_bundle` 參數與 `pki_host_list` 參數。自訂葉憑證的有效期限必須至少為399天。

對於 `<ksc_host>.<smp_domain>` 服務，您可以使用 klsetsrvcert 公用程式將已簽發的管理伺服器自簽署憑證取代為自訂憑證。

> 不支援憑證自動輪換。請注意憑證的有效期，並在憑證過期時進行更新。

若要更新自訂憑證，

1. 在管理員主機上，匯出目前的組態檔。
2. 在匯出的組態檔中，請在 `intermediate_bundle` 安裝參數中指定新的自訂中繼憑證路徑。若您為每項公開服務使用自訂葉憑證，請指定 `console_bundle`、`admsrv_bundle`、`kuma_bundle`、`monitoring_bundle` 和 `api_bundle` 安裝參數。

3. 請執行下列命令並指定已修改組態檔的完整路徑：

```
./kdt apply -i <組態檔完整路徑>
```

自訂憑證隨即更新。

計算和變更用於儲存管理伺服器資料的磁碟空間

管理伺服器資料包括以下物件：

- 有關資產（裝置）的資訊。
- 有關在管理伺服器上為選定的用戶端裝置所記錄的事件的資訊。
- 有關包含資產的網域的資訊。
- 應用程式控制元件的資料。
- 更新。共用資料夾額外需要至少 4 GB 來儲存更新。
- 安裝套件 如果部分安裝套件儲存在管理伺服器上，則共用資料夾還需要額外的可用磁碟空間，其大小相當於所有可供安裝的安裝套件總大小。
- "遠端安裝"工作。如果管理伺服器上存在遠端安裝工作，則需要額外的可用磁碟空間等於要安裝的所有安裝套件的總大小。

計算用於儲存管理伺服器資料的最小磁碟空間

可以使用以下公式粗略估算用於儲存管理伺服器資料所需的最小磁碟空間：

```
(724 * C + 0.15 * E + 0.17 * A + U), KB
```

其中：

- C是資產（裝置）的數量。
- E是要儲存的事件的數量。
- A是Active Directory物件的總數：
  - 裝置帳戶
  - 使用者帳戶
  - 安全群組帳戶
  - 組織單元
- U是更新的大小（至少4GB）。

如果停用網域輪詢，則A被視為等於零。

此公式計算儲存來自受管理裝置的典型資料和更新的典型大小所需的磁碟空間。此公式不包含與應用程式控制元件、安裝套件和遠端安裝工作的受管理裝置數量無關的資料所佔用的磁碟空間容量。

更改用於儲存管理伺服器資料的磁碟空間

用於儲存管理伺服器資料的可用磁碟空間容量，已於部署 Kaspersky Next XDR Expert 前在設定檔中指定（ `ksc_state_size` 參數）。請考量透過公式計算得出的最小磁碟空間需求。

若要部署Kaspersky Next XDR Expert後檢查用於儲存管理伺服器資料的磁碟空間，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke ksc --action getPvSize
```

所需的可用磁碟空間容量（以GB為單位）隨即顯示。

若要在部署Kaspersky Next XDR Expert後變更用於儲存管理伺服器資料的磁碟空間，

請在KDT公用程式所在的管理員主機上執行下列命令並指定所需的可用磁碟空間（以GB為單位）（例如，「50Gi」）：

```
./kdt invoke ksc --action setPvSize --param ksc_state_size='<new_disk_space_amount>Gi'
```

變更指派用於儲存管理伺服器資料的可用磁碟空間容量。

檢視和變更KUMA Core和指標服務的磁碟空間

您可以檢視目前分配給KUMA Core和Metrics服務執行的磁碟空間量。根據需要，您可以變更已分配的磁碟空間。

檢視目前已分配的磁碟空間

檢視磁碟空間的命令不會影響正在執行的服務的執行。

若要檢視分配給KUMA Core的磁碟空間：

在管理員主機上，執行下列命令：

```
./kdt invoke kuma --action getCorePvcSize
```

若要檢視分配給Metrics服務的磁碟空間：

在管理員主機上，執行下列命令：

```
./kdt invoke kuma --action getMetricsPvcSize
```

變更目前已分配的磁碟空間

這些命令會變更 core_disk_request 和 metrics_disk_request 參數。執行命令後，對應的服務隨即停止，磁碟空間將更改，然後服務將重新啟動。應用程式只有在命令成功完成時，才會更新 core_disk_request 和 metrics_disk_request 參數。

您只能增加目前磁碟空間。如果您嘗試設定小於目前值的磁碟空間，命令將傳回錯誤。在這種情況下，服務不會停止。

如果服務停止後發生錯誤，應用程式會嘗試重新啟動服務並保留先前的磁碟空間值。

若要變更分配給KUMA Core的磁碟空間：

在管理員主機上，執行下列命令：

```
./kdt invoke kuma --action setCorePvcSize --param core_disk_request=<value>
```

其中 <value> 是新的磁碟空間大小，例如 50Gi 。

若要變更分配給Metrics服務的磁碟空間：

在管理員主機上，執行下列命令：

```
./kdt invoke kuma --action setMetricsPvcSize --param metrics_disk_request=<value>
```

其中 <value> 是新的磁碟空間大小，例如 50Gi 。

檢視和更改物件儲存體容量

物件儲存體是儲存臨時常規程式資料、警示和事件檔案以及支援外部整合的S3 API的元件。如果物件儲存體磁碟區即將滿載，您可以檢查目前為其配置的容量。您可以使用 KDT 公用程式變更儲存體容量。這可以防止儲存溢位和相關的服務中斷。

若要查看物件儲存體容量：

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke objectstorage --action getDataPvSize
```

命令輸出中會顯示物件儲存體 PV 目前配置的容量（以 GB 為單位，例如 10Gi ）。

若要增加物件儲存體的容量：

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke objectstorage --action setDataPvSize --param volumeDataSize=<new_size>
```

其中，`<new_size>` 是所需的物件儲存體容量，以 GB 為單位（例如 11Gi）。該值必須大於當前容量。

物件儲存體的容量隨即調整。新的物件儲存體容量無需重新啟動服務即可生效。

增加可觀測性儲存體大小

可觀測性元件是提供事件、威脅和資產集中可見性的元件。您可以使用 KDT 增加可觀測性元件 (VictoriaMetrics) 的儲存體大小。

若要手動增加可觀測性元件的儲存體大小，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke observability --action increaseVMPvSize --param prometheus_size=<new_size>
```

其中，`<new_size>` 是所需的儲存體大小，以 GB 為單位（例如 11Gi）。該值必須大於當前容量。

可觀測性元件的儲存體大小會調整為指定值。

輪換Kubernetes叢集憑證

KDT允許您輪換Kubernetes叢集憑證，這些憑證用於存取Kubernetes叢集以及Kaspersky Next XDR Expert的基礎設施元件。Kubernetes叢集憑證位於Kubernetes叢集內的目標主機上。

若要手動輪換Kubernetes叢集憑證，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke foreach --action RotateK0sConfig
```

新的Kubernetes叢集憑證隨即產生。預設保留期為10年。

更新Bootstrap時，Kubernetes叢集憑證會自動更新。

輪換登錄檔存取憑據

KDT可讓您根據組織的資訊安全要求輪替登錄檔存取憑據。

若要手動輪換登錄檔存取憑據，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke bootstrap --action RotateRegistryCreds
```

登錄檔存取憑據隨即更新。

更新Bootstrap時，登錄檔存取憑據會自動更新。

DBMS 認證資料和憑證的輪換

您可以使用 KDT 輪換用於連線至 DBMS 的 DBMS 認證資料和憑證。您可以根據組織的資訊安全要求輪換 DBMS 機密資料。

若要手動輪換 DBMS 認證資料和憑證，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke foreach --action rotatedbcreds
```

DBMS 認證資料和憑證已更新。

新增主機以安裝附加的KUMA服務

如果需要擴充儲存，或為增加的事件流新增新的收集器和關聯器，您可以新增附加的主機來安裝KUMA服務。

您必須在expand.inventory.yml檔案中指定附加主機的參數。該檔案位於分發套件中，其中包含傳輸封存檔案、KDT、組態檔和其他檔案。在expand.inventory.yml檔案中，您可以一次為收集器、關聯器和儲存指定多個附加的主機。確保所選主機的硬體、軟體和安裝需求得到滿足。

若要準備expand.inventory.yml檔案中指定的主機上所需的基礎設施，您需要建立服務目錄，並將服務安裝所需的檔案新增至這些目錄。若要準備基礎設施，請執行下列命令並指定expand.inventory.yml檔案：

```
./kdt invoke kuma --action addHosts --param host_inventory='<path_to_inventory_file>'
```

在expand.inventory.yml檔案中指定的主機上，將服務安裝所需的檔案新增至服務目錄。

以下是用於安裝KUMA服務的附加KUMA清查檔案範例（expand.inventory.yml檔案）。

```
all:
  vars:
    ansible_connection: local
    ansible_user: nonroot
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root
```

```
children:
  kuma_utils:
  kuma_collector:
    hosts:
      kuma1.example.com:
          ansible_host: 0.0.0.0
      kuma2.example.com:
          ansible_host: 0.0.0.0
  kuma_correlator:
    hosts:
      kuma3.example.com:
          ansible_host: 0.0.0.0
      kuma4.example.com:
          ansible_host: 0.0.0.0
  kuma_storage:
    hosts:
      kuma5.example.com:
          ansible_host: 0.0.0.0
      kuma6.example.com:
          ansible_host: 0.0.0.0
```

新增附加的儲存體、收集器或關聯器

您可以為現有基礎設定新增附加的儲存體叢集、收集器或關聯器。如果要新增多個服務，建議依下列順序安裝：儲存體、收集器和關聯器。

若要新增附加的儲存體叢集、收集器或關聯器：

1. 在OSMP主控台的主功能表中，轉至**設定→ KUMA** 。
2. 在OSMP主控台的KUMA部分，為您要安裝在準備好的主機上的每個KUMA服務（儲存體、收集器和關聯器）建立一個資源集。
3. 為儲存體、收集器和關聯器建立服務。
4. 取得服務識別碼以綁定建立的資源集和KUMA服務：
   a. 在 OSMP 解決方案中，前往**資源 → 作用中服務**。
   b. 選擇所需的KUMA服務，然後按一下**複製ID**按鈕。
5. 在expand.inventory.yml清查檔案中kuma_storage、kuma_collector和kuma_correlator部分列出的每個已準備好的主機上安裝KUMA服務。在每台裝置上，在安裝命令中，指定與主機對應的服務ID。執行對應的命令來安裝KUMA服務：
   - 儲存體的安裝命令：

     ```
     sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the
     KUMA Core CA certificate> --id <service ID> --install
     ```

- 收集器的安裝命令：

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
the KUMA Core CA certificate> --id <service ID> --api.port <API port>
```

- 相關器的安裝命令：

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of
the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

收集器和關聯器的安裝命令會在安裝精靈的 **掃描** 索引標籤上自動產生。用於通訊的連接埠會自動新增至命令中。使用產生的命令在主機上安裝收集器和關聯器。這將確保與命令中指定的服務通訊的連接埠可用。

其中：

- <FQDN> 是 KUMA Core 伺服器的完整網域名稱。KUMA Core 的 FQDN 是 <kuma_host>.<smp_domain>。用於連線至 KUMA Core 的連接埠無法變更。預設情況下使用連接埠 7210。
- <fingerprint ID of the KUMA Core CA certificate> 是連線至服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
- <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
- <API port> 是用於與已安裝元件通訊的連接埠。

附加KUMA服務已安裝。

為現有儲存體新增主機

您可以透過新增主機作為新的儲存體叢集節點來擴充現有儲存體（儲存體叢集）。

若要為現有儲存體新增主機：

1. 在OSMP主控台的主功能表中，轉至**設定**→ **KUMA** 。
2. 為儲存體叢集新增節點。為此，請編輯現有儲存體叢集的設定：
   a. 在**資源** → **儲存體**區段中，選取現有儲存體，然後開啟該儲存體進行編輯。
   b. 在**ClickHouse叢集節點**部分，按一下**新增節點**，然後在新節點的欄位中指定角色。從expand.inventory.yml檔案的kuma_storage部分指定對應的主機網域名稱，然後為新節點指定角色。
   c. 儲存您的變更。

您無需建立單獨的儲存體，因為您正在向現有儲存體叢集新增伺服器。

3. 在OSMP主控台的KUMA部分為每個新增的儲存體叢集節點建立儲存服務，然後將這些服務綁定到儲存體叢集。

4. 為每個準備安裝KUMA服務的主機取得儲存體服務識別碼：

   a. 在OSMP主控台的KUMA部分，轉至**資源→活動服務**。

   b. 選擇所需的KUMA服務，然後按一下**複製ID**按鈕。

5. 在expand.inventory.yml清查檔案中kuma_storage部分列出的每個準備主機上安裝儲存體服務。在每台裝置上，在安裝命令中，指定與主機對應的服務ID。執行以下命令以安裝儲存體服務：

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:7210 --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 伺服器的完整網域名稱。KUMA Core 的 FQDN 是 <kuma_host>.<smp_domain>。用於連線至 KUMA Core 的連接埠無法變更。預設情況下使用連接埠 7210。
   - <fingerprint ID of the KUMA Core CA certificate> 是連線至服務時用於身分驗證的 CA 憑證指紋 ID。

     `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

     您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

     為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。

   - <service ID> 是從網頁介面複製的 KUMA 服務 ID。

   附加主機將被新增到儲存體叢集。

在distributed.inventory.yml清查檔案中指定新增的主機，以便在KUMA元件更新時，該檔案包含最新資訊。

取代使用KUMA儲存體的主機

若要將使用KUMA儲存體的主機替換為另一台主機：

1. 填寫expand.inventory.yml檔案，指定要取代的主機的參數。

2. 執行下列命令，並指定expand.inventory.yml檔案以移除主機：

   ```
   ./kdt invoke kuma --action removeHosts --param host_inventory='<path_to_inventory_file>'
   ```

3. 填寫expand.inventory.yml檔案，指定要取代先前主機的新主機的參數，然後執行下列命令：

   ```
   ./kdt invoke kuma --action addHosts --param host_inventory='<path_to_inventory_file>'
   ```

4. 依照KUMA服務新增主機的說明中的步驟2-6，新增一個包含KUMA儲存體的新主機。

   包含KUMA儲存體的主機將被替換為另一個主機。

如果您的儲存體組態包含一個包含兩個副本的分片，並且您使用上述步驟將第二個副本主機替換為新主機，則在安裝新副本時可能會收到錯誤訊息。在這種情況下，新副本將無法運作。

若要修復新增分片新副本時出現的錯誤：

1. 在另一台包含相同分片副本（該分片擁有錯誤新增的副本）的主機上，請使用下列命令啟動ClickHouse用戶端：

   ```
   /opt/kaspersky/kuma/clickhouse/bin/client.sh
   ```

   如果此主機不可用，請在同一儲存體叢集包含副本的任何其他主機上執行用戶端。

2. 運行命令以刪除有關要替換的主機的資料。

   - 如果擁有與錯誤新增的副本相同的分片副本的主機可用，請執行下列命令：

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM TABLE
     kuma.events_local_v2
     ```

   - 如果使用的是另一個具有副本的儲存體叢集主機，請執行下列命令：

     ```
     SYSTEM DROP REPLICA '<replica number of read-only node>' FROM ZKPATH
     '/clickhouse/tables/kuma/<shard number of read-only node>/kuma/events_local_v2
     ```

3. 執行以下命令，使用副本恢復新增主機的運作：

   ```
   SYSTEM RESTORE REPLICA kuma.events_local_v2
   ```

   具有副本的新增主機的可操作性隨即恢復。

使用部署在虛擬機器上的Kaspersky Next XDR Expert

如果您已在虛擬機器上部署了Kaspersky Next XDR Expert，不建議在解決方案執行時使用hypervisor對這些虛擬機器進行快照或遷移操作。在這種情況下，Kaspersky Next XDR Expert將無法正常運作。為確保Kaspersky Next XDR Expert正常運作，請在建立快照或執行遷移之前停止Kubernetes叢集集中的所有虛擬機器。

Kaspersky Next XDR Expert部署的演示

如果您想熟悉Kaspersky Next XDR Expert，您可以執行解決方案的演示部署。

僅可使用Kaspersky Next XDR Expert的演示部署（其中DBMS已安裝在Kubernetes叢集中）來熟悉此解決方案。我們不建議使用此方法解決標準工作任務。對於標準使用，請執行多節點或單節點部署。

在演示部署中，所有Kaspersky Next XDR Expert元件都安裝在Kubernetes叢集的單一節點或多個節點上。

以下情景描述了單節點演示佈署。單節點部署所需的資源較少，因此更常用於演示佈署。在單節點示範部署中，Kubernetes叢集、Kaspersky Next XDR Expert元件和DBMS都安裝在同一目標主機上。此外，您還需要一台部署管理員主機來部署和管理Kubernetes叢集和Kaspersky Next XDR Expert，以及一台用於安裝KUMA服務的目標主機。

在單節點組態中，您至少需要三台主機：

- 1台管理員主機
- 1台目標主機，用於安裝Kubernetes叢集、Kaspersky Next XDR Expert元件和DBMS
- 1台KUMA目標主機，用於安裝KUMA服務

示範部署和標準部署的主要區別在於DBMS的位置。在標準部署（多節點或單節點）中，DBMS安裝在叢集外部的主機上。而在演示佈署中，DBMS安裝在叢集內部的目標主機上。

在部署Open Single Management Platform和Kaspersky Next XDR Expert元件之前，建議您閱讀硬化指南 。

依照此方案，您可以準備演示部署的基礎設施，準備組態檔，並使用Kaspersky Deployment Toolkit工具（以下簡稱KDT）部署解決方案。

此演示部署情境分幾個階段進行：

1. **下載包含Kaspersky Next XDR Expert元件的分發套件**

   分發套件包含以下元件：

   - 包含Kaspersky Next XDR Expert元件和Kaspersky Next XDR Expert和KDT最終使用者產品授權協議的傳輸存檔

     這些元件使用RSA金鑰和GOST R 34.11-2012金鑰進行簽署。

   - 包含KDT公用程式的存檔，以及組態檔和KUMA清查檔案的範本

2. **準備管理員和目標主機**

   準備所選的管理員主機和目標主機以部署Kaspersky Next XDR Expert。

   操作說明：準備管理員主機和目標主機

3. **準備KUMA主機**

   準備KUMA目標主機以安裝KUMA服務（收集器、關聯器和儲存體）。

   操作說明：準備用於安裝KUMA服務的主機

4. **準備用於安裝KUMA服務的KUMA清查檔案**

   準備YAML格式的KUMA清查檔案。KUMA清查檔案包含用於安裝KUMA服務的參數。

   操作說明：準備KUMA清查檔案

5. **準備組態檔**

   準備YAML格式的組態檔。組態檔包含部署目標主機清單和Kaspersky Next XDR Expert元件的安裝參數集。

   操作說明：指定安裝參數

6 Kaspersky Next XDR Expert的部署

使用KDT部署Kaspersky Next XDR Expert。Kaspersky Deployment Toolkit會自動部署Kubernetes叢集，並在該叢集內安裝OSMP元件和其他基礎設施元件。

操作說明：安裝Kaspersky Next XDR Expert

7 安裝KUMA服務

在準備好的KUMA目標主機上安裝KUMA服務（收集器、關聯器和儲存體），這些主機位於Kubernetes叢集之外。

操作說明：安裝KUMA服務

8 設定與Kaspersky Anti Targeted Attack Platform的整合

安裝中央節點，用於接收來自Kaspersky Anti Targeted Attack Platform的遙測資料，然後設定Kaspersky Next XDR Expert與Kaspersky Anti Targeted Attack Platform/KEDR之間的整合，以管理連線到Kaspersky Endpoint Detection and Response伺服器的資產的威脅回應操作。

如有需要，您可以安裝多個中央節點元件，以便彼此獨立使用，或在分散式解決方案模式下組合使用以進行集中管理。若要組合多個中央節點元件，您必須將包含元件的伺服器組織成層次結構。

設定中央節點伺服器時，您必須在**儲存**欄位中指定盡可能小的值，以避免Kaspersky Next XDR Expert和KEDR資料庫之間的資料重複。

準備管理員和目標主機

演示部署的準備工作包括設定管理員主機和目標主機。在單節點演示部署中，Kubernetes叢集、Kaspersky Next XDR Expert元件和DBMS都安裝在同一目標主機上。準備好目標主機並指定組態檔後，您將能夠使用KDT在目標主機上部署Kaspersky Next XDR Expert。

僅可使用Kaspersky Next XDR Expert的演示部署（其中DBMS已安裝在Kubernetes叢集中）來熟悉此解決方案。我們不建議使用此方法解決標準工作任務。對於標準使用，請執行多節點或單節點部署。

準備管理員主機

首先，您需要準備一台裝置作為啟動KDT的管理員主機。該主機可以包含在KDT在部署期間建立的Kubernetes叢集中，也可以不包含在內。如果管理員主機不包含在叢集中，它將僅用於部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。在這種情況下，解決方案的部署和運作只需要一台主機。

若要準備管理員主機：

1. 請確保管理員主機上的硬體和軟體符合KDT的需求。
2. 請在暫存檔案目錄（預設為 `/tmp`）中為 KDT 配置至少 10 GB 的可用空間。若此目錄中的可用空間不足，請執行以下命令以指定另一個目錄的路徑：

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

3. 設定容器執行階段。使用下列其中一個容器執行階段：

- KDT 內建容器執行階段（以 runc 為基礎）。
  若要安裝此執行階段，請執行以下命令：

  ```
  sudo ./kdt init
  ```

  如果內建容器執行階段不適用於您的環境，您可以改用 Docker 容器執行階段。

- Docker 容器執行階段。
  安裝適用於 Docker 版本 25 的軟體包 或稍後。請勿從作業系統維護者儲存區安裝非官方的Docker軟體套件發行版。
  如果無法自動下載 Docker 金鑰環，請手動下載：

  a. 在瀏覽器中開啟 https://download.docker.com/linux/ubuntu/gpg 連結，將金鑰儲存為 docker.asc。

  b. 執行以下命令：

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

  Docker 資料儲存的磁碟分割區（預設為 `/var/lib/docker`）必須至少有 60 GB 可用空間。
  執行安裝後步驟，以設定管理主機，使其能夠與Docker正常運作：

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

4. 對於將包含在叢集中的管理主機，請執行其他準備步驟：

   a. 由於該裝置將充當管理員和目標主機，請確保它符合單節點部署的需求。

   b. 確保管理員主機支援cgroup v2 技術。

準備目標主機

目標主機是用於部署Kaspersky Next XDR Expert並包含在Kubernetes叢集中的實體機或虛擬機。目標主機管理Kubernetes叢集，儲存元資料，並且Kaspersky Next XDR Expert元件也在此主機上運作。演示佈署的最小叢集組態包含一個目標主機，該主機充當主要節點和工作線程節點。Kubernetes叢集、DBMS和Kaspersky Next XDR Expert元件都安裝在該主要工作線程節點上。

KUMA服務（收集器、關聯器和儲存體）可以完全安裝在叢集內部的主要工作線程節點上，也可以完全安裝在Kubernetes叢集外部的獨立主機上，或部分安裝在Kubernetes叢集內部，部分安裝在Kubernetes叢集外部。

如果要從目標主機執行Kaspersky Next XDR Expert部署，則必須依照前面的步驟將該主機設定為管理員主機，然後再對目標主機進行設定。

若要準備目標主機：

1. 確保目標主機上的硬體和軟體符合單節點部署的需求（因為演示部署和單節點部署的部署方案類似）。

   如果KUMA服務安裝在叢集內部，則目標主機必須符合安裝KUMA服務所需的硬體、軟體和安裝需求。

   為了Kaspersky Next XDR Expert正常運作，在裝有Ubuntu系列作業系統的目標主機上，Linux核心版本必須為5.15.0.107或更高版本。

   為了確保 Kubernetes 叢集及其元件正常運作，必須在所有叢集節點上停用交換空間。如果節點已啟用交換空間，KDT 將在部署期間自動將其停用。

   除非目標主機將用作管理員主機，否則不要在目標主機上安裝Docker。KDT將在部署期間安裝所有必要的軟體和依賴項。

2. 請確保掛載在 `/var` 目錄下的檔案系統在目標主機上至少有360GB的可用空間。

   我們建議將 `/opt/lvp/hot` 目錄放置在專用的高效能磁碟子系統上，並將 `/opt/lvp/cold` 目錄放置在另一個高容量磁碟子系統上。

3. 如果尚未安裝sudo套件，請安裝此套件。對於Debian系列作業系統，安裝UFW套件。

4. 設定/etc/environment檔案。如果貴組織的基礎設施使用代理伺服器存取網際網路，則還需要將目標主機連線到網際網路。

5. 在具UFW設定的主要工作線程節點上，允許 IP 轉送功能。在 `/etc/default/ufw` 檔案中，將 `DEFAULT_FORWARD_POLICY` 設定為 `ACCEPT`。

6. 提供對儲存Kaspersky Next XDR Expert所需的以下軟體套件的軟體套件儲存區的存取權限：

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

- python-apt
- systemd
- tar

KDT將在部署期間嘗試從軟體套件儲存區安裝這些軟體套件。您也可以手動安裝這些安裝套件。

7. 確保以下軟體包已安裝在主工作線程節點上：

   - python3-apt
   - curl

   使用KDT從軟體套件儲存區部署期間不會安裝curl和libnfs軟體套件。如果尚未安裝這些安裝套件，則必須手動安裝它們。

8. 為目標主機和Kubernetes叢集閘道保留靜態IP位址。

   Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。

   由於DBMS安裝在Kubernetes叢集內部，因此閘道IP位址是IP位址範圍（例如，192.168.0.1—192.168.0.2）。該範圍內的第一個IP位址是Kaspersky Next XDR Expert服務的位址（不包括DBMS的IP位址）。該範圍內的第二個IP位址是DBMS的IP位址。

   確保目標主機和Kubernetes叢集閘道位於同一個廣播網域。

9. 在您的DNS伺服器上，註冊服務FQDN以連線到Kaspersky Next XDR Expert服務。

   預設情況下，Kaspersky Next XDR Expert服務在以下位址可用：

   - <console_host>.<smp_domain>—存取OSMP主控台介面。
   - <ksc_host>.<smp_domain>—與管理伺服器互動。
   - <kuma_host>.<smp_domain>—存取SIEM元件。
   - <api_host>.<smp_domain>—存取Kaspersky Next XDR Expert API。
   - <monitoring_host>.<smp_domain>—存取OSMP指標。
   - <xdr_edr_ingress_host>.<smp_domain>—與代理程式伺服器互動。

     其中，<console_host>、<ksc_host>、<kuma_host>、<api_host>、<monitoring_host>和<xdr_edr_ingress_host>皆為服務主機名稱，<smp_domain>為服務網域名稱。這些參數是服務FQDN的組成部分，且可在組態檔中指定。如果您未指定服務主機名稱的自訂值，則會使用預設值：`console_host`—「`console`」、`ksc_host`—「`admsrv`」、`kuma_host`—「`kuma`」、`api_host`—「`api`」、`monitoring_host`—「`monitoring`」、`"xdr_edr_ingress_host"`—`"agentserver"`。

   所列的服務FQDN必須解析為Kubernetes叢集的IP位址。例如，如果Kubernetes叢集位址為10.80.23.182，則服務FQDN將如下解析為IP位址：

   - <console_host>.<smp_domain>—10.80.23.182
   - <ksc_host>.<smp_domain>—10.80.23.182
   - <kuma_host>.<smp_domain>—10.80.23.182

- <api_host>.<smp_domain>—10.80.23.182
- <xdr_edr_ingress_host>.<smp_domain>—10.80.23.182

10. 建立將用於部署Kaspersky Next XDR Expert的使用者帳戶。

    這些帳戶用於 SSH 連線，且必須能夠在不輸入密碼的情況下提升權限 (sudo)。為此，請將建立的使用者帳戶新增至 `/etc/sudoers` 檔案。

    檢視詳情

    若要將建立的使用者帳戶新增至 `/etc/sudoers` 檔案：

    1. 執行以下指令：

       ```
       sudo useradd -m -s /bin/bash <user_name>
       sudo usermod -aG sudo <user_name>
       ```

    2. 使用以下指令開啟 `/etc/sudoers` 檔案：

       ```
       sudo visudo
       ```

    3. 在 `# Allow members of group sudo to execute any command` 區段的結尾新增下列行：

       ```
       <user_name> ALL=(ALL) NOPASSWD: ALL
       ```

       其中 `<user_name>` 是所建立使用者的名稱。

    4. 儲存並關閉 `/etc/sudoers` 檔案。

11. 設定管理員和目標主機之間的SSH連線：

    a. 在管理員主機上，使用ssh-keygen公用程式產生SSH金鑰（無需密碼）。

    b. 使用 ssh-copy-id 公用程式將公開金鑰複製至目標主機（例如，複製至 `/home/<user_name>/.ssh` 目錄）。

       如果使用目標主機作為管理員主機，則也必須將公鑰複製到該主機。

12. 為了使Kaspersky Next XDR Expert元件正常運作，根據需要，請在管理員和目標主機的防火牆上開啟所需的連接埠。

13. 在管理員和目標主機上設定透過網路時間協定（NTP）進行時間同步。

14. 如有必要，請準備自訂憑證以用於Kaspersky Next XDR Expert公共服務。

    您可以為每個服務使用一個從組織的根憑證或葉憑證頒發的中間憑證。將使用準備好的自訂憑證取代自簽名憑證。

指定安裝參數

用於在單一節點上部署 Kaspersky Next XDR Expert 的設定檔，包含多節點部署與單節點部署都需要的安裝參數。此外，此組態檔包含僅適用於單節點部署的參數：`openbao_ha_mode`、`openbao_standalone` 和 `default_class_replica_count)`。組態檔範本（singlenode.smp_param.yaml.template）位於具有KDT公用程式的存檔的分發套件中。此組態檔可用於演示安裝。

僅可使用Kaspersky Next XDR Expert的演示部署（其中資料庫管理系統已安裝在Kubernetes叢集中）來熟悉此解決方案。我們不建議將此方法用於一般生產環境。對於標準使用，請執行多節點或單節點部署。

組態檔模板中並未包含下面列出的所有參數。此範本僅包含部署Kaspersky Next XDR Expert之前必須指定的參數。其餘參數設定為預設值，不包含在範本中。您可以手動將這些參數新增至組態檔以覆蓋其值。參數值必須遵循下面所述的規則。在Kaspersky Next XDR Expert部署期間，KDT會檢查是否正確指定了所需的安裝參數。如果組態檔中必需的參數缺失或無效，部署將會中斷。

為了確保KDT與設定檔正確配合使用，請在檔案末端新增一個空白行。

設定檔的 `nodes` 區段包含下表所列的目標主機參數。

節點部分

參數名稱	必要	描述
`desc`	是	節點名稱。 值必須符合以下規則： • 節點名稱長度必須為1到63個字元。 • 節點名稱可以包含以下字元： • 大寫ASCII字母（A-Z） • 小寫ASCII字母（a-z） • 數字（0-9） • 連字符（-） 所有叢集節點必須具有唯一名稱。此要求安裝Kaspersky Next XDR Expert的先決條件之一，並已通過KDT驗證。
`type`	是	節點類型。 對於目標主機，請將 `type` 參數設定為 `primary-worker`，以啟用**單節點示範部署**。此種情況下，目標主機將充當主要節點與工作節點。
`host`	是	節點的IP位址。 主要工作線程節點必須與Kubernetes叢集閘道位於同一子網路中。 該節點需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。
`kind`	否	指定將在此節點上安裝的Kaspersky Next XDR Expert 元件的節點類型。 對於**單節點演示部署**，請將此參數留空，因為所有元件都會安裝在單一節點上。

參數名稱	必要	描述
`user`	是	在目標主機上建立的帳戶的使用者名，用於透過KDT連線到節點。 值必須符合以下規則： • 使用者名稱長度必須為1到31個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 底線 (_)、連字號（-）
`password`	否	用於連接節點的密碼。可以代替由 `ssh_pk` 參數指定的 SSH 金鑰。

其他安裝參數列於設定檔的 `parameters` 區段，如下表所述。

參數部分

參數名稱	必要	描述
`nwc-language`	是	預設指定OSMP主控台介面的語言。安裝後，您可以變更OSMP主控台語言。 可能的參數值： • `enUS`（預設值） • `ruRu` 如果未在組態檔中指定此參數，則使用預設值。
`ingress_ip`	是	Kubernetes叢集閘道的保留靜態IPv4位址。 Kubernetes 叢集閘道用於連線至安裝在 Kubernetes 叢集內部的 Kaspersky Next XDR Expert 元件。閘道必須與主要工作線程節點位於同一子網路中。 Kubernetes叢集閘道需要IPv4位址。KDT 會自動停用叢集節點上的 IPv6。 此參數的值不能是執行部署的同一主機的IP地址。 對於**示範部署**，當您在叢集內部安裝 DBMS 時，DBMS IP 位址會與叢集閘道 IP 位址相同。
`ssh_pk`	是	位於管理主機上 SSH 金鑰私鑰部分的路徑，該金鑰用於透過 KDT 連線至主要工作節點及具有 KUMA 服務的節點（收集器、關聯器與儲存體）。參數值必須為Linux檔案路徑或Base64編碼的檔案內容。
`admin_password`	是	`admin_password` 參數指定安裝過程中 KDT 所建立之 Kaspersky Next XDR Expert 使用者帳戶的密碼。該帳戶的預設使用者名稱為「admin」。 主管理員角色已指派給此使用者帳戶。 密碼必須符合以下規則： • 使用者密碼不能少於10個或多於256個字元。 • 密碼必須包含以下組中三組的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;) • 密碼不得包含任何空格或".@"組合。 手動指定 `admin_password` 參數值（而非透過部署精靈指定）時，請確保此值符合 YAML 標準對字串值的要求： • 包含特殊字元的參數值必須用單引號引起來。 • 參數值中的任何單引號'都必須重複以轉義此單引號。 範例：使用者帳戶密碼 `Any_pass%1234'5678"90` 必須指定為 `admin_password` 參數的值 `'Any_pass%1234''5678"90'`。
`low_resources`	是	指示Kaspersky Next XDR Expert安裝在計算資源有限的目標主機上的參數。 對於**單節點示範部署**，請將 `low_resources` 參數設定為 `true`，使 Kaspersky Next XDR Expert 元件佔用更少的記憶體與 CPU 資源。此外，若啟用此參數，系統將配置 4 GB 的可用磁碟空間，以便在目標主機上安裝 KUMA Core。
`openbao_ha_mode`	是	指示是否在高可用性（HA）模式下執行密鑰儲存的參數。 對於**單節點示範部署**，請將 `openbao_ha_mode` 參數設定為 `false`。
`openbao_standalone`	是	指示是否在獨立模式下執行密鑰儲存的參數。 對於**單節點示範部署**，請將 `openbao_standalone` 參數值設定為 `true`。

參數名稱	必要	描述
`default_class_replica_count`	是	用於儲存 Kaspersky Next XDR Expert 元件與 KDT 的服務資料的磁碟區數量。預設值是 `3`。 對於**單節點示範部署**，請將 `default_class_replica_count` 參數值設定為 `1`。
`core_disk_request`	是	指定KUMA Core運行所需磁碟空間量的參數。 若未指定 `core_disk_request` 參數，且 `low_resources` 參數設定為 `false` 或未指定，KUMA Core 運行所需的預設磁碟空間量為 100 GB。 若未指定 `core_disk_request` 參數，且 `low_resources` 參數設定為 `true`，KUMA Core 運行所需的預設磁碟空間量為 4 GB。 您可以在應用程式部署後變更 `core_disk_request` 參數。
`inventory`	是	位於管理員主機上的KUMA清查檔案的路徑。此清查檔案包含用於部署Kubernetes叢集中未包含的KUMA服務的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。如果所有 KUMA 服務都將安裝在叢集內部，請將 `inventory` 參數設為 `/dev/null`。
`host_inventory`	否	位於管理員主機上的附加KUMA清查檔案的路徑。此檔案包含用於部分新增或刪除具有KUMA服務的主機的安裝參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 若執行 Kaspersky Next XDR Expert 的初始部署或執行需要設定檔的自訂動作，請保留預設參數值 (`/dev/null`)。
`license`	否	位於管理員主機上的KUMA產品授權金鑰的路徑。 參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。 部署完成並登入OSMP後，您可以上傳產品授權金鑰或指定啟動碼。

`nwc_host`
`flow_host`
`hydra_host`
`login_host`
`ksc_host`
`console_host`
`api_host`
`kuma_host`
`monitoring_host`
	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的主機名稱。服務主機名稱與網域名稱（ `smp_domain` 參數值）皆為服務 FQDN 的組成部分。
		參數的預設值：
		• `nwc_host—"console"`
		• `flow_host—"console"`
		• `hydra_host—"console"`
		• `login_host—"console"`
		• `ksc_host—"admsrv"`
		• `console_host—"console"`
		• `api_host—"api"`
		• `kuma_host—"kuma"`
		• `monitoring_host—"monitoring"`

`smp_domain`	是	Kaspersky Next XDR Expert 公開服務的 FQDN 中使用的網域名稱。參數值必須符合最高四級網域的命名要求。 服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 `console_host` 變數的值為 `console`，而 `smp_domain` 變數的值為 `smp.local`，則提供 OSMP 主控台存取權的服務完整名稱為 `console.smp.local`。
`pki_host_list`	否	將生成自簽名或自訂憑證的公共Kaspersky Next XDR Expert服務的主機名稱列表。參數值必須是主機名稱列表，以空格分隔。
`intermediate_enabled`	否	該參數用於指示是否對 Kaspersky Next XDR Expert 公開服務使用自訂中間憑證而非自我簽署憑證。 可能的參數值： • `true` — 使用自訂中間憑證。 • `false` — 使用自我簽署憑證（預設值）。
`intermediate_bundle`	否	用於與 Kaspersky Next XDR Expert 公開服務協作之自訂中間憑證的路徑。若 `intermediate_enabled` 參數設定為 `true`，則指定此參數。參數值必須為 Linux 檔案路徑或 Base64 編碼的檔案內容。自訂中級憑證的有效期限必須至少為399天。

`admsrv_bundle`
`api_bundle`
`console_bundle`
`kuma_bundle`
`monitoring_bundle`
	否	用於與對應的 Kaspersky Next XDR Expert 公開服務協作之自訂葉憑證的路徑：`<ksc_host>.<smp_domain>`、`<api_host>.<smp_domain>`、`<console_host>.<smp_domain>`、`<kuma_host>.<smp_domain>` 和 `<monitoring_host>.<smp_domain>`。參數值必須為Linux檔案路徑或Base64編碼的檔案內容。
		如果您要指定自訂葉憑證，請將 `intermediate_enabled` 參數設定為 `false`，且不要指定 `intermediate_bundle` 參數。

參數名稱	必要	描述
`ksc_state_size`	是	分配用於儲存管理伺服器資料（更新、安裝套件和其他內部服務資料）的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。所需的可用磁碟空間量取決於受管理裝置的數量和其他參數，並且可以計算。 預設值為 30 GB。如果未在設定檔中指定此參數，則使用此值。
`prometheus_size`	是	分配給儲存指標的可用磁碟空間量。以GB為單位，指定為「<amount>GB」。 最小值與預設值皆為5GB。如果未在組態檔中指定此參數，則使用預設值。
`grafana_admin_user`	否	用於透過Grafana工具檢視OSMP指標的帳戶的使用者名稱。 值必須符合以下規則： • 使用者名稱長度必須為1到30個字元。 • 使用者名稱可以包含以下字元： • 小寫字母（a-z） • 數字（0-9） • 特殊字元（_ - .） • 使用者名稱必須以字母開頭。 • 使用者名稱不能包含空格或"@"符號。
`grafana_admin_password`	否	用於透過Grafana工具檢視OSMP指標的帳戶的密碼。 密碼必須符合以下規則： • 使用者密碼不能少於8個或多於256個字元。 • 密碼必須包含下列群組中的字元： • 大寫字母（A-Z） • 小寫字母（a-z） • 數字（0-9） • 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
`loki_size`	是	分配給儲存OSMP日誌的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。 最低建議值和預設值為 40 GB。如果未在組態檔中指定此參數，則使用預設值。
`loki_retention_period`	是	OSMP日誌的儲存週期，超過此週期後日誌將自動刪除。預設值為72小時（將設定檔中的參數值設定為「<time in hours>h」。例如：「72h」）。如果未在組態檔中指定此參數，則使用預設值。
`file_storage_cp`	否	指派給元件用於儲存資料以處理回應操作的可用磁碟空間量。以GB為單位，指定為「<amount>Gi」。最小推薦值為20 GB。
`psql_tls_off`	否	指示是否使用 TLS 協定對 Kaspersky Next XDR Expert 元件與 DBMS 之間的流量進行加密的參數。 若 DBMS 安裝在叢集外部，則預設停用 TLS 加密。對於**示範部署**，若 DBMS 安裝在叢集內部，則必須停用 TLS 加密（`psql_tls_off` 設定為 `true`）。 可能的參數值： • `true` — 不加密流量（預設值）。 • `false` — 加密流量。
`proxy_enabled`	否	指示是否使用代理伺服器將 Kaspersky Next XDR Expert 元件連線至網際網路的參數。若安裝 Kaspersky Next XDR Expert 的主機具有網際網路存取權限，亦可為 Kaspersky Next XDR Expert 元件（例如管理伺服器）的運作以及特定整合（包括卡巴斯基與第三方）提供網際網路存取權限。若要建立代理連線，還須在管理伺服器內容中指定代理伺服器參數。 可能的參數值： • `true` — 使用代理伺服器。 • `false` — 不使用代理伺服器（預設值）。
`proxy_addresses`	否	代理伺服器的IP位址。若代理伺服器使用多個 IP 位址，請指定這些位址，並以空格分隔（例如，`"0.0.0.0 0.0.0.1 0.0.0.2"`）。若 `proxy_enabled` 參數設定為 `true`，則指定此參數。
`proxy_port`	否	用於建立代理連線的連接埠號碼。若 `proxy_enabled` 參數設定為 `true`，則指定此參數。

參數名稱	必要	描述
`trace_level`	否	管理伺服器追蹤檔案的詳盡程度。追蹤在管理伺服器運作期間寫入。 預設值為0，不寫入任何追蹤。 可能的參數值：0–5。 參數值越高，追蹤詳細資訊越詳盡。
`ansible_extra_flags`	否	KDT執行的KUMA Core和KUMA服務部署日誌的詳盡程度。 可能的參數值： • `-v` • `-vv` • `-vvv` • `-vvvv` 隨著旗標中「v」字母數量的增加，日誌將變得更詳盡。如果組態檔中未指定此參數，則將儲存標準元件安裝日誌。
`incident_attachments_max_count_limit`	否	可附加到事件的檔案數量。預設值是 `100`。
`incident_attachments_max_size_limit`	否	已附加到事件的檔案總大小。以位元組為單位。指定時不指明測量單位。預設值是 `26214400`。
`ignore_precheck`	否	該參數用於指示是否在部署前檢查Kubernetes叢集節點的硬體、軟體及網路設定，以確認是否符合解決方案的安裝先決條件。 可能的參數值： • `true` — 略過預檢查。 • `false` — 執行預檢查（預設值）。
`airgap_mode`	否	此參數指示是否執行APT軟體套件管理器預檢查並更新軟體套件快取。這可讓您在實體隔離環境中部署Kaspersky Next XDR Expert。 可能的參數值： • `true` — 略過預檢查和軟體套件快取更新。 • `false` — 執行預檢查並更新軟體套件快取（預設值）。
`grafana_smtp_host`	否	Grafana的SMTP伺服器位址，用於發送有關Kubernetes叢集運行狀況事件的電子郵件通知。請以 `<host>:<port>` 格式指定此參數，例如 `localhost:25`。
`grafana_smtp_user`	否	在SMTP伺服器上進行身份驗證的使用者名稱。
`grafana_smtp_password`	否	在SMTP伺服器上進行身份驗證的密碼。
`grafana_smtp_bundle`	否	包含X.509憑證鏈的檔案，用於驗證與SMTP伺服器的TLS連線。
`grafana_smtp_skip_verify`	否	此參數指示是否跳過SMTP伺服器的TLS憑證驗證。 可能的參數值： • `true`—跳過TLS憑證驗證。 • `false`—執行TLS憑證驗證（預設值）。
`grafana_smtp_from_address`	否	寄件者的電子郵件地址，該地址將顯示在發送電子郵件通知時的「寄件者」欄位中。
`grafana_smtp_from_name`	否	電子郵件通知中顯示的寄件者名稱。
`grafana_smtp_ehlo_identity`	否	連線到SMTP伺服器時，EHLO命令中使用的識別碼。
`grafana_starttls_policy`	否	連線SMTP伺服器時使用STARTTLS的政策。 可能的參數值： • `OpportunisticStartTLS`—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器。 • `MandatoryStartTLS`—需要STARTTLS；如果SMTP伺服器不支援STARTTLS，則失敗。 • `NoStartTLS`—不使用STARTTLS；以不加密的方式連線到SMTP伺服器。 • `empty`—如果SMTP伺服器支援STARTTLS，則使用STARTTLS；否則，以不加密的方式連線到SMTP伺服器（預設值）。
`grafana_smtp_enable_tracing`	否	此參數指示是否啟用SMTP連線偵錯以偵錯電子郵件發送。 可能的參數值： • `true`—啟用SMTP連線偵錯。 • `false`—停用SMTP連線偵錯（預設值）。

參數名稱	必要	描述
tokenhub_access_token	否	存取權杖的存留期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"1h10m"或"2h"。最小可用值為 5m，最大值為 2h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 您可以在應用程式部署後變更 tokenhub_access_token 參數。
tokenhub_refresh_token	否	用於取得新存取權杖的重新整理權杖有效期。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1240h30m"。最小可用值為 12h，最大值為 4320h。 預設值是 24h。如果未在設定檔中指定此參數，則使用此值。 您可以在應用程式部署後變更 tokenhub_refresh_token 參數。
credentials_session_ttl	否	單一登入工作階段的最大閒置時間。 在設定檔中將參數值設定為"<time in hours>h<time in minutes>m<time in seconds>s"。例如，"24h"或"1h30m"。最小可用值為 5m，最大值為 96h。 預設值是 1h。如果未在設定檔中指定此參數，則使用此值。 您可以在應用程式部署後變更 credentials_session_ttl 參數。

以下是單節點示範部署的組態檔範例

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
# Node on which the Kubernetes cluster and Kaspersky XDR will be deployed
nodes:
    # Node name.
  - desc: cdt-1
    # Node type.
    type: primary-worker
   # IP address of the node.
    host: 10.80.23.42
    access:
      ssh:
        # User name of the account.
        user: root
# Parameters for the Kaspersky XDR deployment
parameters:
  # IP address of the Kubernetes cluster gateway.
  - name: ingress_ip
    source:
      value: 10.80.23.182
  # Path to the SSH private key for connection to the primary worker node by KDT.
  - name: ssh_pk
    source:
      path: /root/.ssh/id_rsa
  # Password of the Kaspersky XDR user account that will be created during the
  installation.
  - name: admin_password
    source:
      value: ""
  # The parameter indicating that Kaspersky XDR is installed on the target host with
  limited computing resources.
  - name: low_resources
    source:
      value: "true"
```

```
# The number of disk volumes that are used to store the service data of Kaspersky XDR components and KDT&period; For the single-node deployment, set the parameter value to "1".
- name: default_class_replica_count
  source:
    value: "1"
# The parameter that indicates whether to run the secret storage in the High Availability (HA) mode&period; For the single-node deployment, set the parameter value to "false".
- name: openbao_ha_mode
  source:
    value: "false"
# The parameter that indicates whether to run the secret storage in the standalone mode&period; For the single-node deployment, set the parameter value to "true".
- name: openbao_standalone
  source:
    value: "true"
# Path to the KUMA inventory file that contains the installation parameters for deployment of the KUMA services.
- name: inventory
  source:
    value: "/home/user/inventory.yml"
# The path to the license key of KUMA Core&period; This file is located on the administrator host.
- name: license
  source:
    value: "/home/user/license.key"
# Domain name&period; The service host name and domain name are parts of FQDNs of the Kaspersky XDR services.
- name: smp_domain
  source:
    value: "smp.local"
# List of host names of the Kaspersky XDR services for which a self-signed or custom certificate must be generated.
- name: pki_host_list
  source:
    value: "admsrv api console kumamonitoring"
```

將 Kaspersky Next XDR Expert 從 2.2 版升級至 2.3 版

您可以使用 KDT，將 Kaspersky Next XDR Expert 從 2.2 版升級至 2.3 版。KDT會更新Kubernetes叢集、Kaspersky Next XDR Expert元件以及安裝在叢集外部KUMA目標主機上的KUMA服務。Kaspersky Next XDR Expert 升級過程的步驟不取決於所選的部署選項。

> 您只能按順序將解決方案升級到下一個主要版本。不支援跨多個主要版本升級。
> 熱修復程式不受此限制。您可以安裝目前主要版本中的任何熱修復程式，而無需安裝所有先前的熱修復程式。

若要升級Kaspersky Next XDR Expert：

1. 下載並解壓縮包含Kaspersky Next XDR Expert 2.3版本的分發套件。
2. 請閱讀Kaspersky Next XDR Expert元件分發包中的KDT最終使用者產品授權協議（EULA）。

   當您開始使用KDT時，即表示您確認已完整閱讀、瞭解並接受KDT的EULA條款。

   您可以在升級 Kaspersky Next XDR Expert 後閱讀 KDT 的 EULA。`license_kdt.txt` 檔案位於執行 Kaspersky Next XDR Expert 升級之使用者的 `~/kaspersky_eula` 目錄。
3. 執行以下命令升級Kaspersky Next XDR Expert：

   ```
   ./kdt apply -k <full_path_to_XDR_updates_archive>
   ```

   若要開始升級Kaspersky Next XDR Expert，您必須接受EULA和隱私權政策的條款。

   若使用 `--accept-eula` 旗標，即可在不提示閱讀 OSMP 的 EULA 與「隱私權政策」條款的情況下安裝 Kaspersky Next XDR Expert。此種情況下，您必須在升級 Kaspersky Next XDR Expert 之前閱讀 OSMP 的 EULA 與「隱私權政策」。這些檔案位於包含 Kaspersky Next XDR Expert 元件的分發套件中。透過使用 `--accept-eula` 旗標，您確認已完整閱讀、瞭解並接受 EULA 與「隱私權政策」的條款。

   若要在升級期間閱讀並接受 EULA 與「隱私權政策」的條款，請勿使用 `--accept-eula` 旗標。
4. 若未在前一步驟中使用 `--accept-eula` 旗標，請閱讀 OSMP 的 EULA 與「隱私權政策」。文字顯示在命令行視窗中。按空格鍵檢視下一個文字段。然後，當出現提示時，輸入以下值：

   a. 如果您瞭解並接受 EULA 的條款，請輸入 `y`。

      如果您不接受 EULA 的條款，請輸入 `n`。

   b. 若您瞭解並接受「隱私權政策」的條款，並且同意您的資料將依照「隱私權政策」所述進行處理和傳輸（包括傳輸到第三國），請輸入 `y`。

      如果您不接受「隱私權政策」的條款，請輸入 `n`。

   如果您不接受EULA和隱私權政策的條款，Kaspersky Next XDR Expert將不會升級。

   KDT執行更新並在主控台中顯示其進度。請等待更新完成。Kaspersky Next XDR Expert 已從 2.2 版升級至 2.3 版。
5. 從檔案匯入 OSMP 資源。

   該檔案位於以下路徑：opt/kaspersky/kuma/utils/

檔案密碼為：`w.zS81'ZdTgicHq;`

在**選取要匯入的資源**欄位中，您必須選取所有資源，然後清除**目的地** 核取方塊，以防止取代現有目的地。

已知問題與疑難排解：

如果您要升級至 2.3 版，且已設定由多個 OSMP 實例組成的階層，則子實例繼承的資源及在子實例中建立的資源可能不會顯示在父實例中。如果發生此情況，升級後請在子實例上重新儲存資源。或者，您可以將資源（secret 類型的資源除外）匯出，然後再匯入至相同租用戶。

遷移到 Kaspersky Next XDR Expert

本節介紹將資料從Kaspersky Security Center for Windows、KUMA和Kaspersky KEDR 7.1遷移到Kaspersky Next XDR Expert。

關於從卡巴斯基安全管理中心Windows遷移

依照此情境執行，您可以將管理群組結構、所包含的受管理裝置和其他群組物件（政策、工作、全域工作、標記和裝置分類）從 Kaspersky Security Center Windows 轉移到 Kaspersky Next XDR Expert 的管理之下。

限制：

- 您只能從 Kaspersky Security Center 14.2 Windows 移轉到 Kaspersky Next XDR Expert（自版本 1.0 起）。
- 您只能使用 Kaspersky Security Center Web 控制台來執行此情境。

階段

移轉情境分階段進行：

1. **選擇移轉方法**

   您是透過移轉精靈移轉到 Kaspersky Next XDR Expert。移轉精靈步驟取決於 Kaspersky Security Center Windows 與 Kaspersky Next XDR Expert 的管理伺服器是否已按階層排列：

   - 使用管理伺服器階層移轉

     如果 Kaspersky Security Center Windows 的管理伺服器是 Kaspersky Next XDR Expert 管理伺服器的從屬伺服器，請選擇此選項。您是在 OSMP 主控台內管理移轉程序以及伺服器之間的切換。如果您更喜歡此選項，可以將管理伺服器排列成階層以簡化遷移過程。為此，請在開始遷移之前建立層次結構。

     如果您將從屬管理伺服器連線至Kaspersky Next XDR Expert，請停用管理這些伺服器的網頁主控台的後台整合。

     若要停用後台整合：

     1. 登入管理伺服器網頁主控台。
     2. 在主功能表中，轉至**設定 → 整合**。
     3. 在**背景連線**部分，停用**整合的背景連線 已啟用**切換開關。

   - 使用匯出檔案（ZIP 存檔）進行移轉

     如果 Kaspersky Security Center Windows 與 Kaspersky Next XDR Expert 的管理伺服器未按階層排列，請選擇此選項。您是使用兩個主控台來管理移轉程序：一個是 Kaspersky Security Center Windows 適用的執行個體，另一個是 OSMP 主控台。在這個案例中，您將使用在從 Kaspersky Security Center Windows 匯出期間建立和下載的匯出檔案，將此檔案匯入到 Kaspersky Next XDR Expert。

2. **從卡巴斯基安全管理中心 Windows 匯出資料**

   開啟卡巴斯基安全管理中心 Windows，然後執行移轉精靈。

3. **將資料匯入到 Kaspersky Next XDR Expert**

   繼續執行移轉精靈將匯出的資料匯入到 Kaspersky Next XDR Expert。

   如果伺服器按階層排列，則在相同精靈中成功匯出後，匯入會自動開始。如果伺服器未按階層排列，您會在切換到 Kaspersky Next XDR Expert 後繼續執行移轉精靈。

4. **執行額外操作以手動將物件和設定從 Kaspersky Security Center Windows 傳輸到 Kaspersky Next XDR Expert（可選步驟）**

   您可能還想傳輸無法透過移轉精靈進行傳輸的物件和設定。例如，您也可以執行下列操作：

   - 設定管理伺服器的全域工作
   - 設定網路代理政策設定
   - 建立應用程式安裝套件
   - 建立虛擬伺服器
   - 分配和配置發佈點
   - 設定裝置移動規則。
   - 設定自動標記裝置規則
   - 建立應用程式類別

5. **將匯入的受管理裝置移到 Kaspersky Next XDR Expert 的管理之下**

   若要完成移轉，請將匯入的受管理裝置移到 Kaspersky Next XDR Expert 的管理之下。這可以透過下列其中一種方法進行：

   - 透過 Kaspersky Security Center 群組工作進行

     利用變更管理伺服器工作，將特定用戶端裝置的管理伺服器變更為另一台管理伺服器。

   - 透過 klmover 公用程式

     使用 klmover 公用程式並指定新管理伺服器的連線設定。

   - 透過在受管理裝置上安裝或重新安裝網路代理

     建立新的網路代理安裝套件，在安裝套件內容中指定新管理伺服器的連線設定。使用安裝套件透過遠端安裝工作在匯入的受管理裝置上安裝網路代理。

     您也可以建立並使用獨立安裝套件在本機安裝網路代理。

6. **將網路代理更新到最新版本**

   建議您將網路代理升級到與 Kaspersky OSMP 主控台相同的版本。

7. **確保受管理裝置在新管理伺服器上可見**

   在 Kaspersky Next XDR Expert 管理伺服器上，開啟受管理裝置清單（**資產管理** → **資產（裝置）**），然後檢查**可見**、**網路代理已安裝**與**上一次連線到管理伺服器**欄位中的值。

其他資料移轉方法

除了移轉精靈之外，您還可以傳輸特定工作和政策：

- 從卡巴斯基安全管理中心Windows匯出工作，然後將這些工作匯入到Kaspersky Next XDR Expert。
- 從卡巴斯基安全管理中心Windows匯出政策，然後將這些政策匯入到Kaspersky Next XDR Expert。相關政策設定檔被與所選政策一起匯出和匯入。

從卡巴斯基安全管理中心 Windows 匯出群組物件

遷移管理組結構，包括從Kaspersky Security Center Windows到Kaspersky Next XDR Expert的受管理裝置和其他群組物件，需要您首先選擇要匯出的資料並建立匯出檔案。匯出檔案包含有關要遷移的所有群組物件的資訊。匯出檔案將會用來後續匯入Kaspersky Next XDR Expert。

您可以匯出以下物件：

- 受管理應用程式的工作和政策
- 全域工作
- 自訂裝置分類
- 管理群組結構和包含的裝置
- 指派給轉移裝置的頁簽

開始匯出前，請閱讀有關遷移到Kaspersky Next XDR Expert的一般資訊。選擇遷移方法—透過使用或不使用卡巴斯基安全管理中心Windows和Kaspersky Next XDR Expert管理伺服器的層次結構。

透過遷移精靈匯出受管理裝置和相關群組物件：

1. 根據卡巴斯基安全管理中心Windows和Kaspersky Next XDR Expert的管理伺服器是否排列成層次結構，執行以下操作之一：
   - 如果伺服器排列成層次結構，開啟OSMP主控台，然後切換到卡巴斯基安全管理中心Windows的伺服器。
   - 如果伺服器未排列成層次結構，開啟連線到卡巴斯基安全管理中心 Windows 伺服器的卡巴斯基安全管理中心網頁主控台。
2. 在主功能表中，轉至**操作 → 移轉**。
3. 選擇**移轉到卡巴斯基安全管理中心 Linux 或者 Open Single Management Platform**以啟動精靈並按照其步驟操作。
4. 選取您要匯出的管理群組或子群組。請注意，所選的管理群組或子群組包含不超過 10,000 台裝置。

5. 選取您希望匯出其工作和政策的受管理應用程式。僅選取Kaspersky Next XDR Expert支援的應用程式。不受支援的應用程式的物件仍將被匯出，但它們將無法使用。

6. 使用左側的連結選取全域工作、裝置分類和要匯出的報告。**群組物件**連結允許您從匯出中排除自訂角色、內部使用者和安全群組以及自訂應用程式類別。

匯出檔案（ZIP 封存）已建立。根據您是否使用管理伺服器層次結構支援執行遷移，匯出檔案會被儲存如下：

- 如果伺服器排列成層次結構，匯出檔案將儲存到OSMP主控台伺服器上的臨時資料夾中。
- 如果伺服器未排列成層次結構，則匯出檔案將被下載到您的裝置。

對於具有管理伺服器層次結構支援的遷移，匯入會在成功匯出後自動開始。對於沒有管理伺服器層次結構支援的遷移，您可以手動將儲存的匯出檔案匯入Kaspersky Next XDR Expert。

將匯出檔案匯入Kaspersky Next XDR Expert

若要傳輸您從Kaspersky Security Center Windows匯出的受管理裝置、物件與其設定的相關資訊，您需將其匯入Kaspersky Next XDR Expert。

透過遷移精靈匯入受管理裝置和相關群組物件：

1. 根據卡巴斯基安全管理中心Windows和Kaspersky Next XDR Expert的管理伺服器是否排列成層次結構，執行以下操作之一：

   - 如果伺服器排列成層次結構，則在匯出完成後繼續執行移轉精靈的下一步。在此精靈中成功匯出後，匯入會自動開始（請參閱本說明的步驟 2）。
   - 如果伺服器未排列成層次結構：

     a. 開啟OSMP主控台。

     b. 在主功能表中，轉至**操作 → 移轉**。

     c. 選擇您在從卡巴斯基安全管理中心 Windows 匯出過程中建立並下載的匯出檔案（ZIP 存檔）。開始上傳匯出檔案。

2. 匯出檔案上傳成功後，即可繼續匯入。如果伺服器未排列成層次結構，則可以透過按一下**變更**鏈接，然後選擇所需檔案來指定另一個匯出檔案。

3. Kaspersky Next XDR Expert管理群組的整個層次結構將得以顯示。

   選中目標管理群組旁邊的核取方塊，匯出的管理群組的物件（受管理裝置、政策、工作和其他群組物件）必須還原到該目標管理群組。

4. 開始匯入群組物件。您無法最小化移轉精靈並在匯入期間執行任何並行作業。請等待片刻，直到物件清單中所有物件旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)，匯入隨即完成。

5. 完成匯入時，管理群組的匯出結構，包含裝置的詳細資料，會顯示在所選目標管理群組下。若您還原的物件名稱與現有物件名稱相同，前者會使用增量尾碼新增。

如果在遷移的工作中指定了執行該工作的帳戶的詳細資訊，則匯入完成後您必須開啟該工作並再次輸入密碼。

如果匯入已完成但出現錯誤，您可以執行以下操作之一：

- 對於具有管理伺服器層次結構支援的遷移，您可以再次開始匯入匯出檔案。在這種情況下，您必須按照步驟3中的說明選擇管理群組。
- 對於沒有管理伺服器層次結構支援的遷移，您可以啟動移轉精靈選擇另一個匯出檔案，然後再次匯入。

您可以檢查匯出範圍中包含的群組物件是否已成功匯入Kaspersky Next XDR Expert。為此，請轉到**資產管理**部分並確保匯入的物件出現在相應的子部分中。

請注意，匯入的受管理裝置會顯示在 **受管理裝置** 子區段中，但在網路上看不到這些裝置，而且這些裝置上未安裝或未執行網路代理（**可見**、**網路代理已安裝**及**上一次連線到管理伺服器**欄中顯示 *否*）。

若要完成遷移，您需要將受管理裝置切換至Kaspersky Next XDR Expert的管理範圍，如移轉至Kaspersky Next XDR Expert中的階段5所述。

將受管理裝置切換到Kaspersky Next XDR Expert的管理之下

將受管理裝置、物件及其設定的資訊成功匯入Kaspersky Next XDR Expert後，您需要將受管理裝置切換到Kaspersky Next XDR Expert的管理下才能完成遷移。

您可以透過以下方法之一將受管理裝置移至Kaspersky Next XDR Expert下：

- 使用 klmover 公用程式。
- 使用*變更管理伺服器*工作。
- 透過遠端安裝工作在受管理裝置上安裝網路代理。

要通過安裝網路代理程式將受管理裝置切換為由Kaspersky Next XDR Expert管理：

1. 刪除將在Kaspersky Next XDR Expert管理下切換的匯入受管理裝置上的網路代理程式。
2. 轉到 Kaspersky Security Center Windows 的管理伺服器。
3. 進入**軟體管理 → 安裝套件**，然後開啟網路代理現有安裝套件的屬性。

   如果套件清單中沒有網路代理安裝套件，請下載新的安裝套件。

   您也可以建立並使用獨立安裝套件在本機安裝網路代理。
4. 在**設定**頁簽上， 選擇**連線**部分。指定Kaspersky Next XDR Expert管理伺服器的連線設定。
5. 為匯入的受管理裝置建立遠端安裝工作，然後指定重新配置的網路代理安裝套件。

   您可以透過卡巴斯基安全管理中心 Windows 的管理伺服器或透過充當發佈點的 Windows 裝置安裝網路代理。如果您使用管理伺服器，請啟用**透過管理伺服器使用作業系統資源**選項。如果您使用發佈點，請啟用**透過發佈點使用作業系統資源**選項。
6. 執行遠端安裝工作。

遠端安裝工作成功完成後，轉至Kaspersky Next XDR Expert的管理伺服器並確保受管理裝置在網路中可見，並且網路代理程式已安裝並在其上執行（***可見***中的可見值、**網路代理已安裝**和**網路代理正在執行**列）。

關於從KEDR 7.1遷移

不支援將資料直接從 KEDR 7.1 移轉至 Kaspersky Next XDR Expert 2.3，因為 2.3 版與 2.1 版相比僅有些微功能差異。

若要將資料從 KEDR 7.1 移轉至 Kaspersky Next XDR Expert 2.3：

1. 安裝 Kaspersky Next XDR Expert 2.1。
2. 請依照 Kaspersky Next XDR Expert 2.1 說明 中的說明，執行從 KEDR 7.1 至 Kaspersky Next XDR Expert 2.1 的資料遷移。
3. 將 Kaspersky Next XDR Expert 從 2.1 版升級至 2.3 版。

設定和使用SIEM元件

本節提供有關安裝和設定 KUMA SIEM 系統的資訊。

KUMA服務

*服務*是KUMA的主要元件，可協助系統管理事件：服務可讓您從事件來源接收事件，然後將它們轉換為通用形式，以便於尋找關聯以及儲存和手動分析。每個服務由兩個協同工作的部分組成：

- 服務的一部分是在KUMA主控台內部基於服務資源集建立的。
- 服務的另一部分會作為 KUMA 元件之一，安裝在部署 KUMA 的網路基礎架構中。服務的伺服器部分可以由多個實例組成：例如，相同代理程式或儲存體服務可以同時安裝在多個裝置上。

  > 在伺服器端，KUMA 服務位於 `/opt/kaspersky/kuma` 目錄。

  在高可用性模式下安裝KUMA時，叢集中僅安裝KUMA Core。收集器、關聯器和儲存託管在Kubernetes叢集之外的主機上。

服務的各個部分透過服務ID相互連線。

服務類型：

- 收集器用於接收事件並將其轉換為KUMA格式。
- 關聯器用於分析事件並搜尋定義的模式。
- 儲存體用於保存事件。
- 代理程式用於接收遠端裝置上的事件並將其轉發到KUMA收集器。
- 事件路由器會從收集器和關聯器接收事件流，然後根據設定的篩選器將事件分發至目的地。

在KUMA主控台中，服務以表格形式顯示在**資源→活動服務**部分。可以透過點選**重新整理**按鈕更新服務表，並透過點選活動標頭按列排序。

表格大小不受限制。如果要選擇所有服務，請滾動到表尾，然後選中**選擇全部**核取方塊，該選項將選擇表格中的所有可用服務。

表列：

- **狀態**— 服務狀態：
  - 綠色表示服務正在執行。
  - 紅色表示服務未執行。
  - 黃色是適用於除代理程式之外所有服務的狀態。黃色狀態表示服務正在執行，但存在來自Victoria Metrics的錯誤或警示。您可以將滑鼠遊標停留在狀態上來檢視錯誤訊息。

- 紫色是適用於正在執行的服務的狀態，這些服務在資料庫中的組態檔已更改，但沒有其他錯誤。如果服務的組態檔不正確且發生錯誤（例如來自 VictoriaMetrics 的錯誤），則服務狀態為黃色。

- 灰色 - 如果已刪除的租用戶中存在仍在執行的服務，則該服務在**活動服務**頁面上將顯示為灰色狀態。灰色狀態的服務將保留，以便您複製ID並從伺服器移除服務。只有「主管理員」可以刪除灰色狀態的服務。刪除租用戶後，該租用戶的服務將分配給主租用戶。

- **類型**— 服務類型：**代理程式**、**收集器**、**關聯器**或**儲存體**。
- **名稱**— 服務名稱。按一下服務名稱即可開啟其設定。
- **版本**— 服務版本。
- **租用戶**— 擁有該服務的租用戶的名稱。
- **FQDN** — 服務伺服器的完全限定網域名稱。
- **IP位址**— 安裝服務的伺服器的IP位址。
- **API連接埠**— 遠端程序呼叫連接埠號碼。
- **正常執行時間** — 顯示服務執行的時間。
- **已建立**— 建立服務的日期和時間。

此表可以依升序和降序排序，也可以依**狀態**參數排序。若要對活動服務進行排序，請以滑鼠右鍵按一下快顯功能表並選擇一個或多個狀態。

您可以按一下**服務**視窗上部的按鈕以執行以下操作：

- 新增服務

  您可以基於現有服務資源集建立新服務。如果不先仔細規劃各種服務和使用者的租用戶間互動，我們不建議在主租戶之外建立服務。

- 重新整理

  您可以重新整理活動服務清單。

- 更新組態
- 重新啟動

若要對單一服務執行操作，請以滑鼠右鍵顯示服務以顯示其快顯功能表。以下功能可供使用：

- 重設憑證
- 刪除
- 下載日誌

  如果您想接收詳細資訊，請在服務設定中啟用偵錯模式。

- 複製服務ID

  您需要此ID來安裝、重新啟動、停止或刪除服務。

- 轉至事件

- 轉至活動清單
- 轉至快顯功能表
- 轉至分割區

若要變更服務，請在**資源→活動服務**下選擇一項服務。這會開啟一個視窗，其中包含建立該服務時所依據的資源集。您可以編輯資源集的設定並儲存變更。若要套用已儲存的更改，請重新啟動服務。

如果在變更收集器資源集的設定時，請變更或刪除與其連接的標準化器中的轉換，則編輯將不會儲存，且標準化器本身可能會損壞。如果需要修改已經是服務一部分的標準化器中的轉換，則必須直接在網頁介面中的**資源→標準化器**下對標準化器進行變更。

服務工具

本章節介紹 OSMP 的 **資源和服務 → 有效服務** 區段中可用來處理服務的工具。

獲取服務識別碼

服務識別碼用於將服務中駐留在 OSMP 內並安裝於網路基礎架構中的各個部分綁定為單一複合體。在 OSMP 中建立服務時，會為其指派一個識別碼，然後在將服務安裝到伺服器時使用此識別碼。

若要取得服務的識別碼：

1. 登入 OSMP 並開啟 **資源和服務 → 有效服務**。
2. 選中要取得其ID的服務旁的核取方塊，然後按一下**複製ID**。

   服務的識別碼將被複製到剪貼簿。例如，可以使用此 ID 在伺服器上安裝服務。

停止、啟動和檢查服務狀態

管理 OSMP 時，您可能需要執行下列操作。

- 暫時停止服務。例如，從備份還原Core時，或編輯與作業系統相關的服務設定時。
- 啟動服務。
- 檢查服務狀態。

下表列出管理 OSMP 時可能有用的命令。

用於停止、啟動和檢查服務狀態的命令

服務	停止服務	啟動服務	檢查服務狀態
核心	`sudo systemctl stop kuma-core.service`	`sudo systemctl start kuma-core.service`	`sudo systemctl status kuma-core.service`
具有ID的服務： • 收集器 • 關聯器 • 儲存體	`sudo systemctl stop kuma-<collector/correlator/storage>-<服務ID>.service`	`sudo systemctl start kuma-<collector/correlator/storage>-<服務ID>.service`	`sudo systemctl status kuma-<collector/correlator/storage><服務ID>.service`
沒有ID的服務： • kuma-grafana.service • kuma-mongodb.service • kuma-victoria-metrics.service • kuma-vmalert.service	`sudo systemctl stop kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl start kuma-<grafana/victoria-metrics/vmalert>.service`	`sudo systemctl status kuma-<grafana/victoria-metrics/vmalert>.service`
Windows代理程式	若要停止代理服務： 1. 在KUMA主控台中複製代理程式ID。 2. 連線到要啟動KUMA代理服務的主機。 3. 以具有系統管理權限的使用者身分執行 PowerShell™。 4. 在PowerShell中執行以下命令：`Stop-Service -Name "WindowsAgent-<代理 ID>"`	若要啟動代理服務： 1. 在KUMA主控台中複製代理程式ID。 2. 連線到要啟動KUMA代理服務的主機。 3. 以具有管理員權限的使用者身分執行PowerShell。 4. 在PowerShell中執行以下命令：`Start-Service -Name "WindowsAgent-<代理 ID>"`	若要檢視代理服務的狀態： 1. 在Windows中，轉至開始 → 服務選單，然後在服務清單中雙擊相關的KUMA代理程式。 2. 這將開啟一個視窗；在該視窗中在服務狀態欄位中檢視代理程式的狀態。

重新啟動服務。

重新啟動服務：

1. 登入 OSMP，然後開啟 **資源和服務 → 有效服務**。

2. 勾選服務旁邊的核取方塊並選擇必要的選項：

   - **更新配置**— 對正在運作的服務配置執行熱更新。例如，您可以透過這種方式變更欄位對應設定或目標點設定。

   - **重新啟動**— 停止服務並重新啟動。此選項用於修改連接埠號碼或連接器類型。

     重新啟動 OSMP 代理：

     - 只有當 OSMP Windows 代理在遠端電腦上執行時，才能依照上述方式將其重新啟動。如果遠端電腦上的服務處於非作用中狀態，則嘗試從 OSMP 重新啟動時會收到錯誤。在這種情況下，您必須在遠端 Windows 電腦上重新啟動 OSMP Windows 代理服務。有關重新啟動Windows服務的信息，請參閱特定於遠端Windows電腦作業系統版本的文件。

     - 使用此選項時，OSMP Linux 代理將停止。要再次啟動代理程式，必須執行用於啟動它的命令。

   - **重置憑證** - 刪除服務用於內部通訊的憑證。此選項不可用於續訂核心憑證。若要更新 KUMA 核心憑證，必須重新簽發這些憑證。

刪除Windows代理程式憑證的特殊注意事項：

- 如果代理處於綠色狀態且您選擇**重置憑證**，OSMP 會刪除目前的憑證並建立新憑證，代理會繼續使用新憑證運作。
- 如果代理處於紅色狀態且您選擇**重置憑證**，OSMP 會產生代理未執行的錯誤。在%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<agent ID>\憑證資料夾中，手動刪除internal.cert 和internal.key文件，然後手動啟動代理程式。代理程式啟動時，會自動建立新憑證。

刪除Linux代理程式憑證的特殊注意事項：

1. 無論代理程式狀態如何，都套用網頁介面中的**重設憑證**選項以刪除資料庫中的憑證。
2. 在代理程式安裝資料夾/opt/kaspersky/agent/<Agent ID>/憑證中，手動刪除internal.cert和internal.key檔案。
3. 由於**重置憑證**選項會停止代理程式，因此要繼續其運作，請手動啟動代理程式。代理程式啟動時，會自動建立新憑證。

刪除服務

刪除服務之前，請獲取其ID 。刪除伺服器的服務時需要此ID。

若要在 OSMP 中移除服務：

1. 登入 OSMP 並開啟 **資源和服務 → 有效服務**。
2. 選中您要刪除之政策旁的核取方塊並點選**刪除**。
   確認視窗隨即開啟。
3. 點擊**確定**。

此服務已從 OSMP 中刪除。

若要從伺服器中刪除服務，請執行以下命令：

```
sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage> --id <服務 ID> --uninstall
```

該服務已從伺服器中刪除。

檢視活動查詢清單

主管理員可以檢視其他使用者的查詢，以及目前正在執行的 OSMP 資源。

若要檢視活動查詢表：

1. 在主應用程式視窗中，轉到**監控中→資源和服務→活動服務**部分。
2. 選取相關儲存體旁邊的核取方塊。

3. 在工具欄或選單（⋮）中，按一下**有效查詢**。

   這將打開一個窗口，其中包含**ClickHouse 有效查詢**表。選擇多個儲存體時，表格會顯示來自每個選定儲存體的活動查詢。

資源表包含以下列：

- **啟動時間**顯示查詢啟動的日期和時間。
- **建立者**顯示查詢的發起者。對於使用者查詢，將顯示使用者名稱。對於**資源**類型的查詢，將顯示資源名稱。
- **查詢**是在ClickHouse中執行的SQL查詢文字。
- **類型**是查詢的類型。有下列查詢類型可用：
  - **後台執行**表示使用者使用**在背景執行**按鈕在背景啟動了查詢。
  - **資源**表示由 OSMP 資源發起的內部 SQL 查詢，例如在資料處理或分析期間。
  - **使用者**表示使用者使用**執行查詢**按鈕啟動並正常執行的SQL查詢。
- **儲存體**是執行查詢的ClickHouse儲存體的名稱。

點擊 ⚙ 按鈕以設定查詢表中顯示的直欄。如有必要，您可以透過點擊 ↻ 強制更新資料。

如果您想按特定直欄對查詢進行排序，請點擊其標題，然後在下拉清單中選擇一個可用選項：**升序**或**降序**。

如有必要，您可以取消查詢。

若要取消查詢：

1. 開啟**ClickHouse 有效查詢**表。
2. 選取查詢旁邊的核取方塊，然後按一下**取消查詢**。

   確認視窗隨即開啟。您也可以在**指定理由**欄位中指定取消查詢的原因。
3. 點擊**確定**。

查詢已取消並從表中刪除。稽核事件隨即自動產生。

分割區視窗

如果儲存體服務已建立並安裝，您可以在**分割區**表中檢視其分割區。

*若要開啟**分割區**表：*

1. 登入 OSMP 並開啟 **資源和服務** → **有效服務**。
2. 選中相關儲存體旁的核取方塊，然後按一下**前往磁碟分割頁面**。

分割區表隨即開啟。

此表包含以下列：

- **租用戶**– 擁有儲存資料的租用戶的名稱。
- **已建立**– 分割區建立的日期。
- **空間**– 空間的名稱。
- **大小**– 空間的大小。
- **事件**– 儲存的事件數。
- **傳輸到冷儲存**– 資料從ClickHouse叢集遷移到冷儲存磁碟的日期。
- **過期日期**– 分割區過期的日期。在此日期之後，分割區及其包含的事件將不再可用。

您可以刪除分割區。

若要刪除分割區：

1. 開啟**分割區**表（見上文）。
2. 選取所需分割區左側的核取方塊。
3. 選擇**刪除**。
   確認視窗隨即開啟。
4. 點擊**確定**。

此分割區已刪除。稽核事件分割區無法刪除。

搜尋相關事件

您可以搜尋由關聯器或收集器服務處理的事件。

若要搜尋與關聯器或收集器服務相關的事件：

1. 登入 OSMP 並開啟 **資源和服務** → **有效服務**。
2. 選中所需關聯器或收集器旁的核取方塊，然後按一下**轉至事件**。
   一個新的瀏覽器頁籤隨即開啟，其中開啟了 OSMP **事件**區段。
3. 若要尋找事件，請按一下 圖示。
   將會顯示一個資料表，其中包含透過搜尋運算式 `ServiceID = <所選服務的 ID>` 篩選出的事件。

服務資源集

*服務資源集*是一種資源類型、OSMP 元件，也是一組設定，OSMP 服務會根據這些設定建立並運作。服務的資源集合是資源的集合。

新增至資源集的任何資源，都必須由擁有所建立資源集的同一租用戶擁有。共用租用戶是一個例外，其擁有的資源可用於其他租用戶的資源集。

服務的資源集顯示在 OSMP 的 **資源和服務 → <服務的資源集類型>** 區段中。可用類型：

- 收集器。
- 關聯器。
- 儲存體
- 代理程式。

選擇所需類型後，將開啟一個表，其中包含此類型服務的可用資源集。資源表包含以下列：

- **名稱**— 資源集的名稱。可用於搜尋和排序。
- **已更新**— 資源集上次更新的日期和時間。可用於排序。
- **建立者**— 建立資源集的使用者的名稱。
- **描述**— 資源集的描述。

建立儲存體

儲存體由兩部分組成：一部分在 OSMP 內建立，另一部分安裝在用於儲存事件的網路基礎架構伺服器上。OSMP 儲存體的伺服器部分由彙集成叢集的 ClickHouse 節點組成。ClickHouse叢集可以補充冷儲存磁碟。

每個ClickHouse叢集都必須安裝單獨的儲存體。

在建立儲存之前，請仔細規劃叢集結構並部署必要的網路基礎架構。選擇ClickHouse叢集組態時，請考慮組織的特定事件儲存需求。

我們建議使用 ext4 檔案系統。

儲存體透過幾個步驟建立：

1. **在OSMP中為儲存體建立資源集**
2. **在OSMP中建立儲存服務**
3. **在網路基礎架構中安裝儲存體節點**

建立儲存體叢集節點時，請驗證系統的網路連線並開啟元件所使用的連接埠。

如果變更了儲存體設定，則必須重新啟動服務。

ClickHouse叢集結構

ClickHouse*叢集*是擁有所有彙總的標準化KUMA事件的邏輯裝置群組。它由一個或多個邏輯*分片*組成。

*分片*是擁有叢集中彙總的所有標準化事件的特定**部分**的邏輯裝置群組。它由一個或多個*複本*組成。增加分片的數量可以讓您執行以下操作：

- 透過增加伺服器總數和磁碟空間來彙總更多事件。
- 透過分配與大量新事件相關的負荷來吸收更大的事件**流**。
- 透過在多個裝置之間分配搜尋區域來減少搜尋事件所需的時間。

*複本*是邏輯分片的一部分，擁有該分片資料的單一副本。如果存在多個複本，則表示存在多個副本（資料被複製）。增加複本的數量可以讓您執行以下操作：

- 提高容錯能力。
- 將資料搜尋相關的總負載分散到多台機器上（但若要達到此目的，最好增加分片數量）。

*keeper*是參與**協調整個**叢集層級資料複製的裝置。每個叢集至少需要一個裝置擔任此角色。建議3個裝置擔任此角色。參與協調複製的裝置數量必須是**奇數**。*keeper*和*複本*角色可以組合在同一個裝置上。

ClickHouse叢集節點設定

在建立儲存體之前，請仔細規劃叢集結構並部署必要的網路基礎架構。選擇ClickHouse叢集組態時，請考慮組織的特定事件儲存需求。

建立ClickHouse叢集節點時，請驗證系統的網路連線並開啟元件所使用的連接埠。

對於ClickHouse叢集的每個節點，您需要指定以下設定：

- 完全限定網域名稱 (FQDN) — 存取節點的唯一位址。請指定完整的 FQDN，例如 `kuma-storage.example.com`。
- 分片ID、複本ID和keeper ID - 這些設定的組合決定了節點在ClickHouse叢集結構中的位置和節點角色。

節點角色

節點的角色取決於指定的設定：

- 分片、複本、keeper—節點參與標準化KUMA事件的累積和搜索，並幫助協調叢集範圍的資料複製。
- 分片、複本 - 節點參與標準化KUMA事件的累積和搜尋。
- keeper - 節點**不**彙總標準化事件，但協助協調叢集範圍的資料複製。必須在**資源→儲存體→** <儲存體> **→基本設定→ClickHouse 叢集節點**部分清單的開頭指定專用keeper。

ID需求：

- 如果在同一個叢集中建立多個分片，則分片ID在該叢集內必須是唯一的。
- 如果在同一個分片中建立多個複本，則複本ID在該分片內必須是唯一的。
- Keeper ID在叢集內必須是唯一的。

ClickHouse叢集節點ID的範例：

- 分片1，複本1，keeper 1；
- 分片1，複本2；
- 分片2，複本1；
- 分片2，複本2，keeper 3；
- 分片2，複本3；
- keeper 2。

事件的冷儲存

在 OSMP 中，您可以設定將舊版資料從 ClickHouse 叢集遷移至冷儲存。冷儲存可以使用作業系統中掛載的本機磁碟、Hadoop分散式檔案系統（HDFS）或S3雲端儲存服務（Simple Storage Service）來實現。

從 OSMP 2.1 版開始，儲存在 HDFS 磁碟上的資料將逐步遷移至 S3 雲端儲存。在應用程式的未來版本中，將停止對HDFS檔案系統的支援。

當至少指定一個冷儲存磁碟時，即可啟用冷儲存。如果使用多個儲存體，則必須在每個包含資料的節點上，按照儲存體組態中指定的路徑掛載一個冷儲存磁碟或一個HDFS或S3磁碟。如果未配置冷儲存磁碟，且伺服器的熱儲存磁碟空間不足，則儲存服務將停止。如果同時設定了熱儲存和冷儲存，且冷儲存磁碟空間耗盡，OSMP 儲存服務將停止。我們建議透過在熱存儲中添加自訂事件儲存條件來避免這種情況。

可以新增或刪除冷儲存磁碟。如果您新增了多個冷儲存磁碟，資料將以循環方式寫入這些磁碟。如果要寫入磁碟的資料所佔用的空間超過該磁碟上的可用空間，則這些資料以及所有後續資料將循環寫入下一個冷儲存磁碟。如果您只新增了兩個冷儲存磁碟，資料將寫入剩餘可用空間的磁碟機。

變更冷儲存設定後，必須重新啟動儲存服務。如果服務無法啟動，原因會顯示在儲存日誌中。
如果 S3 儲存的路徑指定不正確，也需要重新啟動服務。請注意，建立的*儲存體.xml*檔案不會自動刪除。您需要手動清空 `/opt/kaspersky/kuma/clickhouse/cfg/config.d/` 資料夾，並重新設定冷儲存。

如果儲存設定中指定的冷儲存磁碟不可用（例如，故障），則可能導致儲存服務運作出錯。在這種情況下，請重新建立具有相同路徑（對於本機磁碟）或相同位址（對於HDFS和S3磁碟）的磁碟，然後將其從儲存設定中移除。

將資料移至冷儲存磁碟的規則

您可以透過根據保留時間或最大儲存大小設定限制來配置ClickHouse叢集熱儲存中事件的儲存條件。使用冷儲存時，OSMP 每隔 15 分鐘以及每次 Core 重新啟動後，都會檢查是否符合指定的儲存條件：

1. OSMP 取得受檢查儲存的分割區，並依冷儲存磁碟和空間將分割區分組。
2. 對於每個空間，OSMP 會檢查是否符合指定的儲存條件。
3. 如果符合條件（例如，空間包含已超過保留時間的資料，或儲存大小已達到或超過條件中指定的限制），OSMP 會將日期最早的所有分割區移至冷儲存磁碟；如果未設定冷儲存磁碟或設定不正確，則會刪除這些分割區。只要空間中設定的儲存條件仍然滿足，就會重複此操作；例如，如果在刪除某個日期的分割區後，儲存大小仍然超過條件中指定的最大大小。

   OSMP 會在資料傳輸開始和結束時，或刪除資料時，產生稽核事件（稽核事件、稽核事件）。
4. 如果在 OSMP 中配置了保留時間，則每當分割區移至冷儲存磁碟時，都會檢查磁碟是否符合所配置的條件。如果在磁碟上找到儲存時間超過**事件保留時間**的事件（該時間從 OSMP 收到事件時起計算），解決方案會刪除這些事件或日期最早的所有分割區。

   刪除資料時，OSMP 會建立稽核事件（稽核事件、稽核事件）。

如果ClickHouse叢集的磁碟已使用97%，則最大的分割區要麼自動轉移到冷儲存磁碟，要麼在沒有冷儲存磁碟的情況下被刪除。

在資料傳輸期間，儲存服務會保持運作，且其在 OSMP Web 介面的**資源 → 作用中服務**區段中會維持綠色狀態。將滑鼠游標停留在狀態圖示上時，會顯示有關資料傳輸的訊息。當刪除冷儲存磁碟時，儲存服務狀態為黃色。

儲存和存取事件的特殊協助工具注意事項

- 使用HDFS磁碟進行冷儲存時，請透過以下方式之一保護您的資料：
  - 在VLAN中設定單獨的實體介面，該介面僅用於HDFS磁碟和ClickHouse叢集。
  - 設定網路分段和流量過濾規則，以排除對HDFS磁碟的直接存取或攔截來自ClickHouse的磁碟流量。

- 位於 ClickHouse 叢集和冷儲存磁碟上的事件同樣可在 OSMP Web 介面中存取。例如，當您搜尋事件或查看與警示相關的事件時。
- 您可以停用冷儲存磁碟上事件或稽核事件的儲存。為此，請在儲存設定中指定以下內容：
  - 如果您不想將事件儲存在冷儲存磁碟上，請執行下列其中一項操作：
    - 若在**保留政策選項**欄位中選取了以GB或百分比為單位的儲存條件，請於**事件保存時間**欄位中指定 `0`。
    - 如果在**保留政策選項**欄位中選取了以天為單位的儲存條件，請在**事件保存時間**欄位中指定與**保留政策選項**欄位中相同的天數。
  - 若不想將稽核事件儲存在冷儲存磁碟上，請於**稽核冷保留期**欄位中指定 `0`（天）。

使用HDFS磁碟的特殊注意事項

- 在連接HDFS磁碟之前，請先於磁碟上為ClickHouse叢集的每個節點建立目錄，格式如下：`<HDFS disk host>/<shard ID>/<replica ID>`。例如，叢集包含兩個節點，每個節點持有同一分片的兩個副本，則必須建立以下目錄：
  - hdfs://hdfs-example-1:9000/clickhouse/1/1/
  - hdfs://hdfs-example-1:9000/clickhouse/1/2/

  ClickHouse叢集節點中的事件將移轉到名稱包含其分片和副本ID的目錄中。如果您變更這些節點設定而沒有在HDFS磁碟上建立對應的目錄，則遷移過程中可能會遺失事件。
- 新增至儲存的HDFS磁碟以JBOD模式運作。這意味著如果其中一個磁碟發生故障，您將無法存取協助工具儲存體。使用HDFS時，請考慮高可用性並設定RAID，並將來自不同副本的資料儲存在不同的裝置上。
- 將事件記錄到HDFS的速度通常低於將事件記錄到本機磁碟的速度。通常，在HDFS中存取事件的速度明顯低於在本機磁碟上存取事件的速度。當同時使用本機磁碟和HDFS磁碟時，資料將依序寫入它們。
- HDFS僅用作ClickHouse的分散式檔案資料的儲存體。使用ClickHouse的壓縮機制（而非HDFS）來壓縮資料。
- ClickHouse伺服器必須具有對應HDFS儲存的寫入存取權限。

移除冷儲存磁碟

在實體斷開冷儲存磁碟之前，請從儲存體設定中刪除這些磁碟。

若要從儲存體設定中刪除磁碟：

- 在 OSMP 中，於 **資源和服務 → 儲存空間** 下，選取相關的儲存體。

  儲存體隨即開啟。

- 在視窗的**冷儲存空間的磁碟**部分中，在所需磁碟的設定群組中，按一下**刪除磁碟**。

  已刪除磁碟中的資料將自動遷移到其他冷儲存磁碟，如果沒有這樣的磁碟，則遷移到ClickHouse叢集。在資料遷移期間，儲存體狀態圖示以黃色突出顯示。資料傳輸開始和結束時，會產生稽核事件（稽核事件、稽核事件）。

- 事件遷移完成後，磁碟將自動從儲存設定中刪除。現在可以安全地斷開連線。

已移除的磁碟仍可能包含事件。如果要刪除它們，可以使用DROP PARTITION命令手動刪除資料分割區。

如果儲存設定中指定的冷儲存磁碟不可用（例如，故障），則可能導致儲存服務運作出錯。在這種情況下，請建立具有相同路徑（對於本機磁碟）或相同位址（對於HDFS磁碟）的磁碟，然後將其從儲存設定中刪除。

中斷連線、封存及連線磁碟分割

如果要最佳化磁碟空間並加快OSMP中的查詢速度，您可以在ClickHouse中分離資料分割區、對分割區建立壓縮檔案，或將分割區移至磁碟機。如有必要，您可以稍後重新附加所需的分割區並執行資料處理。

分離分割區

若要分離分割區：

1. 決定要分離分割區的所有副本上的分片。
2. 使用下列指令取得分割區ID：

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "SELECT partition, name FROM system.parts;" |grep 20231130
   ```

   在此範例中，該指令傳回2023年11月30日的分割區ID。
3. 對於分片的每個副本，使用以下命令並指定分割區ID來分離分割區：

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 DETACH PARTITION ID '<partition ID>'"
   ```

因此，分片的所有副本上的分割區都被分離。現在，您可以將資料目錄移至磁碟機或存檔分割區。

存檔分割區

若要存檔已分離的分割區：

1. 在伺服器的磁碟子系統中找到已分離的分割區：

   ```
   sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <ID of the detached partition>\*
   ```

2. Change to the 'detached' directory that contains the detached partition, and while in the 'detached' directory, perform the archival:

   ```
   sudo cd <path to the 'detached' directory containing the detached partition>
   sudo zip -9 -r detached.zip *
   ```

   例如：

```
sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
sudo zip -9 -r detached.zip *
```

該分割區隨即歸檔。

附加分割區

若要將壓縮檔案中的分割區附加到 OSMP：

1. 增加**保存期間**值。

   OSMP 會依據時間戳記欄位中指定的日期（記錄收到事件的時間）以及您為儲存體設定的**保留期間**值刪除資料。

   在恢復歸檔資料之前，請確保**保存期限**值與時間戳記欄位中的日期重疊。如果不是這種情況，歸檔資料將在1小時內刪除。

2. 將分割區的壓縮檔案放置在儲存體的「detached」區段，然後解壓縮該壓縮檔案：

   ```
   sudo  unzip detached.zip -d <path to the 'detached' directory>
   ```

   例如：

   ```
   sudo  unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   ```

3. 執行命令以附加分區：

   ```
   sudo /opt/kaspersky/kuma/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<partition ID>'"
   Repeat the steps of extracting the archive and attaching the partition on each replica of the shard.
   ```

因此，歸檔分割區隨即附加，且其事件再次可供搜尋。

為儲存體建立資源集

在 OSMP Web 介面中，會根據儲存體的資源集建立儲存服務。

若要在 OSMP Web 介面中為儲存體建立資源集：

1. 在 OSMP 中，於 **資源 → 儲存體** 區段，按一下 **新建**。

   這將開啟**建立儲存空間**視窗。

2. 在**基本設定**頁籤的**儲存體名稱**欄位中，輸入要建立的服務的唯一名稱。該名稱必須包含1到128個Unicode字元。

3. 在**租用戶**下拉清單中，選擇將擁有該儲存空間的租用戶。

4. 在**標籤**下拉清單中，選擇要建立的資源集的標籤。

   此清單包含在資源的租用戶和共享租用戶中建立的所有可用標籤。您可以透過在欄位中輸入其名稱來在清單中找到標籤。如果您輸入的標籤不存在，可以按下**Enter**鍵或按一下**新增**以建立該標籤。

5. 您可以選擇在**描述**欄位中新增最多256個Unicode字元來描述服務。

6. 在**保留政策選項**欄位中，在ClickHouse群集中為儲存體選擇一個事件儲存條件，如果滿足該條件，將導致事件傳輸到冷儲存磁碟，如果冷儲存未設定或設定不正確，則事件將被刪除。此條件適用於預設空間以及已刪除空間中的事件。

   預設情況下，ClickHouse會將事件移動到冷儲存磁碟，或者如果儲存體已滿97%，則會將其刪除。OSMP 在建立儲存體時也會套用額外的 **365 天**儲存條件。您可以設定自訂儲存條件，以使儲存體的效能更穩定。

   若要設定儲存條件，請執行下列其中一項操作：

   - 如果要限制事件的儲存週期，請從下拉清單中選擇**天數**，然後在欄位中指定ClickHouse熱儲存叢集中的最大事件儲存週期（以天為單位）。

     在指定的週期之後，事件將自動傳輸到冷儲存磁碟或從ClickHouse叢集中刪除，從日期最早的分割區開始。最小值是1。預設值是365。

     對於 [OOTB] 儲存體，預設事件儲存週期為兩天。如果要使用此儲存體，可以根據需要變更其事件儲存條件。

   - 如果要限制最大儲存大小，請從下拉清單中選擇**GB** ，然後在欄位中指定最大儲存大小（以 GB 為單位）。

     當儲存達到指定大小時，事件將自動傳輸到冷儲存磁碟或從ClickHouse叢集中刪除，從日期最早的分割區開始。最小值和預設值是1。

   - 如果要將儲存大小限制為儲存體可用磁碟空間的百分比，請從下拉清單中選擇**百分比**，並將最大儲存大小指定為可用磁碟空間的百分比。

     > 您可以透過傳送`'SELECT hostname(), name, total_space FROM system.disks'`查詢，從ClickHouse取得有關可用磁碟空間的資訊。

     當儲存達到其可用磁碟空間的指定百分比時，事件將自動傳輸到冷儲存磁碟或從ClickHouse叢集中刪除，從日期最早的分割區開始。可能的值：1到95。預設值是80。如果要對所有儲存空間使用百分比，則所有空間條件中的百分比總和不得超過95，但我們建議為整個儲存體或單一空間指定最多90%的限制。

     我們不建議指定低於 5% 的值，因為這會增加儲存體中資料遺失的可能性。

     > 如果儲存體是叢集式的，則每個伺服器的已佔用磁碟空間量都是單獨確定的。儲存的資料可能在伺服器上的磁碟之間分佈不均。當*叢集中的任何一部伺服器*達到儲存大小上限時，OSMP 會將事件推送至冷儲存磁碟或刪除事件。

確定已佔用儲存空間大小的演算法

已佔用儲存空間的大小以以下方式決定：

1. 從所有可用的副本中取得有關KUMA磁碟和分割區狀態的資訊。
2. 如果佔用空間超過設定值，KUMA將根據資料儲存類型（熱儲存或冷儲存）採取相應措施。

   對於熱儲存，將對每個可用節點和空間執行以下操作：

   a. 計算副本上該空間各分區的總大小。

   b. 計算副本上的最大空間大小：

   - 如果將儲存大小設定為以GB為單位的絕對值，則副本上的最大空間大小會如下計算：

     `<最大空間大小> = <設定的閾值> / <叢集中的副本數>`

例如，考慮一個包含三個分片的叢集，每個分片包含兩個副本；設定6GB的閾值，且每個副本上的最大資料大小為1GB。

- 如果將儲存大小設為百分比的相對值，則副本上的最大空間計算如下：
  `<最大空間大小> = <副本上的空間大小> / <副本磁碟大小> * 100%`。

  副本磁碟的大小不包括為 `ext4` 預留的空間。

如果超過指定的閾值，主機上的分割區將被刪除或移至冷儲存。所有分片上的分割區都將被刪除。

對於冷儲存，將根據KUMA中設定的事件保留期間（TTL），為每個可用空間刪除分割區。

7. 如果要使用其他儲存條件，請按一下**新增政策選項**並依照步驟6中的說明指定其他儲存條件。
   條件的最大數量為兩個，並且您只能組合以下類型的條件：

   - 天數和儲存大小（以GB為單位）
   - 天數和儲存大小（以百分比為單位）

   如果要移除儲存條件，請按一下此條件旁邊的X圖示。

8. 在**稽核保存週期**欄位中，指定儲存稽核事件的週期（以天為單位）。最小值與預設值皆為 `365`。

9. 如果需要冷儲存，請指定事件儲存時間段：

   - **事件保留時間**指定 OSMP 事件的總儲存期間（以天為單位），從收到事件的時間開始計算。當指定的時間段到期時，事件將自動從冷儲存磁碟中刪除。預設值是0。

     事件保留時間的計算方法是ClickHouse熱儲存叢集中事件保留時間的總和，直到觸發**保留政策選項**設定中指定的條件，以及冷儲存磁碟上的事件保留時間。當其中一個儲存條件觸發後，最早日期的資料分割區將移至冷儲存磁碟，並保留在該處，直到 OSMP 中的事件保留時間到期。

     根據指定的儲存條件，最終的保存時間如下：

     - 如果以天為單位指定儲存條件，則**事件保存時間**必須嚴格大於儲存條件中指定的天數。您可以將事件的冷保留期計算為**事件儲存時間**減去**保留政策選項**設定中指定的天數。

       如果您不想將事件儲存在冷儲存磁碟上，則可以在**事件保存時間**欄位中指定與儲存條件相同的天數。

     - 如果您以磁碟大小（絕對值或百分比）指定儲存條件，則**事件保存時間**的最小值為1。事件的冷儲存持續時間計算為**事件保存時間**減去從收到事件到觸發條件和磁碟分割區填充的天數，但在觸發條件之前，無法計算準確的持續時間。在這種情況下，我們建議為**事件保存時間**指定一個相對較大的值，以避免事件被刪除。

       如果您不想將事件儲存在冷儲存磁碟上，可以將**事件保存時間**設為0。

   - **稽核冷保存週期**—儲存稽核事件的天數。最小值是0。

   只有在添加了至少一個冷儲存磁碟後，**事件保留時間**和**稽核冷保留期**設定才可用。

10. 如果要變更ClickHouse設定，請在**ClickHouse 設定覆寫**欄位中，貼上ClickHouse組態XML檔案/opt/kaspersky/kuma/clickhouse/cfg/config.xml的設定行。無需指定根元素<yandex>，</yandex>。此欄位中傳遞的設定將取代預設設定。

    範例：

    <merge_tree>

<parts_to_delay_insert>600</parts_to_delay_insert>

<parts_to_throw_insert>1100</parts_to_throw_insert>

</merge_tree>

如果想要加快圖表分析和威脅搜尋速度，您可以更改ClickHouse壓縮演算法。預設使用ZSTD演算法。您可以將預設設定替換為LZ4。為此，請在**ClickHouse 設定覆寫**欄位中，如下指定壓縮演算法：

```
<compression>
  <case>
    <method>lz4</method>
  </case>
<compression>
```

> 解決方案將在儲存服務重新啟動後開始應用LZ4演算法。更改演算法之前儲存在儲存體中的所有事件仍將使用ZSTD演算法進行壓縮。

11. 使用**偵錯**切換開關指定是否必須啟用資源日誌記錄。如果希望僅記錄所有KUMA元件的錯誤，請停用偵錯。如果要在日誌中取得詳細信息，請啟用偵錯。

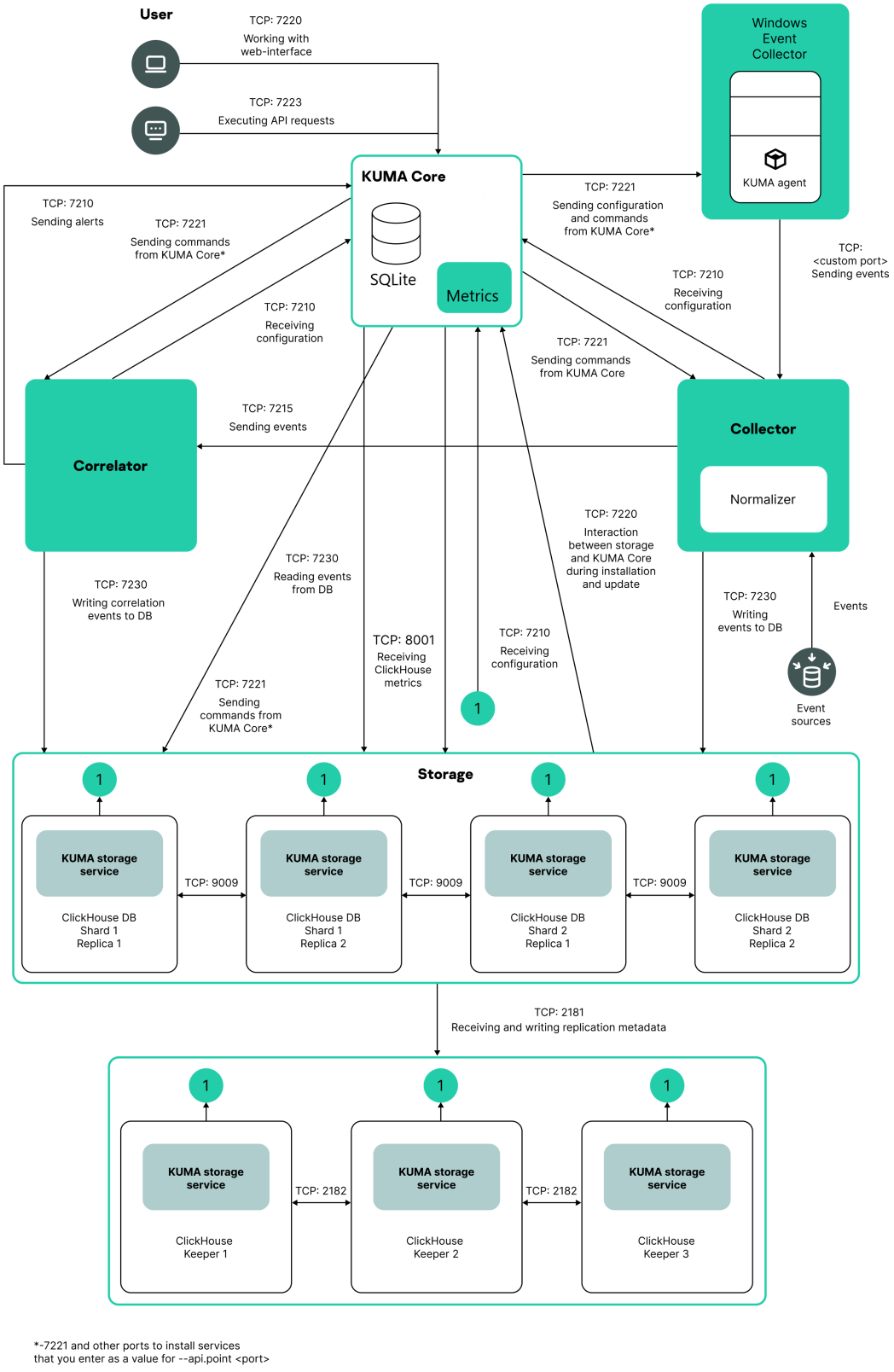
12. 如有需要，請在 **ClickHouse 叢集節點**區段中，將 ClickHouse叢集節點新增至儲存體。

    可以有多個節點。您可以透過點擊**新增節點**按鈕來新增節點，或透過點擊相關節點的X圖示刪除節點。

    可用設定：

    - 在**FQDN**欄位中，輸入要新增之節點的完全限定網域名稱。例如，`kuma-storage-cluster1-server1.example.com`。
    - 在**Shard ID**，**複本 ID**和**Keeper ID**欄位中，指定節點在ClickHouse叢集中的角色。分片和Keeper ID在叢集內必須是唯一的，副本ID在分片內必須是唯一的。以下範例展示如何在分散式安裝中為具有專用儲存體節點的儲存填入**ClickHouse 叢集節點**區段。您可以根據需要調整此範例。

分散式安裝圖



分散式安裝圖

範例：

ClickHouse 叢集節點

FQDN: kuma-storage-cluster1-server1.example.com

分片ID: 0

副本ID: 0
Keeper ID: 1
FQDN: kuma-storage-cluster1server2.example.com
分片ID: 0
副本ID: 0
Keeper ID: 2
FQDN: kuma-storage-cluster1server3.example.com
分片ID: 0
副本ID: 0
Keeper ID: 3
FQDN: kuma-storage-cluster1server4.example.com
分片ID：1
副本ID：1
Keeper ID: 0
FQDN: kuma-storage-cluster1server5.example.com
分片ID：1
副本ID：2
Keeper ID: 0
FQDN: kuma-storage-cluster1server6.example.com
分片ID：2
副本ID：1
Keeper ID: 0
FQDN: kuma-storage-cluster1server7.example.com
分片ID：2
副本ID：2
Keeper ID: 0

13. 如果需要，請在**空間**部分中向儲存中新增空間以分發儲存體的事件。

    可以有多個空間。您可以點選**新增空間**按鈕新增空間，或點選相關空間的X圖示刪除空間。

    可用設定：

    - 在**名稱**欄位中，指定包含1到128個Unicode字元的空間名稱。

    - 在**保留政策選項**欄位中，在ClickHouse群集中為該空間選擇一個事件儲存條件，當滿足該條件時，則將導致事件傳輸到冷儲存磁碟，或者如果冷儲存未設定或設定不正確，則事件將被刪除。新增空間時，OSMP會套用 **365 天**的儲存條件。

      若要設定空間的儲存條件，請執行下列其中一項操作：

      - 如果要限制事件的儲存期間，請從下拉清單中選擇**天數**，然後在欄位中指定ClickHouse熱儲存叢集中的最大事件儲存期間（以天為單位）。

        在指定的週期之後，事件將自動傳輸到冷儲存磁碟或從ClickHouse叢集中刪除，從日期最早的分割區開始。最小值是1。預設值是365。

      - 如果要限制最大儲存空間大小，請從下拉清單中選擇**GB** ，然後在欄位中指定最大空間大小（以GB為單位）。

        當空間達到指定大小時，事件將自動傳輸到冷儲存磁碟或從ClickHouse叢集中刪除，從日期最早的分割區開始。最小值與預設值皆為1。

      - 如果要將空間大小限制為儲存體可用磁碟空間的百分比，請從下拉清單中選擇**百分比**，然後在欄位中指定最大空間大小，作為儲存可用磁碟大小的百分比。在這種情況下，當可用磁碟空間減少時，也會觸發此條件。

        當空間達到指定的儲存可用磁碟空間百分比時，事件將自動傳輸到冷儲存磁碟或從ClickHouse叢集中刪除，從日期最早的分割區開始。可能的值：1到95。預設值是80。如果要對所有儲存空間使用百分比，則所有空間條件中的百分比總和不得超過95，但我們建議為整個儲存體或單一空間指定最多90%的限制。

我們不建議指定較小的百分比值，因為這會增加儲存體中資料遺失的可能性。

使用大小作為儲存條件時，必須確保儲存條件中指定的所有空間的總大小不超過儲存體的實體大小，否則啟動服務時會顯示錯誤。

在具有大小限制的儲存條件中，請對儲存的所有空間使用相同的度量單位（僅使用GB或僅使用百分比值）。否則，如果將條件指定為一個空間的百分比，而將另一個空間的條件指定為GB，則儲存可能會因值不匹配而溢出，從而導致資料遺失。

- 如果要在空間過期且不再相關時將其停用，請選取**唯讀**核取方塊。

  這可以防止事件進入該空間。若要使空間再次處於作用中狀態，請清除**唯讀**核取方塊。預設情況下，此核取方塊處於清除狀態。

- 如有必要，請在**事件保存時間**欄位中，指定KUMA事件的總儲存時間長度（以天為單位），從收到事件的那一刻起計算。當指定的時間段到期時，事件將自動從冷儲存磁碟中刪除。預設值是0。

  事件保留時間的計算方法是ClickHouse熱儲存叢集中事件保留時間的總和，直到觸發**保留政策選項**設定中指定的條件，以及冷儲存磁碟上的事件保留時間。當其中一個儲存條件觸發後，最早日期的資料分割區將移至冷儲存磁碟，並保留在該處，直到 OSMP 中的事件保留時間到期。

  根據指定的儲存條件，最終的保存時間如下：

  - 如果以天為單位指定儲存條件，則**事件保存時間**必須嚴格大於儲存條件中指定的天數。事件的冷儲存期間按**事件儲存時間**減去**保留政策選項**設定中指定的天數計算。

    如果您不想將此空間中的事件儲存在冷儲存磁碟上，則可以在**事件保存時間**欄位中指定與儲存條件相同的天數。

  - 如果您以磁碟大小（絕對值或百分比）指定儲存條件，則**事件保存時間**的最小值為1。事件的冷儲存持續時間計算為**事件保存時間**減去從收到事件到觸發條件和磁碟分割區填充的天數，但在觸發條件之前，無法計算準確的持續時間。在這種情況下，我們建議為**事件保存時間**指定一個相對較大的值，以避免事件被刪除。

    如果您不想將此空間中的事件儲存在冷儲存磁碟上，則可以將**事件保存時間**設為 0。

  只有在添加至少一個冷儲存磁碟後，**事件保存時間**設定才可用。

- 在**篩選器設定**部分，您可以指定條件來識別將放入此空間的事件。若要建立新的篩選器，請在**篩選器**下拉清單中選擇現有篩選器或**新建** 。

  在資源中建立過濾器

  KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

  若要建立篩選器：

  1. 在**篩選器**下拉清單中，選擇**新建**。
  2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
  3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。

4. 在**條件**下，指定事件必須滿足的條件：

   a. 點擊**新增條件**按鈕。

   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。

   c. 在**運算子**下拉清單中，選擇一個運算子。

   篩選器運算子

   - **=** — 左運算元等於右運算元。
   - **<** — 左運算元小於右運算元。
   - **<=** — 左運算元小於或等於右運算元。
   - **>** — 左運算元大於右運算元。
   - **>=** — 左運算元大於或等於右運算元。
   - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
   - **contains** — 左運算元包含右運算元的值。
   - **startsWith** — 左運算元以右運算元的某個值開頭。
   - **endsWith** — 左運算元以右運算元的某個值末端。
   - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
   - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

     待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

     若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
   - **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

     如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
   - **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
   - **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
   - **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
   - **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
   - **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。

- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務建立後，您可以在儲存資源設定中查看和刪除空間。

> 您不需要為稽核事件建立個別空間（稽核事件、稽核事件）。此類型（Type=4）的事件會自動放置在單獨的稽核空間中，儲存週期至少為365天。此空間無法透過 OSMP Web 介面進行編輯或刪除。

14. 如有必要，在**冷儲存空間的磁碟**部分中，將要從ClickHouse叢集傳輸事件以進行長期儲存的磁碟新增至儲存中。

可以有多個磁碟。您可以透過點擊**新增磁碟**按鈕來新增磁碟，也可以透過點選**移除磁碟**按鈕來刪除磁碟。

可用設定：

- 在**類型**下拉清單中，選擇所連線磁碟的網域名稱類型：
  - **本機**—適用於以目錄形式掛載在作業系統中的磁碟。
  - HDFS—適用於Hadoop分散式檔案系統的磁碟。
  - **S3** — 用於KUMA中使用的S3雲端儲存磁碟。

    > 從4.2版本開始，儲存在HDFS磁碟上的資料將逐步遷移到S3磁碟。在應用程式的未來版本中，將停止對HDFS檔案系統的支援。

- 在**名稱**欄位中，指定磁碟名稱。此名稱必須包含1到128個Unicode字元。

  > 在不變更磁碟機路徑的情況下，您無法變更S3磁碟機的名稱。

- 如果磁碟類型選擇為**本機**網域名稱，請在**路徑**欄位中輸入下列值之一。
  - 如果儲存服務部署在本機，請輸入本機磁碟機掛載目錄的絕對路徑。該路徑必須以「/」字元開頭和結尾。

    已掛載的本機磁碟的目錄必須由KUMA使用者擁有。

  - 如果儲存服務部署在Kubernetes叢集上，請輸入路徑： `/opt/cold/` 。要部署儲存服務的Kubernetes叢集節點上的 `/opt/lvp/cold/` 目錄會掛載到 `/opt/cold` 目錄。
- 如果磁碟的網域名稱類型選擇為**HDFS**，請在**主機**欄位中指定HDFS的路徑（例如， `hdfs://hdfs1:9000/clickhouse/` ）。
- 如果您選擇**S3**作為磁碟的網域類型，請指定下列參數：
  - 在**主機**欄位中，輸入S3儲存體的位址（例如， `https://www.company.com/clickhouse/storagefolder/` ）。

    指定S3儲存體位址的規則

    指定S3儲存體位址時，必須符合以下需求：

    - 位址必須以URL格式指定，例如： `https://<web address/IP address of the server>/<path to disk>/`
    - 位址必須以"/"字元結尾。
    - 最大長度為2048個字元。
    - 不允許使用非拉丁字母。

    在不變更磁碟名稱的情況下，您無法變更S3磁碟的位址。

  - 在**密鑰**欄位中，指定用於存取S3儲存體的密鑰。您可以從下拉清單中選擇一個金鑰，也可以按一下**新建**來建立一個密鑰。

15. 在**設定備份和還原**部分中，管理下列設定：

    a. 在**儲存體備份**欄位中，指定要儲存體備份檔案的路徑。例如，/mnt/data。
    路徑需求：
    - 該路徑必須存在，並且在儲存體叢集的所有節點上都必須相同。
    - 使用者必須對指定的目錄具有讀取、寫入和執行權限。
    - 指定的目錄必須屬於第二層或更深層的巢狀目錄。你不能使用第一層巢狀目錄，例如 /backup。
    - 目錄名稱不能包含句點。

- **路徑不得包含以下前綴**。

  指定檔案路徑時不能使用的前綴：

  - /*
  - /bin
  - /boot
  - /dev
  - /etc
  - /home
  - /lib
  - /lib64
  - /proc
  - /root
  - /run
  - /sys
  - /tmp
  - /usr/*
  - /usr/bin/
  - /usr/local/*
  - /usr/local/sbin/
  - /usr/local/bin/
  - /usr/sbin/
  - /usr/lib/
  - /usr/lib64/
  - /var/*
  - /var/lib/
  - /var/run/
  - /opt/kaspersky/kuma/

系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。

檔案位於下列路徑：

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

系統會在指定的路徑下自動建立兩個目錄： **備份**和**還原**。

如果未指定路徑，則排程備份、手動備份、從備份還原和匯入功能將無法使用。

b. 若要設定排程備份，請啟用**排程備份**切換開關。

c. 在**幾天後備份**欄位中，指定分割區建立後若干天（整數），之後將建立備份副本。例如，如果值為**1**，則對前天建立的分割區執行備份。

d. 在**副本**下拉清單中，選擇要備份的副本。選擇同一分片的多個副本會導致資料重複。

e. 在**分割區**下，按一下**新增分割區**並管理下列設定：

a. 在**租用戶**下拉清單中，選擇包含要備份的分割區的租用戶。

b. 在**空間**下拉清單中，選擇屬於要備份的分割區的一個或多個儲存空間。如果未指定值，則備份整個分割區。

您可以管理多個分割區的設定。如有必要，請按一下**新增分割區**並在顯示的欄位中管理新分割區的設定。例如，如果您要備份**稽核**空間，並且您有10個租用戶，則必須為每個租用戶單獨設定備份。

16. 轉至**進階設定**頁籤，並填寫以下欄位：

- 在**緩衝區大小**欄位中，輸入必須將事件傳送到資料庫的緩衝區大小（以位元組為單位）。預設值為128MB。未配置最大值。如果虛擬機器的可用 RAM 少於指定的**緩衝區大小**，OSMP 會將上限設定為 128 MB。

  如果儲存服務的預期流量大於 1 Gbps，建議將**緩衝區大小**設定（以位元組為單位）變更為預期值，並將**緩衝區排清間隔**設定為 2。

  緩衝區大小設定的值可以透過經驗確定。如果儲存空間的**插入 QPS**指標大於 1，且您發現要求佇列持續增長，請遵循檢視 OSMP 指標文章中「插入 QPS」章節的建議，計算並調整**緩衝區大小**設定。

- 在**最大緩衝區大小**欄位中，以位元組為單位指定最大緩衝區大小。預設值為256MB。

  預設情況下，事件每秒寫入資料庫一次。如果EPS上升且事件註冊頻率超過每秒一次，則緩衝區大小會自動增加。緩衝區大小最多增加到**緩衝區大小**值的三倍，但不能超過**最大緩衝區大小**值。當負載恢復正常時，緩衝區大小不變；不會自動減少緩衝區大小。

  如果**最大緩衝區大小**小於或等於**緩衝區大小** ，則緩衝區大小不會改變。

  重新啟動儲存服務會將增加的緩衝區大小重設為**緩衝區大小**欄位中的值。

- 在**緩衝區排清間隔**欄位中，輸入 OSMP 等待緩衝區填滿的時間（以秒為單位）。如果緩衝區尚未填滿，但指定的時間已過，OSMP 會將事件傳送到資料庫。預設值為1秒。

- 在**所需記憶體大小**欄位中，以位元組為單位指定最小可用RAM量。預設值為128MB。

  如果安裝儲存體的節點的可用RAM少於此設定，資料庫插入請求將返回錯誤，事件稍後會記錄。限制記憶體大小可以避免因任何原因導致資料庫事件記錄阻塞，資料開始在記憶體中累積，造成記憶體耗盡的情況。

- 在**磁碟緩衝區大小限製**欄位中，輸入一個值（以位元組為單位）。磁碟緩衝區用於暫時儲存無法傳送以進行進一步處理或儲存的事件。如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。預設值為10GB。

- 使用**磁碟緩衝區**切換開關可啟用或停用磁碟緩衝區。預設情況下已啟用該選項。

- 使用**寫入到本機資料庫表格**切換開關可啟用或停用寫入本機資料庫表。預設情況下停用PKI整合。

  如果啟用，則資料僅寫入儲存所在的主機上。我們建議僅在您已於步驟 **6. 在收集器和/或關聯器上設定平衡功能時，才使用此功能在路由**的**進階設定**區段中，**URL 選擇政策**欄位設定為**輪詢**。

  如果您停用寫入，資料將分佈在叢集的各個分片中。

- 如有必要，請使用**偵錯**切換開關啟用服務操作日誌記錄。

- 您可以應技術支援要求，使用**定期建立傾印**切換開關，以傾印形式產生資源使用率報告（CPU 或 RAM）。

- 在**傾印設定**欄位中，您可以指定建立傾印時要使用的設定。有關如何填寫此欄位的說明，請聯絡技術支援。

儲存體的資源集隨即建立，並顯示在**資源→儲存體**下。現在您可以建立儲存服務。

在OSMP中建立儲存服務

為儲存體建立資源集後，您可以繼續在KUMA中建立儲存服務。

若要在 OSMP 中建立儲存服務：

1. 在KUMA主控台中，在**資源→活動服務**下，按一下**新增服務**。
2. 在開啟的**選擇服務**視窗中，選擇剛為儲存體建立的資源集，然後按一下**建立服務**。

   儲存服務已在 OSMP 中建立，並顯示於 **資源 → 活動服務**區段。現在必須使用服務ID將儲存服務安裝到ClickHouse叢集的每個節點。

在OSMP網路基礎架構中安裝儲存體

要建立儲存體：

1. 登入要安裝服務的伺服器。
2. 建立/opt/kaspersky/kuma/資料夾。
3. 將「kuma」檔案複製到/opt/kaspersky/kuma/資料夾。該檔案位於安裝程式中的/kuma-ansible-installer/roles/kuma/files/資料夾中。

   確保kuma檔案具有足夠的執行權限。

4. 執行以下命令：

```
sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --install
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
- <port> 是 KUMA Core 用於內部通訊的連接埠（預設使用連接埠 7210）。
- <fingerprint ID of the KUMA Core CA certificate> 是連線服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。

- <service ID> 是從網頁介面複製的 KUMA 服務識別碼。

範例：

```
sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --install
```

在同一主機上部署多項 KUMA 服務時，您必須在安裝過程中使用 `--api.port <連接埠>` 參數，為每個元件指定唯一的連接埠。預設使用以下設定值：`--api.port 7221`。

5. 對每個儲存節點重複步驟 1 和 2。

儲存體已安裝。

備份、還原和匯入分割區

具有「一般管理員」角色的使用者可以存取下列 OSMP 操作：

- 排定分割區備份。
- 手動備份分割區。
- 從備份中恢復分割區。
- 從外部 OSMP 實例匯入分割區。

您可以同時設定和使用事件冷儲存和分割區備份。

您可以在稽核事件中檢視分割區備份、還原和匯入的狀態。此外，在開始手動備份分割區、從備份還原分割區或從外部 OSMP 實例匯入分割區後，會在**工作管理員**區段中建立對應的工作。

排定分割區備份

具有主管理員角色的使用者可以設定分割區的排程備份。

若要排定備份：

1. 在主功能表中，轉至**監控→資源與服務→活動服務**部分，然後開啟活動儲存體來管理其設定。
2. 在開啟的**編輯儲存空間**視窗中，在**基本設定**頁籤的**設定備份與還原**部分，管理下列設定：
   a. 在**儲存體備份**欄位中，指定要儲存體備份檔案的路徑。例如，/mnt/data。如果未指定路徑，則無法執行備份。
   b. 啟用**排程備份**切換開關。
   c. 在**在數天後備份**欄位中，指定在建立分割區後多少天建立其備份副本。例如，如果值為**1**，則對前天建立的分割區執行備份。
   d. 在**複本**下拉清單中，選擇要備份的副本。選擇同一分片的多個副本會導致資料重複。
      如果叢集集中使用了多個分片，則**副本**清單僅包含所有分片中都指定的ID的副本。
3. 在**備份磁碟分割**下，按一下**新增磁碟分割**並管理下列設定：
   a. 在**租用戶**下拉清單中，選擇包含要備份的分割區的租用戶。
   b. 在**空間**下拉清單中，選擇屬於要備份的分割區的一個或多個儲存空間。如果未指定值，則備份整個分割區。
      您可以管理多個分割區的設定。如有必要，請按一下**新增磁碟分割**並在顯示的欄位中管理新分割區的設定。例如，如果您要備份**稽核**空間，並且您有10個租用戶，則必須為每個租用戶單獨設定備份。
4. 按一下**儲存**。

儲存設定後，**備份**和**還原**目錄將在指定路徑自動建立。**備份**目錄中會自動建立包含租用戶ID和空間ID的子目錄。例如，如果您將/mnt/data指定為備份路徑，則備份檔案的完整路徑為/mnt/data/backup/<租用戶ID >/<儲存空間ID >/<分割區建立日期>.zip。若要找尋租用戶ID或空間ID，您可以轉至**事件**部分，打開事件卡片並檢視所需的資訊。

若要從備份中還原，需要將備份檔案移至**還原**目錄。

分割區排程備份隨即設定。如果備份失敗，則會產生對應的稽核事件，儲存服務會在**活動服務**部分中顯示黃色狀態，並且當您將滑鼠懸停在黃色狀態指示燈上時，會顯示錯誤訊息。下次啟動排程備份時，會先嘗試備份舊資料。

手動備份分割區

具有主管理員角色的使用者可以手動備份分割區。

若要手動建立分割區備份副本：

1. 在主功能表中，轉至**監控→資源與服務→活動服務**部分，然後開啟活動儲存體來管理其設定。

2. 這將開啟**編輯儲存空間**視窗；在該視窗中，在**基本設定**頁籤的**備份設定**部分中的**儲存體備份**欄位中，指定備份檔案的路徑。例如，/mnt/data。請確保「kuma」使用者擁有對指定目錄的存取權限。

   路徑需求：

   - 該路徑必須存在，並且在儲存體叢集的所有節點上都必須相同。
   - 使用者必須對指定的目錄具有讀取、寫入和執行權限。
   - 指定的目錄必須屬於第二層或更深層的巢狀目錄。你不能使用第一層巢狀目錄，例如 /backup。
   - 目錄名稱不能包含句點。
   - **路徑不得包含以下前綴**。

     指定檔案路徑時不能使用的前綴：

     - `/*`
     - `/bin`
     - `/boot`
     - `/dev`
     - `/etc`
     - `/home`
     - `/lib`
     - `/lib64`
     - `/proc`
     - `/root`
     - `/run`
     - `/sys`
     - `/tmp`
     - `/usr/*`
     - `/usr/bin/`
     - `/usr/local/*`
     - `/usr/local/sbin/`
     - `/usr/local/bin/`

- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。

檔案位於下列路徑：

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/metrics/log/

3. 在主功能表中，轉至**監控→資源與服務→活動服務**部分，然後選取狀態為綠色的儲存服務旁的核取方塊。
4. 在工具列或功能表（⋮）中，選擇**備份**，然後按一下**備份**。

   如果選擇了儲存服務且該服務處於綠色狀態，則**備份**選項可用。

   在以下情況下，此選項不可用：

   - 如果在上一個步驟中，您選取了多個服務旁邊的核取方塊。
   - 如果儲存服務處於紅色狀態。
   - 如果未選取任何核取方塊。
   - 如果您已選取其他類型服務旁的核取方塊。
5. 在開啟的**分割區備份**視窗中，管理以下設定：
   a. 在**租用戶**下拉清單中，選擇包含要備份的分割區的租用戶。
   b. 在**空間**下拉清單中，選擇屬於要備份的分割區的一個或多個儲存空間。如果未指定值，則備份整個分割區。
   c. 在**複本**下拉清單中，選擇要備份的副本或所有副本。選擇同一分片的多個副本會導致資料重複。
   d. 在**日期範圍**欄位中，使用日曆指定要包含在備份中的分割區的日期範圍。
6. 點擊**確定**。
7. 在**將執行備份**確認視窗中，按一下**確定**。

   在**工作管理員**區段中確認設定後，會建立分割區備份工作和稽核事件。

手動備份隨即完成。

儲存設定後，**備份**和**還原**目錄將在指定路徑自動建立。**備份**目錄中會自動建立包含租用戶ID和空間ID的子目錄。例如，如果您將/mnt/data指定為備份路徑，則備份檔案的完整路徑為/mnt/data/backup/<租用戶ID >/<儲存空間ID >/<分割區建立日期>.zip。若要找尋租用戶ID或空間ID，您可以轉至**事件**部分，打開事件卡片並檢視所需的資訊。

若要從備份中還原，需要將備份檔案移至**還原**目錄。

如果手動備份的檔案名稱與排程備份檔案的名稱相同，則會傳回錯誤，提示無法儲存備份檔案。您必須重新命名或刪除檔案，然後再次執行手動備份。

您可以透過查看**工作管理器**中儲存服務的黃色狀態和錯誤訊息，在**活動服務**部分找到備份錯誤訊息，或稽核事件。

從外部 OSMP 實例匯入分割區

具有「一般管理員」角色的使用者可以從外部 OSMP 實例匯入分割區。

若要從外部 OSMP 實例匯入分割區：

1. 使用以下命令授予您在管理備份設定時指定的備份目錄的「kuma」使用者存取權限，以及對備份檔案本身的存取權限：

   ```
   sudo chown kuma <備份目錄的完整路徑>
   sudo chown kuma *.zip
   ```

2. 將要匯入分割區的檔案放入**還原**目錄。分割區將從此目錄匯入。

3. 在主功能表中，轉至**監控→資源和服務→活動服務**部分，然後選取狀態為綠色的儲存服務旁的核取方塊。

4. 在工具列或功能表中（⋮），選擇**備份→匯入**。

5. 在顯示的**從外部實例 OSMP 匯入**視窗中，管理以下設定：

   a. 在**租用戶**下拉清單中，選擇要匯入分割區的租用戶。

   b. 在**複本**下拉清單中，選擇要將分割區匯入的副本。

   c. 在**用於排除項目的欄位**下拉清單中，選取或取消選取核取方塊，即可指定要在匯入過程中刪除的欄位。預設情況下，以下欄位的核取方塊已選取：

   - AggregationRuleName
   - CorrelationRuleName
   - SourceAccountID
   - DestinationAccountID
   - SourceAssetID
   - DestinationAssetID
   - DeviceAssetID

- KUMA擴充事件結構描述欄位：
  - 擴充事件結構描述
  - KSC資產欄位
  - KLCorrelationRulePriority = "KL_CorrelationRulePriority"
  - KLSourceAssetDisplayName = "KL_SourceAssetDisplayName"
  - KLDestinationAssetDisplayName = "KL_DestinationAssetDisplayName"
  - KLDeviceAssetDisplayName = "KL_DeviceAssetDisplayName"
  - KLSourceAccountDisplayName = "KL_SourceAccountDisplayName"
  - KLDestinationAccountDisplayName = "KL_DestinationAccountDisplayName"
  - KLDllHijackingResult = "KL_AI_DLLHijackingCheckResult"

    當您選擇**KUMA擴充事件架構欄位**類別進行刪除時，整個欄位群組都將會被刪除。您無法刪除單一欄位。

預設情況下，以下欄位將被移除，因此在網頁介面中無法選擇：

- ServiceID
- ServiceName
- CorrelationRuleID
- AggregationRuleID

6. 點擊**確定**。
7. 在**將執行匯入**確認視窗中，按一下**確定**。

   在**工作管理員**區段中確認設定後，系統會建立分割區匯入工作和稽核事件。

從外部 OSMP 實例匯入分割區。

從備份中還原分割區

只有具有主管理員角色的使用者才能從備份中還原分割區。

若要從備份中還原分割區：

1. 使用以下命令授予您在管理備份設定時指定的備份目錄的「kuma」使用者存取權限，以及對備份檔案本身的存取權限：

   ```
   sudo chown kuma <備份目錄的完整路徑>
   sudo chown kuma *.zip
   ```

2. 將備份檔案從**備份**目錄移至**還原**目錄。
3. 在主功能表中，轉至**監控→資源與服務→活動服務**部分，然後選取狀態為綠色的儲存服務旁的核取方塊。

4. 在工具列或功能表中（⋮），選擇**備份→還原**。

5. 在開啟的**從目前的 KUMA 安裝還原**視窗中，從**複本**下拉式清單選取一個要從備份還原的複本。

6. 點擊**確定**。

7. 在**將執行還原**確認視窗中，按一下**確定**。
   在**工作管理員**區段中確認設定後，系統會建立分割區還原工作和稽核事件。

分割區備份還原隨即完成。

建立關聯器

關聯器由兩部分組成：一部分在 OSMP 內建立，另一部分安裝在用於處理事件的網路基礎架構伺服器上。

OSMP 中的操作

使用安裝精靈在 OSMP 中建立關聯器。此精靈將必要的資源組合成關聯器的資源集。完成精靈後，服務本身將基於資源集自動建立。

若要在 OSMP 中建立關聯器，

啟動關聯器安裝精靈：

- 在 OSMP 的主功能表中，於 **資源和服務** 下，按一下 **新增關聯器**。
- 在 OSMP 的主功能表中，於 **資源和服務 → 關聯器** 下，按一下 **新增關聯器**。

完成精靈的步驟後，將在 OSMP 中建立關聯器服務。

關聯器的資源集包括以下資源：

- 關聯規則
- 擴充規則（如有需要）；
- 回應規則（如果需要）
- 目標（通常用於將事件傳送到儲存體）

這些資源可以提前準備好，也可以在安裝精靈執行時建立它們。

OSMP 關聯器伺服器上的操作

如果要在打算用於事件處理的伺服器上安裝關聯器，則需要在伺服器上執行安裝精靈最後一步顯示的命令。安裝時，您必須指定在 OSMP 中自動指派給服務的ID，以及用於通訊的連接埠。

測試安裝

建立關聯器後，建議確保其正常運作。

啟動關聯器安裝精靈

若要啟動關聯器安裝精靈：

- 在 OSMP 的主功能表中，於 **資源和服務** 下，按一下 **新增關聯器**。
- 在 OSMP 的主功能表中，於 **資源和服務** → **關聯器** 下，按一下 **新增關聯器**。

遵照精靈的說明。

除了精靈的第一步和最後一步之外，可以任意順序執行精靈的步驟。您可以使用 **下一步** 和 **上一步** 按鈕，或按一下視窗左側的步驟名稱，在各步驟之間切換。

精靈完成後，會在 OSMP 的 **資源與服務** → **資源和服務** 下建立 關聯器，並在 **資源與服務** → **資源和服務** 下新增有效服務。

步驟1：一般關聯器設定

這是安裝精靈的必要步驟。在此步驟中，您可以指定關聯器的主要設定：關聯器名稱和將擁有它的租用戶。

若要定義關聯器的主要設定：

- 在**名稱**欄位中，輸入要建立的服務的唯一名稱。此名稱必須包含1到128個Unicode字元。
- 在**租用戶**下拉式清單中，選取必須擁有關聯器的租用戶。租用戶選擇決定了建立收集器時可用的資源。

  如果您從安裝程式的另一個後續步驟返回此視窗並選擇另一個租用戶，則必須手動編輯已新增至服務的所有資源。只有選定租用戶和共用租用戶的資源才能新增至服務。

- 如果需要，在**工作線程**欄位中指定服務可以並發運行的進程數。預設情況下，工作進程數與安裝服務的伺服器上的vCPU數相同。
- 如有必要，請使用**偵錯**下拉清單啟用服務運作日誌記錄。
- 您可以選擇在**描述**欄位中新增最多256個Unicode字元來描述服務。

關聯器的主要設定已定義。轉到精靈的下一個步驟。

步驟2。全域變數

如果追蹤事件欄位、活動清單或字典中的值不足以涵蓋某些特定的安全場景，則可以使用全域變數和局部變數。您可以使用它們透過實作複雜的威脅偵測邏輯對關聯器收到的值執行各種操作。可以為變數分配特定的函式，然後像查詢普通事件欄位一樣從關聯規則中進行查詢，並在回應中收到觸發的函式結果。

若要在關聯器中新增全域變數，

請按一下**新增變數**按鈕並指定以下參數：

- 在**變數**視窗中，輸入變數的名稱。
  變數命名需求
  - 在關聯器內必須是唯一的。
  - 必須包含1至255個Unicode字元。
  - 不能以字元「$」開頭。
  - 必須以駝峰式大小寫命名。
- 在**值**視窗中，輸入變數函式。
  變數函式描述。

全域變數隨即新增。透過在變數名稱前新增字元$，可以從關聯規則中查詢。可以有多個變數。新增的變數可以使用✕圖示進行編輯或刪除。

轉到精靈的下一個步驟。

步驟 3：關聯

這是安裝精靈中可選但建議執行的步驟。在安裝精靈的**關聯**頁籤上，選擇或建立關聯規則。這些資源定義指示安全相關事故的事件序列。當偵測到這些序列時，關聯器會建立關聯事件和警示。

如果您已將全域變數新增至關聯器，則所有新增的關聯規則都可以查詢它們。

新增至關聯器資源集的關聯規則會顯示在表格中，其中包含以下欄：

- **關聯規則** - 關聯規則資源的名稱。
- **類型** - 關聯規則的類型：**標準**、**簡單**、**運作**。可以透過點選列表頭並選擇相關值，根據此列的值篩選該表。
- **操作** - 觸發關聯規則時關聯器將執行的操作清單。這些操作在關聯規則設定中指示。可以透過點選列表頭並選擇相關值，根據此列的值篩選該表。
  可用值：
  - **輸出**— 此關聯規則所建立的關聯事件將傳送到其他關聯器資源：擴充規則、回應規則，然後傳送到其他 OSMP 服務。
  - **編輯活動清單**— 關聯規則變更活動清單。
  - **迴圈到關聯器**— 關聯事件將會傳送到相同的關聯規則進行重新處理。
  - **分類**— 關聯規則更改資產類別。
  - **事件擴充**— 關聯規則設定為擴充關聯事件。

- **不建立警示**– 當關聯規則觸發而建立關聯事件時，不會為此建立警示。如果您不想在觸發關聯規則時建立警示，但仍想將關聯事件傳送到儲存體，請選取**輸出**和**不觸發警示**核取方塊。如果僅選取**不觸發警示**核取方塊，則關聯事件不會儲存在儲存體中。

- **共享資源**– 關聯規則或關聯規則中使用的資源位於共用租用戶中。

您可以使用**搜尋**欄位搜尋關聯規則。您可以選取相關規則並按一下**刪除**，從資源集中移除已新增的關聯規則。

選擇關聯規則後，一個包含其設定的視窗隨即開啟，您可以編輯這些設定，然後按一下**儲存**即可儲存。如果您在此視窗中按一下**刪除**，關聯規則將取消與資源集的連結。

點選**上移**和**下移**按鈕可變更所選關聯規則在表格中的位置。這會影響處理事件時規則的執行順序。使用**將操作類規則移至頂端**按鈕，可將**操作**類型的關聯規則移至關聯規則清單的開頭。

若要將現有關聯規則連結至關聯器的資源集：

1. 按一下**連結**。

   資源選擇視窗隨即開啟。

2. 選取相關關聯規則並按一下**確定**。

   關聯規則將連結至關聯器的資源集，並顯示在規則表格中。

若要在關聯器的資源集中建立新的關聯規則：

1. 按一下**新增**。

   關聯規則建立視窗隨即開啟。

2. 指定關聯規則設定，然後按一下**儲存**。

   將建立關聯規則並將其連結至關聯器的資源集。它顯示在關聯規則表和**資源→關聯規則**下的資源清單中。

轉到精靈的下一個步驟。

步驟4。擴充

這是安裝精靈的可選步驟。在安裝精靈的「**擴充**」索引標籤中，您可以選取或建立擴充規則，並指定要將哪些來源中的哪些資料新增至關聯器所建立的關聯事件。可以有多個擴充規則。您可以點擊**新增**按鈕來新增擴充規則，也可以點擊 ✕ 按鈕來移除擴充規則。

若要將現有的擴充規則新增至資源集：

1. 按一下**新增**。

   擴充規則設定區塊隨即開啟。

2. 在**擴充規則**下拉清單中，選擇相關資源。

   擴充規則已新增至關聯器的資源集。

若要在資源集中建立新的擴充規則：

1. 按一下**新增**。

   擴充規則設定區塊隨即開啟。

2. 在**擴充規則**下拉清單中，選擇**新建**。

3. 在**來源類型**下拉清單中，選擇要擴充的資料來源並定義其對應的設定：

   - **常數**

     當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定：

     - 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。

     - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

     若針對 `String`、`Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。

     若針對 `Array of strings`、`Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。

   - **字典**

     如果需要從字典類型的**字典**中新增值，則使用此類擴充。

     在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。

     如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。

     例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。

     如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。

     例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。

   - **事件**

     當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定：

     - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

     - 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。

     - 在**轉換**下，您可以建立規則，以便在將原始資料寫入 KUMA 事件欄位之前修改資料。可以從下拉清單中選擇轉換類型。您可以使用**新增轉換**和**刪除轉換**按鈕分別新增或刪除轉換。轉換的順序很重要。

       可用的轉換

轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

可用轉換類型：

- **小寫** — 用於將值的所有字元變為小寫
- **大寫** — 用於將值的所有字元變為大寫
- **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
- **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。
- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。
- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

- **範本**

當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

- 在 **範本**欄位中，輸入 Go 範本。

  事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。

  範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

- 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

範例：

{{.SA.StringArrayOne}}

範例：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

此類擴充用於向私人網路DNS伺服器傳送請求，以將IP位址轉換為網域名稱或反之亦然。IP 位址只會針對以下私人位址轉換為 DNS 名稱：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、100.64.0.0/10、fd00::/8。

下表說明此類擴充的設定。

「dns」擴充類型的參數

設定	描述
網址	要傳送請求的 DNS 伺服器 URL。 您可以使用 **新增 URL** 按鈕指定多個 URL。 如果未指定 **URL** 設定，KUMA 會從本機的 `/etc/resolv.conf` 檔案取得 DNS 伺服器清單。在這種情況下，您需要啟用 **遞迴查詢** 選項。否則將不會執行擴充。
每秒請求數	每秒傳送至 DNS 伺服器的查詢數上限。預設情況下，此值等於KUMA Core伺服器的vCPU數量。

設定	描述
工作模組	服務可以同時執行以並行處理回應規則的事件處理器數量。請指定介於 0 到 999 之間的正整數。如果指定 0，則使用邏輯 CPU 核心數。預設值為`1`。
資料補足佇列中的最大事件數量	重新提交佇列可容納的事件數上限。預設值為`1,000,000`。
逾時時間	等待 DNS 伺服器回應的時間（以秒為單位）。預設值為`5`。
DNS 模式覆寫	使用的解析方法： • **僅轉發 DNS**會將網域名稱解析為 IP 位址。 • **僅反向 DNS**會將 IP 位址解析為網域名稱。 • **轉發並反向 DNS**會將網域名稱解析為 IP 位址，或將 IP 位址解析為網域名稱。
快取存續時間	快取中儲存的值的存活時間（以秒為單位）。預設值為`60`秒。
已停用快取	您可以使用此設定啟用或停用快取。預設情況下啟用快取。
已停用快取重新整理	如果啟用快取更新，當快取的 TTL 到期時，收集器會再次向 DNS 伺服器傳送請求，以更新快取中儲存的資料。此設定僅在啟用快取時可用。預設會啟用快取更新。
遞迴查詢	允許收集器向權威 DNS 伺服器傳送遞迴查詢，以擴充資料。預設值是**停用**。

- **cybertrace**

  此類擴充用於將CyberTrace資料流中的資訊新增至事件欄位。

  可用設定：

  - **URL**（必填）- 在此欄位中，您可以指定要傳送請求的CyberTrace伺服器的URL。
  - **連線數**— KUMA可以同時與CyberTrace伺服器建立的最大連線數。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
  - **RPS** — 每秒傳送至伺服器的最大請求數。預設值是`1000`。
  - **逾時** — 等待CyberTrace伺服器回應的時間長度（以秒為單位）。預設值為`30`。
  - **對應**（必要）— 此設定區塊包含用於將KUMA事件欄位對應到 CyberTrace指標類型的對應表。**KUMA欄位**欄會顯示 KUMA 事件欄位的名稱，而 **CyberTrace 指標**欄會顯示 CyberTrace 指標的類型。

    可用的CyberTrace指標類型：

    - **ip**
    - **網址**
    - **雜湊值**

    在對應表中，您必須提供至少一個字串。您可以點擊**新增行**按鈕新增字串，也可以點擊 ✕ 按鈕刪除字串。

- **時區**

  此類擴充在收集器和關聯器中用於為事件指派特定的時區。在搜尋發生在異常時間（例如夜間）的事件時，時區資訊可能很有用。

選擇此類擴充時，必須從**時區**下拉清單中選擇所需的時區。

請確保託管擴充利用服務的伺服器已設定正確的時區。例如，您可以使用 `timedatectl list-timezones` 命令執行此操作，該命令會顯示伺服器上已設定的所有時區。有關設定時區的詳細資訊，請參閱相應的作業系統說明文件。

當事件進行擴充處理時，所選時區相對於協調世界時 (UTC) 的時間偏移量，會以`+-hh:mm`格式寫入DeviceTimeZone事件欄位。例如，若選取 **Asia/Yekaterinburg** 時區，則會將值 `+05:00` 寫入 DeviceTimeZone 欄位。若經擴充處理的事件在 DeviceTimeZone 欄位中已有值，該值將被覆蓋。

預設情況下，如果未在正在處理的事件中指定時區，且未配置按時區擴充規則，則為事件指派處理事件的服務（收集器或關聯器）所在伺服器的時區。如果伺服器時間發生變化，則必須重新啟動服務。

擴充DeviceTimeZone欄位時允許的時間格式

在收集器中處理傳入的原始事件時，下列時間格式可自動轉換為+-hh:mm格式：

已處理事件中的時間格式	範例
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

若 `DeviceTimeZone` 欄位中的日期格式與上述格式不符，當事件使用時區資訊進行擴充處理時，系統會將收集器伺服器的時區寫入該欄位。您可以為非標準時間格式建立自訂的標準化規則。

4. 使用**偵錯**下拉清單指示是否啟用服務運作的日誌記錄。預設情況下，日誌記錄處於停用狀態。

5. 在**篩選器**部分，您可以指定條件來識別將使用擴充規則處理的事件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。

在資源中建立篩選器

KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

若要建立篩選器：

1. 在**篩選器**下拉清單中，選擇**新建**。

2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。

3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。

4. 在**條件**下，指定事件必須滿足的條件：

   a. 點擊**新增條件**按鈕。

   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。

c. 在**運算子**下拉清單中，選擇一個運算子。

篩選器運算子

- **=** — 左運算元等於右運算元。
- **<** — 左運算元小於右運算元。
- **<=** — 左運算元小於或等於右運算元。
- **>** — 左運算元大於右運算元。
- **>=** — 左運算元大於或等於右運算元。
- **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
- **contains** — 左運算元包含右運算元的值。
- **startsWith** — 左運算元以右運算元的某個值開頭。
- **endsWith** — 左運算元以右運算元的某個值末端。
- **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

新的擴充規則已新增至關聯器的資源集。

轉到精靈的下一個步驟。

步驟 5：回應

這是安裝精靈的可選步驟。在安裝精靈的**回應**頁籤上，您可以選擇或建立回應規則，並指示觸發關聯規則時必須執行的操作。可以有多個回應規則。您可以透過點選**新增**按鈕來新增它們，也可以透過點選 按鈕。

若要將現有回應規則新增至資源集：

1. 按一下**新增**。
   回應規則設定視窗隨即開啟。

2. 在**回應規則**下拉清單中，選擇相關資源。

回應規則隨即新增至關聯器的資源集。

若要在資源集中建立新的回應規則：

1. 按一下**新增**。
   回應規則設定視窗隨即開啟。

2. 在**回應規則**下拉清單中，選擇**新建**。

3. 在**類型**下拉清單中，選擇回應規則的類型並定義其對應的設定：

   - **KSC回應**- 用於自動啟動卡巴斯基安全管理中心資產上工作的回應規則。例如，您可以設定病毒掃描或資料庫更新的自動啟動。

     當OSMP與卡巴斯基安全管理中心整合時，工作會自動啟動。工作僅在從卡巴斯基安全管理中心匯入的資產上執行。

     回應設定

     - **卡巴斯基安全管理中心工作**（必填）—您要啟動的 Open Single Management Platform 工作名稱。工作必須預先建立，且其名稱必須以「`KUMA `」開頭。例如：「`KUMA antivirus check`」。

       可以使用KUMA啟動的Open Single Management Platform工作類型：

       - 更新
       - 病毒掃描

- **事件欄位**（必填）—定義要為其啟動 Open Single Management Platform 工作之資產的事件欄位。可能的值：
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID

  若要向 Open Single Management Platform 傳送請求，您必須確保可透過 UDP 連線至 Open Single Management Platform。

- **執行指令碼**— 自動執行指令碼的回應規則。例如，您可以建立一個指令碼，其中包含在偵測到選定事件時要在OSMP伺服器上執行的命令。

  指令碼檔案儲存於安裝了使用回應資源之關聯器服務的伺服器上：/opt/kaspersky/kuma/correlator/<關聯器 ID>/scripts。

  此伺服器的 `kuma` 使用者需要有執行該指令碼的權限。

  回應設定

  - **逾時時間**— 系統在執行指令碼之前等待的秒數。
  - **指令碼名稱**（必填）——指令碼檔的名稱。

    如果指令碼回應資源已連結至關聯器服務，但 /opt/kaspersky/kuma/correlator/<Correlator ID>/scripts 目錄中沒有指令碼檔案，該服務將無法啟動。
  - **指令碼參數** - 必須傳遞給指令碼的參數或事件欄位值。

    如果指令碼包含對檔案執行的操作，則應指定這些檔案的絕對路徑。

    參數可以用引號 (") 括起來。

    事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是其值必須傳遞至指令碼的事件欄位名稱。

    範例：`-n "\"usr\": {{.SourceUserName}}"`

- **KEDR回應**— 用於自動建立阻止規則、Kaspersky Endpoint Detection and Response和卡巴斯基安全管理中心資產上啟動應用程式的回應規則。

  當 OSMP 與 Kaspersky Endpoint Detection and Response 整合時，將執行自動回應操作。

  回應設定

  - **事件欄位**（必填）— 包含需要執行回應操作的資產的事件欄位。可能的值：
    - SourceAssetID
    - DestinationAssetID
    - DeviceAssetID
  - **工作類型**— 收到與篩選器相符的資料時要執行的回應操作。可用的回應操作類型如下：
    - 啟用網路隔離

選擇此類型的回應時，您需要為下列設定定義值：

- **隔離逾時**— 資產的網路隔離處於活動狀態的小時數。您可以指定從1到9,999小時的數值。
  如有必要，您可以**新增網路隔離排除項**。

  若要新增網路隔離排除項：

  a. 按一下**新增排除項**按鈕。

  b. 選擇不得封鎖的網路流量方向：

  - 入站。
  - 出站。
  - 入站/出站。

  c. 在**資產IP**欄位中，輸入不得封鎖其網路流量的資產的IP位址。

  d. 如果您選擇了**入站**或**出站** ，請在**遠端連接埠**和**本機連接埠**欄位中指定連線連接埠。

  e. 若要新增多個排除項，請點選**新增排除項** ，然後重複上述步驟以填寫**流量方向** 、 **資產IP** 、**遠端連接埠**和**本機連接埠**欄位。

  f. 如果要刪除排除項，請按一下相關排除項下的**刪除**按鈕。

  將排除項新增至網路隔離規則時，Kaspersky Endpoint Detection and Response可能會在規則詳細資料中錯誤顯示連接埠值。這不會影響應用程式效能。有關查看網路隔離規則的更多詳細資訊，請參閱*Kaspersky Anti Targeted Attack Platform說明*。

- 停用網路隔離。
- 新增防護規則。
  選擇此類型的回應時，您需要為下列設定定義值：

  - **用於擷取雜湊值的事件欄位**—KUMA 從中擷取必須禁止啟動之檔案的 SHA256 或 MD5 雜湊值的事件欄位。

    選定的事件欄位和在**事件欄位**中選擇的值必須新增到關聯規則的繼承欄位中。

  - **檔案雜湊值#1——**要封鎖的檔案的SHA256 或MD5雜湊值。

  必須至少填寫上述其中一個欄位。

- 刪除防護規則。
- 啟動應用程式

選擇此類型的回應時，您需要為下列設定定義值：

- **檔案路徑** - 要啟動的進程的檔案路徑。
- **命令列參數** - 要用於啟動檔案的參數。
- **工作目錄** - 啟動時檔案所在的目錄。

當具有主管理員角色的使用者觸發回應規則時，**執行程式**工作會顯示在程式網頁介面的**工作管理員**區段中。此工作的**排程工作**顯示在**工作表**的已建立列中。您可以檢視工作完成結果。

所有列出的操作都可以在具有Kaspersky Endpoint Agent for Windows的資產上執行。在具有Kaspersky Endpoint Agent for Linux的資產上，只能啟動該代理程式。

在軟體級別，使用Kaspersky Endpoint Kaspersky Endpoint Agent for Linux為資產建立阻止規則和網路隔離規則的能力是無限的。KUMA和Kaspersky Endpoint Detection and Response不提供任何有關這些規則應用失敗的通知。

- **透過KICS for Networks回應**— 用於在KICS for Networks資產上自動啟動工作的回應規則。例如，您可以在KICS for Networks中變更資產狀態。

  當OSMP與 KICS for Networks整合時，工作會自動啟動。

  回應設定

  - **事件欄位**（必填）— 包含需要執行回應操作的資產的事件欄位。可能的值：
    - SourceAssetID
    - DestinationAssetID
    - DeviceAssetID
  - **KICS for Networks 工作**—收到符合篩選條件的資料時要執行的回應操作。可用的回應操作類型如下：
    - **將資產狀態變更為已授權**。
    - **將資產狀態變更為未授權**。

    當觸發回應規則時，KUMA將向KICS for Networks傳送API請求，以將指定裝置的狀態變更為**已授權**或**未授權**。

- **透過Active Directory回應**— 用於變更Active Directory使用者權限的回應規則。例如，封鎖使用者。

  如果設定了與Active Directory的整合，則會啟動工作。

  回應設定

  - **帳戶ID來源**— 事件欄位，Active Directory帳戶ID值的來源。可能的值：
    - SourceAccountID
    - DestinationAccountID

- **AD命令**— 觸發回應規則時套用於帳戶的命令。可能的值：
  - 新增帳戶到群組
  - 從群組中刪除帳戶
  - 重設帳戶密碼
  - 封鎖帳戶

- 在**工作線程**欄位中，指定服務可以同時執行的進程數。

  預設情況下，工作線程數量與安裝服務的伺服器上的虛擬處理器數量相同。

  該欄位是可選的。

1. 在**篩選器**部分，您可以指定條件來識別將使用回應規則處理的事件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。

   在資源中建立篩選器

   KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

   若要建立篩選器：

   1. 在**篩選器**下拉清單中，選擇**新建**。
   2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
   3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。
   4. 在**條件**下，指定事件必須滿足的條件：
      a. 點擊**新增條件**按鈕。
      b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。
      c. 在**運算子**下拉清單中，選擇一個運算子。

         篩選器運算子

         - **=** — 左運算元等於右運算元。
         - **<** — 左運算元小於右運算元。
         - **<=** — 左運算元小於或等於右運算元。
         - **>** — 左運算元大於右運算元。
         - **>=** — 左運算元大於或等於右運算元。
         - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。

- **contains** — 左運算元包含右運算元的值。
- **startsWith** — 左運算元以右運算元的某個值開頭。
- **endsWith** — 左運算元以右運算元的某個值末端。
- **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False` 。
- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。
6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

新的回應規則已新增至關聯器的資源集。

轉到精靈的下一個步驟。

步驟 6。路由

這是安裝精靈的可選步驟。在安裝精靈的**路由**頁籤上，您可以選擇或建立目標，並使用設定指示關聯器建立的事件的轉送目標。來自關聯器的事件通常會重新導向到儲存體，以便可以保存它們並在以後需要時檢視。可以根據需要將事件傳送到其他位置。可以有多個目標點。

若要將現有目標新增至關聯器的資源集：

1. 在**新增目標**下拉清單中，選擇要新增的目標資源類型：

   - 如果要設定將已處理的事件轉送到儲存體，請選擇**儲存體**。
   - 如果要設定將已處理的事件轉送至關聯器，請選擇**關聯器**。
   - 如果您想要將事件傳送到其他位置，請選擇**其他**。

     此類資源包括在程式的先前版本中建立的關聯器和儲存體服務。

   將開啟**新增目標**窗口，您可以在其中指定事件轉送的參數。

2. 在**目標**下拉清單中，選擇必要的目標。

   視窗名稱變更為**編輯目標**，並顯示所選資源的設定。可以使用按鈕，在新的瀏覽器頁籤中開啟資源進行編輯。

3. 按一下**儲存**按鈕。

所選目標將顯示在安裝精靈頁籤上。可以透過選擇目標資源並在開啟的視窗中點選**刪除**，從資源集中刪除目標資源。

若要將新目標新增至關聯器的資源集：

1. 在**新增目標**下拉清單中，選擇要新增的目標資源類型：

   - 如果要設定將已處理的事件轉送到儲存體，請選擇**儲存體**。
   - 如果要設定將已處理的事件轉送至關聯器，請選擇**關聯器**。
   - 如果您想要將事件傳送到其他位置，請選擇**其他**。

     此類資源包括在程式的先前版本中建立的關聯器和儲存體服務。

   將開啟**新增目標**窗口，您可以在其中指定事件轉送的參數。

2. 在**基本設定**頁籤上指定設定：

   - 在**目標**下拉清單中，選擇**新建**。
   - 在**名稱**欄位中，輸入目標資源的唯一名稱。此名稱必須包含1到128個Unicode字元。
   - 使用**停用**切換按鈕，指定是否將事件傳送到此目標位置。預設情況下，啟用傳送事件。

- 選擇目標資源的**類型**：
  - 如果要設定將已處理的事件轉送到儲存體，請選擇**儲存體**。
  - 如果要設定將已處理的事件轉送至關聯器，請選擇**關聯器**。
  - 如果要設定將事件傳送到其他位置，請選擇**nats-jetstream**、 **tcp**、**http**、**kafka**或**file**。
- 以hostname:<API連接埠>格式指定事件應傳送到的**URL** 。
  您可以透過點選除**nats-jetstream**和**file**之外的所有類型的**URL**按鈕來指定多個目標位址。
- 對於**nats-jetstream**和**kafka**類型，使用**主題**欄位指定資料應寫入哪個主題。主題必須包含Unicode字元。Kafka主題最多包含255個字元。

3. 如有必要，請在**進階設定**頁籤上指定設定。可用的設定因所選的目標資源類型而異：
   - **壓縮**是下拉清單，您可以在其中啟用Snappy壓縮。預設情況下，壓縮是**停用的**。
   - **代理**是下拉清單，用於選擇代理伺服器。
   - **緩衝區大小**欄位用於設定目標的緩衝區大小（以位元組為單位）。預設值為1MB，最大值為64MB。
   - **逾時**欄位可用於設定其他服務或元件回應的逾時（以秒為單位）。預設值為`30`。
   - **磁碟緩衝區大小限製**欄位用於指定磁碟緩衝區的大小（以位元組為單位）。預設大小是10 GB。
   - **叢集 ID**是NATS叢集的ID。
   - **TLS模式**是下拉清單，您可以在其中指定使用TLS加密的條件：
     - **已停用** （預設）—不使用 TLS 加密。
     - **啟用**— 啟用加密，但不進行驗證。
     - **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA的根憑證和金鑰會在程式安裝期間自動建立，並儲存在KUMA Core伺服器的資料夾/opt/kaspersky/kuma/core/certificates/中。

     使用TLS時，無法將IP位址指定為URL。
   - **URL選擇政策**是下拉清單，您可以在其中選擇一種方法來確定在指定多個URL的情況下將事件傳送到哪個URL：
     - **任何**。只要其中一個可用的URL可以接收事件，事件就會傳送到該URL。如果連線中斷（例如，接收節點斷開連線），則會選擇其他URL作為事件目標。
     - **第一優先**。事件將會傳送到已新增位址清單中的第一個URL。如果該URL不可用，事件將依序傳送到下一個可用節點。當第一個URL再次可用時，事件將再次開始傳送到此URL。
     - **均衡**意味著包含事件的套件均勻分發在清單中可用的URL中。由於封包是在目標緩衝區溢位或刷新計時器上傳送的，因此此URL選擇政策無法保證事件均勻分佈到目標。
   - **分隔符號**用於指定分隔事件的字元。預設使用 `\n`。
   - **路徑**— 如果選擇了**檔案**目標類型，則為檔案路徑。

- **緩衝區排清間隔** — 此欄位用於設定將資料傳送至目的地的時間間隔（以秒為單位）。預設值為`100`。
- **工作線程** — 此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
- 您可以使用**健康情況檢查路徑**和**健康情況檢查逾時**欄位設定健康情況檢查。您也可以透過選中**健康情況檢查已停用**核取方塊來停用健康情況檢查。
- **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。
- **磁碟緩衝區已停用**下拉清單用於啟用或停用磁碟緩衝區的使用。預設情況下，磁碟緩衝區是停用的。
- 在**篩選器**部分，您可以指定條件來定義此資源將處理的事件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。

  在資源中建立篩選器

  KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

  若要建立篩選器：

  1. 在**篩選器**下拉清單中，選擇**新建**。
  2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
  3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。
  4. 在**條件**下，指定事件必須滿足的條件：
     a. 點擊**新增條件**按鈕。
     b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。
     c. 在**運算子**下拉清單中，選擇一個運算子。

        篩選器運算子

        - **=** — 左運算元等於右運算元。
        - **<** — 左運算元小於右運算元。
        - **<=** — 左運算元小於或等於右運算元。
        - **>** — 左運算元大於右運算元。
        - **>=** — 左運算元大於或等於右運算元。
        - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
        - **contains** — 左運算元包含右運算元的值。

- **startsWith** — 左運算元以右運算元的某個值開頭。
- **endsWith** — 左運算元以右運算元的某個值末端。
- **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

4. 按一下**儲存**按鈕。

建立的目標顯示在安裝精靈頁籤上。可以透過選擇目標資源並在開啟的視窗中點選**刪除**，從資源集中刪除目標資源。

轉到精靈的下一個步驟。

步驟 7。設定驗證

這是安裝精靈所需的最後一步。在此步驟中，OSMP 會建立服務資源集，並根據此資源集自動建立服務：

- 關聯器的資源集顯示在**資源→關聯器**下。它可用於建立新的關聯器服務。當此資源集變更時，所有基於此資源集運行的服務將在服務重新啟動後開始使用新參數。為此，您可以點選**儲存並重新啟動服務**和**儲存並更新服務組態**按鈕。

  資源集可像其他資源一樣進行修改、複製、在資料夾之間移動、刪除、匯入及匯出。

- 服務顯示在**資源→活動服務**中。使用安裝精靈建立的服務會在 OSMP 內部執行功能。若要與網路基礎架構的外部部分進行通訊，您需要在伺服器和資產上安裝類似的外部服務。例如，外部關聯器服務應安裝在用於處理事件的伺服器上，外部儲存服務應安裝在已部署ClickHouse服務的伺服器上，外部代理服務應安裝在必須接收和轉送Windows事件的Windows資產上。

若要完成安裝精靈：

1. 按一下**建立並儲存服務**。

   安裝精靈的**安裝驗證**頁籤顯示一個服務表，其中列出了基於在安裝精靈中選擇的資源集所建立的服務。視窗下方顯示了一些命令範例，您必須使用這些命令在目標伺服器和資產上安裝這些服務的外部等效項。

   例如：

   ```
   /opt/kaspersky/kuma/kuma correlator --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
   - <port> 是用於與 KUMA Core 通訊的連接埠。
   - <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

     `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

     您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

     為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。

   - <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
   - <API port> 是用於與已安裝元件通訊的連接埠。

   「kuma」檔案位於安裝程式的/kuma-ansible-installer/roles/kuma/files/目錄中。

用於與 KUMA Core 通訊的連接埠、服務 ID、KUMA Core CA 憑證的指紋 ID，以及用於與服務通訊的連接埠，都會自動新增至命令中。您還必須確保 OSMP 的網路連線，並在必要時開啟其元件使用的連接埠。

2. 按一下**儲存**關閉精靈。

關聯器服務隨即在OSMP中建立。現在，必須在用於處理事件的伺服器上安裝等效服務。

在 OSMP 網路基礎設施中安裝關聯器

關聯器由兩部分組成：一部分在 OSMP 內建立，另一部分安裝在用於處理事件的網路基礎架構伺服器上。關聯器的第二部分安裝在網路基礎架構中。

若要安裝關聯器：

1. 登入要安裝服務的伺服器。
2. 建立/opt/kaspersky/kuma/資料夾。
3. 將「kuma」檔案複製到/opt/kaspersky/kuma/資料夾。該檔案位於安裝程式中的/kuma-ansible-installer/roles/kuma/files/資料夾中。

   確保kuma檔案具有足夠的執行權限。

4. 執行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
   - <port> 是 KUMA Core 用於內部通訊的連接埠（預設使用連接埠 7210）。
   - <fingerprint ID of the KUMA Core CA certificate> 是連線服務時用於身分驗證的 CA 憑證指紋 ID。

     `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

     您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

     為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。

   - <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
   - <API port> 是用於與已安裝元件通訊的連接埠。

   範例：

   ```
   sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
   ```

```
--api.port YYYY --install
```

您可以在安裝精靈的最後一步複製關聯器安裝命令。它會自動指定KUMA Core伺服器的位址和連接埠、待安裝關聯器的識別碼以及關聯器用於通訊的連接埠。安裝前，請確保KUMA元件的網路連線正常。

在同一主機上部署多個 KUMA 服務時，安裝過程中必須使用 `--api.port <port>` 參數，為每個元件指定不重複的連接埠。預設使用以下設定值：`--api.port 7221`。

關聯器隨即安裝。您可以使用它來分析事件中的威脅。

驗證關聯器安裝

若要驗證關聯器是否已準備好接收事件：

1. 在 OSMP 中，轉至**資源和服務 → 有效服務**區段。
2. 確保您安裝的關聯器處於綠色狀態。

若傳入關聯器的事件包含符合關聯規則篩選條件的事件，事件索引標籤將顯示這些事件，且這些事件會帶有 `DeviceVendor=Kaspersky` 與 `DeviceProduct=KUMA` 參數。觸發的關聯規則名稱會顯示為這些關聯事件的名稱。

如果沒有找到關聯事件

您可以建立一個更簡單的關聯規則版本來找尋可能的錯誤。使用一個**簡單的** 關聯規則和單一**輸出**操作。建議建立一個篩選器來找尋 OSMP 定期接收的事件。

更新、新增或刪除關聯規則時，必須更新關聯器的組態。

完成關聯規則測試後，必須從 OSMP 中刪除所有測試和臨時關聯規則，並更新關聯器的組態。

建立 correlator-ng 關聯器

correlator-ng 關聯器是 OSMP 元件，用於關聯及處理來自各種來源的事件。它允許使用關聯規則、選擇器和運算式來篩選、合併和分析事件。

目前版本的Kaspersky Next XDR Expert 包含測試版的correlator-ng，用於試運行。在correlator API的正式版本發布之前，方法、演算法、條件語法以及其他功能和特性可能會發生變化。

在目前版本中，關聯器只能使用YAML組態進行管理。從 KUMA Core 初次取得組態後，您可在檔案中進一步變更設定；無法使用 OSMP 網頁介面管理此關聯器。

Correlator-ng並非標準關聯器模型的直接替代品。

其主要區別在於：

- 規則和選擇器的新語法，與類似SQL的運算式和函式相容。
- 支援連接選擇器：來自不同選擇器的事件將按接收順序並行比較。
- 如果至少有一個選擇器達到其閾值，則`anyMatch`屬性可用於觸發關聯規則。
- 擴充函式集，用於處理資料類型、陣列、字串、時間戳記和CyberTrace欄位。
- 更嚴格的運算式類型要求，以及將欄位和變量值自動轉換為所需類型，以確保正確處理操作。
- 正規運算式語法已變更：correlator-ng使用類似PCRE的語法，而標準關聯器模型使用RE2。

correlator-ng的限制

當前correlator-ng的使用存在一些限制：

- 關聯器無法根據傳入事件自動對資產進行分類，也不支援通常在觸發回應規則時執行的操作。
- 關聯器無法自動使用外部來源（例如DNS查詢、用於計算和檢查的指令碼或CyberTrace系統）的附加資料來擴充事件。
- **儲存體**、**關聯器**和**內部**類型的目標僅在沒有磁碟緩衝區時才支援。
- `S.KL_EventRoute`欄位未新增至關聯事件。
- 關聯器無法使用下列附加欄位擴充關聯事件：`SourceAssetKSCInstanceID`、`SourceAssetKSCHostID`、`DestinationAssetKSCInstanceID`、`DestinationAssetKSCHostID`、`DeviceAssetKSCInstanceID`、`DeviceAssetKSCHostIDKSC`、`S.KL_SourceAccountDisplayName`、`S.KL_DestinationAccountDisplayName`。
- 僅支援部分範本：某些範本可能無法處理，且在某些情況下，`to_string`類型的函式可能無法運作。
- 可用的指標數量有限。
- `debug`參數不會變更日誌記錄等級。
- 儲存桶內容只能以JSON格式匯出。不支援匯入和搜尋儲存桶內容。
- 不支援收集和分析關聯統計資訊以進行效能最佳化。
- 正規運算式不支援 `(?=...)` 和 `(?<=...)` 等結構。
- 活動清單、快顯表單、字典和資產類別的連結必須使用唯一ID而不是名稱。

建立關聯器correlator-ng

目前版本的Kaspersky Next XDR Expert 包含測試版的correlator-ng，用於試運行。在correlator API的正式版本發布之前，方法、演算法、條件語法以及其他功能和特性可能會發生變化。

Correlator-ng作為獨立的KUMA服務部署。其設定由YAML組態檔和進程的命令列選項定義。啟動後，該服務與KUMA Core建立聯繫，接收規則和儲存桶的組態，並開始處理事件。

可以使用一組YAML檔案來管理correlator-ng。每個檔案如下所述。

Correlator-ng組態檔

檔案	描述
config.yaml	包含有關服務的基本信息，包括關聯器的名稱、描述和一般設定。
correlation-rules.yaml	包含關聯規則的組態，包括規則類型：標準、簡單、操作和定期。
selector-includes.yaml	包含關聯到關聯規則以實現重複使用的巢狀篩選器。
active-lists.yaml	包含活動清單的組態。
context-tables.yaml	包含快顯表單的組態。
dictionaries.yaml	包含用於選擇器和關聯規則的靜態字典。
global-variables.yaml	包含關聯規則和選擇器中可用的全域變數。
destinations.yaml	包含具有 ID 和傳送設定的事件目的地（ `storage` 、 `correlator` 、 `internal` ）。

文件在關聯器啟動時會依照以下順序載入：首先是config.yaml，然後是包含規則和選擇器的文件，接著是包含活動清單、快顯表單、字典和全域變數的檔案。目標檔案最後加載，以確保事件路由正確。

systemd-unit和關聯器的啟動

systemd-unit檔案用於將關聯器作為系統服務啟動；該檔案定義了correlator-ng的啟動、停止和重新啟動設定。

組態檔範例

```
[Unit]
Description=KUMA Correlator NG
StartLimitIntervalSec=1
After=network.target
[Service]
Type=simple
Restart=always
RestartPreventExitStatus=99
TimeoutSec=0
RestartSec=5
Environment="RUST_BACKTRACE=full"
User=kuma
Group=kuma
ExecStart=/opt/kuma correlator --id <correlator_service_ID> --core https://<FQDN_of_KUMA_Core>:7210 --wd
/opt/correlator-ng --api.port <correlator 的 API 連接埠>
LimitFSIZE=infinity
LimitCPU=infinity
LimitAS=infinity
LimitNOFILE=500000
LimitNPROC=64000
LimitMEMLOCK=infinity
TasksMax=infinity
TasksAccounting=false
```

```
[Install]
WantedBy=multi-user.target
```

correlator-ng日誌記錄

`--logger.filter`選項可設定correlator-ng的日誌記錄等級。在此選項中，您可以指定與標準`RUST_LOG`變數相同的日誌記錄等級：`trace`、`debug`、`info`、`warn`、`error`。

範例：

```
--logger.filter debug
```

您也可以使用`RUST_BACKTRACE`環境變數。將其設定為`full`可啟用擴充錯誤資訊的輸出。

correlator-ng 支援的資料類型

目前版本的Kaspersky Next XDR Expert 包含測試版的correlator-ng，用於試運行。在correlator API的正式版本發布之前，方法、演算法、條件語法以及其他功能和特性可能會發生變化。

與標準版本的關聯器相比，correlator-ng具有更嚴格的資料模型。這會影響關聯規則、選擇器和事件處理函式。事件、變數或選擇器的每個欄位現在都有定義的類型。自動類型轉換僅用於相容的類型；在其他情況下，必須使用 `to_string`、`to_integer` 和 `to_float` 轉換函式。

支援以下資料類型：

支援的資料類型

資料類型	描述
字串	字串
VecString	字串陣列
I64	64位元整數
VecI64	64位元整數數組
F64	浮點
VecF64	浮點陣列
時間戳記	UNIX時間戳記（以毫秒為單位）
VecTimestamp	UNIX時間戳記數組（以毫秒為單位）
Uuid	UUIDv4格式的唯一ID
VecUuid	UUIDv4值數組
Ip	IPv4 或 IPv6 位址
VecIp	IP位址數組
IpNet	帶有 CIDR 前綴的子網路，例如 `192.168.1.0/24`。
VecIpNet	子網路數組
布林值	布林值（`true` 或 `false`）
VecBool	布林值數組。

更強的類型控制提高了關聯器的效率，並減少了編譯關聯規則時的錯誤。但是，現在所有對數組、字串和時間戳記的操作都必須考慮資料類型，否則可能會發生運行時錯誤。

關聯規則選擇器和運算式

目前版本的Kaspersky Next XDR Expert 包含測試版的correlator-ng，用於試運行。在correlator API的正式版本發布之前，方法、演算法、條件語法以及其他功能和特性可能會發生變化。

在 correlator-ng 中，選擇器可以執行變數可執行的所有操作，並且可以使用函式來處理字串、陣列和數字（例如，`substring`、`tr`、`to_lower`）。使用函式無需建立單獨的變數；選擇器本身就可以使用這些函式。

選擇器使用適用於`WHERE`子句的 SQL 語法進行描述。

使用運算式設定選擇器和變數，以篩選和合併事件。它們支援與變數相同的操作，並能夠建立複雜的條件。有下列運算式類型可用：

編寫涉及常數的值比較運算式時，常數必須放在右邊。這樣，關聯器就可以套用各種最佳化措施。如果常數位於左側，則不進行最佳化。

常數

常數

常數	類型
`1`	I64（整數）
`3.14`	F64（浮點數）
`'myString'`	字串

參照值

參照值

參照	描述
`DeviceVendor`	`DeviceVendor` 事件欄位的值
`S.MyCustomField`	`S.MyCustomField` 複合欄位的值
`$myVariable`	`myVariable` 變數的值

邏輯運算子和群組運算子

邏輯運算子和群組運算子

運算式	描述
`<expression> AND <expression>`	邏輯AND運算子
`<expression> OR <expression>`	邏輯OR運算子
`NOT <expression>`	運算式結果的否定
`IS [NOT] NULL`	檢查值是否缺失（在 correlator-ng 中，未設定的值為 `NULL`）
`()`	分組運算式

比較運算子

比較運算子

運算式	描述
`<expression> = <expression>`	檢查值是否相等
`<expression> > <expression>`	使用 `>` 運算子比較值
`<expression> >= <expression>`	使用 `>=` 運算子比較值
`<expression> < <expression>`	使用 `<` 運算子比較值
`<expression> <= <expression>`	使用 `<=` 操作員比較值
`Type BETWEEN 1 AND 3`	檢查 `Type` 欄位的值是否介於 1 和 3 之間（含 1 和 3）

算術運算子

算術運算子

運算式	描述
`<expression> + <expression>`	加法
`<expression> - <expression>`	減法
`<expression> * <expression>`	乘法
`<expression> / <expression>`	分部
`<expression> % <expression>`	模除

功能

功能

功能	描述
`eq_fold (<left operand expression>, <right operand expression>)`	呼叫 `eq_fold` 函式。

有關可用函式的詳細資訊，請參閱correlator-ng中的資料處理功能部分。

標準關聯規則的屬性

目前版本的Kaspersky Next XDR Expert 包含測試版的correlator-ng，用於試運行。在correlator API的正式版本發布之前，方法、演算法、條件語法以及其他功能和特性可能會發生變化。

correlator-ng 中的**標準**關聯規則支援附加屬性，允許修改「完全相符」的條件並指定選擇器之間事件的匹配。這些屬性擴展了關聯規則桶的標準操作模型，並在分析已放入桶中的事件時應用。

目前correlator-ng的使用支援兩個屬性：

- `anyMatch`
- `joinSelector`

這兩個屬性僅適用於**標準**類型的關聯規則，並且直接用於規則本身的組態。

anyMatch屬性

在關聯器的標準模型中，當桶達到完全相符狀態時，即所有選擇器累積的事件數達到其閾值時，關聯規則就被認為已滿足。

如果在關聯規則的組態中指定 `anyMatch: true`，則當規則中的任何一個選擇器（**恢復**類型的選擇器除外）達到其閾值時，該桶會達到「完全相符」狀態。因此，規則由第一個滿足的條件觸發，無需等待其他選擇器累積事件。每個選擇器繼續根據其組態獨立累積事件，但是，一旦其中一個選擇器達到其閾值，關聯就會立即結束。

由此類規則產生的關聯事件還包含 `$KL_selectorName` 區域變數。此變數的值等於觸發規則的閾值選擇器的標籤。這使得我們可以識別觸發來源，並對結果應用各種後續處理步驟。

> 包含 `anyMatch` 屬性的規則不支援 **逾時時** 類型的觸發器。

JoinSelector屬性

在關聯器的標準模型中，當桶達到完全相符狀態時，即所有選擇器累積的事件數達到其閾值時，關聯規則就被認為已滿足。

如果在關聯規則的組態中指定 `anyMatch: true`，則當規則中的任何一個選擇器（**恢復**類型的選擇器除外）達到其閾值時，該桶會達到「完全相符」狀態。因此，規則由第一個滿足的條件觸發，無需等待其他選擇器累積事件。每個選擇器繼續根據其組態獨立累積事件，但是，一旦其中一個選擇器達到其閾值，關聯就會立即結束。

由此類規則產生的關聯事件還包含 `$KL_selectorName` 區域變數。此變數的值等於觸發規則的閾值選擇器的標籤。這使得我們可以識別觸發來源，並對結果應用各種後續處理步驟。

> 包含 `anyMatch` 屬性的規則不支援 **逾時時** 類型的觸發器。

JoinSelector屬性

`joinSelector` 屬性允許在達到「完全相符」狀態之前，額外檢查同一儲存桶內不同選擇器累積的事件之間的相關性。

該屬性的值是類似 SQL 的運算式，`joinSelector: <運算式>`

此運算式指定了比較不同選擇器事件的條件。它必須是二元運算或函式，且其運算元只能是常數，以及 `with_selector('<selector_tag>', <運算式>)` 形式的運算式。

`with_selector` 函式表示運算式會針對特定選擇器的事件進行評估。

解析組態時，關聯器會自動決定參與運算式的所有選擇器中該選擇器的最小上限值。比較僅針對事件數等於此最小值的情況執行。

例如：

選擇器A的選擇器閾值（事件數）為5，選擇器B的選擇器閾值為9。在運算式 `with_selector('A', DeviceHostName) = with_selector('B', DeviceHostName)` 中，僅比較每個選擇器的前五個事件。

事件依到達順序並行比較：選擇器A的第一個事件與選擇器B的第一個事件進行比較；第二個事件與第二個事件進行比較，依此類推。

`joinSelector` 屬性也可以使用函式。例如：`joinSelector: contains_fold(with_selector('A', $var_A), with_selector('B', DeviceCustomString1))`

此範例使用 `contains_fold` 函式，該函式會檢查為選擇器A計算的 `$var_A` 關聯器變數值是否存在於選擇器B事件的 `DeviceCustomString1` 欄位中，且不區分大小寫。

`joinSelector` 屬性的運算式不支援以下函式：

- `has_ti_detect`
- `has_ti_detect_with_category`
- `has_ti_detect_with_indicator`
- `has_ti_detect_with_category_and_indicator`

correlator-ng中的資料函式

目前版本的Kaspersky Next XDR Expert 包含測試版的correlator-ng，用於試運行。在correlator API的正式版本發布之前，方法、演算法、條件語法以及其他功能和特性可能會發生變化。

correlator-ng中的函式用於選擇器和變數中，以處理事件資料、類型轉換和篩選。

通用語法：

- 必要參數包含在 `< >` 中，選用參數包含在 `[ ]` 中。
- 三個點 `...` 代表不定數量的參數。
- 傳回類型以 `-> <data type>` 表示。字母 `T` 表示類型取決於參數的類型。
- 參數的類型可以是具體類型（例如 `String`、`I64`），也可以是 `T`，這表示任何可用的資料類型。

類型轉換函式

這些函式將值轉換為特定類型。

類型轉換函式

函式	描述
`to_string(< 運算式 >)`	將值轉換為字串。
`to_integer(< 運算式 >)`	將值轉換為整數（I64）。
`to_float(< 運算式 >)`	將數值轉換為浮點數（F64）。
`to_uuid(< 運算式 >)`	將值轉換為UUIDv4。
`to_ip(< 運算式 >)`	將值轉換為IPv4或IPv6位址。
`to_ip_net(< 運算式 >)`	將值轉換為IPNet子網路。
`to_bool(< 運算式 >)`	將值轉換為布林值。
`to_timestamp(< 運算式 >, '[ 時區 ]')`	將數值轉換為時間戳記，並可選擇是否包含時區。

用於比較值的函式

用於比較值的函式

函式	描述
eq_fold(< 左運算元 >, < 右運算元 >) -> Bool	檢查左側值是否與右側值相同，忽略大小寫。
eq_any(< 左運算元 >, < 右運算元 1>, [...]) -> Bool	檢查右側的值是否與左側的值相同。
eq_any_fold(< 左運算元 >, < 右運算元 >, [...]) -> Bool	將左側值與多個右側值進行比較，忽略大小寫。
contains(< 左運算元 >, < 右運算元 >) -> Bool	檢查左側值是否包含右側值。
contains_fold(< 左運算元 >, < 右運算元 >) -> Bool	檢查左側值是否包含右側值，忽略大小寫。
contains_any(< 左運算元 >, < 右運算元 1>, [...]) -> Bool	檢查左側值是否包含右側的任何值。
contains_any_fold(< 左運算元 >, < 右運算元 >, [...]) -> Bool	檢查左側值是否包含右側值中的任何值，忽略大小寫。
starts_with(< 左運算元 >, < 右運算元 >) -> Bool	檢查右側值是否為左側值的前綴。
starts_with_fold(< 左運算元 >, < 右運算元 >) -> Bool	檢查前綴，不區分大小寫。
starts_with_any(< 左運算元 >, < 右運算元 1>, [...]) -> Bool	檢查其中一個右側值是否為左側值的前綴。
starts_with_any_fold(< 左運算元 >, < 右運算元 1>, [...]) -> Bool	檢查其中一個右側值的前綴，不區分大小寫。
ends_with(< 左運算元 >, < 右運算元 >) -> Bool	檢查右側值是否為左側值的後綴。
ends_with_fold(< 左運算元 >, < 右運算元 >) -> Bool	檢查後綴，不區分大小寫。
ends_with_any(< 左運算元 >, < 右運算元 1>, [...]) -> Bool	檢查其中一個右側值是否為左側值的後綴。
ends_with_any_fold(< 左運算元 >, < 右運算元 1>, [...]) -> Bool	檢查後綴，不區分大小寫。
match(< 左運算元 >, < 右運算元 >) -> Bool	檢查左側值是否與右側的正規運算式相符。
match_any(< 左運算元 >, '< 右運算元 1>', '[右運算元 2]', [...]) -> Bool	檢查左側值是否與右側的某個正規運算式相符。

用於處理活動列表、字典和快顯表單的函式

用於處理活動列表、字典和快顯表單的函式

函式	描述
in_active_list('< 活動清單 ID >', < 金鑰元素 1>, [...]) -> Bool	依鍵檢查活動清單中是否存在某個值。
in_context_table('< 快顯表單 ID >', '< 金鑰欄位名稱 1>', < 金鑰欄位值 1>, '[金鑰欄位名稱 2]', [金鑰欄位值 2], [...]) -> Bool	依鍵檢查快顯表單中是否存在值。
in_dictionary('< 字典 ID >', < 金鑰元素 1>, [金鑰元素 2], ...) -> Bool	依鍵檢查字典中是否存在某個值。
dict('< 字典 ID >', < 金鑰 1>, [...]) -> String	按金鑰從字典中傳回一個值。
table_dict('< 字典 ID >', < 欄名稱 >, < 金鑰 1>, [...]) -> String	從表格字典中傳回一個值。
active_list('< 活動清單 ID >', < 欄位名稱 >, < 金鑰 1>, [...]) -> String	從活動清單中傳回一個值。
context_table('< 快顯表單 ID >', '< 欄位名稱 >', '< 金鑰欄位 >', < 值 >) -> T	從快顯表單傳回某個欄位的值。
context_table_list_item('< 快顯表單 ID >', '< 欄位名稱 >', < 索引 >, ...) -> T	從快顯表單中傳回陣列元素。
match_active_list(...)	如果金鑰與正規運算式相符，則從活動清單中傳回一個值。
match_context_table(...)	如果正規運算式匹配，則從快顯表單中傳回一個值。
match_dictionary(...)	如果正規運算式匹配，則從字典中傳回一個值。

子網路功能

子網路功能

函式	描述
`in_subnet(< 左運算元 >, < 子網路 >) -> Bool`	檢查IP位址是否屬於某個子網路。
`in_subnet_any(< 左運算元 >, < 子網路  1>, [...]) -> Bool`	檢查IP位址是否屬於某個子網路。
`in_subnet_active_list(...)`	檢查IP位址是否屬於活動清單中的子網路。
`in_subnet_context_table(...)`	檢查IP位址是否屬於快顯表單中的子網路。
`in_subnet_dictionary(...)`	檢查IP位址是否屬於字典中的子網路。

字串函式

字串函式

函式	描述
`to_lower(< 運算元 >) -> String`	將字串轉換為小寫。
`to_upper(< 運算元 >) -> String`	將字串轉換為大寫。
`substring(< 字串 >, < 子字串開頭 >, [ 子字串結尾 ]) -> String`	傳回一個子字串。
`index_of(< 搜尋內容 >, < 搜尋位置 >) -> I64`	傳回首次出現的位置。
`last_index_of(< 搜尋內容 >, < 搜尋位置 >) -> I64`	傳回最後一次出現的位置。
`tr(< 運算元 >) -> String`	刪除字串開頭和結尾的空白字元。
`replace(< 字串 >, < 子字串 >, < 替換 >) -> String`	替換子字串。
`regexp_replace(< 字串 >, '< 正規運算式 >', '< 替換 >') -> String`	使用正規運算式替換子字串。
`regexp_capture(< 字串 >, '< 正規運算式 >') -> String`	取得與正規運算式相符的子字串。
`str_join('< 分隔符號 >', < 字串  1>, [...]) -> String`	連接多個字串。

陣列函式

陣列函式

函式	描述
`append(< 左運算元 >, < 右運算元 >, '[ 分隔符號 ]') -> T`	在陣列或字串末尾添加一個值。
`prepend(< 左運算元 >, < 右運算元 >, '[ 分隔符號 ]') -> T`	在陣列或字串開頭添加一個值。
`len(< 運算元 >) -> I64`	傳回字串或陣列的長度。
`item(< 陣列 >, < 索引 >) -> T`	透過索引在陣列中傳回一個元素。
`distinct_items(< 陣列 >) -> T`	從陣列中取得唯一元素。
`sort_items(< 陣列 >, '< 排序順序 >') -> T`	對陣列進行排序。

時間戳記函式

時間戳記函式

函式	描述
`now() -> Timestamp`	傳回當前時間戳記。
`year(<timestamp>) -> I64`	傳回年份。
`month(<timestamp>) -> I64`	傳回月份。
`month_str(<timestamp>) -> String`	以字串形式傳回月份。

函式	描述
`weekday(<timestamp>) -> I64`	傳回星期幾。
`weekday_str(<timestamp>) -> String`	以字串形式傳回星期幾。
`day(<timestamp>) -> I64`	傳回月份日期。
`hour(<timestamp>) -> I64`	傳回小時數。
`minute(<timestamp>) -> I64`	傳回分鐘數。
`second(<timestamp>) -> I64`	傳回秒數。
`millisecond(<timestamp>) -> I64`	傳回毫秒數。
`format_timestamp(<timestamp>, '< 格式 >') -> String`	將時間戳記轉換為字串。
`truncate_timestamp(<timestamp>, '< 持續時間 >') -> Timestamp`	將時間戳記四捨五入為整數值。

時間函式

時間函式

函式	描述
`duration_days(<t1>, <t2>) -> I64`	傳回天數差值。
`duration_hours(<t1>, <t2>) -> I64`	傳回小時差值。
`duration_minutes(<t1>, <t2>) -> I64`	傳回分鐘差值。
`duration_seconds(<t1>, <t2>) -> I64`	傳回秒差值。
`duration_milliseconds(<t1>, <t2>) -> I64`	傳回毫秒差值。

數學函式

數學函式

函式	描述
`round(< 運算元 >) -> I64`	將數值四捨五入到最接近的整數。
`ceil(< 運算元 >) -> I64`	將數值向上取整。
`floor(< 運算元 >) -> I64`	將數值向下取整。
`abs(< 運算元 >) -> T`	傳回數值絕對值。
`pow(< 運算元 >, '< 冪次 >') -> T`	將數值提升到冪。
`math_min(< 陣列 >) -> T`	傳回陣列中的最小元素。
`math_max(< 陣列 >) -> T`	傳回陣列中的最大元素。
`math_avg(< 陣列 >) -> F64`	傳回陣列中的平均值。

資料解碼與分析函式

資料解碼與分析函式

函式	描述
`decode_hex_integer(< 字串 >) -> I64`	將十六進位字串轉換為數字。
`decode_hex(< 字串 >) -> String`	解碼十六進位字串。
`decode_base64(< 字串 >) -> String`	解碼Base64字串。
`decode_url(< 字串 >) -> String`	解碼URL編碼字串。
`entropy(< 字串 >) -> F64`	計算字串的Shannon熵。

函式	描述
`has_bit(< 左運算元 >, < 位置 >) -> Bool`	檢查位元是否設定在指定位置。
`has_vulnerability(< 資產 ID >, (<CVE>), [ 嚴重程度 ]) -> Bool`	檢查資產是否有弱點。

其他函式

其他函式

函式	描述
`include('< 謂詞 ID >', '[ 謂詞名稱 ]')`	使用selector-includes.yaml檔案中的預定義謂詞。
`ti('< 類別 >', < 指標 >, '< 欄位 >')`	從專門的TI欄位（CyberTrace）中檢索值。
`with_selector(' 關聯規則選擇器標籤 ', < 運算式 >)`	只能在關聯規則的 `joinSelector` 屬性中使用，用於區分事件集。
`template('< 範本 >', [ 引數 1], [ 引數 2], ...) -> String`	根據範本產生字串，方法是將事件欄位或變數的值插入範本中。
`conditional('< 謂詞 >', <then>, <else>)`	根據謂詞的結果，傳回兩個值之一。
`has_ti_detect*()`	依類別或指標檢查CyberTrace觸發。
`has_ti_detect_with_category('< 類別 >')`	依類別檢查CyberTrace觸發。
`has_ti_detect_with_indicator(< 指標 >)`	依指標檢查CyberTrace觸發。
`has_ti_detect_with_category_and_indicator('< 類別 >', < 指標 >)`	依類別和指標檢查CyberTrace觸發。

建立事件路由器

事件路由器是一種服務，可讓您從收集器和關聯器接收事件流，然後根據設定的篩選器將事件分發到指定的目標。

若要將收集器中的事件傳送至事件路由器，必須建立包含事件路由器位址的 `eventRouter` 目的地資源，並將該資源連結至要將事件傳送至事件路由器的收集器。

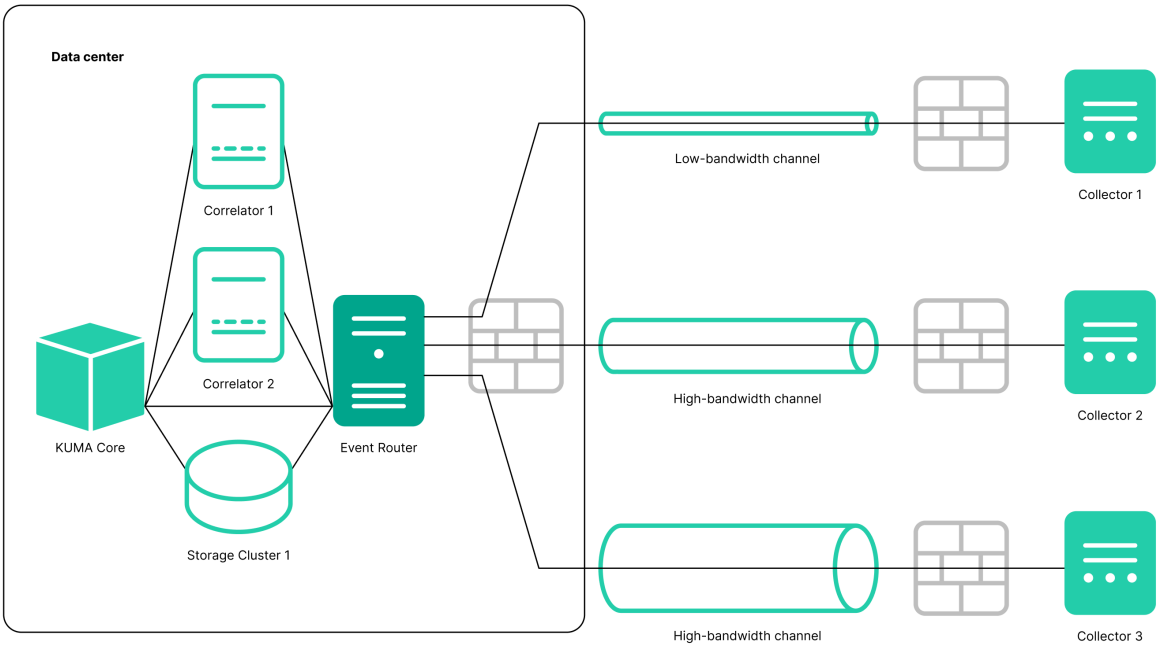
事件路由器會像 `storage` 與 `correlator` 目的地一樣，透過 API 連接埠接收事件。

您可以在**資源**部分建立路由器。

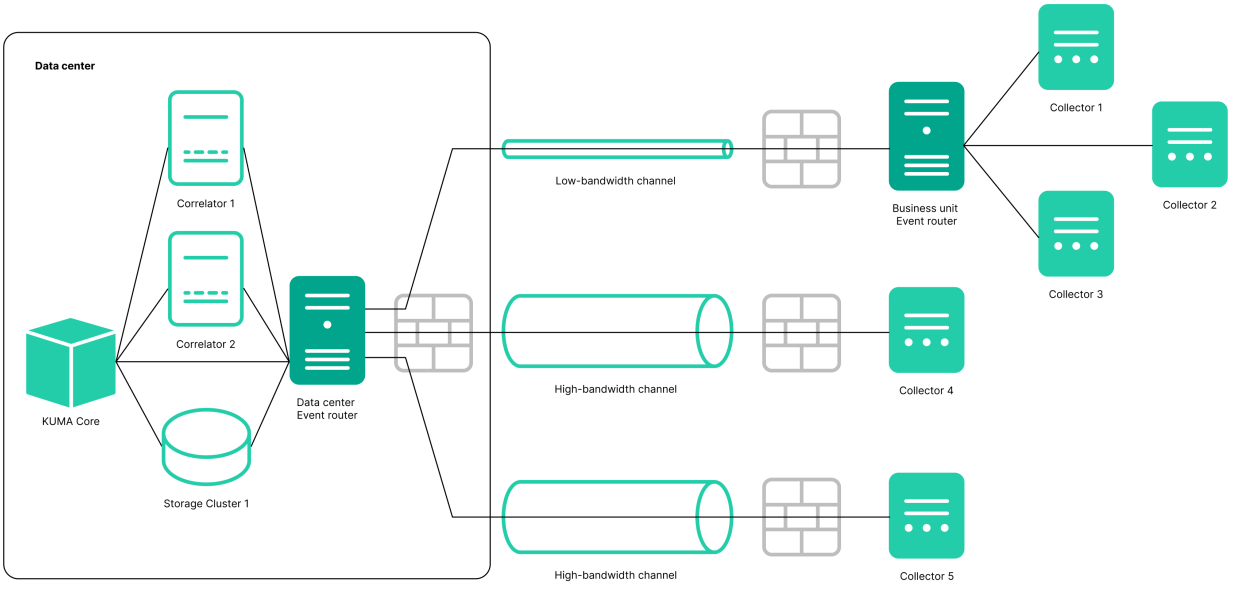
使用事件路由器可以降低連結利用率，這對於低頻寬和繁忙的連結非常重要。

可能的用例：

連接器 — 資料中心內的事件路由器



級聯連線：多個收集器 — 分支機構的事件路由器；分支機構的事件路由器 — 資料中心內的事件路由器



事件路由器必須安裝在Linux裝置上。只有具有主管理員角色的使用者才能建立該服務。您可以在任何租用戶中建立服務；租用戶關係不施加任何限制。

您可以使用以下指標來取得有關服務效能的資訊：

- IO
- Process
- 作業系統

與其他資源一樣，OSMP中的事件路由器會產生下列稽核事件：

- 資源新增成功
- 資源更新成功
- 資源刪除成功

安裝事件路由包含兩個步驟：

1. 使用安裝精靈在OSMP中建立事件路由服務。
2. 在伺服器上安裝事件路由服務。

啟動事件路由器安裝精靈

若要啟動事件路由器安裝精靈：

1. 在 OSMP 的主功能表中，於 **資源和服務** 區段，點擊 **事件路由器**。
2. 在開啟的**事件路由器**視窗中，點擊**新增**按鈕。

遵照精靈的說明。

步驟 1。事件路由器的一般設定

這是安裝精靈的必要步驟。在此步驟中，您將指定事件路由器的主要設定：其名稱以及將擁有它的租用戶。

若要指定事件路由器的基本設定：

1. 在**名稱**欄位中，輸入要建立的服務的唯一名稱。此名稱必須包含1到128個Unicode字元。
2. 在**租用戶**下拉清單中，選擇將擁有該事件路由器的租用戶。屬於租用戶的事件路由器本質上是組織性的，不施加任何限制。
3. 根據需要，在**事件處理器**欄位中指定服務可以並發執行的進程數。預設情況下，事件處理器的數量與安裝服務的伺服器上的vCPU數相同。
4. 如有需要，請使用**偵錯**切換開關來啟用服務操作記錄。
5. 您可以選擇在**描述**欄位中新增最多4000個Unicode字元來描述服務。

事件路由器的基本設定隨即配置。轉到精靈的下一個步驟。

步驟 2。路由

這是安裝精靈的必要步驟。我們建議將事件傳送到至少兩個目標：傳送到關聯器進行分析和傳送到儲存體進行儲存。您也可以選擇另一個事件路由器作為目標。

若要指定事件路由器將從收集器接收的事件傳送到的目標設定：

1. 在安裝精靈的**路由**步驟中，按一下**新增**。
2. 這將開啟**建立目的地**視窗；在該視窗中，指定以下設定：
   a. 在**基本設定**頁籤的**名稱**欄位中，輸入目標的唯一名稱。此名稱必須包含1到128個Unicode字元。
   b. 您可以根據需要使用**狀態**切換開關來啟用或停用該服務。
   c. 在**類型**下拉清單中，選擇目標的類型。以下值可用：
      - nats-jetstream
      - tcp
      - http
      - kafka
      - file
      - 儲存體
      - 關聯器
      - eventRouter
   d. 在**進階設定**頁籤，指定參數值。可設定的參數集取決於在**基本設定**頁籤選擇的目標類型。對於參數及其值的詳情，請按一下本說明「c」段中每種目標類型的連結。

建立的目標顯示在安裝精靈頁籤上。可以透過選擇目標資源並在開啟的視窗中點選**刪除**，從資源集中刪除目標資源。

路由隨即設定。轉到精靈的下一個步驟。

步驟 3。設定驗證

這是安裝精靈所需的最後一步。

若要在安裝精靈中建立事件路由器：

1. 按一下**建立**並儲存服務。
   視窗下部顯示在伺服器上事件路由器必須使用的命令。

範例命令：

```
/opt/kaspersky/kuma/kuma eventrouter --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
- <port> 是用於與 KUMA Core 通訊的連接埠。
- <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
- <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
- <API port> 是用於與已安裝元件通訊的連接埠。

用於與 KUMA Core 通訊的連接埠、CA 憑證指紋 ID、服務 ID，以及用於與服務通訊的連接埠會自動新增至命令中。您還必須確保 OSMP 的網路連線，並在必要時開啟其元件使用的連接埠。

2. 按一下**儲存**關閉精靈。

服務已安裝在 OSMP 中。現在您可以繼續在 OSMP 網路基礎設施中安裝服務。

在伺服器上安裝事件路由器

若要在伺服器上安裝事件路由器：

1. 登入要安裝事件路由服務的伺服器。
2. 建立/opt/kaspersky/kuma/資料夾。
3. 將「kuma」檔案複製到/opt/kaspersky/kuma/目錄。該檔案位於安裝程式中的/kuma-ansible-installer/roles/kuma/files/目錄中。
4. 確保kuma檔案具有足夠的執行權限。如果此檔案不可執行，請使其可執行：

   ```
   sudo chmod +x /opt/kaspersky/kuma/kuma
   ```
5. 將/kuma-ansible-installer/roles/kuma/files/目錄中的 LICENSE 檔案放置於/opt/kaspersky/kuma/目錄中，並執行以下命令接受最終使用者產品授權協議的條款和條件：

   ```
   sudo /opt/kaspersky/kuma/kuma license
   ```

6. 建立「kuma」使用者：

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

7. 使「kuma」使用者成為/opt/kaspersky/kuma目錄及其內所有檔案的擁有者：

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/
```

8. 將OSMP事件路由器連接埠新增至防火牆排除項。

為了使程式正常運行，請確保OSMP元件能夠透過安裝OSMP元件時指定的協定和連接埠，透過網路與其他元件和程式互動。

9. 執行以下命令：

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://<FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
- <port> 是 KUMA Core 用於內部通訊的連接埠（預設使用連接埠 7210）。
- <fingerprint ID of the KUMA Core CA certificate> 是連線服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。

- <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
- <API port> 是用於與已安裝元件通訊的連接埠。

範例：

```
sudo /opt/kaspersky/kuma/kuma eventrouter --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX --api.port YYYY --install
```

事件路由器隨即安裝在伺服器上。您可以使用它來接收來自收集器的事件，並將事件轉發到指定目標。

建立收集器

收集器由兩部分組成：一部分在 OSMP 內建立，另一部分安裝在用於接收事件的網路基礎架構中的伺服器上。

KUMA主控台中的操作

使用安裝精靈在 OSMP 中建立收集器。此精靈將必要的資源組合成收集器的資源集。完成精靈後，服務本身將基於資源集自動建立。

若要在 OSMP 中建立收集器，

啟動收集器安裝精靈：

- 在 OSMP 的主功能表中，於 **資源和服務** 區段，點擊 **新增事件來源**。
- 在 OSMP 的主選單中，於 **資源和服務 → 收集器** 區段，點擊 **新增收集器**。

完成精靈的步驟後，將在 OSMP 中建立收集器服務。

收集器的資源集包括以下資源：

- 收集器
- 標準化器（至少一個）
- 篩選器（如果需要）
- 彙總規則（如果需要）
- 擴充規則（如有需要）；
- 目標（通常定義兩個，用於將事件傳送到關聯器和儲存體）

這些資源可以提前準備好，也可以在安裝精靈執行時建立它們。

OSMP收集器伺服器上的操作

在打算用於接收事件的伺服器上安裝收集器時，執行安裝精靈最後一步顯示的命令。安裝時，您必須指定在 OSMP 中自動指派給服務的ID，以及用於通訊的連接埠。

測試安裝

建立收集器後，建議您確保它正常運作。

啟動收集器安裝精靈

收集器由兩部分組成：一部分在 OSMP 內建立，另一部分安裝在用於接收事件的網路基礎架構伺服器上。安裝精靈將建立收集器的第一部分。

若要啟動收集器安裝精靈：

- 在 OSMP 的主功能表中，於 **資源和服務** 區段，點擊 **新增事件來源**。
- 在 OSMP 的主選單中，於 **資源和服務 → 收集器** 區段，點擊 **新增收集器**。

遵照精靈的說明。

除了精靈的第一步和最後一步之外，可以任意順序執行精靈的步驟。您可以使用 **下一步** 和 **上一步** 按鈕，或按一下視窗左側的步驟名稱，在各步驟之間切換。

精靈完成後，會在 OSMP 的 **資源與服務** → **資源和服務** 下建立收集器，並在 **資源與服務** → **資源和服務** 下新增有效服務。

步驟 1。連線事件來源

這是安裝精靈的必要步驟。在此步驟中，您將指定收集器的主要設定：其名稱以及將擁有它的租用戶。

若要指定收集器的基本設定：

1. 在**收集器名稱**欄位中，為您正在建立的服務輸入一個唯一的名稱。此名稱必須包含1到128個Unicode字元。

   建立某些類型的收集器時，名為「代理：<收集器名稱>，自動建立」的代理程式也會與收集器一起自動建立。如果此類代理程式之前已建立且尚未刪除，則無法建立名為<收集器名稱>的收集器。在這種情況下，您必須為收集器指定其他名稱或刪除先前建立的代理程式。

2. 在**租用戶**下拉式清單中，選取您要指定為收集器擁有者的租用戶。租用戶選擇決定了建立收集器時可用的資源。

   如果您從安裝程式的另一個後續步驟返回此視窗並選擇另一個租用戶，則必須手動編輯已新增至服務的所有資源。只有選定租用戶和共用租用戶的資源才能新增至服務。

3. 如果需要，在**工作線程**欄位中指定服務可以並發運行的進程數。預設情況下，工作進程數與安裝服務的伺服器上的vCPU數相同。

4. 如有必要，請使用**偵錯**下拉清單啟用服務運作日誌記錄。

   即使停用偵錯模式，收集器服務的錯誤訊息也會被記錄。您可以在安裝收集器的電腦上，於 /opt/kaspersky/kuma/collector/<collector ID>/log/collector 目錄中檢視日誌。

5. 您可以選擇在**描述**欄位中新增最多256個Unicode字元來描述服務。

指定收集器的主要設定。轉到精靈的下一個步驟。

步驟 2。傳輸

這是安裝精靈的必要步驟。在安裝精靈的**傳輸**頁籤上，選擇或建立連接器，並在其設定中指定收集器服務的事件來源。

若要將現有連接器新增至資源集，

請從**連接器**下拉清單中選擇所需連接器的名稱。

安裝精靈的**傳輸**頁籤顯示所選連接器的設定。您可以使用 按鈕，在新的瀏覽器頁籤中開啟所選連接器進行編輯。

若要建立新連接器：

1. 從**連接器**下拉清單中選擇**新建** 。
2. 在**類型**下拉清單中，選擇連接器類型，並在**基本設定**和**進階設定**頁籤中指定其設定。可用的設定取決於所選的連接器類型：

   - tcp
   - udp
   - netflow
   - sflow
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - ftp
   - nfs
   - wmi
   - wec
   - snmp

   在標準化階段使用tcp或udp連接器類型時，如果DeviceAddress事件欄位為空，則接收事件的資產的IP位址將寫入該欄位。

   使用**wmi**或**wec**連接器時，將自動建立用於接收Windows事件的代理程式。

   建議使用預設編碼（UTF-8），並且僅當在事件欄位中接收到位字元時才套用其他設定。

若要使 OSMP 收集器監聽 1,000 以下的連接埠，需以根權限執行相關收集器的服務。為此，在安裝收集器後，請將 `AmbientCapabilities = CAP_NET_BIND_SERVICE` 這一行新增至其 systemd 設定檔的 [Service] 區段。
systemd 檔案位於 /usr/lib/systemd/system/kuma-collector-<收集器 `ID`>.service 目錄中。

連接器將會新增到收集器的資源集中。建立的連接器僅可在此資源集中使用，且不會顯示在網頁介面**資源和服務 → 連接器**區段中。

轉到精靈的下一個步驟。

步驟 3。事件解析

這是安裝精靈的必要步驟。在安裝精靈的**事件解析**頁籤上，選擇或建立一個標準化器，其設定將定義將原始事件轉換為標準化事件的規則。您可以為標準化器新增多個事件解析規則以實現複雜的事件處理邏輯。您可以使用測試事件來測試標準化器。

在安裝精靈中建立新的標準化器時，預設情況下它會保存在收集器的資源集中，不能在其他收集器中使用。**儲存標準化器**核取方塊可讓您將標準化器建立為單獨的資源，在這種情況下，可以在租用戶的其他收集器中選擇此標準化器。

如果在變更收集器資源集的設定時，更改或刪除連線到它的標準化器中的轉換，則編輯將不會儲存，並且標準化器本身可能會損壞。如果需要修改已經是服務一部分的標準化器中的轉換，則必須直接在網頁介面中的**資源→標準化器**下對標準化器進行變更。

新增標準化器

若要將現有的標準化器新增至資源集：

1. 按一下**新增事件解析**按鈕。

   這將開啟**基本事件解析**視窗，其中標準化器設定和**標準化方案**頁籤處於活動狀態。

2. 在**標準化器**下拉清單中，選擇所需的標準化器。下拉清單包括屬於收集器租用戶和共用租用戶的標準化器。

   基本事件解析視窗顯示所選標準化器的設定。

   如果要編輯標準化器設定，請在**標準化器**下拉清單中，按一下相關標準化器名稱旁邊的鉛筆圖示。這將開啟具有深色圓圈的**編輯標準化器**視窗。點擊深色圓圈將開啟**基本事件解析**視窗，您可以在其中編輯標準化器設定。

   如果要編輯進階解析設置，請將遊標移到深色圓圈上，以顯示加號圖示；按一下加號圖示即可開啟**進階事件解析**視窗。有關設定進階事件解析的詳細愛心，請參閱以下說明。

3. 點擊**確定**。

標準化器在安裝精靈的**基本事件解析**頁籤上顯示為深色圓圈。按一下圓圈將開啟標準化器選項以供檢視。

若要在收集器中建立新的標準化器：

1. 在事件解析步驟的**解析結構**頁籤上，按一下**新增事件解析**。

   這將開啟**基本事件解析**視窗，其中標準化器設定和**標準化方案**頁籤處於活動狀態。

2. 如果要將標準化器儲存為單獨的資源，請選取**儲存標準化器**核取方塊；這使得已儲存的標準化器可用於租用戶的其他收集器。預設情況下，未選取此核取方塊。

3. 在**名稱**欄位中，輸入標準化器的唯一名稱。此名稱必須包含1到128個Unicode字元。

4. 在**解析方法**下拉清單中，選擇要接收的事件類型。根據您的選擇，您可以使用預設定的規則來符合事件欄位或設定您自己的規則。當您選擇某些解析方法時，可能需要填寫其他設定欄位。

   可用的解析方法：

   - **json**

     此解析方法用於處理JSON資料，其中每個物件（包括其嵌套物件）在檔案中佔用一行。

     在處理具有階層結構資料的檔案時，您可以指定以句點分隔的參數名稱，存取嵌套物件的欄位。例如，可使用 `user.username` 查詢來存取字串 `"user": {"username": "system: node: example-01"}` 中的 `username` 參數。

     檔案將逐行處理。具有嵌套結構的多行物件可能無法正確標準化。

     在使用額外標準化器的複雜標準化方案中，所有嵌套物件都會在第一個標準化層級進行處理；但若未指定額外的標準化條件，正在處理的整個事件就會傳送至額外標準化器。

     換行字元可以是`\n`和`\r\n`。字串必須採用UTF-8編碼。

     如果要傳送原始事件進行進階標準化，請在**進階事件解析**視窗的每個巢狀層級上，在**保留原始事件**下拉清單中選擇**是**。

   - **cef**

     此解析方法用於處理CEF資料。

     選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。

   - **regexp**

     此解析方法用於建立自訂規則，以使用正規運算式的格式處理資料。

     在**標準化**參數區塊的欄位中，新增含有具名擷取群組的正規運算式（使用 RE2 語法）。群組的名稱和值會分別視為原始事件的欄位及其值，並可轉換為 KUMA 格式的事件欄位。

     若要新增事件處理規則：

     1. 將您要處理的資料範例複製到**事件範本**欄位。這是可選的，但建議執行的步驟。

        您也可以點選**使用 KIRA 產生規則運算式**，使用 KIRA 產生規則運算式。在此情況下，產生的規則運算式將自動新增至**標準化**參數區塊。

     2. 在**標準化**參數區塊的欄位中，新增使用 RE2 語法且含有具名擷取群組的正規運算式，例如「(?P<name>regexp)」。新增至**標準化**參數的正規運算式必須與事件完全相符。此外，編寫正規運算式時，建議使用符合文字起始和結束位置的特殊字元：^、$。

        您可以按一下**新增正規運算式**按鈕，新增多個正規運算式。如果需要移除正規運算式，請按一下✕按鈕。

3. 按一下**將欄位名稱複製到對應表**按鈕。

擷取群組名稱顯示在**對應**表的**KUMA欄位**列中。現在，您可以在每個擷取群組旁的欄中選取對應的 KUMA 欄位。如果您依照 CEF 格式命名擷取群組，也可以選取**使用 CEF 語法進行標準化**核取方塊，使用自動 CEF 對應。

已新增事件處理規則。

- **syslog**

  此解析方法用於處理syslog格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。

- **csv**

  此解析方法用於建立處理CSV資料的自訂規則。

  選擇此方法時，您必須在**分隔符號**欄位中指定字串中各值之間的分隔符號。任何單位元組 ASCII 字元都可以用作分隔符號。

- **kv**

  此解析方法用於處理鍵值對格式的資料。

  如果選擇此方法，您必須在下列必填欄位中提供值：

  - **配對分隔符號**—指定用來分隔鍵值對的字元。您可以指定任何單一字元（1位元組）的值，但該字元不得與值分隔符號相同。

  - **值分隔符號**—指定用來分隔金鑰和值的字元。您可以指定任何單一字元（1位元組）的值，但該字元不得與鍵值對的分隔符號相同。

- **xml**

  此解析方法用於處理 XML 資料。檔案中的每個物件（包括其巢狀物件）各佔一行。檔案將逐行處理。

  如果要傳送原始事件進行進階標準化，請在**進階事件解析**視窗的每個巢狀層級上，在**保留原始事件**下拉清單中選擇**是**。

  選擇此方法後，您可以在**XML 屬性**參數區塊中指定要從標籤擷取的金鑰屬性。如果 XML 結構中的同一個標籤具有多個值不同的屬性，您可以在**對應**表格的**來源**欄中指定所需值的金鑰。

  若要新增 XML 金鑰屬性，

  按一下**新增欄位**按鈕，然後在顯示的視窗中指定所需屬性的路徑。

  您可以新增多個屬性。可以使用叉號圖示逐一移除屬性，或按一下**重設**按鈕一次移除所有屬性。

  如果未指定XML關鍵屬性，則在欄位對應過程中，XML值的唯一路徑將由一系列標籤表示。

  標籤編號

  標籤編號功能自 KUMA 2.1.3 起提供。此功能可自動為 XML 事件中的標籤編號，讓您能夠解析含有相同標籤或未命名標籤（例如 <Data>）的事件。

例如，我們將使用**標籤編號**功能，為**Microsoft Windows PowerShell 事件 ID 800** 的 EventData 屬性中的標籤編號。



若要解析此類事件，您必須：

- 設定標籤編號。
- 設定編號標籤與 KUMA 事件欄位之間的資料對應。

KUMA 3.0.x 支援在同一個額外標準化器中同時使用**XML 屬性**和**標籤編號**功能。如果屬性包含未命名標籤或相同標籤，建議使用**標籤編號**功能。如果屬性只包含具名標籤，請使用**XML 屬性**。若要在額外標準化器中使用此功能，您必須依序在事件通往目標額外標準化器的路徑上，為每個額外標準化器以及目標額外標準化器本身啟用「保留原始事件」設定。

如需此功能的實際使用範例，請參閱 MicrosoftProducts 標準化器：「AD FS」和「424」額外標準化器已依序啟用「保留原始事件」設定。

若要設定具有相同名稱或未命名標籤的事件解析：

1. 建立新的標準化器，或開啟現有的標準化器進行編輯。
2. 在標準化器的**基本事件解析**視窗中，從**解析方法**下拉清單選取「xml」，然後在**標籤編號**欄位中點選**新增欄位**。

   在顯示的欄位中，輸入您要為其元素指派編號的標籤完整路徑。例如，Event.EventData.Data。指派給標籤的第一個編號是 0。如果標籤是空的，例如 <Data />，也會為其指派編號。
3. 若要設定資料對應，請在**對應**下點選**新增資料列**，然後執行下列操作：

   a. 在新資料列的**來源**欄位中，輸入標籤的完整路徑及其索引。對於上述範例中的 Microsoft Windows 事件，含索引的完整路徑如下：

      - Event.EventData.Data.0,
      - Event.EventData.Data.1
      - Event.EventData.Data.2，以此類推

   b. 在**KUMA欄位**下拉清單中，選擇KUMA事件中解析後將從編號標籤接收值的欄位。
4. 若要儲存變更：

   - 如果您建立了新的標準化器，請按一下**儲存** 。
   - 如果您編輯了現有的標準化器，請在與該標準化器連結的收集器中按一下**更新設定**。

解析隨即設定。

- **netflow5**

  此解析方法用於處理NetFlow v5格式的資料。

選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 netflow5 類型進行主要解析，則無法進行額外的標準化。

在對應規則中，預設不會在 KUMA 事件的欄位中指出 **netflow5** 的通訊協定類型。解析 NetFlow 格式的資料時，必須在**擴充**標準化器索引標籤上建立一條**常數**資料擴充規則，該規則會將 `netflow` 值新增至 `DeviceProduct` 目標欄位。

- **netflow9**

  此解析方法用於處理NetFlow v9格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 netflow9 類型進行主要解析，則無法進行額外的標準化。

  在對應規則中，預設不會在 KUMA 事件的欄位中指出 **netflow9** 的通訊協定類型。解析 NetFlow 格式的資料時，必須在**擴充**標準化器索引標籤上建立一條**常數**資料擴充規則，該規則會將 `netflow` 值新增至 `DeviceProduct` 目標欄位。

- **sflow5**

  此解析方法用於處理sflow5格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 sflow5 類型進行主要解析，則無法進行額外的標準化。

- **ipfix**

  此解析方法用於處理IPFIX資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 ipfix 類型進行主要解析，則無法進行額外的標準化。

  在對應規則中，預設不會在 KUMA 事件的欄位中指出 **ipfix** 的通訊協定類型。解析 NetFlow 格式的資料時，必須在**擴充**標準化器索引標籤上建立一條**常數**資料擴充規則，該規則會將 `netflow` 值新增至 `DeviceProduct` 目標欄位。

- sql —僅當使用sql類型的連接器時，此方法才可用。

  標準化器使用此方法處理從資料庫選取的資料。

5. 在**保留原始事件**下拉清單中，指定是否將原始原始事件儲存在新建立的標準化事件中。可用值：

   - **不儲存**– 不儲存原始事件。這是預設設定。
   - **僅錯誤** – 若解析事件時發生錯誤，將原始事件儲存於標準化事件的 `Raw` 欄位中。該值便於在服務偵錯時使用。如此，只要事件的 `Raw` 欄位不為空，即可判定存在問題。

     若包含名稱 `*Address` 或 `*Date*` 的欄位不符合標準化規則，這些欄位將被略過。此情況下不會發生標準化錯誤，而且即使已選取**保留原始事件 → 僅錯誤**選項，欄位值也不會顯示在標準化事件的 `Raw` 欄位中。

   - **總是** – 一律將原始事件儲存於標準化事件的 `Raw` 欄位中。

6. 在**保留額外欄位**下拉式清單中，可選取當原始事件欄位未設定對應規則時，是否將其儲存於標準化事件內（參見下文）。資料儲存於 `Extra` 事件欄位。標準化事件可基於儲存於 `Extra` 欄位中的資料進行搜尋與篩選。

   基於「額外」事件欄位資料的篩選：

   基於**額外**事件欄位資料的篩選器條件：

   - 條件 –**如果**。
   - 左運算元 –**事件欄位**。
   - 在此事件欄位中，您可以指定以下其中一個值：
     - **Extra**欄位。
     - Extra 欄位中的值，格式如下：

       `Extra.<field name>`

       例如，`Extra.app`。

       這種類型的值需手動指定。
     - 寫入**Extra**欄位的陣列值須符合以下格式：

       `Extra.<field name>.<array element>`

       例如，`Extra.array.0`。

       陣列中的值從0開始編號。

       這種類型的值需手動指定。

       若要使用 Extra 欄位中深度為 3 或更深層的值，請使用反引號 ``。例如，`Extra.lev1.lev2.lev3`。
   - 運算子 – =。
   - 右運算元 –**常數**。
   - 值 – 您需要用來篩選事件的值。

   預設情況下，不儲存欄位。

7. 將您要處理的資料範例複製到**事件範例**欄位。這是可選的，但建議執行的步驟。

8. 在**對應**表中，設定原始事件欄位到KUMA格式的事件欄位的對應：

a. 在**來源**列中，提供要轉換為KUMA事件欄位的原始事件欄位的名稱。

如需欄位格式的詳細資訊，請參閱「正規化事件資料模型」一文。如需對應的說明，請參閱「預先定義的正規化器欄位對應」一文。

點選**來源**欄中欄位名稱旁邊的按鈕會開啟**轉換**視窗，您可以在其中點選**新增轉換**按鈕來建立規則，以便在將原始資料寫入KUMA事件欄位之前加以修改。

可用的轉換

轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

可用轉換類型：

- **小寫** — 用於將值的所有字元變為小寫
- **大寫** — 用於將值的所有字元變為大寫
- **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
- **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。
- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。

- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

在**轉換**視窗中，您可以透過⣿圖示拖曳新增的規則來交換其順序；您也可以使用✕圖示刪除這些規則。

b. 在**KUMA欄**位列中，從下拉清單中選擇所需的KUMA事件欄位。您可以透過在欄位中輸入欄位名稱來搜尋欄位。

關於 KUMA 欄位欄的建議

我們建議您設定以下KUMA欄位的對應。否則，您將無法在警示詳情和事件詳情中檢視可觀察物件。

建議的KUMA欄位取決於可觀察物件的類型：

- 對於MD5雜湊值和SHA256類型的可觀察物件：
  - FileHash
- 對於URL類型的可觀察物件：
  - RequestUrl
- 對於IP位址類型的可觀察物件：
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress

- SourceTranslatedAddress
- SourceAddress

- 對於網域名稱類型的可觀察物件：
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain
  - SourceDnsDomain
  - SourceNtDomain
- 對於使用者名稱類型的可觀察物件：
  - DestinationUserName
  - SourceUserName
- 對於主機名稱類型的可觀察物件：
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. 若前一步驟選取的 KUMA 事件欄位名稱以 `DeviceCustom*` 或 `Flex*` 開頭，可在**標籤**欄位中新增唯一的自訂標籤。

可使用 **新增資料列** 按鈕新增表格資料列。可使用 ✕ 按鈕逐一刪除資料列，或使用 **全部清除** 按鈕一次刪除所有資料列。

如果您要KUMA使用資產資訊擴充事件，並在觸發關聯規則時在警示卡中顯示資產訊息，請在**對應**表中根據資產的用途設定主機位址和主機名欄位的對應。例如，對應可以套用至SourceAddress和SourceHostName，或DestinationAddress和DestinationHostName欄位。擴充後，事件卡將包含SourceAssetID或DestinationAssetID欄位，以及指向資產卡的連結。此外，擴充後，資產資訊也會顯示在警示卡中。

如果您已將資料載入到**事件範例**欄位中，則此表將包含一個**範例**列，其中包含從原始事件欄位轉移到KUMA事件欄位的值範例。

如果KUMA事件欄位的大小小於其中放置的值的長度，則此值將被截斷為事件欄位的大小。

9. 點擊**確定**。

標準化器在安裝精靈的**事件解析**頁籤上顯示為深色圓圈。如果要開啟標準化器設定進行檢視，按一下深色圓圈。將滑鼠遊標停留在圓圈上時，一個加號隨即顯示。點選它即可新增事件解析規則（請參閱下方說明）。

使用附加資料擴充標準化事件

您可以透過在標準化器中建立擴充規則，為新建立的標準化事件新增更多資料。這些擴充規則儲存在建立它們的標準化器中。可以有多個擴充規則。

若要新增擴充規則至標準化器：

1. 選擇主規範化規則或附加規範化規則以開啟一個視窗，然後在此視窗中點選**擴充**頁籤。

2. 按一下**新增擴充規則**按鈕。

   擴充規則參數區塊隨即出現。您可以透過點選 ✕ 按鈕刪除設定群組。

3. 從**來源類型**下拉清單中選擇擴充類型。根據所選類型，可能還需要完成進階設定。

   可用的擴充規則來源類型：

   - **常數**

     當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定：

     - 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。

     - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

     若針對 `String`、`Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。

     若針對 `Array of strings`、`Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。

   - **字典**

     如果需要從字典類型的**字典**中新增值，則使用此類擴充。

     在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。

     如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。

     例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。

     如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。

     例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。

   - **表格**

     如果您需要從表格類型的**字典**中新增值，請使用此類擴充。

     在**字典名稱**下拉清單中選擇此擴充類型後，請選擇用於提供值的字典。在**鍵欄位**設定群組中，按一下**新增欄位**按鈕以選擇其值用於選擇字典條目的事件欄位。

在**對應**表中，設定用於提供資料的字典欄位和用於接收資料的事件欄位：

- 在**字典欄位**直欄中，選擇字典欄位。可用欄位取決於所選的字典資源。
- 在 **KUMA 欄位**直欄中，選取要寫入值的事件欄位。對於某些選取的欄位（ `*custom*` 與 `*flex*` ），您可以在**標籤**直欄中，為寫入其中的資料指定名稱。

可以透過點選**新增元素**按鈕來新增表格行。可以透過按一下✕按鈕來刪除直欄。

- **事件**

當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定：

- 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。
- 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。
- 按一下🔧按鈕會開啟**轉換**視窗，您可以在其中使用**新增轉換**按鈕建立規則，在將原始資料寫入 KUMA 事件欄位前對其進行修改。

  可用的轉換

  轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

  可用轉換類型：

  - **小寫** — 用於將值的所有字元變為小寫
  - **大寫** — 用於將值的所有字元變為大寫
  - **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
  - **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。
  - **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
    - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
    - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
  - **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
  - **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
  - **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
  - **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
    - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
    - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。

- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。

- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

當您使用事件擴充功能，且在 **來源類型** 設定中選取 **事件**，並使用延伸事件結構描述的欄位作為引數時，須注意以下特殊事項：

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `String` 類型的欄位，則值會以 TSV 格式寫入目標欄位。

  範例：SA.StringArray 延伸事件結構描述欄位包含以下值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 DeviceCustomString1 事件結構描述欄位。操作結果為：DeviceCustomString1 欄位包含 ["string1", "string2", "string3"]。

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `Array of strings` 類型的欄位，則來源欄位的值會附加至目標欄位的值，並存入目標欄位，以逗號 (",") 作為分隔符號。

  範例：延伸事件結構描述欄位 SA.StringArrayOne 包含值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 SA.StringArrayTwo 事件結構描述欄位。操作結果為：SA.StringArrayTwo 欄位包含 "string1"、"string2"、"string3"。

- **範本**

  當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

  - 在 **範本**欄位中，輸入 Go 範本。

    事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。

範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

- 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

範例：

{{.SA.StringArrayOne}}

範例：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

4. 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

   此設定不適用於**表格**類型的擴充來源。

5. 如果要在標準化器日誌中啟用詳細資訊，請將**調試**切換開關設定為啟用。預設情況下，會停用詳細資訊。

6. 點擊**確定**。

具有附加資料的事件擴充規則將會新增到標準化器和選定的解析規則中。

設定連結到IP位址的解析

您可以將來自多個IP位址、不同類型的來源的事件導向到同一個收集器，收集器將套用對應的設定標準化器。

您可以將此方法用於連接器類型為UDP、TCP或HTTP的收集器。若於收集器的**傳輸**步驟中指定了 UDP、TCP 或 HTTP 連接器，則在**事件解析**步驟中，可於**解析設定**頁籤上指定多個IP位址，並為來自這些指定位址的事件選取要使用的標準化器。可用的標準化器類型如下：json、cef、regexp、syslog、csv、kv、xml。

在已設定連結至IP位址的標準化器的收集器中，如果您將連接器類型變更為UDP、TCP或HTTP以外的任何類型，**解析設定**頁籤將消失，並且在**解析**步驟中僅指定先前指定的第一個標準化器。此頁籤將立即從網頁介面中消失，但變更將在儲存資源後套用。若要還原先前的設定，請結束收集器安裝精靈且不要儲存。

對於 Syslog 與 regexp 類型的標準化器，可根據DeviceProcessName欄位的值指定額外的標準化條件來使用標準化鏈。與附加標準化的差異在於您可以指定共用標準化器。

若要設定連結到IP位址的解析：

1. 在**事件解析**步驟中，轉至**解析設定**頁籤。

2. 在**IP位址**欄位中，指定一個或多個將從中接收事件的IP位址。您可以指定多個IP位址，並以逗號分隔。可用格式：IPv4。位址清單的長度不受限制；但是，我們建議指定合理數量的位址以保持收集器負載平衡。如果要在一個收集器中套用多個標準化器，則此欄位為必填項。

   限制：對於每個IP+標準化器組合，IP位址必須是唯一的。OSMP會檢查位址是否唯一。如果您為不同的標準化器指定相同的IP位址，則會顯示**該欄位必須是唯一的**訊息。

   如果要將所有事件傳送到同一個標準化器而不指定IP位址，我們建議建立單獨的收集器。如果您想將同一個標準化器應用於來自大量IP位址的事件，我們還建議建立一個具有一個標準化器的單獨收集器；這有助於提高效能。

3. 在**標準化器**欄位中，建立一個標準化器或從下拉清單中選擇一個現有的標準化器。下拉清單旁邊的箭頭將您轉到**解析架構**頁籤。

   如果設定了連接器類型，則會觸發標準化：UDP、TCP、HTTP；在HTTP情況下必須指定事件來源標頭。

   考慮到可用的連接器，以下標準化器類型可用於自動來源識別：json、cef、regexp、syslog、csv、kv、xml。

4. 如果選擇了Syslog或regexp標準化器類型，則可以**額外條件**。如果在主標準化器中設定了DeviceProcessName的**欄位對應**，則可以進行條件標準化。在**條件**下，在DeviceProcessName欄位中指定進程名稱，並建立一個標準化器，或從下拉清單中選擇一個現有的標準化器。您可以指定DeviceProcessName+標準化器的多個組合，標準化過程將一直執行，直到找到第一個匹配項。

已設定與IP位址關聯的解析。

建立事件標準化規則結構

若要實作複雜的事件處理邏輯，您可以為標準化器新增多個事件解析規則。事件根據指定的條件在解析規則之間傳輸。建立解析規則的順序很重要。事件按順序處理，並使用箭頭顯示其路徑。

若要建立附加解析規則：

1. 建立一個標準化器（請參閱上方說明）。

   建立的標準化器在視窗中顯示為深色圓圈。

2. 將滑鼠遊標停留在圓圈上，然後按一下出現的加號按鈕。

3. 在開啟的**額外事件解析**視窗中，指定附加事件解析規則的參數：

   - **額外標準化條件**頁籤：

     如果要傳送原始事件進行額外標準化，請在**保留原始事件**下拉清單中選擇**是**。預設值為**否**。我們建議將原始事件傳遞給json和xml類型的標準化器。如果您要將原始事件傳送到第二、第三等嵌套層級進行附加標準化，請在每個嵌套層級中，在**保留原始事件**下拉清單中選擇**是**。

     若要僅將具有特定欄位的事件傳送至附加標準化器，請在**要傳入標準化器的欄位**的欄位中指定此欄位。

     在此頁籤上，您還可以定義其他條件。當滿足這些條件時，將傳送事件以進行進一步解析。

   - **標準化架構**頁籤：

     在此頁籤上，您可以設定事件處理規則，類似於主標準化器設定（請參閱上方說明）。**保留原始事件**設定不可用。**事件範例**欄位顯示建立初始標準化器時指定的值。

   - **擴充**頁籤：

     在此頁籤上，您可以設定事件擴充規則（請參閱上方說明）。

4. 點擊**確定**。

附加解析規則已新增至標準化器。它會顯示為深色區塊，其中包含觸發此規則的條件。您可以點選附加解析規則來變更其設定。如果將滑鼠遊標停留在附加解析規則上，將出現一個加號按鈕。您可以按一下此按鈕以建立新的附加解析規則。若要刪除標準化器，請使用帶有垃圾桶圖示的按鈕。

視窗右上角包含一個搜尋視窗，您可以在其中依名稱搜尋解析規則。

轉到精靈的下一個步驟。

步驟 4。事件篩選

這是安裝精靈的可選步驟。安裝精靈的**事件篩選**頁籤可讓您選擇或建立篩選器，其設定指定選擇事件的條件。您可以為收集器新增多個篩選器。您可以透過 ⣿ 圖示拖曳篩選器來調換順序，也可以刪除篩選器。篩選器透過AND運算子組合。

若要將現有篩選器新增至收集器資源集，

請按一下**新增篩選器**按鈕，然後從**篩選器**下拉清單中選擇所需的篩選器。

若要新增篩選器資源集：

1. 按一下**新增篩選器**按鈕，然後從**篩選器**下拉清單中選擇**新建**。
2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。如果您決定在不同服務之間重複使用相同的篩選器，這將非常有用。預設情況下，此核取方塊處於未選取狀態。
3. 如果選取了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器的名稱。此名稱必須包含1到128個Unicode字元。
4. 在**條件**部分，指定篩選的事件必須滿足的條件：
   - 按一下**新增條件**按鈕可新增篩選條件。您可以選擇兩個值（兩個運算元，左運算元和右運算元），並指派要使用選取值執行的運算。運算的結果為True或False。
     - 在**運算子**下拉清單中，選擇篩選器要執行的函式。

       在此下拉清單中，如果運算子應忽略值的大小寫，則可以選取**大小寫不相符**核取方塊。如果選取**InSubnet**、**InActiveList**、**InCategory**、**InActiveDirectoryGroup**操作員，則會忽略此核取方塊。預設情況下，此核取方塊已清除。

       篩選器運算子

       - **=** — 左運算元等於右運算元。
       - **<** — 左運算元小於右運算元。
       - **<=** — 左運算元小於或等於右運算元。
       - **>** — 左運算元大於右運算元。
       - **>=** — 左運算元大於或等於右運算元。
       - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
       - **contains** — 左運算元包含右運算元的值。
       - **startsWith** — 左運算元以右運算元的某個值開頭。
       - **endsWith** — 左運算元以右運算元的某個值末端。
       - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
       - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。

- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。

- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。

- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。

- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。

- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。

- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。

- **inContextTable**檢查指定快顯表單中條目的存在情況。

- **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

- 在**左運算元**和**右運算元**下拉清單中，選擇要篩選的資料來源。選擇後，進階設定隨即顯示 。使用它們來確定將傳遞給篩選器的確切值。例如，選擇**活動清單**時，您需要指定活動清單的名稱、條目鍵和條目鍵欄位。

- 您可以使用**如果**下拉清單來選擇是否需要建立否定篩選條件。

點選✕按鈕可以刪除條件。

- **新增群組**按鈕用於新增條件群組。**且**可在**且**、**或**、**非**之間切換。

  點選✕按鈕可以刪除條件群組。

- 點選**新增篩選器**，您可以將在**選擇篩選器**下拉清單中選擇的現有篩選器新增至條件。您可以點選 導覽至巢狀篩選器。

  點選✕按鈕可以刪除巢狀篩選器。

篩選器已新增。

轉到精靈的下一個步驟。

步驟 5。事件彙總

這是安裝精靈的可選步驟。安裝精靈的**事件彙總**頁籤可讓您選擇或建立彙總規則，其設定指定彙總相同類型事件的條件。您可以為收集器新增多個彙總規則。

若要將現有彙總規則新增至一組收集器資源，

請按一下**新增彙總規則** ，然後在下拉清單中選擇**彙總規則** 。

若要將新的彙總規則新增至一組收集器資源：

1. 按一下**新增彙總規則**按鈕，然後從**彙總規則**下拉清單中選擇**新建** 。

2. 在**名稱**欄位中輸入新建立的彙總規則的名稱。此名稱必須包含1到128個Unicode字元。

3. 在**閾值**欄位中，指定在彙總規則觸發且事件被彙總之前必須累積多少個事件。預設值為`100`。

4. 在**觸發後規則有效期**欄位中，指定收集器必須累積待彙總事件的時間長度（以秒為單位）。該時間到期之時，彙總規則將被觸發並建立新的彙總事件。預設值為`60`。

5. 在**相同欄位**部分中，按一下**新增欄位**按鈕以選擇將用於標識相同類型事件的欄位。透過點選具有十字圖示的按鈕，可以刪除選定的事件。

6. 在**唯一欄位**部分中，您可以按一下**新增欄位**以選擇即使事件包含**相同欄位**部分中列出的欄位，也將取消事件彙總資格的欄位。透過點選具有十字圖示的按鈕，可以刪除選定的事件。

7. 在**總和欄位**部分中，您可以按一下**新增欄位**按鈕來選擇在彙總過程中將對其值進行求和的欄位。透過點選具有十字圖示的按鈕，可以刪除選定的事件。

8. 在**篩選器**部分，您可以指定條件來定義此資源將處理的事件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。

   在資源中建立篩選器

   KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

   若要建立篩選器：

   1. 在**篩選器**下拉清單中，選擇**新建**。

   2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。

   3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。

   4. 在**條件**下，指定事件必須滿足的條件：

      a. 點擊**新增條件**按鈕。

      b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。

      c. 在**運算子**下拉清單中，選擇一個運算子。

      篩選器運算子

      - **=** — 左運算元等於右運算元。
      - **<** — 左運算元小於右運算元。
      - **<=** — 左運算元小於或等於右運算元。

- **>** — 左運算元大於右運算元。
- **>=** — 左運算元大於或等於右運算元。
- **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
- **contains** — 左運算元包含右運算元的值。
- **startsWith** — 左運算元以右運算元的某個值開頭。
- **endsWith** — 左運算元以右運算元的某個值末端。
- **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

新增彙總規則。您可以透過點選 ✕ 按鈕來刪除它。

轉到精靈的下一個步驟。

步驟 6。事件擴充

這是安裝精靈的可選步驟。在安裝精靈的**事件擴充**頁籤上，您可以指定應將哪些資料從哪些來源新增至收集器處理的事件中。可以使用擴充規則或LDAP所取得的資料來擴充事件。

基於規則的擴充

可以有多個擴充規則。您可以按一下**新增擴充規則**按鈕來新增它們，也可以按一下 ✕ 按鈕來刪除它們。您可以使用現有的擴充規則，也可以直接在安裝精靈中建立規則。

若要將現有的擴充規則新增至資源集：

1. 按一下**新增擴充規則**

   這將會開啟擴充規則設定區塊。

2. 在**擴充規則**下拉清單中，選擇相關資源。

擴充規則已新增至收集器的資源集。

若要在資源集中建立新的擴充規則：

1. 按一下**新增擴充規則**

   這將會開啟擴充規則設定區塊。

2. 在**擴充規則**下拉清單中，選擇**新建**。

3. 在**來源類型**下拉清單中，選擇要擴充的資料來源並定義其對應的設定：

   - **常數**

     當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定：

     - 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。

     - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

     若針對 `String`、`Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。

     若針對 `Array of strings`、`Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。

   - **字典**

     如果需要從字典類型的**字典**中新增值，則使用此類擴充。

     在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。

     如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。

例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。

如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。

例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。

- **事件**

  當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定：

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。
  - 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。
  - 在**轉換**下，您可以建立規則，以便在將原始資料寫入 KUMA 事件欄位之前修改資料。可以從下拉清單中選擇轉換類型。您可以使用**新增轉換**和**刪除轉換**按鈕分別新增或刪除轉換。轉換的順序很重要。

    可用的轉換

    轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

    可用轉換類型：

    - **小寫** — 用於將值的所有字元變為小寫
    - **大寫** — 用於將值的所有字元變為大寫
    - **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
    - **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。
    - **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
      - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
      - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
    - **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
    - **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
    - **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。

- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。
- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

- **範本**

  當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

  - 在 **範本**欄位中，輸入 Go 範本。

    事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。

    範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。
  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

  若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

  如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

  範例：

{{.SA.StringArrayOne}}

範例：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

  此類擴充用於向私人網路DNS伺服器傳送請求，以將IP位址轉換為網域名稱或反之亦然。IP 位址只會針對以下私人位址轉換為 DNS 名稱：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、100.64.0.0/10、fd00::/8。

  下表說明此類擴充的設定。

  「dns」擴充類型的參數

設定	描述
網址	要傳送請求的 DNS 伺服器 URL。 您可以使用 **新增 URL** 按鈕指定多個 URL。 如果未指定 **URL** 設定，KUMA 會從本機的 `/etc/resolv.conf` 檔案取得 DNS 伺服器清單。在這種情況下，您需要啟用 **遞迴查詢** 選項。否則將不會執行擴充。
每秒請求數	每秒傳送至 DNS 伺服器的查詢數上限。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
工作模組	服務可以同時執行以並行處理回應規則的事件處理器數量。請指定介於 0 到 999 之間的正整數。如果指定 0，則使用邏輯 CPU 核心數。預設值為 `1`。
資料補足佇列中的最大事件數量	重新提交佇列可容納的事件數上限。預設值為 `1,000,000`。
逾時時間	等待 DNS 伺服器回應的時間（以秒為單位）。預設值為 `5`。
DNS 模式覆寫	使用的解析方法： - **僅轉發 DNS**會將網域名稱解析為 IP 位址。 - **僅反向 DNS**會將 IP 位址解析為網域名稱。 - **轉發並反向 DNS**會將網域名稱解析為 IP 位址，或將 IP 位址解析為網域名稱。
快取存續時間	快取中儲存的值的存活時間（以秒為單位）。預設值為 `60` 秒。
已停用快取	您可以使用此設定啟用或停用快取。預設情況下啟用快取。
已停用快取重新整理	如果啟用快取更新，當快取的 TTL 到期時，收集器會再次向 DNS 伺服器傳送請求，以更新快取中儲存的資料。此設定僅在啟用快取時可用。預設會啟用快取更新。
遞迴查詢	允許收集器向權威 DNS 伺服器傳送遞迴查詢，以擴充資料。預設值是**停用**。

- **cybertrace**

  此類擴充用於將CyberTrace資料流中的資訊新增至事件欄位。

  可用設定：

  - **URL**（必填）- 在此欄位中，您可以指定要傳送請求的CyberTrace伺服器的URL。
  - **連線數**— KUMA可以同時與CyberTrace伺服器建立的最大連線數。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
  - **RPS** — 每秒傳送至伺服器的最大請求數。預設值是 `1000`。
  - **逾時** — 等待CyberTrace伺服器回應的時間長度（以秒為單位）。預設值為 `30`。

- **對應**（必要）— 此設定區塊包含用於將KUMA事件欄位對應到 CyberTrace指標類型的對應表。**KUMA 欄位**欄會顯示 KUMA 事件欄位的名稱，而 **CyberTrace 指標**欄會顯示 CyberTrace 指標的類型。

  可用的CyberTrace指標類型：

  - **ip**
  - **網址**
  - **雜湊值**

  在對應表中，您必須提供至少一個字串。您可以點擊**新增行**按鈕新增字串，也可以點擊 ✕ 按鈕刪除字串。

- **時區**

  此類擴充在收集器和關聯器中用於為事件指派特定的時區。在搜尋發生在異常時間（例如夜間）的事件時，時區資訊可能很有用。

  選擇此類擴充時，必須從**時區**下拉清單中選擇所需的時區。

  > 請確保託管擴充利用服務的伺服器已設定正確的時區。例如，您可以使用 `timedatectl list-timezones` 命令執行此操作，該命令會顯示伺服器上已設定的所有時區。有關設定時區的詳細資訊，請參閱相應的作業系統說明文件。

  當事件進行擴充處理時，所選時區相對於協調世界時 (UTC) 的時間偏移量，會以`+-hh:mm`格式寫入DeviceTimeZone事件欄位。例如，若選取 **Asia/Yekaterinburg** 時區，則會將值 `+05:00` 寫入 DeviceTimeZone 欄位。若經擴充處理的事件在 DeviceTimeZone 欄位中已有值，該值將被覆蓋。

  預設情況下，如果未在正在處理的事件中指定時區，且未配置按時區擴充規則，則為事件指派處理事件的服務（收集器或關聯器）所在伺服器的時區。如果伺服器時間發生變化，則必須重新啟動服務。

  擴充DeviceTimeZone欄位時允許的時間格式

  在收集器中處理傳入的原始事件時，下列時間格式可自動轉換為+-hh:mm格式：

已處理事件中的時間格式	範例
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

  若 `DeviceTimeZone` 欄位中的日期格式與上述格式不符，當事件使用時區資訊進行擴充處理時，系統會將收集器伺服器的時區寫入該欄位。您可以為非標準時間格式建立自訂的標準化規則。

- **地理資料**

  此類擴充用於將IP地理資料新增至事件位址。了解有關將IP位址連結到地理資料的更多資訊。

  選取此類型時，在**將地理資料對應到事件欄位**下，您必須指定要從哪個事件欄位讀取IP位址、選取所需的地理資料屬性，並定義要將地理資料寫入哪些事件欄位：

  1. 在**具有IP位址的事件欄位**下拉清單中，選擇從中讀取IP位址的事件欄位。上傳到KUMA的地理資料與此IP位址相符。

您可以使用**新增具有IP位址的事件欄位**按鈕來指定需要擴充地理資料的多個具有IP位址的事件欄位。您可以透過點擊**刪除具有IP位址的事件欄位**按鈕來刪除以這種方式新增的事件欄位。

當選取`SourceAddress`、`DestinationAddress`和`DeviceAddress`事件欄位時，**套用預設對應**按鈕將可供使用。您可以按一下此按鈕，新增地理資料屬性與事件欄位的預先設定的對應配對。

2. 對於需要從中讀取IP位址的每個事件欄位，選擇地理資料的類型以及要將地理資料寫入的事件欄位。

   您可以使用**新增地理資料屬性**按鈕為**地理資料屬性-要寫入的事件欄位**新增欄位對。您也可以為一個IP位址設定不同類型的地理資料，以便將其寫入不同的事件欄位。若要刪除欄位對，請按一下 ✕。

   - 在**地理資料屬性**欄位中，選擇應將與讀取的IP位址對應的地理資料寫入事件。可用的地理資料屬性：**國家**、**地區**、**城市**、**經度**、**緯度**。
   - 在**要寫入的事件欄位**中，選擇必須將所選地理資料屬性寫入的事件欄位。

   您可以將相同的地理資料屬性寫入不同的事件欄位。如果設定要寫入相同事件欄位的多個地理資料屬性，則事件將使用序列中的最後一個對應進行擴充。

4. 使用**偵錯**下拉清單指示是否啟用服務運作的日誌記錄。預設情況下，日誌記錄處於停用狀態。

5. 在**篩選器**部分，您可以指定條件來識別將由擴充規則資源處理的事件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。

   在資源中建立篩選器

   KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

   若要建立篩選器：

   1. 在**篩選器**下拉清單中，選擇**新建**。
   2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
   3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。
   4. 在**條件**下，指定事件必須滿足的條件：
      a. 點擊**新增條件**按鈕。
      b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。
      c. 在**運算子**下拉清單中，選擇一個運算子。

      篩選器運算子

      - **=** — 左運算元等於右運算元。
      - **<** — 左運算元小於右運算元。

- **<=** — 左運算元小於或等於右運算元。
- **>** — 左運算元大於右運算元。
- **>=** — 左運算元大於或等於右運算元。
- **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
- **contains** — 左運算元包含右運算元的值。
- **startsWith** — 左運算元以右運算元的某個值開頭。
- **endsWith** — 左運算元以右運算元的某個值末端。
- **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。
6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

新的擴充規則已新增至收集器的資源集。

LDAP擴充

若要使用LDAP啟用擴充：

1. 按一下**利用 LDAP 資料新增資料補足**。

   這會開啟LDAP擴充設定群組。

2. 在**LDAP 帳戶對應**設定區塊中，按一下**新網域**按鈕以指定使用者帳戶的網域。您可以指定多個帳戶。

3. 在**LDAP 對應**表中，定義將KUMA欄位對應到LDAP屬性的規則：

   - 在**KUMA欄位**欄中，指定您要將其資料與LDAP屬性進行比較的KUMA事件欄位。
   - 在**LDAP屬性**列中，指定必須與KUMA事件欄位進行比較的屬性。下拉清單包含標準屬性，可以使用**自訂屬性**進行擴充。

     在使用自訂屬性設定事件擴充之前，請確保在AD中設定了自訂屬性。

     若要使用自訂屬性擴充帳戶活動：

     1. 在**LDAP連線設定**中新增自訂AD帳戶屬性。

        標準的**從AD匯入的屬性**不能新增為自訂屬性。例如，若將標準的 `accountExpires` 屬性新增為自訂屬性，KUMA 會在儲存連線設定時傳回錯誤。

        可以從Active Directory請求以下帳戶屬性：

        - `accountExpires`
        - `badPasswordTime`
        - `cn`
        - `co`
        - `company`
        - `department`
        - `description`
        - `displayName`
        - `distinguishedName`
        - `division`
        - `employeeID`
        - `givenName`
        - `l`

- lastLogon
- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf（此屬性可在關聯分析期間用於搜尋）
- mobile
- name
- objectCategory
- objectGUID（即使使用者未指定此屬性，也總會從 Active Directory 請求此屬性）
- objectSID
- physicalDeliveryOfficeName
- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

在LDAP連線設定中新增自訂屬性後，收集器中要接收的**LDAP屬性**下拉清單將自動包含新屬性。自訂屬性由屬性名稱旁的問號來識別。如果為多個網域新增了相同的屬性，則此屬性在下拉清單中僅列出一次。您可以將滑鼠遊標移到問號上來檢視網域。網域名稱顯示為連結。在點選連結時，則如果之前未新增此網域，它將自動新增到**LDAP帳戶對應**中。

如果在LDAP連線設定中刪除了自訂屬性，請從收集器的對應表手動刪除包含此屬性的行。每次匯入帳戶時，KUMA中的帳戶屬性資訊都會更新。

2. 匯入帳戶。

3. 在收集器的**LDAP對應**表中，定義將KUMA欄位對應到LDAP屬性的規則。

4. 重新啟動收集器。

   重新啟動收集器後，KUMA開始使用帳戶擴充事件。

- 在**要寫入的KUMA事件欄位**列中，指定如果對應成功，則將從LDAP匯入的使用者帳戶的ID放置在KUMA事件的哪個欄位中。

您可以按一下**新增行**按鈕在表格中新增字串，也可以按一下 ✕ 按鈕刪除字串。您可以使用**套用預設對應**按鈕，以標準值填入對應表。

已將針對從LDAP接收的資料的事件擴充規則新增至收集器的資源群組。

如果使用LDAP為現有收集器新增擴充或變更擴充設定，則必須停止並重新啟動服務。

轉到精靈的下一個步驟。

步驟 7。路由

這是安裝精靈的可選步驟。在安裝精靈的**路由**頁籤上，您可以選擇或建立目標，並使用設定指示收集器處理的事件的轉送目標。通常，收集器的事件會路由到兩個點：路由到關聯器，用於分析和搜尋威脅；以及路由到儲存體，用於儲存和以便以後檢視已處理的事件。可以根據需要將事件傳送到其他位置。可以有多個目標點。

若要將現有目標新增至收集器資源集：

1. 在**新增目標**下拉清單中，選擇要新增的目標資源類型：

   - 如果要設定將已處理的事件轉送到儲存體，請選擇**儲存體**。
   - 如果要設定將已處理的事件轉送至關聯器，請選擇**關聯器**。
   - 如果您想要將事件傳送到其他位置，請選擇**其他**。

     此類資源包括在程式的先前版本中建立的關聯器和儲存體服務。

   將開啟**新增目標**窗口，您可以在其中指定事件轉送的參數。

2. 在**目標**下拉清單中，選擇必要的目標。

   視窗名稱變更為**編輯目標**，並顯示所選資源的設定。若要在新瀏覽器頁籤中開啟目標設定進行編輯，請點選 ↗。

3. 按一下**儲存**按鈕。

所選目標將顯示在安裝精靈頁籤上。可以透過選擇目標資源並在開啟的視窗中點選**刪除**，從資源集中刪除目標資源。

若要將新的目標資源新增至收集器資源集：

1. 在**新增目標**下拉清單中，選擇要新增的目標資源類型：

   - 如果要設定將已處理的事件轉送到儲存體，請選擇**儲存體**。
   - 如果要設定將已處理的事件轉送至關聯器，請選擇**關聯器**。
   - 如果您想要將事件傳送到其他位置，請選擇**其他**。

     此類資源包括在程式的先前版本中建立的關聯器和儲存體服務。

   將開啟**新增目標**窗口，您可以在其中指定事件轉送的參數。

2. 在**基本設定**頁籤上指定設定：

   - 在**目標**下拉清單中，選擇**新建**。
   - 在**名稱**欄位中，輸入目標資源的唯一名稱。此名稱必須包含1到128個Unicode字元。
   - 使用**停用**切換按鈕，指定是否將事件傳送到此目標位置。預設情況下，啟用傳送事件。
   - 選擇目標資源的**類型**：
     - 如果要設定將已處理的事件轉送到儲存體，請選擇**儲存體**。
     - 如果要設定將已處理的事件轉送至關聯器，請選擇**關聯器**。
     - 如果要設定將事件傳送到其他位置，請選擇**nats-jetstream**、**tcp**、**http**、**kafka**或**file**。
   - 以hostname:<API連接埠>格式指定事件應傳送到的**URL**。
     您可以使用**URL**按鈕為除**nats-jetstream**、**file**和**diode**以外的所有類型指定多個目標位址。
   - 對於**nats-jetstream**和**kafka**類型，使用**主題**欄位指定資料應寫入哪個主題。主題必須包含Unicode字元。Kafka主題最多包含255個字元。

3. 如有必要，請在**進階設定**頁籤上指定設定。可用的設定因所選的目標資源類型而異：

   - **壓縮**是下拉清單，您可以在其中啟用Snappy壓縮。預設情況下，壓縮是**停用的**。
   - **代理**是下拉清單，用於選擇代理伺服器。
   - **緩衝區大小**欄位用於設定目標的緩衝區大小（以位元組為單位）。預設值為1MB，最大值為64MB。
   - **逾時**欄位可用於設定其他服務或元件回應的逾時（以秒為單位）。預設值為`30`。
   - **磁碟緩衝區大小限製**欄位用於指定磁碟緩衝區的大小（以位元組為單位）。預設大小是10 GB。
   - **叢集 ID**是NATS叢集的ID。

- **TLS模式**是下拉清單，您可以在其中指定使用TLS加密的條件：

  - **已停用**（預設）—不使用 TLS 加密。

  - **啟用**— 啟用加密，但不進行驗證。

  - **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA的根憑證和金鑰會在程式安裝期間自動建立，並儲存在KUMA Core伺服器的資料夾/opt/kaspersky/kuma/core/certificates/中。

  使用TLS時，無法將IP位址指定為URL。

- **URL選擇政策**是下拉清單，您可以在其中選擇一種方法來確定在指定多個URL的情況下將事件傳送到哪個URL：

  - **任何**。只要其中一個可用的URL可以接收事件，事件就會傳送到該URL。如果連線中斷（例如，接收節點斷開連線），則會選擇其他URL作為事件目標。

  - **第一優先**。事件將會傳送到已新增位址清單中的第一個URL。如果該URL不可用，事件將依序傳送到下一個可用節點。當第一個URL再次可用時，事件將再次開始傳送到此URL。

  - **均衡**意味著包含事件的套件均勻分發在清單中可用的URL中。由於封包是在目標緩衝區溢位或刷新計時器上傳送的，因此此URL選擇政策無法保證事件均勻分佈到目標。

- **分隔符號**用於指定分隔事件的字元。預設使用 `\n`。

- **路徑**— 如果選擇了**檔案**目標類型，則為檔案路徑。

- **緩衝區排清間隔** — 此欄位用於設定將資料傳送至目的地的時間間隔（以秒為單位）。預設值為`100`。

- **工作線程** — 此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。

- 您可以使用**健康情況檢查路徑**和**健康情況檢查逾時**欄位設定健康情況檢查。您也可以透過選中**健康情況檢查已停用**核取方塊來停用健康情況檢查。

- **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

- **磁碟緩衝區已停用**下拉清單用於啟用或停用磁碟緩衝區的使用。預設情況下，磁碟緩衝區是停用的。

  如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。

  如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

- 在**篩選器**部分，您可以指定條件來定義此資源將處理的事件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。

  在資源中建立篩選器

  KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

若要建立篩選器：

1. 在**篩選器**下拉清單中，選擇**新建**。

2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。

3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。

4. 在**條件**下，指定事件必須滿足的條件：

   a. 點擊**新增條件**按鈕。

   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。

   c. 在**運算子**下拉清單中，選擇一個運算子。

   篩選器運算子

   - **=** — 左運算元等於右運算元。
   - **<** — 左運算元小於右運算元。
   - **<=** — 左運算元小於或等於右運算元。
   - **>** — 左運算元大於右運算元。
   - **>=** — 左運算元大於或等於右運算元。
   - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
   - **contains** — 左運算元包含右運算元的值。
   - **startsWith** — 左運算元以右運算元的某個值開頭。
   - **endsWith** — 左運算元以右運算元的某個值末端。
   - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
   - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

     待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

     若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
   - **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

     如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
   - **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
   - **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。

- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

4. 按一下**儲存**按鈕。

建立的目標顯示在安裝精靈頁籤上。可以透過選擇目標資源並在開啟的視窗中點選**刪除**，從資源集中刪除目標資源。

轉到精靈的下一個步驟。

步驟 8。設定驗證

這是安裝精靈所需的最後一步。在此步驟中，OSMP 會建立服務資源集，並根據此資源集自動建立服務：

- 收集器的資源集顯示在**資源和服務→收集器**下。它可用於建立新的收集器服務。當此資源集變更時，所有基於此資源集運行的服務將在服務重新啟動後開始使用新參數。為此，您可以點選**儲存並重新啟動服務**和**儲存並更新服務組態**按鈕。

  資源集可像其他資源一樣進行修改、複製、在資料夾之間移動、刪除、匯入及匯出。

- 服務顯示在**資源和服務→有效服務**中。使用安裝精靈建立的服務會在 OSMP 內部執行功能。若要與網路基礎架構的外部部分進行通訊，您需要在伺服器和資產上安裝類似的外部服務。例如，應在用作事件接收方的伺服器上安裝外部收集器服務，並應在已部署ClickHouse服務的伺服器上安裝外部儲存服務，應在必須接收和轉送Windows事件的Windows資產上安裝外部代理服務。

若要完成安裝精靈：

1. 按一下**建立並儲存服務**。

安裝精靈的**安裝驗證**頁籤顯示一個服務表，其中列出了基於在安裝精靈中選擇的資源集所建立的服務。視窗下方顯示了一些命令範例，您必須使用這些命令在目標伺服器和資產上安裝這些服務的外部等效項。

例如：

```
/opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
- <port> 是用於與 KUMA Core 通訊的連接埠。
- <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
- <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
- <API port> 是用於與已安裝元件通訊的連接埠。

「kuma」檔案位於安裝程式的/kuma-ansible-installer/roles/kuma/files/目錄中。

用於與 KUMA Core 通訊的連接埠、KUMA Core CA 憑證的指紋 ID、服務 ID，以及用於與服務通訊的連接埠會自動新增至命令中。您還必須確保 OSMP 的網路連線，並在必要時開啟其元件使用的連接埠。

2. 按一下**儲存收集器**關閉精靈。

收集器服務已在 OSMP 中建立。現在，您將在用於接收事件的伺服器上安裝類似服務。

如果為收集器選擇了 wmi 或 wec 連接器，則也必須安裝自動建立的 OSMP 代理。

在KUMA網路基礎架構中安裝收集器

收集器由兩部分組成：一部分在KUMA主控台內建立，另一部分安裝在用於接收事件的網路基礎架構伺服器上。收集器的第二部分安裝在網路基礎架構中。

若要安裝收集器：

1. 登入要安裝服務的伺服器。
2. 建立/opt/kaspersky/kuma/資料夾。

3. 將「kuma」檔案複製到/opt/kaspersky/kuma/資料夾。該檔案位於安裝程式中的/kuma-ansible-installer/roles/kuma/files/資料夾中。

   確保kuma檔案具有足夠的執行權限。如果此檔案不可執行，請使其可執行：

   ```
   sudo chmod +x /opt/kaspersky/kuma/kuma
   ```

4. 將/kuma-ansible-installer/roles/kuma/files/目錄中的 LICENSE 檔案放置於/opt/kaspersky/kuma/目錄中，並執行以下命令接受最終使用者產品授權協議的條款和條件：

   ```
   sudo /opt/kaspersky/kuma/kuma license
   ```

5. 建立「kuma」使用者：

   ```
   sudo useradd --system kuma && usermod -s /usr/bin/false kuma
   ```

6. 使「kuma」使用者成為/opt/kaspersky/kuma目錄及其內所有檔案的擁有者：

   ```
   sudo chown -R kuma:kuma /opt/kaspersky/kuma/
   ```

7. 執行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA
   Core CA certificate> --id <service ID> --api.port <API port>
   ```

   其中：

   - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
   - <port> 是用於與 KUMA Core 通訊的連接埠。
   - <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

     `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

     您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

     為確保 KUMA Core CA 憑證通過驗證，建議在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
   - <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
   - <API port> 是用於與已安裝元件通訊的連接埠。

   範例：

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
   --api.port YYYY
   ```

   如果在執行命令時偵測到錯誤，請確保設定正確。例如，所需存取級別的可用性、收集器服務和核心之間的網路可用性，以及所選API連接埠的唯一性。修復錯誤後，繼續安裝收集器。

如果沒有發現錯誤，且KUMA主控台中的收集器狀態變為*綠色*，請停止命令執行並繼續下一步。

可以在安裝程式精靈的最後一步複製該命令。它會自動指定KUMA Core伺服器的位址和連接埠、要安裝的收集器的識別碼以及收集器用於通訊的連接埠。

在同一主機上部署多個 KUMA 服務時，您必須在安裝過程中使用 `--api.port <port>` 參數為每個元件指定唯一的連接埠。預設使用以下設定值：`--api.port 7221`。

安裝前，請確保KUMA元件的網路連線正常。

8. 新增 `--install` 金鑰，然後重新執行該命令：

```
sudo /opt/kaspersky/kuma/kuma collector --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --api.port <API port> --install
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完整網域名稱。
- <port> 是用於與 KUMA Core 通訊的連接埠（預設使用連接埠 7210）。
- <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為確保 KUMA Core CA 憑證通過驗證，建議在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
- <service ID> 是從網頁介面複製的 KUMA 服務識別碼。
- <API port> 是用於與已安裝元件通訊的連接埠。

範例：

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX --api.port YYYY --install
```

9. 將KUMA收集器連接埠新增至防火牆排除項。

為了使程式正常運行，請確保KUMA元件能夠透過安裝KUMA元件時指定的協定和連接埠，透過網路與其他元件和程式互動。

收集器隨即安裝。您可以使用收集器從事件來源接收資料，並將資料傳送以供處理。

驗證收集器安裝

若要驗證收集器是否已準備好接收事件：

1. 在KUMA主控台中，請轉至**資源** → **活動服務**部分。
2. 確保您安裝的收集器處於綠色狀態。

   如果收集器的狀態不是綠色，請在安裝它的裝置上查看此服務的日誌，位於/opt/kaspersky/kuma/collector/<collector ID>/log/collector目錄中。無論啟用或停用偵錯模式，都會記錄錯誤。

如果收集器安裝正確，並且您確定資料來自事件來源，則當您搜尋與收集器關聯的事件時，表格應該顯示事件。

*若要使用KUMA主控台的**事件**部分檢查標準化錯誤：*

1. 確保收集器服務正在執行。
2. 確保事件來源正在向KUMA提供事件。
3. 確保您在KUMA主控台的**資源**部分的僅限錯誤資源的**保留原始事件**下拉清單中選擇了**僅錯誤**。
4. 在KUMA的**事件**部分中，使用以下參數搜尋事件：

   - `ServiceID = <待檢查的收集器 ID>`
   - `Raw != ""`

   如果透過此搜尋找到任何事件，則表示存在標準化錯誤，應對其進行調查。

若要使用Grafana™儀表板檢查標準化錯誤：

1. 確保收集器服務正在執行。
2. 確保事件來源正在向KUMA提供事件。
3. 開啟度量指標部分並點選KUMA收集器連結。
4. 查看標準化小工具的錯誤部分是否顯示任何錯誤。

   如果有任何錯誤，則表示存在標準化錯誤，應進行調查。

對於WEC和WMI收集器，必須確保使用唯一連接埠連接到其代理程式。此連接埠在收集器安裝精靈的**傳輸**部分。

確保收集器運作不間斷

從事件來源到KUMA的不間斷事件流對於保護網路基礎架構至關重要。可以透過將事件流自動轉發到更多收集器來確保連續性：

- 在KUMA端，必須安裝兩個或更多相同的收集器。
- 在事件來源端，必須使用協力廠商伺服器負載管理工具（例如rsyslog或nginx）來設定收集器之間的事件流控制。

使用此收集器組態，即使收集器伺服器因任何原因無法使用，也不會遺失任何傳入事件。

請記住，當事件流在收集器之間切換時，每個收集器將分別彙總事件。

如果KUMA收集器啟動失敗，且其日誌包含「panic: runtime error: slice bounds out of range [8:0]」錯誤：

1. 停用收集器。

   ```
   sudo systemctl stop kuma-collector-<收集器 ID>
   ```

2. 刪除DNS擴充快取檔案。

   ```
   sudo rm -rf /opt/kaspersky/kuma/collector/<收集器 ID>/cache/enrichment/DNS-*
   ```

3. 刪除事件快取檔案（磁碟緩衝區）。僅當您能夠丟棄收集器磁碟緩衝區中的事件時才執行此命令。

   ```
   sudo rm -rf /opt/kaspersky/kuma/collector/<收集器 ID>/buffers/*
   ```

4. 啟動收集器服務。

   ```
   sudo systemctl start kuma-collector-<收集器 ID>
   ```

使用rsyslog控制事件流

若要在事件來源伺服器上啟用rsyslog事件流控制：

1. 建立兩個或更多相同的收集器，以確保事件接收不間斷。
2. 在事件來源伺服器上安裝 rsyslog（請參閱 rsyslog 文件）。
3. 將用於在收集器之間轉送事件流的規則新增至組態檔 /etc/rsyslog.conf：

   ```
   *&period; * @@ <main collector server FQDN>: <port for incoming events>
   $ActionExecOnlyWhenPreviousIsSuspended on
   *&period; * @@ <backup collector server FQDN>: <port for incoming events>
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

   範本組態檔

   指定一個主要收集器和兩個備用收集器的範本組態檔。收集器設定為在TCP連接埠5140上接收事件。

```
*.* @@kuma-collector-01.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended on
& @@kuma-collector-02.example.com:5140
& @@kuma-collector-03.example.com:5140
$ActionExecOnlyWhenPreviousIsSuspended off
```

4. 透過執行以下命令啟用自動啟動：

   `systemctl restart rsyslog`。

現在已在事件來源伺服器上啟用事件流控制。

使用nginx控制事件流

若要使用 nginx 控制事件流，您需要建立並設定 nginx 伺服器，以接收來自事件來源的事件，然後將這些事件轉送至收集器。

若要在事件來源伺服器上啟用nginx事件流控制：

1. 建立兩個或更多相同的收集器，以確保事件接收不間斷。
2. 在用於事件流控制的伺服器上安裝nginx。
   - Oracle Linux 8.6中的安裝命令：

     `$sudo dnf install nginx`
   - Ubuntu 20.4中的安裝命令：

     `$sudo apt-get install nginx`

     從原始碼安裝時，您必須使用 `-with-stream` 選項進行編譯：
     `$ sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`
3. 在nginx伺服器上，將stream模組新增至nginx.conf 組態檔，該檔案包含在收集器之間轉送事件流的規則。

   範本流模組

   在範本模組中，事件流在收集器kuma-collector-01.example.com 和 kuma-collector-02.example.com之間分配，它們透過TCP連接埠5140和UDP連接埠5141接收事件。平衡使用nginx.example.com ngnix伺服器。

```
stream {
upstream syslog_tcp {
server kuma-collector-1.example.com:5140;
server kuma-collector-2.example.com:5140;
}
upstream syslog_udp {
server kuma-collector-1.example.com:5141;
server kuma-collector-2.example.com:5141;
}
server {
listen nginx.example.com:5140;
proxy_pass syslog_tcp;
}
server {
listen nginx.example.com:5141 udp;
proxy_pass syslog_udp;
proxy_responses 0;
}
}
worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile為工作線程開啟的檔案（RLIMIT_NOFILE）數量限制。worker_connections為工作線程可以同時開啟的最大連線數。
在事件來源伺服器上，將事件轉送到ngnix伺服器。
```

4. 透過執行以下命令重新啟動nginx：

   ```
   systemctl restart nginx
   ```

5. 事件來源伺服器上現已啟用事件流控制。

   現在已在事件來源伺服器上啟用事件流控制。

Nginx Plus可能需要微調平衡，但某些平衡方法，如Round Robin和Lest Least Connections，在ngnix的基本版本中可用。

如需瞭解設定 nginx 的詳細資訊，請參閱nginx 說明文件。

預定義收集器

下表列出的預定義收集器包含在OSMP分發套件中。

如果您需要讓預定義的 OOTB 資源適用於貴組織的基礎架構，請使用複製操作。您也可以匯出及匯入資源。不保證手動建立的預定義資源副本能正常運作。

預定義收集器

名稱	敘述
[OOTB] CEF	收集透過TCP協定接收的CEF事件。
[OOTB] Kaspersky EDR	以 JSON 格式收集來自 Kaspersky Endpoint Detection and Response 的事件。
[OOTB] KSC	透過Syslog TCP協定收集來自卡巴斯基安全管理中心的事件。

名稱	敘述
[OOTB] KSC SQL	使用MS SQL資料庫查詢收集來自卡巴斯基安全管理中心的事件。
[OOTB] Syslog	透過Syslog協定收集事件。
[OOTB] Syslog-CEF	收集透過UDP協定到達並具有Syslog標頭的CEF事件。

建立代理程式

KUMA代理程式由兩部分組成：一部分在OSMP內建立，第二部分安裝在伺服器或網路基礎架構中的資產上。

代理程式的建立分為幾個步驟：

1. **在OSMP中為代理程式建立資源集**
2. **在OSMP中建立代理程式服務**
3. **將代理程式的伺服器部分安裝到將轉送訊息的資產中**

當您建立具有wmi或wec傳輸類型的收集器時，可以自動建立用於Windows資產的KUMA代理程式。儘管這些代理程式的資源和服務集是在收集器安裝精靈中建立的，但仍必須將它們安裝到將用於轉發訊息的資產中。

為代理程式建立資源集

在 OSMP 中，代理服務是根據代理的資源集建立，該資源集會整合連接器和目標。

若要在 OSMP 中為代理建立資源集：

1. 在 OSMP 中，於 **資源和服務** → **代理程式** 下，點擊 **新增代理程式**。
   這將開啟一個用於建立代理程式的視窗，其中**基底設定**頁籤處於活動狀態。
2. 在**基底設定**頁籤上指定以下設定：
   - 在**代理程式名稱**欄位中，為建立的服務輸入一個唯一的名稱。此名稱必須包含1到128個Unicode字元。
   - 在**租用戶**下拉清單中，選擇將擁有此儲存體的租用戶。
   - 如果需要，請將**偵錯**切換開關移至活動位置以啟用服務運作日誌記錄。
   - 您可以選擇在**描述**欄位中新增最多256個Unicode字元來描述服務。
3. 按一下加號圖示 (+) 為代理建立連線，並切換至已新增的**連線 <number>**頁籤。
   您可以按一下加號圖示 (×) 來移除頁籤。

4. 在**連接器**下，新增連接器：

- 如果要選擇現有的連接器，請從下拉清單中選擇它。
- 如果要建立新的連接器，請在下拉清單中選擇**新建**，然後指定以下設定：
  - 在**名稱**欄位中指定連接器名稱。此名稱必須包含1到128個Unicode字元。
  - 在**類型**下拉清單中，選擇連接器類型，並在**基本設定**和**進階設定**頁籤中指定其設定。可用的設定取決於所選的連接器類型：
    - tcp
    - udp
    - nats-jetstream
    - kafka
    - http
    - file
    - ftp
    - nfs
    - wmi
    - wec
    - snmp

    代理類型由代理程式中使用的連接器決定。唯一的例外是目的地為二極體類型的代理程式。這些代理程式被視為二極體代理程式。

    在標準化階段使用tcp或udp連接器類型時，如果DeviceAddress事件欄位為空，則接收事件的資產的IP位址將寫入該欄位。

    在代理程式、收集器和連接器中編輯先前建立的wec或wmi連線的能力受到限制。您可以將連線類型從**wec**變更為**wmi** ，反之亦然，但不能將**wec**或**wmi**連線變更為任何其他連線類型。同時，在編輯其他連線類型時，您無法選擇**wec**或**wmi**類型。您可以建立連線，而不受連接器類型的任何限制。
- 您可以選擇在**描述**欄位中新增最多4,000個Unicode字元來描述資源。

連接器將會新增到代理程式資源集的選定連線。建立的連接器僅可在此資源集中使用，且不會顯示在網頁介面**資源和服務** → **連接器**區段中。

5. 在**目標**設定群組中，新增目標。

   - 如果要選擇現有目標，請從下拉清單中選擇。
   - 如果要建立新目標，請在下拉清單中選擇**新建**並指定以下設定：
     - 在**名稱**欄位中指定目標名稱。此名稱必須包含1到128個Unicode字元。
     - 在**類型**下拉清單中，選擇目標類型，並在**基本設定**和**進階設定**頁籤中指定其設定。可用的設定取決於所選的目標類型：
       - **nats-jetstream** — 用於NATS通訊。
       - **tcp** — 用於TCP通訊。
       - **http** —用於HTTP通訊。
       - **二極體** —用於使用資料二極體傳輸事件。
       - **kafka** — 用於Kafka通訊。
       - **file** — 用於寫入檔案。
   - 您可以選擇在**描述**欄位中新增最多4,000個Unicode字元來描述資源。

   > 代理程式目標的進階設定（例如TLS模式和壓縮）必須與要連結到代理程式的收集器的進階目標設定相符。

   可以有多個目標點。您可以按一下**新增目標**按鈕來新增，也可以按一下 ✕ 按鈕來刪除。

6. 對要建立的每個代理程式連線重複步驟3-5。

7. 按一下**儲存**按鈕。

代理的資源集隨即建立並顯示在**資源和服務** → **代理程式**下。現在，您可以在KUMA中建立代理服務。

在OSMP中建立代理程式服務

為代理建立資源集後，您可以繼續在OSMP中建立代理服務。

若要在OSMP中建立代理服務：

1. 在OSMP的主功能表中，於**資源和服務** → **有效服務**下，按一下**新增服務**。

2. 在開啟的**選擇服務**視窗中，選擇剛為代理程式建立的資源集，然後按一下**建立服務**。

代理服務隨即在OSMP中建立，並顯示在**資源和服務** → **有效服務**下。現在，代理服務必須安裝在要將資料轉發給收集器的每個資產上。安裝過程中會使用服務ID 。

在OSMP網路基礎架構中安裝代理程式

在OSMP中建立代理服務後，您可以繼續將代理安裝到將用於將資料轉發至收集器的網路基礎架構資產上。

安裝前，請先驗證系統的網路連線並開啟其元件所使用的連接埠。

在Linux資產上安裝KUMA代理程式

關閉裝置或重新啟動伺服器時，安裝在Linux裝置上的KUMA代理程式會停止。為避免手動啟動代理程式，我們建議使用在伺服器重新啟動時自動啟動應用程式的系統（例如Supervisor）來安裝代理程式。若要自動啟動代理程式，請在組態檔中定義自動啟動和自動重新啟動設定。有關配置設定的更多詳細資訊，請參閱自動應用程式啟動系統的官方文檔。在Supervisor中配置設定的範本，您可以根據需要進行調整：

```
[program:agent_<agent name>] command=sudo /opt/kaspersky/kuma/kuma agent --core
https://<KUMA Core server FQDN>:<port used by KUMA Core>

autostart=true

autorestart=true
```

若要將KUMA代理程式安裝到Linux資產：

1. 登入要安裝服務的伺服器。
2. 建立以下目錄：
   - /opt/kaspersky/kuma/
   - /opt/kaspersky/agent/
3. 將「agent」檔案複製到/opt/kaspersky/kuma/目錄。「agent」檔案位於在 KUMA 清查檔案中指定為 `kuma_utils` 變數值之主機上的 `/opt/kaspersky/kuma/utils` 目錄中。

   確保kuma檔案具有足夠的執行權限。
4. 執行以下命令：

   ```
   sudo /opt/kaspersky/kuma/kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA
   certificate> --id <agent ID> --wd <path>
   ```

   其中：
   - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
   - <port> 是 KUMA Core 用於內部通訊的連接埠（預設使用連接埠 7210）。

- <fingerprint ID of the KUMA Core CA certificate> 是連線服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，這表示建立連線時不會驗證 KUMA Core 的憑證授權單位 (CA) 憑證。如果使用 `insecure` 值，則憑證授權單位 (CA) 憑證重新簽發後，無需更新指紋。
  如果要指定指紋 ID 以驗證 KUMA Core 的憑證授權單位 (CA) 憑證，請前往 **資源和服務 → 作用中服務**，然後在功能表 (⋮) 中選取 **複製憑證指紋**。然後在代理安裝命令中使用複製的 ID。如果憑證授權單位 (CA) 憑證重新簽發，請從 Web 介面複製新的憑證指紋，並使用更新後的參數值重新啟動服務。

- <agent ID> 是在 OSMP 中建立的代理服務 ID。

- <path> 是已安裝代理檔案所在目錄的路徑。如果未指定此旗標，檔案將儲存在 kuma 檔案所在的目錄中。

範例：

```
sudo /opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX
```

KUMA代理程式已安裝在Linux資產上。此代理會將資料轉送至 OSMP，您可以設定一個收集器來接收這些資料。

在 Windows 資產上安裝 KUMA 代理程式

在將Open Single Management Platform代理程式安裝到Windows資產之前，伺服器管理員必須在Windows資產上建立一個具有EventLogReaders和作為服務登入權限的使用者帳戶。必須使用此使用者帳戶來啟動代理程式。
如果您想以本機帳戶執行代理，則需要管理員權限和「以服務方式登入」權限。如果您想遠端執行收集並僅讀取網域帳戶下的日誌，EventLogReaders權限就足夠了。

若要將 KUMA 代理程式安裝到 Windows 資產：

1. 將 kuma.exe 檔案複製到 Windows 資產上的資料夾。建議安裝在 `C:\Users\<User name>\Desktop\KUMA` 資料夾中。

   kuma.exe 檔案位於主機上的 `/opt/kaspersky/kuma/utils` 目錄中，該主機在 KUMA 清單檔案中指定為 `kuma_utils` 變數的值。

2. 使用管理員權限在Windows資產上啟動命令提示字元並找到包含kuma.exe檔案的資料夾。

3. 執行以下命令：

   ```
   kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <agent
   ID> --user <user> --install [--accept-eula]
   ```

   其中：

   - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。

   - <port> 是 KUMA Core 用於內部通訊的連接埠（預設使用連接埠 7210）。

- <fingerprint ID of the KUMA Core CA certificate> 是連線服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，這表示建立連線時不會驗證 KUMA Core 的憑證授權單位 (CA) 憑證。如果使用 `insecure` 值，則憑證授權單位 (CA) 憑證重新簽發後，無需更新指紋。
  如果要指定指紋 ID 以驗證 KUMA Core 的憑證授權單位 (CA) 憑證，請前往 **資源和服務 → 作用中服務**，然後在功能表 (⋮) 中選取 **複製憑證指紋**。然後在代理安裝命令中使用複製的 ID。如果憑證授權單位 (CA) 憑證重新簽發，請從 Web 介面複製新的憑證指紋，並使用更新後的參數值重新啟動服務。

- <agent ID> 是在 OSMP 中建立的代理服務 ID。

- <user> 是用於執行代理的使用者帳戶名稱，包括網域。

若要執行代理，必須接受「最終使用者產品授權協議」。在命令中新增 `--accept-eula` 選項，即可在代理安裝期間自動接受「最終使用者產品授權協議」。這可讓您以非互動方式執行安裝程式。若不指定此選項，須在安裝 KUMA 代理期間手動接受或拒絕產品授權協議。

例如：

- 安裝 KUMA 代理程式而不自動接受最終使用者產品授權協議：

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install
```

- 安裝 KUMA 代理並自動接受最終使用者產品授權協議：

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install --accept-eula
```

在安裝 KUMA 代理期間使用 `--accept-eula` 選項，即表示您同意並接受最終使用者產品授權協議的條款與條件。

執行 `kuma help agent` 命令即可取得說明資訊。

4. 如果您在安裝代理程式時沒有自動接受最終使用者產品授權協議，則在安裝過程中，系統將提示您閱讀最終使用者產品授權協議的文本，您可以選擇接受或拒絕該協議。

5. 如果您選擇在安裝時自動接受最終使用者產品授權協議並希望閱讀最終使用者產品授權協議的文本，或者如果在安裝過程中未自動向您提供最終使用者產品授權協議的文本，請運作以下命令：

```
kuma.exe license --show
```

若要接受最終使用者產品授權協議，請執行以下命令並按 `y`：

```
kuma.exe license
```

6. 通過以下方式之一指定代理用戶的密碼：

- 手動。

- 安裝代理程式時從檔案中獲取。

為避免手動輸入密碼，您可以將密碼新增至.TXT檔案中，並將該檔案放在與代理可執行檔相同的目錄中。

指定命令中包含密碼的檔案。例如：

```
kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install < <name of the file with the password>.txt
```

密碼檔案中的所有資料（例如，密碼.txt）都會作為密碼重定向到命令，不包括行尾字元（\n\r、\n）。

安裝後儲存代理程式資料夾的路徑：C:\ProgramData\Kaspersky Lab\KUMA\agent\${agent_id}.

若在使用 < <密碼檔案名稱>.txt標誌安裝代理之前，沒有接受「最終使用者產品授權協議」(EULA)，系統會顯示一條錯誤訊息，提示尚未接受協議。

您可以透過以下方式接受EULA：

a. 在密碼檔案中，您可以指定EULA接受標誌。為此，包含密碼的檔案必須包含兩行：第一行包含"y"，用於聲明接受 EULA；第二行包含密碼。例如：

y

<password>

代理程式安裝命令如下所示：

```
kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install < <name of the file with the password>.txt
```

在這種情況下，您在安裝代理程式時無需額外接受EULA。

若在使用密碼檔案執行命令之前已接受 EULA，則檔案中的第一行會被解譯為密碼，且安裝會中止並顯示 `Access denied` 錯誤。

b. 您可以使用--accept-eula標誌同時接受EULA和執行靜默安裝。

代理程式安裝命令如下所示：

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --accept-eula --install < <name of the file with the password>.txt
```

確保檔案中的第一行僅指定了密碼，否則將出錯。

系統會建立 `C:\ProgramData\Kaspersky Lab\KUMA\agent\<` 代理 `ID>` 資料夾，並在其中安裝 KUMA 代理服務。代理會將 Windows 事件轉送至 KUMA，而您可以設定收集器來接收這些事件。

代理服務安裝後會自動啟動。該服務也設定為在發生任何故障時重新啟動。可以從 KUMA 網頁介面重新啟動代理程式，但前提是服務處於活動狀態。否則，需要在Windows資產上手動重新啟動服務。

從Windows資產中刪除Open Single Management Platform代理程式

若要從Windows資產中刪除KUMA代理程式：

1. 在Windows電腦上以管理員權限啟動命令提示符，並找到包含kuma.exe檔案的資料夾。
2. 執行下列任意命令：
   - `kuma.exe agent --cfg <path to agent configuration file> --uninstall`
   - `kuma.exe agent --id <在 KUMA 中建立的代理服務 ID> --uninstall`

指定的KUMA代理程式已從Windows資產中刪除。Windows事件不再傳送到KUMA。

設定服務時，您可以在安裝前透過使用下列命令執行代理程式來檢查組態是否有錯誤：

```
kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <service ID> --user <user>
```

自動建立的代理程式

使用wec或wmi連接器建立收集器時，會自動建立用於接收Windows事件的代理程式。

自動建立的代理程式具有以下特殊條件：

- 自動建立的代理程式只能有一個連線。
- 自動建立的代理會顯示於 **資源和服務 → 代理程式** 下，且其名稱末端會標示 `auto created`。代理程式可被檢視，也可被刪除。
- 自動建立的代理程式的設定是根據**連接事件來源**和**傳輸**部分的收集器設定自動定義的。您只能變更已建立代理程式的收集器的設定。
- 自動建立的代理程式的描述取自**連接事件來源**部分的收集器描述。
- 自動建立的代理程式的偵錯功能可在收集器的**連線事件來源**部分中啟用和停用。
- 刪除具有自動建立代理程式的收集器時，系統會提示您選擇將收集器與代理程式一起刪除還是僅刪除收集器。僅刪除收集器時，代理程式將變為可編輯狀態。
- 刪除自動建立的代理程式時，收集器的類型將變更為**http** ，並且連接位址將從收集器的**URL**欄位中刪除。
- 如果wec或wmi連接器中至少一個Windows日誌名稱指定錯誤，代理程式將不會從連接器中列出的任何Windows日誌接收事件。同時，代理程式狀態將顯示為綠色狀態。每60秒將重複嘗試接收事件，並且錯誤訊息將新增至服務日誌中。

在KUMA介面中，建立收集器時會同時出現自動建立的代理程式。但是，它們仍然必須安裝在將用於轉發訊息的資產上。

更新代理程式

更新OSMP版本時，也必須更新安裝在遠端裝置上的WMI和WEC代理。

若要更新代理，請使用管理員帳戶並依照下列步驟操作：

1. 在OSMP的主功能表中，前往**資源和服務 → 有效服務 → 代理程式**區段，選擇要更新的代理並複製其ID。
   刪除舊代理程式後，需要此ID來安裝具有相同ID的新代理程式。
2. 在Windows中的**服務**部分中，開啟代理程式並按一下**停止**。
3. 在命令列中，轉到安裝代理程式的資料夾並執行命令以從伺服器中刪除代理程式。
   kuma.exe agent --id <在 KUMA 中建立的代理服務的 ID> --uninstall
4. 將新代理程式放在同一資料夾中。
5. 在命令列中，轉到包含新代理程式的資料夾，然後從該資料夾使用步驟1中的代理程式ID執行安裝命令。

   ```
   kuma agent --core <FQDN>:<port> --pair.fingerprint <fingerprint ID of the KUMA Core CA certificate> --id <agent ID> --user <user> --install
   ```

   其中：

   - <FQDN> 是 KUMA Core 伺服器的完全限定網域名稱。
   - <port> 是 KUMA Core 用於內部通訊的連接埠（預設使用連接埠 7210）。
   - <fingerprint ID of the KUMA Core CA certificate> 是連線服務時用於身分驗證的 CA 憑證指紋 ID。

     `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

     您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

     為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
   - <agent ID> 是在 OSMP 中建立的代理服務 ID。
   - <user> 是用來執行代理的使用者帳戶名稱，包括網域。

代理程式已更新。

將事件從隔離網段傳輸到KUMA

資料傳輸場景

資料二極體可用於將事件從隔離網段傳輸到KUMA。資料傳輸的組織方式如下：

1. 安裝在獨立伺服器上的KUMA代理程式，其具有**二極體**目標，接收事件並將其移至資料二極體將從中取得事件的目錄。

   代理程式將事件彙總在緩衝區中，直到溢位或在最後一次寫入磁碟後持續使用者定義的時間段。然後，事件被寫入代理程式暫存目錄中的檔案。該檔案被移至資料二極體處理的目錄；其名稱是檔案內容雜湊值(SHA256)和檔案建立時間的組合。

2. 資料二極體將檔案從隔離伺服器目錄移至外部伺服器目錄。

3. 安裝在外部伺服器上的具有**二極體**連接器的KUMA收集器從資料二極體放置檔案的目錄中的檔案中讀取並處理事件。

   從檔案讀取所有事件後，該檔案將自動刪除。在讀取事件之前，會根據檔案名稱中的雜湊值驗證檔案內容。如果內容驗證失敗，則刪除該檔案。

在所述場景中，KUMA元件負責將事件移至隔離網段內的特定目錄，並接收來自外部網段中特定目錄的事件。資料二極體將包含事件的檔案從隔離網段的容器傳送到外部網段的容器。

對於隔離網段內的每個資料來源，您必須建立自己的KUMA收集器和代理程式，並設定資料二極體以與單獨的目錄協同工作。

設定KUMA元件

設定用於從隔離網段傳輸資料的KUMA元件包括以下步驟：

1. 在外部網段中建立收集器服務。

   在此步驟中，您必須建立並安裝一個收集器，以接收和處理資料二極體將從隔離網段傳輸的檔案。您可以使用收集器安裝精靈建立收集器及其所需的所有資源。

   在**傳輸**步驟中，您必須選擇或建立**二極體**類型的連接器。在連接器中，您必須指定資料二極體將從隔離網段移動檔案到的目錄。

   執行收集器的使用者「kuma」必須對資料二極體從隔離網段移動資料到的目錄具有讀取/寫入/刪除權限。

2. 為 KUMA 代理建立資源集。

   在此步驟中，您必須為 KUMA 代理建立資源集，該代理將在隔離網段中接收事件，並準備將事件傳輸至資料二極體。二極體代理程式資源集具有以下需求：

   - 代理程式中的目標必須具有**二極體**類型。在此資源中，您必須指定資料二極體將從哪個目錄將檔案移至外部網段。
   - 您無法為二極體代理程式選擇**sql**或**netflow**類型的連接器。
   - 必須在二極體代理程式的連接器中停用TLS模式。

3. 將代理組態檔下載為JSON檔案。

   a. 必須將來自二極體類型目標的代理資源集下載為JSON檔案。

   b. 如果代理資源集中使用了機密資源，則必須手動將機密資料新增至組態檔。

4. 在隔離網段中安裝KUMA代理服務。

   在此步驟中，您必須根據上一個步驟建立的代理程式組態檔將代理安裝在隔離網段中。它可以安裝到Linux和Windows裝置上。

設定資料二極體

必須如下設定資料二極體：

- 資料必須以原子方式從隔離伺服器的目錄（KUMA代理程式放置資料的位置）傳輸到外部伺服器的目錄（KUMA收集器讀取資料的位置）。
- 必須從隔離伺服器中刪除已傳輸的檔案。

有關設定資料二極體的資訊，請參閱貴組織使用的資料二極體的文檔。

特殊注意事項

處理隔離網段時，不支援使用SQL和NetFlow的操作。

使用上述場景時，由於代理程式位於隔離網段中，因此無法透過KUMA主控台進行管理。此類代理程式不會顯示在活動的KUMA服務清單中。

二極體代理程式組態檔

可以將建立的一組具有二極體類型目標的代理程式資源下載為組態檔。在隔離網段中安裝代理程式時使用此檔案。

若要下載組態檔：

在 OSMP 的主選單中，於 **資源和服務 → 代理程式** 下，選擇具有「二極體」目標的相關代理資源集，然後按一下 **下載設定**。

代理程式設定組態會根據瀏覽器的設定，以 JSON 檔案格式下載。代理資源組中使用的密鑰會以空值狀態下載。其 ID 於檔案的 `secrets` 區段中指定。若要在隔離網路段中使用組態檔安裝代理，必須手動將密鑰新增至組態檔（例如，指定代理連接器中用於接收事件的URL與密碼）。

您必須使用存取控制清單 (ACL) 來設定在將安裝代理程式的伺服器上存取檔案的權限。執行二極體代理程式的使用者帳戶必須具有檔案讀取存取權限。

以下是具有kafka連接器的二極體代理程式組態檔的範本。

```
{
"config": {
"id": "<代理程式資源集的ID>"
"name": "<代理程式資源集的名稱>"
"proxyConfigs": [
{
"connector": {
"id": "<連接器的ID。此範本展示了kafka類型的連接器，但其他類型的連接器也可以在二極體代理程式中使用。如果直接在代理程式資源集合中建立連接器，則ID未定義。>",
"name": "<連接器的名稱>"
"kind": "kafka",
"connections": [
{
"kind": "kafka",
"urls": [
"localhost:9093"
],
"host": "",
"port": "",
"secretID": "<密鑰的ID>"
"clusterID": "",
"tlsMode": "",
"proxy": null,
"rps": 0,
"maxConns": 0,
"urlPolicy": "",
"version": "",
"identityColumn": "",
"identitySeed": "",
"pollInterval": 0,
"query": "",
"stateID": "",
"certificateSecretID": "",
"authMode": "pfx",
"secretTemplateKind": "",
"certSecretTemplateKind": ""
}
],
"topic": "<kafka主題名稱>"
"groupID": "<kafka群組ID>,
"delimiter": "",
"bufferSize": 0,
"characterEncoding": "",
"query": "",
"pollInterval": 0,
"workers": 0,
"compression": "",
"debug": false,
"logs": [],
"defaultSecretID": "",
"snmpParameters": [
{
"name": "-",
"oid": "",
"key": ""
}
],
"remoteLogs": null,
"defaultSecretTemplateKind": ""
},
"destinations": [
{
"id": "<目標的ID。如果目標直接在代理程式資源集中建立，則不會定義ID。>",
"name": "<目標名稱>",
"kind": "diode",
"connection": {
"kind": "file",
"urls": [
"<指向目錄的路徑，目標應該放置資料二極體將從隔離網段傳輸的事件>",
"<臨時目錄的路徑，其中放置事件，為二極體的資料傳輸做準備>"
],
"host": "",
"port": "",
"secretID": "",
"clusterID": "",
"tlsMode": "",
"proxy": null,
"rps": 0,
```

```
"maxConns": 0,
"urlPolicy": "",
"version": "",
"identityColumn": "",
"identitySeed": "",
"pollInterval": 0,
"query": "",
"stateID": "",
"certificateSecretID": "",
"authMode": "",
"secretTemplateKind": "",
"certSecretTemplateKind": ""
},
"topic": "",
"bufferSize": 0,
"flushInterval": 0,
"diskBufferDisabled": false,
"diskBufferSizeLimit": 0,
"healthCheckPath": "",
"healthCheckTimeout": 0,
"healthCheckDisabled": false,
"timeout": 0,
"workers": 0,
"delimiter": "",
"debug": false,
"disabled": false,
"compression": "",
"filter": null,
"path": ""
}
]
}
],
"workers": 0,
"debug": false
},
"secrets": {
"<密鑰ID>": {
"pfx": "<pfx加密金鑰>",
"pfxPassword": "<pfx加密金鑰的密碼。changeit值從KUMA匯出，而不是實際密碼。在組態檔中，您必須手動指定密鑰的內容>"
}
},
"tenantID": "<租用戶ID>"
}
```


密鑰欄位說明

密鑰欄位

欄位名稱	類型	描述
`user`	字串	使用者名稱
`password`	字串	密碼
`token`	字串	權杖
`urls`	字串陣列	URL清單
`publicKey`	string	公開金輪（用於PKI）
`privateKey`	字串	私密金鑰（用於PKI）
`pfx`	包含base64編碼的pfx檔案的字串	PFX 檔案的Base64編碼內容。在Linux中，您可以透過執行以下命令來取得檔案的base64編碼： `base64 -w0 src > dst`
`pfxPassword`	字串	PFX的密碼
`securityLevel`	字串	用於SNMPv3協定。可能的值：`NoAuthNoPriv`、`AuthNoPriv`、`AuthPriv`
`community`	字串	用於snmp1

authProtocol	字串	用於SNMPv3協定。可能的值：MD5、SHA、SHA224、SHA256、SHA384、SHA512
privacyProtocol	字串	用於SNMPv3協定。可能的值：DES、AES
privacyPassword	字串	用於snmp3
certificate	包含base64編碼的pem檔案的字串	PEM檔案的base64編碼內容。在Linux中，您可以透過執行以下命令來取得檔案的base64編碼： `base64 -w0 src > dst`

在隔離網段中安裝Linux代理程式

若要將KUMA代理程式安裝到隔離網段中的Linux裝置：

1. 將以下檔案放在Linux伺服器上的隔離網段中，代理程式將用它來接收事件，資料二極體將從中將檔案移動到外部網段：

   - 代理程式組態檔。

     您必須使用存取控制清單（ACL）來設定組態檔的存取權限，以便只有KUMA使用者才能擁有檔案讀取存取權限。

   - 可執行檔 /opt/kaspersky/kuma/kuma（“kuma”檔案位於安裝程式中的 /kuma-ansible-installer/roles/kuma/files/folder 資料夾中）。

2. 執行以下命令：

   ```
   sudo ./kuma agent --cfg <path to the agent configuration file> --wd <path to the directory where the files of the agent being installed will reside&period; If this flag is not specified, the files will be stored in the directory where the kuma file is located>
   ```

代理服務安裝並執行在隔離網段中的伺服器上。它接收事件並將其轉發到資料二極體，以便將其發送到外部網段。

在隔離網段中安裝Windows代理程式

在將Open Single Management Platform代理程式安裝到Windows資產之前，伺服器管理員必須在Windows資產上建立一個具有EventLogReaders和作為服務登入權限的使用者帳戶。必須使用此使用者帳戶來啟動代理程式。

若要將KUMA代理程式安裝到隔離網段中的Windows裝置上：

1. 將下列檔案放置在隔離網段中的Windows伺服器上，代理程式將使用此網段接收事件，資料二極體將從此網段將檔案移至外部網段：

   - 代理程式組態檔。

     您必須使用存取控制清單（ACL）來設定組態檔的存取權限，以便該檔案只能由將執行代理的使用者帳戶讀取。

   - Kuma.exe可執行檔。此檔案位於安裝程式中的/kuma-ansible-installer/roles/kuma/files/目錄中。

建議使用 C:\Users\<user name>\Desktop\KUMA 資料夾。

2. 使用管理員權限在Windows資產上啟動命令提示字元並找到包含kuma.exe檔案的資料夾。

3. 執行以下命令：

```
kuma.exe agent --cfg <path to the agent configuration file> --user <user name that will run the agent, including the domain> --install
```

您可以透過執行以下命令來取得安裝程式說明資訊：

```
kuma.exe help agent
```

4. 輸入用於執行代理程式的使用者帳戶的密碼。

系統會建立 C:\Program Files\Kaspersky Lab\KUMA\agent\<Agent ID> 資料夾，並在其中安裝 KUMA 代理服務。代理會將事件移動至該資料夾，以便由資料二極體進行處理。

安裝代理程式時，代理程式組態檔將會移至目錄 C:\Program Files\ 卡巴斯基 Lab\KUMA\agent\<設定檔中指定的代理程式ID>。kuma.exe檔案將會移至C:\Program Files\Kaspersky Lab\KUMA目錄。

安裝代理程式時，其組態檔不得位於代理程式的安裝目錄中。

代理服務安裝後，會自動啟動。該服務也設定為在發生任何故障時重新啟動。

從Windows資產中刪除Open Single Management Platform代理程式

若要從Windows資產中刪除KUMA代理程式：

1. 在Windows電腦上以管理員權限啟動命令提示符，並找到包含kuma.exe檔案的資料夾。

2. 執行下列任意命令：

   - kuma.exe agent --cfg <path to agent configuration file> --uninstall
   - kuma.exe agent --id <在 KUMA 中建立的代理服務 ID> --uninstall

指定的KUMA代理程式已從Windows資產中刪除。Windows事件不再傳送到KUMA。

設定服務時，您可以在安裝前透過使用下列命令執行代理程式來檢查組態是否有錯誤：

```
kuma.exe agent --cfg <path to agent configuration file>
```

將事件從 Windows 裝置傳輸到 OSMP

若要將事件從Windows裝置傳輸到OSMP，需要結合使用KUMA代理和收集器。資料傳輸的組織方式如下：

1. 安裝在電腦上的 KUMA 代理會接收 Windows 事件：
   - 使用WEC連接器：代理程式在訂閱下接收到達主機的事件，以及伺服器日誌。
   - 使用WMI連接器：代理程式連線到組態中指定的遠端伺服器並接收事件。
2. 代理將事件（未經預處理）傳送到目標中指定的收集器。
   您可以設定代理程式，以便將不同的日誌傳送到不同的收集器。
3. 收集器從代理程式接收事件，執行完整的事件處理週期，並將處理後的事件傳送到目標。

當使用Windows事件轉送 (WEF) 從Windows主機集中收集事件時，建議從WEC代理程式接收事件。代理程式必須安裝在收集事件的伺服器上；它充當Windows事件收集器 (WEC)。我們不建議在您想要接收事件的每個端點主機上都安裝KUMA代理。

使用WEC代理程式接收事件的設定流程在附錄中詳細描述：使用KUMA代理程式 (WEC) 設定從 Windows 裝置接收事件。

如需 Windows 事件轉送技術的詳細資訊，請參閱 Microsoft® 官方文件。

我們建議在以下情況下使用WMI代理程式接收事件：

- 如果無法使用WEF技術實現事件的集中收集，同時又禁止在事件來源伺服器上安裝協力廠商軟體（例如KUMA代理程式）。
- 如果您需要從少量主機取得事件—每個 KUMA 代理不超過 500 個主機。

若要將Windows日誌連線為事件來源，我們建議使用**新增事件來源**精靈。使用精靈建立具有WEC或WMI連接器的收集器時，會自動建立用於接收Windows事件的代理程式。您也可以手動建立收集Windows事件所需的資源。

分幾個階段建立和安裝用於接收Windows事件的代理程式和收集器：

1. **為代理程式建立資源集**

   代理程式連接器：

   建立代理程式時，在**連線**頁籤上，必須建立或選擇WEC或WMI類型的連接器。

   如果WEC或WMI連接器中至少一個Windows日誌名稱指定錯誤，則代理程式會從連接器中列出的所有Windows日誌（有問題的日誌除外）接收事件。同時，代理程式狀態將顯示為綠色狀態。每60秒將重複嘗試接收事件，並且錯誤訊息將新增至服務日誌中。

   代理程式目標：

   代理程式目標的類型取決於您使用的資料傳輸方法：nats、tcp、http、diode、kafka和檔案。

   必須將 `\0` 值用作目標分隔符號。

   代理程式目標的進階設定（例如分隔符號、壓縮和TLS模式）必須與要連結到代理程式的收集器連接器的進階目標設定相符。

2. **在OSMP中建立代理程式服務**

3. **在 Windows 電腦上安裝 KUMA 代理，以從該電腦接收 Windows 事件。**

   安裝前，請確保系統元件可以存取網路並開啟必要的網路連接埠：

   - 連接埠7210，TCP：從具有收集器的伺服器到核心。
   - 連接埠7210，TCP：從代理伺服器到核心。
   - 建立連接器時在**URL**欄位中設定的連接埠：從代理伺服器到具有收集器的伺服器。

4. **建立並安裝收集器。**

   建立一組收集器時，在**傳輸**步驟中，必須建立或選擇一個連接器，收集器將使用此連接器從代理程式接收事件。連接器類型必須與代理目標的類型相符。

連接器的進階設定（例如分隔符號、壓縮和TLS模式）必須與要連結到代理程式的代理目標的進階設定相符。為了使某些常規程式正常運作，您可能需要設定收集器的其他擴充功能。

若要在收集器中編輯擴充規則設定：

1. 按一下新增擴充規則以新增擴充規則，並在對應欄位中指定下列資訊：
   - **名稱**：為規則指定任意名稱。
   - **來源類型**：dns。
   - **URL**：網域控制器的IP位址。
   - **每秒請求數**：5。
   - **工作線程**：2。
   - **快取TTL**：3600。
2. 按一下新增擴充規則以新增擴充規則，並執行下列操作：
   a. 填充以下欄位：
      - **名稱**：為規則指定任意名稱。
      - **來源類型**：事件。
      - **來源字段**：DestinationNTDomain。
      - **目標欄位**：DestinationNTDomain。
   b. 按一下**新增轉換**並在對應欄位中指定以下資訊：
      - **類型**：append。
      - **常數**：`.RU`。
      - **類型**：replace。
      - **字元**：`RU.RU`。
      - **使用字元**：`RU`。

3. 重複步驟2中的子步驟，並將SourceNTDomain指定為**來源欄位**和**目標欄位**。

4. 使用LDAP資料新增擴充規則，並執行下列操作：

   - 在**LDAP 帳戶對應**下，指定網域控制站的名稱。
   - 按一下**套用預設對映**以使用標準值填入對映表。

設定代理以接收來自隔離網段的 Netflow 事件

若要接收來自隔離網路區段的 NetFlow 事件，會使用安裝在該區段內的專用代理。代理會作為中繼節點：在本機接收 NetFlow 事件，並將其轉送至已設定 NetFlow 連接器的收集器。

事件從代理到收集器的傳輸是透過 UDP 協定進行的。

若要設定接收 NetFlow 事件：

1. 建立或設定具有 NetFlow 連接器的收集器，然後在**傳輸**步驟的**進階設定**索引標籤上，將**緩衝區大小**設為 **65467**。

2. 確保隔離區段允許傳出 UDP 流量到收集器。

3. 建立用於接收事件的代理，並設定將事件傳送至具有 **NetFlow** 連接器的收集器：

   a. 在 OSMP 主選單中，於 **資源和服務 → 代理程式** 下，按一下 **建立**。

   b. 在開啟的 **建立代理程式** 視窗中，於 **基底設定** 索引標籤上，指定 **名稱** 和 **租用戶** 設定。

   c. 在 **設定資源 #{{index}}** 索引標籤上，於 **連接器** 下的 **基本設定** 索引標籤上，指定以下設定：

      - 在**名稱**欄位中，指定連接器的名稱。
      - **類型**—指定 **udp** 連接器類型。
      - **URL**—指定將安裝用於接收 NetFlow 事件之代理的主機。

   d. 在 **設定資源 #{{index}}** 索引標籤上，於 **連接器** 下的 **進階設定** 索引標籤上，指定以下設定：

      - 將 **緩衝區大小** 設定為 **65467**。這是以位元組為單位的緩衝區大小上限。

   e. 在 **設定資源 #{{index}}** 索引標籤上，於 **目的地** 下的 **基本設定** 索引標籤上，指定以下設定：

      - 在**名稱**欄位中，指定目的地的名稱。
      - **類型**—指定用於傳送事件的 UDP 協定。
      - **URL**—指定已安裝具有 **NetFlow** 連接器之收集器的主機。

   f. 在 **設定資源 #{{index}}** 索引標籤上，於 **目的地** 下的 **進階設定** 索引標籤上，指定以下設定：

      - 將 **緩衝區大小** 設定為 **65467**。這是以位元組為單位的緩衝區大小上限。

g. 點擊**建立**。

h. 在隔離網段中安裝代理。它可以安裝到Linux和Windows裝置上。

已設定從隔離網段接收 NetFlow 事件。

AI服務

本章節提供有關 Kaspersky Next XDR Expert 所支援的AI服務的資訊。

使用KIRA分析警示和事件

您可以使用Kaspersky Investigation & Response Assistant（KIRA）來分析警示和事件。作為分析的結果，您將收到自動生成的警示或事件描述，包括簡短摘要、可觀察物件清單、事件時間線、警示或事件報告和緩解建議。

此功能可加快安全事件的調查和初步分析，並且無論警示或安全事件中包含何種事件類型，均可使用。

使用協力廠商LLM提供者（**自訂**模式）時，請求將直接傳送到指定的API。使用者選擇提供者、模式和參數。資料處理是在所選服務的一側進行的。

符合以下條件時，即可使用此功能：

- 目前有一個包含AI模組的產品授權。

  如果產品授權已過期，分析結果仍可透過快取生命週期內的工作獲取，即自結果快取之日起14天內。

- 已設定與協力廠商 LLM 提供者 API 的連線。
- 該使用者擁有**警示和事件**功能區域的**寫入**權限。

使用LLM提供者設定與KIRA的整合

KIRA 支援下列第三方 LLM 提供者：

- GPT-5.4
- Deepseek-V4-Pro
- Kimi K2.6
- GLM-5.1
- MiniMax M2.7

若要使用第三方LLM提供者設定KIRA整合：

1. 取得AI模組的產品授權，並在KUMA中啟動其功能。
2. 在主應用程式視窗中，轉至**設定→KUMA→開啟KUMA設定**部分。

   這將開啟KUMA設定視窗。
3. 在**整合**部分，按一下**AI服務**
4. 這將開啟一個視窗；在該視窗中，轉至**Kaspersky Investigation & Response Assistant**頁籤。
5. 啟用**狀態**切換開關，即可啟用與KIRA的整合。

   預設情況下，切換開關是關閉的。
6. 在**模式**下，選擇與KIRA互動的**自訂**模式。依預設會選取**KSN**模式。
7. 在**基本URL**欄位中，輸入提供者的API位址（例如，https://api.openai.com/v1）。位址必須以http://或https://開頭
8. 在**API金鑰**下拉式選單中，選取或建立**權杖**類型的金鑰。

   若要建立新密鑰，請選擇**新建**。如果您使用的API不需要金鑰，請在**API金鑰**欄位中指定值為**api-key**的金鑰。
9. 在**模型**欄位中，指定您的提供者使用的模型的名稱（例如，gpt-4-turbo、llama3-70b）。
10. 在**最大提示大小**欄位中，指定請求中的最大權杖數。
11. 在**代理伺服器**下拉清單中，選擇先前建立的資源或建立新資源。
12. 選擇KIRA回應語言：俄語或繁體中文（台灣）。KUMA以您選擇的語言傳送和儲存KIRA回應。

    預設情況下，會選取俄文。
13. 點選**新增JSON檔案**按鈕，上傳包含模型參數和HTTP標頭的檔案。

    在此檔案中，您可以指定向LLM提供者發出的請求的其他參數（例如，`temperature`、`max_tokens`）。您也可以指定其他HTTP標頭。為此，您需要使用`"headers"`金鑰。如果檔案中指定了多個`"headers"`金鑰，則只會使用其中第一個。

    檔案內容範例

    ```
    {
      "temperature": 0.5,
      "max_tokens": 20000,
      "headers": {
        "OpenAI-Organization": "ORG_ID"
      }
    }
    ```

    如果 JSON 檔案中指定下列至少一個參數，AI 服務會傳回錯誤：`messages`、`model`、`audio`、`function_call`、`functions`、`modalities`、`n`、`parallel_tool_calls`、`prediction`、`response_format`、`stop`、`stream`、`stream_options`、`tool_choice`、`tools`、`web_search_options`。
14. 點選**測試連線**向指定的API發出測試請求。
15. 按一下**儲存**。

    點擊**儲存**後，系統會提示您接受最終使用者產品授權協議的條款和條件。如果您不接受最終使用者產品授權協議，您將無法儲存設定或繼續使用該功能。

儲存設定後，將顯示可用權杖數量。權杖每天都會補充。

整合隨即設定，您可以繼續進行分析。所有事件（包括新事件和先前接收的事件）均可進行分析。

使用KIRA進行分析

設定整合後，您可以使用KIRA分析警示和事件。

若要執行分析：

1. 開啟警示或事件詳情。
2. 在警示或事件詳情上方的工具列中，按一下**AI分析→使用KIRA進行分析**。

   如果您有足夠的權杖，系統將啟動分析和**在KIRA中查詢**工作。

   處理請求可能需要30秒或更長時間。

   即使請求回傳錯誤，表示請求的主題在拒絕清單中，權杖也會被消耗；剩餘權杖的資訊也會被更新。

警示或事件的分析隨即完成。

若要檢視分析結果，請在警示或事件詳情上方的工具列中，按一下**AI分析→檢視報告**。在**使用KIRA進行分析**視窗中，分析結果將顯示以下詳細資訊：

- 警示或事件的簡要概述。
- 可觀測物件清單。
- 警示或事件時間線及事件發生順序。
- 案例報告。
- 上次請求的日期和時間。
- 已消耗權杖的數量。

您可以按一下**重新分析**按鈕以執行新的分析，並忽略儲存在快取中的先前分析資料。此分析會消耗權杖。

「使用KIRA進行分析」工作可能發生的錯誤

使用KIRA進行警示和事件分析時可能會發生錯誤。

可能發生的錯誤

HTTP代碼	描述
400	服務請求無效或用戶端憑證無效。可能的原因：缺少必要參數或參數值無效；用於KSN的用戶端憑證已過期或由不受信任的憑證授權單位核發。
401	驗證失敗。用戶端憑證有效，但限制資料庫中沒有對應的記錄。可能的原因：記錄被刪除、未及時建立，或由於技術錯誤而發布了不正確的資料。
403	已超出每日權杖限額。
404	未知或不支援的使用者工作

HTTP代碼	描述
413	已超出請求權杖限額。請求包含過多的輸入權杖。每個請求允許的最大權杖數為16,000個，包括服務參數。如果超過此限制，則不進行分析。
500	內部服務錯誤。處理請求時發生未指明的錯誤。
502	AI服務不可用。KIRA無法連線。
503	服務連線錯誤。未能從KIRA取得存取權杖。
其他	連線錯誤。KSN服務傳回的未在上方列出的其他錯誤代碼。
無程式碼	KUMA端請求處理錯誤。可能的原因包括：無法讀取KSN的回應、無法將資料儲存到資料庫，或無法檢索整合設定。

使用KIRA以自然語言建立搜尋查詢

在**威脅搜尋**部分，您可以使用自然語言輸入事件搜尋查詢，使用Kaspersky Investigation & Response Assistant（KIRA）自動將查詢轉換為資料庫查詢語法，檢查查詢的正確性並在必要時對其進行細化，然後執行系統生成的查詢並取得事件搜尋結果。每次發送請求時，都會產生一個稽核事件。如果在產生請求時發生錯誤，則會顯示錯誤代碼。

權杖數量限制在以下選項中共享：

- 使用KIRA以自然語言進行搜尋查詢
- 使用KIRA進行分析

權杖總數取決於查詢和回應。您可以預覽查詢和回應將消耗的權杖數量，並編輯回應來減少權杖消耗。

如果滿足以下條件，則該功能在俄羅斯地區可用：

- 目前有一個包含AI模組的產品授權。
- 設定KIRA整合時上傳了憑證。您可以從技術支援處取得PFX格式的憑證檔案（打包在<企業名稱>.ZIP存檔中）以及憑證密碼。
- 使用者具有以下其中一個具備相應存取權限的角色：主管理員、管理員、二級分析師、一級分析師和初級分析師。只有角色為主管理員的使用者才能設定整合。

使用KIRA建立自然語言搜尋查詢並將其轉換為SQL查詢

設定好KIRA整合後，就可以開始產生搜尋查詢來找尋事件了。

若要使用KIRA建立自然語言搜尋查詢並將其轉換為SQL查詢：

1. 在**威脅搜尋**部分，在 SQL 查詢欄位下方按一下按鈕（ ）。
2. 這將開啟**KIRA SQL查詢產生器**視窗；在該視窗的查詢欄位中，輸入您希望KIRA轉換為SQL的查詢文字。

   例如：顯示2024年1月15日至16日的所有事件，其中檔案名稱為「file.txt」。

   支援俄語和英語的查詢轉換。
3. 點選**產生**按鈕。

生成的SQL查詢顯示在輸出欄位中。

例如：

```
SELECT *
FROM events
WHERE FileName = 'file.txt'
ORDER BY Timestamp DESC
```

產生的期間顯示在**期間**欄位：

例如：

2024-01-15T00:00:00.000 - 2024-01-16T00:00:00.000

如果您未在輸入中指定事件搜尋的時間範圍，則使用**事件**頁籤中設定的期間。例如，如果在**事件**中設定了「5分鐘」，並且查詢是在1月15日15:30發出的，則期間設定為2026-01-15T15:25:00.000 - 2026-01-15T15:30:00.000

您可以在套用產生的查詢之前編輯**SQL查詢**和**時間間隔**欄位中的值。

4. 如果您想知道發送查詢將消耗多少權杖，請按一下**計算所需權杖數量**。
5. 如果您想使用產生的SQL查詢執行事件搜索，請按一下**套用**按鈕。

   KIRA SQL查詢產生器視窗將自動關閉。

   產生的SQL查詢將自動插入到**威脅搜尋**頁籤的主查詢欄位中。

   絕對時間範圍欄位會自動填入產生的查詢中的值。

   例如：2026-01-15T00:00:00.000 - 2026-01-15T00:00:00.000
6. 如果您想使用產生的SQL查詢執行事件搜索，請按一下**執行查詢**。

自然語言搜尋查詢將轉換為SQL查詢，並取得事件搜尋結果。

使用自然語言建構查詢時可能出現的錯誤

可能發生的錯誤

HTTP代碼	描述
400	無效的用戶端憑證。
404	請求錯誤。
401	缺少憑證資訊。聯絡技術支援。
403	今日權杖數量已用盡。
413	請求的權杖數量已達上限。請減少請求數量。
422	自然語言請求無法轉換為SQL語法。
500	服務出現未知錯誤。
502	KIRA服務不可用。
503	取得服務存取權杖時發生錯誤。
其他	未知錯誤。
無程式碼	處理請求時發生錯誤。

設定偵測DLL劫持

DLL劫持是一種攻擊技術，它將存在弱點的合法軟體與惡意的動態連結程式庫（DLL）一起傳遞給目標系統。當存在弱點的軟體啟動時，它不會驗證動態程式庫的合法性，而是透過檔案名稱載入它。因此，惡意代碼會在合法軟體的上下文中執行。DLL劫持攻擊很難偵測，因為被劫持的軟體是合法的。為了偵測此類攻擊，會使用 AI 模組。AI模組分析應用程式的啟動和運行時參數，並識別出合法軟體啟動時攜帶惡意程式庫的可疑行為。

為了取得狀態，KUMA 會向 KSN 傳送請求。此請求包含分析所需的事件欄位資訊。收到請求後，KSN會傳送以下分析結果之一：

- `0` – **未分類**。為了取得狀態，您需要重新傳送請求。您可以使用**執行重複請求設定**來配置請求的重新傳送。
- `1` – **未知**。收到此狀態時，該程式庫不被視為惡意的。
- `2` – **可疑**。如果設定了相應的關聯規則，則收到此結果會建立警示。
- `3` – **惡意軟體**。如果設定了相應的關聯規則，則收到此結果會建立警示。與**可疑**判定相比，**惡意軟體**判定代表DLL劫持偵測的可能性更高。

結果將以數值和文字備注的形式寫入事件的KL_AI_DLLHijackingCheckResult欄位。

DLL劫持攻擊在事件擴充階段進行偵測。這是透過**檢查 DLL 劫持**擴充類型來實現的。您可以將此類擴充功能嵌入到收集器或關聯器中。我們建議將此類擴充功能嵌入到關聯器中。這樣，KSN服務的負載將顯著低於在收集器中檢查事件時的負載。

若要使用**檢查 DLL 劫持**類型的擴充功能，您的產品授權必須包含AI模組。主管理員也必須在**卡巴斯基安全網路**區段（**設定 → 整合 → AI服務 → 卡巴斯基安全網路**）中接受附加的KSN 聲明。如果您的KUMA實例有多位主管理員，只需其中一位接受KSN 聲明即可。

使用關聯器中的事件擴充功能偵測DLL劫持攻擊

若要使用關聯器中的事件擴充功能設定DLL劫持攻擊偵測：

1. 在應用程式Web介面中，選擇**資源 → 關聯器**。
2. 開始建立關聯器或開啟現有關聯器的設定。
3. 新增「檢查DLL劫持」類型的擴充功能。

   設定擴充功能時，您需要指定與建立KSN請求所需的參數相對應的欄位清單。確保您指定的欄位已在收集器中進行標準化填寫。
4. 在擴充功能設定的**篩選參數**清單中，選擇以下篩選器：**「[OOTB] DLL劫持擴充事件**。關聯器篩選器。如果清單中缺少此篩選器，請從儲存庫匯入。您也可以自行設定篩選器。
5. 若要設定應用程式在收到**可疑**或**惡意軟體**判定時產生警示，請建立對應的關聯規則。建立關聯規則時，請選擇簡單或標準類型，然後在**選擇器**頁籤中，在篩選參數中指定兩個條件：

   `KL_AI_DLLHijackingCheckResult = 2` 或 `KL_AI_DLLHijackingCheckResult = 3`

此外，在關聯規則中，指定新增擴充功能時指定的欄位（請參閱說明中的步驟3）。如果您建立了簡單類型的關聯規則，則必須將欄位列在**傳播欄位**設定中，如果您建立了標準類型的關聯規則，則必須列在**相同欄位**設定中。

使用收集器中的事件擴充功能來偵測DLL劫持攻擊

我們不建議在收集器中使用**DLL劫持**擴充功能。這會增加KSN服務的負載。相反，請將此類擴充功能新增至關聯器。

若要在收集器中使用事件擴充功能設定DLL劫持攻擊偵測：

1. 在應用程式 Web 介面中，選擇 **資源 → 收集器**。
2. 開始建立收集器或開啟現有收集器的設定。
3. 新增「檢查DLL劫持」類型的擴充功能。

   設定擴充功能時，您需要指定與建立KSN請求所需的參數相對應的欄位清單。確保您指定的欄位已在收集器中進行標準化填寫。
4. 在擴充功能設定的**篩選參數**清單中，選擇以下篩選器：**「[OOTB] DLL劫持擴充事件**。收集器篩選器。如果清單中缺少此篩選器，請從儲存庫匯入。您也可以自行設定篩選器。
5. 若要設定應用程式在收到**可疑**或**惡意軟體**判定時產生警示，請建立對應的關聯規則。建立關聯規則時，請選擇簡單或標準類型，然後在**選擇器**頁籤中，在篩選參數中指定兩個條件：

   `KL_AI_DLLHijackingCheckResult = 2` 或 `KL_AI_DLLHijackingCheckResult = 3`

   此外，在關聯規則中，請指定您在新增擴充功能時指定的欄位（請參閱說明中的步驟3）以及KL_AI_DLLHijackingCheckResult欄位。如果您建立了簡單類型的關聯規則，則必須將欄位列在**傳播欄位**設定中，如果您建立了標準類型的關聯規則，則必須列在**相同欄位**設定中。

AI資產分數和狀態。

如果您的產品授權包含AI模組，則可以安裝**AI 資產分數與狀態**服務。

AI服務有助於精確評估由觸發的關聯規則所產生的關聯事件的嚴重等級。

AI服務從可用儲存體叢集中取得具有非空白**受影響資產**欄位的關聯事件，建立預期事件序列，並訓練AI模型。基於觸發的關聯規則鏈，AI服務計算此類事件序列是否為該基礎設施的典型模式。非典型模式會提高資產的分數。

AI服務會計算**AI分數**和**AI狀態**，並顯示於資產卡中。如果移除產品授權金鑰， **AI分數**和**AI狀態**欄位將從資產卡中隱藏。重新新增產品授權金鑰後， **AI分數**和**AI狀態**欄位的值將再次顯示。

AI分數是一個數值，用於量化資產活動的非典型程度，以及是否值得關注。**AI狀態**欄位的可能值為：**低**、**中**、**高**、**緊急**。AI分數的值範圍為0到1。

四個範圍分別對應四個狀態：

低：0 ≤ 分數 < 0.25

中：0.25 ≤ 分數 < 0.5

高：0.5 ≤ 分數 < 0.75

緊急：0.75 ≤ 分數 ≤ 1

您可以在搜尋資產時，根據**AI分數**和**AI狀態**欄位進行篩選。您也可以根據**AI分數**和**AI狀態**欄位設定資產的主動分類，一旦AI服務為資產指派了分數，資產就會被自動移至與風險等級對應的類別。

您可以建立多類別結構，並根據計算的風險值自動填入資產。

在**設定→資產稽核**部分，您可以設定在資產新增到某個類別時產生的稽核事件。稽核事件可以納入關聯規則，並且您可以在儀表板和報告中監控這些事件。

若要在儀表板監控資產類別變更，請建立一個**事件**小工具，並包含類似於以下內容的查詢：

```
SELECT count(ID) AS `metric`,
formatDateTime(toTimeZone(fromUnixTimestamp64Milli(Timestamp), 'Europe/Moscow'),
'%d.%m.%Y %H:%m:%S') AS `value` FROM `events`

where DeviceVendor = 'Kaspersky' and DeviceProduct = 'KUMA' and

DeviceEventCategory = 'Audit assets' and DeviceAction= 'asset added to category'

and DeviceCustomString1 = 'Main/Categorized assets/ML/score>0.5'

GROUP BY Timestamp ORDER BY value LIMIT 250
```

若要在儀表板監控資產狀態分佈，請建立一個**依嚴重等級分組的資產**小工具。如果產品授權包含AI模組，則可以使用**依嚴重等級分組的資產**小工具。圓餅圖顯示依狀態分組的資產數量。

每次重新啟動AI服務時，AI服務都會從頭開始訓練模型，並重新評估當天事件中提及的資產的分數。

在組態檔中指定的目錄儲存AI服務從KUMA儲存體叢集取得的指定天數的事件。例如，如果組態檔指定12天，則AI服務會取得過去12天的事件。目錄中最舊的事件將被刪除。訓練好的模型儲存在同一目錄中。

模型會在UTC時間午夜重新訓練。對於當天（UTC）事件中提及的所有資產，每小時重新評估一次資產分數。

服務日誌儲存在/var/log/syslog中。

安裝AI資產分數和狀態服務

安裝AI資產分數和狀態服務

若要安裝此服務：

1. 解壓縮分發套件中包含的**mlservice-installer-XX.tgz**存檔。

   mlservice-installer-XX.tgz存檔包含用於安裝和刪除服務的指令碼，以及config.yaml組態檔。

2. 在config.yaml組態檔中，在`kuma_address`設定中，指定安裝KUMA Core主機的FQDN和KUMA Core用於監聽AI服務連線的連接埠。

   在高可用性組態中，必須指定連接埠7226。您可以為其餘設定保留預設值。安裝完成後，服務將使用config.yaml檔案中指定的設定啟動。

3. 如果您想要將服務安裝在遠端主機上，請在inventory.yaml檔案中指定遠端主機的位址，並確保您擁有網路存取權限。預設情況下，該服務依inventory.yaml檔案中指定的方式安裝在本機上。

4. 在KUMA網頁介面中取得Core憑證。為此，請在KUMA網頁介面的主視窗中，按一下視窗底部的使用者帳戶名稱以開啟選單，然後選擇**AI服務憑證**。憑證將下載到您的預設下載目錄。

   如有必要，您可以重新簽發AI服務憑證。

5. 將下載的憑證檔案重新命名為**core-external-ca.cert**。

6. 將KUMA Core憑證檔案保存在安裝程式目錄下的roles/mlservice/files目錄中。

7. 切換到服務檔案所在的目錄，然後從該目錄執行以下命令：

   `./install < inventory.yaml 的路徑 >`

8. 如果您接受最終使用者產品授權協議的條款和條件，請按Y。如果您不接受最終使用者產品授權協議的條款和條件，則無法繼續安裝此服務。您可以在mlservice-installer/eula目錄中找到包含最終使用者產品授權協議文字的檔案。

9. 安裝程式會在安裝過程中產生憑證和金鑰，並將它們放置在config.yaml組態檔中指定的目錄中。您必須將憑證上傳到KUMA。

   在KUMA網頁介面中，依序進入**設定→整合→AI服務**部分的**AI 資產分數與狀態**窗口，填寫以下欄位：

   a. 在**URL**欄位中，指定KUMA Core主機的FQDN以及KUMA Core監聽AI服務的連接埠，例如：<KUMA Core主機的FQDN>:7226。連接埠號碼必須與組態檔中指定的連接埠號碼相符。請確保該連接埠未被其他應用程式佔用。

      對於高可用性組態的KUMA安裝，**URL**欄位不會顯示在介面中，連接埠值取自KUMA_APPRAISER_AI_API_PORT環境變數，且該連接埠將為KUMA Core主機的所有IP位址開啟。

   b. 在**憑證**下拉清單中，選擇**新建憑證**以開啟**建立密鑰**視窗；在該視窗中，將**憑證**指定為金鑰類型，並從config.yaml組態檔中指定的目錄上傳憑證。

   c. 開啟**狀態**切換開關。預設情況下，切換開關是關閉的。

   d. 按一下**儲存**。

   安裝完成後，該服務將立即嘗試以1分鐘的間隔連線KUMA，持續15分鐘。如果在KUMA網頁介面中未新增憑證，則連線將失敗，服務將停止。在這種情況下，您可以新增憑證並重新啟動AI服務；該服務將嘗試重新連線。

   儲存設定後，取得Core 伺服器記錄，並確認其中不含「<port number>: bind: address already in use」錯誤。

AI服務隨即安裝。

移除AI資產分數和狀態服務

若要移除AI服務，請切換到AI服務檔案所在的目錄，然後從該目錄執行下列命令：

```
./uninstall <path to inventory.yaml>
```

重新簽發AI服務憑證

若要重新簽發AI服務憑證：

1. 在 OSMP 主控台中，前往 **設定** → **其他** → **一般** 區段。
2. 在**Core 設定**中，找到**AI 服務憑證**設定，點擊**重新簽發**按鈕。
3. 點擊**確定**以確認操作。
4. 用新憑證替換/opt/kaspersky/mlservice目錄中的憑證。
5. 執行 `systemctl restart mlservice` 指令重新啟動AI分數和AI狀態服務；同時重新啟動 KUMA Core。

新的AI服務憑證隨即套用。

AI資產分數和狀態服務的設定

可用的AI服務設定

設定	描述
`cert_file_path`	安裝程式產生的憑證所在的目錄路徑。 預設路徑： /opt/kaspersky/mlservice/service.crt 您可以指定不同的路徑。在這種情況下，請確保啟動該服務的使用者有權存取指定的目錄。
`key_file_path`	安裝程式產生的金鑰所在的目錄路徑。 預設路徑： /opt/kaspersky/mlservice/service.key 您可以指定不同的路徑。在這種情況下，請確保啟動該服務的使用者有權存取指定的目錄。
`kuma_address`	KUMA Core安裝所在主機的FQDN以及KUMA Core監聽AI服務的連接埠。若要進行高可用性組態，必須指定連接埠7226。 範例： <KUMA Core安裝所在主機的FQDN>:7226
`kuma_cert_file_path`	KUMA Core憑證所在目錄的路徑。 預設路徑： /opt/kaspersky/mlservice/core-external-ca.cert
`event_storage_path`	服務存放接收到的關聯事件的目錄路徑。 預設路徑： /var/mlservice/events
`model_storage_path`	服務存放已訓練模型的目錄路徑。 預設路徑： /var/mlservice/models
`period_for_train_days`	您希望從可用儲存叢集中取得涉及資產的關聯事件的天數，以便訓練模型。 預設設定為12天。 這意味著目錄將包含過去<N>天的事件。最舊的事件將被刪除。
`events_overlap_in_seconds`	重疊時間。當按排程下載用於評估資產分數的事件時，事件的檢索時間是從當天最後一次下載事件的時間減去events_overlap_in_seconds設定的值開始計算的。 預設值是 60 秒。 例如：接收到最後一個事件的時間為8:58。下一批事件下載的開始時間為8:57。

設定事件來源

本章節提供有關設定從各種來源接收事件的資訊。

設定接收Auditd事件

KUMA可讓您監控和稽核Linux裝置上的Auditd事件。

在設定事件接收之前，請確保為Auditd事件建立新的KUMA收集器。

設定接收Auditd事件包括以下步驟：

1. 在網路基礎設施中安裝KUMA收集器。
2. 設定事件來源伺服器。
3. 驗證KUMA收集器是否收到Auditd事件。
   您可以透過在KUMA主控台中搜尋相關事件來驗證Auditd事件來源伺服器是否設定正確。

安裝KUMA收集器以接收Auditd事件

建立收集器後，要使用rsyslog設定事件接收，必須在用於接收事件的網路基礎架構伺服器上安裝收集器。

有關安裝KUMA收集器的詳細資訊，請參閱在網路基礎架構中安裝收集器部分。

設定事件來源伺服器

rsyslog服務用於將事件從伺服器傳輸到KUMA收集器。

若要設定從伺服器到收集器的事件傳輸：

1. 確保事件來源伺服器上安裝了rsyslog服務。為此，請執行以下命令：
   ```
   systemctl status rsyslog.service
   ```
   如果伺服器上未安裝rsyslog服務，請透過執行以下命令來安裝它：
   - 對於基於RPM的版本：
     ```
     yum install rsyslog
     ```
   - 對於基於Debian或Ubuntu的版本：
     ```
     apt-get install rsyslog
     ```

   透過執行以下命令啟用此服務：

```
systemctl enable rsyslog.service
systemctl start rsyslog.service
```

2. 在/etc/rsyslog.d資料夾中，建立包含下列內容的audit.conf檔案：

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
*.* @<KUMA collector IP address>:<KUMA collector port>
```

> 如果您想透過 TCP 傳送事件，請插入以下行來取代檔案中的最後一行：
> `*.* @@<KUMA collector IP address>:<KUMA collector port>`。

3. 將變更儲存至audit.conf檔案。

4. 重新啟動rsyslog服務。

```
systemctl restart rsyslog.service
```

事件來源伺服器已設定。有關事件的資料從伺服器傳輸到KUMA收集器。

設定接收KATA/EDR事件

您可以在 KUMA SIEM系統中設定接收Kaspersky Anti Targeted Attack Platform事件。

在設定事件接收之前，請確保為KATA/EDR 事件建立KUMA收集器。

> 在KUMA主控台中建立收集器時，請確保連接埠號碼與設定將Kaspersky Anti Targeted Attack Platform事件匯出到 KUMA 的步驟4c中指定的連接埠相符，並且連接器類型與步驟4d中指定的類型相對應。

> 若要使用Syslog接收Kaspersky Anti Targeted Attack Platform事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] KATA**標準化器。

設定接收KATA/EDR事件包括以下步驟：

1. 設定轉發KATA/EDR事件

2. 在網路基礎架構中安裝KUMA收集器

3. 在KUMA收集器中驗證接收KATA/EDR事件

   您可以透過在KUMA主控台中搜尋相關事件來驗證KATA/EDR事件來源伺服器是否設定正確。Kaspersky Anti Targeted Attack Platform事件在搜尋結果表中顯示為KATA。

設定將KATA/EDR事件匯出至KUMA

若要設定將事件從Kaspersky Anti Targeted Attack Platform匯出至KUMA：

1. 在任何可以存取中央節點伺服器的電腦上的瀏覽器中，輸入託管中央節點元件的伺服器的IP位址。
   一個用於輸入Kaspersky Anti Targeted Attack Platform使用者憑證的視窗隨即開啟。
2. 在使用者憑證輸入視窗中，選取**本機管理員**核取方塊並輸入管理員憑證。
3. 請轉至**設定** → **SIEM system**部分。
4. 指定下列設定：
   a. 選取**活動日誌**和**偵測**核取方塊。
   b. 在**主機/IP**欄位中，輸入KUMA收集器的IP位址或主機名稱。
   c. 在**連接埠**欄位中，指定要連線到KUMA收集器的連接埠號碼。
   d. 在**協定**欄位中，從清單中選擇**TCP**或**UDP** 。
   e. 在**主機 ID**欄位中，指定要在SIEM系統日誌中指示為偵測來源的伺服器主機ID。
   f. 在**警示頻率**欄位中，輸入發送訊息的間隔：1到59分鐘。
   g. 如有必要，請啟用TLS加密功能。
   h. 點選**套用**。

將Kaspersky Anti Targeted Attack Platform事件匯出至KUMA隨即設定。

建立KUMA收集器以接收KATA/EDR事件

配置事件匯出設定後，必須在KUMA主控台中建立用於Kaspersky Anti Targeted Attack Platform事件的收集器。

有關建立KUMA收集器的詳細資訊，請參閱建立收集器。

在KUMA主控台中建立收集器時，請確保連接埠號碼與設定將Kaspersky Anti Targeted Attack Platform事件匯出到 KUMA 的步驟4c中指定的連接埠相符，並且連接器類型與步驟4d中指定的類型相對應。

若要使用Syslog接收Kaspersky Anti Targeted Attack Platform事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] KATA**標準化器。

安裝KUMA收集器以接收KATA/EDR事件

建立收集器後，若要設定接收Kaspersky Anti Targeted Attack Platform事件，請在用於接收事件的網路基礎架構伺服器上安裝新的收集器。

有關安裝KUMA收集器的詳細資訊，請參閱在網路基礎架構中安裝收集器部分。

設定Open Single Management Platform以將事件匯出至KUMA SIEM系統

KUMA可讓您從Open Single Management Platform管理伺服器接收事件並將其匯出至KUMA SIEM系統。

設定Open Single Management Platform的匯出與接收分階段進行：

1. 設定Open Single Management Platform事件的匯出。
2. 設定KUMA收集器。
3. 在網路基礎設施中安裝KUMA收集器。
4. 驗證KUMA收集器是否接收到Open Single Management Platform事件

   您可以使用KUMA主控台搜尋相關事件，以驗證來自Open Single Management Platform管理伺服器的事件是否已正確匯出至KUMA SIEM系統。

   若要在表格中顯示CEF格式的Open Single Management Platform事件，請輸入下列搜尋運算式：

   ```
   SELECT * FROM `events` WHERE DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
   ```

設定KUMA收集器以收集Open Single Management Platform事件

從Open Single Management Platform管理伺服器配置CEF格式的事件匯出後，在KUMA主控台中配置收集器。

若要為Open Single Management Platform事件設定KUMA收集器：

1. 在KUMA主控台中，選擇**資源→收集器**。
2. 在收集器清單中，找到具有**[OOTB] KSC**標準化器的收集器並將其開啟進行編輯。
3. 在**傳輸**步驟中，在**URL**欄位中，指定收集器用於接收Open Single Management Platform事件的連接埠。

   該連接埠必須與KUMA SIEM系統伺服器的連接埠相符。
4. 在**事件解析**步驟中，請確保已選擇**[OOTB] KSC**標準化器。

5. 在**路由**步驟中，請確保將下列目的地新增至收集器資源集：

   - **儲存**。將處理過的事件傳送到儲存。
   - **關聯器**。將處理過的事件傳送到關聯器。

   如果未新增**儲存體**和**關聯器**目標，請建立它們。

6. 在**設定驗證**頁籤中，按一下**建立並儲存服務**。

7. 複製出現的安裝KUMA收集器的命令。

安裝KUMA收集器以收集Open Single Management Platform事件

設定用於收集CEF格式的Open Single Management Platform事件的收集器後，在用於接收事件的網路基礎設施伺服器上安裝KUMA收集器。

有關安裝KUMA收集器的詳細資訊，請參閱在網路基礎設施中安裝收集器部分。

設定從MS SQL接收Open Single Management Platform事件

KUMA可讓您從MS SQL資料庫接收Open Single Management Platform事件的資訊。

在配置之前，請確保您已經為來自MS SQL的Open Single Management Platform事件建立了KUMA收集器。

> 在KUMA網頁介面中建立收集器時，在**傳輸**步驟中，選擇**[OOTB] KSC SQL**連接器。

> 若要從MS SQL資料庫接收Open Single Management Platform事件，請在**事件解析**步驟中選擇**[OOTB]KSC from SQL**規範化器。

設定事件接收包含以下步驟：

1. 在MS SQL中建立帳戶。
2. 設定SQL Server® 瀏覽器服務。
3. 建立密鑰
4. 設定連接器。
5. 在網路基礎設施中安裝收集器。
6. 驗證KUMA收集器是否收到來自MS SQL的事件。
   您可以透過在KUMA網頁介面中搜尋相關事件來驗證從MS SQL接收事件是否配置正確。

在MS SQL資料庫中建立帳戶

要從MS SQL接收卡巴斯基安全管理中心事件，需要一個具有連線和使用資料庫所需權限的使用者帳戶。

若要建立一個使用MS SQL的帳戶：

1. 請登入安裝了卡巴斯基安全管理中心的MS SQL伺服器。
2. 使用**SQL Server Management Studio** ，使用具有管理員權限的帳戶連線到MS SQL。
3. 在物件資源管理器窗格中，延伸**安全性**部分。
4. 右鍵點選**登入**資料夾，然後從快顯功能表中選擇**新建登入**。
   登入 - 新建視窗隨即開啟。
5. 在**一般**頁籤上，按一下**登入名稱**欄位旁邊的**搜尋**按鈕。
   選取使用者或群組視窗隨即開啟。
6. 在**輸入要選擇的物件名稱（範本）」**欄位中，指定物件名稱並點選**確定** 。
   選擇使用者或群組視窗隨即關閉。
7. 在**登入 - 新建**視窗的**一般**頁籤中，選擇**Windows驗證**選項。
8. 在**預設資料庫**欄位中，選擇卡巴斯基安全管理中心資料庫。
   預設的卡巴斯基安全管理中心資料庫名稱為KAV。
9. 在**使用者對應**頁籤上，設定帳戶權限：
   a. 在**對應到此登入的使用者**部分，選擇卡巴斯基安全管理中心資料庫。
   b. 在**資料庫角色成員資格**部分，選取**db_datareader**和**public**權限旁的核取方塊。
10. 在**狀態**頁籤上，設定將帳戶連線到資料庫的權限：
    - 在**連線到資料庫引擎的權限**部分，選擇**授予**。
    - 在**登入**部分，選擇**已啟用**。
11. 點擊**確定**。
    登入 - 新建視窗隨即關閉。

若要檢查帳戶權限：

1. 使用已建立的帳戶執行**SQL Server Management Studio** 。
2. 轉到任何MS SQL資料庫表並根據表進行選擇。

配置SQL Server瀏覽器服務

在MS SQL中建立帳戶後，必須設定SQL Server Browser服務。

若要設定SQL Server Browser服務：

1. 開啟**SQL Server組態管理器**。
2. 在左邊窗格中，選取**SQL Server服務**。
   服務清單隨即開啟。
3. 透過下列方式之一開啟**SQL Server瀏覽器**服務內容：
   - 按兩下**SQL Server瀏覽器**服務的名稱。
   - 右鍵按一下**SQL Server瀏覽器**服務的名稱，然後從快顯功能表中選擇**內容**。
4. 在開啟的**SQL Server瀏覽器內容**視窗中，選擇**服務**頁籤。
5. 在**啟動模式**欄位中，選擇**自動**。
6. 選擇**登入**頁籤，然後按一下**開始**按鈕。
   SQL Server瀏覽器服務的自動啟動隨即啟用。
7. 透過以下操作啟用和設定**TCP/IP**協議：
   a. 在左側窗格中，延伸**SQL Server網路組態**部分並選擇**<SQL 伺服器名稱>子部分的協定**。
   b. 右鍵按一下**TCP/IP**協議，然後從快顯功能表中選擇**啟用**。
   c. 在開啟的**警告**視窗中，點擊**確定**。
   d. 透過以下其中一組方式開啟**TCP/IP**協定內容：
      - 按兩下**TCP/IP**協定。
      - 右鍵按一下**TCP/IP**協議，然後從快顯功能表中選擇**內容**。
   e. 選擇**IP 位址**頁籤，然後在**IPALL**部分的**TCP連接埠**欄位中指定連接埠1433。
   f. 按一下**套用**以儲存變更。
   g. 按一下**確定**以關閉視窗。
8. 透過執行下列操作重新啟動**SQL Server（<SQL Server名稱>）**服務：
   a. 在左邊窗格中，選取**SQL Server服務**。
   b. 在右側的服務清單中，以滑鼠右鍵按一下**SQL Server（<SQL Server名稱>）**服務，然後從快顯功能表中選擇**重新啟動**。
9. 在**具有進階安全性的Windows Defender防火牆**中，允許伺服器在TCP連接埠1433上的入站連線。

在KUMA中建立密鑰

在MS SQL中建立和設定帳戶後，必須在KUMA主控台中新增密鑰。此資源用於儲存連線到MS SQL的憑證。

若要建立KUMA密鑰：

1. 在KUMA主控台中，開啟**資源 → 密鑰**部分。
   可用的密鑰清單隨即顯示。
2. 按一下**新增密鑰**按鈕以建立新密鑰。
   密鑰視窗隨即顯示。
3. 輸入有關密鑰的資訊：
   a. 在**名稱**欄位中，為新增的密鑰選擇名稱。
   b. 在**租用戶**下拉清單中，選擇將擁有所建立資源的租用戶。
   c. 在**類型**下拉清單中，選取**urls**。
   d. 在**URL**欄位中，指定以下形式的字串：
   `sqlserver://[<網域>%5C]<使用者名稱>:<密碼>@<伺服器>:1433/<資料庫名稱>`
   其中：
   - 網域為網域名稱。
   - %5C為網域/使用者分隔符號。代表URL格式中的"\"字元。
   - 使用者名稱為已建立的MS SQL帳戶的名稱。
   - 密碼為已建立的MS SQL帳戶的密碼。
   - 伺服器為安裝卡巴斯基安全管理中心之MS SQL資料庫所在伺服器的名稱或IP位址。
   - 資料庫名稱為卡巴斯基安全管理中心的資料庫的名稱。預設名稱為KAV。

   範例：
   `sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV`

   如果MS SQL資料庫帳戶密碼包含特殊字元（@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ; ），請將其轉換為URL格式。
4. 按一下**儲存**按鈕。

出於安全原因，儲存密鑰後，URL欄位中指定的字串將被隱藏。

設定連接器

若要將KUMA連線到MS SQL資料庫，必須設定連接器。

若要設定連接器：

1. 在KUMA主控台中，請轉至**資源→連接器**部分。
2. 在連接器清單中，找到**[OOTB] KSC SQL**連接器並開啟它進行編輯。

   如果連接器不可編輯，請複製它並開啟連接器副本進行編輯。

   如果**[OOTB] KSC SQL**連接器不可用，請聯絡您的系統管理員。
3. 在**基本設定**頁籤上的**URL**下拉清單中，選擇為連線到MS SQL資料庫而建立的密鑰。
4. 按一下**儲存**按鈕。

配置KUMA收集器以從MS SQL資料庫接收卡巴斯基安全管理中心事件

配置事件匯出設定後，必須在KUMA主控台中為從MS SQL接收的卡巴斯基安全管理中心事件建立收集器。

有關建立KUMA收集器的詳細資訊，請參閱建立收集器。

在KUMA主控台中建立收集器時，在**傳輸**步驟中選擇**[OOTB] KSC SQL連接器**。

若要從MS SQL接收卡巴斯基安全管理中心事件，在**事件解析**步驟中選擇**[OOTB] KSC from SQL**標準化器。

安裝KUMA收集器以從MS SQL資料庫接收卡巴斯基安全管理中心事件

設定收集器以從MS SQL接收卡巴斯基安全管理中心事件後，在您要接收事件的網路基礎架構收集器上安裝KUMA收集器。

有關安裝KUMA收集器的詳細資訊，請參閱在網路基礎架構中安裝收集器部分。

設定使用KUMA代理程式 (WEC) 從Windows裝置接收事件

KUMA可讓您使用WEC KUMA代理程式接收有關來自Windows裝置的事件的資訊。

設定接收事件包含以下步驟：

1. 設定從Windows裝置接收事件的政策。
2. 使用Windows事件收集器服務設定集中接收事件。
3. 授予檢視事件的權限。
4. 授予作為服務登入的權限。
5. 設定KUMA收集器。
6. 安裝KUMA收集器。
7. 將事件從Windows裝置轉送到KUMA。

設定稽核來自Windows裝置的事件

您可以在Windows裝置上為單一裝置或域中的所有裝置設定事件稽核。

本章節介紹如何在單一裝置上設定稽核以及如何使用網域群組政策設定稽核。

在Windows裝置上設定稽核政策

若要在裝置上設定稽核政策：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `secpol.msc` 並點擊**確定**。
   本機安全性政策視窗隨即開啟。
3. 選擇**安全性設定→本機政策→稽核政策**。
4. 在右側窗格中，按兩下開啟要為其啟用成功和不成功嘗試稽核的政策的內容。
5. 在**<政策名稱> 內容**視窗的**本機安全設定**頁籤上，選取**成功**和**失敗**核取方塊以追蹤成功和中斷的嘗試。
   建議為以下政策啟用成功和不成功嘗試的稽核：
   - 稽核登入
   - 稽核政策變更
   - 稽核系統事件
   - 稽核登入事件
   - 稽核帳戶管理

裝置上的稽核政策組態已完成。

使用群組政策設定稽核

除了在單一裝置上設定稽核政策之外，還可以使用網域群組政策設定稽核。

若要使用群組政策設定稽核：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `gpedit.msc` 並點擊**確定**。
   本機群組政策編輯器視窗隨即開啟。
3. 選擇**電腦組態→ Windows組態→安全性設定→本機政策→稽核政策**。
4. 在右側窗格中，按兩下開啟要為其啟用成功和不成功嘗試稽核的政策的內容。
5. 在**<政策名稱> 內容**視窗的**本機安全設定**頁籤上，選取**成功**和**失敗**核取方塊以追蹤成功和中斷的嘗試。
   建議為以下政策啟用成功和不成功嘗試的稽核：
   - 稽核登入
   - 稽核政策變更
   - 稽核系統事件
   - 稽核登入事件
   - 稽核帳戶管理

如果您想從大量伺服器接收Windows日誌，或者不允許在網域控制器上安裝KUMA代理程式，建議將Windows日誌重新導向設定到設定了Windows事件收集器服務的單一伺服器。

稽核政策現已設定在伺服器或工作站上。

使用Windows事件收集器服務設定集中接收來自Windows裝置的事件

Windows事件收集器服務可讓您集中接收有關執行Windows的伺服器和工作站上的事件的資料。您可以使用Windows事件收集器服務訂閱在遠端裝置上註冊的事件。

您可以設定以下類型的事件訂閱：

- **來源發起的訂閱**。遠端裝置將事件資料傳送至群組政策中指定位址的Windows事件收集器伺服器。有關訂閱設定過程的詳細資訊，請參閱設定從事件來源伺服器的資料傳輸部分。
- **收集器發起的訂閱**。Windows事件收集器伺服器連接到遠端裝置並獨立地從本機日誌收集事件。有關訂閱組態過程的詳細資訊，請參閱設定Windows事件收集器服務部分。

設定從事件來源伺服器傳輸資料

您可以透過設定將資料從遠端裝置傳輸到Windows事件收集器伺服器來接收伺服器和工作站上的事件的資訊。

準備步驟

1. 透過在PowerShell主控台中執行下列命令來驗證是否在事件來源伺服器上設定了Windows遠端管理服務：

   ```
   winrm get winrm/config
   ```

   如果未設定Windows遠端管理服務，請執行以下命令對其進行初始化：

   ```
   winrm quickconfig
   ```

2. 如果事件來源伺服器是網域控制器，請以管理員身分在PowerShell中執行下列指令，讓Windows日誌可透過網路使用：

   ```
   wevtutil set-log security /ca:’O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)
   ```

   透過執行以下命令驗證存取權限：

   ```
   wevtutil get-log security
   ```

在事件來源伺服器上設定防火牆

若要讓Windows事件收集器伺服器能夠接收Windows日誌項目，必須在事件來源伺服器上開啟入站連接埠。

若要開啟入站連線的連接埠：

1. 在事件來源伺服器上，按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入`wf.msc`，然後按一下**確定**。

   具有進階安全性的Windows Defender防火牆視窗隨即開啟。
3. 轉至**入站規則**部分，然後按一下**操作**窗格中的**新建規則**。

   新建入站規則精靈隨即開啟。
4. 在**規則類型**步驟中，選擇**連接埠**。
5. 在**協定和連接埠**步驟中，將**TCP**選為協定。在**特定本機連接埠**欄位中，指示相關連接埠號碼：

   - 5985（用於 HTTP 存取）
   - 5986（用於 HTTPS 存取）

   您可以指示其中一個連接埠，或同時指示兩個連接埠。
6. 在**操作**步驟中，選擇**允許連線**（預設選取）。
7. 在**描述檔**步驟中，清除**私有**和**公用**核取方塊。
8. 在**名稱**步驟中，指定新入站連線規則的名稱，然後按一下**完成**。

從事件來源伺服器傳輸資料的設定隨即完成。

Windows事件收集器伺服器必須具有讀取事件來源伺服器上的Windows日誌的權限。這些權限可以指派給Windows事件收集器伺服器帳戶和特殊使用者帳戶。有關授予權限的詳細資訊，請參閱授予使用者檢視Windows事件日誌的權限。

設定Windows事件收集器服務

Windows事件收集器伺服器可以獨立連線到裝置並收集任何嚴重程度的事件資料。

若要設定Windows事件收集器伺服器接收事件資料：

1. 在事件來源伺服器上，按**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `services.msc` 並點擊**確定**。
   服務視窗隨即開啟。
3. 在服務清單中，找到並啟動**Windows事件收集器**服務。
4. 透過執行下列操作開啟**事件檢視器**snap-in：
   a. 按組合鍵**Win+R**開啟**執行**視窗。
   b. 在開啟的視窗中，輸入 `eventvwr` 並點擊**確定**。
5. 轉至**訂閱**部分，然後按一下**操作**窗格中的**建立訂閱**。
6. 在開啟的**訂閱內容**視窗中，指定訂閱的名稱和描述，並定義以下設定：
   a. 在**目標日誌**欄位中，從清單中選擇**轉送的事件**。
   b. 在**訂閱類型和來源電腦**部分中，按一下**選擇電腦**按鈕。
   c. 在開啟的**電腦**視窗中，點選**新增網域電腦**按鈕。
   選中電腦視窗隨即開啟。
   d. 在**輸入要選擇的物件名稱（範本）**欄位中，列出要從中接收事件資訊的裝置名稱。點擊**確定**。
   e. 在**電腦**視窗中，檢查Windows事件收集器伺服器將從中收集事件資料的裝置清單，然後按一下**確定**。
   f. 在**訂閱內容**視窗的**收集的事件**欄位中，按一下**選擇事件**按鈕。
   g. 在開啟的**請求篩選器**視窗中，指定要接收裝置事件資料的頻次和資料。
   h. 如有必要，在**<所有事件代碼>**欄位中，列出要接收或不想接收其資訊的事件代碼。點擊**確定**。

7. 如果要使用特殊帳戶檢視事件資料，請執行下列操作：

   a. 在**訂閱內容**視窗中，按一下**進階**按鈕。

   b. 在開啟的**進階訂閱設定**視窗的使用者帳戶設定中，選擇**特定使用者**。

   c. 按一下**使用者和密碼**按鈕，然後輸入所選使用者的帳戶憑證。

事件收集器服務的設定隨即完成。

若要驗證設定是否正確以及Windows事件收集器伺服器是否正在接收事件資料：

在**事件檢視器**snap-in中，請轉至**事件檢視器（本機）→ Windows日誌→轉送的事件**。

授予檢視Windows事件的權限

您可以授予檢視特定裝置或網域中所有裝置的Windows事件的權限。

若要授予檢視特定裝置上的事件的權限：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `compmgmt.msc`，然後點擊**確定**。
   電腦管理視窗隨即開啟。
3. 轉至**電腦管理（本機）→本機使用者和群組→群組**。
4. 在右側窗格中，選擇**事件日誌讀取器**群組並按兩下開啟政策內容。
5. 點選**內容：事件日誌讀取器**視窗底部的**新增**按鈕。
   選擇使用者、電腦或群組視窗隨即開啟。
6. 在**輸入要選擇的物件名稱（範本）**欄位中，列出您要授予檢視事件資料權限的使用者或裝置的名稱。點擊**確定**。

若要授予檢視網域中所有裝置的事件的權限：

1. 使用管理員權限登入網域控制器。
2. 按組合鍵**Win+R**開啟**執行**視窗。
3. 這會開啟一個視窗；請在該視窗中輸入 `dsa.msc`，然後按一下 **確定**。
   Active Directory使用者和電腦視窗隨即開啟。
4. 轉至**Active Directory使用者和電腦→ <網域名稱> →內建**。
5. 在右側窗格中，選擇**事件日誌讀取器**群組並按兩下開啟政策內容。
   在**內容：事件日誌讀取器**視窗中，開啟**成員**頁籤並按一下**新增**按鈕。
   選擇使用者、電腦或群組視窗隨即開啟。
6. 在**輸入要選擇的物件名稱（範本）**欄位中，列出您要授予檢視事件資料權限的使用者或裝置的名稱。點擊**"確定"**。

授予作為服務登入的權限

您可以向特定裝置或網域中的所有裝置授予作為服務登入的權限。**作為服務登入**權限可讓您使用已被授予此權限的帳戶啟動進程。

*若要授予裝置**作為服務登入**權限：*

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `secpol.msc` 並點擊**確定**。
   本機安全性政策視窗隨即開啟。
3. 轉至**安全性設定→本機政策→使用者權限指派**。
4. 在右側窗格中，按兩下開啟**作為服務登入**政策的內容。
5. 在開啟的**內容：作為服務登入**視窗中，按一下**新增使用者或群組**按鈕。
   選擇使用者或群組隨即視窗。
6. 在**輸入物件名稱來選擇（範本）**欄位中，列出要授予作為服務登入權限的帳戶或裝置的名稱。點擊**確定**。

在授予權限之前，請確保要授予**作為服務登入**權限的帳戶或裝置未在**拒絕作為服務登入**政策的內容中列出。

*若要授予網域中的裝置**作為服務登入**權限：*

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `gpedit.msc` 並點擊**確定**。
   本機群組政策編輯器視窗隨即開啟。
3. 選擇**電腦組態→ Windows組態→安全性設定→本機政策→使用者權限指派**。
4. 在右側窗格中，按兩下開啟**作為服務登入**政策的內容。
5. 在開啟的**內容：作為服務登入**視窗中，按一下**新增使用者或群組**按鈕。
   選擇使用者或群組隨即視窗。
6. 在**輸入物件名稱來選擇（範本）**欄位中，列出要授予作為服務登入權限的使用者或裝置的名稱。點擊**確定**。

在授予權限之前，請確保要授予**作為服務登入**權限的帳戶或裝置未在**拒絕作為服務登入**政策的內容中列出。

設定KUMA收集器以接收來自Windows裝置的事件

完成裝置上的稽核原則設定、建立事件訂閱和授予所有必要的權限後，需要在KUMA主控台中為來自Windows裝置的事件建立收集器。

有關建立KUMA收集器的詳細資訊，請參閱建立收集器。

若要接收來自Windows裝置的事件，請在KUMA收集器安裝精靈中定義下列收集器設定：

1. 在**傳輸**步驟中，定義下列設定：
   a. 在**連接器**視窗中，選擇**建立**。
   b. 在**類型**欄位中，選擇**http** 。
   c. 在**分隔符號**欄位中，選擇**\0** 。
2. 在**進階設定**頁籤的**TLS模式**欄位中，選擇**附驗證** 。
3. 在**事件解析**步驟中，按一下**新增事件解析**按鈕。
4. 在開啟的**基本事件解析**視窗的**標準化器**欄位中，選擇**[OOTB] Windows Extended v.1.0**並按**確定** 。
5. 在**路由**步驟中，新增以下目標：
   - **儲存**。將處理過的事件傳送到儲存。
   - **關聯器**。將處理過的事件傳送到關聯器。

   如果未新增**儲存體**和**關聯器**目標，請建立它們。
6. 在**設定驗證**頁籤中，按一下**建立並儲存服務**。
7. 複製出現的安裝KUMA收集器的命令。

安裝KUMA收集器以從Windows裝置接收事件

設定收集器以接收Windows事件後，在用於接收事件的網路基礎架構的伺服器上安裝KUMA收集器。

有關安裝KUMA收集器的詳細資訊，請參閱在網路基礎架構中安裝收集器部分。

設定使用KUMA代理程式（WEC）將事件從Windows裝置轉送至KUMA

要完成資料轉送組態，必須建立WECKUMA代理程式，然後將其安裝在要從中接收事件資訊的裝置上。

有關在Windows裝置上建立和安裝WEC KUMA代理程式的更多詳細資訊，請參閱將事件從Windows裝置轉送至KUMA部分。

設定使用KUMA代理程式 (WMI)從Windows裝置接收事件。

KUMA可讓您使用WMI KUMA代理程式接收來自Windows裝置的事件資訊。

設定接收事件包含以下步驟：

1. 設定用於管理KUMA的稽核設定。
2. 設定從事件來源伺服器傳輸資。
3. 授予檢視事件的權限。
4. 授予作為服務登入的權限。
5. 建立KUMA收集器。

   若要從Windows裝置接收事件，請在KUMA收集器安裝精靈的**事件解析**步驟中，在**標準化器**欄位中選擇**[OOTB] Windows Extended v.1.0**。
6. 安裝KUMA收集器。
7. 將事件從Windows裝置轉送到KUMA 。

   要完成資料轉發設定，您必須建立一個WMI KUMA代理程式，然後將其安裝在您想要接收事件資訊的裝置上。

設定用於管理KUMA的審核設定

您可以在Windows裝置上使用本機政策在特定裝置上設定稽核事件，也可以使用群組政策在網域中的所有裝置上設定稽核事件。

本章節介紹如何在單一裝置上設定稽核以及如何使用網域群組政策設定稽核。

使用本機政策設定稽核

若要使用本機政策設定稽核：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `secpol.msc` 並點擊**確定**。

   本機安全性政策視窗隨即開啟。
3. 選擇**安全性設定→本機政策→稽核政策**。
4. 在右側窗格中，按兩下開啟要為其啟用成功和不成功嘗試稽核的政策的內容。
5. 在**<政策名稱> 內容**視窗的**本機安全設定**頁籤上，選取**成功**和**失敗**核取方塊以追蹤成功和中斷的嘗試。

   建議為以下政策啟用成功和不成功嘗試的稽核：

   - 稽核登入
   - 稽核政策變更
   - 稽核系統事件

- 稽核登入事件
- 稽核帳戶管理

裝置上的稽核政策組態已完成。

使用群組政策設定稽核

除了在單一裝置上設定稽核之外，還可以使用網域群組政策設定稽核。

若要使用群組政策設定稽核：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `gpedit.msc` 並點擊**確定**。
   本機群組政策編輯器視窗隨即開啟。
3. 選擇**電腦組態→ Windows組態→安全性設定→本機政策→稽核政策**。
4. 在右側窗格中，按兩下開啟要為其啟用成功和不成功嘗試稽核的政策的內容。
5. 在**<政策名稱> 內容**視窗的**本機安全設定**頁籤上，選取**成功**和**失敗**核取方塊以追蹤成功和中斷的嘗試。
   建議為以下政策啟用成功和不成功嘗試的稽核：
   - 稽核登入
   - 稽核政策變更
   - 稽核系統事件
   - 稽核登入事件
   - 稽核帳戶管理

稽核政策現已設定在伺服器或工作站上。

設定從事件來源伺服器傳輸資料

準備步驟

1. 在事件來源伺服器上，按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `services.msc` 並點擊**確定**。
   服務視窗隨即開啟。

3. 在服務清單中，找到以下服務：
   - 遠端過程呼叫 (RpcS)
   - RPC Endpoint Mapper (RpcEptMapper)
4. 檢查**狀態**列以確認這些服務具有**正在執行**狀態。

在事件來源伺服器上設定防火牆

如果事件來源伺服器上的連接埠對入站連線開放，則Windows Management Instrumentation伺服器可以接收Windows日誌項目。

若要開啟入站連線的連接埠：

1. 在事件來源伺服器上，按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入`wf.msc`，然後按一下**確定**。

   具有進階安全性的Windows Defender防火牆視窗隨即開啟。
3. 在**具有進階安全性的Windows Defender防火牆**視窗中，轉至**入站規則**部分，然後在**操作**窗格中按一下**新建規則**。

   這將開啟**新建入站規則精靈**。
4. 在**新建入站規則精靈**的**規則類型**步驟中，選擇**連接埠**。
5. 在**協定和連接埠**步驟中，將**TCP**選為協定。在**特定本機連接埠**欄位中，指示相關連接埠號碼：
   - `135`
   - `445`
   - `49152-65535`
6. 在**操作**步驟中，選擇**允許連線**（預設選取）。
7. 在**描述檔**步驟中，清除**私有**和**公用**核取方塊。
8. 在**名稱**步驟中，指定新入站連線規則的名稱，然後按一下**完成**。

從事件來源伺服器傳輸資料的設定隨即完成。

授予檢視Windows事件的權限

您可以授予檢視特定裝置或網域中所有裝置的Windows事件的權限。

若要授予檢視特定裝置上的事件的權限：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `compmgmt.msc`，然後點擊**確定**。

   電腦管理視窗隨即開啟。
3. 轉至**電腦管理（本機）→本機使用者和群組→群組**。
4. 在右側窗格中，選擇**事件日誌讀取器**群組並按兩下開啟政策內容。
5. 點選**內容：事件日誌讀取器**視窗底部的**新增**按鈕。

   選擇使用者、電腦或群組視窗隨即開啟。
6. 在**輸入要選擇的物件名稱（範本）**欄位中，列出您要授予檢視事件資料權限的使用者或裝置的名稱。點擊**確定**。

若要授予檢視網域中所有裝置的事件的權限：

1. 使用管理員權限登入網域控制器。
2. 按組合鍵**Win+R**開啟**執行**視窗。
3. 這會開啟一個視窗；請在該視窗中輸入 `dsa.msc`，然後按一下 **確定**。

   Active Directory使用者和電腦視窗隨即開啟。
4. 在**Active Directory使用者和電腦**視窗中，轉至**Active Directory使用者和電腦**部分 → **<網域名稱>** →**內建**。
5. 在右側窗格中，選擇**事件日誌讀取器**群組並按兩下開啟政策內容。

   在**內容：事件日誌讀取器**視窗中，開啟**成員**頁籤並按一下**新增**按鈕。

   選擇使用者、電腦或群組視窗隨即開啟。
6. 在**選擇使用者、電腦或群組**視窗的**輸入要選擇的物件名稱（範本）**欄位中，列出要授予其檢視事件資料權限的使用者或裝置的名稱。點擊**"確定"**。

授予作為服務登入的權限

您可以向特定裝置或網域中的所有裝置授予作為服務登入的權限。**作為服務登入**權限可讓您使用已被授予此權限的帳戶啟動進程。

在授予權限之前，請確保要授予**作為服務登入**權限的帳戶或裝置未在**拒絕作為服務登入**政策的內容中列出。

若要授予裝置作為服務登入權限：

1. 按組合鍵**Win+R**開啟**執行**視窗。
2. 在開啟的視窗中，輸入 `secpol.msc` 並點擊**確定**。

   本機安全性政策視窗隨即開啟。
3. 在**本機安全性政策**視窗中，轉至**安全性設定→ 本機政策 → 使用者權限指派**部分。
4. 在右側窗格中，按兩下開啟**作為服務登入**政策的內容。

5. 這將開啟**內容：作為服務登入**視窗；在此視窗中，按一下**新增使用者或群組** 。
   這將開啟**選擇使用者或群組**視窗。

6. 在**輸入物件名稱來選擇（範本）**欄位中，列出要授予作為服務登入權限的帳戶或裝置的名稱。點擊**確定**。

若要授予網域中的裝置作為服務登入權限：

1. 按組合鍵**Win+R**開啟**執行**視窗。

2. 在開啟的視窗中，輸入 `gpedit.msc` 並點擊**確定**。
   本機群組政策編輯器視窗隨即開啟。

3. 選擇**電腦組態→ Windows組態→安全性設定→本機政策→使用者權限指派**。

4. 在右側窗格中，按兩下開啟**作為服務登入**政策的內容。

5. 這將開啟**內容：作為服務登入**視窗；在此視窗中，按一下**新增使用者或群組** 。
   這將開啟**選擇使用者或群組**視窗。

6. 在**輸入物件名稱來選擇（範本）**欄位中，列出要授予作為服務登入權限的使用者或裝置的名稱。點擊**"確定"**。

設定接收PostgreSQL事件

KUMA可讓您使用rsyslog監視和稽核Linux裝置上的PostgreSQL稽核事件。

使用pgAudit外掛程式稽核事件。此外掛程式支援PostgreSQL 9.5及更高版本。有關pgAudit外掛程式的詳細資訊，請參閱https://github.com/pgaudit/pgaudit 。

設定接收事件包含以下步驟：

1. 安裝pdAudit外掛程式。

2. 為PostgreSQL事件建立KUMA收集器。
   若要使用rsyslog接收PostgreSQL事件，請在收集器安裝精靈的**事件解析**步驟中，選取**[OOTB] PostgreSQL pgAudit syslog**正規化器。

3. 在KUMA網路基礎架構中安裝收集器。

4. 設定事件來源伺服器。

5. 驗證KUMA收集器中是否收到PostgreSQL事件
   您可以在KUMA主控台的搜尋相關事件部分驗證PostgreSQL事件來源伺服器是否已正確設定。

安裝pgAudit外掛程式

若要安裝pgAudit外掛程式：

1. 在作業系統命令列上，以具有管理員權限的使用者身分執行下列命令：

```
sudo apt update
```

```
sudo apt -y install postgresql-<PostgreSQL version>-pgaudit
```

您必須選擇與PostgreSQL版本相符的外掛程式版本。有關PostgreSQL版本和相符外掛程式版本的資訊，請參閱https://github.com/pgaudit/pgaudit#postgresql-version-compatibility 。

範本：

```
sudo apt -y install postgresql-12-pgaudit
```

2. 找到postgres.conf組態檔。為此，請在PostgreSQL命令列上執行以下命令：

```
show data_directory
```

回應將指示組態檔的位置。

3. 建立postgres.conf組態檔的備份副本。

4. 打開postgres.conf檔案並將其中的值複製或替換為下面列出的值。

```
## pgAudit settings
shared_preload_libraries = 'pgaudit'
## database logging settings
log_destination = 'syslog'
## syslog facility
syslog_facility = 'LOCAL0'
## event ident
syslog_ident = 'Postgres'
## sequence numbers in syslog
syslog_sequence_numbers = on
## split messages in syslog
syslog_split_messages = off
## message encoding
lc_messages = 'en_US.UTF-8'
## min message level for logging
client_min_messages = log
## min error message level for logging
log_min_error_statement = info
## log checkpoints (buffers, restarts)
log_checkpoints = off
## log query duration
log_duration = off
## error description level
log_error_verbosity = default
## user connections logging
log_connections = on
## user disconnections logging
log_disconnections = on
## log prefix format
```

```
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
## log_statement
log_statement = 'none'
## hostname logging status&period; dns bane resolving affect
#performance!
log_hostname = off
## logging collector buffer status
#logging_collector = off
## pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```

5. 使用下列命令重新啟動PostgreSQL服務：
   ```
   sudo systemctl restart postgresql
   ```
6. 若要將pgAudit外掛程式載入到PostgreSQL，請在PostgreSQL命令列上執行以下命令：
   ```
   CREATE EXTENSION pgaudit
   ```

pgAudit外掛程式隨即安裝。

設定Syslog伺服器以傳送事件

rsyslog服務用於將事件從伺服器傳輸到KUMA。

若要設定從安裝了PostgreSQL的伺服器向收集器傳送事件：

1. 若要驗證事件來源伺服器上是否安裝了rsyslog服務，請以管理員身分執行下列命令：
   ```
   sudo systemctl status rsyslog.service
   ```
   如果伺服器上未安裝rsyslog服務，請透過執行以下命令來安裝它：
   - 對於基於RPM的版本：
     ```
     yum install rsyslog
     ```
   - 對於基於Debian或Ubuntu的版本：
     ```
     apt-get install rsyslog
     ```

   透過執行以下命令啟用此服務：
   ```
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```
2. 在/etc/rsyslog.d/目錄中，建立一個包含以下內容的pgsql-to-siem.conf檔案：
   ```
   If $programname contains 'Postgres' then @< 收集器的 IP 位址 >:< 收集器的連接埠 >
   For example:
   If $programname contains 'Postgres' then @192.168.1.5:1514
   ```

若要透過TCP傳送事件，檔案的內容必須如下：

```
If $programname contains 'Postgres' then @@192.168.1.5:2514
```

將變更儲存到pgsql-to-siem.conf組態檔。

3. 將以下行新增至/etc/rsyslog.conf組態檔：

```
$IncludeConfig /etc/pgsql-to-siem.conf
$RepeatedMsgReduction off
```

將變更儲存到/etc/rsyslog.conf組態檔。

4. 重新啟動rsyslog服務。

```
sudo systemctl restart rsyslog.service
```

設定接收IVK Kolchuga-K事件

您可以設定從IVK Kolchuga-K系統到KUMASIEM系統的事件接收。

設定接收事件包含以下步驟：

1. 設定將IVK Kolchuga-K事件傳送至KUMA 。
2. 建立KUMA收集器以接收來自IVK Kolchuga-K系統的事件。

   若要使用Syslog接收IVK Kolchuga-K事件，請在收集器安裝精靈的**事件解析**步驟中，選擇**[OOTB] Kolchuga-K syslog**標準化器。
3. 安裝KUMA收集器以接收IVK Kolchuga-K事件。
4. 驗證是否在KUMA中接收到IVK Kolchuga-K事件。

   您可以在KUMA主控台的搜尋相關事件部分驗證IVK Kolchuga-K事件來源是否設定正確。

設定將IVK Kolchuga-K事件匯出至KUMA

若要設定透過syslog將IVK Kolchuga-K防火牆的事件匯出至KUMA收集器：

1. 使用管理員權限透過SSH連線至防火牆。
2. 建立/etc/services和/etc/syslog.conf檔案的備份副本。
3. 在/etc/syslog.conf組態檔中，指定KUMA收集器的FQDN或IP位址。例如：

   . @kuma.example.com

   或

   . @192.168.0.100

   將更改儲存到/etc/syslog.conf組態檔。
4. 在/etc/services組態檔中，指定KUMA收集器使用的連接埠和協定。例如：

   syslog 10514/udp

   將更改儲存到/etc/services組態檔。

5. 重新啟動防火牆的syslog伺服器：

   ```
   service syslogd restart
   ```

設定接收CryptoPro NGate事件

您可以在KUMA SIEM系統中設定接收CryptoPro NGate事件。

設定接收事件包含以下步驟：

1. 設定將CryptoPro NGate事件匯出到KUMA。
2. 建立用於接收CryptoPro NGate事件的KUMA收集器。

   若要使用 Syslog 接收 CryptoPro NGate 事件，請在收集器安裝精靈的 **事件解析** 步驟中，選取 **[OOTB] NGate syslog** 正規化器。
3. 建立用於接收CryptoPro NGate事件的KUMA收集器。
4. 驗證KUMA收集器接收CryptoPro NGate事件的情況。

   您可以在KUMA主控台的搜尋相關事件部分驗證CryptoPro NGate事件來源伺服器是否設定正確。

設定將CryptoPro NGate事件匯出到KUMA

若要設定將事件從CryptoPro NGate傳送到KUMA：

1. 連線到NGate管理系統的網頁介面。
2. 將遠端syslog伺服器連線到管理系統。為此：
   a. 開啟包含syslog伺服器清單的頁面：**外部服務** → **syslog伺服器** → **新增syslog伺服器**。
   b. 輸入syslog伺服器的設定，然後點選。
3. 將syslog伺服器指派給組態以記錄叢集的日誌。為此：
   a. 在**叢集** → **摘要**部分，選擇要設定的叢集。
   b. 在**組態**頁籤上，點選相關叢集的**組態**控制項以轉至組態設定頁面。
   c. 在正在設定的組態的**Syslog伺服器**欄位中，點選**指派**。
   d. 選取要指派的syslog伺服器的核取方塊，然後點選。

      您可以指派無限數量的伺服器。

      若要新增syslog伺服器，請點選。
   e. 發布組態以啟動新設定。

4. 將syslog伺服器指派給管理系統，用於記錄管理員活動日誌。為此：

   a. 選擇**管理中心設定**功能表項目，然後在顯示的頁面上的**Syslog伺服器**下，按一下**指派** 。

   b. 在**將Syslog伺服器指派給管理中心**視窗中，選取要指派的syslog伺服器的核取方塊，然後按一下。
   您可以指派無限數量的伺服器。

因此，CryptoPro NGate的事件將會傳送到KUMA。

設定接收Ideco UTM事件

您可以透過Syslog協定在KUMA中設定接收Ideco UTM應用程式事件。

設定接收事件包含以下步驟：

1. 設定將Ideco UTM事件匯出到KUMA 。
2. 設定用於接收Ideco UTM的KUMA收集器。
   若要接收Ideco UTM事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] Ideco UTM syslog**標準化器。
3. 建立用於接收Ideco UTM事件的KUMA收集器。
4. 驗證KUMA接收Ideco UTM事件的情況。
   您可以在KUMA主控台的搜尋相關事件部分驗證Ideco UTM事件來源伺服器是否設定正確。

設定將Ideco UTM事件匯出到KUMA

若要設定將Ideco UTM事件傳送到KUMA：

1. 使用具有管理員權限的使用者帳戶連線至 Ideco UTM Web 介面。
2. 在**系統訊息轉送**功能表中，將**Syslog**切換開關移至**啟用**位置。
3. 對於**IP位址**設定，請指定KUMA收集器的IP位址。
4. 對於連接埠設定，請輸入KUMA收集器正在監聽的連接埠。
5. 按一下**儲存**以套用變更。

已設定將 Ideco UTM 事件傳送到 KUMA。

設定接收KWTS事件

您可以設定KUMA接收來自Kaspersky Web Traffic Security分析和篩選系統的事件。

設定接收事件包含以下步驟：

1. 設定將KWTS事件匯出到KUMA 。
2. 建立用於接收KWTS事件的KUMA收集器。

   若要接收KWTS事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] KWTS**標準化器。
3. 安裝用於接收KWTS事件的KUMA收集器。
4. 驗證KUMA收集器接收KWTS事件的情況。

   您可以在KUMA主控台的搜尋相關事件部分驗證KWTS事件匯出是否設定正確。

設定將KWTS事件匯出到KUMA

若要設定將KWTS事件匯出到KUMA：

1. 透過SSH以root身分連線到KWTS伺服器。
2. 在進行變更之前，請建立以下檔案的備份副本：
   - /opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template
   - /etc/rsyslog.conf
3. 確保/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template組態檔中的設定具有以下值，並根據需要進行變更：

   ```
   "siemSettings":
   {
   "enabled": true,
   "facility": "Local5",
   "logLevel": "Info",
   "formatting":
   {
   ```
4. 儲存您的變更。
5. 若要透過UDP傳送事件，請對/etc/rsyslog.conf組態檔進行下列變更：

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local5.* @<< KUMA 收集器的 IP 位址 >:< 收集器的連接埠 >>
   ```

   如果要透過TCP傳送事件，最後一行應如下所示：

   ```
   local5.* @@<< KUMA 收集器的 IP 位址 >:< 收集器的連接埠 >>
   ```

6. 儲存您的變更。
7. 使用下列命令重新啟動rsyslog服務：

   ```
   sudo systemctl restart rsyslog.service
   ```

8. 轉至KWTS網頁介面，再轉至**設定- Syslog**頁籤，然後啟用**有關流量設定檔的日誌資訊**選項。
9. 按一下**儲存**按鈕。

設定接收KLMS事件

您可以設定KUMA SIEM系統接收來自Kaspersky Linux Mail Server (KLMS) 郵件流量分析和篩選系統的事件。

設定接收事件包含以下步驟：

1. 設定將KLMS事件匯出到KUMA
2. 建立用於接收KLMS事件的KUMA收集器

   若要接收 KLMS 事件，請在收集器安裝精靈的 **事件解析** 步驟中，選取 **[OOTB] KLMS syslog CEF 正規化器**。
3. 安裝用於接收KLMS事件的KUMA收集器
4. 驗證KUMA收集器接收KLMS事件的情況

   您可以在KUMA主控台的搜尋相關事件部分驗證KLMS事件來源伺服器是否設定正確。

設定將KLMS事件匯出到KUMA

若要設定將KLMS事件匯出到KUMA：

1. 透過SSH連線到KLMS伺服器，並轉至**技術支援模式**功能表。
2. 使用klms-control公用程式將設定下載到settings.xml檔案：

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f
   /tmp/settings.xml
   ```

3. 確保/tmp/settings.xml檔案中的設定具有下列值；如有必要，請進行變更：

   ```
   <siemSettings>
   <enabled>1</enabled>
   <facility>Local1</facility>
   ...
   </siemSettings>
   ```

4. 使用下列命令套用設定：

   ```
   sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```

5. 若要透過UDP傳送事件，請對/etc/rsyslog.conf組態檔進行下列變更：

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local1.* @<< KUMA 收集器的 IP 位址 >:< 收集器的連接埠 >>
```

如果要透過TCP傳送事件，最後一行應如下所示：

```
local1.* @@<< KUMA 收集器的 IP 位址 >:< 收集器的連接埠 >>
```

6. 儲存您的變更。
7. 使用下列命令重新啟動rsyslog服務：

```
sudo systemctl restart rsyslog.service
```

設定接收KSMG事件

您可以設定KUMA SIEM系統接收來自Kaspersky Secure Mail Gateway(KSMG) 1.1郵件流量分析和篩選系統的事件。

設定接收事件包含以下步驟：

1. 設定將KSMG事件匯出至KUMA
2. 建立用於接收KSMG事件的KUMA收集器

   若要接收KSMG事件，請在收集器安裝程式的**事件解析**步驟中選擇**[OOTB] KSMG**標準化器。
3. 安裝用於接收KSMG事件的KUMA收集器
4. 驗證KUMA收集器接收KSMG事件的情況

   您可以在KUMA主控台的搜尋相關事件部分驗證KSMG事件來源伺服器是否設定正確。

設定將KSMG事件匯出至KUMA

若要設定將KSMG事件匯出到KUMA：

1. 使用具有管理員權限的帳戶透過SSH連線到KSMG伺服器。
2. 使用KSMG-control公用程式將設定下載至settings.xml檔案：

```
sudo /opt/kaspersky/ksmg/bin/ksmg-control --get-settings EventLogger -n -f
/tmp/settings.xml
```

3. 確保/tmp/settings.xml檔案中的設定具有下列值；如有必要，請進行變更：

```
<siemSettings>
<enabled>1</enabled>
```

```
<facility>Local1</facility>
```

4. 使用下列命令套用設定：

   ```
   sudo /opt/kaspersky/ksmg/bin/ksmg-control --set-settings EventLogger -n -f
   /tmp/settings.xml
   ```

5. 若要透過UDP傳送事件，請對/etc/rsyslog.conf組態檔進行下列變更：

   ```
   $WorkDirectory /var/lib/rsyslog
   $ActionQueueFileName ForwardToSIEM
   $ActionQueueMaxDiskSpace 1g
   $ActionQueueSaveOnShutdown on
   $ActionQueueType LinkedList
   $ActionResumeRetryCount -1
   local1.* @<< KUMA 收集器的 IP 位址 >:< 收集器的連接埠 >>
   ```

   如果要透過TCP傳送事件，最後一行應如下所示：

   ```
   local1.* @@<< KUMA 收集器的 IP 位址 >:< 收集器的連接埠 >>
   ```

6. 儲存您的變更。

7. 使用下列命令重新啟動rsyslog服務：

   ```
   sudo systemctl restart rsyslog.service
   ```

設定接收PT NAD事件

您可以設定在KUMA SIEM系統中接收PT NAD事件。

設定接收事件包含以下步驟：

1. 設定將PT NAD事件匯出到KUMA 。
2. 建立用於接收PT NAD事件的KUMA收集器。

   若要使用Syslog接收PT NAD事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] PT NAD json**標準化器。

3. 安裝用於接收PT NAD事件的KUMA收集器。
4. 驗證KUMA收集器接收PT NAD事件的情況。

   您可以在KUMA主控台的搜尋相關事件部分驗證PT NAD事件來源伺服器是否設定正確。

設定將PT NAD事件匯出到KUMA

透過Syslog將事件從PT NAD 11匯出到KUMA涉及以下步驟：

1. 設定ptdpi-worker@notifier模組。
2. 設定傳送包含活動、攻擊和危害指標資訊的syslog訊息。

設定ptdpi-worker@notifier模組。

若要啟用傳送偵測到的資訊安全威脅資訊的功能，您必須設定ptdpi-worker@notifier模組。

在多伺服器組態中，必須在主伺服器上遵循這些說明。

若要設定ptdpi-worker@notifier模組，請執行下列操作：

1. 開啟/opt/ptsecurity/etc/ptdpi.settings.yaml檔案：
   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```
2. 在**一般設定**設定群組中，取消「工作線程」設定的注釋，並將「notifier」新增至其值清單。
   例如：
   ```
   workers: ad alert dns es hosts notifier
   ```
3. 在檔案末尾附加一行以下格式：notifier.yaml.nad_web_url: <PT NAD主控台的URL>
   例如：
   ```
   notifier.yaml.nad_web_url: https://ptnad.example.com
   ```
   ptdpi-worker@notifier模組在傳送訊息時使用指定的URL產生會話和活動卡的連結。
4. 重新啟動感應器。
   ```
   sudo ptdpictl restart-all
   ```

ptdpi-worker@notifier模組隨即設定。

設定傳送包含活動、攻擊和危害指標資訊的syslog訊息

組態檔中可能不存在以下說明中列出的設定。如果缺少設定，則必須將其新增到檔案中。

在多伺服器PT NAD組態中，編輯主伺服器上的設定。

若要設定傳送包含活動、攻擊和危害指標資訊的syslog訊息：

1. 開啟/opt/ptsecurity/etc/ptdpi.settings.yaml檔案：
   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```
2. 預設情況下，PT NAD 會以俄語傳送活動資訊。若要接收英文資訊，請將 notifier.yaml.syslog_notifier.locale 設定的值變更為 en。
   例如：
   ```
   notifier.yaml.syslog_notifier.locale: en
   ```
3. 在notifier.yaml.syslog_notifier.addresses設定中，新增一個包含向KUMA傳送事件設定的部分。
   <連線名稱>設定只能包含拉丁字母、數字和底線字元。
   對於「address」設定，請指定KUMA收集器的IP位址。
   其他設定可以省略，在這種情況下將使用預設值。
   ```
   notifier.yaml.syslog_notifier.addresses:
   ```

```
<Connection name>:

address: <For sending to a remote server, specify protocol: UDP (default) or TCP, address and port; for local connection, specify Unix domain socket>

doc_types: [<Comma-separated message types ('alert' for information about attacks, 'detection' for activities, and 'reputation' for information about indicators of compromise)&period; By default, all types of messages are sent>]

facility: <Numeric value of the subject category>

ident: <software tag>

<Connection name>:

...
```

以下是透過 TCP 和 UDP 將包含活動、攻擊和入侵指標資訊的 syslog 訊息傳送至兩部遠端伺服器，而不寫入本機記錄檔的設定範例：

```
notifier.yaml.syslog_notifier.addresses:

remote1:

address: tcp://198.51.100.1:1514

remote2:

address: udp://198.51.100.2:2514
```

4. 將變更儲存在/opt/ptsecurity/etc/ptdpi.settings.yaml中。
5. 重新啟動ptdpi-worker@notifier模組：

   ```
   sudo ptdpictl restart-worker notifier
   ```

透過Syslog向KUMA傳送事件隨即設定。

設定使用MariaDB稽核外掛程式接收事件

KUMA允許使用MariaDB稽核外掛程式稽核事件。此外掛程式支援MySQL 5.7和MariaDB。此稽核外掛程式不支援MySQL 8。有關此外掛程式的詳細資訊可在MariaDB官方網站上找到。

我們建議使用MariaDB稽核外掛程式1.2或更高版本。

設定接收事件包含以下步驟：

1. 設定MariaDB稽核外掛程式以傳送MySQL事件並設定Syslog伺服器以傳送事件。
2. 設定MariaDB稽核外掛程式以傳送MariaDB事件並設定Syslog伺服器以傳送事件。
3. 為MySQL 5.7和MariaDB事件建立KUMA收集器。

   若要使用MariaDB稽核外掛程式接收MySQL 5.7和MariaDB事件，請在KUMA收集器安裝精靈的**事件解析**步驟中，於**正規化器**欄位選取**[OOTB] MariaDB Audit Plugin syslog**。
4. 在KUMA網路基礎架構中安裝收集器。
5. 驗證KUMA收集器是否接收MySQL和MariaDB事件。

   若要驗證MySQL和MariaDB事件來源伺服器是否設定正確，您可以搜尋相關事件。

設定MariaDB稽核外掛程式以傳送MySQL事件

MariaDB稽核外掛程式支援MySQL 5.7版本（最高5.7.30），並與MariaDB綁定在一起。

若要使用MariaDB稽核外掛程式設定MySQL 5.7事件報告：

1. 下載MariaDB分發套件並解壓縮。

   您可以從MariaDB官方網站下載MariaDB分發套件。MariaDB分發套件的作業系統必須與執行MySQL 5.7的作業系統相同。

2. 透過執行下列命令，使用具有管理員權限的帳戶連線到MySQL 5.7：

   ```
   mysql -u <使用者名稱> -p
   ```

3. 若要取得MySQL 5.7外掛程式所在的目錄，請在MySQL 5.7命令列下執行下列命令：

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

4. 在第3步取得的目錄中，從 <分發套件解壓縮到的目錄>/mariadb-server-<版本>/lib/plugins/server_audit.so 複製 MariaDB 稽核外掛程式。

5. 在作業系統的命令列下，執行以下命令：

   ```
   chmod 755 <分發套件解壓縮到的目錄> server_audit.so
   ```

   例如：

   ```
   chmod 755 /usr/lib64/mysql/plugin/server_audit.so
   ```

6. 在MySQL 5.7命令列下，執行以下命令：

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

7. 建立/etc/mysql/mysql.conf.d/mysqld.cnf組態檔的備份副本。

8. 在 /etc/mysql/mysql.conf.d/mysqld.cnf 設定檔的 `[mysqld]` 區域中，新增以下行：

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   若要停用某些稽核事件群組的事件匯出功能，請從 `server_audit_events` 設定中移除部分值。有關設定的描述可在 MariaDB 稽核外掛程式廠商的網站上找到。

9. 儲存對組態檔的變更

10. 透過執行下列命令之一重新啟動MariaDB服務：

    - `systemctl restart mysqld`，適用於使用 systemd 初始化的系統。
    - `service mysqld restart`，適用於使用 init 初始化的系統。

    用於MySQL 5.7的MariaDB稽核外掛程式隨即設定。您可以根據需要在MySQL 5.7命令列下執行以下命令：

- `show plugins`，以檢視目前的外掛程式清單。
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'`，以檢視目前的稽核設定。

設定MariaDB稽核外掛程式以傳送MariaDB事件

MariaDB稽核外掛程式從5.5.37和10.0.10版本開始包含在MariaDB分發套件中。

若要使用MariaDB審計外掛程式設定MariaDB事件匯出：

1. 透過執行下列命令，使用具有管理員權限的帳戶連線至MariaDB ：

   ```
   mysql -u <username> -p
   ```

2. 若要檢查外掛程式是否存在於作業系統外掛程式所在的目錄中，請在MariaDB命令列下執行下列指令：

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

3. 在作業系統的命令列下，執行以下命令：

   ```
   ll <上一個命令取得的目錄> | grep server_audit.so
   ```

   如果命令輸出為空且外掛程式不在目錄中，則可以將MariaDB稽核外掛程式複製到此目錄或使用較新版本的MariaDB。

4. 在MariaDB命令列下，執行以下命令：

   ```
   install plugin server_audit soname 'server_audit.so'
   ```

5. 建立/etc/mysql/my.cnf組態檔的備份副本。

6. 在 /etc/mysql/my.cnf 組態檔的 `[mysqld]` 區段中，新增以下行：

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   若要停用某些稽核事件群組的事件匯出功能，請從 `server_audit_events` 設定中移除部分值。有關設定的描述可在 MariaDB 稽核外掛程式廠商的網站上找到。

7. 儲存對組態檔的變更

8. 透過執行下列命令之一重新啟動MariaDB服務：

   - `systemctl restart mariadb` 適用於使用 systemd 初始化的系統。
   - `service mariadb restart` 適用於使用 init 初始化的系統。

用於MariaDB的MariaDB稽核外掛程式隨即設定。您可以根據需要在MariaDB命令列下執行下列命令：

- `show plugins`，以檢視目前的外掛程式清單。
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'`，以檢視目前的稽核設定。

設定Syslog伺服器以傳送事件

rsyslog服務用於將事件從伺服器傳輸到收集器。

若要設定從安裝了MySQL或MariaDB的伺服器向收集器傳送事件：

1. 在進行任何變更之前，請建立/etc/rsyslog.conf組態檔的備份副本。
2. 若要透過UDP傳送事件，請在/etc/rsyslog.conf組態檔中新增下列行：
   `*.* @<KUMA 收集器的 IP 位址>:<KUMA 收集器的連接埠>`
   例如：
   `*.* @192.168.1.5:1514`
   如果要透過TCP傳送事件，則此行應如下所示：
   `*.* @@192.168.1.5:2514`
   將變更儲存到/etc/rsyslog.conf組態檔。
3. 重新啟動rsyslog服務。
   `sudo systemctl restart rsyslog.service`

設定接收Apache Cassandra事件

KUMA允許接收有關Apache Cassandra事件的資訊。

設定接收事件包含以下步驟：

1. 在KUMA中設定Apache Cassandra事件日誌記錄。
2. 建立用於Apache Cassandra事件的KUMA收集器。
   若要接收Apache Cassandra事件，請在KUMA收集器安裝精靈的**傳輸**步驟中選擇一個**檔案**類型連接器；在**事件解析**步驟的**標準化器**欄位中，選擇**[OOTB] Apache Cassandra檔案**。
3. 在KUMA網路基礎設施中安裝收集器。
4. 驗證KUMA收集器是否接收Apache Cassandra事件。
   若要驗證Apache Cassandra事件來源伺服器是否設定正確，您可以搜尋相關事件。

在KUMA中設定Apache Cassandra事件日誌記錄

若在KUMA中設定Apache Cassandra事件日誌記錄：

1. 確保安裝Apache Cassandra的伺服器有5GB的可用磁碟空間。
2. 使用具有管理員權限的帳戶連線到Apache Cassandra伺服器。
3. 在進行變更之前，請建立以下組態檔的備份副本：
   - /etc/cassandra/cassandra.yaml
   - /etc/cassandra/logback.xml
4. 確保/etc/cassandra/cassandra.yaml組態檔中的設定具有以下值；根據需要進行更改：
   a. 在 `audit_logging_options` 區段中，將 `enabled` 設定設為 `true`。
   b. 在 `logger` 區段中，將 `class_name` 設定設為 `FileAuditLogger`。
5. 將以下行新增到/etc/cassandra/logback.xml組態檔中：

```
<!-- Audit Logging (FileAuditLogger) rolling file appender to audit.log -->
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
<file>${cassandra.logdir}/audit/audit.log</file>
<rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
<!-- rollover daily -->
<fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-
dd}.%i.zip</fileNamePattern>
<!-- each file should be at most 50MB, keep 30 days worth of history, but at most 5GB
-->
<maxFileSize>50MB</maxFileSize>
<maxHistory>30</maxHistory>
<totalSizeCap>5GB</totalSizeCap>
</rollingPolicy>
<encoder>
<pattern>%-5level [%thread] %date{ISO8601} %F:%L - %replace(%msg){'\n', '
'}%n</pattern>
</encoder>
</appender>
<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log -->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
<appender-ref ref="AUDIT"/>
</logger>
```

6. 將變更儲存至組態檔

7. 使用下列命令重新啟動Apache Cassandra服務：

   a. `sudo systemctl stop cassandra.service`

   b. `sudo systemctl start cassandra.service`

8. 重新啟動後，使用下列命令檢查Apache Cassandra的狀態：

   ```
   sudo systemctl status cassandra.service
   ```

   確保命令輸出包含以下字元序列：

   ```
   Active: active (running)
   ```

Apache Cassandra事件匯出隨即設定。事件位於/var/log/cassandra/audit/目錄的audit.log檔案(${cassandra.logdir}/audit/audit.log) 中。

設定接收FreeIPA事件

您可以透過Syslog協定在KUMA中設定接收FreeIPA事件。

設定接收事件包含以下步驟：

1. 設定將FreeIPA事件匯出到KUMA 。
2. 建立用於接收FreeIPA事件的KUMA收集器。

   若要接收FreeIPA事件，請在KUMA收集器安裝精靈的**事件解析**步驟中，在**標準化器**欄位中選擇**[OOTB] FreeIPA**。
3. 在網路基礎設施中安裝KUMA收集器。
4. 驗證KUMA是否接收FreeIPA事件。

   若要驗證FreeIPA事件來源伺服器是否設定正確，您可以搜尋相關事件。

設定將FreeIPA事件匯出至KUMA

若要設定透過Syslog協定以JSON格式將FreeIPA事件匯出至KUMA：

1. 使用具有管理員權限的帳號透過SSH連線至FreeIPA伺服器。
2. 在/etc/rsyslog.d/目錄中，建立一個名為freeipa-to-siem.conf的檔案。
3. 將以下行新增至/etc/rsyslog.d/freeipa-to-siem.conf組態檔：

   ```
   $ModLoad imfile
   $InputFileName /var/log/httpd/error_log
   $InputFileTag tag_FreeIPA_log:
   $InputFileStateFile FreeIPA_log
   $InputRunFileMonitor
   $InputFileName /var/log/dirsrv/slapd-*/audit
   $InputFileTag tag_FreeIPA_log:
   ```

```
$InputFileStateFile FreeIPA_log_audit
$InputRunFileMonitor
$InputFileName /var/log/dirsrv/slapd-*/errors
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_errors
$InputRunFileMonitor
$InputFileName /var/log/dirsrv/slapd-*/access
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_access
$InputRunFileMonitor
$InputFileName /var/log/krb5kdc.log
$InputFileTag tag_FreeIPA_log:
$InputFileStateFile FreeIPA_log_krb5kdc
$InputRunFileMonitor
template(name="ls_json" type="list" option.json="on") {
constant(value="{")
constant(value="\"@timestamp\":\"") property(name="timegenerated"
dateFormat="rfc3339")
constant(value="\",\"@version\":\"1")
constant(value="\",\"message\":\"") property(name="msg")
constant(value="\",\"host\":\"") property(name="fromhost")
constant(value="\",\"host_ip\":\"") property(name="fromhost-ip")
constant(value="\",\"logsource\":\"") property(name="fromhost")
constant(value="\",\"severity_label\":\"") property(name="syslogseverity-text")
constant(value="\",\"severity\":\"") property(name="syslogseverity")
constant(value="\",\"facility_label\":\"") property(name="syslogfacility-text")
constant(value="\",\"facility\":\"") property(name="syslogfacility")
constant(value="\",\"program\":\"") property(name="programname")
constant(value="\",\"pid\":\"") property(name="procid")
constant(value="\",\"syslogtag\":\"") property(name="syslogtag")
constant(value="\"}\n")
}
if $syslogtag contains 'tag_FreeIPA_log' then {
*.* action(type="omfwd" target="< KUMA 收集器的 IP 位址 >" port="< KUMA 收集器的連接埠 >"
protocol="< udp 或 tcp >" template="ls_json")
stop
}
```

4. 將以下行新增至/etc/rsyslog.conf組態檔：

```
$IncludeConfig /etc/freeipa-to-siem.conf
$RepeatedMsgReduction off
```

5. 儲存對組態檔的變更。

6. 重新啟動rsyslog服務。

```
sudo systemctl restart rsyslog.service
```

設定接收VipNet TIAS事件

您可以透過Syslog協定在KUMA中設定接收ViPNet TIAS事件。

設定接收事件包含以下步驟：

1. 設定將ViPNet TIAS事件匯出到KUMA 。

2. 建立用於接收ViPNet TIAS事件的KUMA收集器。

   若要使用Syslog接收ViPNet TIAS事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] Syslog-CEF**標準化器。

3. 安裝用於接收ViPNet TIAS事件的KUMA收集器。

4. 驗證KUMA接收ViPNet TIAS事件的情況。

   您可以在KUMA主控台的搜尋相關事件部分驗證ViPNet TIAS事件來源伺服器是否設定正確。

設定將ViPNet TIAS事件匯出至KUMA

若要設定透過syslog協定將ViPNet TIAS事件匯出至KUMA：

1. 使用具有管理員權限的使用者帳戶連線至ViPNet TIAS網頁介面。

2. 轉至**管理-整合**部分。

3. 在**整合**頁面上，轉至Syslog頁籤。

4. 在接收伺服器清單的工具列中，按一下**新建伺服器** 。

5. 這將開啟新伺服器卡；在此卡中：

   1. 在**伺服器位址**欄位中，輸入KUMA收集器的IP位址或網域名稱。

      例如，10.1.2.3或syslog.siem.ru

   2. 在**連接埠**欄位中，指定KUMA收集器的入站連接埠。預設埠號為514。

   3. 在**協定**清單中，選擇KUMA收集器正在監聽的傳輸層協定。預設情況下會選取UDP。

   4. 在**組織**清單中，使用核取方塊選擇ViPNet TIAS基礎設施的組織。

      僅針對基於從基礎設施選定組織的感應器收到的事件檢測到的事件傳送訊息。

   5. 在**狀態**清單中，使用核取方塊選擇事件狀態。

      僅當事件指派了選定狀態時，才會發送訊息。

6. 在**嚴重等級**清單中，使用核取方塊選擇事件的嚴重等級。

   僅發送有關具有所選嚴重等級的事件的訊息。預設情況下，清單中僅選擇高嚴重等級。

7. 在**UI語言**清單中，選擇要在訊息中接收有關事件的資訊的語言。預設情況下，會選取俄文。

6. 按一下**新增**。

7. 在清單的工具列中，**將不以CEF格式傳送事件資訊**切換開關設定為啟用。

   因此，當偵測到新事件或先前偵測到的事件的狀態發生變更時，根據設定期間選擇的狀態，相應的資訊將透過syslog協定以CEF格式傳送到接收伺服器的指定位址。

8. 按一下**儲存變更**。

設定將事件匯出到KUMA收集器。

設定接收Nextcloud事件

您可以在KUMA中設定接收Nextcloud 26.0.4事件。

設定接收事件包含以下步驟：

1. 設定Nextcloud事件稽核。

2. 設定Syslog伺服器以傳送事件。

   rsyslog服務用於將事件從伺服器傳輸到收集器。

3. 建立用於接收Nextcloud事件的KUMA收集器。

   要接收Nextcloud事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] Nextcloud syslog**標準化器，並在**傳輸**步驟中選擇**tcp**或**udp**連接器類型。

4. 安裝KUMA收集器以接收Nextcloud事件

5. 在KUMA收集器中驗證Nextcloud事件的接收情況

   您可以在KUMA主控台的搜尋相關事件部分驗證Nextcloud事件來源伺服器是否設定正確。

設定Nextcloud事件稽核

若要設定將Nextcloud事件匯出至KUMA：

1. 在安裝了Nextcloud的伺服器上，建立/home/localuser/www/nextcloud/config/config.php組態檔的備份副本。

2. 編輯/home/localuser/www/nextcloud/config/config.php Nextcloud組態檔。

3. 依如下所示編輯設定：

```
'log_type' => 'syslog',
'syslog_tag' => 'Nextcloud',
'logfile' => '',
'loglevel' => 0,
```

```
'log.condition' => [
'apps' => ['admin_audit'],
],
```

4. 重新啟動Nextcloud服務：

   ```
   sudo service restart nextcloud
   ```

設定將事件匯出到KUMA收集器。

設定Syslog伺服器以傳送Nextcloud事件

若要設定從安裝了Nextcloud的伺服器向收集器傳送事件：

1. 在/etc/rsyslog.d/目錄中，建立一個Nextcloud-to-siem.conf檔案，其內容如下：

   ```
   If $programname contains 'Nextcloud' then @<收集器的 IP 位址>:<收集器的連接埠>
   ```

   範例：

   ```
   If $programname contains 'Nextcloud' then @192.168.1.5:1514
   ```

   若要透過TCP傳送事件，檔案的內容必須如下：

   ```
   If $programname contains 'Nextcloud' then @<收集器的 IP 位址>:<收集器的連接埠>
   ```

2. 將變更儲存到Nextcloud-to-siem.conf組態檔。

3. 建立/etc/rsyslog.conf檔案的備份副本。

4. 將以下行新增至/etc/rsyslog.conf組態檔：

   ```
   $IncludeConfig /etc/Nextcloud-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. 儲存您的變更。

6. 重新啟動rsyslog服務。

   ```
   sudo systemctl restart rsyslog.service
   ```

將Nextcloud事件匯出至收集器隨即設定。

設定接收Snort事件

您可以在 KUMA 中設定接收 Snort® 3 事件。

設定接收事件包含以下步驟：

1. 設定Snort事件的日誌記錄。

2. 建立用於接收Snort事件的KUMA收集器。

   若要接收Snort事件，在收集器安裝精靈的**事件解析**步驟中，選擇**[OOTB] Snort 3 json檔案**標準化器，並在**傳輸**步驟中選擇**檔案**連接器類型。

3. 安裝KUMA收集器以接收Snort事件

4. 在KUMA收集器中驗證Snort事件的接收情況

   您可以在KUMA主控台的搜尋相關事件部分驗證Snort事件來源伺服器是否設定正確。

設定Snort事件的日誌記錄

請確定執行 Snort 的伺服器至少有 500 MB 的可用磁碟空間，以儲存單一 Snort 事件日誌。
當日誌達到 500 MB 時，Snort 會自動建立新檔案，其名稱包含 unixtime 格式的目前時間。
建議監控磁碟空間使用量。

若要設定Snort事件日誌記錄：

1. 使用具有管理員權限的帳戶，連線至安裝 Snort 的伺服器。

2. 編輯Snort組態檔。為此，請在命令列中執行以下命令：

   ```
   sudo vi /usr/local/etc/snort/snort.lua
   ```

3. 在組態檔中，編輯alert_json區塊：

   ```
   alert_json =
   {
   file = true,
   limit = 500,
   fields = 'seconds action class b64_data dir dst_addr dst_ap dst_port eth_dst eth_len \
   eth_src eth_type gid icmp_code icmp_id icmp_seq icmp_type iface ip_id ip_len msg mpls
   \
   pkt_gen pkt_len pkt_num priority proto rev rule service sid src_addr src_ap src_port \
   target tcp_ack tcp_flags tcp_len tcp_seq tcp_win tos ttl udp_len vlan timestamp',
   }
   ```

4. 要完成組態，請執行以下命令：

   ```
   sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l
   /var/log/snort -i <Snort 正在監聽的介面名稱> -m 0x1b
   ```

   因此，Snort事件就會記錄到/var/log/snort/alert_json.txt中。

設定接收Suricata事件

您可以在KUMA中設定Suricata 7.0.1事件的接收。

設定接收事件包含以下步驟：

1. 設定將Suricata事件匯出到KUMA
2. 建立用於接收Suricata事件的KUMA收集器。

   若要接收Suricata事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] Suricata json檔案**標準化器，並在**傳輸**步驟中選擇**檔案**連接器類型。
3. 安裝KUMA收集器以接收Suricata事件
4. 在KUMA收集器中驗證Suricata事件的接收情況

   您可以在KUMA主控台的搜尋相關事件部分驗證Suricata事件來源伺服器是否設定正確。

設定Suricata事件日誌記錄。

若要設定Suricata事件日誌記錄：

1. 透過SSH連線到具有管理使用者帳戶的伺服器。
2. 建立/etc/suricata/suricata.yaml檔案的備份副本。
3. 在/etc/suricata/suricata.yaml組態檔的eve-log部分設定下列值：

   ```
   - eve-log:
   enabled: yes
   filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
   filename: eve.json
   ```
4. 將變更儲存至/etc/suricata/suricata.yaml組態檔。

因此，Suricata事件將記錄到/usr/local/var/log/suricata/eve.json檔案中。

Suricata不支援限制eve.json事件檔案的大小。如有必要，您可以使用輪換來管理日誌大小。例如，要設定每小時日誌輪換，請將以下行新增至組態檔：

```
outputs:

- eve-log:

filename: eve-%Y-%m-%d-%H:%M.json

rotate-interval: hour
```

設定接收FreeRADIUS事件

您可以在KUMA中設定FreeRADIUS 3.0.26事件的接收。

設定接收事件包含以下步驟：

1. 設定FreeRADIUS事件的稽核。
2. 設定Syslog伺服器以傳送FreeRADIUS事件。
3. 建立用於接收FreeRADIUS事件的KUMA收集器。

   若要接收FreeRADIUS事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] FreeRADIUS syslog**標準化器，並在**傳輸**步驟中選擇**tcp**或**udp**連接器類型。
4. 安裝用於接收FreeRADIUS事件的KUMA收集器。
5. 驗證KUMA收集器中FreeRADIUS事件的接收情況。

   您可以在KUMA主控台的搜尋相關事件部分驗證FreeRADIUS事件來源伺服器是否設定正確。

設定FreeRADIUS事件稽核

若要 FreeRADIUS系統中設定事件稽核：

1. 使用具有管理員權限的使用者帳戶連線到安裝了FreeRADIUS系統的伺服器。
2. 建立FreeRADIUS組態檔的備份副本：

   ```
   sudo cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius /3.0/radiusd.conf.bak
   ```
3. 開啟FreeRADIUS組態檔進行編輯：

   ```
   sudo nano /etc/freeradius/3.0/radiusd.conf
   ```
4. 在「日誌」部分，如下編輯設定：

   ```
   destination = syslog
   syslog_facility = daemon
   stripped_names = no
   auth = yes
   auth_badpass = yes
   auth_goodpass = yes
   ```
5. 儲存組態檔。

FreeRADIUS事件稽核隨即設定。

設定Syslog伺服器以傳送FreeRADIUS事件

rsyslog服務用於將事件從FreeRADIUS伺服器傳輸到KUMA收集器。

若要設定從安裝了FreeRADIUS的伺服器向收集器傳送事件：

1. 在/etc/rsyslog.d/目錄中，建立FreeRADIUS-to-siem.conf檔案並在其中新增下列行：

   `If $programname contains 'radiusd' then @<收集器的 IP 位址>:<收集器的連接埠>`

   若要透過TCP傳送事件，檔案的內容必須如下：

```
If $programname contains 'radiusd' then @<收集器的 IP 位址>:<收集器的連接埠>
```

2. 建立/etc/rsyslog.conf檔案的備份副本。
3. 將以下行新增至/etc/rsyslog.conf組態檔：

   ```
   $IncludeConfig /etc/FreeRADIUS-to-siem.conf
   $RepeatedMsgReduction off
   ```

4. 儲存您的變更。
5. 重新啟動rsyslog服務。

   ```
   sudo systemctl restart rsyslog.service
   ```

將FreeRADIUS伺服器事件匯出到KUMA收集器隨即設定。

設定接收VMware vCenter事件

您可以在KUMA SIEM系統中設定接收VMware vCenter事件。

設定接收事件包含以下步驟：

1. 設定與VMware vCenter的連線。
2. 建立用於接收VMware vCenter事件的KUMA收集器。

   若要接收VMware vCenter事件，請在收集器安裝精靈的**傳輸**步驟中選擇VMware連接器類型。指定所需的設定：

   - VMware API的可用URL，例如https://vmware-server.com:6440。
   - VMware憑據—指定連線到VMware API的使用者名稱和密碼的密鑰。

   在**事件解析**步驟中，選擇**[OOTB] VMware vCenter API**標準化器。
3. 安裝用於接收VMware vCenter事件的KUMA收集器。
4. 驗證KUMA收集器接收VMware vCenter事件的情況

   您可以在KUMA主控台的搜尋相關事件部分驗證VMware vCenter事件來源伺服器是否設定正確。

設定與VMware vCenter的連線

若要設定與VMware vCenter的連線以接收事件：

1. 使用具有管理員權限的使用者帳戶連線到VMware vCenter網頁介面。
2. 轉至**安全性與使用者**部分，然後選擇**使用者**。
3. 建立使用者帳戶。
4. 轉到**角色**部分，並將**唯讀：查看物件詳細資訊，但不進行更改**角色指派給已建立的帳戶。

您將此使用者帳戶的憑據用於收集器的密鑰。

有關建立使用者帳戶的詳細資訊，請參閱VMware vCenter說明文件。

用於接收事件的VMware vCenter連線隨即設定。

設定接收zVirt事件

您可以在KUMA中設定接收zVirt 3.1事件。

設定接收事件包含以下步驟：

1. 設定將zVirt事件匯出到KUMA。
2. 建立用於接收zVirt事件的KUMA收集器。

   若要接收zVirt事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] OrionSoft zVirt syslog**標準化器，並在**傳輸**步驟中選擇**tcp**或**udp**連接器類型。
3. 安裝用於接收zVirt事件的KUMA收集器
4. 驗證KUMA收集器中zVirt事件的接收情況

   您可以在KUMA主控台的搜尋相關事件部分驗證zVirt事件來源伺服器是否設定正確。

設定zVirt事件的匯出

ZVirt可以在自託管引擎安裝模式下將事件傳送到外部系統。

若要設定將zVirt事件匯出到KUMA：

1. 在zVirt網頁介面中的**資源**下，選擇**虛擬機**。
2. 選取執行 HostedEngine 虛擬機的電腦，然後按一下**編輯**。
3. 在**編輯虛擬機**視窗中，轉至**日誌記錄**部分。
4. 選取**確定Syslog伺服器位址**核取方塊。
5. 在文字方塊中，按以下格式輸入收集器資訊：`<KUMA 收集器的 IP 位址或 FQDN>：<KUMA 收集器的連接埠>`。
6. 如果要使用TCP而不是UDP傳送日誌，請選取**使用TCP連線**核取方塊。

事件匯出隨即設定。

設定接收Zeek IDS事件

您可以在KUMA中設定Zeek IDS 1.8事件的接收。

設定接收事件包含以下步驟：

1. 轉換Zeek IDS事件日誌格式。

   KUMA標準化器支援JSON格式的Zeek IDS日誌。若要將事件傳送到KUMA標準化器，必須將日誌檔案轉換為JSON格式。

2. 建立用於接收Zeek IDS事件的KUMA收集器。

   若要接收Zeek IDS事件，請在收集器安裝精靈的**事件解析**步驟中選擇**[OOTB] ZEEK IDS json**檔案標準化器，然後在**傳輸**步驟中選擇**檔案**連接器類型。

3. 安裝KUMA收集器以接收Zeek IDS事件

4. 驗證KUMA收集器中Zeek IDS事件的接收情況

   您可以在KUMA主控台的搜尋相關事件部分驗證Zeek IDS事件來源伺服器是否設定正確。

Zeek IDS事件日誌格式的轉換

預設情況下，Zeek IDS事件會記錄在/opt/zeek/logs/current目錄中的檔案中。

「[OOTB] ZEEK IDS json file」標準化器支援 JSON 格式的 Zeek IDS 日誌。若要將事件傳送到KUMA標準化器，必須將日誌檔案轉換為JSON格式。

每次接收Zeek IDS事件之前都必須重複此過程。

若要轉換Zeek IDS事件日誌格式：

1. 使用具有管理員權限的使用者帳戶連線到安裝了Zeek IDS的伺服器。

2. 建立必須儲存JSON事件日誌的目錄：

   ```
   sudo mkdir /opt/zeek/logs/zeek-json
   ```

3. 變更為此目錄：

   ```
   sudo cd /opt/zeek/logs/zeek-json
   ```

4. 執行使用jq公用程式的命令將原始事件日誌格式轉換為目標格式：

   ```
   jq &period; -c <需轉換為其他格式的記錄檔案的路徑> >> <新檔案名稱>.log
   ```

   範例：

   ```
   jq &period; -c /opt/zeek/logs/current/conn.log >> conn.log
   ```

   執行此命令的結果是，如果此檔案之前不存在，則會在/opt/zeek/logs/zeek-json目錄中建立新檔案。如果該檔案已經存在於目前目錄中，則新資訊將附加到檔案末尾。

使用ETW連接器設定接收DNS伺服器事件

事件追蹤Windows連接器（以下簡稱ETW連接器）是一種記錄DNS伺服器上應用程式和驅動程式生成的事件的機制。您可以使用ETW連接器在開發過程中排查錯誤或找尋惡意活動。

ETW連接器對DNS伺服器效能的影響微乎其微。例如，一台運行在現代硬體上且每秒處理高達10萬次查詢（QPS）的DNS伺服器，在使用ETW連接器時可能會出現5%的效能下降。如果DNS伺服器每秒處理高達5萬次請求，則不會觀察到效能下降。我們建議在使用ETW連接器時監控DNS伺服器的效能，無論每秒請求數為何。

預設情況下，您可以在Windows Server 2016或更高版本上使用ETW連接器。如果安裝了事件日誌記錄和變更稽核更新，Windows Server 2012 R2也支援ETW連接器。該更新可從Microsoft 支援網站取得。

ETW連接器包含以下元件：

- *提供者*是產生事件並將其傳送到ETW連接器的軟體。例如，Windows核心或裝置驅動程式可以充當提供者。在編寫程式碼時，開發人員必須指定提供者要傳送到ETW連接器的事件。事件可以表示開發人員認為重要的函式的執行，例如，允許存取安全帳戶管理器（SAM）的函式。
- *消費者*是接收和使用來自ETW連接器的提供者產生的事件的軟體。例如，KUMA可以充當消費者。
- *控制器*是管理提供者和消費者之間互動的軟體。例如，Logman或Wevtutil公用程式可以充當控制器。提供程式向控制器註冊以向消費者傳送事件。控制器可以啟用或停用提供者。如果提供者已停用，則不會產生事件。

  控制器使用追蹤會話進行提供者和使用者之間的通訊。追蹤會話也用於根據指定的參數篩選資料，因為使用者可能需要不同的事件。

使用ETW連接器設定接收DNS伺服器事件包含以下步驟：

1. Windows端的設定。
2. 建立KUMA收集器。

   建立KUMA收集器時，請依照下列步驟操作：

   a. 在收集器安裝精靈的步驟2中：

      1. 在**類型**下拉清單中，選擇**tcp**連接器類型。您也可以指定**http**連接器類型和其他具有安全傳輸驗證的連接器類型。
      2. 在**URL**欄位中，輸入KUMA收集器將監聽來自KUMA代理程式的連線所使用的FQDN和連接埠號碼。您可以指定任何未佔用的連接埠號碼。
      3. 在**分隔符號**欄位中，輸入\n。

   b. 在收集器安裝精靈的步驟3中，在**標準化器**下拉清單中選擇一個標準化器。我們建議選擇預定義的Windows事件擴充標準化器，**[OOTB] Microsoft DNS ETW日誌json**。

   c. 在收集器安裝精靈的步驟7中，新增一個用於儲存事件的**儲存體**類型目標。如果您打算使用事件關聯，則還需要新增一個**關聯器**類型目標。

   d. 在收集器安裝精靈的步驟8中，按一下**建立並儲存服務** ，然後在視窗下方複製用於在伺服器上安裝KUMA收集器的命令。

3. 在伺服器上安裝KUMA收集器。

   請執行下列操作：

   a. 使用具有根權限的使用者帳戶連線到KUMA命令列介面。

   b. 執行您在收集器安裝精靈的步驟8中複製的命令來安裝KUMA收集器。

c. 如果要將KUMA收集器連接埠新增至防火牆排除項並更新防火牆設定，請執行下列命令：

1. `firewall-cmd --add-port=<collector port number>/tcp --permanent`

2. `firewall-cmd --reload`

KUMA收集器隨即安裝，KUMA主控台中KUMA收集器服務的狀態隨即變更為綠色。

4. 建立KUMA代理程式。

建立KUMA代理程式時，請依照下列步驟操作：

a. 轉至**連線1**頁籤。

b. 在**連接器**下，從**連接器**下拉清單中選擇**建立**，並指定以下設定：

1. 在**類型**下拉清單中，選擇**etw**連接器類型。

2. 在**工作階段名稱**欄位中，輸入您在Windows端使用ETW連接器設定DNS伺服器事件接收時指定的提供者名稱。

c. 在**目標**下，從**目標**下拉清單中選擇**建立**，並指定以下設定：

1. 在**類型**下拉清單中，選擇tcp目標類型。

2. 在**URL**欄位中，輸入KUMA收集器將監聽來自KUMA代理程式的連線所使用的FQDN和連接埠號碼。該值必須與您在收集器安裝精靈的步驟2中指定的值相符。

d. 轉到**進階設定**頁籤，在**磁碟緩衝區大小限制**欄位中輸入1073741824。

5. 建立KUMA代理服務。

您需要複製已建立的KUMA代理服務的ID。為此，請按一下KUMA代理服務，然後在快顯表單中選擇**複製ID**。

6. 為KUMA代理程式建立帳戶。

建立一個網域使用者或本機Windows使用者帳戶，用於執行KUMA代理程式並讀取分析日誌。您需要將建立的使用者帳戶新增至**效能日誌使用者**使用者群組，並授予該使用者帳戶**登入服務**權限。

7. 在Windows伺服器上安裝KUMA代理程式。

您需要在將接收來自提供者的事件的Windows伺服器上安裝KUMA代理程式。為此：

a. 將KUMA Core伺服器的FQDN新增到Windows伺服器上的主機檔案或DNS伺服器中。

b. 在Windows伺服器上建立資料夾C:\Users\<使用者名稱>\桌面\KUMA。

c. 將KUMA安裝套件封存檔案中的kuma.exe檔案複製到資料夾C:\Users\<使用者名稱>\桌面\KUMA。

d. 以管理員身份執行命令解釋器。

e. 切換到資料夾C:\Users\<使用者名稱>\ 桌面\KUMA，並執行以下命令：

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core <FQDN>:7210 --id <agent ID>
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完整網域名稱。
- <agent ID> 是在 OSMP 中建立的代理服務 ID。

在KUMA主控台的**資源 →活動服務**部分，請確保KUMA代理服務正在運作且其狀態為綠色，然後中止該命令。

f. 透過以下方式之一啟動KUMA代理程式安裝：

- 如果要使用網域使用者帳戶啟動KUMA代理程式安裝，請執行以下命令：

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core <FQDN>:7210 --pair.fingerprint <fingerprint ID
of the KUMA Core CA certificate> --id <agent ID> --user <user> --install
```

其中：

- <FQDN> 是 KUMA Core 伺服器的完整網域名稱。
- <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

  您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

  為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。
- <agent ID> 是在 OSMP 中建立的代理服務 ID。
- <user> 是用來執行代理的使用者帳戶名稱，包括網域。

- 如果要使用本機使用者帳戶啟動KUMA代理程式安裝，請執行下列命令：

  `C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core <FQDN>:7210 --pair.fingerprint <KUMA Core CA 憑證的指紋 ID> --id <agent ID> --user <user> --install`

  其中：

  - <FQDN> 是 KUMA Core 伺服器的完整網域名稱。
  - <fingerprint ID of the KUMA Core CA certificate> 是連接服務時用於身分驗證的 CA 憑證指紋 ID。

    `--pair.fingerprint` 參數為選用。建立服務時，OSMP 會自動將此選項新增至安裝命令，並指定指紋 ID。

    您可以在不指定 `--pair.fingerprint` 選項的情況下安裝服務。在此情況下，OSMP 預設使用 `insecure` 值，建立連線時會略過 KUMA Core CA 憑證的驗證。如果值為 `insecure`，則重新簽發 CA 憑證後不需要更新指紋。

    為了確保 KUMA Core CA 憑證得到驗證，建議您在安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。重新簽發 CA 憑證時，您需要從網頁介面複製新的憑證指紋，並使用更新後的指紋 ID 重新啟動服務。

- <agent ID> 是在 OSMP 中建立的代理服務 ID。
- <user> 是用來執行代理的使用者帳戶名稱，包括網域。

您需要輸入KUMA代理程式使用者帳戶的密碼。

KUMA Windows代理服務<KUMA代理服務ID>隨即安裝在Windows伺服器上。在KUMA主控台的**資源 → 活動服務**部分，如果KUMA代理服務未運作且狀態為紅色，則需要確保連接埠7210可用，並且從KUMA代理程式到KUMA收集器的Windows收集器連接埠也可用。

若要從Windows伺服器移除KUMA代理服務，請執行下列命令：

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --id <agent ID> --uninstall
```

其中：

<agent ID> 是在 OSMP 中建立的代理服務 ID。

8. 驗證KUMA收集器接收DNS伺服器事件的情況

   您可以在KUMA主控台的**搜尋相關事件**部分驗證是否已正確設定使用ETW連接器接收DNS伺服器事件。

Windows端的設定

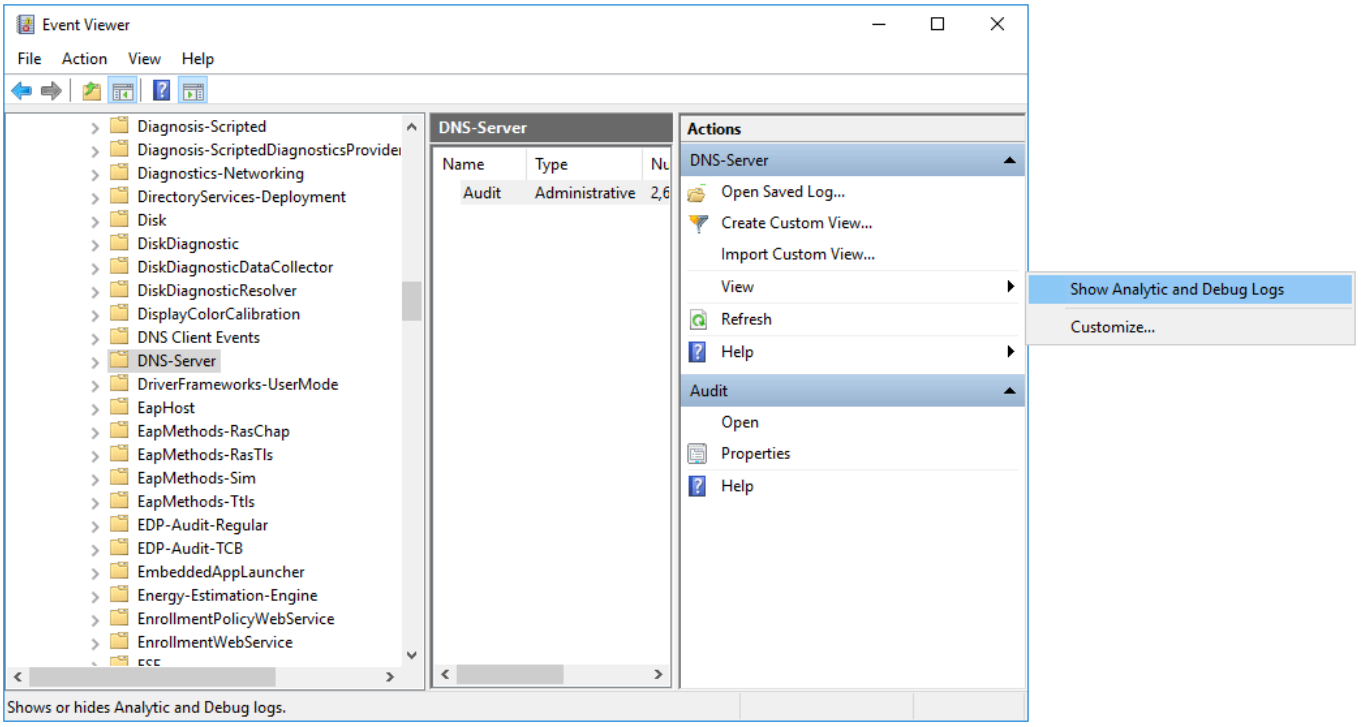
若要在Windows端使用ETW連接器設定DNS伺服器事件接收，請執行下列操作：

1. 執行下列指令啟動事件檢視器：

   eventvwr.msc

2. 在開啟的視窗中，轉至**應用程式與服務日誌→ Microsoft → Windows → DNS伺服器**資料夾。

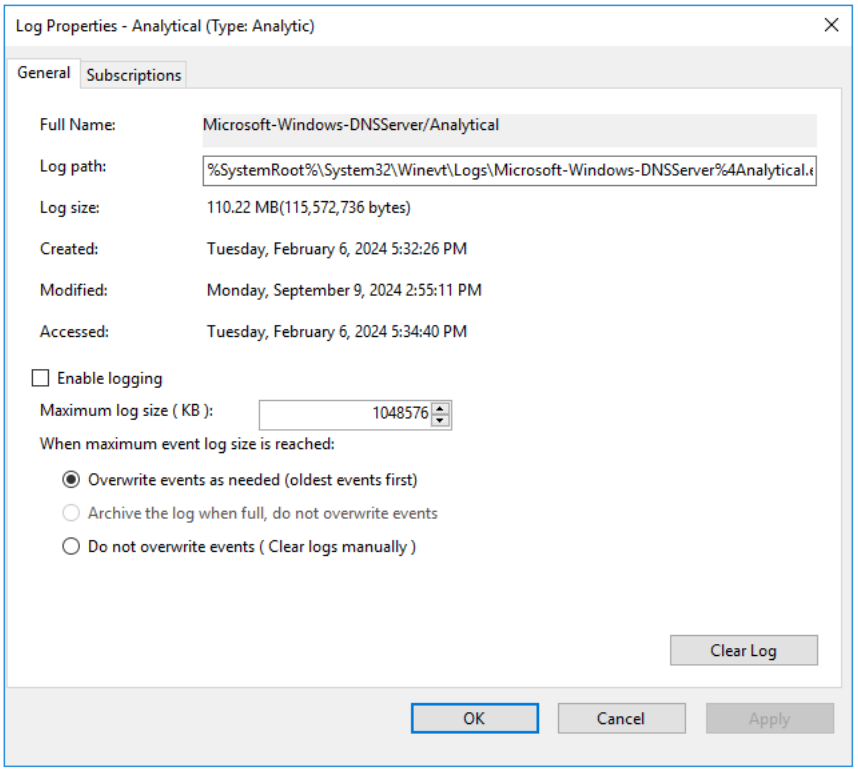
3. 開啟**DNS伺服器**資料夾的快顯表單，然後選擇**檢視 → 顯示分析和偵錯日誌**。



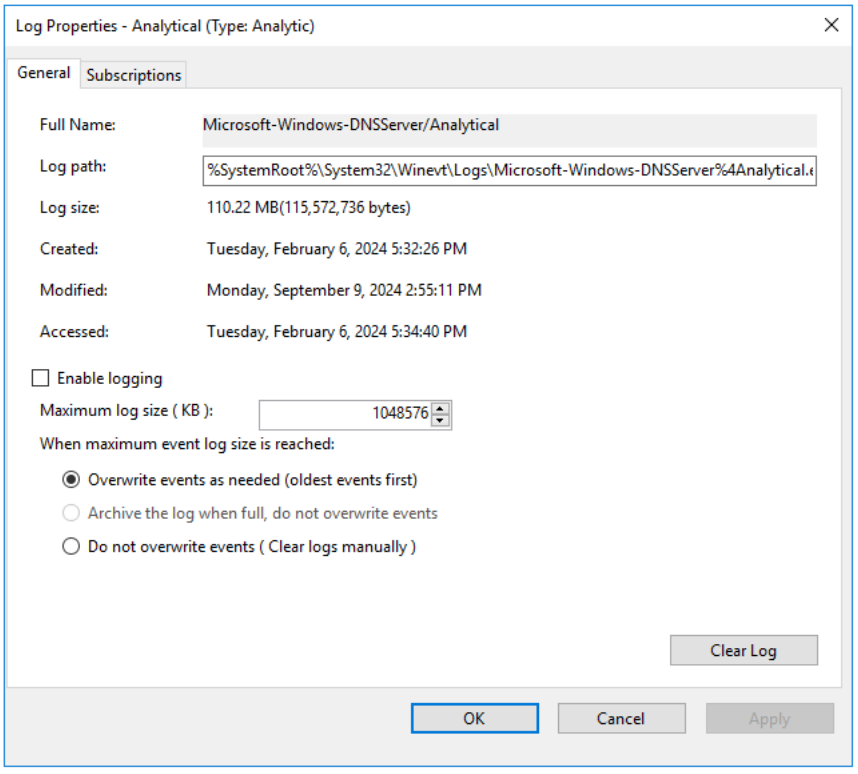
稽核偵錯日誌和**分析**日誌隨即顯示。

4. 設定分析日誌：

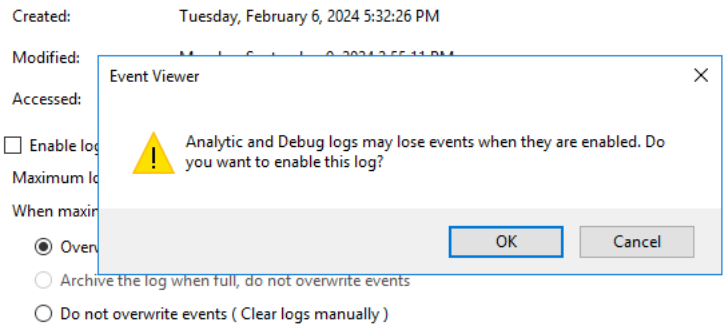
a. 開啟**分析**日誌的快顯表單，然後選擇**內容**。



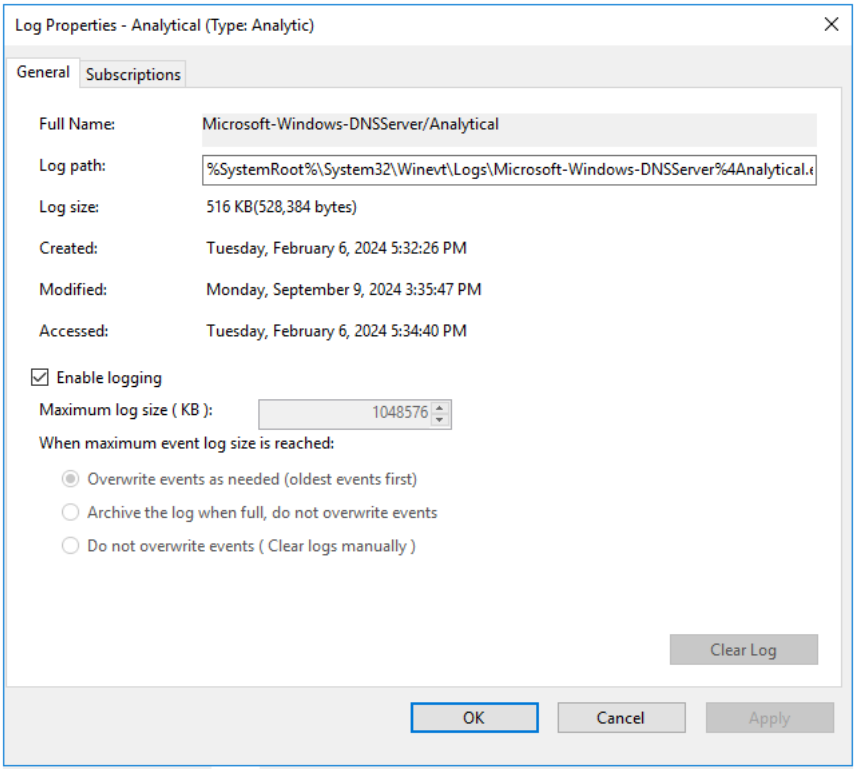
a. 在開啟的視窗中，確保**最大日誌大小（KB）**欄位的值設定為1048576。



a. 選取**啟用日誌記錄**核取方塊，然後在確認視窗中，按一下**確定**。

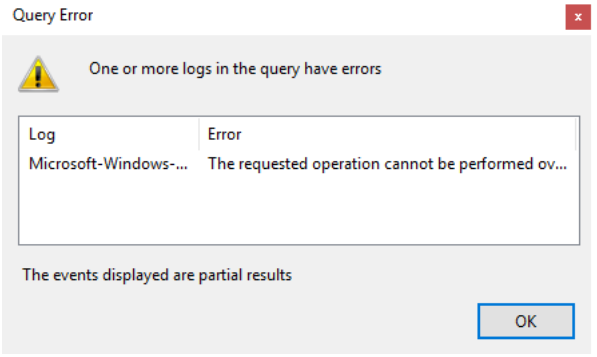


必須如下設定分析日誌：

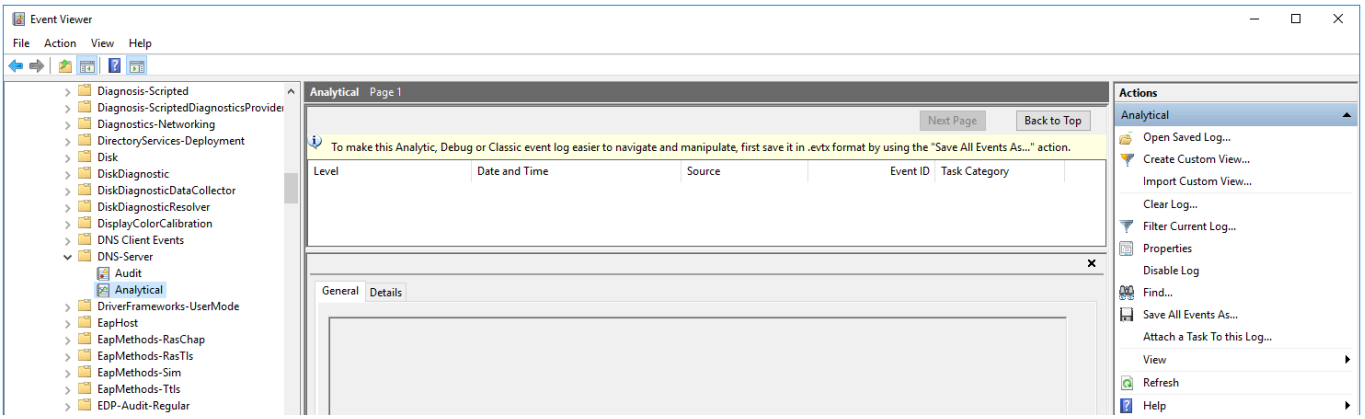


a. 按一下**套用** ，然後按一下**確定**。

錯誤視窗隨即顯示。

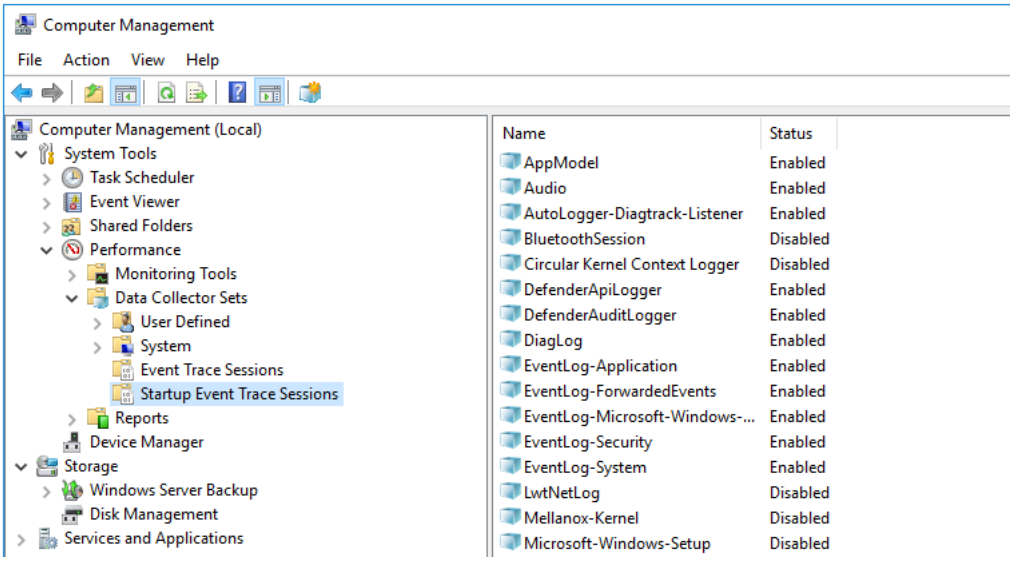


啟用分析日誌輪替後，事件將不會顯示。若要檢視事件，請在**操作**窗格中，按一下**停止日誌記錄**。



5. 以管理員身分啟動電腦管理。

6. 在開啟的視窗中，轉至**系統工具 → 效能 → 啟動事件追蹤會話**資料夾。

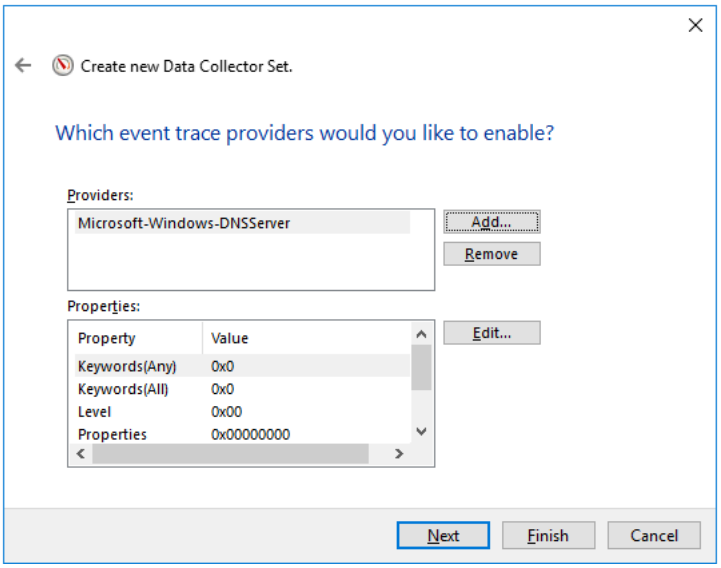


7. 建立提供者：

   a. 開啟**啟動事件追蹤會話**資料夾的快顯表單，然後選擇**建立 → 資料收集器集**。

   b. 這會開啟一個視窗；請在該視窗中輸入提供者名稱，然後按一下**下一步**。

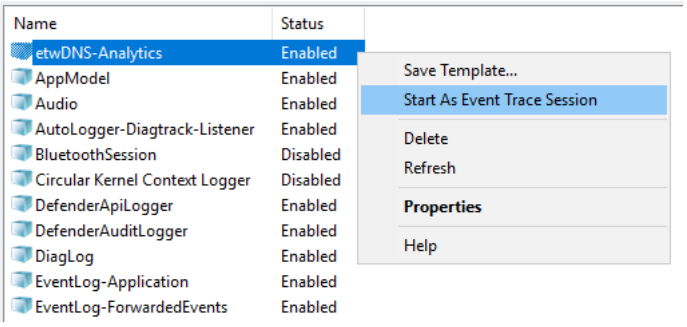
   c. 按一下**新增...**，然後在顯示的視窗中，選擇**Microsoft-Windows-DNSServer**提供者。



具有ETW連接器的KUMA代理程式僅適用於System.Provider.Guid: {EB79061A-A566-4698-9119-3ED2807060E7} - Microsoft-Windows-DNSServer。

a. 按一下**下一步**兩次，然後按一下**完成**。

8. 開啟已建立的提供者的快顯表單，然後選擇**啟動為事件追蹤會話**。

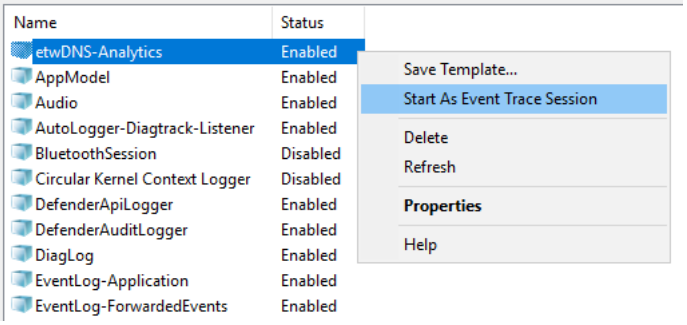


9. 轉至**事件追蹤會話**資料夾。

事件追蹤會話隨即顯示。

10. 開啟已建立的事件追蹤會話的快顯表單，然後選擇**內容**。

11. 這會開啟一個視窗；在該視窗中，選取**追蹤會話**索引標籤，然後在**串流模式**下拉式清單中選取**即時**。



12. 按一下**套用** ，然後按一下**確定**。

使用ETW連接器接收DNS伺服器事件隨即設定。

使用Kaspersky Endpoint Security for Windows設定接收Windows事件

從 Kaspersky Endpoint Security for Windows 12.6 版開始，可以將 Windows 記錄檔中的事件傳送至 KUMA 收集器。如此一來，KUMA 無需在主機上安裝 KUMA 代理，即可從所有安裝 KES for Windows 12.6 的主機取得 Windows 記錄檔中的事件（僅支援一組有限的 Microsoft 產品 EventIDs）。在KES for Windows版本12.6–12.12中，具有相同參數的事件被篩選：僅傳送第一個事件，而後續的類似事件不會傳輸。如果系統產生大量類似事件，其中一些事件仍可能會被傳送。通常必須產生成百上千個此類事件，才會發生這種情況。參數不同的事件（例如，不同使用者登入時）將不受限制地傳輸。篩選邏輯由卡巴斯基專家定義，旨在減少傳輸的事件量，同時不遺失攻擊偵測所需的資料。

若要啟動此功能，您需要：

- 有效的 KUMA 授權
- KSC 14.2或更高版本
- KES for Windows 12.6或更高版本

設定接收事件包含以下步驟：

1. 將標準化器匯入 Kaspersky Next XDR Expert。

   在 Kaspersky Next XDR Expert 中，您必須設定透過卡巴斯基更新伺服器進行更新。

   按一下匯入資源 ，然後在可安裝的標準化器清單中，選擇**[OOTB] Microsoft Products via KES WIN** 。

2. 建立用於接收 Windows 事件的 KUMA 收集器。

   若要接收Windows事件，請在**傳輸**步驟中選擇**TCP**或**UDP**，並指定收集器必須監聽的連接埠號碼。在**事件解析**步驟中，選擇**[OOTB] Microsoft Products via KES WIN**標準化器。在**事件篩選**步驟中，選擇**[OOTB] Microsoft Products via KES WIN -用於收集器的事件篩選器**篩選器。

3. 向 Kaspersky 技術支援申請金鑰。

   如果您的授權不包含用於啟用將 Windows 記錄傳送至 KUMA 收集器之功能的金鑰，請將以下訊息傳送給技術支援：`週三已購買 KUMA 授權，目前使用的是 KES for Windows 12.6 版.我們想要啟用將 Windows 記錄傳送至 KUMA 收集器的功能。請提供金鑰檔案以啟用此功能。` Kaspersky Next XDR Expert 的新使用者不需要向技術支援提出申請，因為新使用者會取得 2 個金鑰，分別用於 KUMA 授權及啟用 KES for Windows 功能。

   收到您的訊息後，您將收到一個金鑰檔案。

4. KSC和KES for Windows端的設定。

   必須將可啟用 Windows 事件傳送至 KUMA 收集器功能的金鑰檔案匯入 KSC，並依照指示散發至 KES 端點。您還必須將 Kaspersky Next XDR Expert 伺服器位址新增至 KES 政策，並指定網路連線設定。

5. 驗證 KUMA 收集器是否收到 Windows 事件

   您可以在 OSMP Console 的搜尋相關事件區段中，確認 Windows 事件來源伺服器是否已正確設定。

   下表列出了KES for Windows傳輸的Microsoft產品事件：

事件日誌	事件ID
DNS伺服器	150
DNS伺服器	770
MSExchange管理	1
安全性	4781
安全性	6416
安全性	1100
安全性	1102 / 517
安全性	1104
安全性	1108
安全性	4610 / 514
安全性	4611
安全性	4614 / 518
安全性	4616 / 520

事件日誌	事件ID
安全性	4622
安全性	4624 / 528 / 540
安全性	4625 / 529
安全性	4648 / 552
安全性	4649
安全性	4662
安全性	4663
安全性	4672 / 576
安全性	4696
安全性	4697 / 601
安全性	4698 / 602
安全性	4702
安全性	4704 / 608
安全性	4706
安全性	4713/617
安全性	4715
安全性	4717 / 621
安全性	4719 / 612
安全性	4720 / 624
安全性	4722 / 626
安全性	4723 / 627
安全性	4724 / 628
安全性	4725 / 629
安全性	4726 / 630
安全性	4727
安全性	4728 / 632
安全性	4729 / 633
安全性	4732 / 636
安全性	4733 / 637
安全性	4738 / 642
安全性	4739/643
安全性	4740 / 644
安全性	4741
安全性	4742 / 646
安全性	4756 / 660
安全性	4757 / 661
安全性	4765
安全性	4766
安全性	4767
安全性	4768 / 672
安全性	4769 / 673

事件日誌	事件ID
安全性	4770
安全性	4771 / 675
安全性	4775
安全性	4776 / 680
安全性	4778 / 682
安全性	4780 / 684
安全性	4794
安全性	4798
安全性	4817
安全性	4876 / 4877
安全性	4882
安全性	4885
安全性	4886
安全性	4887
安全性	4890
安全性	4891
安全性	4898
安全性	4899
安全性	4900
安全性	4902
安全性	4904
安全性	4905
安全性	4928
安全性	4946
安全性	4947
安全性	4948
安全性	4949
安全性	4950
安全性	4964
安全性	5025
安全性	5136
安全性	5137
安全性	5138
安全性	5139
安全性	5141
安全性	5142
安全性	5143
安全性	5144
安全性	5145
安全性	5148
安全性	5155

事件日誌	事件ID
安全性	5376
安全性	5377
安全性	5632
安全性	5888
安全性	5889
安全性	5890
安全性	676
作業系統	1
系統	104
系統	1056
系統	12
系統	13
系統	6011
系統	7040
系統	7045
系統，來源Netlogon	5723
系統，來源Netlogon	5805
終端服務遠端連線管理器	1149
終端服務遠端連線管理器	1152
終端服務遠端連線管理器	20523
終端服務遠端連線管理器	258
終端服務遠端連線管理器	261
Windows PowerShell	400
Windows PowerShell	500
Windows PowerShell	501
Windows PowerShell	800
應用程式，來源ESENT	301
應用程式，來源ESENT	302
應用程式，來源ESENT	325
應用程式，來源ESENT	326
應用程式，來源ESENT	327
應用程式，來源ESENT	2001
應用程式，來源ESENT	2003
應用程式，來源ESENT	2005
應用程式，來源ESENT	2006
應用程式，來源ESENT	216
應用程式	1000
應用程式	1002
應用程式	1 / 2

Codemaster Mirada

您可以在 Kaspersky SIEM (KUMA) 中設定接收 Codemaster Mirada 事件。

設定接收事件包含以下步驟：

1 設定Codemaster Mirada系統的稽核

Codemaster Mirada系統可以透過Syslog協定傳送事件。

1. 使用具有管理員權限的使用者帳戶連線至 Codemaster Mirada 網頁介面。
2. 前往 **設定** → **Syslog** 區段。
3. 使用切換開關啟用事件傳輸服務。
4. 點擊圓圈中的點圖示選擇協定的類型和格式。
5. 在**主機**欄位中，指定KUMA收集器的IP位址。
6. 在**協定**欄位中，指定**UDP**或**TCP**傳輸協定。
7. 對於**連接埠**設定，指定KUMA收集器正在監聽的連接埠。
   預設連接埠為514。
8. 在**格式**欄位中，指定**RFC 3164**標準。
9. 點擊頁面底部的**儲存**按鈕來儲存變更。

2 建立用於接收 Codemaster Mirada 事件的 KUMA 收集器

若要接收 Codemaster Mirada 事件，請在建立收集器時，於**事件解析**步驟選取**[OOTB] Codemaster Mirada syslog**正規化器，並於**傳輸**步驟選取**tcp**或**udp**連接器類型。

3 在網路基礎架構中安裝收集器

設定收集器以接收 Codemaster Mirada 事件後，請在網路基礎架構中用於接收事件的伺服器上安裝 KUMA 收集器。

4 驗證 KUMA 收集器是否收到 Codemaster Mirada 事件

若要驗證 Codemaster Mirada 事件來源伺服器是否已正確設定，您可以在 Kaspersky SIEM (KUMA) 網頁介面中搜尋相關事件。

設定接收Codemaster Mirada事件

Codemaster Mirada系統可以透過Syslog協定傳送事件。

若在Codemaster Mirada系統中設定事件稽核：

1. 使用具有管理員權限的使用者帳戶連線到Codemaster Mirada網頁介面。
2. 前往 **設定** → **Syslog** 區段。
3. 使用切換開關啟用事件傳輸服務。
4. 點擊圓圈中的點圖示選擇協定的類型和格式。
5. 在**主機**欄位中，指定KUMA收集器的IP位址。
6. 在**協定**欄位中，指定**UDP**或**TCP**傳輸協定。
7. 對於**連接埠**設定，指定KUMA收集器正在監聽的連接埠。
   預設埠號為 514。
8. 在**格式**欄位中，指定**RFC 3164**標準。
9. 點擊頁面底部的**儲存**按鈕來儲存變更。

設定接收Postfix事件

您可以在KUMA中設定接收Postfix 事件。僅當使用TCP協定透過syslog傳送事件時，才能進行整合。本文所述資源適用於KUMA 3.0及更高版本。

設定接收事件包含以下步驟：

1. 設定CommuniGate Pro以傳送事件
2. 建立用於接收Postfix事件的KUMA收集器。
3. 驗證KUMA收集器接收Postfix事件的情況
   您可以在KUMA主控台的搜尋相關事件部分驗證Postfix事件來源伺服器是否設定正確。

Postfix系統產生兩種格式的事件：

- 包含訊息資訊（有唯一ID）的多行事件。這些事件的格式如下：
  <syslog PRI> time host process_name: ID：來自基本事件1的資訊

<syslog PRI> time host process_name: ID：來自基本事件2的資訊

- 包含錯誤資訊（不含ID）的單行事件。這些事件的格式如下：

  <syslog PRI> time host process_name: 嚴重等級：用於解析的基本資訊

一組 KUMA 資源用於處理 Postfix 事件；建立收集器時必須套用此資源集：

- 標準化器
- 彙總規則
- 目標篩選器

收集器基於事件ID彙總多行基本事件，對其進行標準化，並將彙總後的事件傳送到儲存體和關聯器。

彙總後的事件的格式如下：

Service information from the aggregation rule: ID: information from base event 1, information from base event 2, information from base event n

彙總後，接收的事件被傳送到同一個收集器，在該收集器中對彙總後的事件進行標準化。

Postfix事件處理演算法

以下演算法用於處理Postfix事件：

1. 初始標準化

   在此階段，對透過syslog接收的以「<」字元開頭的基本事件執行初始標準化。事件轉換為適合後續彙總的格式：從事件中提取第一個字元並放入FlexString1欄位，識別符放入ExternalID欄位，主機名稱放入DeviceHostName欄位。基本標準化在主標準化器中執行。

2. 檢查彙總

   檢查該事件是否屬於彙總事件。因此，對於非彙總事件（第一個字元不是"{"且ID不為空），請套用彙總規則，然後將彙總事件傳送以進行重新標準化。

3. 套用彙總規則

   在此階段，彙總規則套用至事件，基礎事件被整理並採用以下形式：

   來自彙總規則的服務資訊：ID：來自基礎事件1的資訊，來自基礎事件2的資訊，來自基礎事件n的資訊

4. 彙總之後，將整理好的事件傳回同一個收集器，以便將彙總後的事件進行標準化。

   若要閉合事件處理循環，必須將同一個收集器指定為目標。在圖表中，目標被命名為「循環」，以引起人們對事件處理循環的注意。你可以給目標取一個任意名稱。

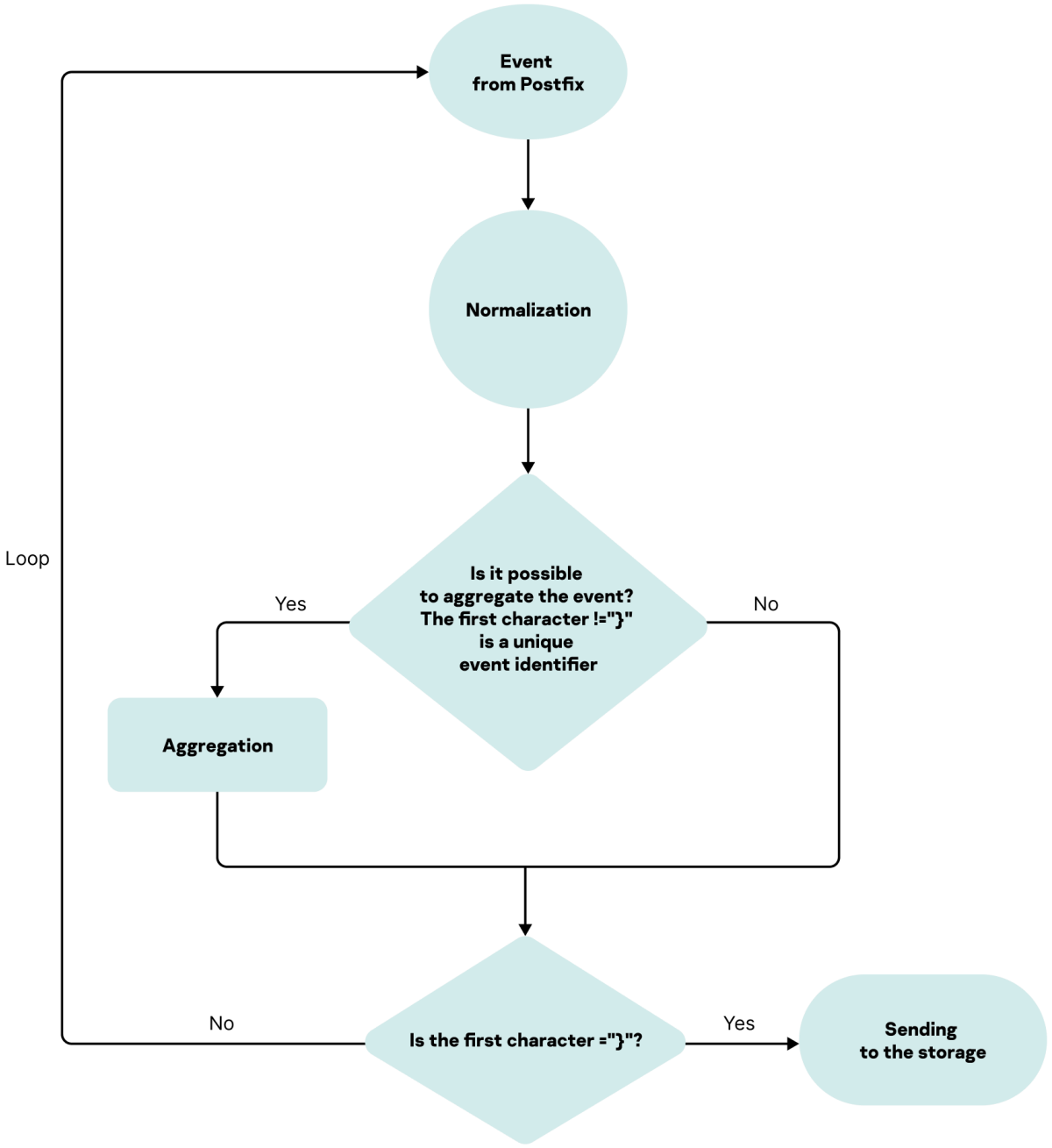
5. 彙總事件的標準化

   將以「{」字元開頭的聚合事件進行標準化，在以下附加的標準化器中執行：彙總事件，彙總事件。訊息鍵值解析器，彙總事件。訊息規則運算式1，彙總事件。訊息規則運算式2。

6. 傳輸到儲存體和關聯器

   彙總和標準化的事件將被傳送到儲存體和關聯器。

下圖顯示了Postfix事件處理的流程圖。



Postfix系統事件處理流程圖

設定Postfix以傳送事件

預設情況下，Postfix系統的稽核事件輸出到/var/log/maillog或/var/log/mail。

若要將事件傳送至KUMA：

1. 建立/etc/rsyslog.conf檔案的備份副本。
2. 開啟檔案/etc/rsyslog.conf進行編輯。

3. 在檔案/etc/rsyslog.conf末尾新增下列行：

   ```
   mail.* @@<IP address of the KUMA collector>:<port of the KUMA collector>
   ```

4. 儲存檔案/etc/rsyslog.conf。

5. 重新啟動rsyslog服務。

   ```
   sudo systemctl restart rsyslog
   ```

設定KUMA收集器以接收和處理Postfix事件

若要設定KUMA收集器以接收Postfix事件：

1. 從KUMA儲存庫匯入[OOTB] Postfix軟體套件。此軟體套件適用於KUMA 3.0及更新版本。

2. 建立一個新的收集器，並在收集器安裝精靈中設定以下內容：

   1. 在**傳輸**步驟中，在**類型**欄位中選擇**tcp**類型，並在**URL**欄位中指定收集器的FQDN或IP位址和連接埠。

   2. 在**事件解析**步驟中，按一下**新增事件解析**，然後在顯示的**基本事件解析**視窗中，從**標準化器**下拉清單中選擇**[OOTB] Postfix syslog**標準化器。

   3. 在**事件彙總**步驟中，按一下**新增彙總**規則，然後在顯示的**事件彙總**視窗中，從**彙總規則**下拉清單中選擇**[OOTB] Postfix。彙總規則**。

   4. 在**路由**步驟中，按一下**新增**，然後在顯示的**建立目的地**視窗中，依序建立三個目標節點：同一個名為 Loop 的收集器、儲存體與關聯器。

      a. 建立名為 Loop 的目標，並設定以下參數。

      - 在**基本設定基本設定類型**下拉清單中，選擇**tcp**傳輸類型；在**URL**欄位中，指定您先前在本說明的步驟2.1中指定的收集器的FQDN或IP位址和連接埠。
      - 在**進階設定**頁籤上的**篩選器**下拉清單中，選擇**Postfix。事件彙總篩選器**篩選器。

        此組態對於將彙總事件傳送到相同收集器以進行後續標準化是必要的。

      b. 建立關聯器目標：

      c. 在**基本設定**頁籤的**類型**下拉清單中，選擇**關聯器**，然後填寫**URL**欄位。

      d. 在**進階設定**頁籤上的**篩選器**下拉清單中，選擇**Postfix。傳送至儲存體和關聯器的彙總事件**。

      e. 建立儲存體目標：

      - 在**基本設定**頁籤的**類型**下拉清單中，選擇**儲存**，然後填寫**URL**欄位。
      - 在**進階設定**頁籤上的**篩選器**下拉清單中，選擇**Postfix。傳送至儲存體和關聯器的彙總事件**。

        此組態對於將彙總的標準化事件傳送到儲存體和關聯器是必要的。

3. 點擊**建立**按鈕。

   收集器服務是根據KUMA主控台中指定的設定建立的。在伺服器上安裝該服務的命令隨即顯示。

4. 複製收集器安裝命令並在相關伺服器上執行。

收集器設定為接收和處理Postfix事件。

設定接收CommuniGate Pro事件

您可以在 KUMA 中設定接收 CommuniGate® Pro 6.1 事件。僅當使用TCP協定透過syslog傳送事件時，才能進行整合。本文所述資源適用於KUMA 3.0及更高版本。現支援處理SIP模組事件（此類事件包含「SIPDATA」字元序列）。

設定接收事件包含以下步驟：

1. 設定CommuniGate Pro以傳送事件
2. 設定KUMA收集器以接收CommuniGate Pro事件
3. 驗證KUMA收集器接收CommuniGate Pro事件的情況

   您可以在KUMA主控台的搜尋相關事件部分驗證CommuniGate Pro事件來源伺服器是否設定正確。

CommuniGate Pro系統會產生一個稽核事件，該事件由多個獨立的記錄組成，如下所示：

```
<event code> timestamp ID direction: information from base event 1

<event code> timestamp ID direction: information from base event 2

<event code> timestamp ID direction: base information n
```

系統會使用一組 KUMA 資源來處理 CommuniGate Pro 事件；建立收集器時必須套用這組資源：

- 標準化器
- 彙總規則
- 目標篩選器

收集器基於事件ID彙總多行基本事件，對其進行標準化，並將彙總後的事件傳送到儲存體和關聯器。

彙總後的事件的格式如下：

```
Service information from the aggregation rule: ID: information from base event 1,
information from base event 2, information from base event n
```

彙總後，接收的事件被傳送到同一個收集器，在該收集器中對彙總後的事件進行標準化。

CommuniGate Pro事件處理演算法

以下演算法用於處理CommuniGate Pro事件：

1. 初始標準化

   在此階段，對基本事件進行初始標準化。基本事件的第一個字元是數字。事件轉換為適合後續彙總的格式：從事件中提取第一個字元並將其放入DeviceCustomString1欄位，將標識符放入ExternalID欄位，並將主機名稱放入DeviceHostName欄位。基本標準化在主標準化器中執行。

2. 檢查彙總

   檢查該事件是否屬於彙總事件。因此，會對非彙總事件（第一個字元是數字）套用彙總規則，然後將彙總後的事件傳送以重新進行標準化。彙總使用**[OOTB] CommuniGate Pro執行。彙總規則**。

3. 套用彙總規則

   在此階段，彙總規則套用至事件，基礎事件被整理並採用以下形式：

   來自彙總規則的服務資訊：ID：來自基礎事件1的資訊，來自基礎事件2的資訊，來自基礎事件n的資訊

   彙總後，整理後的事件被送回同一收集器，以對彙總事件進行標準化。

   若要閉合事件處理循環，必須將同一個收集器指定為目標。在圖表中，目標被命名為「循環」，以引起人們對事件處理循環的注意。你可以給目標取一個任意名稱。

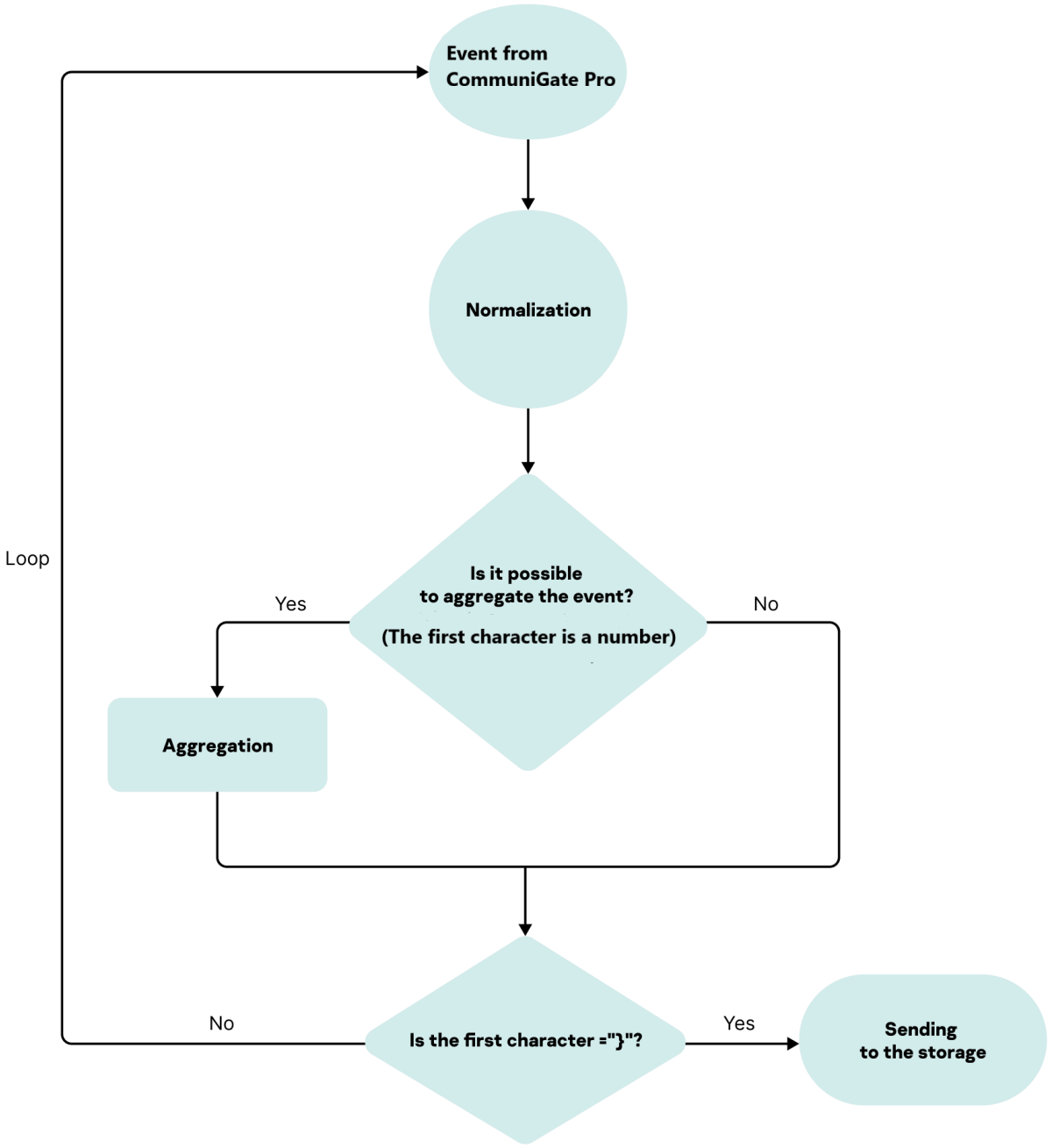
4. 彙總事件的標準化

   以「{」字元開頭的彙總事件的標準化在以下附加的標準化器中執行：聚合事件、聚合事件 - 鍵值部分。

5. 傳輸到儲存體和關聯器

   彙總和標準化的事件將被傳送到儲存體和關聯器。

下圖展示了CommuniGate Pro事件處理流程圖。



CommuniGate Pro 系統事件處理流程圖

設定CommuniGate Pro以傳送事件

預設情況下，CommuniGate Pro稽核事件會傳送到/var/CommuniGate/SystemLogs/目錄中的.log檔案。

若要將事件傳送至KUMA，您需要在CommuniGate Pro伺服器上安裝KUMA代理程式，並將其設定為讀取/var/CommuniGate/SystemLogs/目錄中的.log檔案，並透過TCP將其傳送至KUMA收集器。

若要建立代理程式來讀取事件並將其傳輸到KUMA：

1. 在KUMA主控台中，轉至**資源和服務 → 代理程式**，然後按一下**新增**。
2. 這將開啟**建立代理程式**視窗；在該視窗的**基本設定**頁籤中，在**名稱**欄位中指定代理程式名稱。

3. 在**組態 #1**頁籤中，填寫以下欄位：

   a. 在**基本設定**頁籤的**連接器**設定群組中，為連接器設定以下值：

      1. 在**名稱**欄位中，輸入名稱，例如，`CommuniGate file`。
      2. 在**類型**下拉清單中，選取**檔案**。
      3. 在**檔案路徑**欄位中，輸入以下值：
         /var/CommuniGate/SystemLogs/.*.log

   b. 在**基本設定**頁籤的**目標**設定群組中，為目標設定以下值：

      1. 在**名稱**欄位中，輸入名稱，例如，`CommuniGate TCP collector`。
      2. 在**類型**下拉清單中，選取**tcp**。
      3. 在**URL**欄位中，輸入KUMA收集器的FQDN或IP位址和連接埠。

4. 點擊**建立**按鈕。

5. 在KUMA中建立代理服務時，將代理安裝程式安裝在要從中向收集器傳輸資料的網路基礎設施裝置上。

設定KUMA收集器以接收和處理CommuniGate Pro事件

設定KUMA收集器以接收CommuniGate Pro事件：

1. 從KUMA儲存庫匯入[OOTB] CommuniGate Pro軟體套件。此軟體套件適用於KUMA 3.0及更新版本。

2. 建立一個新的收集器，並在收集器安裝精靈中設定以下內容：

   1. 在**傳輸**步驟中，在**類型**欄位中選擇**tcp**類型，並在**URL**欄位中指定收集器的FQDN或IP位址和連接埠。

   2. 在**事件解析**步驟中，按一下**新增事件解析**，然後在顯示的**基本事件解析**視窗中，在**標準化器**下拉清單中，選擇**[OOTB] CommuniGate Pro**標準化器。

   3. 在**事件彙總**步驟中，按一下**新增彙總規則**，然後在顯示的**事件彙總**視窗中，在**彙總規則**下拉清單中選擇**[OOTB] CommuniGate Pro。彙總規則**。

   4. 在**路由**步驟中，按一下**新增**，然後在顯示的**建立目的地**視窗中，依序建立三個目標節點：同一個名為 Loop 的收集器、儲存體與關聯器。

      a. 建立名為 Loop 的目標，並設定以下參數。

      - 在**基本設定**頁籤上的**類型**下拉清單中，選擇**tcp**傳輸類型；在**URL**欄位中，指定您先前在本說明的步驟2.1中指定的收集器的FQDN或IP位址和連接埠。
      - 在**進階設定**頁籤上的**篩選器**下拉清單中，選擇**[OOTB] CommuniGate Pro。事件彙總篩選器**篩選器。

      此組態對於將彙總事件傳送到相同收集器以進行後續標準化是必要的。

b. 建立關聯器目標：

- 在**基本設定**頁籤的**類型**下拉清單中，選擇**關聯器**，然後填寫**URL**欄位。
- 在**進階設定**頁籤上的**篩選器**下拉清單中，選擇**[OOTB] CommuniGate Pro。傳送至儲存體和關聯器的彙總事件**。

c. 建立儲存體目標：

- 在**基本設定**頁籤的**類型**下拉清單中，選擇**儲存**，然後填寫**URL**欄位。
- 在**進階設定**頁籤上的**篩選器**下拉清單中，選擇**[OOTB] CommuniGate Pro。傳送至儲存體和關聯器的彙總事件**。

此組態對於將彙總的標準化事件傳送到儲存體和關聯器是必要的。

3. 點擊**建立**按鈕。
   收集器服務是根據KUMA主控台中指定的設定建立的。在伺服器上安裝該服務的命令隨即顯示。
4. 複製收集器安裝命令並在相關伺服器上執行。

用於接收和處理CommuniGate Pro事件的收集器隨即設定。

設定接收Yandex Cloud事件

您可以在KUMA中設定接收Yandex Cloud事件。標準化器支援處理儲存在.json檔案中的組態層級稽核事件。

設定接收事件包含以下步驟：

1. 設定稽核Yandex Cloud事件。
2. 設定匯出Yandex Cloud事件。
3. 設定KUMA收集器以接收和處理Yandex Cloud事件。
   若要在KUMA收集器安裝精靈中接收Yandex Cloud事件：
   1. 在KUMA收集器安裝精靈的**傳輸**步驟中，選擇**檔案**類型的連接器。
   2. 在**URL**欄位中，輸入`/var/log/yandex-cloud/<audit_trail_id>/*/*/*/*.json`，其中<audit_trail_id>是稽核的 ID。
   3. 在**事件解析**步驟中，在**標準化器**欄位中，選擇**[OOTB] Yandex Cloud**。
4. 在KUMA網路基礎架構中安裝收集器。
5. 驗證KUMA收集器接收Yandex Cloud事件的情況
   若要驗證Yandex Cloud事件來源伺服器是否設定正確，您可以搜尋相關事件。

設定稽核Yandex Cloud事件

設定事件匯出分階段進行：

1. 準備使用Yandex Cloud的環境。
2. 建立稽核日誌儲存桶。
3. 在金鑰管理服務中建立加密金鑰。
4. 啟用儲存桶加密。
5. 建立服務帳戶。
6. 建立靜態金鑰。
7. 為服務帳戶指派角色。
8. 建立稽核追蹤。

準備使用Yandex Cloud的環境。

若要管理組態，您需要Yandex Cloud CLI；請安裝並初始化它。

注意：依預設，稽核作業將於 CLI 設定檔中指定的 Yandex Cloud 資料夾內執行。您可以使用 `--folder-name` 或 `--folder-id` 參數指定不同的資料夾。

若要設定稽核功能，您需要一個活動的計費帳戶，因為使用Yandex Cloud基礎設施需要付費。

若要設定Yandex Cloud稽核功能，您需要一個活動的計費帳戶：

1. 轉至管理主控台，然後登入Yandex Cloud或註冊。
2. 在Yandex Cloud計費頁面上，請確保您已連接計費帳戶，且該帳戶處於「活動」或「試用活動」狀態。如果您還沒有計費帳戶，請建立一個。

如果您有活動的計費帳戶，可以在雲端頁面上建立或選擇基礎設施運作所在的Yandex Cloud 資料夾。

為稽核日誌建立儲存桶

若要建立儲存桶：

1. 在管理主控台中，轉至要建立儲存桶的資料夾，例如**example-folder**。
2. 選擇**物件儲存**服務。
3. 點擊**建立儲存桶**。

4. 在儲存桶建立頁面上：
    1. 根據命名規則輸入儲存桶名稱。例如**kumabucket**。
    2. 根據需要，可限制儲存桶的最大大小。大小為0表示無限制，相當於啟用了**無限制**選項。
    3. 在存取類型中，選擇**受限**。
    4. 選擇預設儲存類別。
    5. 點擊**建立儲存桶**。

    儲存桶隨即建立。

在「金鑰管理服務」中建立加密金鑰

若要建立加密金鑰：

1. 在管理主控台中，轉到**example-folder**資料夾。
2. 選擇**金鑰管理服務**。
3. 按一下**建立金鑰**按鈕，並指定以下設定：
    - 名稱（例如，**kuma-kms**）。
    - 加密演算法，**AES-256**。
    - 其餘設定保留預設值。
4. 點擊**建立**按鈕。

    加密金鑰隨即建立。

啟用儲存桶加密

若要啟用儲存桶加密：

1. 在管理主控台中，轉到您之前建立的儲存桶。
2. 在左方窗格中，選取**加密**。
3. 在**KMS金鑰**欄位中，選擇**kuma-kms**金鑰。
4. 按一下**儲存**按鈕。

    儲存桶加密隨即啟用。

建立服務帳戶

若要建立服務帳戶（追蹤帳戶和儲存桶帳戶各一個）：

1. 建立**sa-kuma**服務帳戶：
    1. 在管理主控台中，轉至**example-folder**資料夾。
    2. 在螢幕上方，轉至**服務帳戶**頁籤。
    3. 按一下**建立服務帳戶**，然後輸入服務帳戶的名稱，例如**sa-kuma**，並確保名稱符合以下命名規則：
        - 長度：3到63個字符
        - 可以包含小寫拉丁字母、數字和連字號
        - 第一個字元必須是字母，最後一個字元不能是連字號
    4. 點擊**建立**按鈕。
2. 建立**sa-kuma-bucket**服務帳戶：
    1. 在管理主控台中，轉至**example-folder**資料夾。
    2. 在螢幕上方，轉至**服務帳戶**頁籤。
    3. 按一下**建立服務帳戶**，然後輸入服務帳戶的名稱，例如**sa-kuma-bucket**，並確保名稱符合以下命名規則：
        - 長度：3到63個字符
        - 可以包含小寫拉丁字母、數字和連字號
        - 第一個字元必須是字母，最後一個字元不能是連字號
    4. 點擊**建立**按鈕。

服務帳戶隨即建立。

建立靜態金鑰

掛載儲存桶時，您需要金鑰ID和私鑰。您可以使用管理主控台或CLI建立金鑰。

若要使用管理主控台建立金鑰：

1. 在管理主控台中，轉到**example-folder**資料夾。
2. 在螢幕上方，轉至**服務帳戶**頁籤。
3. 選擇**sa-kuma-bucket**服務帳戶，然後按一下其名稱所在的行。

4. 在頂部窗格中，按一下**新建金鑰**。

5. 選擇**建立靜態存取金鑰**。

6. 輸入金鑰描述，然後按一下**建立**。

7. 儲存ID和密鑰。

靜態存取金鑰隨即建立。關閉對話框後，金鑰值將不可用。

若要使用CLI建立金鑰：

1. 為**sa-kuma-bucket**服務帳戶建立存取金鑰：

```
yc iam access-key create --service-account-name sa-kuma-bucket
```

結果：

```
access_key:
id: aje*******k2u
service_account_id: aje******usm
created_at: "2022-09-22T14:37:51Z"
key_id: 0n8*******0YQ
secret: JyT*******zMP1
```

2. 儲存key_id和「secret」值中的金鑰。您將無法再次取得金鑰值。

存取金鑰隨即建立。

為服務帳戶指派角色

若要將audit-trails.viewer、storage.uploader和kms.keys.encrypterDecrypter角色指派給sa-kuma服務帳戶：

1. 在CLI中，將audit-trails.viewer角色指派給資料夾：

```
yc resource-manager folder add-access-binding \
--role audit-trails.viewer \
--id <folder_id> \
--service-account-id <service_account_id>
```

其中：

- `--role` 是指派的角色。
- `--id` 是 'example-folder' 資料夾的 ID。
- `--service-account-id` 是 sa-kuma 服務帳戶的 ID。

2. 將storage.uploader角色指派給具有儲存桶的資料夾：

```
yc resource-manager folder add-access-binding \
--role storage.uploader \
--id <folder_id> \
```

```
--service-account-id <service_account_id>
```

其中：

- `--role` 是指派的角色。
- `--id` 是 'example-folder' 資料夾的 ID。
- `--service-account-id` 是 sa-kuma 服務帳戶的 ID。

3. 將kms.keys.encrypterDecrypter角色指派給kuma-kms加密金鑰：

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

其中：

- `--role` 是指派的角色。
- `--id` 是 kuma-kms KMS 金鑰的 ID。
- `--service-account-id` 是 sa-kuma 服務帳戶的 ID。

若要將storage.viewer和kms.keys.encrypterDecrypter角色指派給sa-kuma-bucket服務帳戶：

1. 在CLI中，將storage.viewer角色指派給該資料夾：

```
yc resource-manager folder add-access-binding \
--id <folder_id> \
--role storage.viewer \
--service-account-id <service_account_id>
```

其中：

- `--id` 是 'example-folder' 資料夾的 ID。
- `--role` 是指派的角色。
- `--service-account-id` 是 sa-kuma-bucket 服務帳戶的 ID。

2. 將kms.keys.encrypterDecrypter角色指派給kuma-kms加密金鑰：

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

其中：

- `--role` 是指派的角色。
- `--id` 是 kuma-kms KMS 金鑰的 ID。
- `--service-account-id` 是 sa-kuma-bucket 服務帳戶的 ID。

建立稽核追蹤

若要建立稽核追蹤：

1. 在管理主控台中，轉到**example-folder**資料夾。
2. 選擇**稽核追蹤**服務。
3. 按一下**建立追蹤**，並指定要建立的追蹤的名稱，例如**kuma-trail**。
4. 在**目標**部分，指定目標物件的參數：
   - **目標**：**物件儲存體**。
   - **儲存桶**：儲存桶的名稱，例如**kumabucket** 。
   - **物件前綴**：稽核日誌檔全名中使用的可選參數。

     如果將稽核日誌和協力廠商資料儲存在同一個儲存桶中，請使用前綴。不要對儲存桶中的日誌和其他物件使用相同的前綴，因為這可能會導致日誌和協力廠商物件相互覆蓋。
   - **加密金鑰**：指定用於加密儲存桶的kuma-kms加密金鑰。
5. 在**服務帳戶**部分，選擇**sa-kuma**。
6. 在**收集管理事件**部分，指定用於收集稽核事件日誌的設定：
   - **收集事件**：選擇**啟用**。
   - **資源**：選擇**資料夾**。
   - **資料夾**：無須填寫，其中包含目前資料夾的名稱。
7. 在**收集資料事件**的**收集事件**欄位中，選擇**停用**。
8. 點擊**建立**按鈕。

設定匯出Yandex Cloud事件

儲存桶必須掛載到將要安裝KUMA收集器的伺服器上。

若要掛載儲存桶：

1. 在伺服器上，為「kuma」使用者建立目錄：

   ```
   sudo mkdir /home/kuma
   ```
2. 在伺服器上，建立一個具有sa-kuma-bucket服務帳戶靜態存取金鑰的檔案，並授予「kuma」使用者對應的存取權限：

   ```
   sudo bash -c 'echo <access_key_ID>:<secret_access_key> > /home/kuma/.passwd-s3fs'
   sudo chmod 600 /home/kuma/.passwd-s3fs
   sudo chown -R kuma:kuma /home/kuma
   ```

3. 安裝s3fs軟體套件：

   ```
   sudo apt install s3fs
   ```

4. 建立目錄，用於掛載儲存桶，並授予kuma使用者權限：

   ```
   sudo mkdir /var/log/yandex-cloud/
   sudo chown kuma:kuma /var/log/yandex-cloud/
   ```

5. 掛載儲存桶：

   ```
   sudo s3fs kumabucket /var/log/yandex-cloud -o passwd_file=/home/kuma/.passwd-s3fs -o url=https://storage.yandexcloud.net -o use_path_request_style -o uid=$(id -u kuma) -o gid=$(id -g kuma)
   ```

   您可以透過向/etc/fstab新增一行來設定要在作業系統啟動時安裝的儲存桶，例如：

   ```
   s3fs#kumabucket /var/log/yandex-cloud fuse _netdev,uid=<kuma_uid>,gid=<kuma_gid>,use_path_request_style,url=https://storage.yandexcloud.net,passwd_file=/home s3fs 0 0
   ```

   其中：

   <kuma_uid>是作業系統中kuma使用者的ID。

   <kuma_gid>是作業系統中kuma使用者群組的ID。

   若要找尋kuma_uid和kuma_gid，請在主控台中執行以下命令：

   ```
   id kuma
   ```

6. 驗證儲存桶是否已掛載：

   ```
   sudo ls /var/log/yandex-cloud/
   ```

   如果一切設定正確，則該命令將傳回<audit_trail_id>，其中<audit_trail_id>是稽核追蹤ID。

Yandex Cloud事件匯出隨即設定。事件將以.json檔案的形式儲存在目錄中：

/var/log/yandex-cloud/{audit_trail_id}/{year}/{month}/{day}/*.json

設定接收Microsoft 365事件

您可以在 KUMA 中設定接收來自 Microsoft 365 (Office 365®) 雲端解決方案的事件。

設定接收事件包含以下步驟：

1. 使用標準 Microsoft 方法設定存取 Office 365 管理 API https://learn.microsoft.com/en-us/office/office-365-management-api/get-started-with-office-365-management-apis 。

   若要在KUMA中接收事件，請授予必要的API權限：

   Microsoft.Graph

   Directory.Read.All

   Office 365管理API

   ActivityFeed.Read

   ActivityFeed.Read.Dlp

2. 建立KUMA收集器。

若要接收Microsoft 365事件，請使用下列參數建立收集器：

- 在**傳輸**步驟中，指定**office365**連接器類型。
- 在**解析事件**步驟中，指定**[OOTB] Microsoft Office 365 JSON**標準化器。

3. 在KUMA網路基礎架構中安裝收集器
4. 驗證KUMA收集器接收Windows Microsoft 365事件的情況

   若要驗證Microsoft 365事件來源伺服器是否設定正確，您可以搜尋相關事件。

設定接收Kontinent加密系統事件

Kaspersky Next XDR Expert 安裝套件包含 kuma-kont 公用程式，該公用程式由一個可執行檔和一個組態檔組成。支援的作業系統包括Astra Linux、 Ubuntu 22.04 LTS以及RED OS 7.3和8。此公用程式可讓您連線至 MSSQL 資料庫、接收 Kontinent 加密系統事件，並以 JSON 格式將資料傳送至 KUMA 收集器。Kontinent 3.9.2支援資料導入。

設定從 MSSQL 資料庫擷取 Kontinent 事件並將其傳送至 KUMA 收集器，涉及以下步驟：

1. 準備接收Kontinent事件。

   在此步驟中，您需要建立一個將接收事件的KUMA收集器，還需要在MSSQL資料庫中建立一個使用者。

2. 設定kuma-kont公用程式。

   在此步驟中，您需要建立公用程式及其服務的組態檔。

3. 啟動kuma-kont公用程式。

   啟動後，公用程式會開始從 MS SQL 資料庫匯出事件，並將其傳送至 KUMA 收集器。它會在kuma-kont.log檔案中保留日誌。

準備接收Kontinent事件

1. 建立KUMA收集器。

   1. 建立用於接收Kontinent 3.9事件的KUMA收集器。

      若要使用收集器安裝精靈接收Kontinent 3.9系統的稽核事件，請在**事件解析**步驟中選擇**[OOTB] SecurityCode Continent 3.9 json**標準化器。此外，在**傳輸**頁籤上，您需要根據*設定Kontinent 3.9事件匯出*說明的第2.1.4段指定連接埠和協定。

   2. 在 Kaspersky Next XDR Expert 網路基礎架構中安裝收集器。

2. 在MS SQL DBMS中建立帳戶

   在資料庫中建立帳戶，並賦予其連接和讀取以下表資料的最低必要權限：ALERTLOG、SERVERACCESSLOG、SYSTEMLOG、PACKETLOG、FILTERS。

3. 確保網路連線。

   您必須確保執行公用程式的伺服器與 Kontinent 系統資料庫伺服器之間，以及執行公用程式的伺服器與 KUMA 收集器伺服器之間的網路連線。

設定kuma-kont公用程式

設定kuma-kont公用程式涉及以下步驟：

1. 建立kuma-kont-config.yaml組態檔。
2. 創建kuma-kont服務。

建立kuma-kont-config.yaml組態檔

若要建立kuma-kont-config.yaml組態檔：

1. 執行以下命令，前往 Kaspersky Next XDR Expert 安裝程式目錄：
   `cd kuma-ansible-installer/roles/kuma/files`
2. 解壓縮kuma-kont.tar封存檔案：
   `tar -xvf kuma-kont.tar`
3. 轉至此公用程式的目錄：
   `cd kuma-kont`
4. 複製kuma-ptvm-config-template.yaml範本來建立名為kuma-ptvm-config.yaml的組態檔：
   `cp kuma-kont-config-template.yaml kuma-kont-config.yaml`
5. 變更設定檔的讀取權限：
   `sudo chown <使用者名稱>:<群組> kuma-kont-config.yaml`
   `sudo chmod 600 kuma-kont-config.yaml`
   將<使用者名稱>替換為服務將使用的作業系統使用者名稱。
6. 編輯kuma-kont-config.yaml組態檔中的設定。
   指定以下參數的值：
   - 一般設定：state_file、log_file_path。
   - Kontinent資料庫：名稱、使用者、密碼、主機、連接埠。
   - KUMA 收集器：位址、連接埠、通訊協定。
     kuma-kont-config-template.yaml檔案中提供了一個組態範例。
7. 將變更儲存到檔案。

組態檔隨即建立。

建立服務

若要創建kuma-kont服務：

1. 更改可執行檔的執行權限：

   ```
   sudo chown <使用者名稱>:<群組> <可執行檔路徑>
   sudo chmod 700 <可執行檔路徑>
   ```

2. 建立包含以下內容的/etc/systemd/system/kuma-kont.service檔案：

   ```
   [Unit]
   Description=Connector Kontinent 3.9
   After=network.target
   [Service]
   User=<使用者名稱>
   ExecStart=<可執行檔路徑> --config <組態檔路徑>
   Restart=always
   RestartSec=10
   [Install]
   WantedBy=multi-user.target
   ```

   將<使用者名稱>替換為服務將使用的作業系統使用者名稱。

3. 指定可執行檔的路徑。

   在ExecStart欄位中指定kuma-kont可執行檔的路徑。

   例如，如果kuma-kont檔案位於/usr/bin/目錄中，則保留預設值。

4. 指定組態檔的路徑。

   在ExecStart欄位中指定kuma-kont-config.yaml組態檔的路徑。例如，如果kuma-kont-config.yaml檔案位於/path/to/目錄中，則指定此路徑。

   kuma-kont.service檔案範例

   ```
   [Unit]
   Description=Continent Service
   After=network.target
   [Service]
   User=user-example
   ExecStart=./usr/bin/kuma-kont --config /path/to/kuma-kont-config.yaml
   Restart=always
   RestartSec=10
   [Install]
   WantedBy=multi-user.target
   ```

5. 載入systemd組態：

   ```
   sudo systemctl daemon-reload
   ```

6. 讓服務在啟動時運作：

   ```
   sudo systemctl enable kuma-kont
   ```

kuma-kont公用程式將在系統啟動時作為服務啟動。

啟動和管理kuma-kont服務

若要啟動該公用程式服務，請執行以下命令：

```
sudo systemctl start kuma-kont
```

開始從 MSSQL 資料庫收集事件，並將事件傳送至 KUMA 收集器。

可以使用以下命令控制該公用程式服務：

1. 啟動kuma-kont服務：
   ```
   sudo systemctl start kuma-kont
   ```
2. 停止kuma-kont服務：
   ```
   sudo systemctl stop kuma-kont
   ```
3. 重新啟動kuma-kont服務：
   ```
   sudo systemctl restart kuma-kont
   ```

您也可以使用以應用程式形式執行的KUMA-kont公用程式傳送事件。若要開始將事件傳送至KUMA收集器，您需要在可執行檔所在的目錄中執行以下命令：

```
./kuma-kont --config < kuma-kont-config.yaml 檔案的路徑 >
```

連線中斷時的行為

與MSSQL資料庫的連線。

如果與MSSQL資料庫的連接中斷，則該公用程式會嘗試每隔n秒（其中n等於組態檔中poll_interval設定的值）重新連線，直至連線恢復。

與KUMA收集器的連線

如果使用TCP通訊協定傳送事件，當與KUMA收集器的連線中斷時，該公用程式也會嘗試恢復連線。連線嘗試之間的間隔會增加，直至達到一小時，之後每小時嘗試重新連線一次。

已知限制

來自 `AlertLog` 資料表且 AL_CATEGORY=5 的事件尚未完全解碼。

kuma-kont-config.yaml組態檔中的設定

下表列出了您可以在kuma-kont-config.yaml檔案中指定的設定。

設定	描述
`debug`	**一般設定**群組中的可選設定。 需要偵測等級日誌輸出時使用。 如果為false，則僅包含啟動和停止訊息，以及在傳送過程中發生的錯誤訊息。 可用值： • **true** • **false** 預設設定：**false**。
`need_reconnect`	**一般設定**群組中的可選設定。 此設定決定公用程式是否重新連線到資料庫來發出每個請求。 可用值： • **true** • **false** 預設設定：**false**。
`state_file`	**一般設定**群組中的必填設定。 儲存已處理日誌狀態的JSON檔案的絕對路徑。 該檔案將自動在此路徑建立。 請確保使用者擁有足夠的權限來寫入此目錄。 例如：/home/user/kuma-kont/state.json
`log_file_path`	**一般設定**群組中的必填設定。 用於記錄連接器活動的日誌檔案的絕對路徑。 該檔案將自動在此路徑建立。 請確保使用者擁有足夠的權限來寫入此目錄。 例如：/home/user/kuma-kont/kuma-kont.log
`poll_interval`	**一般設定**群組中的可選設定。 資料庫輪詢間隔。 預設設定為10秒。 對於高EPS，我們建議將值設為小於15秒。
`name`	**Kontinent資料庫**群組中的必填設定。 接收Kontinent日誌的資料庫名稱。
`user`	**Kontinent資料庫**群組中的必填設定。 資料庫使用者的名稱。
`password`	**Kontinent資料庫**群組中的必填設定。 資料庫使用者的密碼。
`host`	**Kontinent資料庫**群組中的必填設定。 資料庫伺服器的URL。
`port`	**Kontinent資料庫**群組中的必填設定。 資料庫伺服器的連接埠。 請確保可以從安裝了該公用程式的伺服器存取它。
`limit`	**Kontinent資料庫**群組中的可選設定。 限制每次輪詢可從資料庫下載的事件數量。 預設值為每次資料庫輪詢100,000個事件。 如果EPS較高，建議使用等於或大於此值。
`alert_log`	**上次ID**群組中的可選設定。 指定要從哪個 AlertLog 類型的事件開始將事件傳送至 KUMA 收集器。 僅在首次執行時或狀態檔案不存在時生效。 預設值是 0。
`packet_log`	**上次ID**群組中的可選設定。 指定要從哪個 PacketLog 類型的事件開始將事件傳送至 KUMA 收集器。 僅在首次執行時或狀態檔案不存在時生效。 預設值是 0。

設定	描述
server_access_log	**上次ID**群組中的可選設定。 指定要從哪個 ServerAccessLog 類型的事件開始將事件傳送至 KUMA 收集器。 僅在首次執行時或狀態檔案不存在時生效。 預設值是 0。
system_log	**上次ID**群組中的可選設定。 指定要從哪個 SystemLog 類型的事件開始將事件傳送至 KUMA 收集器。 僅在首次執行時或狀態檔案不存在時生效。 預設值是 0。
address	**KUMA 收集器**群組中的必要設定。 安裝 KUMA 收集器之伺服器的完整網域名稱 (FQDN) 或 IP 位址。
port	**KUMA 收集器**群組中的必要設定。 KUMA 收集器的連接埠。
protocol	**KUMA 收集器**群組中的必要設定。 KUMA 收集器使用的資料傳輸協定。 如果使用 udp 通訊協定，當與 KUMA 收集器的連線中斷時，事件不會重新傳送。 可用值： • **tcp** • **udp**

與其他解決方案整合

在本章節中，您將了解如何將KUMA與其他解決方案整合以擴充其功能。

與卡巴斯基安全管理中心整合

您可以在OSMP主控台中建立或編輯卡巴斯基安全中心整合設定。

在OSMP主控台中，您可以檢視一個、多個或所有KUMA租用戶與選取卡巴斯基安全管理中心伺服器的整合。如果啟用了與卡巴斯基安全中心的整合，您可以手動匯入資產、編輯自動排程匯入間隔或暫時停用排程匯入。

設定卡巴斯基安全管理中心資產的資料重新整理間隔

KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

- 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
- 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

若要設定卡巴斯基安全管理中心資產的資料重新整理間隔:

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要匯入KSC資產資訊的租用戶。

   這會開啟租用戶內容視窗。
3. 在**設定**頁籤的**偵測與回應**下，按一下**資產設定**。
4. 在**KSC匯入**頁籤中，確保**狀態**切換開關已開啟。
5. 指定從卡巴斯基安全管理中心自動匯入資產資訊和資產弱點資訊的間隔：

   - 在**硬體資訊**下的**匯入間隔（小時）**欄位中，輸入自動匯入資產基本屬性資訊的間隔時間（以小時為單位）。預設設定為1小時。
   - 在**資產屬性**下的**導入間隔（小時）**欄位中，輸入自動導入其他資產屬性資訊的間隔時間（以小時為單位）。預設設定為12小時。

     匯入資產屬性（弱點、軟體、所有者）資訊可能需要下載大量資料，耗時較長，因此建議設定比硬體資訊匯入更長的間隔時間。
6. 按一下**儲存**按鈕。

所選租用戶的卡巴斯基安全管理中心資產的資料重新整理設定即會配置。

如果您所需的租用戶未在租用戶清單中，請使用OSMP主控台將其新增至租用戶清單。

排程匯入卡巴斯基安全管理中心資產

若要設定匯入卡巴斯基安全管理中心資產的排程：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**卡巴斯基安全管理中心**。

   卡巴斯基安全管理中心整合視窗隨即開啟。
3. 選擇您要安排匯入卡巴斯基安全管理中心資產的租用戶。

   卡巴斯基安全管理中心整合視窗隨即開啟。
4. 如有必要，請取消選取**已停用**核取方塊，以啟用所選租用戶與卡巴斯基安全管理中心的整合。預設情況下，此核取方塊已清除。

   若要暫時停用所選租用戶與卡巴斯基安全管理中心的整合，請選取**已停用**核取方塊。這將關閉卡巴斯基安全管理中心資產的排程匯入。
5. 在**資料重新整理間隔**欄位中，指定 KUMA 更新卡巴斯基安全管理中心裝置資料的時間間隔。

   間隔以小時為單位，且必須為整數。

預設時間間隔為12小時。

6. 按一下**儲存**按鈕。

為所選租用戶排程匯入卡巴斯基安全管理中心資產的指定設定隨即套用。

手動匯入卡巴斯基安全管理中心資產

KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

- 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
- 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

若要手動匯入卡巴斯基安全管理中心資產：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要匯入KSC資產資訊的租用戶。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤的**偵測與回應**下，按一下**資產設定**。
4. 在**KSC匯入**頁籤中，確保**狀態**切換開關已開啟。
5. 指定從卡巴斯基安全管理中心自動匯入資產資訊和資產弱點資訊的間隔：
   - 若要匯入資產基本屬性資訊，請在**硬體資訊**下，按一下**匯入**按鈕。
   - 若要匯入資產其他屬性資訊，請在**資產屬性**下，按一下**匯入**按鈕。

此時將建立*KSC資產導入*工作。無論設定的排程為何，都會匯入指定租用戶的卡巴斯基安全管理中心資產。

檢視卡巴斯基安全管理中心伺服器的層次結構

若要檢視卡巴斯基安全管理中心伺服器的層次結構：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**卡巴斯基安全管理中心**。
   卡巴斯基安全管理中心整合視窗隨即開啟。
3. 在**租用戶**下拉清單，選取要檢視其層次結構的租用戶。
   連線參數視窗隨即開啟。
4. 在**連線參數**視窗中，按一下**載入層次結構**。

連線參數視窗中將顯示指定租用戶的卡巴斯基安全管理中心伺服器層次結構。

匯入卡巴斯基安全管理中心資料庫事件

在KUMA中，您可以從卡巴斯基安全管理中心SQL資料庫接收事件。使用收集器接收事件，收集器使用下列資源：

- 預定義連接器：[OOTB] KSC MSSQL或[OOTB] KSC MySQL。
- 預定義[OOTB] KSC from SQL標準化器

設定從卡巴斯基安全管理中心匯入事件涉及下列步驟：

1. 建立預定義連接器的副本。

   預定義連接器的設定不可編輯，因此，若要設定與資料庫伺服器的連線，必須建立預定義連接器的副本。

2. 建立連接器：
   - 在網頁介面中。
   - 在伺服器上。

若要設定從卡巴斯基安全管理中心匯入事件：

1. 建立與卡巴斯基安全管理中心使用的資料庫類型相對應的預定義連接器的副本：

   a. 在OSMP主控台的**監控 → 資源 → 連接器**部分中，在資料夾層次結構中找到相關的預定義連接器，選取該連接器旁的核取方塊，然後按一下**複製**。

   b. **這將開啟**建立連接器視窗；在該視窗的**基本設定**頁籤中，在**預設查詢**欄位中，如有必要，請將KAV資料庫名稱取代為您所使用的卡巴斯基安全管理中心資料庫的名稱。

   以下為卡巴斯基安全管理中心SQL資料庫查詢範例

   SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

   ev.product_name AS product_name, ev.product_version AS product_version,

   ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As msg,

   CASE

   WHEN ev.rise_time is not NULL THEN
   DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time)

   ELSE ev.rise_time

   END

   AS endTime,

   CASE

   WHEN ev.registration_time is not NULL

```
THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )

ELSE ev.registration_time

END

AS kscRegistrationTime,

cast(ev.par7 as varchar(4000)) as sourceUserName,

hs.wstrWinName as dHost,

hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,

CAST(hs.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp / 256 % 256 AS VARCHAR) + '.' +

CAST(hs.nlp % 256 AS VARCHAR) AS sourceAddress,

serv.wstrWinDomain as kscNtDomain,

CAST(serv.nlp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp / 256 / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp / 256 % 256 AS VARCHAR) + '.' +

CAST(serv.nlp % 256 AS VARCHAR) AS kscIP,

CASE

WHEN virus.tmVirusFoundTime is not NULL

THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )

ELSE ev.registration_time

END

AS virusTime,

virus.wstrObject As filePath,

virus.wstrVirusName as virusName,

virus.result_ev as result

FROM KAV.dbo.ev_event as ev

LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId

INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1
```

Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus

where registration_time >= DATEADD(minute, -191, GetDate())

c. 將滑鼠遊標放在**URL**欄位中，然後在顯示的清單中，在您正在使用的密鑰所在行按一下 。

d. 這將開啟**密鑰**視窗；在該視窗的**URL**欄位中，透過以下格式指定伺服器連線位址：

`sqlserver://user:password@kscdb.example.com:1433/database`

其中：

- `user` — 具有所需資料庫 public 與 db_datareader 權限的使用者帳戶。
- `password` — 使用者帳戶密碼。
- `kscdb.example.com:1433` — 資料庫伺服器的位址與連接埠。
- `database` — 卡巴斯基安全管理中心資料庫的名稱。預設為「KAV」。

按一下**儲存**按鈕。

e. 在**建立連接器**視窗的**連線**部分的**查詢**欄位中，將「KAV」資料庫名稱取代為您正在使用的卡巴斯基安全管理中心資料庫的名稱。

如果要使用查詢引用的ID直欄，則必須執行此操作。

按一下**儲存**按鈕。

2. 在網頁介面中安裝收集器：

a. 透過以下方式之一啟動收集器安裝精靈：

- 請在OSMP主控台的**監控 → 資源**部分中，按一下**新增事件來源**。
- 在OSMP主控台的**監控 → 資源 → 收集器**部分中，按一下**新增收集器**。

b. 在安裝精靈的步驟1**連線事件來源**中，指定收集器名稱並選擇租用戶。

c. 在安裝精靈的步驟2**傳輸**中，選擇您在步驟1中建立的連接器的副本。

d. 在安裝精靈的步驟3**事件解析**中，在**解析方案**頁籤上，按一下**新增事件解析**。

e. 這會開啟**基本事件解析**視窗；在該視窗的**正規化方案**頁籤上，從**正規化程式**下拉式清單中選取**[OOTB] KSC from SQL**，然後按一下**確定**。

f. 如有必要，請根據收集器的需求指定其他設定。為了匯入事件，在安裝精靈的其餘步驟中編輯設定是可選的。

g. 在安裝精靈的步驟8**安裝驗證**中，按一下**建立並儲存服務** 。

視窗下部顯示在伺服器上安裝收集器必須使用的命令。將此命令複製到剪貼簿。

h. 透過點選**儲存收集器**以關閉收集器安裝精靈。

3. 在伺服器上安裝收集器。

為此，在要接收卡巴斯基安全管理中心事件的伺服器上，執行在網頁介面中建立收集器後複製到剪貼簿的命令。

因此，收集器就安裝好了，並且可以從卡巴斯基安全管理中心的SQL資料庫接收事件。

您可以在網頁介面的**事件**部分檢視卡巴斯基安全管理中心事件。

Kaspersky Endpoint Detection and Response整合

Kaspersky Endpoint Detection and Response（以下也稱為「KEDR」）是Kaspersky Anti Targeted Attack Platform的功能單元，用於保護企業LAN中的資產。

您可以設定KUMA與Kaspersky Endpoint Detection and Response的集成，以管理連接到Kaspersky Endpoint Detection and Response伺服器的資產以及卡巴斯基安全管理中心資產的威脅回應操作。執行操作的命令由Kaspersky Endpoint Detection and Response伺服器接收，然後將這些命令轉發到安裝在資產上的Kaspersky Endpoint Agent。

您還可以將事件匯入KUMA並接收有關Kaspersky Endpoint Detection and Response警示的資訊（有關警示的更多詳細資訊，請參閱Kaspersky Anti Targeted Attack Platform說明中的*設定與SIEM系統的整合*部分）。

當KUMA與Kaspersky Endpoint Detection and Response整合時，您可以對具有Kaspersky Endpoint Agent的Kaspersky Endpoint Detection and Response資產執行下列操作：

- 管理資產的網路隔離。
- 管理防護規則。
- 啟動應用程式。

若要取得有關設定回應管理整合的說明，請聯絡您的客戶經理或技術支援。

使用kafka連接器匯入Kaspersky Endpoint Detection and Response事件

匯入Kaspersky Endpoint Detection and Response事件時，遙測以明文形式傳輸，可能會被入侵者截獲。

可以使用Kafka連接器將Kaspersky Endpoint Detection and Response 4.0、4.1、5.0和5.1事件匯入KUMA。

匯入Kaspersky Endpoint Detection and Response 4.0和4.1事件有幾個限制：

- 如果在Kaspersky Endpoint Detection and Response中使用KATA和KEDR產品授權金鑰，則可以匯入事件。
- 如果安裝在單獨伺服器上的感應器元件被用作Kaspersky Endpoint Detection and Response的一部分，則**無法**匯入事件。

若要匯入事件，請執行Kaspersky Endpoint Detection and Response和KUMA中的操作。

匯入Kaspersky Endpoint Detection and Response 4.0或4.1事件

要將Kaspersky Endpoint Detection and Response 4.0或4.1事件匯入KUMA：

在Kaspersky Endpoint Detection and Response中：

1. 使用SSH或終端登入要從中匯出事件的中央節點伺服器的管理主控台。
2. 當系統提示時，輸入安裝Kaspersky Endpoint Detection and Response期間設定的管理員帳號名稱和密碼。
   程式元件管理員功能表隨即顯示。
3. 在程式元件管理員功能表中，選擇**技術支援模式**。
4. 按一下**Enter**。
   將開啟技術支援模式確認視窗。
5. 確認您要在技術支援模式下操作應用程式。為此，請選擇**是**並按**Enter** 。
6. 執行以下命令：
   ```
   sudo -i
   ```
7. 在 `/etc/sysconfig/apt-services` 組態檔的 `KAFKA_PORTS` 欄位中，刪除值 `10000`。

   如果從屬中央節點伺服器或安裝在單獨伺服器上的感應器元件連線到中央節點伺服器，則需要允許透過連接埠10000連線到您修改了組態檔的伺服器。

   我們不建議將此連接埠用於KUMA之外的任何外部連線。若要將連接埠10000上的連線僅限於KUMA，請執行下列命令：

   ```
   iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP
   ```
8. 在組態檔 `/usr/bin/apt-start-sedr-iptables` 的 `WEB_PORTS` 欄位中，新增值 `10000`，並使用逗號分隔且不要加入空格。
9. 執行以下命令：
   ```
   sudo sh /usr/bin/apt-start-sedr-iptables
   ```

現在，在Kaspersky Endpoint Detection and Response端匯出事件的準備工作已經完成。

在Kaspersky Next XDR Expert的SIEM元件中：

1. 在 KUMA Core 伺服器上，以 `<IP address> centralnode` 格式將中央節點伺服器的 IP 位址新增至以下任一檔案中：
   - `%WINDIR%\System32\drivers\etc\hosts`—適用於 Windows。
   - `/etc/hosts file`—適用於 Linux。

2. 在OSMP主控台中，建立Kafka類型的連接器。

   建立連接器時，指定以下參數：

   - 在 **URL** 欄位中，指定 `<Central Node server IP address>:10000`。
   - 在 **主題** 欄位中，指定 `EndpointEnrichedEventsTopic`。
   - 在**使用者群組**欄位中，指定任何唯一名稱。

3. 在OSMP主控台中，建立收集器。

   使用上一步建立的連接器作為收集器的傳輸。使用「[OOTB] KEDR 遙測」作為收集器的正規化器。

如果收集器成功建立並安裝，則Kaspersky Endpoint Detection and Response事件將匯入KUMA。您可以在事件表中找到並檢視這些事件。

匯入Kaspersky Endpoint Detection and Response 5.0和5.1事件

匯入Kaspersky Endpoint Detection and Response 5.0和5.1事件時有幾個限制：

- 事件匯入僅適用於Kaspersky Endpoint Detection and Response的非高可用性版本。
- 如果在Kaspersky Endpoint Detection and Response中使用KATA和KEDR產品授權金鑰，則可以匯入事件。
- 如果安裝在單獨伺服器上的感應器元件被用作Kaspersky Endpoint Detection and Response的一部分，則**無法**匯入事件。

若要將Kaspersky Endpoint Detection and Response 5.0或5.1事件匯入KUMA：

在Kaspersky Endpoint Detection and Response中：

1. 使用SSH或終端登入要從中匯出事件的中央節點伺服器的管理主控台。
2. 當系統提示時，輸入安裝Kaspersky Endpoint Detection and Response期間設定的管理員帳號名稱和密碼。

   程式元件管理員功能表隨即顯示。
3. 在程式元件管理員功能表中，選擇**技術支援模式**。
4. 按一下**Enter**。

   將開啟技術支援模式確認視窗。
5. 確認您要在技術支援模式下操作應用程式。為此，請選擇**是**並按**Enter** 。
6. 在 `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.py` 設定檔中，為 `WEB_PORTS` 常數指定附加連接埠 `10000`：

   ```
   WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
   ```

   ```
   You do not need to perform this step for Kaspersky Endpoint Detection and Response 5.1 because the port is specified by default.
   ```
7. 執行以下指令：

   ```
   kata-firewall stop
   ```

```
kata-firewall start --cluster-subnet <network mask for addressing cluster servers>
```

現在，在Kaspersky Endpoint Detection and Response端匯出事件的準備工作已經完成。

在Kaspersky Next XDR Expert的SIEM元件中：

1. 在 KUMA Core 伺服器上，以 `<IP address> kafka.services.external.dyn.kata` 格式將中央節點伺服器的 IP 位址新增至以下任一檔案中：
   - `%WINDIR%\System32\drivers\etc\hosts`—適用於 Windows。
   - `/etc/hosts file`—適用於 Linux。
2. 在OSMP主控台中，建立Kafka類型的連接器。
   建立連接器時，指定以下參數：
   - 在 **URL** 欄位中，指定 `<Central Node server IP address>:10000`。
   - 在 **主題** 欄位中，指定 `EndpointEnrichedEventsTopic`。
   - 在**使用者群組**欄位中，指定任何唯一名稱。
3. 在OSMP主控台中，建立收集器。
   使用上一步建立的連接器作為收集器的傳輸。建議使用*[OOTB] KEDR遙測*標準化器作為收集器的標準化器。

如果收集器成功建立並安裝，則Kaspersky Endpoint Detection and Response事件將匯入KUMA。您可以在事件表中找到並檢視這些事件。

使用kata/edr連接器匯入Kaspersky Endpoint Detection and Response事件

若要使用kata/edr連接器從主機匯入Kaspersky Endpoint Detection and Response 5.1或更早版本的事件：

1. 在SIEM元件中設定接收事件。為此，在OSMP主控台中，使用「kata/edr」聯結器建立並安裝收集器或編輯現有收集器，然後儲存修改後的設定並重新啟動收集器。
2. 在KEDR方面，接受來自SIEM元件的授權請求，以便開始在Kaspersky Next XDR Expert中接收事件。

因此，設定整合後，KEDR事件將開始傳送至Kaspersky Next XDR Expert。

建立用於接收來自KEDR事件的收集器

若要建立用於接收來自KEDR事件的收集器：

1. 在OSMP主控台中，轉到**資源與服務→收集器**，選擇**新增收集器**。
2. 這將開啟**建立收集器**視窗；在該視窗中，在步驟 1**連線事件來源中**，指定任意**收集器名稱**，然後在下拉清單中選擇適當的**租用戶**。

3. 在步驟2**傳輸**中，執行以下操作：

   1. 在**基本設定**頁籤上：

      a. 在**連接器**欄位中，選擇**建立**，如果要使用先前建立的連接器，請開始輸入連接器的名稱。

      b. 在**連線類型**下拉清單中，選擇**kata/edr**連接器。選擇kata/edr連接器類型後，將顯示更多需要填寫的欄位。

      c. 在**URL**欄位中，請以 <主機名稱或IP位址>:<連接埠，預設為443> 格式指定連線至KEDR伺服器的位址。若 KEDR 解決方案部署於叢集中，點擊**新增**可以新增所有節點。KUMA 將依序連線至每個指定節點。若KEDR解決方案採分散式組態安裝，則在KUMA端，必須為每台KEDR伺服器分別設定獨立的收集器。

      d. 在**密鑰**欄位中，選擇**建立**以建立新密鑰。這將開啟**建立密鑰**視窗；在該視窗中，指定**名稱**，然後按一下**產生並下載憑證和私有加密金鑰**。

      因此，certificate.zip存檔將下載到瀏覽器的下載資料夾；該存檔包含key.pem金鑰檔案和cert.pem憑證檔案。解壓縮存檔。點擊**上傳憑證**並選擇cert.pem檔案。按一下**上傳私密金鑰**並選擇key.pem檔案。點擊**建立**按鈕。密鑰會新增至**密鑰**下拉式清單，並自動選取。

      您也可以從**密鑰**清單中選擇已建立的密鑰。KUMA使用選定的密鑰連接到KEDR。

      e. **外部ID**欄位包含外部系統的ID。授權KUMA伺服器時，此ID會顯示在KEDR網頁介面中。KUMA會自動產生ID，並且**外部ID**欄位會自動預先填入。

   2. 在**進階設定**頁籤上：

      a. 若要取得收集器日誌中的詳細資訊，請將**偵錯**切換開關移至啟用位置。

      b. 如果需要，請在**字元編碼**欄位中，選擇要轉換為UTF-8的來源資料的編碼。我們僅建議在標準化事件的欄位中發現無效字元時設定轉換。預設情況下，不指定值。

      c. 指定每次向KEDR發出請求的最大**事件的數量**。預設值為0，這表示KUMA使用KEDR伺服器上指定的值。有關詳細資訊，請參閱KATA說明。您可以指定任意值，但不得超過KEDR端的值。如果您指定的值超過KEDR伺服器上指定的**最大事件數量**設定的值，KUMA收集器日誌將顯示錯誤*錯誤請求：max_events N大於允許的值*。

      d. 填寫**事件擷取逾時時間**欄位，以便在指定的時間段後接收事件。預設值是0。這意味著應用KEDR伺服器的預設值。有關詳細資訊，請參閱KATA說明。此欄位指定KEDR伺服器必須在多久後向KUMA傳送事件。KEDR伺服器使用兩個參數：最大事件數和事件獲取逾時時間。當收集到指定數量的事件或設定的時間已到（以先發生者為準）時，將傳送事件。如果已到指定時間，但尚未收集到指定數量的事件，則KEDR伺服器將傳送已收集的事件，而無需等待更多事件。

      e. 在**用戶端逾時時間**欄位中，指定KUMA必須等待KEDR伺服器回應的時間（以秒為單位）。預設值：1,800秒；顯示為0。**用戶端逾時時間**在用戶端逾時時間欄位中指定。**用戶端逾時時間**必須大於伺服器的**事件擷取逾時時間**，才能等待伺服器回應，而不會透過新請求中斷目前事件收集工作。如果KEDR伺服器的回應最終未抵達，KUMA將重複該請求。

      f. 在**KEDRQL 篩選器**欄位中，指定篩選請求的條件。因此，系統將從KEDR接收預先篩選的事件。有關可用篩選器欄位的詳細資訊，請參閱KATA說明。

4. 在步驟3 **解析**中，按一下**新增事件解析**，然後在**基本事件解析**視窗中選取**[OOTB] KEDR遙測**。

5. 若要在網頁介面中完成收集器的建立，按一下**建立並儲存服務**。然後從網頁介面複製收集器安裝命令，並在要安裝收集器的伺服器的命令列上執行此安裝命令。

   如果您正在編輯現有收集器，請按一下**儲存並重新啟動服務**。

因此，收集器已建立並準備好傳送請求。收集器會顯示在**資源與服務 → 作用中服務**區段中，且狀態為黃色，

直到KEDR接受來自KUMA的授權請求為止。

在KEDR端授權KUMA

在KUMA中建立收集器後，要使來自KUMA的請求開始抵達KEDR，必須在KEDR端接受KUMA授權請求。授權請求被接受後，KUMA收集器會自動向KEDR傳送排程請求並等待回應。等待期間，收集器的狀態為黃色；收到請求的第一個回應後，收集器的狀態變為綠色。

因此，整合隨即設定，您可以在OSMP主控台的**事件**部分檢視來自KEDR的事件。

初始請求會擷取在整合設定完成前已發生的部分歷史事件。所有歷史事件完成傳輸後，當前事件才會開始送達。若變更 **URL** 設定值或現有收集器的**外部 ID**，KEDR 會將後續請求視為初始請求處理。在以修改後的設定啟動 KUMA 收集器後，系統將重新傳輸部分歷史事件。如果您不想接收歷史事件，請前往相關收集器的設定，在正規化器中設定KEDR與KUMA `timestamp`欄位的對應，並在收集器安裝精靈的「事件篩選」步驟中指定依`timestamp`篩選的條件 — 啟動收集器時，事件的`timestamp`必須大於`timestamp`。

可能出現的錯誤和解決方案

如果在收集器日誌中看到 *衝突：具有以下 IP 和憑證摘要的外部系統已存在。請將其刪除或提供新的憑證* 錯誤，請在收集器的連接器中使用憑證建立新的密鑰。

如果您在收集器日誌中看到事件請求的回應中出現「*找不到接續權杖*」錯誤，請建立新的連接器，將其連接至收集器並重新啟動收集器；或者，在收集器的連接器中使用新憑證建立新的密鑰。如果您不想接收錯誤發生之前產生的事件，請在收集器中設定時間戳篩選器。

設定在KUMA警示中顯示Kaspersky Endpoint Detection and Response偵測的連結

當收到Kaspersky Endpoint Detection and Response偵測時，KUMA會為每個偵測建立警示。您可以在KUMA警示資訊中設定顯示Kaspersky Endpoint Detection and Response偵測的連結。

如果您在Kaspersky Endpoint Detection and Response中僅使用一個中央節點伺服器，則可以設定顯示偵測的連結。如果在分散式解決方案模式下使用Kaspersky Endpoint Detection and Response，則無法在KUMA中設定顯示Kaspersky Endpoint Detection and Response偵測的連結。

要設定在KUMA警示詳情中顯示偵測的連結，您需要完成Kaspersky Endpoint Detection and Response網頁介面和KUMA中的步驟。

在Kaspersky Endpoint Detection and Response網頁介面中，您需要設定應用程式與KUMA作為SIEM系統的整合。有關設定整合的詳細資訊，請參閱*Kaspersky Anti Targeted Attack Platform*說明文件中的*設定與SIEM系統的整合*部分。

在OSMP主控台中設定顯示連結包含以下步驟：

1. 新增包含Kaspersky Endpoint Detection and Response中央節點伺服器（您要從該伺服器接收偵測資料）資訊的資產，並為該資產指派類別。
2. 建立關聯規則。
3. 建立關聯器。

您可以使用預設定的關聯規則。在本例中，在OSMP主控台中設定顯示連結包括以下步驟：

1. 建立關聯器。

   選擇 `[OOTB] KATA Alert` 關聯規則。
2. 新增包含Kaspersky Endpoint Detection and Response中央節點伺服器（您要從該伺服器接收偵測資料）資訊的資產，並為該資產指派 `KATA standAlone` 類別。

步驟 1。新增資產並為其指派類別

首先，您需要建立一個類別，該類別將指派給要新增的資產。然後新增資產。

若要新增資產：

1. 在主功能表中，轉至**資產管理 → 資產（裝置） → 偵測與回應**。
2. 按一下**新增**按鈕。

   新增資產詳情區域將在視窗右側開啟。
3. 定義下列資產參數：
   a. 在**資產名稱**欄位中，輸入資產名稱。
   b. 在**租用戶**下拉清單中，選擇將擁有該資產的租用戶。
   c. 在**IP位址**欄位中，指定要從中Kaspersky Endpoint Detection and Response中央節點伺服器的IP位址。
   d. 在**類別**欄位中，選擇您在上一個步驟中新增的類別。

   > 若使用的是預定義關聯規則，則需選取 `KATA standAlone` 類別。

   e. 如有需要，定義下列欄位的值：
   - 在**FQDN**欄位中，指定Kaspersky Endpoint Detection and Response伺服器的完全限定網域名稱。
   - 在**MAC位址**欄位中，指定中央節點Kaspersky Endpoint Detection and Response中央節點伺服器的MAC位址。
   - 在**所有者**欄位中，定義資產所有者的名稱。
4. 按一下**儲存**按鈕。

步驟 2。新增關聯規則

若要新增關聯規則：

1. 在主功能表中，轉至**監控→資源與服務**。
2. 選擇**關聯規則**，然後按一下**建立關聯規則**按鈕。
3. 在**一般**頁籤中，指定以下設定：
   a. 在**名稱**欄位中，輸入規則名稱。
   b. 在**類型**下拉清單中，選取**簡單**。
   c. 在**傳播欄位**欄位中，新增下列欄位：DeviceProduct、DeviceAddress、EventOutcome、SourceAssetID、DeviceAssetID。
   d. 如有需要，定義下列欄位的值：
      - 在**觸發率限制**欄位中，定義每秒觸發規則的最大次數。
      - 在**嚴重等級**欄位中，定義觸發規則後將建立的警示和關聯事件的嚴重等級。
      - 在**描述**欄位中，提供任何其他資訊。
4. 在**選擇器→設定**頁籤上，指定以下設定：
   a. 在**篩選器**下拉清單中，選擇**新建**。
   b. 在**條件**欄位中，點選**新增群組**按鈕。
   c. 在您新增的群組的運算子欄位中，選擇**AND**。
   d. 新增依KATA值篩選的條件：
      1. 在**條件**欄位中，按一下**新增條件**按鈕。
      2. 在條件欄位中，選擇**如果**。
      3. 在**左運算元**欄位中，選擇**事件欄位**。
      4. 在**事件欄位**欄位中，選擇**DeviceProduct**。
      5. 在**運算子**欄位中，選擇=。
      6. 在**右運算元**欄位中，選擇**常數**。
      7. 在**值**欄位中，輸入KATA。
   e. 新增類別篩選條件：
      1. 在**條件**欄位中，按一下**新增條件**按鈕。
      2. 在條件欄位中，選擇**如果**。
      3. 在**左運算元**欄位中，選擇**事件欄位**。

4. 在**事件**欄位中，選擇**DeviceAssetID**。

5. 在**運算子**欄位中，選擇**inCategory**。

6. 在**右運算元**欄位中，選擇**常數**。

7. 按一下按鈕。

8. 選擇您放置Kaspersky Endpoint Detection and Response中央節點伺服器資產的類別。

9. 按一下**儲存**按鈕。

f. 在**條件**欄位中，點選**新增群組**按鈕。

g. 在您新增的群組的運算子欄位中，選擇**OR**。

h. 新增依事件類別識別碼篩選的條件：

1. 在**條件**欄位中，按一下**新增條件**按鈕。

2. 在條件欄位中，選擇**如果**。

3. 在**左運算元**欄位中，選擇**事件欄位** 。

4. 在**事件欄位**欄位中，選擇**DeviceEventClassID**。

5. 在**運算子**欄位中，選擇=。

6. 在**右運算元**欄位中，選擇**常數**。

7. 在**值**欄位中，輸入**taaScanning**。

i. 對下列每個事件類別ID重複F中的步驟1-7：

- file_web.
- file_mail.
- file_endpoint.
- file_external.
- ids.
- url_web.
- url_mail.
- dns.
- iocScanningEP.
- yaraScanningEP.

5. 在**操作**頁籤中，指定以下設定：

   a. 在**操作**部分中，開啟**在每個事件上**下拉清單。

   b. 選取**輸出**核取方塊。

   c. 在**擴充**部分中，按一下**新增擴充**按鈕。

   d. 在**來源類型**下拉清單中，選擇**範本**。

   e. 在**範本**欄位中，輸入*https://{{.DeviceAddress}}:8443/katap/#/alerts?id={{.EventOutcome}}*。

   f. 在**目標欄位**下拉清單中，選擇**DeviceExternalID**。

   g. 請根據需要開啟**偵錯**切換開關以記錄與資源操作相關的資訊。

6. 按一下**儲存**按鈕。

步驟 3：建立關聯器

您需要啟動關聯器安裝精靈。在精靈的步驟 3中，您需要選擇依照本指南新增的關聯規則。

建立關聯器後，從 Kaspersky Endpoint Detection and Response 接收偵測結果時所建立的警報詳情中，會顯示這些偵測結果的連結。此連結顯示在關聯事件詳情（ **威脅搜尋**部分）的**DeviceExternalID**欄位中。

如果您希望 Kaspersky Endpoint Detection and Response Central Node 伺服器的 FQDN 顯示在偵測詳情的 DeviceHostName 欄位中，則需要為該伺服器建立 DNS 記錄，並在精靈的步驟 4中建立 DNS 擴充規則。

與Kaspersky CyberTrace整合

Kaspersky CyberTrace（以下簡稱CyberTrace）是一種將威脅資料流與SIEM解決方案整合的工具。它為使用者提供了對分析資料的即時訪問，提高了他們對安全決策的認識。

您可以透過以下方式之一將CyberTrace與KUMA整合：

- 整合CyberTrace指標搜尋功能，以使用來自CyberTrace資料流的資訊擴充KUMA事件。
- 將整個CyberTrace網頁介面整合到KUMA以獲得對CyberTrace的完全存取權限。

  只有當您的CyberTrace產品授權包含多使用者功能時，才可以進行CyberTrace主控台整合。

整合CyberTrace指標搜尋

若要整合CyberTrace指標搜尋：

1. 設定CyberTrace以接收和處理KUMA請求。

   您可以在快速啟動精靈中安裝CyberTrace後立即設定與KUMA的整合，也可以稍後在CyberTrace網頁介面中設定。

2. 建立事件擴充規則。

   在擴充規則中，您可以指定要使用CyberTrace中的哪些資料來擴充事件。

3. 建立一個收集器來接收您想要使用CyberTrace資料擴充的事件。

4. 將擴充規則連結到收集器。

5. 儲存並建立服務：

   - 如果將規則連結到新的收集器，請按一下**儲存並建立**，在開啟的視窗中複製收集器ID，然後使用複製的ID透過命令列介面在伺服器上安裝收集器。
   - 如果將規則連結到現有收集器，請按一下**儲存並重新啟動服務**以套用設定。

   CyberTrace指標搜尋整合的設定已完成，KUMA事件將使用CyberTrace資料進行擴充。

CyberTrace 資料擴充測試範例

預設情況下，KUMA不會測試與CyberTrace的連線。

如果您想測試與CyberTrace的整合並確保事件擴充功能正常運作，您可以依照以下範例的步驟操作或根據您的情況調整範例。此範例展示了一個整合測試，它執行擴充功能並顯示事件包含指定的測試URL。

若要執行測試：

1. 使用下表所列的參數建立測試擴充規則。

設定	參數值
名稱	測試CT擴充
租用戶	共用
來源類型	cybertrace
URL	<您要向其傳送請求的cybertrace伺服器的URL>:9999
對應	KUMA欄位：RequestURL CyberTrace指標：url
除錯	已啟用

1. 使用下列參數建立測試收集器：

   在步驟**2傳輸**中，指定http連接器。

   在步驟**3解析**中，指定標準化器並選擇json解析方法，設定RequestUrl – RequestUrl欄位的對應。

   在步驟**6擴充**中，指定「測試CT擴充」規則。

   在步驟**7資訊傳送**中，指定必須傳送事件的儲存體。

2. 按一下**建立並儲存服務**。

   視窗中顯示安裝收集器的完整命令。

3. 按一下**複製**將命令複製到剪貼簿並在命令列中執行該命令。等待指令完成後，返回KUMA主控台，然後按一下**儲存收集器** 。

   測試收集器隨即建立，並測試擴充規則將連結到該收集器。

4. 使用命令列介面向收集器傳送請求，該請求將觸發事件，隨後該事件會以測試 URL `http://fakess123bn.nu` 進行擴充處理。例如：

   ```
   curl --request POST \
     --url http://<安裝收集器的主機 ID>:<收集器的連接埠>/input \
     --header 'Content-Type: application/json' \
     --data '{"RequestUrl":"http://fakess123bn.nu"}'
   ```

5. 轉至KUMA的**事件**部分，並執行以下查詢以篩選事件輸出並找到擴充的事件：

   ```
   SELECT * FROM `events` WHERE RequestUrl = 'http://fakess123bn.nu' ORDER BY Timestamp DESC LIMIT 250
   ```

   結果：

   擴充處理成功完成，事件現在包含一個值為 `http://fakess123bn.nu` 的 **RequestURL** 欄位，以及附帶 CyberTrace 資料的 TI 指標與指標分類。

如果測試沒有導致擴充，例如，如果缺少TI指標，我們建議執行以下操作：

1. 檢查收集器和擴充規則的設定。

2. 使用下列命令下載收集器日誌並尋找日誌中的錯誤：

   ```
   tail -f /opt/kaspersky/kuma/collector/<collector ID>/log/collector
   ```

設定CyberTrace以接收和處理請求

您可以在快速啟動精靈或稍後在程式網頁介面中將CyberTrace設定為安裝KUMA後立即接收和處理來自KUMA的請求。

若要在快速啟動精靈中設定CyberTrace以接收和處理請求：

1. 程式安裝完成後，等待CyberTrace快速啟動精靈啟動。

   歡迎使用Kaspersky CyberTrace視窗將開啟。

2. 在 **選取 SIEM** 下拉式清單中，選取您要從中接收資料的 SIEM 系統類型，然後按一下 **下一步** 按鈕。

   連線參數視窗隨即開啟。

3. 請執行下列操作：

   a. 在**服務監聽**設定區塊中，選擇**IP和連接埠**選項。

   b. 在 **IP 位址**欄位中輸入 `0.0.0.0`。

   c. 在 **連接埠**欄位中，輸入用於接收事件的連接埠，預設連接埠為 `9999`。

   d. 在 **服務傳送事件至**下方，請在 **IP 位址或主機名稱**欄位中指定 `127.0.0.1`，並在 **連接埠**欄位中指定 `9998`。

   保留其他所有選項的預設值。

   e. 按一下**下一步**。

   代理設定視窗隨即開啟。

4. 如果您的組織正在使用代理伺服器，請定義連線到它的設定。如果沒有，請將所有欄位留空，然後按一下**下一步**。

   監聽設定視窗隨即開啟。

5. 在**Kaspersky CyberTrace產品授權金鑰**欄位中，新增CyberTrace的產品授權金鑰。

6. 在**Kaspersky Threat Data Feeds憑證**欄位中，新增可讓您從伺服器下載更新的資料來源的憑證，然後按一下**下一步**。

CyberTrace將設定。

若要在程式網頁介面中設定CyberTrace接收和處理請求：

1. 在CyberTrace網頁介面中，選擇**設定-服務**。
2. 在**連線設定**區塊中：
   a. 選擇**IP和連接埠**選項。
   b. 在**IP 位址**欄位中輸入`0.0.0.0`。
   c. 在**連接埠**欄位中指定用於接收事件的連接埠，預設連接埠為`9999`。
3. 在**網頁介面**設定區塊的**IP 位址或主機名稱**欄位中，輸入`127.0.0.1`。
4. 在上面的工具列中，按一下**重新啟動CyberTrace服務**。
5. 選擇**設定 - 事件格式**。
6. 在**警示事件格式**欄位中，輸入`%Date% alert=%Alert%%RecordContext%`。
7. 在**偵測事件格式**欄位中，輸入`Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`。
8. 在**記錄內容格式**欄位中，輸入`|%ParamName%=%ParamValue%`。
9. 在**可操作欄位內容格式**欄位中，輸入`%ParamName%:%ParamValue%`。

CyberTrace將設定。

更新CyberTrace設定後，您必須重新啟動CyberTrace伺服器。

建立事件擴充規則

若要建立事件擴充規則：

1. 在主功能表中，轉至**監控→資源與服務→擴充規則**。
2. 在視窗左側，選擇或建立一個資料夾用於存放新規則。

   可用的擴充規則清單隨即顯示。

3. 按一下**建立**以建立新規則。

   擴充規則視窗隨即顯示。

4. 輸入規則組態參數：

   a. 在**名稱**欄位中，輸入規則的唯一名稱。此名稱必須包含1到128個Unicode字元。

   b. 在**租用戶**下拉清單中，選擇將擁有此資源的租用戶。

   c. 在**來源類型**下拉清單中，選擇**CyberTrace**。

   d. 指定要連線的CyberTrace伺服器的**URL** 。例如，*example.domain.com:9999*.

   e. 如有必要，使用**連線數量**欄位指定OSMP可以同時建立的到CyberTrace伺服器的最大連線數。預設情況下，此值等於KUMA Core伺服器的vCPU數量。

   f. 在 **RPS** 欄位中，輸入 OSMP 每秒可向 CyberTrace 伺服器傳送的請求數。預設值是 `1000`。

   g. 在**擴充佇列中的最大事件數**欄位中，指定儲存在擴充佇列中以重新傳送的最大事件數。預設值為 `1000000`。

   h. 在**逾時**欄位中，指定 OSMP 等待 CyberTrace 伺服器回應的最大秒數。在收到回應或時間到期之前，事件不會被傳送至關聯器。若在逾時之前收到回應，該回應將被新增至事件的`TI`欄位，事件處理會繼續進行。預設值是 `30`。

   i. 使用**偵錯**下拉清單指示是否啟用服務運作的日誌記錄。預設情況下，日誌記錄處於停用狀態。

   j. 在**標籤**下拉清單中，選擇事件擴充規則的標籤。

   k. 如有必要，在**描述**欄位中新增最多4,000個Unicode字元來描述資源。

   l. 在**對應**下，您必須指定要透過 CyberTrace 檢查的事件欄位，並定義將 KUMA 事件欄位對應至 CyberTrace 指標類型的規則：

      - 在**KUMA欄位**直欄中，選擇必須將其值傳送給CyberTrace的欄位。
      - 在**CyberTrace指標**直欄中，為每個選定的欄位選擇CyberTrace指標類型：
        - **ip**
        - **網址**
        - **雜湊值**

      您必須向表格提供至少一個字串。您可以點擊**新增**按鈕新增字串，也可以點擊✕按鈕刪除字串。

   m. 在**篩選器**部分，您可以指定條件來識別將使用擴充規則處理的事件。您可以從**篩選器**下拉清單中選擇一個現有的篩選器，或者**建立**一個新的篩選器。

      在資源中建立過濾器

      KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

若要建立篩選器：

1. 在**篩選器**下拉清單中，選擇**新建**。

2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。

3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。

4. 在**條件**下，指定事件必須滿足的條件：

   a. 點擊**新增條件**按鈕。

   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。

   c. 在**運算子**下拉清單中，選擇一個運算子。

   篩選器運算子

   - **=** — 左運算元等於右運算元。
   - **<** — 左運算元小於右運算元。
   - **<=** — 左運算元小於或等於右運算元。
   - **>** — 左運算元大於右運算元。
   - **>=** — 左運算元大於或等於右運算元。
   - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
   - **contains** — 左運算元包含右運算元的值。
   - **startsWith** — 左運算元以右運算元的某個值開頭。
   - **endsWith** — 左運算元以右運算元的某個值末端。
   - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
   - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

     待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

     若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
   - **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

     如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
   - **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
   - **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。

- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。
6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

5. 按一下**建立**按鈕。

新的擴充規則隨即建立。

CyberTrace指標搜尋整合現已設定完成。現在您可以將建立的擴充規則新增至收集器。您必須重新啟動KUMA收集器才能套用新設定。

若事件詳細資訊區域中的任何 CyberTrace 欄位包含「[{」或「}]」值，則表示 CyberTrace 資料饋送的資訊處理不正確，部分資料可能無法顯示。從KUMA複製事件 **TI指標**欄位的值並在指標區域的CyberTrace中搜尋該值，即可取得所有資料饋送資訊。所有相關資訊將顯示在CyberTrace的**指標上下文**區域。

整合CyberTrace介面

您可以將CyberTrace網頁介面與OSMP主控台整合。啟用此整合後，OSMP主控台包含一個**CyberTrace**部分，該部分提供對CyberTrace網頁介面的存取。您可以在OSMP主控台的**設定→KUMA→開啟 KUMA 設定→Kaspersky CyberTrace**部分中設定整合。

若要在OSMP主控台中整合CyberTrace網頁介面：

1. 在主功能表中，轉至**監控→資源與服務→密鑰**。
   可用密鑰清單隨即顯示。
2. 按一下新增按鈕以**建立**新密鑰。此資源用於儲存CyberTrace伺服器的憑證。
   密鑰視窗隨即顯示。

3. 輸入有關密鑰的資訊：

   a. 在**名稱**欄位中，為新增的密鑰選擇名稱。此名稱必須包含1到128個Unicode字元。

   b. 在**租用戶**下拉清單中，選擇將擁有此資源的租用戶。

   c. 在**類型**下拉清單中，選取**憑證**。

   d. 在**使用者**和**密碼**欄位中，輸入CyberTrace伺服器的憑證。

   e. 如有必要，從**標籤**下拉清單中選取密鑰的標籤。

   f. 如有必要，在**描述**欄位中新增最多4,000個Unicode字元來描述資源。

4. 按一下**建立**按鈕。

   CyberTrace伺服器憑證現已儲存，可用於其他KUMA資源。

5. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

6. 在**威脅情報**下，按一下**Kaspersky CyberTrace**。

   這將開啟**Kaspersky CyberTrace 整合**視窗。

7. 對以下參數進行必要的變更：

   - **狀態**— 如果要將CyberTrace網頁介面整合到KUMA主控台，請啟用此切換開關。
   - **主機**（必填）— 輸入CyberTrace伺服器的位址。
   - **連接埠**（必填）— 輸入CyberTrace伺服器的連接埠；管理網頁介面的預設連接埠為443。
   - 在**密鑰**下拉清單中，選擇先前建立的密鑰。
   - 在**允許主機**下拉清單中，選擇支援CORS技術的主機。
   - 在**CyberTrace主要版本**欄位中，選擇CyberTrace版本。可能的值： **<5**、**≥ 5.0**。如果選擇了版本**≥ 5.0**，則請求將在CyberTrace的一般租用戶中執行，並使用Kaspersky CyberTrace 5.0及更高版本提供的新版API。如果您選擇**<5** ，則請求將使用Kaspersky CyberTrace 4.x API。預設值是**<5**。

8. 您可以透過以下方式設定對CyberTrace網頁介面的存取：

   - 登入OSMP主控台時使用主機名稱或IP位址。

     為此，在**允許主機**部分中，按一下**新增主機**，然後在顯示的欄位中輸入裝置的IP或主機名稱。

   - 登入OSMP主控台時使用FQDN。

     如果您使用Mozilla Firefox瀏覽器管理主控台，CyberTrace部分可能無法顯示資料。在這種情況下，請設定資料顯示（請參閱下文）。

9. 按一下**儲存**按鈕。

CyberTrace現在已與OSMP整合，**CyberTrace**部分顯示在OSMP主控台中。

*若要在Mozilla Firefox中使用FQDN登入OSMP主控台時設定**CyberTrace**部分中的資料顯示：*

1. 清除瀏覽器快取。
2. 在瀏覽器的網址列中，輸入包含連接埠號的OSMP主控台的FQDN。
   將打開一個視窗，向您警告潛在的安全威脅。
3. 按一下**詳細資訊**按鈕。
4. 在視窗下方，點選**接受風險並繼續**按鈕。
   將為OSMP主控台的URL建立排除項。
5. 在瀏覽器的網址列中，輸入包含連接埠號的OSMP主控台的URL。
6. 轉至**CyberTrace**部分。

資訊將顯示在此部分中。

更新CyberTrace拒絕清單（內部TI）

將CyberTrace網頁介面整合到OSMP主控台時，您可以使用KUMA事件的資訊更新CyberTrace拒絕清單或**內部TI**。

若要更新CyberTrace內部TI：

1. 從事件表、警示視窗或關聯事件視窗開啟事件詳細資訊區域，然後按一下網域、網址、IP位址或檔案雜湊值上的連結。
   快顯功能表隨即開啟。
2. 選擇**新增至CyberTrace的內部TI**。

所選物件現已新增至CyberTrace拒絕清單中。

透過LDAP連線

在OSMP主控台中，可在**設定→KUMA→開啟 KUMA 設定→LDAP伺服器**下建立和管理LDAP的連線。**依租用戶區分的 LDAP 伺服器整合**部分顯示為其建立了LDAP連線的租用戶。可以建立或刪除租用戶。

如果您選擇租用戶，則**LDAP 伺服器整合**視窗將會打開，顯示包含現有LDAP連線的表格。您可以建立或編輯連線。在此視窗中，您可以變更傳送至LDAP伺服器的查詢頻率，並設定過時資料的保存週期。

啟用整合後，有關Active Directory帳戶的資訊將在警示視窗、關聯事件詳細視圖視窗和事件視窗中可用。如果按一下視窗的**相關使用者**部分中的帳戶名稱，將開啟**帳戶詳情**窗口，其中包含從Active Directory匯入的資料。

在擴充收集器和分析中的事件時，也可以使用來自LDAP的資料。

匯入的Active Directory屬性

可以從Active Directory請求以下帳戶屬性：

- accountExpires
- badPasswordTime
- cn
- co
- company
- department
- description
- displayName
- distinguishedName
- division
- employeeID
- givenName
- l
- lastLogon
- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf（此屬性可在關聯分析期間用於搜尋）
- mobile
- name
- objectCategory
- objectGUID（即使使用者未指定此屬性，也總會從 Active Directory 請求此屬性）
- objectSID
- physicalDeliveryOfficeName

- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

有關Active Directory屬性的詳細資訊，請參閱Microsoft說明文件。

啟用和停用LDAP整合

您可以同時啟用或停用租用戶的所有LDAP連線，也可以單獨啟用和停用LDAP連線。

若要啟用或停用租用戶的所有LDAP連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器** ，然後選擇要為其啟用或停用所有LDAP連線的租用戶。
   LDAP 伺服器整合視窗隨即開啟。
3. 啟用或停用**狀態**切換開關。
4. 按一下**儲存**按鈕。

若要啟用或停用特定的LDAP連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器** ，然後選擇要為其啟用或停用所有LDAP連線的租用戶。
   LDAP 伺服器整合視窗隨即開啟。
3. 在連線表中，啟用或停用相關連線的**狀態**切換開關。
4. 按一下**儲存**按鈕。

將租用戶新增至LDAP伺服器整合清單

若要將租用戶新增至與LDAP伺服器整合的租用戶清單：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器**。
   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。
3. 點選**為新的租用戶新增設定**按鈕。
   LDAP 伺服器整合視窗隨即顯示。
4. 在**租用戶**下拉清單中，選擇需要新增的租用戶。
5. 按一下**儲存**按鈕。

選定的租用戶將會新增至LDAP伺服器整合清單中。

若要從與LDAP伺服器整合的租用戶清單中刪除租用戶：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器**。
   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。
3. 選取您要刪除之租用戶旁的核取方塊，並點選**刪除**。
4. 確認刪除租用戶。

選定的租用戶將從LDAP伺服器整合清單中刪除。

建立LDAP伺服器連線

若要建立與Active Directory的新LDAP連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器**。
   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。
3. 選擇或建立要為其建立LDAP連線的租用戶。
   LDAP 伺服器整合視窗隨即開啟。
4. 按一下**新增連線**按鈕。
   連線參數視窗隨即開啟。

5. 新增一個包含連線到Active Directory伺服器的帳戶憑據的密鑰。為此：

   a. 如果您之前新增了密鑰，請在**密鑰**下拉清單中選擇現有密鑰（使用**憑證**類型）。
   可以透過點選鉛筆圖示（ ）來更改所選密鑰。

   b. 如果要建立新的密鑰，請點選加號圖示（ ＋ ）。
   密鑰視窗隨即開啟。

   c. 在**名稱**（必填）欄位中，輸入包含1到128個Unicode字元的密鑰名稱。

   d. 在**使用者**和**密碼**（必填）欄位中，輸入用於連線到Active Directory伺服器的帳戶憑證。
   您可以採用下列格式之一輸入使用者名稱：<使用者名稱>@<網域> 或 <網域><使用者名稱>。

   e. 在**描述**欄位中，輸入最多4,000個Unicode字元的描述。

   f. 按一下**儲存**按鈕。

6. 在**名稱**（必填）欄位中，輸入LDAP連線的唯一名稱。
   字串長度必須為1到128個Unicode字元。

7. 在**URL**（必填）欄位中，以`<hostname or IP address of server>:<port>`格式輸入網域控制器的位址。

   > 如果出現伺服器可用性問題，您可以指定多個具有網域控制器的伺服器，並用逗號分隔它們。所有指定的伺服器必須位於同一個網域中。

8. 如果要對與網域控制站的連線使用TLS加密，請從**類型**下拉清單中選擇下列選項之一：

   - **startTLS**。
     使用startTLS方法時，它首先透過連接埠389建立未加密的連線，然後傳送加密請求。如果STARTTLS命令以錯誤結束，則連線終止。

     > 確保連接埠389已開啟。否則，將無法與網域控制器建立連線。

   - **ssl**。
     使用SSL時，會立即透過連接埠636建立加密連線。

   - **insecure**。

   使用加密連線時，無法將IP位址指定為URL。

9. 如果您在上一個步驟啟用了TLS加密，請新增TLS憑證。為此：

   a. 如果您之前已上傳憑證，請從**憑證**下拉清單中選擇它。
   如果之前未新增憑證，下拉清單將顯示**無資料**。

   b. 如果要上傳新憑證，請按一下位於**憑證**清單右側的加號圖示（ ＋ ）。
   密鑰視窗隨即開啟。

   c. 在**名稱**欄位中，輸入憑證新增後將顯示在憑證清單中的名稱。

d. 按一下**上傳憑證檔案**按鈕以新增包含Active Directory憑證的檔案。支援Base64格式的X.509憑證公鑰。

e. 請根據需要在**描述**欄位中提供有關憑證的任何相關資訊。

f. 按一下**儲存**按鈕。

憑證將被上傳並顯示在**憑證**清單中。

10. 在**逾時（秒）**欄位中，指示等待網域控制器伺服器回應的時間。

    如果在**URL**欄位中指定多個位址，KUMA 會在指定的秒數內等待第一個伺服器回應。如果在此時間內未收到回應，則會嘗試連線到下一個伺服器。如果在指定的時間內未有任何指定的伺服器回應，則連線將終止並出現錯誤。

11. 在**基本DN**欄位中，輸入應執行搜尋要求的目錄的基本可分辨名稱。

12. 在**自訂AD帳戶屬性**欄位中，指定**要用於擴充事件的其他屬性**。

    在使用自訂屬性設定事件擴充之前，請確保在AD中設定了自訂屬性。

    若要使用自訂屬性擴充帳戶活動：

    1. 在**LDAP連線設定**中新增自訂AD帳戶屬性。

       標準的**從AD匯入的屬性**不能新增為自訂屬性。例如，若將標準的 `accountExpires` 屬性新增為自訂屬性，KUMA 會在儲存連線設定時傳回錯誤。

       可以從Active Directory請求以下帳戶屬性：

       - `accountExpires`
       - `badPasswordTime`
       - `cn`
       - `co`
       - `company`
       - `department`
       - `description`
       - `displayName`
       - `distinguishedName`
       - `division`
       - `employeeID`
       - `givenName`
       - `l`
       - `lastLogon`

- lastLogonTimestamp
- Mail
- mailNickname
- managedObjects
- manager
- memberOf（此屬性可在關聯分析期間用於搜尋）
- mobile
- name
- objectCategory
- objectGUID（即使使用者未指定此屬性，也總會從 Active Directory 請求此屬性）
- objectSID
- physicalDeliveryOfficeName
- pwdLastSet
- sAMAccountName
- sAMAccountType
- sn
- streetAddress
- telephoneNumber
- title
- userAccountControl
- UserPrincipalName
- whenChanged
- whenCreated

在LDAP連線設定中新增自訂屬性後，收集器中要接收的**LDAP屬性**下拉清單將自動包含新屬性。自訂屬性由屬性名稱旁的問號來識別。如果為多個網域新增了相同的屬性，則此屬性在下拉清單中僅列出一次。您可以將滑鼠遊標移到問號上來檢視網域。網域名稱顯示為連結。在點選連結時，則如果之前未新增此網域，它將自動新增到**LDAP帳戶對應**中。

如果在LDAP連線設定中刪除了自訂屬性，請從收集器的對應表手動刪除包含此屬性的行。每次匯入帳戶時，KUMA中的帳戶屬性資訊都會更新。

2. 匯入帳戶。

3. 在收集器的**LDAP對應**表中，定義將KUMA欄位對應到LDAP屬性的規則。

4. 重新啟動收集器。

   重新啟動收集器後，KUMA開始使用帳戶擴充事件。

13. 如果不想使用此LDAP連線，請選取**已停用**核取方塊。

    預設情況下，此核取方塊已清除。

14. 按一下**儲存**按鈕。

LDAP與Active Directory的連線隨即建立並顯示在**依租用戶區分的 LDAP 伺服器整合**視窗中。

儲存連線後，將立即請求來自Active Directory的帳戶資訊，然後以指定的頻率更新。

如果要為一個租用戶同時使用多個LDAP連線，則需要確保每個連線中指示的網域控制站位址都是唯一的。否則，KUMA只允許您啟用其中一個連線。檢查網域控制站位址時，應用程式不會檢查連接埠是否唯一。

建立LDAP伺服器連線的副本

您可以透過複製現有連線來建立LDAP連線。在這種情況下，原始連線的所有設定都會複製到新建立的連線中。

若要複製LDAP連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**整合**下，按一下**LDAP伺服器**。

   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。

3. 選擇要複製LDAP連線的租用戶。

   LDAP 伺服器整合視窗隨即開啟。

4. 選擇相關連線。

5. 在開啟的**連線參數**視窗中，按一下**重複連線**按鈕。

   「新連線」視窗隨即開啟。 copy 這個詞會新增至連線名稱。

6. 請根據需要變更相關設定。

7. 按一下**儲存**按鈕。

新連線隨即建立。

如果要為一個租用戶同時使用多個LDAP連線，則需要確保每個連線中指示的網域控制站位址都是唯一的。否則，KUMA只允許您啟用其中一個連線。檢查網域控制站位址時，應用程式不會檢查連接埠是否唯一。

變更LDAP伺服器連線

若要變更LDAP伺服器連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器**。
   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。
3. 選擇要為其變更LDAP伺服器連線的租用戶。
   LDAP 伺服器整合視窗隨即開啟。
4. 按一下要變更的LDAP伺服器連線。
   包含所選LDAP伺服器連線設定的視窗隨即開啟。
5. 對設定進行必要的更改。
6. 按一下**儲存**按鈕。

LDAP伺服器連線即更改。重新啟動使用LDAP伺服器資料擴充的KUMA服務，以使變更生效。

變更資料更新頻率

KUMA查詢LDAP伺服器以更新帳戶資料。執行時間：

- 建立新連線後立即執行。
- 更改現有連線的設定後立即執行。
- 根據常規排程，每隔幾小時。預設情況下，每12小時。
- 每當使用者建立更新帳戶資料的工作時。

查詢LDAP伺服器時，會在KUMA主控台的**工作管理器**部分中建立一個工作。

若要變更KUMA查詢LDAP伺服器的排程：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**整合**下，按一下**LDAP伺服器**。
   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。

3. 選擇相關租用戶。

   LDAP 伺服器整合視窗隨即開啟。

4. 在**資料刷新間隔**欄位中，以小時為單位指定所需的頻率。預設值是12。

查詢排程已更改。

變更資料儲存週期

如果不再從Active Directory伺服器接收有關這些帳戶的資訊，則預設情況下，接收到的使用者帳戶資料將在KUMA中儲存90天。該時間段之後，資料將被刪除。

刪除KUMA帳戶資料後，新事件和現有事件將不再包含此資訊。帳戶資訊也將在警示中不可用。如果要檢視整個警示儲存期間的帳戶資訊，則必須將帳戶資料儲存期限設定為比警示儲存期限更長。

若要變更帳戶資料的儲存期限：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**整合**下，按一下**LDAP伺服器**。

   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。

3. 選擇相關租用戶。

   LDAP 伺服器整合視窗隨即開啟。

4. 在**資料儲存時間**欄位中，指定您需要儲存從LDAP伺服器收到的資料的天數。

帳戶資料儲存期限已變更。

啟動帳號資料更新工作

建立與Active Directory伺服器的連線後，將自動建立取得帳戶資料的工作。執行時間：

- 建立新連線後立即執行。
- 更改現有連線的設定後立即執行。
- 根據常規排程，每隔幾小時。預設情況下，每12小時。可以更改排程。

可以手動建立帳戶資料更新工作。您可以下載所有連線的資料，也可以下載所需租用戶的一個連線的資料。

若要為租用戶的所有LDAP連線啟動帳戶資料的更新工作：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**整合**下，按一下**LDAP伺服器**。

   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。

3. 選擇相關租用戶。

   LDAP 伺服器整合視窗隨即開啟。

4. 按一下**匯入帳戶**按鈕。

從選定租用戶接收帳戶資料的工作將會新增至KUMA主控台的**工作管理器**部分。

若要為租用戶的LDAP連線啟動帳戶資料更新工作：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**整合**下，按一下**LDAP伺服器**。

   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。

3. 選擇相關租用戶。

   LDAP 伺服器整合視窗隨即開啟。

4. 選擇相關的LDAP伺服器連線。

   連線參數視窗隨即開啟。

5. 按一下**匯入帳戶**按鈕。

從租用戶選取的連線接收帳戶資料的工作將會新增至KUMA主控台的**工作管理器**部分。

刪除LDAP伺服器連線

若要刪除LDAP與Active Directory的連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**整合**下，按一下**LDAP伺服器**。

   依租用戶區分的 LDAP 伺服器整合視窗隨即開啟。

3. 選擇擁有相關LDAP連線的租用戶。

   LDAP 伺服器整合視窗隨即開啟。

4. 選取您要刪除LDAP連線，並點選**刪除**按鈕。

5. 確認刪除連線。

LDAP與Active Directory的連線隨即刪除。

Kaspersky Industrial CyberSecurity for Networks整合

Kaspersky Industrial CyberSecurity for Networks（以下簡稱「KICS for Networks」）是一款旨在保護工業企業基礎設施免受資訊安全威脅並確保其不間斷運作的應用程式。該應用程式透過分析工業網路流量來識別製程參數值的偏差，偵測網路攻擊的跡象，並監控網路裝置的運作和當前狀態。

KICS for Networks 4.0或更高版本可以與KUMA整合。整合設定後，您可以在KUMA中執行下列工作：

- 將資產資訊從KICS for Networks匯入KUMA。
- 將資產狀態變更命令從KUMA傳送到KICS for Networks。

> 與KUMA不同，KICS for Networks將資產稱為裝置。

必須在兩個應用程式中設定KICS for Networks和KUMA的整合：

1. 在KICS for Networks中，您需要建立一個KUMA連接器並儲存此連接器的通訊資料包。
2. 在KUMA中，連接器的通訊資料包用於建立與KICS for Networks的連線。

> 本章節中所述的整合適用於匯入資產資訊。KICS for Networks也可以設定為向KUMA傳送事件。為此，您需要在KICS for Networks中建立SIEM/Syslog連接器，並在KUMA端設定收集器。

在KICS for Networks中設定整合

> 應用程式支援與KICS for Networks 4.0或更新版本整合。

> 建議在結束Process Control規則學習模式後設定KICS for Networks和KUMA的整合。如需詳細資訊，請參閱KICS for Networks說明文件。

在KICS for Networks端，整合組態包括建立*KUMA類型的連接器*。在KICS for Networks中，連接器是專門的應用程式模組，可讓KICS for Networks與接收系統（包括KUMA）交換資料。有關建立連接器的更多詳細資訊，請參閱KICS for Networks的說明文件。

將連接器新增至KICS for Networks時，會自動為該連接器建立*通訊資料包*。這是用於連線到KICS for Networks的加密組態檔案，在KUMA端設定整合時使用。

在KUMA中設定整合

> 建議在結束Process Control規則學習模式後設定KICS for Networks和KUMA的整合。如需詳細資訊，請參閱KICS for Networks說明文件。

若要在KUMA中設定與KICS for Networks的整合：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要為其建立與KICS for Networks整合的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤的**偵測與回應**下，按一下**資產設定**。

4. 在**KICS/KATA匯入**頁簽上，按一下**新增**按鈕。
5. 這將開啟**建立連線**視窗。
6. 若要啟用或停用連線，請開啟或關閉**狀態**切換開關
7. 按一下加號圖示 (+)，然後選擇在KICS for Networks中建立的通訊資料包。
8. 在**通訊資料套件密碼**欄位中，輸入通訊資料包的密碼。
9. 在**API 版本**欄位中，輸入將用於與KICS/KATA通訊的KICS/KATA API版本。預設情況下，使用版本4。
10. 按一下**新增**按鈕。
11. 如果要使用KUMA回應規則更改網路資產的KICS狀態，請開啟**啟用回應操作**切換開關。
12. 按一下**儲存**按鈕。

與KICS for Networks的整合隨即在KUMA中設定，視窗將顯示KICS for Networks連接器將執行的節點的IP位址及其ID。

啟用和停用與KICS for Networks的整合

若要為租用戶啟用或停用KICS for Networks整合：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要匯入KICS/KATA資產的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤的**偵測與回應**下，按一下**資產設定**。
4. 在**KICS/KATA匯入**頁籤上，啟用或停用**狀態**切換開關。
5. 按一下**儲存**按鈕。

變更資料更新頻率

KUMA查詢KICS for Networks以更新其資產資訊。執行時間：

- 建立新整合後立即執行。
- 更改現有整合設定後立即執行。
- 根據常規排程，每隔幾小時。預設情況下，每3小時執行一次。
- 每當使用者建立更新資產資料的工作時。

查詢KICS for Networks時，會在OSMP主控台的**工作管理器**部分中建立一個工作。

若要編輯匯入KICS for Networks資產資訊的排程：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要匯入KICS/KATA資產的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤的**偵測與回應**下，按一下**資產設定**。
4. 在**KICS/KATA匯入**頁籤上，在**匯入間隔（小時）**欄位中，指定OSMP更新KICS/KATA資產資料的時間間隔。

匯入排程已變更。

匯入KICS for Networks資產資訊時的特殊注意事項

匯入資產

資產將根據資產匯入規則匯入。僅匯入具有**已授權**和**未授權**狀態的資產。

KICS for Networks資產由以下參數組合來識別：

- 設定整合的KICS for Networks實例的IP位址。
- KICS for Networks連接器ID用於設定整合。
- 指派給KICS for Networks實例中資產（或「裝置」）的ID。

匯入弱點資訊

匯入資產時，KUMA也會接收KICS for Networks中活動弱點的資訊。如果弱點在KICS for Networks中被標記為「已修復」或「可忽略」，則下次匯入時，有關此弱點的資訊將從KUMA中刪除。

資產弱點資訊會以KICS for Networks的本地化語言顯示在**資產詳細資料**視窗的**弱點**區段中。

在KICS for Networks中，弱點被稱為風險，並分為幾種類型。所有類型的風險都會匯入KUMA。

匯入資料的儲存期限

如果不再從KICS for Networks收到有關先前匯入的資產的資訊，則該資產將在30天後刪除。

變更KICS for Networks資產的狀態

設定整合後，您可以從KUMA更改KICS for Networks資產的狀態。狀態可以自動更改，也可以手動更改。

只有當您在連線到KICS for Networks的設定中啟用了回應時，才能更改資產狀態。

手動更改KICS for Networks資產的狀態

在可用的租用戶中擁有主管理員、管理員和分析師角色的使用者可以手動更改從KICS for Networks匯入的資產的狀態。

若要手動更改KICS for Networks資產狀態：

1. 在主功能表中，轉至**資產管理→資產（裝置）→偵測和響應**。
2. 點按要編輯的資產。

   資產詳細資訊區域在視窗右側開啟。
3. 在**KICS for Networks中的狀態**下拉清單中，選擇您需要指派給KICS for Networks資產的狀態。*已授權*或*未授權*狀態可用。

資產狀態已變更。新狀態顯示在KICS for Networks和KUMA中。

自動變更KICS for Networks資產的狀態

使用回應規則自動變更KICS for Networks資產的狀態。必須將規則新增至關聯器，關聯器將決定觸發這些規則的條件。

與Neurodat SIEM IM整合

Neurodat SIEM IM是一個資訊安全監控系統。

您可以設定將KUMA事件匯出到Neurodat SIEM IM。根據傳入事件和關聯規則，Neurodat SIEM IM會自動產生資訊安全事件。

若要設定與Neurodat SIEM IM的整合：

1. 使用具有管理員權限的帳戶透過SSH連線到Neurodat SIEM IM伺服器。
2. 建立/opt/apache-tomcat-<伺服器版本>/conf/neurodat/soz_settings.properties組態檔的備份副本。

3. 在/opt/apache-tomcat-<伺服器版本>/conf/neurodat/soz_settings.properties組態檔中，如下編輯以下設定：

   - `kuma.on=true`
     此設定是Neurodat SIEM IM與KUMA互動的屬性。
   - `job_kuma=com.cbi.soz.server.utils.scheduler.KumaIncidentsJob`
   - `jobDelay_kuma=5000`
   - `jobPeriod_kuma=60000`

4. 儲存組態檔的更改。

5. 執行以下命令重新啟動tomcat服務：

   ```
   sudo systemctl restart tomcat
   ```

6. 在KUMA中取得使用者的權杖。為此：

   a. 在主功能表中，轉至**設定→API權杖**。
   這將開啟**API權杖**視窗。

   b. 按一下**新增令牌**按鈕。
   新增權杖視窗隨即開啟。

   c. 請根據需要設定權杖到期期：

      - 選取**無到期日**核取方塊。
      - 在**到期日**欄位中，使用日曆指定建立的權杖的到期日和時間。

   d. 點選**產生**按鈕。
   使用者詳細資訊區域中將顯示包含自動產生權杖的**權杖**欄位。請複製該權杖。
   關閉視窗後，權杖將不再顯示。如果您在關閉視窗前未複製權杖，則必須產生新的權杖。

   e. 按一下**儲存**按鈕。

7. 使用「管理員」帳戶或其他具有您正在設定的組織的管理員角色或所有組織的管理員角色的帳戶登入Neurodat SIEM IM。

8. 在**管理 → 組織結構**功能表項目中，選擇或建立要從KUMA接收事件的組織。

9. 在組織表單中，執行以下操作：

   a. 選取**設定與KUMA的整合**核取方塊。

   b. 在**KUMA IP 位址和連接埠**欄位中，指定 KUMA API 位址，例如 `https://192.168.58.27:7223/api/v1/`。

   c. 在**KUMA API金鑰**欄位中，指定在步驟6中取得的使用者權杖。

   d. 保存組織資訊。

與KUMA的整合隨即設定。

Neurodat SIEM IM測試存取KUMA，如果成功，則會顯示一條訊息，提示已準備好從KUMA接收資料。

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform（以下也稱為「KASAP」）是一個線上學習平台，讓使用者能夠在日常工作中學習資訊安全規則及相關威脅，並透過實際案例進行練習。

KASAP可與KUMA整合。設定整合後，您可在KUMA中執行下列工作：

- 更改使用者學習群組。
- 檢視使用者參加的課程及其獲得的憑證資訊。

KASAP與KUMA的整合包括設定API連線至KASAP。此操作在兩個解決方案中進行：

1. 在KASAP中，建立授權權杖並取得API請求的位址。
2. 在KUMA中，指定KASAP中API請求的位址，新增API請求的授權權杖，並指定KASAP管理員的電子郵件地址以接收通知。

在KASAP中建立權杖並取得API請求的連結

為了獲得授權，從KUMA到KASAP的API請求必須由KASAP中建立的權杖簽署。只有公司管理員可以建立權杖。

建立權杖

若要建立權杖：

1. 登入KASAP網頁介面。
2. 在**控制面板**區段中，點選**匯入和同步**，然後開啟**Open API**索引標籤。
3. 點選**新建權杖**按鈕，然後在開啟的視窗中選擇用於整合的API方法：
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
4. 點選**產生令牌**按鈕。
5. 複製權杖並以任何方便的方式儲存。在KUMA中設定整合需要此權杖。

權杖不會以開放形式儲存在KASAP系統中。關閉**取得權杖**視窗後，您將無法查看該權杖。如果您關閉視窗而不複製權杖，則需要再次按一下**新建權杖**按鈕，以便系統產生新的權杖。

簽發的權杖有效期為12個月。超過此期限後，權杖將被撤銷。如果6個月內未使用，簽發的權杖也將被撤銷。

取得API請求的連結

若要取得KASAP中用於API請求的連結：

1. 登入KASAP平台主控台。
2. 在**控制面板**區段中，點選**匯入和同步**，然後開啟**Open API**索引標籤。
3. 使用Open API存取KASAP的連結位於視窗底部。複製連結並以任何方便的方式儲存。在KUMA中設定整合需要此連結。

在KUMA中設定整合

若要設定KUMA與KASAP的整合：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟**KUMA設定**視窗。
2. 在**整合**下，點擊**Kaspersky Automated Security Awareness Platform**。
   Kaspersky Automated Security Awareness Platform視窗將開啟。
3. 在**密鑰**欄位中，按一下加號圖示 (+)，透過輸入從KASAP收到的權杖來建立**權杖**的密鑰：
   a. 在**名稱**欄位中，輸入密鑰的名稱。必須包含1至255個Unicode字元。
   b. 在**權杖**欄位中，輸入用於向KASAP發出API請求的授權權杖。
   c. 根據需要在**描述**欄位中新增密鑰描述。
   d. 按一下**儲存**按鈕。
4. 在**KASAP Open API URL**欄位中，指定KASAP用於API請求的位址。
5. 在**KASAP管理員電子郵件**欄位中，指定KASAP管理員的電子郵件地址，當使用KUMA將使用者新增至學習群組時，該管理員將收到通知。
6. 請根據需要在**代理**下拉清單中選擇用於連線到KASAP的代理伺服器資源。
7. 若要停用或啟用與KASAP的整合，請選取或清除**已停用**核取方塊。
8. 按一下**儲存**按鈕。

與KASAP的整合隨即在KUMA中設定。查看有關警示和事件的資訊時，您可以選擇關聯使用者來查看他們參加過的學習課程並更改他們的學習群組。

檢視KASAP使用者資訊並變更學習群組

設定KASAP和KUMA的整合後，當您檢視有關關聯使用者的資料時，來自KASAP的以下資訊將在警示和事件中可用：

- 使用者所屬的學習群組。
- 使用者通過的培訓。
- 計劃的培訓和當前進度。
- 收到的憑證。

若要從KASAP檢視有關使用者的資料：

1. 在OSMP主控台的**警示**或**事件**部分中，選擇相關的警示或事件。
2. 在**相關使用者**部分中，按一下所需的帳戶。
   帳戶詳細資訊視窗在螢幕右側開啟。
3. 選擇**KASAP課程詳細資訊**頁籤。

   此視窗顯示來自KASAP的有關使用者的資訊。

您可在KASAP中變更使用者的學習群組。

若要在KASAP中變更使用者學習群組：

1. 在OSMP主控台的**警示**或**事件**部分中，選擇相關的警示或事件。
2. 在**相關使用者**部分中，按一下所需的帳戶。
   帳戶詳細資訊視窗在螢幕右側開啟。
3. 在**指派KASAP群組**下拉清單中，選擇要將使用者指派的KASAP學習群組。
4. 點選**套用**。

   使用者將移至所選的KASAP群組，KASAP公司管理員將收到學習群組變更的通知，並重新計算所選學習群組的學習計畫。

有關學習群組以及如何開始使用的詳細資訊，請參閱KASAP 說明文件。

向Telegram傳送通知

此整合為範例，可能需要根據使用的版本及基礎架構的具體情況進行額外設定。
進階技術支援的條款與條件不適用於此整合；支援請求的處理不保證回應時間。

您可以設定在觸發KUMA關聯規則時向Telegram傳送通知。這可以減少對威脅的回應時間，並在必要時讓更多人了解情況。

設定Telegram通知涉及以下步驟：

1. **建立和設定Telegram機器人**
   一個特殊的機器人會傳送有關觸發的關聯規則的通知。它可以向私人或群組Telegram聊天傳送通知。
2. **建立用於傳送通知的指令碼**
   您必須建立指令碼並將其儲存在安裝了關聯器的伺服器上。
3. **在KUMA中設定通知**
   設定一個啟動指令碼傳送通知的KUMA回應規則，並將此規則新增至關聯器。

建立和設定Telegram機器人

若建立和設定Telegram機器人：

1. 在Telegram應用程式中，找到BotFather機器人並開始聊天。
2. 在聊天中，點選**開始**。
3. 使用以下命令建立一個新機器人：
   `/newbot`
4. 輸入機器人的名稱。
5. 輸入機器人的登入名稱。
   機器人隨即建立。您會收到一個類似於t.me/<bot login>的聊天連結和用於聯絡機器人的權杖。
6. 如果要在群組聊天中使用機器人，而不是在私人訊息中使用，請編輯隱私權設定：
   a. 在BotFather聊天中，輸入以下命令：
      `/mybots`
   b. 在清單中選取相關的機器人。
   c. 點擊**機器人設定→群組隱私權**，然後選擇**關閉**。
      機器人現在可以向群組聊天傳送訊息。
7. 要與您建立的機器人開始聊天，請使用您在步驟5中獲得的 t.me/<botlogin>連結，然後點選**開始**。
8. 如果您希望機器人向使用者傳送私人訊息：
   a. 在與機器人的聊天中，傳送任何訊息。
   b. 點選https://t.me/getmyid_bot連結，並點擊**開始**。
   c. 回應包含 `Current chat ID`。您需要此值來設定訊息的傳送功能。

9. 如果您希望機器人向群組聊天傳送訊息：

   a. 請將https://t.me/getmyid_bot新增到群組聊天中，以便接收來自KUMA的通知。

      機器人會向群組聊天傳送訊息，訊息內容包含 `Current chat ID` 值。您需要此值來設定訊息的傳送功能。

   b. 請從群組中移除該機器人。

10. 透過機器人傳送測試訊息。為此，請將以下連結貼到瀏覽器的位址列中：

    `https://api.telegram.org/bot<token>/sendMessage?chat_id=<chat_id>&text=test`

    其中 `<token>` 為在第 5 步取得的值，而 `<chat_id>` 為在第 8 步或第 9 步取得的值。

因此，測試訊息應該出現在個人或群聊中，瀏覽器回應中的JSON應該不發生錯誤。

建立傳送通知的指令碼

若要建立指令碼：

1. 在安裝了關聯器的伺服器的主控台中，建立一個指令碼檔案，並新增以下行：

   ```
   #!/bin/bash
   set -eu
   CHAT_ID=<Current chat ID value obtained at step 8 or 9 of the Telegram bot setup instructions>
   TG_TOKEN=<token value obtained at step 5 of the Telegram bot setup instructions>
   RULE=$1
   TEXT="<b>$RULE</b> rule triggered"
   curl --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
   ```

   如果關聯器伺服器無法存取網際網路，您可以使用代理伺服器：

   ```
   #!/bin/bash
   set -eu
   CHAT_ID=<Current chat ID value obtained at step 8 or 9 of the Telegram bot setup instructions>
   TG_TOKEN=<token value obtained at step 5 of the Telegram bot setup instructions>
   RULE=$1
   TEXT="<b>$RULE</b> rule triggered."
   PROXY=<代理伺服器的位址與連接埠>
   curl --proxy $PROXY --data-urlencode "chat_id=$CHAT_ID" --data-urlencode "text=$TEXT" --data-urlencode "parse_mode=HTML" https://api.telegram.org/bot$TG_TOKEN/sendMessage
   ```

2. 將指令碼儲存至關聯器目錄/opt/kaspersky/kuma/correlator/<必須回應事件的關聯器ID>/scripts/。

   有關取得關聯器ID的資訊，請參閱取得服務識別碼部分。

3. 使「kuma」使用者成為檔案的擁有者並授予執行權限：

   ```
   chown kuma:kuma /opt/kaspersky/kuma/correlator/<必須回應的關聯器ID>/scripts/<指令碼名稱>.sh
   chmod +x /opt/kaspersky/kuma/correlator/<必須回應的關聯器ID>/scripts/<指令碼名稱>.sh
   ```

在 KUMA 中設定通知傳送

若要設定向Telegram傳送KUMA通知：

1. 建立回應規則：
   a. 在主功能表中，前往**監控 → 資源與服務 → 回應規則**，然後按一下**新增回應規則**。
   b. 這將開啟**建立回應規則**視窗；在該視窗中，在**名稱**欄位中輸入規則的名稱。
   c. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。
   d. 在**類型**下拉清單中，選擇**執行指令碼**。
   e. 在**指令碼名稱**欄位中，輸入指令碼的名稱。
   f. 在**指令碼引數**欄位中，輸入 `{{.Name}}`。
   這將關聯事件的名稱作為指令碼的引數傳遞。
   g. 按一下**儲存**按鈕。
2. 將回應規則新增至關聯器：
   a. 在主功能表中，轉到**監控→資源與服務→關聯器**，然後選擇關聯器，將建立用於傳送通知的指令碼放在其資料夾中。
   b. 在步驟樹中，選擇**回應規則**。
   c. 按一下**新增**按鈕。
   d. 在**回應規則**下拉清單中，選擇在本說明的第1步驟中新增的規則。
   e. 在步驟樹中，選擇**安裝驗證**。
   f. 點選**儲存並重新啟動服務**按鈕。
   g. 按一下**儲存**按鈕。

將有關觸發的KUMA規則的通知傳送至Telegram隨即設定。

UserGate整合

此整合為範例，可能需要根據使用的版本及基礎架構的具體情況進行額外設定。
進階技術支援的條款與條件不適用於此整合；支援請求的處理不保證回應時間。

UserGate是一個網路基礎設施安全解決方案，可以保護個人資訊免受外部入侵、未經授權的存取、病毒和惡意軟體的風險。

與 UserGate 整合允許在觸發KUMA回應規則時自動封鎖來自IP位址、URL或網域的威脅。

設定整合涉及以下步驟：

1. 在UserGate中設定整合
2. 準備回應規則的指令碼
3. 設定KUMA回應規則

在UserGate中設定整合

若要在UserGate中設定整合：

1. 使用管理員帳戶連線到UserGate網頁介面。
2. 轉至**UserGate →管理員→管理員設定檔**，然後按一下**新增**。
3. 在**設定檔設定**視窗中，指定設定檔名稱，例如，`API`。
4. 在**API權限**頁籤上，為下列物件新增讀寫權限：
   - 內容
   - 核心
   - 防火牆
   - nlists
5. 按一下**儲存**按鈕。
6. 在**UserGate →管理員**部分中，按一下**新增→新增本機管理員**。
7. 在**管理員內容**視窗中，指定管理員的登入名稱和密碼。
   在**管理員設定檔**欄位中，選擇在步驟3中建立的設定檔。
8. 按一下**儲存**按鈕。
9. 在瀏覽器的網址列中，在 UserGate 的位址與連接埠後新增 `?features=zone-xml-rpc`，然後按 **ENTER** 鍵。
10. 轉至**網路→區域**部分，對於要用於API互動的介面區域，轉至**存取控制**頁籤並選取**管理服務的XML-RPC**旁的核取方塊。
    如有必要，您可以將KUMA關聯器的IP位址新增到允許的位址清單中，其關聯規則必須在UserGate中觸發封鎖。
11. 按一下**儲存**按鈕。

準備與UserGate整合的指令碼

若要準備使用的指令碼：

1. 複製要觸發UserGate 中URL、IP位址或網域封鎖的關聯器的ID：

   a. 在主選單中，前往 **監控 → 資源與服務 → 作用中的服務**。

   b. 選取要取得其ID的關聯器旁的核取方塊，然後按一下**複製ID**。

   關聯器ID將被複製到剪貼簿。

2. 下載指令碼：

   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. 開啟指令碼檔案，在**輸入UserGate參數**部分的**登入**和**密碼**參數中，指定在UserGate中設定整合的步驟7中所建立的UserGate管理員帳戶的憑證。

4. 將下載的指令碼放在KUMA關聯器伺服器上的以下路徑：/opt/kaspersky/kuma/correlator/<第1步中的關聯器ID>/scripts/。

5. 透過SSH連線至關聯器伺服器並設定步驟4中的路徑:

   ```
   cd /opt/kaspersky/kuma/correlator/< 第1步中的關聯器ID >/scripts/
   ```

6. 執行以下命令：

   ```
   chmod +x ug.py && chown kuma:kuma ug.py
   ```

指令碼已準備就緒。

設定與UserGate整合的回應規則

若要設定回應規則：

1. 建立回應規則：

   a. 在主功能表中，前往**監控 → 資源與服務 → 回應規則**，然後按一下**新增回應規則**。

   b. 這將開啟**建立回應規則**視窗；在該視窗中，在**名稱**欄位中輸入規則的名稱。

   c. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。

   d. 在**類型**下拉清單中，選擇**執行指令碼**。

   e. 在**指令碼名稱**欄位中，輸入指令碼的名稱。`ug.py`。

f. 在**指令碼引數**欄位中，指定：

- 根據被封鎖物件的類型執行以下某項操作：
  - `blockurl`，透過 URL 封鎖存取
  - `blockip`，透過 IP 位址封鎖存取
  - `blockdomain`，透過網域名稱封鎖存取
- `-i {{<` 根據操作類型，須從中取得被封鎖物件值的 `KUMA` 欄位 `>}}`

```
範例：
blockurl -i {{.RequetstUrl}}
```

g. 在**條件**部分，新增與關聯規則相對應的條件，這些條件在觸發時需要在UserGate中封鎖。

h. 按一下**儲存**按鈕。

2. 將回應規則新增至關聯器：

a. 在主選單中，前往 **監控 → 資源與服務 → 關聯器**，選擇需要執行回應且其目錄中已放置指令碼的關聯器。

b. 在步驟樹中，選擇**回應規則**。

c. 按一下**新增**按鈕。

d. 在**回應規則**下拉清單中，選擇在本說明的第1步驟中新增的規則。

e. 在步驟樹中，選擇**安裝驗證**。

f. 點選**儲存並重新載入服務** 。

g. 按一下**儲存**按鈕。

回應規則已連結到關聯器並準備就緒。

與Kaspersky Web Traffic Security整合

此整合為範例，可能需要根據使用的版本及基礎架構的具體情況進行額外設定。
進階技術支援的條款與條件不適用於此整合；支援請求的處理不保證回應時間。

您可以設定與Kaspersky Web Traffic Security網頁流量分析和篩選系統（以下也稱為「KWTS」）的整合。

設定整合涉及建立允許執行KWTS工作的KUMA回應規則。必須提前在 KWTS網頁介面中建立工作。

設定整合涉及以下步驟：

1. 在KWTS中設定整合
2. 準備用於回應規則的指令碼
3. 設定KUMA回應規則

在KWTS中設定整合

若要在KWTS中準備整合：

1. 使用管理員帳戶連線到 KWTS網頁介面，並建立一個具有檢視和建立/編輯規則權限的角色。
   有關建立角色的更多詳細資訊，請參閱*Kaspersky Web Traffic Security的說明*。
2. 將建立的角色指派給具有NTML身分驗證的使用者。
   您可以改用本機管理員帳號。
3. 在**規則**部分，轉至**存取**頁籤，然後按一下**新增規則**。
4. 在**操作**下拉清單中，選擇**封鎖** 。
5. 在**流量篩選**下拉清單中，選擇**URL**值，然後在右側的欄位中輸入不存在或已知的惡意位址。
6. 在**名稱**欄位中，輸入規則的名稱。
7. 使用**狀態**切換開關啟用規則。
8. 按一下**新增**按鈕。
9. 在KWTS網頁介面中，開啟剛剛建立的規則。
10. 記下瀏覽器網址列中頁面位址末端顯示的ID值。
    在KUMA中設定回應規則時必須使用此值。

整合在KWTS端準備就緒。

準備用於與KWTS整合的指令碼

若要準備使用的指令碼：

1. 複製要觸發KWTS中URL、IP位址或網域名稱封鎖的關聯規則的關聯器ID：
   a. 在主選單中，前往 **監控 → 資源與服務 → 作用中的服務**。
   b. 選取要取得其ID的關聯器旁的核取方塊，然後按一下**複製ID**。
      關聯器ID將被複製到剪貼簿。
2. 下載指令碼與程式庫：
   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/
3. 將下載的指令碼放在 KUMA 關聯器伺服器上的以下路徑：/opt/kaspersky/kuma/correlator/<第 1 步中的關聯器 ID>/scripts/。
4. 透過SSH連線至關聯器伺服器並設定步驟3中的路徑:
   `cd /opt/kaspersky/kuma/correlator/<第 1 步中的關聯器 ID>/scripts/`

5. 執行以下命令：

```
chmod +x kwts.py kwtsWebApiV6.py && chown kuma:kuma kwts.py kwtsWebApiV6.py
```

指令碼已準備就緒。

設定用於與KWTS整合的回應規則

若要設定回應規則：

1. 建立回應規則：
   a. 在主功能表中，前往**監控** → **資源與服務** → **回應規則**，然後按一下**新增回應規則**。
   b. 這將開啟**建立回應規則**視窗；在該視窗中，在**名稱**欄位中輸入規則的名稱。
   c. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。
   d. 在**類型**下拉清單中，選擇**執行指令碼**。
   e. 在**指令碼名稱**欄位中，輸入指令碼的名稱 kwts.py。
   f. 在**指令碼引數**欄位中，指定：
      - `--host` — KWTS 伺服器的位址。
      - `--username` — 在 KWTS 中建立的使用者帳戶的名稱或本機管理員的名稱。
      - `--password` — KWTS 使用者帳戶密碼。
      - `--rule_id` — 在 KWTS 中建立的規則 ID。
      - 根據被封鎖物件的類型指定以下其中一個選項：
        - `--url` — 指定要從中取得 URL 的 KUMA 事件欄位，例如，`{{.RequestUrl}}`。
        - `--ip` — 指定要從中取得 IP 位址的 KUMA 事件欄位，例如，`{{.DestinationAddress}}`。
        - `--domain` — 指定要從中取得網域名稱的 KUMA 事件欄位，例如，`{{.DestinationHostName}}`。
      - `--ntlm` — 若 KWTS 使用者是使用 NTLM 身分驗證建立的，請指定此選項。

        範例：
        ```
        --host <address> --username <user> --password <pass> --rule_id <id> --url {{.RequestUrl}}
        ```
   g. 在**條件**部分，新增與關聯規則對應的條件，這些條件在觸發時需要在KWTS中封鎖。
   h. 按一下**儲存**按鈕。
2. 將回應規則新增至關聯器：
   a. 在主選單中，前往 **監控** → **資源與服務** → **關聯器**，選擇需要執行回應且其目錄中已放置指令碼的關聯器。
   b. 在步驟樹中，選擇**回應規則**。

c. 按一下**新增**按鈕。

d. 在**回應規則**下拉清單中，選擇在本說明的第1步驟中新增的規則。

e. 在步驟樹中，選擇**安裝驗證**。

f. 點選**儲存並重新載入服務** 。

g. 按一下**儲存**按鈕。

回應規則已連結到關聯器並準備就緒。

與Kaspersky Secure Mail Gateway整合

此整合為範例，可能需要根據使用的版本及基礎架構的具體情況進行額外設定。
進階技術支援的條款與條件不適用於此整合；支援請求的處理不保證回應時間。

您可以設定與Kaspersky Secure Mail Gateway郵件流量分析和篩選系統（以下也稱為「KSMG」）的整合。

設定整合涉及建立允許執行KSMG工作的KUMA回應規則。工作必須提前在KSMG網頁介面中建立。

設定整合涉及以下步驟：

1. 在KSMG中設定整合
2. 準備回應規則的指令碼
3. **設定KUMA回應規則**

在KSMG中設定整合

若要在KSMG中準備整合：

1. 使用管理員帳號連線到KSMG網路介面並建立具有檢視和建立/編輯規則權限的角色。
   有關建立角色的更多詳細資訊，請參閱*Kaspersky Secure Mail Gateway說明*。
2. 將建立的角色指派給具有NTML身分驗證的使用者。
   您可以使用「管理員」本機管理員帳號。
3. 在**規則**部分中，按一下**建立**。
4. 在左窗格中，選取**一般**部分。
5. 使用**狀態**切換開關啟用規則。
6. 在**規則名稱**欄位，指定新規則的名稱。
7. 在**模式**下，選擇符合此規則條件的其中一個郵件處理選項。

8. 在**電子郵件地址**頁籤上的**寄件者**下，輸入不存在或已知的惡意寄件者地址。

9. 在**電子郵件地址**頁籤上的**收件者**下，指定相關收件者或使用「*」字元選擇所有收件者。

10. 按一下**儲存**按鈕。

11. 在KSMG網路介面中，開啟您剛剛建立的規則。

12. 記下瀏覽器網址列中頁面位址末端顯示的ID值。
    在KUMA中設定回應規則時必須使用此值。

整合在KSMG端準備就緒。

準備用於與KSMG整合的指令碼

若要準備使用的指令碼：

1. 複製其關聯規則必須觸發KSMG中郵件寄件者IP位址或電子郵件位址封鎖的關聯器ID：

   a. 在主選單中，前往 **監控 → 資源與服務 → 作用中的服務**。

   b. 選取要取得其ID的關聯器旁的核取方塊，然後按一下**複製ID**。
      關聯器ID將被複製到剪貼簿。

2. 下載指令碼與程式庫：
   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/

3. 將下載的指令碼放在 KUMA 關聯器伺服器上的以下路徑：/opt/kaspersky/kuma/correlator/<第 1 步中的關聯器 ID>/scripts/。

4. 透過SSH連線至關聯器伺服器並設定步驟3中的路徑:
   `cd /opt/kaspersky/kuma/correlator/<第 1 步中的關聯器 ID>/scripts/`

5. 執行以下命令：
   `chmod +x ksmg.py ksmgWebApiV2.py && chown kuma:kuma ksmg.py ksmgWebApiV2.py`

指令碼已準備就緒。

從RedCheck匯入資產資訊

此整合為範例，可能需要根據使用的版本及基礎架構的具體情況進行額外設定。
進階技術支援的條款與條件不適用於此整合；支援請求的處理不保證回應時間。

RedCheck是一個用於監控和管理組織資訊安全的系統。

您可以將RedCheck網路裝置掃描報告中的資產資訊匯入KUMA。

匯入操作可以從簡單的「弱點」和「清查」報告中以CSV格式進行，並按主機分組。

匯入的資產將顯示在OSMP主控台的**資產管理→資產（裝置）→偵測和回應**部分。您可以根據需要編輯資產的設定。

資料透過API使用redcheck-tool.py公用程式匯入。該公用程式需要Python 3.6或更高版本以及以下程式庫：

- csv
- re
- json
- 請求
- argparse
- sys

若要從RedCheck報告匯入資產資訊：

1. 請以CSV格式在RedCheck中產生網路資產掃描報告，並將報告檔案複製到指令碼所在的伺服器。
   有關掃描工作和輸出檔案格式的更多詳細資訊，請參閱RedCheck說明文件。
2. 使用權杖建立一個檔案，用於訪問KUMA REST API。
   建立權杖的帳戶必須符合以下要求：
   - 管理員或分析師角色。
   - 存取將匯入資產的租用戶。
   - 使用API請求的權限：GET /assets、GET /tenants 、POST/assets/import。
3. 下載指令碼：
   https://box.kaspersky.com/d/2dfd1d677c7547a7ac1e/
4. 將redcheck-tool.py工具複製到託管KUMA Core的伺服器，並使該工具的檔案可執行：
   `chmod +x <redcheck-tool.py 檔案的路徑>`
5. 執行redcheck-tool.py公用程式：
   `python3 redcheck-tool.py --kuma-rest <KUMA REST API 伺服器的位址與連接埠> --token <API 權杖> --tenant <資產必須放置在其中的租用戶名稱> --vuln-report <「Vulnerabilities」報告檔案的完整路徑> --inventory-report <「Inventory」報告檔案的完整路徑>`

   ```
   範例：
   python3 --kuma-rest kuma.example.com:7223 --token 949fc03d97bad5d04b6e231c68be54fb --tenant Main --vuln-report
   /home/user/vuln.csv --inventory-report /home/user/inventory.csv
   ```

   可為匯入操作使用額外的旗標與命令。例如，`-v` 命令會顯示有關已接收資產的詳盡報告。「Redcheck-tool.py的標誌和命令」表中提供了可用標誌和命令的詳細說明。亦可使用 `--help` 命令來檢視可用旗標與命令的相關資訊。

資產資訊從RedCheck報告匯入到KUMA。主控台顯示有關新資產和更新資產數量的資訊。

範例：

```
inventory has been imported for 2 host(s)
software has been imported for 5 host(s)
vulnerabilities has been imported for 4 host(s)
```

擴充匯入資訊範例：

```
[inventory import] Host: localhost Code: 200 Response: {'insertedIDs': {'0': '52ca11c6-a0e6-4dfd-8ef9-
bf58189340f8'}, 'updatedCount': 0, 'errors': []}
[inventory import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {'0': '1583e552-5137-4164-92e0-
01e60fb6edb0'}, 'updatedCount': 0, 'errors': []}
[software import][error] Host: localhost Skipped asset with FQDN localhost or IP 127.0.0.1
[software import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.2 Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.1 Code: 200 Response: {'insertedIDs': {'0': '0628f683-c20c-4107-abf3-
d837b3dbbf01'}, 'updatedCount': 0, 'errors': []}
[vulnerabilities import] Host: localhost Code: 200 Response: {'insertedIDs': {}, 'updatedCount': 1, 'errors': []}
[vulnerabilities import] Host: 10.0.0.3 Code: 200 Response: {'insertedIDs': {'0': 'ed01e0a8-dcb0-4609-ab2b-
91e50092555d'}, 'updatedCount': 0, 'errors': []}
inventory has been imported for 2 host(s)
software has been imported for 1 host(s)
vulnerabilities has been imported for 4 host(s)
```

匯入資產時，該工具的運作方式如下：

- KUMA會覆蓋透過API匯入的資產資料，並刪除其已解決弱點的資訊。
- KUMA會略過含有無效資料的資產。

redcheck-tool.py的旗標和命令

標記和命令	強制	描述
`--kuma-rest <KUMA 伺服器的位址和連接埠>`	是	預設情況下，連接埠7223用於API請求。您可以根據需要變更連接埠。
`--token <token>`	是	選項的值必須僅包含權杖。 必須為正在為其產生API權杖的使用者帳戶指派管理員或分析師角色。
`--tenant <租用戶名稱>`	是	您要從 RedCheck 報告匯入資產的 KUMA 租用戶名稱。
`--vuln-report <「弱點」報告的完整路徑>`	是	「弱點」報告檔案，格式為CSV。
`--inventory-report <「清查」報告檔案的完整路徑>`	否	「清查」報告檔案，格式為CSV。
`-v`	否	顯示有關匯入資產的擴充資訊。

可能發生的錯誤

錯誤訊息	描述
未找到租用戶%w	未找到租用戶名稱。
租用戶搜尋錯誤：意外狀態碼：%d	搜尋租用戶時收到意外的HTTP回應代碼。
資產搜尋錯誤：意外狀態碼：%d	搜尋資產時收到意外HTTP回應代碼。
[%w import][error]主機：%w略過了FQDNlocalhost或IP 127.0.0.1的資產	匯入清查/弱點資訊時，略過了主機cfqdn=localhost或ip=127.0.0.1。

設定接收Sendmail事件

您可以在KUMA SIEM系統中設定接收Sendmail郵件代理事件。

設定接收事件包含以下步驟：

1. 設定Sendmail日誌記錄。
2. 設定事件來源伺服器。
3. 建立KUMA收集器。
   若要接收Sendmail事件，請在收集器安裝精靈中使用下列值：
   - 在**事件解析**步驟中，選擇**[OOTB] Sendmail syslog**標準化器。
   - 在**傳輸**步驟中，選擇**tcp**或**udp**連接器類型。
4. 安裝KUMA收集器。
5. 驗證KUMA收集器接收Sendmail事件的情況
   您可以在OSMP主控台的搜尋相關事件部分驗證Sendmail事件來源伺服器是否設定正確。

設定Sendmail日誌記錄

預設情況下，Sendmail系統事件會記錄到syslog中。

若要確保日誌設定正確：

1. 透過SSH連線到安裝了Sendmail系統的伺服器。
2. 執行以下命令：
   `cat /etc/rsyslog.d/50-default.conf`
   該命令應傳回以下字串：
   `mail.* -/var/log/mail.log`

如果日誌記錄設定正確，您可以繼續設定Sendmail事件的匯出。

設定匯出Sendmail事件

事件透過rsyslog服務從Sendmail郵件代理伺服器傳送到KUMA收集器。

若要設定將Sendmail事件傳輸到收集器：

1. 使用具有管理員權限的帳戶連線到安裝了Sendmail的伺服器。
2. 在/etc/rsyslog.d/目錄中，建立Sendmail-to-siem.conf檔案並新增下列行：
   `If $programname contains 'sendmail' then @<收集器的 IP 位址>:<收集器的連接埠>`

   範例：
   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   若要透過TCP傳送事件，檔案的內容必須如下：
   `If $programname contains 'sendmail' then @@<收集器的 IP 位址>:<收集器的連接埠>`
3. 建立/etc/rsyslog.conf檔案的備份副本。

4. 將以下行新增至/etc/rsyslog.conf組態檔：

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. 儲存您的變更。

6. 重新啟動rsyslog服務。

   ```
   sudo systemctl restart rsyslog.service
   ```

設定與外部SIEM系統的集成

OSMP可以使用Syslog協定，將應用程式網頁介面中的警示和使用者操作資訊傳送到您企業已使用的外部SIEM系統。

外部SIEM系統可以是：

- Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- 第三方SIEM系統

若要傳輸資料，您需要根據所選的協定，建立tcp或udp類型的目標。透過TCP傳輸資料時，可以使用TLS加密。為此，請在建立目標時指定TLS憑證。

若要上傳用於加密與SIEM系統連線的TLS憑證：

1. 在建立tcp類型目標的視窗中，選取**進階設定**標籤。
2. 在**TLS模式**欄位中，選取以下其中一個值：

   - **自訂CA**

     如果要上傳憑證文件，請選擇此項目。在**自訂CA**欄位中，指定包含憑證檔案的密鑰。您可以選擇現有密鑰或建立新密鑰。若要建立密鑰，請從清單中選擇**新建**，然後在顯示的視窗中上傳TLS憑證。

   - **自訂PFX**

     如果您想上傳PFX格式的憑證文件，請選擇此項目。在**PFX密鑰**欄位中，指定包含憑證檔案的密鑰。您可以選擇現有密鑰或建立新密鑰。若要建立密鑰，請從清單中選擇**新建**，然後在顯示的視窗中上傳包含TLS憑證的PFX檔案。

3. 根據需要，管理其他目標設定。按一下**建立**按鈕。

上傳的TLS憑證將用於與SIEM系統建立加密連線。

管理KUMA

本節說明 KUMA 的一般設定。

設定KUMA Core

若要設定 KUMA Core 設定：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**其他**下，按一下**常見**。

   這會開啟**常見**視窗。

3. 在**Core設定**區域中，指定下方設定：

   - 使用**偵錯**切換開關來啟用或停用系統操作日誌記錄（偵錯模式）。預設情況下，切換開關是關閉的。
   - 如果啟用偵錯模式，您可以使用**傾印 KSC HTTP 流量**切換開關來啟用或停用轉儲卡巴斯基安全管理中心的HTTP流量的功能。
   - 如果啟用了卡巴斯基安全管理中心的HTTP流量轉儲，您可以使用**定期轉儲**切換開關來啟用或停用將卡巴斯基安全管理中心的HTTP請求和回應轉儲到事件日誌的功能。

     選取**啟用定期轉儲**核取方塊後，請在**轉儲設定**下指定轉儲設定。
   - 在**每週起始日**下拉清單中，選擇要用於整個KUMA實例的一週的第一天。在KUMA的所有部分中選擇期間和指定時間間隔時，會套用選定的值。預設值為**星期一**。只有具有主管理員角色的使用者才能修改此設定。選定的值儲存在KUMA Core設定中。
   - 在**KUMA 資源當地語系化**下拉清單中，選擇從儲存庫匯入之KUMA資源的本地化語言。預設語言為英文。如果變更此設定，則只會以所選語言匯入新的KUMA資源。如果您先前曾以其他語言匯入資源，這些資源將保持不變。若要變更先前匯入資源的語言，您需要從儲存庫重新匯入這些資源。

     KUMA 資源當地語系化設定與 Kaspersky Next XDR Expert 語言設定無關。您可以在這些設定中選擇不同的本地化語言。在此情況下，例如，資源表中文字的語言可能與介面的本地化語言不同。

     KUMA 資源當地語系化設定不會影響手動建立的資源。
   - 如有必要，請按一下**重新簽發**按鈕以重新簽發AI服務憑證和內部CA憑證。

     > 重新簽發AI服務憑證後，您必須手動重新啟動所有服務。若要套用新的AI服務憑證，您必須重新啟動KUMA Core。

4. 如果您不想使用自簽發KUMA憑證，請在**外部 TLS 配對**部分上傳TLS對的憑證和金鑰。

   點選**更新憑證**按鈕，即可更新TLS對的憑證。

5. 在**Core 內容**下，指定以下設定：

   - 選取**SQLite 壓縮**核取方塊，並指定磁碟空間大小（以GB為單位）。這樣可以減少資料庫大小，從而更有效地利用磁碟空間。

     預設情況下，此核取方塊處於選取狀態，磁碟空間設定為10,000GB。
   - 在**啟動標記**欄位中，指定一個適用的標籤。

- 在**警示保留期（天）**欄位中，以天為單位指定警示的保留期。您可以指定任何大於0的值。

  預設保留期為365天。

- 在**資產大量合併大小**欄位中，指定在合併開始之前，所有資產將被拆分成一個群組（批次）中的資產數量。程式會依序處理每個資產群組：合併、驗證並保存資產。如果指定值為10，則100個資產將拆分成10個群組，每組10個資產，然後逐組處理。指定較小的值會產生較小的群組，這使得合併速度更快，因為應用程式每步處理的資料更少。

  您可以指定任何大於0的值。預設設定為10。

- 在**可同時啟動的最大服務數量**欄位中，指定KUMA可以同時啟動的服務數量。

  預設設定為10。

  同時執行的服務過多會降低KUMA資料的處理速度。

- 在**關聯規則排除項目存續時間（小時）**欄位中，指定關聯規則排除項的生命週期（以小時為單位）。您可以指定1到8760（24*365）之間的值（包含1和8760）。

  預設設定為72。

- 在**Core 服務目的地（用於傳送事件）的磁碟緩衝區大小 (MB)**欄位中，指定為每個服務分配的Core磁碟緩衝區的大小。當內部事件無法傳送到關聯器時，將使用此緩衝區。您可以設定大於0的任何緩衝區大小。

  預設設定為1024MB。

- 在**透過 Core 服務目的地傳送事件的逾時時間（秒）**欄位中，指定傳送事件時與服務建立連線的逾時時間。您可以指定大於0秒的任何逾時時間。

  預設設定為15秒。

- 在**Core 獲授權執行自助服務工作的時段（小時）**欄位中，指定Core可以執行自助服務操作的時間（UTC時間）。KUMA Core 每天都會執行此類操作。您可以指定0到23之間的值（包含0和23）。

  週三建議在夜間使用者未使用 KUMA Core 功能時進行 KUMA Core 維護。

  預設設定為1（UTC時間）。

- 在**最大儲存檔案大小 (MB)**欄位中，指定下載的 GeoIP 資料庫和存放庫套件的壓縮資料大小上限。

  預設設定為300MB。

- 在**資源歷程記錄保留期（天）**欄位中，指定資源變更歷史記錄的保留期（以天為單位）。您可以設定大於或等於0的任何值。

  預設設定為12天。

- 在**從 UI 發出叢集請求的逾時時間（秒）**欄位中，指定KUMA網頁用戶端在請求儲存體清單後必須等待回應的時間。您可以設定大於0的任何值。

  預設設定為30秒。

- 在**儲存空間節點健康檢查的逾時時間（秒）**欄位中，指定請求對特定儲存體節點進行可用性檢查後等待回應的時間。您可以設定大於0的任何值。

  預設設定為30秒。

- 如有必要，請在**KUMA UI負載平衡器主機名稱和連接埠**欄位中，指定KUMA使用者介面負載平衡器的主機名稱和連接埠。

鑑於KUMA Core的分散式特性，可以將多個Core節點設定為叢集。您可以透過負載平衡器設定與叢集的連線。

> 您只能指定一個平衡器URL。

平衡器URL必須以`hostname:port`格式指定，其中

- `hostname`是負載平衡器的主機名稱。
- `port`是負載平衡器的連接埠。

> 不允許使用其他平衡器URL格式。

6. 按一下**儲存**。

代理

代理伺服器用於儲存代理伺服器組態設定，例如在目標中。支援http類型。

可用設定：

- **名稱**（必填）- 代理伺服器的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）- 擁有該資源的租用戶名稱。
- **單獨密鑰** - 如果選取此核取方塊，視窗將顯示必填的**URL**欄位（您可以在其中指定連線URL），以及一個包含「憑證」類型密鑰的**密鑰**下拉清單。透過這種方式，如果您用於連線的使用者帳戶的密碼發生變更，您可以檢視連線資訊，而無需重新建立大量連線。如果清除此核取方塊，則**URL**和**密鑰**欄位不可用。預設情況下，此核取方塊已清除。
- **URL**（必填）是用於指定連線URL的欄位。它與「憑證」類型的密鑰一起使用。如果選取**單獨密鑰**核取方塊，則可用。
- **密鑰**是一個下拉清單，用於選擇現有密鑰或建立「憑據」類型的新密鑰。若已選取**單獨密鑰**核取方塊，則可使用下拉清單。
- **使用密鑰中的 URL**（必填）—一個下拉清單，用於選擇儲存代理伺服器URL的密鑰資源。如果需要，可以透過點擊加號圖示（＋）在代理伺服器建立視窗中建立密鑰。可以透過點選鉛筆圖示（）來更改所選密鑰。
- **不用於以下網域**—一個或多個需要直接存取的網域。
- **描述**—最多4,000個Unicode字元。

連線到SMTP伺服器

KUMA可以設定為使用SMTP伺服器傳送電子郵件通知。如果使用者在其個人資料設定中選取**接收電子郵件通知**核取方塊，則使用者將收到通知。

只能新增一個SMTP伺服器來處理KUMA通知。SMTP伺服器連線在OSMP主控台的**設定→KUMA→開啟 KUMA 設定→通用→SMTP 伺服器設定**下進行管理。

若要設定SMTP伺服器連線：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
2. 這將開啟KUMA設定視窗。
3. 在**其他**下，按一下**常見**。
4. 這會開啟**常見**視窗。
5. 在**SMTP 伺服器設定**區塊中，變更相關設定：

- **已停用**— 如果要停用與SMTP伺服器的連線，請選取此核取方塊。
- **主機**（必填）— SMTP主機採用下列格式之一：主機名稱、IPv4、IPv6。
- **連接埠**（必填）— SMTP連接埠。該值必須是1到65,535之間的整數。
- **寄件者**（必填）— 訊息寄件者的電子郵件地址。例如，`kuma@company.com`。
- **KUMA Core 伺服器的別名**— 網路中使用的KUMA Core伺服器的名稱。必須與FQDN不同。
- 如有必要，請使用**密鑰**下拉清單選擇憑證類型的**密鑰**，其中包含用於連線到SMTP伺服器的帳戶憑證。

  新增密鑰

  若要建立密鑰：

  1. 在**名稱**欄位中，輸入密鑰的名稱。
  2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。
  3. 如有必要，在**描述**欄位中輸入密鑰的描述。
  4. 按一下**建立**按鈕。

  密鑰將會新增並顯示在**密鑰**下拉清單中。

- 在**監控通知間隔**下拉清單中選擇必要的通知頻率。

  來自來源的觸發監控政策的通知將在選定時間段後重複，直到來源的狀態再次變為綠色。

  如果選擇了**通知一次**設定，您將只會收到一次有關監控啟用政策啟動的通知。

- 如果您不想接收有關事件來源狀態的通知，請開啟**停用監控通知**切換按鈕。預設情況下，切換開關是關閉的。

- 點擊**測試連線**按鈕。KUMA 會將測試訊息傳送至目前使用者設定檔中指定的電子郵件地址。即使未選取使用者設定檔中的**接收電子郵件通知**核取方塊，仍會傳送測試訊息。

  請檢查您的電子郵件收件匣。如果測試訊息已送達，表示 SMTP 伺服器設定正確。如果傳送訊息時發生錯誤，請檢查 SMTP 伺服器設定。錯誤會顯示在介面中，並且也記錄在 KUMA Core 記錄中。如果訊息已傳送但未送達信箱，請檢查 SMTP 伺服器記錄中的錯誤訊息。

建議您每次變更 SMTP 伺服器設定或通知範本時，都傳送測試訊息。

6. 按一下**儲存**按鈕。

SMTP伺服器連線現已設定，使用者可以接收來自KUMA的電子郵件。

處理卡巴斯基安全管理中心工作

您可以將卡巴斯基安全管理中心資產連線到KUMA，並將資料庫和應用程式模組更新下載到這些資產，或使用卡巴斯基安全管理中心工作對其執行病毒掃描。工作在KUMA主控台中啟動。

若要在連線到KUMA的資產上執行卡巴斯基安全中心工作，建議使用以下指令碼：

1. **在卡巴斯基安全管理中心管理主控台中建立使用者帳戶**

   此帳戶的憑證在建立密鑰以與卡巴斯基安全管理中心建立連線時使用，並可用於建立工作。

   有關建立使用者帳戶和為使用者指派權限的更多詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

2. **在卡巴斯基安全管理中心中建立KUMA工作**

3. **設定KUMA與卡巴斯基安全管理中心整合**

4. **將資產資訊從卡巴斯基安全管理中心匯入KUMA**

   受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

   KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

   - 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
   - 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

   若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

   1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
   2. 按一下**匯入**，然後選擇以下操作之一：
      - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。

        這將開啟**匯入KSC資產**視窗。
      - 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。

        這將開啟**匯入KSC資產屬性**視窗。
   3. 在下拉清單，選取要為其執行匯入的租用戶。

      在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。

如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。

4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

5. **為匯入的資產指派類別**

匯入後，資產將自動放入**未分類裝置**群組中。您可以將現有類別之一指派給匯入的資產，也可以建立一個類別並將其指派給資產。

6. **在資產上執行工作**

您可以在資產資訊中手動執行工作，或設定工作自動執行。

在卡巴斯基安全管理中心中建立KUMA工作

您可以在連線到KUMA的卡巴斯基安全中心資產上執行防病毒資料庫和應用程式模組更新工作，以及病毒掃描工作。資產必須安裝Kaspersky Endpoint Security for Windows或Kaspersky Endpoint Security for Linux。工作在OSMP主控台中建立。

如需瞭解如何在安裝 Kaspersky Endpoint Security for Windows 的資產上建立 *更新* 和 *病毒掃描* 工作的詳細資訊，請參閱 *Kaspersky Endpoint Security for Windows* 說明指南。

如需瞭解如何在安裝 Kaspersky Endpoint Security for Linux 的資產上建立*更新*和*病毒掃描*工作的詳細資訊，請參閱 *Kaspersky Endpoint Security for Linux* 說明指南。

工作名稱必須以 "kuma" 開頭（不區分大小寫且不帶引號）。例如，`KUMA antivirus check`。否則，該工作不會顯示在KUMA主控台的可用工作清單中。

手動啟動卡巴斯基安全管理中心工作

您可以在連線到KUMA的卡巴斯基安全中心資產上手動執行防病毒資料庫、應用程式模組更新工作和病毒掃描工作。資產必須安裝Kaspersky Endpoint Security for Windows或Kaspersky Endpoint Security for Linux。

首先，您需要設定卡巴斯基安全管理中心與KUMA的整合並在卡巴斯基安全管理中心中建立工作。

若要手動啟動卡巴斯基安全管理中心工作：

1. 在KUMA主控台中，轉至**資產**部分，然後選擇從卡巴斯基安全管理中心匯入的資產。

資產詳情視窗隨即開啟。

2. 點選**OSMP回應**。

如果啟用了與擁有所選資產的卡巴斯基安全中心的連線，則會顯示此按鈕。

3. 在開啟的**選擇工作**視窗中，選取要啟動的工作旁邊的核取方塊，然後按一下**啟動**按鈕。

卡巴斯基安全管理中心將啟動所選工作。

某些類型的工作僅適用於某些資產。

您只能取得執行Windows作業系統的資產的弱點和軟體資訊。

自動啟動卡巴斯基安全管理中心工作

您可以為連線到KUMA的卡巴斯基安全中心資產設定防病毒資料庫和應用程式模組更新工作的自動啟動以及病毒掃描工作。資產必須安裝Kaspersky Endpoint Security for Windows或Kaspersky Endpoint Security for Linux。

首先，您需要設定卡巴斯基安全管理中心與KUMA的整合並在卡巴斯基安全管理中心中建立工作。

設定卡巴斯基安全管理中心工作的自動啟動包含以下步驟：

步驟 1。新增關聯規則

若要新增關聯規則：

1. 在KUMA主控台中，選擇**資源**部分。
2. 選擇**關聯規則**，然後按一下**新增關聯規則**按鈕。
3. 在**一般**頁籤中，指定以下設定：
   a. 在**名稱**欄位中，輸入規則名稱。
   b. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。
   c. 在**類型**下拉清單中，選取**簡單**。
   d. 在**傳播欄位**中，新增下列欄位：DestinationAssetID。
   e. 如有需要，定義下列欄位的值：
      - 在**觸發率限制**欄位中，定義每秒觸發規則的最大次數。
      - 在**嚴重等級**欄位中，定義觸發規則後將建立的警示和關聯事件的嚴重等級。
      - 在**描述**欄位中，提供任何其他資訊。

4. 在**選擇器 → 設定**頁籤中：

   a. 在**篩選器**下拉清單中，選擇**新建**。

   b. 在**條件**欄位中，點選**新增群組**按鈕。

   c. 在您新增的群組的運算子欄位中，選擇**AND** 。

   d. 若要新增依DeviceProduct欄位值篩選的條件：

      1. 在**條件**欄位中，按一下**新增條件**按鈕。
      2. 在條件欄位中，選擇**如果**。
      3. 在**左運算元**欄位中，選擇事件欄位。
      4. 在**事件欄位**中，選擇DeviceProduct。
      5. 在**運算子**欄位中，選擇=。
      6. 在**右運算元**欄位中，選擇**常數**。
      7. 在**值**欄位中，輸入OSMP。

   e. 若要新增依名稱欄位值篩選的條件：

      1. 在**條件**欄位中，按一下**新增條件**按鈕。
      2. 在條件欄位中，選擇**如果**。
      3. 在**左運算元**欄位中，選擇事件欄位。
      4. 在事件欄位中，選擇名稱。
      5. 在**運算子**欄位中，選擇=。
      6. 在**右運算元**欄位中，選擇**常數**。
      7. 在**值**欄位中，輸入事件的名稱。當偵測到此事件時，工作將自動啟動。

         例如，如果要在卡巴斯基安全管理中心註冊*偵測到惡意的物件*事件時啟動*病毒掃描*工作，請在**值**欄位中指定此名稱。

         您可以在事件詳情的**名稱**欄位中檢視事件名稱。

5. 在**操作**頁籤中，指定以下設定：

   a. 在**操作**部分中，開啟**在每個事件上**下拉清單。

   b. 選取**輸出**核取方塊。

      您無需填入其他欄位。

6. 按一下**儲存**按鈕。

關聯規則將會建立。

步驟 2：建立關聯器

您需要啟動關聯器安裝精靈。在精靈的步驟 3中，您需要選擇依照本指南新增的關聯規則。

DeviceHostName欄位必須顯示資產的網域名稱（FQDN）。若未顯示，請為此資產建立 DNS 記錄，並在精靈的步驟 4中建立 DNS 擴充規則。

步驟 3。新增篩選器

若要新增篩選器：

1. 在KUMA主控台中，選擇**資源**部分。
2. 選擇**篩選器**，然後按一下**新增篩選器**按鈕。
3. 在**名稱**欄位中，指定篩選器名稱。
4. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。
5. 在**條件**欄位中，點選**新增群組**按鈕。
6. 在您新增的群組的運算子欄位中，選擇**AND** 。
7. 若要新增依DeviceProduct欄位值篩選的條件：
   a. 在**條件**欄位中，按一下**新增條件**按鈕。
   b. 在條件欄位中，選擇**如果**。
   c. 在**左運算元**欄位中，選擇事件欄位。
   d. 在**事件**欄位中，選擇類型。
   e. 在**運算子**欄位中，選擇=。
   f. 在**右運算元**欄位中，選擇**常數**。
   g. 在**值**欄位中，輸入3。
8. 若要新增依名稱欄位值篩選的條件：
   a. 在**條件**欄位中，按一下**新增條件**按鈕。
   b. 在條件欄位中，選擇**如果**。
   c. 在**左運算元**欄位中，選擇事件欄位。
   d. 在事件欄位中，選擇名稱。
   e. 在**運算子**欄位中，選擇=。
   f. 在**右運算元**欄位中，選擇**常數**。
   g. 在**值**欄位中，輸入步驟1中建立的關聯規則的名稱。

步驟 4。新增回應規則

若要新增回應規則：

1. 在KUMA主控台中，選擇**資源**部分。
2. 選擇**回應規則**，然後按一下**新增回應規則**按鈕。
3. 在**名稱**欄位中，輸入規則名稱。
4. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。
5. 在**類型**下拉清單中，選擇**透過OSMP回應**。
6. 在**Open Single Management Platform工作**下拉清單中，選擇要啟動的卡巴斯基安全管理中心工作。
7. 在**事件欄位**下拉清單中，選取DestinationAssetID.。
8. 在**工作線程**欄位中，指定服務可以同時執行的進程數。
   預設情況下，工作進程數與安裝關聯器服務的伺服器上的虛擬處理器數相同。

- 在**描述**欄位中，您最多可以新增4,000個Unicode字元。
- 在**篩選**下拉清單中，選擇在本說明的步驟3中新增的篩選器。

要向卡巴斯基安全管理中心傳送請求，您必須確保卡巴斯基安全管理中心透過UDP協議可用。

如果回應規則由共用租用戶擁有，則主要租用戶所連線之卡巴斯基安全管理中心伺服器中的工作，會顯示為可供選擇的卡巴斯基安全管理中心工作。

如果回應規則選擇了租用戶連線到的卡巴斯基安全管理中心伺服器中沒有的工作，則不會針對此租用戶的資產執行該工作。例如，當兩個租用戶使用同一個關聯器時，就可能發生這種情況。

步驟 5。在關聯器中新增回應規則

若要在關聯器中新增回應規則：

1. 在KUMA主控台中，選擇**資源**部分。
2. 選擇**關聯器**。
3. 在關聯器清單中，選擇在本說明的步驟2中新增的關聯器。
4. 在步驟樹中，選擇**回應規則**。
5. 按一下**新增**按鈕。
6. 在**回應規則**下拉清單中，選擇在本說明的第4步驟中新增的規則。
7. 在步驟樹中，選擇**安裝驗證**。

8. 點選**儲存並重新啟動服務**按鈕。

9. 按一下**儲存**按鈕。

回應規則將會新增至關聯器。

將為連線到KUMA的卡巴斯基安全管理中心資產上的防病毒資料庫和應用程式模組更新工作以及病毒掃描工作設定自動啟動。當在資產上偵測到威脅並且KUMA收到相應事件時，這些工作將啟動。

檢查卡巴斯基安全管理中心工作的狀態

在KUMA主控台中，您可以檢查卡巴斯基安全管理中心工作是否已啟動，或者是否已完成對監聽卡巴斯基安全管理中心事件的收集器所擁有的事件的搜尋。

若要檢查卡巴斯基安全管理中心工作的狀態：

1. 在KUMA中，選擇**資源→活動服務**。

2. 選擇設定為從卡巴斯基安全管理中心伺服器接收事件的收集器，然後按一下**轉至事件**按鈕。

KUMA的**事件**部分將會開啟一個新的瀏覽器頁籤。表格顯示來自卡巴斯基安全管理中心伺服器的事件。工作的狀態可在**名稱**直欄中檢視。

卡巴斯基安全管理中心事件欄位：

- **名稱**— 工作的狀態或類型。
- **訊息**— 有關工作或事件的訊息。
- **FlexString<number>Label**—從卡巴斯基安全管理中心接收的屬性名稱。例如，`FlexString1Label=TaskName`。
- **FlexString<number>** — FlexString<number>Label 屬性的值。例如，`FlexString1=Download updates`。
- **DeviceCustomNumber<number>Label** — 與工作狀態相關的屬性的名稱。例如，`DeviceCustomNumber1Label=TaskOldState`。
- **DeviceCustomNumber<number>** — 與工作狀態相關的值。例如，`DeviceCustomNumber1=1` 表示工作正在執行。
- **DeviceCustomString<number>Label** — 與偵測到的弱點相關的屬性名稱：例如，病毒名稱、受感染的應用程式。
- **DeviceCustomString<number>** — 與偵測到的弱點相關的值。例如，屬性-值配對 `DeviceCustomString1Label=VirusName` 和 `DeviceCustomString1=EICAR-Test-File` 表示偵測到 EICAR 測試病毒。

KUMA日誌

元件日誌

預設情況下，所有KUMA元件僅記錄錯誤。若要接收日誌中的詳盡資料，請在元件設定中設定**偵錯**模式。

日誌將持續附加，直到達到5GB。當日誌達到 5 GB 時，系統會將其封存為壓縮檔案，並將新事件寫入新的日誌。歸檔將在日誌資料夾中保存7天，7天後將被刪除。伺服器上最多同時儲存四個歸檔日誌。每當建立新的日誌歸檔時，如果歸檔總數大於四個，則最舊的日誌歸檔將被刪除。

以下元件可使用**偵錯**模式：

服務：
• 儲存庫
• 關聯器
• 收集器
• 代理程式
	要啟用它，請使用服務設定中的**偵錯**切換開關。
	
	儲存位置：服務安裝目錄。例如，/opt/kaspersky/kuma/<服務名稱>/log/<服務名稱>。您可以從KUMA主控台的**資源→活動服務**部分下載服務日誌，方法是選擇所需的服務並按一下**日誌**。
	
	可以透過執行journalctl和tail命令來檢視Linux電腦上的日誌。例如：
	• 儲存體。若要從伺服器上安裝的儲存體傳回最新日誌，請執行下列命令：
	`journalctl -f -u kuma-storage-< 儲存體ID >`
	• 關聯器。若要從伺服器上安裝的關聯器傳回最新日誌，請執行下列命令：
	`journalctl -f -u kuma-correlator-< 關聯器ID >`
	• 收集器。若要從伺服器上安裝的特定收集器傳回最新日誌，請執行以下命令：
	`journalctl -f -u kuma-collector-< 收集器ID >`
	• 代理程式。若要從伺服器上安裝的代理程式傳回最新日誌，請執行下列命令：
	`tail -f /opt/kaspersky/agent/< 代理 ID >/log/agent`
	如果為Windows電腦上的代理程式指派了作為服務登入權限，則始終會記錄其活動。選取**偵錯**核取方塊後，可以更詳細地指定資料。Windows電腦上的代理程式日誌可以在位於路徑%PROGRAMDATA%\Kaspersky Lab\KUMA\<代理ID>\agent.log的檔案中檢視。Linux 電腦上的代理日誌儲存在代理安裝目錄中。

資源： • 連接器 • 目標 • 擴充規則	若要啟用它，請使用資源連結到的服務設定中的**偵錯**切換開關。 日誌儲存在託管使用相關資源的已安裝服務的裝置上。可以在連結到資源的服務日誌中檢視資源的詳盡資料。

KUMA通知

標準通知

可以將KUMA設定為使用SMTP伺服器傳送電子郵件通知。為此，請設定與SMTP伺服器的連線，並為應接收通知的使用者選取**接收電子郵件通知**核取方塊。

KUMA會自動通知使用者以下事件：

- 報告已建立（報告範本中列出的使用者會收到通知）。
- 工作已執行（建立工作的使用者會收到通知）。
- 有新的資源包可用。可以透過更新KUMA儲存庫來取得它們（在工作設定中指定了電子郵件地址的使用者將收到通知）。

編輯KUMA使用者設定檔

若要編輯KUMA使用者設定檔：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**存取權限**下，按一下**設定檔**。

   這會開啟**設定檔**視窗。

3. 指定下列設定：

   - 在**時區**欄位中，選擇要在KUMA中顯示時間戳記的時區。該清單根據使用者作業系統的設定產生，並考慮了夏令時。預設使用使用者瀏覽器的時區。
   - 選取**使用ISO 8601格式**核取方塊，即可以ISO 8601格式顯示時間戳記（例如，2026-02-08T17:35:27+03:00）。此格式用於KUMA網頁介面中使用日期和時間的縮寫或完整顯示的部分，並套用至整個KUMA系統。設定的格式儲存在KUMA Core設定中。
   - 如果您希望使用者接收來自KUMA的**SMTP通知**，請選取接收電子郵件通知核取方塊。
   - **顯示不可列印字元**—如果您希望KUMA網頁介面顯示空格、製表符和換行符等不可列印字元，請選取此核取方塊。如果選取**顯示不可列印字元**核取方塊，您可以按**Ctrl/Command+***啟用或停用不可列印字元的顯示。

     空格和製表符會顯示在規範化器、關聯規則、篩選器和連接器的所有輸入欄位（**描述**除外）中，以及**事件**區段中用於搜尋事件的SQL查詢中。空格顯示為圓點。製表符在規範化器、關聯規則、篩選器和連接器中顯示為短橫線。在其他欄位中，製表符顯示為一個或兩個圓點。

     換行符顯示在所有支援多行輸入的輸入欄位中，例如事件搜尋欄位。
   - 在**空間集合**下拉清單中，選取要授予存取權限的一個或多個空間集旁的核取方塊。如果使用者未選擇任何空間集，則授予其對預設空間集的存取權限。

4. 按一下**儲存**按鈕。

KUMA使用者設定檔隨即修改。

管理租用戶

租用戶顯示在「設定」→「KUMA」→「開啟KUMA設定」→「租用戶」下的表格中。您可以按一下欄位來排序表格。

可用直欄：

- **名稱**是租用戶的名稱。
- **EPS限制**是產品授權確定的總EPS定額中分配給租用戶的EPS（每秒事件）定額。
- **描述**是租用戶的描述。
- **建立日期**是指租用戶建立的日期。
- **更新時間** — 租用戶資訊的最近修改日期和時間。

您可以匯出租用戶清單，例如，以便在活動清單或快顯表單小工具中顯示租用戶名稱。在這種情況下，請先匯出租用戶清單，然後再將其匯入字典。為此，請按一下**匯出→用於字典**按鈕。包含租用戶清單的檔案將下載到您的電腦。

您也可以將租用戶清單中的所有資訊匯出到文件。為此，請按一下**匯出→所有欄位**按鈕。包含租用戶清單的檔案將下載到您的電腦。

管理憑證

本節說明如何使用憑證。

下載憑證

您可以在 OSMP Web 介面中下載下列憑證：

- REST API CA 憑證。

  此憑證用於驗證提供 KUMA 公用 API 的 API 伺服器身分。從 MaxPatrol 報告匯入資料時，您也可以使用此憑證。

  如果您想使用公司的憑證和金鑰，而不是自我簽署的 Web 介面憑證，則可以變更憑證。

  下載後，可以將憑證匯入作業系統或瀏覽器的信任存放區。之後，用戶端將信任由 OSMP 核發並由憑證授權單位簽署的 TLS 憑證。

  下載的 CA 憑證不應進行編輯。如果您需要變更節點名稱清單 (SAN)，或使用企業憑證授權單位核發的憑證，則應核發新的 TLS 憑證，並在 OSMP 的**設定 → KUMA → 開啟 KUMA 設定 → 一般 → 外部 TLS 配對**區段中上傳該憑證。

  如果叢集包含多個執行 KUMA Core 服務的節點，而且預期會直接連線至每個節點，建議使用 SAN 中包含所有 KUMA Core 節點 FQDN 的 TLS 憑證。否則，瀏覽器可能會顯示警告，指出節點名稱與憑證不符。

  節點的 FQDN 是在核發新 TLS 憑證時於主體別名 (SAN) 欄位中指定。您不需要修改下載的 REST API CA 憑證。

- 微服務 CA 憑證。

  此憑證用於在未指定自有憑證的情況下，使用 TLS 將日誌來源連線至被動收集器時進行驗證。

- AI 服務憑證。

  此憑證是安裝**資產 AI 評級和 AI 狀態**服務所必需。

若要下載憑證：

1. 在 OSMP Web 介面中，前往**資源和服務 → 作用中服務**區段。
2. 在工具列的 (⋮) 選單中選取命令：
   - **下載 REST API CA 憑證**
   - **下載微服務 CA 憑證**
   - **下載 AI 服務憑證**

   憑證會儲存至瀏覽器設定中指定的資料夾。

若要複製憑證指紋：

1. 在 OSMP Web 介面中，前往**資源和服務 → 作用中服務**區段。
2. 在工具列中，從 (⋮) 選單選取**複製指紋**。

   憑證指紋 ID 已複製到剪貼簿。使用 CA 憑證的指紋 ID 作為服務安裝命令中 `--pair.fingerprint` 選項的值，以便在服務首次連線至 KUMA Core 時驗證 KUMA Core 憑證。

修改自我簽署的網頁介面憑證

您可以使用公司憑證和金鑰取代自我簽署的網頁介面憑證。例如，如果您想要使用企業 CA 核發的憑證取代自我簽署的 CA Core 憑證，則必須提供 PEM 格式的 `external.cert` 和未加密的 `external.key`。

本說明介紹如何使用 PFX 格式的企業憑證取代自我簽署的 CA Core 憑證。您可以參考這些說明，並根據需求調整步驟。

若要使用 PFX 格式的企業憑證取代 OSMP 網頁介面憑證：

1. 如果您使用 PFX 容器中的憑證和金鑰，請使用 OpenSSL 將 PFX 檔案轉換為 PEM 格式的憑證和加密金鑰：

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nokeys -out external.cert
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nocerts -nodes -out external.key
   ```

   執行指令時，您必須指定 PFX 金鑰密碼（Enter Import Password）。

   您將取得 PEM 格式的 `external.cert` 憑證和 `external.key`。

2. 如果您的 `external.key` 未加密，請確保金鑰採用 PKCS#8 格式。如果金鑰檔案以 `BEGIN RSA PRIVATE KEY` 標記開頭，Kaspersky SIEM 將無法處理該檔案。在此情況下，請使用以下指令轉換檔案：

   ```
   openssl rsa -in rsa_private.key -outform PEM -out private.key
   ```

   此指令產生的檔案以 `BEGIN PRIVATE KEY` 標記開頭，OSMP 可接受此類金鑰檔案。

3. 在 OSMP 網頁介面中，開啟**設定 → KUMA → 開啟 KUMA 設定 → 一般**區段。
4. 在 **外部 TLS 配對**下，上傳 PEM 格式的 `external.cert` 和未加密的 `external.key`。

5. 重新啟動 KUMA Core：

```
systemctl restart kuma-core
```

6. 重新整理網頁，或重新啟動您用來管理 OSMP 網頁介面的瀏覽器。

您的公司憑證和金鑰已更換。

重新簽發內部 CA 憑證

只有具備主管理員角色的使用者才能重新簽發內部 CA 憑證。

若要重新簽發並套用內部 CA 憑證：

1. 在網頁介面中，開啟**設定 → KUMA → 開啟 KUMA 設定 → 一般**區段。
2. 在核心設定下，按一下**重新簽發內部 CA 憑證**按鈕。
3. 在開啟的視窗中確認重新簽發憑證。

   KUMA 服務的 CA 憑證和 ClickHouse 的 CA 憑證會重新簽發。必須套用重新簽發的憑證。
4. 連線至部署了收集器、關聯器和事件路由器服務的主機：
   a. 執行以下命令以停止所有服務：

   ```
   sudo systemctl stop kuma-<collector/correlator/eventRouter/metrics>-<service_ID>.service
   ```

   其中：

   <service_ID> 是從 OSMP 網頁介面複製的服務 ID。

   b. 使用以下命令，從 `/opt/kaspersky/kuma/<service type>/<service ID>/certificates` 目錄中刪除 `internal.cert` 和 `internal.key` 檔案：

   ```
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.cert
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.key
   ```
5. 連線至部署儲存服務的主機：
   a. 停止所有儲存服務：

   ```
   sudo systemctl stop kuma-<storage>-<service_ID>.service
   ```

b. 使用以下命令，從 `/opt/kaspersky/kuma/storage/<service ID>/certificates` 目錄中刪除 `internal.cert` 和 `internal.key` 檔案：

```
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.cert
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.key
```

6. 使用以下命令，從 `/opt/kaspersky/kuma/clickhouse/certificates` 目錄中刪除所有 ClickHouse 憑證：

```
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.cert
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.key
```

7. 連線至部署代理服務的主機：

a. 停止 Windows 代理和 Linux 代理的服務。

b. 從代理的工作目錄中刪除 `internal.cert` 和 `internal.key` 檔案。

8. 重新啟動 KUMA Core 以套用新的 CA 憑證：

- 若要在單一伺服器上部署及進行分散式部署，請執行以下命令：

```
sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
```

- 若要在 Kubernetes 叢集中部署，請在任一控制器上執行以下命令：

```
sudo k0s kubectl exec deployment/metrics -n kuma -- rm -rf /opt/kaspersky/kuma/metrics/certificates
sudo k0s kubectl rollout restart deployment metrics -n kuma
sudo k0s kubectl rollout restart deployment/core-deployment -n kuma
```

> 建議使用命令重新啟動 KUMA Core，因為透過 Web 介面重新啟動只會重新啟動 KUMA Core 儲存區，而不會重新啟動整個 KUMA Core。

9. 重新啟動所有已停止的服務：

```
sudo systemctl start kuma-<collector/correlator/eventRouter/storage/metrics>-<service_ID>.service --
pair.fingerprint <CA_cert_ID>
```

其中：

- <service_ID> 是從 KUMA Web 介面複製的服務 ID。
- <CA_cert_ID> 是連線服務時用於驗證的 CA 憑證指紋 ID。

  `--pair.fingerprint` 參數為選用。建立服務時，KUMA 會自動將此選項新增至安裝命令，並指定指紋 ID。
  您可以安裝服務而不指定 `--pair.fingerprint` 選項。在此情況下，KUMA 預設使用 `insecure` 值，因此建立連線時會略過 KUMA Core CA 憑證的驗證。若設為 `insecure`，重新簽發 CA 憑證後便不需要更新指紋。

  為確保 KUMA Core CA 憑證通過驗證，建議安裝服務時保留含有指紋 ID 的 `--pair.fingerprint` 選項。在此情況下，重新簽發 CA 憑證時，您需要從 **資源和服務** → **作用中服務** → 選單（⋮）→ **複製指紋**區段複製指紋 ID。

已套用內部 CA 憑證。

重新簽發特定服務的憑證

若要重設特定服務的憑證：

1. 在網頁介面中，前往**資源與服務 → 使用中的服務**區段。
2. 選取要重新簽發憑證之服務旁的核取方塊。
3. 在工具列或功能表 ⋮ 中，選取**重設憑證**。

   此選項無法用於續訂 KUMA Core 憑證。若要更新 KUMA Core 憑證，必須重新簽發憑證並套用內部 CA 憑證。

4. 刪除服務安裝目錄中的舊憑證。

   解決方案將自動產生新憑證。您不需要重新啟動執行中的服務，新憑證會自動套用。已停止的服務必須重新啟動，才能套用憑證。

刪除Windows代理程式憑證的特殊注意事項：

- 如果代理處於綠色狀態，OSMP 會刪除目前的憑證並產生新憑證。代理將繼續使用新憑證運作。
- 如果代理處於紅色狀態，系統會顯示錯誤，指出代理未執行。在 `%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<agent ID>\certificates` 代理安裝資料夾中，刪除 `internal.cert` 和 `internal.key` 檔案，並手動啟動代理。代理程式啟動時，會自動建立新憑證。

刪除Linux代理程式憑證的特殊注意事項：

- 無論代理處於何種狀態，都會透過網頁介面重設憑證。
- 在 `/opt/kaspersky/agent/<agent ID>/certificates` 代理安裝資料夾中，刪除 `internal.cert` 和 `internal.key` 檔案。
- 由於重設憑證會停止代理，您必須手動啟動代理才能恢復其運作。代理程式啟動時，會自動建立新憑證。

使用地理資料

可以將IP位址或IP位址範圍到地理資料的對應清單上傳到KUMA，以用於擴充事件。

地理資料格式

地理資料能以UTF-8編碼的CSV檔案格式上傳到KUMA。逗號用作分隔符號。檔案第一行包含欄位標頭：`Network,Country,Region,City,Latitude,Longitude`。

CSV中的欄位標頭名稱	欄位描述	範例
Network	IP位址採用下列其中一種格式： • IP位址 • IP位址範圍 • CIDR格式的IP位址。 IPv4 和 IPv6 位址可以混合使用。 必填欄位。	• 192.168.2.24 • 192.168.2.25-192.168.2.35 • 131.10.55.70/8 • 2001:DB8::0/120
Country	您的組織使用的國家/地區名稱。例如，這可以是其名稱或代碼。 必填欄位。	• Russia • RU
Region	您的組織使用的區域名稱。例如，這可以是其名稱或代碼。	• Sverdlovsk Oblast • RU-SVE
City	您的組織使用的城市名稱。例如，這可以是其名稱或代碼。	• Yekaterinburg • 65701000001
Latitude	所描述位置的緯度（十進位格式）。此欄位可以為空，在這種情況下，將資料匯入KUMA時將使用值0。	56.835556
Longitude	所描述位置的經度（十進位格式）。此欄位可以為空，在這種情況下，將資料匯入KUMA時將使用值0。	60.612778

將地理資料從MaxMind轉換為IP2Location

KUMA 可以使用來自 MaxMind、IP2Location 或其他相容格式的地理資料。待轉換檔案的名稱必須符合以下範本：(GeoIP2|GeoLite2)-(City|Country)-Blocks-IPv(4|6).csv。但是，您必須將要使用的檔案轉換為KUMA支援的格式。您可以使用以下指令碼進行轉換。請確保檔案不包含重複記錄。例如，如果檔案只有幾列，則不同的記錄可能包含來自同一網路且具有相同地理資料的資料。此類檔案無法轉換。若要成功執行轉換，請確保沒有重複的行，並且每行至少包含一個唯一欄位。

下載指令碼

執行指令碼需要Python 3.12及更高版本。

指令碼啟動命令：

```
python converter.py --type <type of geographic data being processed: "maxmind" or "ip2location"> --out <directory where a CSV file containing geographic data in KUMA format will be placed> --input <path to the ZIP archive containing geographic data from MaxMind or IP2location>
```

使用 `--help` 旗標執行指令碼時，會顯示可用指令碼參數的說明：`python converter.py --help`

用於轉換包含MaxMind ZIP檔案中的俄羅斯IP位址範圍資料庫的檔案的命令：

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out geoip_maxmind_ru.csv
```

若未指定 `--lang` 參數，指令碼預設會從 ZIP 壓縮檔案中的 GeoLite2-City-Locations-en.csv 檔案接收資訊。

對於 MaxMind，若未使用 `--lang` 參數，等效於以下命令：

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

用於從IP2Location ZIP封存檔案轉換檔案的命令：

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out
geoip_ip2location.csv
```

用於從多個IP2Location ZIP檔案轉換檔案的命令：

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP
IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out geoip_ip2location_ipv4_ipv6.csv
```

> `--lang` 參數不用於 IP2Location。

必填欄位集

MaxMind來源檔案GeoLite2-City-Blocks-IPv4.csv 和 GeoLite2-City-Blocks-IPv6.csv必須包含以下欄位集：

network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

來源資料範例集：

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius

1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000

1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

其餘具有區域代碼的CSV檔案必須包含下列資料集：

geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

來源資料範例集：

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,
subdivision_1_iso_code,subdivision_1_name,subdivision_2_iso_code,subdivision_2_name,
city_name,metro_code,time_zone,is_in_european_union

1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0

7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

來源IP2Location檔案必須包含網路範圍、國家、地區、城市、緯度和經度的資料

來源資料範例集：

```
"0","16777215","-","-","-","-","0.000000","0.000000","-","-"

"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"

"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+
```

如果來源檔案包含與本部分所示的欄位不同的欄位集，或者如果某些欄位缺失，則轉換後目標CSV檔案中缺失的欄位將為空。

匯入和匯出地理資料

如有必要，您可以手動將地理資料匯入和匯出到KUMA。地理資料以CSV檔案的形式匯入和匯出。如果地理資料匯入成功，先前新增的資料將被覆寫，並在 KUMA 中產生稽核事件（稽核事件、稽核事件）。

若要將地理資料匯入KUMA：

1. 準備一個包含地理資料的CSV檔案。

   從MaxMind和IP2Location接收的地理資料必須轉換為KUMA支援的格式。

2. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

3. 在**其他**下，按一下**常見**。

   這會開啟**常見**視窗。

4. 在**GeoIP 設定**區塊中，按一下**從檔案匯入**按鈕，然後選擇一個包含地理資料的CSV檔案。

   等待地理資料匯入完成。如果重新整理頁面，資料匯入將中斷。

地理數據將上傳到KUMA。

若要從KUMA匯出地理資料：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在**其他**下，按一下**常見**。

   這會開啟**常見**視窗。

3. 在**GeoIP 設定**區塊中，按一下**匯出**按鈕。

地理資料將根據您的瀏覽器設定下載為名為geoip.csv（UTF-8編碼）的CSV檔案。

資料以與上傳時相同的格式匯出，IP位址範圍除外。若匯入 KUMA 的檔案中以 `1.0.0.0/24` 格式標示位址範圍，則匯出檔案中該範圍將以 `1.0.0.0-1.0.0.255` 格式顯示。

地理資料的預設對應

設定地理資料擴充規則時，若選擇 `SourceAddress`、`DestinationAddress` 和 `DeviceAddress` 事件欄位作為 IP 位址來源，則 **套用預設對應** 按鈕將變為可用。點擊此按鈕可新增地理資料屬性與事件欄位的預設定對應組，如下文所述。

SourceAddress事件欄位的預設對應

地理資料屬性	事件欄位
國家	`SourceCountry`
區域	`SourceRegion`
城市	`SourceCity`
Latitude	`SourceLatitude`
Longitude	`SourceLongitude`

DestinationAddress事件欄位的預設對應

地理資料屬性	事件欄位
國家	`DestinationCountry`
區域	`DestinationRegion`
城市	`DestinationCity`
Latitude	`DestinationLatitude`
Longitude	`DestinationLongitude`

DeviceAddress事件欄位的預設對應

地理資料屬性	事件欄位
國家	`DeviceCountry`
區域	`DeviceRegion`
城市	`DeviceCity`
Latitude	`DeviceLatitude`
Longitude	`DeviceLongitude`

使用知識庫

在 OSMP 主控台中，您可以找到 **知識庫** 區段，您可在其中以更直觀的方式管理卡巴斯基套件和資源。在此區段中，您可以檢視可用和已安裝的套件與資源、評估已安裝資源對 MITRE ATT&CK 技術的涵蓋範圍、監控資源版本的最新狀態、依指定參數進行搜尋和篩選，以及安裝個別資源或整個套件。

套件包含用於設定 OSMP 的資源集合。套件可從卡巴斯基儲存庫下載。

如果到目前為止尚未從儲存庫下載任何套件，則 **知識庫** 區段中的套件和資源清單會是空的。若要取得可供安裝的套件和資源，您需要設定預先定義資源的更新。
如需有關如何從儲存庫取得資源的詳細資訊，請參閱更新資源區段。

若要開啟 **知識庫** 區段，請在 OSMP 主控台中，前往 **監控 → 資源和服務 → 知識庫** 區段。

此區段包含一些小工具，可顯示您的解決方案實例中套件和資源的摘要資訊。若要顯示或隱藏小工具，請點擊 圖示。以下小工具可供使用：

- **套件狀態** 會顯示具有以下狀態的套件數量：
  - **可用**表示套件可供安裝。
  - **已安裝**表示整個套件已安裝。
  - **緊急**表示套件包含需要盡快安裝的高優先順序資源。
  - **新增**表示套件是在三個月內新增至儲存庫，且使用者尚未安裝或檢視該套件。
- **資源狀態** 會顯示具有以下狀態的各類型資源數量：
  - **可用**表示資源可供安裝。
  - **已安裝**表示資源已安裝，且不需要更新。
  - **需要更新**表示儲存庫中有該資源的較新版本可用。
- **MITRE 技術涵蓋範圍，{{ filter }}** 會顯示所選資源所涵蓋的 MITRE ATT&CK 技術數量或涵蓋率百分比的資訊。

小工具也可作為頁面上表格的篩選器。當您在小工具中選取值時，表格會根據選取的篩選器自動更新。例如，您可以只顯示具有 **需要更新** 狀態的資源。

此區段會顯示以下索引標籤：

- 在 **套件** 索引標籤上，會顯示包含資源的套件清單（這是預設索引標籤）。
- 在 **資源** 索引標籤上，會顯示個別資源的清單。

您可以使用**搜尋**欄位搜尋套件或資源。搜尋只會在目前開啟的索引標籤上執行。當您在索引標籤之間切換時，輸入的搜尋查詢會保留並套用至選取的索引標籤。在 **搜尋** 欄位中，您可以輸入資源名稱、事件來源、事件類型、套件名稱或任何子字串。

若要篩選 **套件** 和 **資源** 索引標籤的內容，請點選篩選器 圖示。

您可以在 **套件** 和 **資源** 索引標籤上，透過點選相關參數的欄標題並選取 **升序** 或 **降序** 來排序表格。您也可以依 **資源種類** 或 **狀態** 欄篩選表格，方法是點選相關欄的標題並選取需要顯示的值。

檢視套件詳細資料

若要檢視可用的套件，

在 OSMP 主控台中，開啟 **監控** → **資源和服務** → **知識庫** 區段，然後前往 **套件** 標籤（預設已選取）。

套件 標籤會顯示可用套件的表格，其中包含以下欄：

- **名稱** 是套件的名稱。
- **版本** 是套件的版本。
- **發佈日期** 是套件發行的日期。
- **資源種類** 是套件中包含的資源類型：
  - 活動清單
  - 快顯表單
  - 標準化器
  - 事件彙總規則
  - 關聯規則
  - 擴充規則
  - 字典
  - 篩選器
  - 通知範本
- **資源數量** 是套件中的資源數量。
- **狀態** 是套件的狀態。
  - **可用**表示套件可供安裝。
  - **已安裝**表示整個套件已安裝。
  - **緊急**表示套件包含需要盡快安裝的高優先順序資源。
  - **新增** 表示套件是新的且可供安裝。
- **說明** 是套件的描述。

若要檢視套件的資訊，請點擊其名稱。這會開啟一個包含套件資訊的視窗，其中包含 **一般** 和 **變更記錄** 索引標籤。

下列資訊會顯示在 **一般** 索引標籤上：

- 檔案名稱
- 敘述
- 發佈日期
- 版本

此索引標籤也包含 **待匯入的資源** 區段，該區段會顯示套件中包含的資源清單。您可以在此篩選資源，並只選取需要安裝的資源。

變更記錄 索引標籤會顯示套件變更的相關資訊。

檢視資源詳細資料

若要檢視可用資源，

在 OSMP 主控台中，開啟**監控 → 資源與服務 → 知識庫**區段，然後前往**資源**索引標籤。

資源索引標籤會顯示可用資源的表格，其中包含以下欄：

- **名稱**—資源的名稱。
- **資源種類**—可用的資源類型：
  - 活動清單
  - 快顯表單
  - 標準化器
  - 事件彙總規則
  - 關聯規則
  - 擴充規則
  - 字典
  - 篩選器
  - 通知範本
- **安裝日期**是資源安裝在 KUMA 中的日期。
- **租用戶**是安裝該資源的租用戶。

  如果相同資源安裝在多個租用戶中，則會在表格中顯示為群組。若要檢視該資源在每個安裝所在租用戶中的詳細資訊，請展開群組。

- **版本**是資源的版本。
- **狀態**是資源的狀態。
  - **可用**表示資源可供安裝。
  - **已安裝**表示資源已安裝。
  - **需要更新**表示資源有較新版本可用。
- **套件名稱**列出包含此資源的套件。
- **供應商標籤**是資源供應商指派的標籤。
- **MITRE 技術**是與資源相關聯的 MITRE ATT&CK 技術。

若要檢視資源的相關資訊，請點擊其名稱。這會開啟資源資訊視窗，其中包含**一般資訊**和**已關聯資源**索引標籤。

在**已關聯資源**索引標籤上，您可以檢視連結至所選資源的資源。您也可以在**資源**索引標籤上，透過點擊**顯示相依性**按鈕來檢視相依性。

安裝和更新套件與資源

安裝套件

只有在套件包含的所有資源皆已安裝時，套件才會取得**已安裝**狀態。

若要安裝整個套件：

1. 前往**監控** → **資源和服務** → **知識庫** → **套件**區段。
2. 執行以下操作之一：
   - 選取相關套件旁的核取方塊，然後點擊**安裝**按鈕。
   - 點擊套件名稱以開啟視窗，然後在該視窗中點擊**安裝**按鈕。
3. 選取租用戶。
4. 點擊**安裝**按鈕。
   之後，資源會匯入至 OSMP，並可供進一步設定。

安裝個別資源

若要從套件安裝個別資源：

1. 前往**監控 → 資源和服務 → 知識庫 → 資源**區段。
2. 執行以下操作之一：
   - 選取相關資源旁的核取方塊，然後點擊**安裝**按鈕。
   - 點擊資源名稱以開啟視窗，然後在該視窗中點擊**安裝**按鈕。
3. 選取租用戶。
4. 點擊**安裝**按鈕。

更新資源

如果已安裝的資源有新版本可用，該資源會取得**需要更新**狀態。

若要更新資源：

1. 前往**監控 → 資源和服務 → 知識庫 → 資源**區段。
2. 選取一或多個狀態為**需要更新**的資源旁的核取方塊。
3. 點擊**更新**按鈕。

KUMA資源

*資源*是KUMA元件，包含用於實現各種功能的參數：例如，與給定的網址建立連線或根據某些規則轉換資料。這些元件以各種組合組裝成服務的資源集，這些資源集進一步用作建立KUMA服務的基礎。

資源位於 KUMA 主控台的**資源**區段中。

在**資源**和**規則**下，您可以找到以下類型的資源：

- **標準化器**- 此類資源包含用於將傳入事件轉換為KUMA使用的格式的規則。在標準化器中處理後，原始事件將被標準化，並可由其他KUMA資源和服務處理。
- **連接器**—此類資源包含用於建立網路連線的設定。
- **目標** - 此類資源包含將事件轉送到目標進行進一步處理或儲存的設定。
- **篩選器** - 此類資源包含從事件流中拒絕或選擇單一事件的事件條件。
- **活動清單**— 此類資源由關聯器在根據關聯規則分析事件時用於動態資料處理。

- **字典**— 此類資源用於儲存鍵及其值，其他KUMA資源和服務可能需要這些鍵及其值。
- **代理**— 此類資源包含使用代理伺服器的設定。
- **密鑰**— 此類資源用於安全地儲存KUMA與外部服務互動所需的機密資訊（例如憑證）。
- **快顯表單**— 此類資源由KUMA關聯器用於根據關聯規則分析事件。
- **通知範本**—此類資源用於傳送關於新警示的通知。
- **關聯規則**- 此類資源包含用於識別指示威脅的事件模式的規則。如果滿足這些資源中指定的條件，則會產生關聯事件。
- **聚合規則**—此類資源包含將多個相同類型的基本事件合併為一個聚合事件的規則。
- **擴充規則**—此類資源包含使用來自第三方來源的資訊補充事件的規則。
- **回應規則**— 此類資源用於關聯器，例如，在滿足特定條件時執行指令碼或啟動卡巴斯基安全管理中心工作。
- **資料收集與分析規則**—此類資源包含可排程對儲存區執行含聚合函數之 SQL 查詢的規則。從 SQL 查詢取得的資料隨後會用於關聯分析。

當您按一下資源類型時，會開啟一個視窗，其中顯示包含此類型可用資源的表格。資源表包含以下列：

- **名稱**— 資源的名稱。可用於搜尋資源並對其進行排序。
- **更新時間**— 資源上次更新的日期和時間。可用於對資源進行排序。
- **建立者**— 建立資源的使用者名稱。
- **描述**— 資源的描述。

表格大小不受限制。如果要選擇所有資源，請捲動至表格末端並選取**全選**核取方塊，這將選擇表格中所有可用的資源。

資源可以整理成資料夾。資料夾結構顯示在視窗左側：根資料夾對應於租用戶，包含租用戶所有資源的清單。巢狀根資料夾中的所有其他資料夾顯示單一資料夾的資源。選擇資料夾後，它包含的資源將作為表格顯示在視窗右側窗格中。

可以建立、編輯、複製、從一個資料夾移動到另一個資料夾以及刪除資源。也可以匯出和匯入資源。

KUMA 附帶一組預先定義的資源，這些資源可透過 [OOTB]< 資源名稱 > 名稱識別。OOTB資源受到保護，不能進行編輯。

如果要讓預先定義的OOTB資源適應組織的基礎設施：

1. 在**資源**-<資源類型> 部分中，選擇要編輯的OOTB資源。
2. 在KUMA主控台的上部，按一下**複製**，然後按一下**儲存**。

   名為 [OOTB]< 資源名稱 > - copy 的新資源顯示在 Web 介面中。
3. 根據需要編輯預定義資源的副本並儲存變更。

調整後的資源可供使用。

資源操作

若要管理KUMA資源，您可以建立、移動、複製、編輯、刪除、匯入和匯出它們。這些操作適用於所有資源，無論資源類型為何。

KUMA資源位於資料夾中。您可以新增、重新命名、移動或刪除資源資料夾。

建立、重新命名、移動和刪除資源資料夾

資源可以整理到資料夾中。資料夾結構顯示在視窗左側：根資料夾對應於租用戶，包含租用戶所有資源的清單。巢狀根資料夾中的所有其他資料夾顯示單一資料夾的資源。選擇資料夾後，它包含的資源將作為表格顯示在視窗右側窗格中。

您可以建立、重新命名、移動和刪除資料夾。

若要建立資料夾：

1. 在樹中選擇需要新資料夾的資料夾。
2. 按一下**新增資料夾**按鈕。

   資料夾隨即建立。

若要重新命名資料夾：

1. 在資料夾結構中找到所需的資料夾。
2. 將滑鼠游標停在資料夾名稱上。

   ...圖示將出現在資料夾名稱附近。
3. 開啟...下拉式清單，然後選取**重新命名**。

   資料夾名稱將變為活動狀態以供編輯。
4. 輸入新資料夾名稱，然後按**ENTER鍵**。

   > 資料夾名稱不能為空。

   資料夾將被重新命名。

若要移動資料夾，

請按一下資料夾名稱，將其拖曳到資料夾結構中的所需位置。

> 資料夾無法從一個租用戶拖曳到另一個租用戶。

若要刪除資料夾：

1. 在資料夾結構中找到所需的資料夾。
2. 將滑鼠游標停在資料夾名稱上。
   ...圖示將出現在資料夾名稱附近。
3. 開啟 ... 下拉式清單，然後選取**刪除**。
   確認視窗隨即出現。
4. 點擊**確定**。

資料夾將被刪除。

> 程式不會刪除包含檔案或子資料夾的資料夾。

建立、複製、移動、編輯和刪除資源

您可以建立、移動、複製、編輯和刪除資源。

若要建立資源：

1. 在主功能表中，轉至**監控 → 資源 → <資源類型>**。
2. 選擇或建立要新增新資源的資料夾。
   根資料夾對應於租用戶。若要使資源可供特定租用戶使用，必須在該租用戶的資料夾中建立該資源。
3. 點選**新增<資源類型>**按鈕。
   用於設定所選資源類型的視窗將開啟。可用的設定參數取決於資源類型。
4. 在**名稱**欄位中輸入唯一的資源名稱。
5. 指定必需參數（標有紅色星號）。
6. 如有必要，指定可選參數（非必需）。
7. 按一下**儲存**按鈕。

將建立資源並可用於服務和其他資源。

若要將資源移至新資料夾：

1. 在主功能表中，轉至**監控 → 資源 → <資源類型>**。
2. 在資料夾結構中找到所需的資源，然後選取要移動的資源旁邊的核取方塊。您可以選取多個資源。
   ⣿ 圖示會出現在所選資源旁邊。
3. 使用 ⣿ 圖示將資源拖曳到所需資料夾。

資源將被移至新資料夾。

您只能將資源移至建立資源的租用戶的資料夾。資源無法移動到其他租用戶的資料夾。

若要複製資源：

1. 在主功能表中，轉至**監控 → 資源 → <資源類型>**。
2. 在資料夾結構中找到所需的資源，然後選取要複製的資源旁的核取方塊，然後按一下**複製**。
   一個視窗將開啟，其中包含您選擇複製的資源的設定。可用的設定參數取決於資源類型。
   `<selected resource name> - copy` 值會顯示在 **名稱** 欄位中。
3. 對參數進行必要的更改。
4. 在**名稱**欄位中輸入唯一名稱。
5. 按一下**儲存**按鈕。

資源的副本將被建立。

若要編輯資源：

1. 在主功能表中，轉至**監控 → 資源 → <資源類型>**。
2. 在資料夾結構中找到所需的資源，然後選擇該資源。
   將會開啟一個視窗，其中包含所選資源的設定。可用的設定參數取決於資源類型。
3. 對參數進行必要的更改。
4. 按一下**儲存**按鈕。

資源將被更新。如果此資源已在服務中使用，請重新啟動服務以套用新設定。

若要刪除資源：

1. 在主功能表中，轉至**監控 → 資源 → <資源類型>**。
2. 在資料夾結構中找到所需的資源。
3. 選取您要刪除之政策旁的核取方塊並點擊**刪除**。
   確認視窗隨即開啟。
4. 點擊**確定**。

資源將被刪除。

將資源關聯到服務

現在您可以將資源（關聯規則、擴充規則、回應規則、彙總規則和目標）關聯到收集器、關聯器和事件路由器等服務。可用的服務取決於所選資源的型別。

若要將資源關聯到服務：

1. 在主功能表中，轉至**監控→資源和服務→<資源名稱>**部分。
2. 選取要關聯的每個資源旁邊的核取方塊，然後在工具列或功能表中（⋮），點選**連結至服務→關聯到<服務名稱>**。

   您也可以在編輯資源設定時將資源關聯到服務。為此，請按一下資源名稱，選擇**服務**頁籤，然後按一下**連結至服務→關聯至<服務名稱>**。

   > 管理關聯規則的設定時，可以使用**關聯器**頁籤將規則關聯到關聯器。

3. 在顯示的**<服務名稱>**視窗中，選取所需服務旁的核取方塊，然後按一下**確定**。

該資源隨即關聯到該服務。

若要將資源與服務取消關聯：

1. 在主功能表中，轉至**監控→資源和服務→<資源名稱>**部分。
2. 點擊資源並選擇**服務**頁籤。

   > 對於關聯規則，將顯示**關聯器**頁籤。

3. 選取要取消關聯資源的每個服務旁的核取方塊。
4. 點擊**刪除**並確認取消與該服務的關聯。

該資源隨即與該服務取消關聯。

更新資源

KUMA更新子系統提供接收、儲存和套用事件處理和威脅偵測所需資源的機制。此子系統包含兩種獨立的更新機制：

- **儲存庫更新**—下載資源套件並能夠對其進行審查、分析和匯入租用戶的機制。
- **OSMP更新** - 無需使用者參與和手動匯入即可接收和套用資源的自動機制。

兩種機制均可使用以下更新來源：

- Kaspersky 更新伺服器。
- 自訂來源（儲存庫或更新鏡像）。

更新子系統會擴充KUMA的功能，以應對威脅情勢和基礎設施的變化。無需直接存取網際網路即可使用它，有助於確保系統處理的資料的隱私。

更新資源工作流程

若要更新資源，請執行下列步驟：

1. 更新儲存庫以將資源包交付至儲存庫。儲存庫更新有兩種模式：
   - 自動更新
   - 手動更新
2. 將資源包從更新後的儲存庫匯入租用戶。
3. 匯入完成後，請確保對映更新的資源。如有必要，請將資源連結到收集器、關聯器或代理程式，並更新設定。

儲存庫更新

卡巴斯基定期發布可從儲存庫匯入的資源包。您可以在**儲存庫更新**工作的設定中指定電子郵件地址。首次執行任務後，KUMA會開始向指定位址傳送有關可用更新套件的通知。

儲存庫更新機制允許檢索軟體套件、查看其內容，並決定是否將其部署到作業系統基礎設施中。儲存庫更新可以自動或手動執行。

如果您的基礎設施中還有其他卡巴斯基應用程序，則可以將KUMA連線到現有的更新鏡像。

若要啟用自動更新：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
2. 在**其他**下，按一下**更新設定**。
3. 在**儲存庫更新**下，設定**資料刷新間隔（小時）**。預設值是24小時。
4. 指定**更新來源**。提供以下功能：
   - Kaspersky 更新伺服器。
     您可以在知識庫中查看伺服器清單。
   - 自訂來源：
     - HTTP伺服器上共用資料夾的URL。
     - 安裝KUMA Core的主機上的本機資料夾的完整路徑。
       如果使用本機資料夾，則kuma系統使用者必須具有此資料夾及其內容的讀取權限。

5. 按一下**新增**按鈕指定**用於通知的電子郵件**。儲存庫中匯入到租用戶的新資源包或新版本資源包的通知將傳送到指定的電子郵件地址。

   如果指定KUMA使用者的電子郵件地址，則必須在使用者設定檔中選取**接收電子郵件通知**核取方塊。對於不屬於任何KUMA使用者的電子郵箱，無需其他設定即可接收訊息。在所有情況下都必須指定連線到SMTP伺服器的設定。

6. 按一下**儲存**按鈕。更新工作隨即啟動。然後，工作將根據排程重新啟動。

若要手動啟動儲存庫更新：

1. 若要停用自動更新，請在**設定→KUMA→開啟 KUMA 設定→更新設定→儲存庫更新**區段中，開啟**停用自動更新**切換開關。預設情況下，切換開關處於關閉狀態。您也可以在不停用自動更新的情況下啟動手動儲存庫更新。手動啟動更新不會影響自動更新排程。

2. 指定**更新來源**。提供以下功能：

   - Kaspersky 更新伺服器。
   - 自訂來源：
     - HTTP伺服器上共用資料夾的URL。
     - 安裝KUMA Core的主機上的本機資料夾的完整路徑。

       如果使用本機資料夾，則kuma使用者必須有權存取此資料夾及其內容。

3. 按一下**新增**按鈕指定**用於通知的電子郵件**。儲存庫中匯入到租用戶的新資源包或新版本資源包的通知將傳送到指定的電子郵件地址。

   如果指定KUMA使用者的電子郵件地址，則必須在使用者設定檔中選取**接收電子郵件通知**核取方塊。對於不屬於任何KUMA使用者的電子郵箱，無需其他設定即可接收訊息。在所有情況下都必須指定連線到SMTP伺服器的設定。

4. 按一下**執行更新**。這樣，您就可以同時儲存設定並手動啟動**儲存庫更新**工作。

OSMP更新

如果產品授權支援，OSMP更新機制會自動接收並套用資源。OSMP更新在背景自動執行，無需手動匯入、分析或核准軟體套件。

更新完成後，新的事件欄位和關聯規則無需額外設定即可用於處理。

若要設定OSMP更新：

1. 在主選單中，轉至**設定→KUMA→開啟 KUMA 設定→更新設定**。
2. 指定**更新來源**。提供以下功能：
   - Kaspersky 更新伺服器。
   - 自訂來源：
     - HTTP伺服器上共用資料夾的URL。
     - 安裝KUMA Core的主機上的本機資料夾的完整路徑。

       如果使用本機資料夾，則kuma使用者必須有權存取此資料夾及其內容。如果使用自訂來源，請根據需要設定代理設定。
3. 在**OSMP更新**的**資料刷新間隔（分鐘）**欄位中，指定自動更新檢查和下載的頻率（以分鐘為單位）。預設值是 30。
4. 按一下**儲存**按鈕。

預設情況下，**停用自動更新**切換開關處於關閉狀態，OSMP更新會根據**資料刷新間隔（分鐘）**欄位中指定的間隔自動執行。

如果要停用OSMP自動更新，請開啟**停用自動更新**切換開關並按一下**儲存**。在這種情況下，將不會執行自動更新檢查和下載。若要手動啟動OSMP更新，請按一下**執行更新**。

使用Kaspersky Update Utility設定自訂來源

您可以透過Kaspersky Update Utility使用自訂更新來源，在沒有網路連線的情況下更新資源。

設定包含以下步驟：

1. 使用Kaspersky Update Utility設定自訂來源：
   a. 在公司區域網路中的其中一台電腦上安裝並設定Kaspersky Update Utility。
   b. 在Kaspersky Update Utility設定中設定將更新複製到共用資料夾。
2. 設定從自訂來源更新KUMA儲存區。

使用Kaspersky Update Utility設定自訂來源：

您可以從卡巴斯基技術支援網站下載Kaspersky Update Utility分發套件。

1. 在Kaspersky Update Utility中，啟用KUMA更新下載：
   - 在**應用程式-邊界控制**下，選取KUMA旁的核取方塊以啟用更新功能。
   - 若使用命令列操作 Kaspersky Update Utility，請將以下行新增至 updater.ini 設定檔的 [ComponentSettings] 區段，或為現有行指定 `true` 值：

     ```
     KasperskyUnifiedMonitoringAndAnalysisPlatform_XDR_1_1=true
     ```

2. 在**下載**部分，指定更新來源。預設情況下，使用卡巴斯基更新伺服器作為更新來源。

3. 在**下載**部分的**更新資料夾**設定群組中，指定Kaspersky Update Utility下載更新的共用資料夾。提供以下功能：

   - 指定安裝Kaspersky Update Utility的主機上的本機資料夾。部署用於分發更新的HTTP伺服器並在其上發布本機資料夾。在OSMP主控台中，在**設定 → KUMA → 開啟 KUMA 設定 → 儲存庫更新 → 自訂來源**部分，指定在HTTP伺服器上發佈的本機資料夾URL。

   - 指定安裝Kaspersky Update Utility的主機上的本機資料夾。使此本機資料夾可透過網路存取。在安裝KUMA的主機上掛載可透過網路存取的本機資料夾。在OSMP主控台的**設定 → KUMA → 開啟 KUMA 設定 → 儲存庫更新 → 自訂來源**部分中，指定本機資料夾的完整路徑。

有關使用Kaspersky Update Utility的詳細資訊，請參閱卡巴斯基知識庫。

匯出資源

如果共用資源對使用者隱藏，使用者無法匯出共用資源或使用共用資源的資源。

若要匯出資源：

1. 在主功能表中，轉至**監控 → 資源 → 關聯規則**。

2. 按一下**匯出資源**。
   將開啟**匯出資源**視窗，其中顯示所有可用的資源樹。

3. 在**密碼**欄位中輸入必須用於保護匯出資料的密碼。

4. 在**租用戶**下拉清單中，選擇要匯出其資源的租用戶。

5. 選取要匯出的資源旁邊的核取方塊。
   如果選定的資源連結到其他資源，則連結的資源也會被匯出。

6. 按一下**匯出**按鈕。

使用瀏覽器設定將受密碼保護的檔案中資源儲存在您的電腦上。「密鑰」資源匯出為空白。

匯入資源

若要匯入資源：

1. 在主功能表中，轉至**監控 → 資源**。

2. 按一下**匯入資源**。
   資源匯入視窗隨即打開。

3. 在 **租用戶** 下拉式清單中，選取將擁有匯入資源的租用戶。

4. 在**匯入源**下拉清單中，選擇下列選項之一：

- **檔案**

  如果您選擇此選項，請輸入密碼並點擊**匯入**按鈕。

- **儲存庫**

  選擇此選項後，將顯示可匯入的資源包清單。我們建議您確保儲存庫更新日期相對較新，並在必要時設定自動更新。

  您可以選擇一個或多個要匯入的資源包，然後點擊**匯入**按鈕。公用租用戶的依賴資源將會匯入到共用租用戶中，其餘資源將匯入到所選租用戶中。您無需共用租用戶的特殊權限；您只需擁有在所選租用戶中匯入的權限即可。

  匯入的資源標記為**此資源是資源包的一部分。您可以刪除它，但無法編輯**的匯入資源只能刪除。若要重新命名、編輯或移動匯入的資源，請點選**複製**按鈕複製該資源，然後使用資源副本執行所需的操作。匯入資源包的未來版本時，副本不會更新，因為它是一個單獨的物件。

  標記為**此資源是資源包的一部分**且位於`Integration`目錄中的匯入資源可以編輯。例如，您可以在`Integration`目錄中編輯關聯規則的排除項篩選器。排除項篩選器包含一系列條件，用於防止關聯規則誤報觸發。根據您的網路環境，可以在使用關聯規則之前或期間為排除項篩選器新增條件，以減少誤報。預設情況下，卡巴斯基提供的排除項篩選器會加入到關聯規則選擇器中。

  匯入軟體套件的後續版本時，已編輯的資源不會被軟體套件中的相應資源替換，從而可以保留您的變更。與臨時排除項不同，對排除項篩選器所做的變更會永久套用。

  儲存庫中的資源會依據 KUMA Core 設定 區段中 KUMA 資源本地化設定所指定的語言，從儲存庫匯入。

5. 如果從檔案匯入的資源與現有資源發生衝突，請解決衝突。閱讀下文以了解更多關於資源衝突的資訊。

   a. 如果匯入資源的名稱、類型和GUID與現有資源的名稱、類型和GUID 完全相符，則會開啟**衝突**視窗，其中的表格會顯示衝突資源的類型和名稱。解決顯示的衝突：

   - 若要以新資源替換現有資源，請點選**取代**。

     若要替換所有衝突資源，請點選**全部取代**。

   - 若要保留現有資源，請按一下**略過**。

     對於依賴資源（即與其他資源關聯的資源），**略過**選項不可用；您只能**取代**依賴資源。

     若要保留所有現有資源，請按一下**全部略過**。

   b. 點擊**解決**按鈕。

資源將會匯入到KUMA。匯入的「密鑰」資源為空白。

匯入使用擴充事件結構描述的資源

如果匯入使用擴充事件結構描述的一個或多個欄位的標準化器，KUMA會自動建立在標準化器中使用的擴充結構描述欄位。

如果匯入在其邏輯中使用擴充事件結構描述欄位的其他類型的資源，則會成功匯入資源。為確保匯入的資源正常運作，必須在「標準化器」類型的資源中建立擴展事件結構描述的相應欄位。

如果將使用擴展事件結構描述欄位的標準化器匯入KUMA，並且KUMA中已存在相同的欄位，則使用先前建立的欄位。

關於衝突解決

當從檔案將資源匯入KUMA時，會將它們與現有資源進行比較；比較以下參數：

- 名稱和類型如果匯入的資源的名稱和種類參數與現有資源的名稱和種類參數相符，則匯入的資源的名稱會自動變更。

- 如果兩個資源的識別符相符，則會出現衝突，使用者必須解決該衝突。當您將資源匯入到匯出它們的同一個KUMA伺服器時，可能會發生這種情況。

解決衝突時，您可以選擇以匯入的資源*替換現有資源*，或*保留現有資源*，略過匯入的資源。

某些資源是連結的：例如，在某些類型的連接器中，必須指定連接器密鑰。如果密鑰連結到連接器，則也會匯入它們。此類連結資源將一起匯出和匯入。

匯入的特殊注意事項：

1. 資源將匯入到選定的租用戶。

2. 如果連結的資源在共用租用戶中，則匯入時它最終會位於共用租用戶中。

3. 在**衝突**視窗中，**父級**直欄始終顯示在匯入期間選擇的資源中最頂層的父資源。

4. 如果在匯入過程中發生衝突，並且您選擇將現有資源替換為新資源，這意味著連結到被替換資源的所有其他資源都會自動替換為匯入的資源。

已知錯誤：

1. 在下列情況下，連結資源最終位於匯入期間指定的租用戶中，而不是共用租用戶中，如**衝突**視窗所示：

   a. 關聯資源最初位於共用租用戶中。

   b. 在**衝突**視窗中，針對來自共用租用戶的連結資源的所有父物件選擇**略過**。

   c. 您保留共用租用戶中的連結資源以進行替換。

2. 匯入後，在下列情況下，類別沒有在篩選器中指定的租用戶：

   a. 篩選器包含來自不同租用戶的連結資產類別。

   b. 資產類別名稱相同。

   c. 您正在將具有連結資產類別的此篩選器匯入到新伺服器。

3. 在租用戶1中，在下列情況下，資產類別的名稱是相同的：

   a. 在租用戶1中，您有一個篩選器，其中包含來自租用戶1和共用租用戶的連結資產類別。

   b. 連結資產類別的名稱相同。

   c. 您正在將這樣的篩選器從租用戶1匯入到共用租用戶。

4. 您無法將衝突的資源匯入同一租用戶。

「*不允許將衝突的資源匯入同一租用戶*」錯誤表示匯入的資源包包含來自不同租用戶的衝突資源，因此無法匯入共用租用戶。

解決方案：選擇共用以外的租用戶來匯入資源包。在這種情況下，在匯入過程中，原本位於共用租用戶中的資源將會匯入至共用租用戶，而來自其他租用戶的資源將會匯入至匯入期間所選的租用戶。

5. 只有主管理員可以將類別匯入共用租用戶。

   *只有主管理員可以將類別匯入共用租用戶*錯誤表示匯入的資源包包含連結了共用資產類別的資源。KUMA Core 日誌中會顯示類別或連結了共用資產類別的資源。Core日誌的路徑：

   /opt/kaspersky/kuma/core/log/core

   解決方案。您可以選取以下其中一個方法：

   - 請勿匯入連結了共用類別的資源：清除相關資源旁的核取方塊。
   - 請使用一般管理員帳戶執行匯入。

6. 只有一般管理員可以將資源匯入共用租用戶。

   *只有主管理員可以將資源匯入共用租用戶*錯誤表示匯入的資源包包含連結了共用資源的資源。連結了共用資源的資源會顯示在 KUMA Core 日誌中。Core日誌的路徑：

   /opt/kaspersky/kuma/core/log/core

   解決方案。您可以選取以下其中一個方法：

   - 請勿匯入連結了來自共用租用戶資源的資源以及共用資源本身：清除相關資源旁的核取方塊。
   - 請使用一般管理員帳戶執行匯入。

標籤管理

為了幫助管理資源，KUMA允許您為資源新增標籤。您可以使用標籤搜尋元件，以及管理標籤、關聯或取消關聯標籤。

您無法為從其他資源介面建立的資源新增標籤。標籤只能從資源本身的卡片中新增。您也無法為不可編輯的資源新增標籤。

標籤管理

標籤清單顯示在**設定→KUMA→開啟KUMA設定→標籤**部分，並以表格形式顯示，包含以下列：**名稱**、**租用戶**和**用於資源**。

在**標籤**表格中，您可以：

- 依**名稱**和**用於資源**欄位對標籤進行排序。
- 依**租用戶**欄位的值進行篩選。
- 依**名稱**欄位找尋標籤。
- 轉到具有所選標籤的資源清單。

新增標籤

若要新增標籤：

1. 在主選單中，轉至**監控→資源與服務**，然後選擇一個資源。
2. 在表格上方的窗格中，按一下**新增**。
3. 在所選資源的**標籤**欄位中，新增標籤或從清單中選擇一個標籤。
4. 點擊**建立**按鈕。

   新標籤隨即新增。

您也可以從現有標籤中新增標籤。

新增標籤時，請注意以下事項：

- 您可以新增多個標籤。
- 標籤可以包含各種字母（例如西里爾字母、拉丁字母或希臘字母）、數字、底線和空格。
- 除底線和空格外，標籤不能包含任何特殊字元。
- 標籤可以大寫或小寫，但儲存後，標籤始終以小寫形式顯示。
- 標籤會繼承它所在資源的租用戶。
- 標籤是資源的一部分，只要建立或使用該標籤的資源存在，標籤就一直存在。
- 標籤在同一租用戶內是唯一的。
- 標籤作為資源的一部分，與資源一起匯入或匯出。

依標籤搜尋

在**資源**部分，您可以搜尋資源：

- 依標籤
- 依資源名稱

搜尋將涵蓋所有資源類型和服務。

搜尋結果會顯示資源和服務清單。

如要依標籤找尋資源：

1. 在主選單中，轉至**監控→資源與服務**，然後選擇一個資源。
2. 在資源表中，選擇**標籤**直欄。
3. 在顯示的**搜尋**欄位中，輸入或選擇標籤名稱。
   在資源本身和資源清單中依標籤搜索，會返回輸入的文字與標籤名稱的完整匹配項和部分匹配項。

   如果指定的標籤出現在某些資源中，則顯示這些資源的清單。

在資源清單中，您可以：

- 依名稱和資源或服務類型對清單進行排序。
- 依資源或服務類型或標籤篩選資源或服務。
- 關聯或取消關聯標籤。

當新增依賴資源時顯示標籤

新增依賴資源時，該資源的標籤會顯示在**篩選設定**的下拉清單中。

無法在單行中顯示的資源標籤將被隱藏。特殊指示器會顯示隱藏的標籤。

下拉清單可以依資源名稱和資源標籤進行篩選。

關聯和取消關聯標籤

若要將標籤關聯到資源或從資源中取消關聯標籤：

1. 在主功能表中，轉至**監控→資源與服務**。
2. 選取**清單**頁籤。
3. 在**名稱**欄位中，選取相關資源旁的核取方塊。
4. 在清單上方的窗格中，選擇**標籤**頁籤。
5. 按一下**關聯**或**取消關聯**，選擇所需的標籤或新建標籤。

   選定的標籤將關聯到資源或從資源中取消關聯。

   您也可以在資源卡中關聯或取消關聯標籤。

標準化器

標準化器用於將來自各種來源的不同格式的原始事件轉換為KUMA事件資料模型。標準化的事件可供其他KUMA資源和服務處理。

標準化器由*主*事件解析規則和可選的*附加事件解析規則*組成。透過建立主解析規則和附加解析規則集，您可以實現複雜的事件處理邏輯。資料根據**額外標準化條件**設定中指定的條件沿著解析規則樹傳遞。解析規則的建立順序很重要：事件會依序處理，處理順序以箭頭表示。

現在有以下事件標準化選項可用：

- 1個收集器 — 1個標準化器

  如果您有許多相同類型的事件或許多可能產生相同類型事件的IP位址，我們建議使用此方法。您只需使用一個標準化器來設定一個收集器，這在效能方面是最佳的。

- 1 個收集器 — 連結到IP的多個標準化器

  此方法適用於具有UDP、TCP或HTTP類型連接器的收集器。若於收集器的「傳輸」步驟中指定了UDP、TCP或HTTP連接器，則在「事件解析」步驟中，可於「解析設定」頁籤上指定多個IP位址，並為來自這些指定位址的事件選取要使用的標準化器。以下標準化器類型可供使用：`json`、`cef`、`regexp`、`syslog`、`csv`、`kv`、`xml`。對於 `syslog` 與 `regexp` 類型的標準化器，可根據 DeviceProcessName 欄位的值指定額外的標準化條件。

標準化器的建立分為幾個步驟：

1. **準備建立標準化器**

   可以在KUMA主控台中建立標準化器：

   - 在**監控** → **資源** → **標準化器**部分。
   - 建立收集器時，在事**事件解析**步驟。

   然後必須在標準化器中建立解析規則。

2. **為事件建立主解析規則**

   透過點選**新增事件解析**按鈕可以建立主解析規則。這將開啟**事件解析**視窗，您可以在其中指定主解析規則的設定：

   - 指定事件解析設定。
   - 指定事件擴充設定。

   事件的主解析規則在標準化器中顯示為深色圓圈。您可以透過點擊此圓圈來查看或修改主解析規則的設定。將滑鼠遊標停留在圓圈上時，一個加號隨即顯示。點擊它即可新增解析規則。

   主解析規則的名稱在KUMA中用作標準化器名稱。

3. **建立附加事件解析規則**

將滑鼠游標停留在與標準化器對應的圓圈或區塊上時，點擊顯示的加號圖標，即可開啟**額外事件解析**視窗，您可以在其中指定附加解析規則的設定：

- 指定將資料傳送到新標準化器的條件。
- 指定事件解析設定。
- 指定事件擴充設定。

附加事件解析規則在標準化器中顯示為深色區塊。此區塊顯示附加解析規則的觸發條件、附加解析規則的名稱和事件欄位。當此事件欄位可用時，資料將傳遞給標準化器。按一下附加解析規則的區塊以檢視或修改其設定。

如果將滑鼠游標停留在附加標準化器上，則會出現一個加號按鈕。您可以按一下此按鈕來建立新的附加事件解析規則。若要刪除標準化器，請使用帶有垃圾桶圖示的按鈕。

4. **完成標準化器的建立**

若要完成標準化器的建立，請按一下**儲存**。

在右上角的搜尋欄位中，您可以按名稱搜尋附加解析規則。

對於標準化器資源，您可以在除描述欄位之外的所有輸入欄位中啟用**控制字元的顯示**。

如果在變更收集器資源集的設定時，更改或刪除連線到它的標準化器中的轉換，則編輯將不會儲存，並且標準化器本身可能會損壞。若要修改已經是服務一部分的標準化器中的轉換，則必須直接在OSMP主控台中的**監控 → 資源 → 標準化器**下對標準化器進行變更。

事件解析設定

在標準化器設定視窗的標準化方案頁籤中**建立事件解析規則**時，您可以設定將傳入事件轉換為KUMA格式的規則。

若要定義事件解析設定：

1. 在 **卡巴斯基儲存庫中的資源版本**欄位中，會指定資源版本號。

   此欄位不可編輯。僅適用於卡巴斯基提供的資源，並用於管理資源更新。

2. 在**名稱**欄位（必填）中，輸入解析規則的唯一名稱。必須包含1至255個Unicode字元。主解析規則的名稱用作標準化器的名稱。

3. 在**租用戶**欄位（必填）中，輸入擁有資源的租用戶名稱。

   此設定不適用於額外的解析規則。

4. 在**解析方法**下拉清單中，選擇要接收的事件類型。根據您的選擇，您可以使用預設定的規則來符合事件欄位或設定您自己的規則。當您選擇某些解析方法時，可能需要填寫其他設定欄位。

   可用的解析方法：

   - **json**

     此解析方法用於處理JSON資料，其中每個物件（包括其嵌套物件）在檔案中佔用一行。

     在處理具有階層結構資料的檔案時，您可以指定以句點分隔的參數名稱，存取嵌套物件的欄位。例如，可使用 `user.username` 查詢來存取字串 `"user": {"username": "system: node: example-01"}` 中的 `username` 參數。

檔案將逐行處理。具有嵌套結構的多行物件可能無法正確標準化。

在使用額外標準化器的複雜標準化方案中，所有嵌套物件都會在第一個標準化層級進行處理；但若未指定額外的標準化條件，正在處理的整個事件就會傳送至額外標準化器。

換行字元可以是`\n`和`\r\n`。字串必須採用UTF-8編碼。

如果要傳送原始事件進行進階標準化，請在**進階事件解析**視窗的每個巢狀層級上，在**保留原始事件**下拉清單中選擇**是**。

- **cef**

  此解析方法用於處理CEF資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。

- **regexp**

  此解析方法用於建立自訂規則，以使用正規運算式的格式處理資料。

  在**標準化**參數區塊的欄位中，新增含有具名擷取群組的正規運算式（使用 RE2 語法）。群組的名稱和值會分別視為原始事件的欄位及其值，並可轉換為 KUMA 格式的事件欄位。

  若要新增事件處理規則：

  1. 將您要處理的資料範例複製到**事件範本**欄位。這是可選的，但建議執行的步驟。

     您也可以點選**使用 KIRA 產生規則運算式**，使用 KIRA 產生規則運算式。在此情況下，產生的規則運算式將自動新增至**標準化**參數區塊。

  2. 在**標準化**參數區塊的欄位中，新增使用 RE2 語法且含有具名擷取群組的正規運算式，例如「(?P<name>regexp)」。新增至**標準化**參數的正規運算式必須與事件完全相符。此外，編寫正規運算式時，建議使用符合文字起始和結束位置的特殊字元：^、$。

     您可以按一下**新增正規運算式**按鈕，新增多個正規運算式。如果需要移除正規運算式，請按一下✕按鈕。

  3. 按一下**將欄位名稱複製到對應表**按鈕。

     擷取群組名稱顯示在**對應**表的**KUMA欄位**列中。現在，您可以在每個擷取群組旁的欄中選取對應的 KUMA 欄位。如果您依照 CEF 格式命名擷取群組，也可以選取**使用 CEF 語法進行標準化**核取方塊，使用自動 CEF 對應。

  已新增事件處理規則。

- **syslog**

  此解析方法用於處理syslog格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。

- **csv**

  此解析方法用於建立處理CSV資料的自訂規則。

  選擇此方法時，您必須在**分隔符號**欄位中指定字串中各值之間的分隔符號。任何單位元組 ASCII 字元都可以用作分隔符號。

- **kv**

  此解析方法用於處理鍵值對格式的資料。

  如果選擇此方法，您必須在下列必填欄位中提供值：

  - **配對分隔符號**—指定用來分隔鍵值對的字元。您可以指定任何單一字元（1位元組）的值，但該字元不得與值分隔符號相同。
  - **值分隔符號**—指定用來分隔金鑰和值的字元。您可以指定任何單一字元（1位元組）的值，但該字元不得與鍵值對的分隔符號相同。

- **xml**

  此解析方法用於處理 XML 資料。檔案中的每個物件（包括其巢狀物件）各佔一行。檔案將逐行處理。

  如果要傳送原始事件進行進階標準化，請在**進階事件解析**視窗的每個巢狀層級上，在**保留原始事件**下拉清單中選擇**是**。

  選擇此方法後，您可以在**XML 屬性**參數區塊中指定要從標籤擷取的金鑰屬性。如果 XML 結構中的同一個標籤具有多個值不同的屬性，您可以在**對應**表格的**來源**欄中指定所需值的金鑰。

  若要新增 XML 金鑰屬性，

  按一下**新增欄位**按鈕，然後在顯示的視窗中指定所需屬性的路徑。

  您可以新增多個屬性。可以使用叉號圖示逐一移除屬性，或按一下**重設**按鈕一次移除所有屬性。

  如果未指定XML關鍵屬性，則在欄位對應過程中，XML值的唯一路徑將由一系列標籤表示。

  標籤編號

  標籤編號功能自 KUMA 2.1.3 起提供。此功能可自動為 XML 事件中的標籤編號，讓您能夠解析含有相同標籤或未命名標籤（例如 <Data>）的事件。

  例如，我們將使用**標籤編號**功能，為**Microsoft Windows PowerShell 事件 ID 800** 的 EventData 屬性中的標籤編號。

  若要解析此類事件，您必須：

  - 設定標籤編號。
  - 設定編號標籤與 KUMA 事件欄位之間的資料對應。

  KUMA 3.0.x 支援在同一個額外標準化器中同時使用**XML 屬性**和**標籤編號**功能。如果屬性包含未命名標籤或相同標籤，建議使用**標籤編號**功能。如果屬性只包含具名標籤，請使用**XML 屬性**。若要在額外標準化器中使用此功能，您必須依序在事件通往目標額外標準化器的路徑上，為每個額外標準化器以及目標額外標準化器本身啟用「保留原始事件」設定。

  如需此功能的實際使用範例，請參閱 MicrosoftProducts 標準化器：「AD FS」和「424」額外標準化器已依序啟用「保留原始事件」設定。

若要設定具有相同名稱或未命名標籤的事件解析：

1. 建立新的標準化器，或開啟現有的標準化器進行編輯。

2. 在標準化器的**基本事件解析**視窗中，從**解析方法**下拉清單選取「xml」，然後在**標籤編號**欄位中點選**新增欄位**。

   在顯示的欄位中，輸入您要為其元素指派編號的標籤完整路徑。例如，Event.EventData.Data。指派給標籤的第一個編號是 0。如果標籤是空的，例如 <Data />，也會為其指派編號。

3. 若要設定資料對應，請在**對應**下點選**新增資料列**，然後執行下列操作：

   a. 在新資料列的**來源**欄位中，輸入標籤的完整路徑及其索引。對於上述範例中的 Microsoft Windows 事件，含索引的完整路徑如下：

   - Event.EventData.Data.0,
   - Event.EventData.Data.1
   - Event.EventData.Data.2，以此類推

   b. 在**KUMA欄位**下拉清單中，選擇KUMA事件中解析後將從編號標籤接收值的欄位。

4. 若要儲存變更：

   - 如果您建立了新的標準化器，請按一下**儲存** 。
   - 如果您編輯了現有的標準化器，請在與該標準化器連結的收集器中按一下**更新設定**。

解析隨即設定。

- **netflow5**

  此解析方法用於處理NetFlow v5格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 netflow5 類型進行主要解析，則無法進行額外的標準化。

  > 在對應規則中，預設不會在 KUMA 事件的欄位中指出 **netflow5** 的通訊協定類型。解析 NetFlow 格式的資料時，必須在**擴充**標準化器索引標籤上建立一條**常數**資料擴充規則，該規則會將 `netflow` 值新增至 `DeviceProduct` 目標欄位。

- **netflow9**

  此解析方法用於處理NetFlow v9格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 netflow9 類型進行主要解析，則無法進行額外的標準化。

  > 在對應規則中，預設不會在 KUMA 事件的欄位中指出 **netflow9** 的通訊協定類型。解析 NetFlow 格式的資料時，必須在**擴充**標準化器索引標籤上建立一條**常數**資料擴充規則，該規則會將 `netflow` 值新增至 `DeviceProduct` 目標欄位。

- **sflow5**

  此解析方法用於處理sflow5格式的資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 sflow5 類型進行主要解析，則無法進行額外的標準化。

- **ipfix**

  此解析方法用於處理IPFIX資料。

  選擇此方法時，您可以按一下**套用預設對應**按鈕，使用預先設定的規則將事件轉換為 KUMA 格式。如果選擇 ipfix 類型進行主要解析，則無法進行額外的標準化。

  > 在對應規則中，預設不會在 KUMA 事件的欄位中指出 **ipfix** 的通訊協定類型。解析 NetFlow 格式的資料時，必須在**擴充**標準化器索引標籤上建立一條**常數**資料擴充規則，該規則會將 `netflow` 值新增至 `DeviceProduct` 目標欄位。

- sql —僅當使用sql類型的連接器時，此方法才可用。

  標準化器使用此方法處理從資料庫選取的資料。

5. 在**保留原始事件**下拉清單中，指定是否將原始原始事件儲存在新建立的標準化事件中。可用值：

   - **不儲存**— 不儲存原始事件。這是預設設定。
   - **僅錯誤** — 若解析事件時發生錯誤，將原始事件儲存於標準化事件的 `Raw` 欄位中。該值便於在服務偵錯時使用。如此，只要事件的 `Raw` 欄位不為空，即可判定存在問題。

     > 若包含名稱 `*Address` 或 `*Date*` 的欄位不符合標準化規則，這些欄位將被略過。此情況下不會發生標準化錯誤，而且即使已選取**保留原始事件** → **僅錯誤**選項，欄位值也不會顯示在標準化事件的 `Raw` 欄位中。

   - **總是**— 一律將原始事件儲存於標準化事件的 `Raw` 欄位中。

   此設定不適用於額外的解析規則。

6. 在**保留額外欄位**下拉式清單中，可選取當原始事件欄位未設定對應規則時，是否將其儲存於標準化事件內（參見下文）。資料儲存於 `Extra` 事件欄位。標準化事件可基於儲存於 `Extra` 欄位中的資料進行搜尋與篩選。

   基於「額外」事件欄位資料的篩選：

   基於**額外**事件欄位資料的篩選器條件：

   - 條件 —**如果**。
   - 左運算元 —**事件欄位**。
   - 在此事件欄位中，您可以指定以下其中一個值：
     - **Extra**欄位。
     - Extra 欄位中的值，格式如下：

`Extra.<field name>`

例如，`Extra.app`。

這種類型的值需手動指定。

- 寫入**Extra**欄位的陣列值須符合以下格式：

  `Extra.<field name>.<array element>`

  例如，`Extra.array.0`。

  陣列中的值從0開始編號。

  這種類型的值需手動指定。

  若要使用 Extra 欄位中深度為 3 或更深層的值，請使用反引號 ``。例如，`Extra.lev1.lev2.lev3`。

- 運算子 — =。
- 右運算元 —**常數**。
- 值 — 您需要用來篩選事件的值。

預設情況下，不儲存欄位。

7. 在**描述**欄位中，指定資源描述：最多4,000個Unicode字元。

   此設定不適用於額外的解析規則。

8. 在**事件範例**欄位中，您可以提供要處理的資料範例。

   此設定不適用於以下解析方法：**netflow5**、**netflow9**、**sflow5**、**ipfix**、**sql**。

   如果**事件範例**成功，並且從原始事件取得的資料類型與KUMA欄位的類型相符，則事件範例欄位將填入從原始事件取得的資料。

   例如，引號中的值「192.168.0.1」不會顯示在來源位址欄位中，在這種情況下，值192.168.0.1會顯示在**事件範例**欄位中。

9. 在**對應**表中，設定原始事件欄位到KUMA格式的事件欄位的對應：

   a. 在**來源**列中，提供要轉換為KUMA事件欄位的原始事件欄位的名稱。

   如需欄位格式的詳細資訊，請參閱「正規化事件資料模型」一文。如需對應的說明，請參閱「預先定義的正規化器欄位對應」一文。

   點選**來源**欄中欄位名稱旁邊的按鈕會開啟**轉換**視窗，您可以在其中點選**新增轉換**按鈕來建立規則，以便在將原始資料寫入KUMA事件欄位之前加以修改。

   可用的轉換

   轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

   可用轉換類型：

   - **小寫** — 用於將值的所有字元變為小寫
   - **大寫** — 用於將值的所有字元變為大寫
   - **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
   - **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。

- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。
- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

在**轉換**視窗中，您可以透過⣿圖示拖曳新增的規則來交換其順序；您也可以使用✕圖示刪除這些規則。

b. 在**KUMA欄**位列中，從下拉清單中選擇所需的KUMA事件欄位。您可以透過在欄位中輸入欄位名稱來搜尋欄位。

關於 KUMA 欄位欄的建議

我們建議您設定以下KUMA欄位的對應。否則，您將無法在警示詳情和事件詳情中檢視可觀察物件。

建議的KUMA欄位取決於可觀察物件的類型：

- 對於MD5雜湊值和SHA256類型的可觀察物件：
  - FileHash
- 對於URL類型的可觀察物件：
  - RequestUrl
- 對於IP位址類型的可觀察物件：
  - DeviceCustomIPv6Address1
  - DeviceCustomIPv6Address2
  - DeviceCustomIPv6Address3
  - DeviceCustomIPv6Address4
  - DestinationTranslatedAddress
  - DeviceTranslatedAddress
  - DestinationAddress
  - DeviceAddress
  - SourceTranslatedAddress
  - SourceAddress
- 對於網域名稱類型的可觀察物件：
  - DestinationDnsDomain
  - DeviceDnsDomain
  - DeviceNtDomain
  - DestinationNtDomain

- SourceDnsDomain
- SourceNtDomain

- 對於使用者名稱類型的可觀察物件：
  - DestinationUserName
  - SourceUserName
- 對於主機名稱類型的可觀察物件：
  - DestinationHostName
  - DeviceHostName
  - SourceHostName

c. 若前一步驟選取的 KUMA 事件欄位名稱以 `DeviceCustom*` 或 `Flex*` 開頭，可在**標籤**欄位中新增唯一的自訂標籤。

可使用 **新增資料列** 按鈕新增表格資料列。可使用 ✕ 按鈕逐一刪除資料列，或使用 **全部清除** 按鈕一次刪除所有資料列。

如果您要KUMA使用資產資訊擴充事件，並在觸發關聯規則時在警示卡中顯示資產訊息，請在**對應**表中根據資產的用途設定主機位址和主機名欄位的對應。例如，對應可以套用至SourceAddress和SourceHostName，或DestinationAddress和DestinationHostName欄位。擴充後，事件卡將包含SourceAssetID或DestinationAssetID欄位，以及指向資產卡的連結。此外，擴充後，資產資訊也會顯示在警示卡中。

如果您已將資料載入到**事件範例**欄位中，則此表將包含一個**範例**列，其中包含從原始事件欄位轉移到KUMA事件欄位的值範例。

如果KUMA事件欄位的大小小於其中放置的值的長度，則此值將被截斷為事件欄位的大小。

擴充事件結構描述

在標準化事件時，除了標準KUMA事件結構描述欄位外，還可以使用擴充事件結構描述欄位。下表顯示了擴充事件結構描述欄位類型的資訊。

使用過多擴展事件結構描述的唯一欄位可能會降低系統效能、增加儲存事件所需的磁碟空間，並使資訊難以理解。

我們建議您有意識地選擇要在標準化器和關聯中使用的擴展事件結構描述的最小附加欄位集。

若要使用擴充事件結構描述欄位：

- 開啟現有的事件標準化器或建立新的事件標準化器。
- 指定標準化器的基本設定。
- 點擊**新增行**。
- 對於**來源**設置，輸入原始事件中來源欄位的名稱。

- 對於**KUMA 欄位**設置，輸入您正在建立的擴充事件結構描述欄位的名稱（請參閱下表）。您也可以使用擴充事件結構描述的現有欄位。

  標準化事件的擴展資料模型的欄位：

欄位名稱 在KUMA欄位設定中指定	資料類型	在標準化器中的可用性	描述
S.<欄位名稱>	字串	所有類型	`String` 類型的欄位
N.<欄位名稱>	數字	所有類型	`Number` 類型的欄位
F.<欄位名稱>	浮點型	所有類型	`Float` 類型的欄位
SA.<欄位名稱>	字串陣列	KV, JSON	`Array of strings` 類型的欄位。陣列元素的順序與原始事件元素的順序相同。
NA.<欄位名稱>	整數陣列	KV, JSON	一個 `Array of integers` 類型的欄位。陣列元素的順序與原始事件元素的順序相同。
FA.<欄位名稱>	浮點陣列	KV, JSON	`Array of floats` 類型的欄位。陣列元素的順序與原始事件元素的順序相同。

建立延伸事件結構描述欄位時，首碼`S.`、`N.`、`F.`、`SA.`、`NA.`、`FA.`為必填項，且首碼必須嚴格採用大寫格式。

請將<欄位名稱>替換為實際欄位名稱。該欄位名稱可使用英文字母與數字。不允許使用空格字元。

- 點擊**確定**。
- 點擊**儲存**以完成編輯事件標準化器。

將儲存標準化器並建立附加欄位。儲存標準化器後，即可在其他標準化器中使用附加欄位。

注意：若原始事件欄位中的資料與KUMA欄位的類型不相符，則不會在事件標準化期間儲存該值。例如，字串 `test` 無法寫入 `Number` 類型的 DeviceCustomNumber1 KUMA 欄位。

如果您希望在搜尋事件、準備報告以及對儲存中的事件執行其他操作時盡量減少儲存伺服器上的負載，請將KUMA事件結構描述欄位作為首選，將擴展事件結構描述欄位作為第二選擇，並將Extra欄位作為最後的選擇。

擴充事件結構描述

您可以在規範化器中使用擴充事件結構欄位來規範化事件，也可以在其他KUMA 資源中使用，例如用作小工具欄位或用於篩選和搜尋事件。您可以在**設定→KUMA→開啟KUMA設定→擴充欄位集**部分查看KUMA中所有擴充事件結構欄位的清單。所有租用戶的擴充事件架構欄位清單均相同。

在該區段的頂部，會顯示擴充套件欄位集的版本號。此版本用於管理擴充欄位的更新。

只有具備主管理員、租用戶管理員、二級分析師、一級分析師、初級分析師、讀取共用資源和管理共用資源角色的使用者，才能檢視擴充事件結構欄位表。

擴充事件結構欄位表包含以下資訊：

- **類型**— 擴充事件結構欄位的資料類型。

  可能的資料類型：

類型	在標準化器中的可用性	資料類型
S	所有類型	字串。
N	所有類型	數字。

類型	在標準化器中的可用性	資料類型
F	所有類型	浮點數。
SA	KV, JSON	字串陣列。 陣列元素的順序與原始事件元素的順序相同。
NA	KV, JSON	整數陣列。 陣列元素的順序與原始事件元素的順序相同。
FA	KV, JSON	浮點陣列。 陣列元素的順序與原始事件元素的順序相同。

- **欄位名稱**— 擴充事件結構欄位的名稱，不包含類型。

  您可以點選名稱來編輯擴充事件結構欄位的設定。

- **狀態**— 擴充事件結構欄位是否可用於資源。

  您可以**啟用**或**停用**切換開關，以啟用或停用在新資源中使用此擴充事件結構欄位。但是，停用的欄位仍然在已運行的資源組態中使用，直到您從組態中手動刪除該欄位；該欄位在**事件**部分的表格直欄清單中仍然可用，用於管理舊事件。

  只有具有主管理員角色的使用者才能停用擴充事件結構欄位。

- **更新日期**— 擴充事件結構欄位的最後修改日期和時間。

- **建立者**— 建立擴展事件結構欄位的使用者的名稱。

- **依賴項**—使用擴充事件結構欄位的KUMA 資源、儀表板版面配置、報告、預設，以及用於搜尋事件來源的欄位集數量。

  您可以點擊該數字以開啟一個窗格，其中包含使用此欄位的所有資源和其他KUMA實體的表格。對於每個依賴項，表格會顯示其名稱、租用戶（僅適用於資源）和類型。表格中的依賴項依名稱排序。點擊依賴項的名稱即可進入其頁面（儀表板佈局、預設和已儲存的使用者查詢除外）。

  您只能查看您有權存取的租用戶的資源和擴充事件結果欄位的依賴項。如果您沒有該租用戶的存取權限，則其資源將不會顯示在表中，但仍會計入依賴項的數量。

- **描述**— 欄位的文字描述。

預設情況下，擴充事件結構欄位表會依更新日期降序排列。如有必要，您可以透過點擊直欄標題並選擇**升序**或**降序**來對表格進行排序；您也可以依欄位名稱進行上下文搜尋。

預設情況下，以下服務擴充事件結構欄位會自動新增至KUMA：

- `KL_EventRoute`，類型為 `S`，用於儲存事件路徑的資訊。

  您可以在規範化器中使用此欄位，在活動清單中用作鍵或值，在擴充規則中，在資料收集和分析規則中用作查詢欄位，在關聯規則中使用。此欄位不能用於偵測事件來源。

- 以下欄位將會新增至關聯事件：

  - `KL_CorrelationRulePriority`，類型為 `N`
  - `KL_SourceAssetDisplayName`，類型為 `S`
  - `KL_DestinationAssetDisplayName`，類型為 `S`
  - `KL_DeviceAssetDisplayName`，類型為 `S`

- `KL_SourceAccountDisplayName`，類型為 `S`
- `KL_DestinationAccountDisplayName`，類型為 `S`

您不能使用此服務欄位搜尋事件。

您無法編輯、刪除、匯出或停用服務欄位。所有包含 `KL_` 前綴的擴充事件結構欄位都是服務欄位，只能從卡巴斯基伺服器進行管理。我們不建議在新增擴充事件結構欄位時使用 `KL_` 前綴。

新增擴充事件結構欄位

具有主管理員、租用戶管理員、第 2 級分析師、第 1 級分析師、初級分析師或管理共用資源角色的使用者，可以新增擴充事件結構欄位。

若要新增擴充事件結構欄位：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟KUMA設定**部分。
   這將開啟KUMA設定視窗。
2. 在**其他**下，按一下**擴充欄位集**。
   這將打開**擴展欄位集**視窗。
3. 點擊表格頂部的**新增**按鈕。
   這將開啟**建立擴充結構**窗格。
4. 啟用或停用**狀態**切換開關，以啟用或停用此擴充事件結構欄位。
   切換開關預設為開啟。禁用的欄位仍保留在**事件**部分的表格直欄清單中，用於管理舊事件。
5. 在**類型**欄位中，選擇擴充事件結構欄位的資料類型。
   可能的資料類型

類型	在標準化器中的可用性	資料類型
S	所有類型	字串。
N	所有類型	數字。
F	所有類型	浮點數。
SA	KV, JSON	字串陣列。 陣列元素的順序與原始事件元素的順序相同。
NA	KV, JSON	整數陣列。 陣列元素的順序與原始事件元素的順序相同。
FA	KV, JSON	浮點陣列。 陣列元素的順序與原始事件元素的順序相同。

6. 在**名稱**欄位中，指定擴充事件結構欄位的名稱。
   命名擴充事件結構欄位時，請注意以下事項：
   - 名稱在KUMA實例中必須是唯一的。
   - 名稱區分大小寫。例如，`Field_name` 和 `field_name` 是不同的名稱。
   - 您可以使用拉丁字母、西里爾字母和數字。不允許使用空格或“~`@#$%^&*()+-[]{}|\|/."<>:!,.?=”字元。

- 如果要使用擴充事件結構欄位搜尋事件來源，則只能使用拉丁文字元和數字。
- 最大長度為128個字元。

7. 如有必要，請在**描述**欄位中輸入擴充事件結構欄位的描述。

   我們建議描述擴展事件結構欄位的用途。描述中僅允許使用Unicode字元。最大長度為256個字元。

8. 按一下**儲存**按鈕。

新的擴充事件結構欄位將會新增並顯示在表格頂部。系統會為建立擴充事件結構欄位產生一個稽核事件。如果已啟用該欄位，則可以在規範化器中和設定資源時使用它。

編輯擴充事件結構欄位

具有主管理員、租用戶管理員、第 2 級分析師、第 1 級分析師、初級分析師及管理共用資源角色的使用者，可以編輯現有的擴充事件結構欄位。

若要編輯擴充事件結構欄位：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟KUMA設定**部分。

   這將開啟KUMA設定視窗。

2. 在**其他**下，按一下**擴充欄位集**。

   這將打開**擴展欄位集**視窗。

3. 點擊要編輯的欄位名稱。

   這將開啟**編輯擴充結構**窗格。此窗格顯示所選欄位的設置，以及**依賴項**表，其中包含用於尋找使用此欄位的事件來源的資源、儀表板佈局、報告、預設和欄位集的清單。表中僅顯示您有權存取的租用戶的資源。如果該欄位用於您無權存取的租用戶的資源，則這些資源不會顯示在表中。表中的資源會依名稱排序。

   點擊資源或實體的名稱即可進入其頁面（儀表板資源、預設和已儲存的使用者查詢除外）。

4. 在可用設定中進行您需要的更改。

   只有當擴充事件結構欄位沒有依賴項時，才能編輯**類型**和**欄位名稱**設定。您可以編輯任何擴充事件結構欄位的**狀態**和**描述**設定。但是，狀態為**已停用**的欄位仍會在已運行的資源組態中使用，直到您從組態中手動刪除該欄位；該欄位在**事件**部分的表格直欄清單中仍然可用，用於管理舊事件。

   若要使用**狀態**欄位停用擴充事件結構欄位，需要主管理員角色。

5. 按一下**儲存**按鈕。

擴充事件結構欄位隨即更新。系統會產生一條關於欄位修改的稽核事件。

匯入和匯出擴充事件結構欄位

您可以透過從JSON檔案匯入，一次新增多個擴充事件結構欄位。您還可以將所有擴充事件結構欄位以及相關資訊匯出到檔案中，例如，將欄位列表傳播到其他KUMA實例以維護資源。

具有主管理員、租用戶管理員、第 2 級分析師、第 1 級分析師、初級分析師和管理共享資源角色的使用者可以匯入和匯出擴充事件結構欄位。具有「讀取共享資源」角色的使用者只能匯出擴展事件結構欄位。

若要從檔案中將擴充事件結構欄位匯入KUMA：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟KUMA設定**部分。
   這將開啟KUMA設定視窗。
2. 在**其他**下，按一下**擴充欄位集**。
   這將打開**擴展欄位集**視窗。
3. 點擊**匯入**按鈕。
4. 這會開啟一個視窗；在該視窗中，選擇一個包含擴充事件結構欄位物件清單的JSON檔案。
   JSON檔案範例：

```
[
{"kind": "SA",
"name": "<fieldName1>",
"description": "<description1>",
"disabled": false},
{"kind": "N",
"name": "<fieldName2>",
"description": "<description2>",
"disabled": false},
....
{"kind": "FA",
"name": "<fieldNameX>",
"description": "<descriptionX>",
"disabled": false}
]
```

從檔案匯入欄位時，系統會檢查欄位名稱是否與同類型欄位衝突。如果KUMA中已存在同名同類型的欄位，則不會從檔案匯入這些欄位。

擴充事件結構欄位將從檔案匯入到KUMA。系統會產生一個關於欄位匯入的稽核事件，並且每個新增的欄位都會產生一個單獨的稽核事件。

若要將擴充事件結構欄位匯出至檔案：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟KUMA設定**部分。
   這將開啟KUMA設定視窗。
2. 在**其他**下，按一下**擴充欄位集**。
   這將打開**擴展欄位集**視窗。

3. 如果要匯出特定的擴充事件結構欄位：

   a. 選取表格第一列中所需欄位的核取方塊。

      您不能選擇服務欄位。

   b. 點按表格頂部的**匯出所選選項**按鈕。

4. 如果要匯出所有擴充事件結構欄位，請按一下表格頂部的**全部匯出**按鈕。

系統會下載一個包含擴充事件結構欄位物件清單及其相關資訊的JSON檔案。

刪除擴充事件結構欄位

只有具有主管理員角色的使用者才能刪除擴充事件結構欄位。

您只能刪除非服務欄位、狀態為**已停用**且未在KUMA資源和其他實體中使用（無依賴關係）的擴充事件結構欄位。我們建議您在經過足夠長的時間後再刪除擴展事件結構欄位，以確保所有使用該欄位的事件都已從KUMA中刪除。刪除欄位後，該欄位將不再顯示在事件提示中。

若要刪除擴充事件結構欄位：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟KUMA設定**部分。

   這將開啟KUMA設定視窗。

2. 在**其他**下，按一下**擴充欄位集**。

   這將打開**擴展欄位集**視窗。

3. 選取表格第一列中要刪除的一個或多個欄位旁的核取方塊。

   若要選擇所有欄位，您可以選中第一直欄標題中的核取方塊。

4. 點按表格頂部的**刪除**按鈕。

   刪除按鈕僅在所有選取欄位均已停用且無依賴關係時才處於活動狀態。如果至少有一個欄位已啟用或存在依賴關係，則該按鈕將處於非活動狀態。

   如果您要刪除的欄位在至少一個KUMA資源中使用（存在依賴關係），但您無法存取其租用戶，則選取該欄位時**刪除**按鈕將處於活動狀態，但嘗試刪除時會顯示錯誤。

所選欄位將被刪除。系統會產生一個關於欄位刪除的稽核事件。

在規範化器中使用擴充事件結構欄位

使用擴充事件結構欄位時，收集器可處理的事件大小上限仍為 4 MB。下表顯示了有關擴充事件結構欄位類型的資訊（說明的第6步）。

使用過多擴展事件結構描述的唯一欄位可能會降低系統效能、增加儲存事件所需的磁碟空間，並使資訊難以理解。

我們建議您有意識地選擇要在標準化器和關聯中使用的擴展事件結構描述的最小附加欄位集。

若要使用擴充結構模式的欄位：

1. 開啟現有的標準化器或建立新的標準化器。
2. 指定標準化器的基本設定。
3. 點擊**新增行**。
4. 對於**來源**設置，輸入原始事件中來源欄位的名稱。
5. 對於**KUMA欄位**設定，請開始輸入擴充事件結構欄位的名稱，然後從下拉清單中選擇該欄位。
   下拉清單中的擴充事件結構欄位名稱採用`<type>.<field name>`格式。
6. 按一下**儲存**按鈕來儲存事件規範化器。

規範化器隨即與選定的擴充事件結構欄位一起儲存。

如果原始事件欄位中的資料與KUMA欄位的類型不相符，如果無法執行類型轉換，則在事件規範化期間不會儲存該值。例如，字串 `test` 無法寫入 Number 類型的 `DeviceCustomNumber1` KUMA 欄位。

如果您希望在搜尋事件、準備報告以及對儲存中的事件執行其他操作時，盡可能降低儲存伺服器的負載，請優先使用 KUMA 事件結構欄位，其次使用擴充事件結構欄位，最後才使用 `Extra` 欄位。

使用 KIRA 產生正規表示式

透過卡巴斯基調查與回應助理，您可以根據使用 **regexp** 剖析方法之正規化器的事件範例，自動建立一或多個正規表示式。此功能適用於具有主管理員、租用戶管理員、二級分析師、一級分析師和初級分析師角色的使用者。

若要產生正規表示式：

1. 取得AI模組的產品授權，並在KUMA中啟動其功能。
2. 設定 KIRA 整合，使用第三方 LLM 提供者（**自訂**模式）。
3. 開始建立正規化器或開啟現有正規化器的設定。
4. 在 **標準化架構** 索引標籤的 **解析方法** 下拉式清單中，選取 **regexp**。
5. 在 **事件範例** 欄位中，新增您要用來建立正規表示式的一或多個事件範例。
   您最多可以新增 10 個單行事件。
6. 按一下 **使用 KIRA 產生規則運算式** 按鈕。
7. 確認您的要求。
   要求處理完成後，會顯示一個視窗，其中包含下列資訊：
   - 產生時花費的 Token 數量
   - 產生的正規表示式，並以顏色醒目提示群組和對應的範例事件片段。

   每個產生的正規表示式都以 (?:ai)? 字元群組開頭。

在含有已建立表示式的視窗中，您可以編輯和複製正規表示式，並按一下 **套用** 按鈕來套用產生結果。

如果正規表示式產生失敗或未產生預期結果，這可能表示您使用的提供者模型無法正確識別事件的元件或產生正規表示式。請嘗試重新開始產生。如果錯誤再次發生，請在 **事件範例** 欄位中新增更多類似範例，然後重新開始產生。發生錯誤後重新開始產生時，不會花費額外的 Token。

套用結果後，產生的正規表示式會自動新增至 **標準化** 欄位。如果已產生多個正規表示式，則會自動為每個表示式產生相應數量的欄位。正規表示式會依照產生的順序新增，如有需要，您可以透過 ⠿ 圖示拖曳表示式來變更順序。

8. 套用產生的正規表示式後，請按一下 **確定** 按鈕，然後按一下 **儲存** 按鈕，以儲存正規化器設定。

標準化器中的擴充功能

在標準化器設定視窗的擴充頁籤中**建立事件解析規則**時，您可以設定使用擴充規則為標準化事件欄位新增額外資料的規則。這些擴充規則儲存在建立它們的標準化器的設定中。

點擊**新增擴充規則**按鈕即可建立擴充規則。可以有多個擴充規則。您可以透過點擊 ✕ 按鈕來刪除擴充規則。

擴充規則設定區塊中可用的設定：

- **來源類型**（必要） - 用於選擇擴充類型的下拉清單。根據所選類型，可能會顯示其他也需要填寫的進階設定。

  可用的擴充規則來源類型：

  - **常數**

    當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定：

    - 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。
    - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

    若針對 `String`、`Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。

    若針對 `Array of strings`、`Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。

  - **字典**

    如果需要從字典類型的**字典**中新增值，則使用此類擴充。

    在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。

    如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。

    例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。

如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。

例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。

- **表格**

  如果您需要從表格類型的**字典**中新增值，請使用此類擴充。

  在**字典名稱**下拉清單中選擇此擴充類型後，請選擇用於提供值的字典。在**鍵欄位**設定群組中，按一下**新增欄位**按鈕以選擇其值用於選擇字典條目的事件欄位。

  在**對應**表中，設定用於提供資料的字典欄位和用於接收資料的事件欄位：

  - 在**字典欄位**直欄中，選擇字典欄位。可用欄位取決於所選的字典資源。
  - 在 **KUMA 欄位**直欄中，選取要寫入值的事件欄位。對於某些選取的欄位（ `*custom*` 與 `*flex*` ），您可以在**標籤**直欄中，為寫入其中的資料指定名稱。

  可以透過點選**新增元素**按鈕來新增表格行。可以透過按一下✕按鈕來刪除直欄。

- **事件**

  當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定：

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。
  - 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。
  - 按一下🔧按鈕會開啟**轉換**視窗，您可以在其中使用**新增轉換**按鈕建立規則，在將原始資料寫入 KUMA 事件欄位前對其進行修改。

    可用的轉換

    轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

    可用轉換類型：

    - **小寫** — 用於將值的所有字元變為小寫
    - **大寫** — 用於將值的所有字元變為大寫
    - **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
    - **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。
    - **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
      - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
      - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。

- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。

- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。

- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。

- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。

  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。

  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。

- 將編碼字串轉換為文字：

  - **decodeHexString** —用於將HEX字串轉換為文字。

  - **decodeBase64String** —用於將Base64字串轉換為文字。

  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。

- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。

- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。

- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

當您使用事件擴充功能，且在 **來源類型** 設定中選取 **事件**，並使用延伸事件結構描述的欄位作為引數時，須注意以下特殊事項：

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `String` 類型的欄位，則值會以 TSV 格式寫入目標欄位。

  範例：SA.StringArray 延伸事件結構描述欄位包含以下值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 DeviceCustomString1 事件結構描述欄位。操作結果為：DeviceCustomString1 欄位包含 ["string1", "string2", "string3"]。

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `Array of strings` 類型的欄位，則來源欄位的值會附加至目標欄位的值，並存入目標欄位，以逗號 (",") 作為分隔符號。

  範例：延伸事件結構描述欄位 SA.StringArrayOne 包含值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 SA.StringArrayTwo 事件結構描述欄位。操作結果為：SA.StringArrayTwo 欄位包含 "string1"、"string2"、"string3"。

- **範本**

  當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

  - 在 **範本**欄位中，輸入 Go 範本。

    事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。

    範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

  若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

  如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

  範例：

  {{.SA.StringArrayOne}}

  範例：

  {{- range $index, $element := .SA.StringArrayOne -}}

  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **目標欄位**（必填）— 用於選擇應接收資料的KUMA事件欄位的下拉清單。
  此設定不適用於**表格**類型的擴充來源。

將資料傳送到額外標準化器的條件

建立附加事件解析規則時，您可以指定條件。當滿足這些條件時，事件將被傳送到建立的解析規則進行處理。可以在**額外事件解析**視窗的**額外標準化條件**頁籤上指定條件。此頁籤不適用於基本解析規則。

可用設定：

- **使用原始事件**—如果要傳送原始事件進行額外標準化，請在**保留原始事件**下拉清單中選擇**是**。預設值為**否**。我們建議將原始事件傳遞給json和xml類型的標準化器。如果您要將原始事件傳送到第二、第三等嵌套層級進行額外標準化，請在每個嵌套層級中，在**保留原始事件**下拉清單中選擇**是**。

- **要傳入標準化器的欄位**——表示事件欄位，如果您只希望傳送在標準化器設定中設定了欄位的事件進行額外解析。

  如果此欄位為空，則完整事件將傳送到額外的標準化器進行處理。

- 篩選器集 - 用於定義標準化器接收的事件必須滿足的複雜條件。

  您可以使用**新增條件**按鈕，新增包含用於識別條件之欄位的字串（請參閱下文）。

  您可以點選**新增群組**按鈕來新增篩選器群組。群組運算子可以在**AND** 、 **OR**和**NOT**之間切換。您可以新增其他條件群組，也可以將單一條件新增至篩選器群組。

  您可以透過拖曳圖示來交換條件和條件群組；您也可以使用圖示來刪除它們。

篩選條件設定：

- **左運算元** 和**右運算元** - 用於指定運算子要處理的值。

  在左運算元 中，您必須指定傳入標準化器的事件的來源欄位。例如，如果在**基本事件解析**視窗中設定了eventType - DeviceEventClass對映，則在**額外事件解析**視窗的**額外標準化條件**頁籤中，您必須在篩選器的左運算元欄位中指定eventType。資料僅作為文字字串處理。

- 運算子：

  - **=** – 左右運算元完全相符。
  - **startsWith** – 左運算元以右運算元中指定的字元開頭。
  - **endsWith** – 左運算元以右運算元中指定的字元結尾。
  - **match** – 左運算元與右運算元中指定的規則運算式 (RE2) 相符。
  - **in** –左運算元與右運算元中指定的值之一相符。

可以透過點擊按鈕來轉換傳入的資料。**轉換**視窗打開，您可以在其中點擊**新增轉換**按鈕，建立用於在對來源資料執行任何操作之前轉換來源資料的規則。在**轉換**視窗中，您可以透過按圖示拖動新增的規則來交換它們；您也可以使用圖示來刪除它們。

可用的轉換

轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

可用轉換類型：

- **小寫** — 用於將值的所有字元變為小寫
- **大寫** — 用於將值的所有字元變為大寫
- **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
- **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。

- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。
- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

支援的事件來源

KUMA支援來自下表所列系統的事件的標準化。分發套件中包含這些系統的標準化器。

支援的事件來源

系統名稱	標準化器名稱	類型	標準化器描述
1C EventJournal	[OOTB] 1C EventJournal Normalizer	xml	專用於處理1C系統的事件日誌。事件來源為1C日誌。
1C TechJournal	[OOTB] 1C TechJournal Normalizer	regexp	專用於處理技術事件日誌。事件源為1C技術日誌。
Absolute Data and Device Security (DDS)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
AhnLab Malware Defense System (MDS)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Ahnlab UTM	[OOTB] Ahnlab UTM	regexp	專用於處理來自Ahnlab系統的事件。事件來源包括系統日誌、操作日誌、連線及 IPS 模組。
AhnLabs MDS	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Alcatel AOS-W	[OOTB] Alcatel AOS-W syslog	regexp	專用於處理透過 syslog 從 Alcatel AOS-W 6.4 接收的部分事件。
Alcatel Network Switch	[OOTB] Alcatel Network Switch syslog	Syslog	專用於處理透過 syslog 從 Alcatel 網路交換器接收的特定類型事件。
Apache Cassandra	[OOTB] Apache Cassandra file	regexp	專用於處理來自Apache Cassandra資料庫4.0版日誌的事件。
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Atlassian Confluence	[OOTB] Atlassian Jira Confluence檔案	regexp	專用於處理儲存在檔案中的Atlassian Jira和Atlassian Confluence 系統（Jira 9.12、Confluence 8.5）的事件。
Atlassian Jira	[OOTB] Atlassian Jira Confluence檔案	regexp	專用於處理儲存在檔案中的Atlassian Jira和Atlassian Confluence 系統（Jira 9.12、Confluence 8.5）的事件。
Avanpost FAM	[OOTB] Avanpost FAM syslog	regexp	專用於處理透過syslog接收的Avanpost Federated Access Manager (FAM) 1.9事件。
Avanpost IDM	[OOTB] Avanpost IDM syslog	regexp	專用於處理透過syslog接收的Avanpost IDM系統事件。
Avanpost PKI	[OOTB] Avanpost PKI syslog CEF	Syslog	專用於處理透過Syslog以CEF格式接收來自Avanpost PKI 6.0的事件。
Avaya Aura Communication Manager	[OOTB] Avaya Aura Communication Manager syslog	regexp	專用於處理透過Syslog從Avaya Aura Communication Manager 7.1接收到的部分事件。
Avigilon Access Control Manager (ACM)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Ayehu eyeShare	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Arbor Pravail	[OOTB] Arbor Pravail syslog	Syslog	專用於處理透過Syslog從Arbor Pravail系統接收到的事件。

系統名稱	標準化器名稱	類型	標準化器描述
Aruba Aruba AOS-S	[OOTB] Aruba Aruba AOS-S syslog	regexp	專用於處理透過Syslog從搭載Aruba AOS-S 16.10韌體的Aruba網路裝置接收到的某些類型的事件。標準化器支援以下類型的事件：帳戶事件、ACL事件、ARP防護事件、身分驗證事件、主控台事件、環路防護事件。
Barracuda Cloud Email Security Gateway	[OOTB] Barracuda Cloud Email Security Gateway syslog	regexp	專用於透過Syslog處理來自Barracuda Cloud Email Security Gateway的事件。
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Barracuda Web Security Gateway	[OOTB] Barracuda Web Security Gateway syslog	Syslog	專用於處理透過Syslog從Barracuda Web Security Gateway 15.0接收的部分事件。
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
BeyondTrust's BeyondInsight	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	Syslog	專用於處理透過 syslog 接收的 DDOS Mitigator 防護系統事件。
Bloombase StoreSafe	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
BMC CorreLog	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Bricata ProAccel	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Brinqa Risk Analytics	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	專用於處理來自Symantec Endpoint Protection系統的事件。
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Brocade Fabric OS	[OOTB] Brocade Fabric OS syslog	Syslog	專用於處理透過Syslog從Brocade Fabric 9.1接收到的事件。
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	專用於處理透過Syslog從Canonical LXD 5.18版系統接收到的事件。
Checkpoint	[OOTB] Checkpoint syslog	Syslog	[OOTB] Checkpoint syslog — 專用於處理透過Syslog協定從Checkpoint R81防火牆接收到的事件。
Cisco® 存取控制伺服器 (ACS)	[OOTB] Cisco ACS syslog	regexp	專用於處理透過Syslog接收到的Cisco存取控制伺服器 (ACS) 系統事件。
Cisco ASA	[OOTB] Cisco ASA 和 IOS® syslog	Syslog	專用於處理透過 syslog 接收到的 Cisco ASA 和 Cisco IOS 裝置特定事件。
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	專用於處理Cisco Email Security Appliance（WSA）代理伺服器的事件日誌（即access.log檔案）。

系統名稱	標準化器名稱	類型	標準化器描述
Cisco ESA syslog	[OOTB] Cisco ESA syslog	Syslog	專用於處理透過 syslog 從 Alcatel 網路交換器接收的特定類型事件。
Cisco Firepower Threat Defense	[OOTB] Cisco ASA 和 IOS Syslog	Syslog	專用於處理透過Syslog從以下網路裝置：Cisco ASA, Cisco IOS, Cisco Firepower Threat Defense 7.2接收到的事件。
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	專用於處理透過 syslog 接收的 Cisco Identity Services Engine (ISE) 系統事件。
Cisco IOS	[OOTB] Cisco ASA 和 IOS Syslog	Syslog	專用於處理透過 syslog 接收到的 Cisco ASA 和 Cisco IOS 裝置特定事件。
Cisco Netflow v5	[OOTB] NetFlow v5	netflow5	專用於處理來自Cisco Netflow版本5的事件。
Cisco NetFlow v9	[OOTB] NetFlow v9	netflow9	專用於處理來自Cisco Netflow版本9的事件。
Cisco Prime	[OOTB] Cisco Prime syslog	Syslog	專用於處理透過 syslog 接收的 Cisco Prime 系統 3.10 版事件。
Cisco Secure Email Gateway (SEG)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Cisco Secure Firewall Management Center	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Cisco Unified 通訊管理員	[OOTB] Cisco Unified 通訊管理員	regexp	專用於處理來自 Cisco Unified 通訊管理員 11.5.1 的事件類型。
Cisco WLC	[OOTB] Cisco WLC syslog	regexp	此標準化器專用於透過Syslog從Cisco WLC網路裝置（2500系列無線控制器、5500系列無線控制器、8500系列無線控制器、Flex7500系列無線控制器）接收到的某些類型事件。
Cisco WSA	[OOTB] Cisco WSA file, [OOTB] Cisco WSA syslog	regexp	[OOTB] Cisco WSA檔案。此標準化器專用於處理Cisco WSA代理伺服器（版本14.2和15.0）的事件日誌。此標準化器支援處理使用下列範本產生的事件：%t %e %a %w/%h %s %2r %A %H/%d %c %D %Xr %? BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%. %) %q %k %u %m [OOTB] Cisco WSA syslog.此標準化器專用於處理透過Syslog接受的Cisco WSA系統（版本15.0）的事件。
Citrix NetScaler®	[OOTB] Citrix NetScaler syslog	regexp	專用於處理從Citrix NetScaler 13.7負載平衡器和Citrix ADC NS13.0接收到的事件。
Claroty Continuous Threat Detection	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
CloudPassage Halo	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Codemaster Mirada	[OOTB] Codemaster Mirada syslog	Syslog	專用於處理透過 syslog 接收的 Codemaster Mirada 系統事件。
CollabNet Subversion Edge	[OOTB] CollabNet Subversion Edge syslog	Syslog	專用於處理透過 syslog 從 Subversion Edge（版本 6.0.2）系統接收的事件。
CommuniGate Pro	[OOTB] CommuniGate Pro	regexp	專用於處理KUMA代理透過TCP傳送的CommuniGate Pro 6.1系統事件。
Corvil Network Analytics	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Cribl Stream	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
CrowdStrike Falcon Host	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
CyberArk Privileged Threat Analytics (PTA)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。

系統名稱	標準化器名稱	類型	標準化器描述
CyberPeak Spektr	[OOTB] CyberPeak Spektr syslog	Syslog	專用於處理透過 syslog 接收的 CyberPeak Spektr 系統第 3 版事件。
Cyberprotect Cyber Backup	[OOTB] Cyberprotect Cyber Backup SQL [OOTB] Cyberprotect Cyber Backup syslog	sql、規則運算式	[OOTB] Cyberprotect Cyber Backup SQL 是專用於處理連接器從 Cyber Backup 系統（16.5 版）資料庫接收之事件的正規化器。 [OOTB] Cyberprotect Cyber Backup syslog 是專用於處理透過 Syslog 以 CEF 格式從 Cyber Backup 系統（17.2、17.3、18.5 版）接收之事件的正規化器。此套件適用於 KUMA 3.2 版或更新版本。
DeepInstinct	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Delinea Secret Server	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Dell Network Switch	[OOTB] Dell Network Switch syslog	regexp	專用於處理透過 syslog 從 Dell 網路交換器接收的特定類型事件。
Digital Guardian Endpoint Threat Detection	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
BIND DNS server	[OOTB] BIND syslog [OOTB] BIND file	Syslog regexp	[OOTB] BIND Syslog專用於處理透過Syslog接收到的BIND DNS伺服器事件。 [OOTB] BIND file專用於處理BIND DNS伺服器的事件日誌。
Docsvision	[OOTB] Docsvision syslog	Syslog	專用於處理透過 syslog 從 Docsvision 系統接收的稽核事件。
Dovecot	[OOTB] Dovecot Syslog	Syslog	專用於處理透過 syslog 接收的 Dovecot 郵件伺服器事件。事件來源為POP3/IMAP日誌。
Dragos Platform	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Dr.Web Enterprise Security Suite	[OOTB] Syslog-CEF	Syslog	專用於處理Dr.Web Enterprise Security Suite 13.0.1的CEF格式事件。
EclecticIQ Intelligence Center	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Edge Technologies AppBoard and enPortal	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Eltex ESR	[OOTB] Eltex ESR syslog	Syslog	設計用於處理透過 syslog 從 Eltex ESR 網路裝置接收的部分事件。
Eltex MES	[OOTB] Eltex MES syslog	regexp	設計用於處理透過 syslog 從 Eltex MES 網路裝置接收的事件（支援的裝置型號：MES14xx、MES24xx、MES3708P）。
ESET Protect	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Extreme Networks Summit Wireless Controller	[OOTB] Extreme Networks Summit Wireless Controller	regexp	此標準化器專用於Extreme Networks Summit無線控制器（型號：WM3700，韌體版本：5.5.5.0-018R）的某些稽核事件。
Factor-TS Dionis NX	[OOTB] Factor-TS Dionis NX syslog	regexp	專用於處理透過 syslog 從 Dionis-NX 系統（版本 2.0.3）接收的某些稽核事件。
F5™ 進階 Web 應用程式防火牆	[OOTB] F5 Advanced Web Application Firewall syslog	regexp	專用於處理透過 syslog 從 F5 Advanced Web Application Firewall 系統接收的稽核事件。
F5 BigIP Advanced Firewall Manager (AFM)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。

系統名稱	標準化器名稱	類型	標準化器描述
FFRI FFR yarai	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
FireEye CM Series	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
FireEye Malware Protection System	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Forcepoint NGFW	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Forcepoint SMC	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Fortinet FortiAnalyzer	[OOTB] Syslog-CEF	Syslog	專為處理透過 syslog 以 CEF 格式從 Fortinet FortiAnalyzer 7.0、7.2 接收的事件而設計。
Fortinet FortiADC	[OOTB] FortiADC syslog KV	regexp	專為處理透過 Syslog 以金鑰-值格式從 Fortinet FortiADC 7.1 負載平衡器接收的事件類型而設計。
Fortinet FortiGate®	[OOTB] Syslog-CEF	regexp	專用於處理透過Syslog從Fortinet FortiGate 7.0和7.2接收到的CEF格式事件。
Fortinet FortiGate	[OOTB] FortiGate syslog KV	Syslog	專用於透過Syslog處理來自FortiGate防火牆（版本7.0）的事件。事件來源為鍵值格式的FortiGate日誌。
Fortinet Fortimail	[OOTB] Fortimail	regexp	專用於處理FortiMail電子郵件防護系統事件。事件來源為Fortimail郵件系統日誌。
Fortinet FortiSOAR	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Fortinet FortiWeb	[OOTB] Syslog-CEF	Syslog	專用於處理來自 Fortinet FortiWeb 7.6.1 系統的 CEF 格式事件。
FreeBSD™	[OOTB] FreeBSD file	regexp	專用於處理儲存在檔案中的FreeBSD作業系統（版本13.1-RELEASE）的事件。 此標準化器可以處理由praudit公用程式產生的檔案。 範例： praudit -xl /var/audit/AUDITFILE >> file_name.log
FreeIPA	[OOTB] FreeIPA	json	專用於處理來自FreeIPA系統的事件。事件來源為Free IPA目錄服務日誌。
FreeRADIUS	[OOTB] FreeRADIUS syslog	Syslog	專為處理透過 syslog 接收的 FreeRADIUS 系統事件而設計。此正規化器支援來自 FreeRADIUS 3.0 版的事件。
GajShield Firewall	[OOTB] GajShield Firewall syslog	regexp	專為處理透過 syslog 從 GAJ_OS_Bulwark_Firmware_v4.35 版 GajShield 防火牆接收的部分事件而設計。
Garda Monitor	[OOTB] Garda Monitor syslog	Syslog	專為處理透過 syslog 接收的 Garda Monitor 3.4 版系統事件而設計。
Gardatech GardaDB	[OOTB] Gardatech GardaDB syslog	Syslog	專為處理透過 syslog 接收的 Gardatech Perimeter 5.3、5.4 版系統事件而設計。
Gardatech Perimeter	[OOTB] Gardatech Perimeter syslog	Syslog	專為處理透過 syslog 接收的 Gardatech Perimeter 5.3 版系統事件而設計。
Gigamon GigaVUE	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
HAProxy	[OOTB] HAProxy syslog	Syslog	專用於處理HAProxy系統的日誌。此標準化器支援HAProxy 2.8及以上版本的HTTP日誌、TCP日誌和錯誤日誌類型的事件。
HashiCorp Vault	[OOTB] HashiCorp Vault json	json	專用於處理從HashiCorp Vault 1.16系統接收到的JSON格式事件。此標準化器包在KUMA 3.0及更高版本中可用。
Huawei Eudemon	[OOTB] Huawei Eudemon	regexp	專用於處理來自華為Eudemon防火牆的事件。事件來源為華為Eudemon防火牆的日誌。
Huawei iManager 2000	[OOTB] Huawei iManager 2000 file	regexp	此標準化器支援處理Huawei iManager 2000系統的部分事件，這些事件儲存在\client\logs\rpc, \client\logs\deploy\ossDeployment檔案中。

系統名稱	標準化器名稱	類型	標準化器描述
Huawei USG	[OOTB] Huawei USG Basic	Syslog	專為處理透過 syslog 從 Huawei USG 安全閘道接收的事件而設計。
Huawei VRP	[OOTB] Huawei VRP syslog	regexp	專為處理透過 syslog 接收的部分 Huawei VRP 系統事件類型而設計。此標準化器對事件資料進行部分事件分類。此標準化器在KUMA 3.0及更高版本中可用。
IBM InfoSphere Guardium	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Ideco UTM	[OOTB] Ideco UTM Syslog	Syslog	專用於處理透過 syslog 從 Ideco UTM 接收的事件。此正規化程式支援 Ideco UTM 14.7、14.10、17.5 的事件。
Illumio Policy Compute Engine (PCE)	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Imperva Incapsula	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Imperva SecureSphere	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Indeed Access Manager	[OOTB] Indeed Access Manager syslog	Syslog	專用於處理透過 syslog 從 Indeed Access Manager 系統接收的事件。
Indeed PAM	[OOTB] Indeed PAM syslog	Syslog	專用於處理Indeed PAM（特權存取管理器）版本2.6的事件。
Indeed SSO	[OOTB] Indeed SSO xml	xml	專用於處理Indeed SSO（單一登入）系統事件。此標準化器支援KUMA 2.1.3及更高版本。
InfoWatch Person Monitor	[OOTB] InfoWatch Person Monitor SQL	sql	專用於處理來自InfoWatch Person Monitor 10.2的MS SQL資料庫的系統稽核事件。
InfoWatch Traffic Monitor	[OOTB] InfoWatch Traffic Monitor SQL	sql	專用於處理連接器從InfoWatch Traffic Monitor系統資料庫接收到的事件。
Intralinks VIA	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
IPFIX	[OOTB] IPFIX	ipfix	專用於處理IP Flow Information Export（IPFIX）格式的事件。
Juniper JUNOS™	[OOTB] Juniper - JUNOS	regexp	專用於處理從Juniper網路裝置接收到的稽核事件。
Kaspersky Anti Targeted Attack (KATA)	[OOTB] KATA	cef	專用於處理來自Kaspersky Anti Targeted Attack活動日誌的警示或事件。
Kaspersky CyberTrace	[OOTB] CyberTrace	regexp	專用於處理Kaspersky CyberTrace的事件。
Kaspersky Endpoint Detection and Response Optimum	[OOTB] KEDR telemetry	json	專用於處理由KATA標記的Kaspersky EDR遙測。事件來源為 kafka、EnrichedEventTopic。
Kaspersky Endpoint Security for Linux	[OOTB] KESL syslog cef [OOTB] KESL json	Syslog、json	[OOTB] KESL syslog cef 正規化器專用於透過 syslog 處理來自 Kaspersky Endpoint Security for Linux (KESL) 12.2 的 CEF 格式事件。 [OOTB] KESL json 正規化器專用於處理來自 Kaspersky Endpoint Security for Linux (KESL) 12.5 的 JSON 格式事件。
KICS/KATA	[OOTB] KICS4Net v2.x	cef	專用於處理KICS/KATA 2.x的事件。
KICS/KATA	[OOTB] KICS4Net v3.x	Syslog	專用於處理KICS/KATA 3.x的事件。
KICS/KATA 4.2	Kaspersky Industrial CyberSecurity for Networks 3.1	Syslog	專用於處理透過 syslog 從 KICS/KATA 4.2 系統接收的事件。
Kaspersky KISG	[OOTB] Kaspersky KISG syslog	Syslog	專用於處理透過 syslog 從 Kaspersky IoT Secure Gateway (KISG) 3.0 接收的事件。

系統名稱	標準化器名稱	類型	標準化器描述
Kaspersky NGFW	[OOTB] Kaspersky NGFW CEF	cef	專用於處理從 Kaspersky NGFW 系統 1.0、1.2 版接收的 CEF 格式事件。
Open Single Management Platform	[OOTB] KSC	cef	專用於處理來自Open Single Management Platform的CEF格式事件。
Open Single Management Platform	[OOTB] KSC from SQL	sql	專用於處理連接器從Open Single Management Platform系統資料庫接收到的事件。
Kaspersky Security for Linux Mail Server	[OOTB] KLMS Syslog CEF	Syslog	專用於處理透過 syslog 從 Kaspersky Security for Linux Mail Server 接收的 CEF 格式事件。
Kaspersky Security for MS Exchange SQL	[OOTB] Kaspersky Security for MS Exchange SQL	sql	此標準化器專用於儲存在資料庫中的Kaspersky Security for Exchange (KSE) 9.0的事件。
Kaspersky Secure Mail Gateway (KSMG)	[OOTB] KSMG Syslog CEF	Syslog	專用於透過Syslog處理來自Kaspersky Secure Mail Gateway 2.0的CEF格式事件。
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS Syslog CEF	Syslog	專用於處理透過Syslog從Kaspersky Web Traffic Security接收到的CEF格式事件。
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS (KV)	Syslog	專用於處理Kaspersky Web Traffic Security的鍵值格式事件。
Kemptechnologies LoadMaster	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Kerio Control	[OOTB] Kerio Control	Syslog	專用於處理Kerio Control防火牆的事件。
KUMA	[OOTB] KUMA forwarding	json	專用於處理從KUMA轉發的事件。
LastLine Enterprise	[OOTB] LastLine Enterprise syslog cef	Syslog	專用於處理透過 syslog 以 CEF 格式從 LastLine Enterprise 7.3、8.1、9.1 接收的事件。
Libvirt	[OOTB] Libvirt syslog	Syslog	專用於處理透過 syslog 接收的 Libvirt 8.0.0 版本事件。
Lieberman Software ERPM	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Linux	[OOTB] Linux audit and iptables Syslog v1	Syslog	專用於處理Linux作業系統事件。此標準化器不支援處理ENRICHED格式的事件。
Linux auditd	[OOTB] Linux auditd syslog for KUMA 3.2	Syslog	專用於處理透過 syslog 接收的 Linux 作業系統稽核事件（auditd 套件）。此標準化器支援已由KUMA收集器3.2或更高版本處理的事件。
Linux auditd	[OOTB] Linux auditd file for KUMA 3.2	regexp	專用於處理儲存到檔案的Linux作業系統的稽核事件（auditd套件）。此標準化器支援已由KUMA收集器3.2或更高版本處理的事件。
MariaDB	[OOTB] MariaDB Audit Plugin Syslog	Syslog	專用於處理透過 syslog 從 MariaDB 稽核外掛程式接收的事件。
McAfee Endpoint DLP	[OOTB] McAfee Endpoint DLP syslog	Syslog	專用於處理透過 syslog 從 McAfee Endpoint DLP Windows 11.10.200 接收的事件。
Microsoft 365 (Office 365)	[OOTB] Microsoft Office 365 json	json	此標準化器專用於處理Microsoft 365事件。
Microsoft Active Directory同盟服務（AD FS）	[OOTB] Microsoft Products for KUMA 3	xml	專用於處理Microsoft AD FS事件。[OOTB] Microsoft Products for KUMA 3標準化器在KUMA 3.0.1及更高版本中支援此事件來源。

系統名稱	標準化器名稱	類型	標準化器描述
Microsoft Active Directory域服務（AD DS）	[OOTB] 適用於KUMA 3的Microsoft產品	xml	專用於處理Microsoft AD DS事件。[OOTB] Microsoft Products for KUMA 3標準化器在KUMA 3.0.1及更高版本中支援此事件來源。
Microsoft Defender	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	專用於處理Microsoft Defender事件。
Microsoft DHCP	[OOTB] MS DHCP file	regexp	專用於處理Microsoft DHCP伺服器事件。事件來源為Windows DHCP伺服器日誌。
Microsoft DNS	[OOTB] DNS Windows	regexp	專用於處理Microsoft DNS伺服器事件。事件來源為Windows DNS伺服器日誌。此標準化器不支援在啟用**詳細資料**選項的情況下處理偵錯日誌事件。
Microsoft Exchange	[OOTB] Exchange CSV	csv	專用於處理Microsoft Exchange系統事件日誌。事件來源為Exchange伺服器MTA日誌。
Microsoft Hyper-V	[OOTB] Microsoft產品, [OOTB] 適用於KUMA 3的Microsoft產品, [OOTB] 透過KES WIN使用的Microsoft產品	xml	專用於處理Microsoft Windows事件。 事件來源為Microsoft Hyper-V日誌：Microsoft-Windows-Hyper-V-VMMS-Admin，Microsoft-Windows-Hyper-V-Compute-Operational，Microsoft-Windows-Hyper-V-Hypervisor-Operational，Microsoft-Windows-Hyper-V-StorageVSP-Admin，Microsoft-Windows-Hyper-V-Hypervisor-Admin，Microsoft-Windows-Hyper-V-VMMS-Operational，Microsoft-Windows-Hyper-V-Compute-Admin。
Microsoft IIS	[OOTB] IIS Log File Format	regexp	此標準化器以https://learn.microsoft.com/en-us/windows/win32/http/iis-logging中所述的格式處理事件。事件來源為Microsoft IIS日誌。
Microsoft網路政策伺服器（NPS）	[OOTB] Microsoft產品, [OOTB] 適用於KUMA 3的Microsoft產品, [OOTB] 透過KES WIN使用的Microsoft產品	xml	此標準化器用於處理Microsoft Windows作業系統事件。事件源為網路政策伺服器事件。
Microsoft SCCM	[OOTB] Microsoft SCCM file	regexp	專用於處理Microsoft SCCM 2309系統事件。此標準化器支援處理儲存在AdminService.log 檔案中的部分事件。
Microsoft SharePoint® Server	[OOTB] Microsoft SharePoint Server diagnostic log file	regexp	此標準化器支援處理診斷日誌中儲存的部分Microsoft SharePoint Server 2016事件。
Microsoft Sysmon	[OOTB] Microsoft產品, [OOTB] 適用於KUMA 3的Microsoft產品, [OOTB] 透過KES WIN使用的Microsoft產品	xml	此標準化器專用於處理Microsoft Sysmon模組事件。
Microsoft Windows 7, 8.1, 10, 11	[OOTB] Microsoft產品, [OOTB] 適用於KUMA 3的Microsoft產品, [OOTB] 透過KES WIN使用的Microsoft產品	xml	專用於處理Microsoft Windows作業系統的安全性、系統和應用程式日誌中的部分事件。[OOTB] Microsoft Products via KES WIN標準化器支援Kaspersky Endpoint Security12.6透過Syslog傳送到KUMA的有限數量的稽核事件類型。
Microsoft-Windows-PowerShell™	[OOTB] Microsoft Products, [OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	專用於處理Microsoft Windows PowerShell日誌事件。

系統名稱	標準化器名稱	類型	標準化器描述
Microsoft-Windows-PowerShell-Operational	[OOTB] Microsoft Products for KUMA 3, [OOTB] Microsoft Products via KES WIN	xml	專用於處理Windows PowerShell-Operational日誌事件。[OOTB] Microsoft Products via KES WIN標準化器支援Kaspersky Endpoint Security12.6透過Syslog傳送到KUMA的有限數量的稽核事件類型。
Microsoft → Windows → 系統日誌 → Netlogon	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	專用於處理XML格式的Microsoft → Windows → 系統日誌 → Netlogon日誌事件。
Microsoft → Windows → 工作排程器 → 操作	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	專用於處理XML格式的Microsoft → Windows → 工作排程器 → 操作日誌事件。
Microsoft → Windows → WinRM → 操作	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	專用於處理XML格式的Microsoft → Windows → WinRM → 操作日誌事件。
Microsoft SQL Server	[Deprecated] [OOTB] Microsoft SQL Server xml	xml	專用於處理MS SQL Server 2008、2012、2014和2016的事件。此標準化器支援KUMA 2.1.3及更高版本。
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft 產品, [OOTB] 適用於KUMA 3的Microsoft產品, [OOTB] 透過KES WIN使用的Microsoft產品	xml	專用於處理Microsoft Windows事件。事件來源為位於「應用程式和服務日誌 - Microsoft - Windows - TerminalServices-LocalSessionManager - Operational」下的日誌。[OOTB] Microsoft Products via KES WIN標準化器支援Kaspersky Endpoint Security12.6透過Syslog傳送到KUMA的有限數量的稽核事件類型。
Microsoft Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022	[OOTB] Microsoft 產品, [OOTB] 適用於KUMA 3的Microsoft產品, [OOTB] 透過KES WIN使用的Microsoft產品	xml	專用於處理來自Microsoft Windows Server作業系統的安全和系統日誌的部分事件。[OOTB] Microsoft Products via KES WIN標準化器支援Kaspersky Endpoint Security12.6透過Syslog傳送到KUMA的有限數量的稽核事件類型。
Microsoft Windows Server 2000	[OOTB] SNMP.Windows {XP/2003}	json	專用於處理使用SNMP協定從執行Microsoft Windows XP和Microsoft Windows 2003作業系統的工作站和伺服器接收到的事件。
Microsoft WSUS	[OOTB] Microsoft WSUS file	regexp	專為處理透過 syslog 接收的 Gardatech Perimeter 5.3、5.4 版系統事件而設計。
MikroTik	[OOTB] MikroTik syslog	regexp	專用於處理透過 syslog 從 MikroTik 裝置接收的事件。
Minerva Labs Minerva EDR	[OOTB] Minerva EDR	regexp	專用於處理來自Minerva EDR系統的事件。

系統名稱	標準化器名稱	類型	標準化器描述
MongoDb	[OOTB] MongoDb syslog	Syslog	專用於處理透過 syslog 從 MongoDB 7.0 資料庫接收的部分事件。
Multifactor Radius Server for Windows	[OOTB] Multifactor Radius Server for Windows syslog	Syslog	專用於處理透過Syslog從適用於Microsoft Windows的Multifactor Radius Server 1.0.2接收到的事件。
Aurora MySQL 5.7	[OOTB] MariaDB Audit Plugin Syslog	Syslog	專用於處理透過 syslog 從 MariaDB 稽核外掛程式接收的事件。
NetApp ONTAP (AFF, FAM)	[OOTB] NetApp syslog, [OOTB] NetApp file	regexp	[OOTB] NetApp syslog — 專用於處理透過Syslog接收到的NetApp系統（版本 — ONTAP 9.12）事件。 [OOTB] NetApp檔案 — 專用於處理儲存在檔案中的NetApp系統（版本 — ONTAP 9.12）事件。
NetApp SnapCenter	[OOTB] NetApp SnapCenter file	regexp	專用於處理NetApp SnapCenter系統（SnapCenter Server 5.0）的部分事件。此正規化器支援處理 C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\napManagerWeb.*.log 檔案中的部分事件。SnapManagerWeb.*.log檔案中支援的XML格式事件類型：SmDiscoverPluginRequest，SmDiscoverPluginResponse，SmGetDomainsResponse，SmGetHostPluginStatusRequest，SmGetHostPluginStatusResponse，SmGetHostRequest，SmGetHostResponse，SmRequest.此標準化器支援處理來自C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\audit.log檔案的部分事件。
NetIQ Identity Manager	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
NetScout Systems nGenius Performance Manager	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Netskope Cloud Access Security Broker	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Netwrix Auditor	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Nextcloud	[OOTB] Nextcloud syslog	Syslog	專用於處理透過 syslog 接收的 Nextcloud 26.0.4 版事件。此標準化器不儲存來自偵錯欄位的資訊。
Nexthink Engine	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Nginx	[OOTB] nginx 正規表示式	regexp	專用於處理Nginx網頁伺服器的日誌事件。
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
One Identity Privileged Session Management	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
OpenLDAP	[OOTB] OpenLDAP	regexp	專用於逐行處理auditlog.ldif檔案中OpenLDAP 2.5系統的某些事件。
Open VPN®	[OOTB] OpenVPN file	regexp	專用於處理OpenVPN系統事件日誌。
Oracle	[OOTB] Oracle Audit Trail	sql	專用於處理連接器直接從Oracle資料庫接收到的資料庫稽核事件。
OrionSoft Termit	[OOTB] OrionSoft Termit syslog	Syslog	專用於處理透過 Syslog 從 OrionSoft Termit 2.2、2.3、2.4 系統接收到的事件。
Orion soft zVirt	[OOTB] Orion Soft zVirt syslog	regexp	專用於處理Orion soft zVirt 3.1虛擬化系統事件。
PagerDuty	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。

系統名稱	標準化器名稱	類型	標準化器描述
Palo Alto Networks NGFW	[OOTB] PA-NGFW (Syslog-CSV)	Syslog	專用於處理透過Syslog從Palo Alto Networks防火牆接收到的CSV格式事件。
Palo Alto Networks PANOS	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Parsec ParsecNET	[OOTB] Parsec ParsecNET	sql	專用於處理連接器從Parsec ParsecNET 3系統資料庫接收到的事件。
Password	[OOTB] Password syslog	Syslog	專用於處理透過Syslog從Password 050219系統接收到的事件。
Penta Security WAPPLES	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Positive Technologies ISIM	[OOTB] PTsecurity ISIM	regexp	專用於處理來自PT Industrial Security Incident Manager系統的事件。
Positive Technologies Network Attack Discovery (NAD)	[OOTB] PT NAD json	json	專用於處理來自PT NAD的 json格式事件。此標準化器支援來自PT NAD 11.1和11.0的事件。
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	專用於處理PT Sandbox系統事件。
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF	Syslog	專用於處理來自PTsecurity（網頁應用程式防火牆）系統的事件。
Postfix	[OOTB] Postfix syslog	regexp	[OOTB] Postfix 軟體套件包含用於處理Postfix 3.6事件的資源集。它支援處理透過 TCP 接收的 syslog 事件。此軟體套件適用於KUMA 3.0及更新版本。
PostgreSQL pgAudit	[OOTB] PostgreSQL pgAudit Syslog	Syslog	專用於處理 PostgreSQL 資料庫 pgAudit 稽核外掛程式的事件，這些事件透過 syslog 接收。
PowerDNS	[OOTB] PowerDNS syslog	Syslog	專用於處理透過 syslog 接收的 PowerDNS Authoritative Server 4.5 事件。
Proftpd	[OOTB] Proftpd syslog	regexp	專用於處理透過Syslog從Proftpd 1.3.8c接收到的事件。
Proofpoint® 內部威脅管理	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Proxmox	[OOTB] Proxmox file	regexp	專用於處理儲存在檔案中的Proxmox 7.2-3系統事件。此標準化器支援處理存取和pveam日誌中的事件。
PT NAD	[OOTB] PT NAD json	json	專用於處理來自PT NAD的 json格式事件。此標準化器支援來自PT NAD 11.1和11.0的事件。
QEMU - 虛擬機監控程式日誌	[OOTB] QEMU - Hypervisor file	regexp	專用於處理儲存在檔案中的QEMU虛擬機監控程式事件。支援QEMU 6.2.0和Libvirt 8.0.0。
QEMU - 虛擬機日誌	[OOTB] QEMU - Virtual Machine file	regexp	專用於處理儲存在檔案中的QEMU hypervisor 6.2.0的虛擬機日誌事件。
Radware DefensePro AntiDDoS	[OOTB] Radware DefensePro AntiDDoS	Syslog	專用於處理透過Syslog從DDOS Mitigator防護系統接收到的事件。
Reak Soft Blitz Identity Provider	[OOTB] Reak Soft Blitz Identity Provider file	regexp	專用於處理儲存在檔案中的Reak Soft Blitz Identity Provider 5.16系統事件。
RedCheck桌面版	[OOTB] RedCheck Desktop file	regexp	專用於處理儲存在檔案中的RedCheck Desktop 2.6系統日誌。
RedCheck WEB	[OOTB] RedCheck WEB file	regexp	專用於處理儲存在文件中的RedCheck Web 2.6系統日誌。

系統名稱	標準化器名稱	類型	標準化器描述
RED SOFT RED ADM	[OOTB] RED SOFT RED ADM syslog	regexp	專用於處理透過Syslog從RED ADM系統（RED ADM：工業版1.1）接收到的事件。 此標準化器支援處理： - 管理子系統事件 - 控制器事件
ReversingLabs N1000 Appliance	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Rubicon Communications pfSense	[OOTB] pfSense Syslog	Syslog	專用於處理透過Syslog從pfSense防火牆接收到的事件。
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	專用於處理來自pfSense防火牆的事件。這些事件的Syslog標頭不包含主機名稱。
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
SecurityCode Continent 4	[OOTB] SecurityCode Continent 4 syslog	regexp	專用於處理透過 syslog 接收的 SecurityCode Continent 系統版本 4 事件。
Sendmail	[OOTB] Sendmail syslog	Syslog	專用於處理透過 syslog 接收的 Sendmail 版本 8.15.2 事件。
SentinelOne	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Skype™ for Business	[OOTB] Microsoft Products for KUMA 3	xml	專用於處理來自Skype for Business系統日誌、Lync Server日誌的部分事件。
Snort	[OOTB] Snort 3 json file	json	專用於處理Snort 3的JSON格式事件。
Sophos Central	[OOTB] Sophos Central syslog	Syslog	專用於處理由 Sophos-Central-SIEM-Integration 指令碼透過 syslog，以 CEF 格式從 Sophos Central 1.2 接收的部分事件。
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall	Syslog	專用於處理透過Syslog從SonicWall TZ防火牆接收到的事件。
Solar WebProxy	[OOTB] Solar WebProxy syslog	regexp	專用於處理透過Syslog從Solar WebProxy 4.2接收到的siem-log格式事件。
SolarWinds DameWare® MRC	[OOTB] SolarWinds DameWare MRC xml	xml	此標準化器支援處理儲存在Windows應用程式日誌中的部分DameWare Mini Remote Control (MRC) 7.5事件。此標準化器處理由dwmrcs提供者產生的事件。
Sophos Firewall	[OOTB] Sophos Firewall syslog	regexp	專為處理透過 syslog 從 Sophos Firewall 20 接收的事件而設計。
Sophos XG	[OOTB] Sophos XG	regexp	專用於處理來自Sophos XG防火牆的事件。
Squid	[OOTB] Squid access Syslog	Syslog	專為處理透過 syslog 協定接收的 Squid 代理伺服器事件而設計。
Squid	[OOTB] Squid access.log file	regexp	專用於處理來自Squid代理伺服器的Squid日誌事件。事件來源為access.log日誌
Staffcop Enterprise	[OOTB] Staffcop Enterprise syslog CEF	regexp	專用於處理透過 syslog 從 Staffcop Enterprise 5.4、5.5 接收的 CEF 格式事件。
S-Terra VPN Gate	[OOTB] S-Terra	Syslog	專用於處理來自S-Terra VPN Gate裝置的事件。
Stormshield 防火牆	[OOTB] Stormshield 防火牆 syslog	Syslog	專用於透過 Syslog 處理來自 Stormshield 防火牆 4.8 和 5.0 的金鑰-值格式事件。
Suricata	[OOTB] Suricata json file	json	此軟體套件包含儲存在JSON檔案中的Suricata 7.0.1事件的標準化器。 此標準化器支援處理以下事件類型：flow、anomaly、alert、dns、http、ssl、tls、ftp、ftp_data、ftp、smb、rdp、pgsql、modbus、quic、dhcp、bittorrent_dht、rfb。

系統名稱	標準化器名稱	類型	標準化器描述
ThreatConnect Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
ThreatQuotient	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Tionix Cloud Platform	[OOTB] Tionix Cloud Platform syslog	Syslog	專用於處理透過 syslog 接收的 Tionix Cloud Platform 系統 2.9 版事件。此標準化器對事件資料進行部分事件分類。此標準化器在KUMA 3.0及更高版本中可用。
Tionix VDI	[OOTB] Tionix VDI file	regexp	此標準化器支援處理儲存在tionix_Intmov.log檔案中的部分Tionix VDI 2.8系統事件。
TrapX DeceptionGrid	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
趨勢科技™ Control Manager	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Trend Micro Deep Security	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Trend Micro NGFW	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Unbound	[OOTB] Unbound Syslog	Syslog	專用於處理透過 syslog 接收的 Unbound DNS 伺服器事件。
UserGate	[OOTB] Syslog-CEF	Syslog	專用於處理透過 syslog 從 UserGate 系統接收的 CEF 格式事件。
Varonis DatAdvantage	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Veriato 360	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
ViPNet TIAS	[OOTB] ViPNet TIAS syslog	Syslog	專用於處理透過Syslog接收到的ViPNet TIAS 3.8事件。
VMware ESXi	[OOTB] VMware ESXi syslog	regexp	專用於處理透過syslog接收到的VMware ESXi事件（支援ESXi 5.5、6.0、6.5、7.0版本的有限事件集）。
VMWare Horizon	[OOTB] VMware Horizon - Syslog	Syslog	專用於處理透過syslog從VMware Horizon 2106系統接收到的事件。
VMwareCarbon Black EDR	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Vmware vCenter	[OOTB] VMware vCenter API	xml	專用於處理透過API接收到的VMware vCenter 7事件。
Vormetric Data Security Manager	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Votiro Disarmer for Windows	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Vsftpd	[OOTB] Vsftpd syslog	regexp	專用於處理透過Syslog從Vsftpd 3.0.5接收到的事件。
Wallix AdminBastion	[OOTB] Wallix AdminBastion syslog	regexp	專用於處理透過syslog從Wallix AdminBastion系統接收到的事件。
WatchGuard - Firebox	[OOTB] WatchGuard Firebox	Syslog	專用於處理透過Syslog接收到的WatchGuard Firebox事件。
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。

系統名稱	標準化器名稱	類型	標準化器描述
Winchill Fracas	[OOTB] PTC Winchill Fracas	regexp	專用於處理Windchill FRACAS故障註冊系統事件。
Yandex Browser企業版	[OOTB] Yandex Browser	json	專用於處理從Yandex Browser 23或24.4企業版接收到的事件。
Yandex Cloud	[OOTB] Yandex Cloud	regexp	專用於處理部分 Yandex Cloud 稽核事件。此正規化器支援處理組態層級的稽核記錄事件：IAM（Yandex Identity and Access Management）、Compute（Yandex Compute Cloud）、Network（Yandex Virtual Private Cloud）、Storage（Yandex Object Storage）、Resourcemanager（Yandex Resource Manager）。
Zabbix	[OOTB] Zabbix SQL	sql	專用於處理Zabbix 6.4事件。
Zecurion DLP	[OOTB] Zecurion DLP syslog	regexp	專用於處理透過Syslog接收到的Zecurion DLP 12.0系統事件。
ZEEK IDS	[OOTB] ZEEK IDS json file	json	專用於處理ZEEK IDS系統的JSON格式日誌。此標準化器支援ZEEK IDS 1.8的事件。
Zettaset BDEncrypt	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
Zscaler Nanolog多媒體串流服務（NSS）	[OOTB] Syslog-CEF	Syslog	專用於處理CEF格式的事件。
IT-Bastion – SKDPU	[OOTB] Syslog-CEF	Syslog	專用於處理透過Syslog從IT-Bastion SKDPU系統接收到的CEF格式事件。
A-Real Internet Control Server (ICS)	[OOTB] A-real IKS syslog	regexp	專用於處理透過 syslog 接收的 A-Real Internet Control Server (ICS) 系統事件。此標準化器支援來自A-Real ICS 7.0及更高版本的事件。
Biznes Resheniya Compass	[OOTB] Biznes Resheniya Compass	regexp	專用於處理透過 Kafka 接收的 Biznes Resheniya Compass 6.7.7 和 6.7.8 稽核事件類型。
Apache網頁伺服器	[OOTB] Apache HTTP Server file	regexp	專用於處理儲存在檔案中的Apache HTTP Server 2.4事件。此標準化器支援處理來自通用或組合日誌格式的應用程式日誌以及錯誤日誌的事件。 錯誤日誌事件的預期格式： `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Apache web server	[OOTB] Apache HTTP Server syslog	Syslog	專用於處理透過 syslog 接收的 Apache HTTP Server 事件。此標準化器支援處理來自通用或組合日誌格式的存取日誌以及錯誤日誌的Apache HTTP Server 2.4事件。 錯誤日誌事件的預期格式： `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Lighttpd web server	[OOTB] Lighttpd syslog	Syslog	專用於處理透過 syslog 接收的 Lighttpd 系統存取事件。此標準化器支援處理Lighttpd 1.4事件。 存取日誌事件的預期格式： `$remote_addr $http_request_host_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"`
IVK Kolchuga-K	[OOTB] Kolchuga-K Syslog	Syslog	專用於處理透過 syslog 接收的 IVK Kolchuga-K 系統（版本 LKNV.466217.002）事件。
InfoTeCS ViPNet IDS	[OOTB] Syslog-CEF	Syslog	專用於處理透過 syslog 從 infotecs ViPNet IDS 系統接收的 CEF 格式事件。
InfoTeCS ViPNet Coordinator	[OOTB] VipNet Coordinator Syslog	Syslog	專用於處理透過 syslog 接收的 ViPNet Coordinator 系統事件。
Kod Bezopasnosti—Continent	[OOTB][regexp] Continent IPS/IDS & TLS	regexp	專用於處理來自Continent IPS/IDS裝置日誌的事件。
Kod Bezopasnosti—Continent	[OOTB] Continent SQL	sql	專用於從資料庫獲取Continent系統事件。
Kod Bezopasnosti SecretNet 7	[OOTB] SecretNet SQL	sql	專用於處理連接器從SecretNet系統資料庫接收到的事件。

系統名稱	標準化器名稱	類型	標準化器描述
Confident – Dallas Lock Unified Control Center	[OOTB] Confident Dallas Lock syslog CEF	regexp	專用於處理從Dallas Lock Unified Control Center 4.0接收到的CEF格式事件。
CryptoPro NGate	[OOTB] Ngate Syslog	Syslog	專用於處理透過Syslog從CryptoPro NGate系統接收到的事件。
H3C (Huawei-3Com) routers	[OOTB] H3C Routers syslog	regexp	此標準化器專用於透過Syslog從H3C（Huawei-3Com）SR6600網路裝置（Comware 7韌體）接收到的某些類型事件。此標準化器支援標準事件格式（符合RFC 3164格式）。
NT Monitoring and Analytics	[OOTB] Syslog-CEF	Syslog	專用於處理透過syslog從NT Monitoring and Analytics系統接收到的CEF格式事件。
BlueCoat代理伺服器	[OOTB] BlueCoat Proxy v0.2	regexp	專用於處理BlueCoat代理伺服器事件。事件來源為BlueCoat代理伺服器事件日誌。
SKDPU NT Access Gateway	[OOTB] Bastion SKDPU-GW	Syslog	專用於處理透過Syslog接收到的SKDPU NT Access Gateway系統事件。
Solar Dozor	[OOTB] Solar Dozor Syslog	Syslog	專用於處理透過 Syslog 從 Solar Dozor 7.9 版系統接收的事件。此標準化器支援自訂格式事件，不支援CEF格式事件。
-	[OOTB] Syslog header	Syslog	專用於處理透過Syslog接收到的事件。此標準化器解析Syslog事件的標頭，但不會解析事件的訊息欄位。如有必要，您可以使用其他標準化器來解析訊息欄位。

連接器

連接器用於在KUMA服務之間建立連接並主動和被動接收事件。

此程式具有以下可用的連接器類型：

- tcp—用於透過TCP被動接收資料。適用於Windows和 Linux代理程式。
- udp—用於透過UDP被動接收資料。適用於Windows和Linux代理程式。
- netflow—用於被動接收NetFlow格式的事件。
- sflow—用於被動接收SFlow格式的事件。
- nats-jetstream—用於與NATS訊息代理程式通訊。適用於Windows和Linux代理程式。
- kafka—用於與Apache Kafka資料匯流排通訊。適用於Windows和Linux代理程式。
- http—用於透過HTTP接收事件。適用於Windows和Linux代理程式。
- sql—用於從資料庫中選擇資料。
  此程式支援以下類型的SQL資料庫：
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach

- Oracle
- Firebird
- ClickHouse

- 檔案—用於從文字檔案檢索資料。適用於Linux代理程式。
- 1c-log和1c-xml用於從1C日誌接收資料。適用於Linux代理程式。
- 二極體 - 用於在工業ICS網路中使用資料二極體進行單向資料傳輸。
- ftp - 用於透過檔案傳輸協定接收資料。適用於Windows和 Linux代理程式。
- sftp - 用於透過安全檔案傳輸協定接收資料。適用於Windows和 Linux代理程式。
- nfs - 用於透過網路檔案系統協定接收資料。適用於Windows和 Linux代理程式。
- wmi - 用於使用Windows管理規範取得資料。適用於Windows代理程式。
- wec—用於透過Windows事件轉送 (WEF) 和Windows事件收集器 (WEC) 接收資料，或Windows主機的本機作業系統日誌。適用於Windows代理程式。
- snmp—用於使用簡易網路管理通訊協定接收資料。適用於Windows和 Linux代理程式。
- snmp-trap—用於使用簡易網路管理通訊協定陷阱 (SNMP陷阱) 接收資料。適用於Windows和 Linux代理程式。
- kata/edr—用於透過API接收KEDR資料。
- vmware—用於透過API接收VMware vCenter資料。
- elastic—用於接收Elasticsearch資料。
- etw—用於接收擴充DNS伺服器日誌。
- universalAPI— 用於接收來自任何支援JSON回應的REST API的資料。支援按唯一ID和迭代模式進行篩選。
- smb—用於透過SMB（Server Message Block）通訊協定接收資料。適用於Linux代理程式。
- http-streaming—用於透過HTTP接收串流事件。連接器會分段處理要求本文，從而減少記憶體使用量。適用於Windows和 Linux代理程式。

檢視連接器設定

若要檢視連接器設定：

1. 在主功能表中，轉至**監控 → 資源 → 連接器**。
2. 在資料夾結構中，選擇包含相關連接器的資料夾。
3. 選擇要檢視其設定的連接器。

連接器的設定顯示在兩個頁籤上：**基本設定**和**進階設定**。有關每個連接器設定的詳細說明，請參閱*連接器設定*部分。

新增連接器

您可以為除描述欄位之外的所有輸入欄位啟用**非列印字元的顯示**。

若要新增連接器：

1. 在主功能表中，轉至**監控 → 資源 → 連接器**。
2. 在資料夾結構中，選擇要放置連接器的資料夾。

   根資料夾對應於租用戶。若要使連接器可供特定租用戶使用，必須在該租用戶的資料夾中建立資源。

   如果資料夾樹中沒有所需的資料夾，則需要建立它。
   預設情況下，新增的連接器會在**共用**資料夾中建立。
3. 點擊**新增連接器**按鈕。
4. 定義所選連接器類型的設定。
   *連接器設定*部分提供了必須為每種連接器類型指定的設定。
5. 按一下**儲存**按鈕。

連接器設定

本章節介紹KUMA支援的所有連接器類型的設定。

Tcp類型

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）- 擁有該資源的租用戶名稱。
- **類型**（必填）— 連接器類型， **tcp**。
- **URL**（必填）—您需要連線的 URL。可用格式：主機名稱:連接埠、IPv4:連接埠、IPv6:連接埠、:連接埠。
- **Auditd**是將從連接器收到的auditd日誌事件記錄分組為單一事件的機制的切換開關。Auditd 僅支援 \n 分隔符號。若啟用切換開關，**分隔符號**欄位將無法使用。如果在代理連接器中啟用了**Auditd**切換開關，則必須在代理程式向其傳送事件的收集器的連接器中設定\n分隔符號。

- **分隔符號**用於指定代表事件之間分隔符號的字元。可用值：`\n`、`\t`、`\0`。若未指定分隔符號（選取的值為空），則預設值為 `\n`。

- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **緩衝區大小**用於設定連接器的緩衝區大小。預設值為1MB，最大值為64MB。

- **字元編碼** 設定指定字元編碼。預設值是UTF-8。

- **事件緩衝TTL**是緩衝區的生存時間，用於將記錄分組為單一auditd事件。只有啟用了**Auditd**切換開關，此欄位才可用。倒數計時從收到第一個事件行時開始，或在上一個TTL過期後立即開始。可能的值：50毫秒到3000毫秒。預設值是2000毫秒。

- **傳輸標頭**— 對於auditd事件，您必須指定一個規則運算式來辨識auditd日誌的各個部分。您可以使用預設值或加以編輯。規則運算式必須包含record_type_name、record_type_value和event_sequence_number群組。如果多行auditd事件包含前綴，則第一個記錄將保留該前綴，而後續條目將丟棄該前綴。

  您可以透過點擊**重設為預設值**來恢復到原始值。

- **TLS模式** — 使用PEM x509格式憑證的TLS加密模式：

  - **停用**（預設）—不使用TLS加密。

  - **啟用**— 使用加密但不進行憑證驗證。

  - **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA 的根憑證和金鑰會在程式安裝期間自動建立，並儲存在 KUMA Core 伺服器的 /opt/kaspersky/kuma/core/certificates/ 資料夾中。

  - **自訂PFX** — 使用加密。選擇此選項後，必須在外部憑證授權單位中使用PKCS#12容器格式的私鑰產生憑證。然後，必須將憑證從金鑰庫匯出，並將其作為PFX密鑰上傳到KUMA主控台。**新增PFX密鑰**。

    若要建立PFX密鑰：

    1. 在**名稱**欄位中，輸入PFX密鑰的名稱。
    2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。
    3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。
    4. 按一下**建立**按鈕。

    PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。

  使用TLS時，無法將IP位址指定為URL。

- **壓縮**- 您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。

- **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

udp類型

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）- 擁有該資源的租用戶名稱。
- **類型**（必填）— 連接器類型，**udp**。
- **URL**（必填）—您需要連線的 URL。可用格式：主機名稱:連接埠、IPv4:連接埠、IPv6:連接埠、:連接埠。
- **Auditd**是將從連接器收到的auditd日誌事件記錄分組為單一事件的機制的切換開關。Auditd 僅支援 \n 分隔符號。若啟用切換開關，**分隔符號**欄位將無法使用。如果在代理連接器中啟用了**Auditd**切換開關，則必須在代理程式向其傳送事件的收集器的連接器中設定\n分隔符號。
- **分隔符號**用於指定代表事件之間分隔符號的字元。可用值：`\n`、`\t`、`\0`。若未指定分隔符號（選取的值為空），則不分隔事件。
- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **緩衝區大小**用於設定連接器的緩衝區大小。預設值為16KB，最大值為64KB。
- **處理程式數量**是服務可以同時執行以並行處理回應規則的處理程序數。您可以使用下列公式確定處理程序的數量：(<CPU核心數>/2) + 2。
- **字元編碼** 設定可指定字元編碼。預設值是`UTF-8`。
- **事件緩衝TTL**是緩衝區的生存時間，用於將記錄分組為單一auditd事件。只有啟用了**Auditd**切換開關，此欄位才可用。倒數計時從收到第一個事件行時開始，或在上一個TTL過期後立即開始。可能的值：50毫秒到3000毫秒。預設值是2000毫秒。
- **傳輸標頭**— 對於auditd事件，您必須指定一個規則運算式來辨識auditd日誌的各個部分。您可以使用預設值或加以編輯。規則運算式必須包含record_type_name、record_type_value和event_sequence_number群組。如果多行auditd事件包含前綴，則第一個記錄將保留該前綴，而後續條目將丟棄該前綴。

  您可以透過點擊**重設為預設值**來恢復到原始值。
- **壓縮**- 您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。
- **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

Netflow類型

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型， **netflow** 。

- **URL**（必填）—您需要連線的 URL。
- **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **緩衝區大小**用於設定連接器的緩衝區大小。預設值為16KB，最大值為64KB。
  - **工作線程**— 用於設定連接器的工作線程數量。預設值是1。
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

Sflow類型

可針對以 sFlow 格式接收的事件使用其他正規化。

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填） - 擁有該資源的租用戶名稱。
- **類型**（必需）—連接器類型， **sflow**。
- **URL**（必填）—您需要連線的 URL。可用格式：主機名稱:連接埠、IPv4:連接埠、IPv6:連接埠、:連接埠。
- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **緩衝區大小**用於設定連接器的緩衝區大小。預設值為1MB，最大值為64MB。
- **工作線程**— 用於設定連接器的工作線程數量。預設值是1。
- **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
- **偵錯**— 可讓您啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

Nats-jetstream 類型

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填） - 擁有該資源的租用戶名稱。

- **類型**（必填）— 連接器類型，**nats-jetstream**。
- **URL**（必填）—您需要連線的 URL。
- **主題**（必填）— NATS訊息的主題。必須包含Unicode字元。
- **分隔符號**用於指定代表事件之間分隔符號的字元。可用值：`\n`、`\t`、`\0`。若未指定分隔符號（選取的值為空），則不分隔事件。
- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **緩衝區大小**用於設定連接器的緩衝區大小。預設值為16KB，最大值為64KB。
- **群組 ID** — NATS 訊息的 GroupID 參數。必須包含1至255個Unicode字元。預設值是`default`。
- **工作線程**— 用於設定連接器的工作線程數量。預設值是1。
- **字元編碼** 設定可指定字元編碼。預設值是`UTF-8`。
- **叢集 ID**是NATS叢集的ID。
- **TLS模式**指定是否使用TLS加密：
  - **停用**（預設）—不使用TLS加密。
  - **啟用**— 使用加密但不進行憑證驗證。
  - **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA 的根憑證和金鑰會在程式安裝期間自動建立，並儲存在 KUMA Core 伺服器的 /opt/kaspersky/kuma/core/certificates/ 資料夾中。
  - **自訂CA** — 使用加密並驗證憑證是否由憑證授權單位簽署。包含憑證的密鑰可從**自訂CA**下拉清單中選擇，選擇此選項後會顯示該清單。

    建立由憑證授權單位簽署的憑證。

    您可以在KUMA Core伺服器上建立CA簽署的憑證（以下命令範例使用OpenSSL）。

    若要建立由憑證授權單位簽署的憑證：

    1. 產生憑證授權單位要使用的金鑰，例如：

       ```
       openssl genrsa -out ca.key 2048
       ```

    2. 為產生的金鑰建立憑證，例如：

       ```
       openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<憑證授權單位的通用主機名稱>" -out ca.crt
       ```

    3. 建立私鑰並要求憑證授權單位對其進行簽署，例如：

       ```
       openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<KUMA 伺服器的通用主機名稱>" -out server.csr
       ```

4. 建立由憑證授權單位簽署的憑證。您需在 `subjectAltName` 變數中包含為其建立憑證之伺服器的網域名稱或 IP 位址，例如：

   ```
   openssl x509 -req -extfile <(printf
   "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in
   server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. 在 Open Single Management Platform 網頁介面中，將建立的 `server.crt` 憑證上傳至 **憑證** 類型的機密項目，然後在 **自訂 CA** 下拉式清單中選取該 **憑證** 類型的機密項目。

使用TLS時，無法將IP位址指定為URL。

若要在協力廠商裝置上使用KUMA憑證，您必須將憑證檔案副檔名從CERT變更為CRT。否則，可能會傳回錯誤x509：憑證由未知單位簽署。

- **壓縮**- 您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。
- **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

連接器，Kafka類型

kafka類型的連接器用於在使用Windows和Linux代理程式時與Apache Kafka資料匯流排進行通訊。下表描述了**kafka**類型連接器的設定。

使用**kafka**類型的連接器，KUMA可以接收未壓縮和壓縮形式的事件。壓縮使用**kafka**支援的以下壓縮演算法進行：gzip、snappy、zstd或lz4。以壓縮形式到達的事件會自動解壓縮。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
類型	連接器類型：**kafka**。 必需設定。
標記	資源搜尋標籤。 可選設定。
URL	URL（必填）—您需要連線的 URL。現支援以下URL格式： • `< 主機名稱 >:< 連接埠號碼 >` • `< IPv4 位址 >:< 連接埠號碼 >` • `< IPv6 位址 >:< 連接埠號碼 >` 您可以使用以下格式指定 IPv6 位址：`[< IPv6 位址 >%< 介面 >:< 連接埠號碼 >`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以新增多個 URL，也可以移除 URL。如果URL欄位包含製表符或空格，KUMA不允許儲存資源或服務。若要新增URL，請按一下**+ 新增**按鈕。若要刪除URL，請按一下其旁邊的刪除✕圖示。 必需設定。

設定	描述
授權	連接到**URL**欄位中指定的URL時所授權類型： • **已停用**。預設選擇該值。 • **Plain**。這種類型的授權使用SASL/PLAIN機制執行，該機制以純文字形式傳輸使用者名稱和密碼。通常情況下，TLS用於在SASL/PLAIN中提供傳輸安全性（加密）。 如果選擇此選項，請在**密鑰**下拉清單中指定包含使用者帳戶憑據的密鑰，以便在連線到目標時進行授權。您可以選擇現有密鑰或建立新密鑰。若要建立新密鑰，請選擇**新建**。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立密鑰？** *若要建立密鑰：* 1. 在**名稱**欄位中，輸入密鑰的名稱。 2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。 3. 如有必要，在**描述**欄位中輸入密鑰的描述。 4. 點擊**建立**按鈕。 密鑰將會新增並顯示在**密鑰**下拉清單中。 • **PFX**指的是使用PFX密鑰進行TLS加密。您必須在外部憑證授權機構中使用PKCS#12容器格式的私鑰生成憑證，從金鑰庫匯出PFX檔案，並將PFX檔案作為PFX密鑰上傳到KUMA網頁介面。如果選擇此值，請在**PFX 密鑰**下拉清單中指定一個由憑證授權單位簽署的PFX憑證。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇**新建**。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立PFX密鑰？** *若要建立PFX密鑰：* 1. 在**名稱**欄位中，輸入PFX密鑰的名稱。 2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。 3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。 4. 按一下**建立**按鈕。 PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。 如果您使用多個憑證鏈來驗證伺服器，我們建議使用OpenSSL建立PFX檔案，以確保憑證鏈中憑證的順序正確。 • **SCRAM-SHA-256**使用安全連線機制進行授權，該機制使用SHA256雜湊值進行安全身份驗證並防止資料被攔截。 • **SCRAM-SHA-512**使用安全連線機制進行授權，該機制使用SHA512雜湊值進行安全身份驗證並防止資料被攔截。 當在**密鑰**下拉清單中選擇**SCRAM-SHA-256**或**SCRAM-SHA-512**作為授權類型時，請指定一個包含密碼的密鑰進行授權。您可以選擇現有密鑰或建立新密鑰。若要建立新的密鑰，請在**密鑰**下拉清單中，選擇**新建**。
主題	Kafka訊息的主題。訊息的最大長度為255個字元。不允許使用空格和製表符。您可以使用以下字元：a–z、A–Z、0–9、“.”、“_”、“-”。 必需設定。
GroupID	Kafka訊息的`GroupID`參數值。該值的最大長度為255個字元。您可以使用以下字元：a–z、A–Z、0–9、“.”、“_”和“-”。
分隔符號	標記事件之間邊界的字元： • **\n** • **\t** • **\0** 如果您未在此下拉清單中選擇值，則預設選擇空值。在這種情況下，連接器不會將一個事件拆分成多個事件，而是原封不動地將其傳遞給規範化器。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。
服務處理數量。	服務可以同時執行以並行處理回應規則的事件處理器數量。 該值必須為不超過999的正整數。 預設情況下，處理程式的數量是256。
字元編碼	字符編碼。預設值是**UTF-8**。

設定	描述

TLS模式	TLS加密模式。使用TLS加密時，您無法在基本設定**基本設定URL**欄位中指定IP位址。可用值：
	• **停用**表示不使用TLS加密。預設選擇該值。
	• **啟用**表示使用加密，但憑證未經驗證。
	• **自訂CA**表示使用加密並驗證憑證是否由憑證授權單位簽署。如果選擇此值，請在**自訂CA**下拉清單中，指定由憑證授權單位簽署的憑證所對應的密鑰。您可以選擇現有密鑰或建立新密鑰。若要建立新密鑰，請選擇**新建**。
	若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。
	如何建立由憑證授權單位簽署的憑證？
	您可以在KUMA Core伺服器上建立CA簽署的憑證（以下命令範例使用OpenSSL）。
	若要建立由憑證授權單位簽署的憑證：
	1. 產生憑證授權單位要使用的金鑰，例如：
	`openssl genrsa -out ca.key 2048`
	2. 為產生的金鑰建立憑證，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 憑證授權單位的通用主機名稱 >" -out ca.crt`
	3. 建立私鑰並要求憑證授權單位對其進行簽署，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 伺服器的通用主機名稱 >" -out server.csr`
	4. 建立由憑證授權單位簽署的憑證。您需在 `subjectAltName` 變數中包含為其建立憑證之伺服器的網域名稱或 IP 位址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform 網頁介面中，將建立的 `server.crt` 憑證上傳至 **憑證** 類型的機密項目，然後在 **自訂 CA** 下拉式清單中選取該 **憑證** 類型的機密項目。
	若要在協力廠商裝置上使用KUMA憑證，您必須將憑證檔案副檔名從CERT變更為CRT。否則，您可能會收到 `x509: certificate signed by unknown authority` 錯誤。

要擷取的訊息大小	請求中一則訊息的大小（以位元組為單位）。如果未指定值或指定為0，則套用預設值16MB。它不能超過2,147,483,647個位元組。
最大擷取等待時間	一則訊息的逾時時間（以秒為單位）。如果沒有指定值或指定為0，則套用預設值5秒。最大可能值為：2,147,483,647。
連線逾時時間	Kafka broker連線逾時時間（以秒為單位）。 最大可能值為：2,147,483,647。預設值是 30 秒。
讀取逾時時間	讀取操作逾時時間（以秒為單位）。 最大可能值為：2,147,483,647。預設值是 30 秒。
寫入逾時時間	寫入操作逾時時間（以秒為單位）。 最大可能值為：2,147,483,647。預設值是 30 秒。
群組活動訊號間隔	群組狀態更新間隔（以秒為單位）。 更新間隔不能超過會話時間。建議值為會話時間的1/3。最大可能值為：2,147,483,647。預設值是 3 秒。
工作階段逾時時間	會話時間（以秒為單位）。 最大可能值為：2,147,483,647。預設值是 10 秒。
最大處理時間	單一執行緒處理一則訊息的最大持續時間（以毫秒為單位）。 最大可能值為：2,147,483,647。預設值為100毫秒。
已啟用自動提交	預設啟用。

設定	描述
自動提交間隔	自動提交間隔（以秒為單位）。預設值為1秒。 最大可能值為：18,446,744,073,709,551,615。可以指定任何正數。

kata/edr類型

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填） - 擁有該資源的租用戶名稱。
- **類型**（必填）— 連接器類型，**kata/edr**。
- **URL**（必填）— 可從KATA/EDR伺服器接收遙測資料的URL。URL必須包含主機和連接埠；預設連接埠為443。如果KATA/EDR部署在叢集中，您可以指定多個URL以確保連線的高可用性。
- **密鑰**（必填）是一個下拉清單，您可以在其中選擇儲存用於連線到KATA/EDR伺服器的憑據的密鑰。您可以從下拉清單中選擇密鑰資源，或透過點選加號圖示 (+) 建立一個密鑰資源。建立密鑰時，可以指定自訂憑證和私鑰，也可以自動產生新的自簽署憑證和私鑰。可以透過點擊鉛筆圖示（ ）來變更所選密鑰。
- **外部ID** — 外部系統的ID。KUMA會自動在此欄位中產生ID。
- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **調試**— 一個切換開關，用於指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。
- **字元編碼**— 用於轉換為UTF-8的來源字元編碼設定。我們僅建議在標準化事件的欄位中發現無效字元時設定轉換。預設值：未選擇。
- **事件的數量**— 一個請求中的最大事件數。預設情況下，使用KATA/EDR伺服器上設定的值。
- **事件擷取逾時時間**是等待從KATA/EDR伺服器接收事件的時間（以秒為單位）。預設值為 0，這表示使用KATA/EDR伺服器上指定的值。
- **用戶端逾時時間**是等待KATA/EDR伺服器回應的時間（以秒為單位）。預設值：1,800秒；顯示為0。
- **KEDRQL 篩選器**— 對KATA/EDR伺服器的請求的篩選器。有關查詢語言的更多詳細資訊，請參閱KEDR說明。

連接器，http類型

http類型的連接器用於在使用Windows和Linux代理程式時透過HTTP接收事件。下表描述了**http**類型連接器的設定。

使用**http**類型的連接器，KUMA可以接收未壓縮和壓縮形式的事件。以壓縮形式到達的事件，例如 Kaspersky Endpoint Security for Windows 事件，會自動解壓縮。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
類型	連接器類型：**http**。 必需設定。
標記	資源搜尋標籤。 可選設定。
URL	URL（必需）—您需要連線的 URL。您可以按以下格式之一輸入URL： • `< 主機名稱 >:< 連接埠號碼 >` • `< IPv4 位址 >:< 連接埠號碼 >` • `< IPv6 位址 >:< 連接埠號碼 >` • `:< 連接埠號碼 >` 若要將事件來源中的資料傳送到連接器，指定的URL必須以 `/input` 結尾。 必需設定。
分隔符號	標記事件之間邊界的字元： • **\n** • **\t** • **\0** 如果您未在此下拉清單中選擇值，則預設選擇空值。在這種情況下，連接器不會將一個事件拆分成多個事件，而是原封不動地將其傳遞給規範化器。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。
字元編碼	字符編碼。預設值是**UTF-8**。

設定	描述
TLS模式	TLS加密模式。使用TLS加密時，您無法在**基本設定**的基本設定欄位中指定IP位址。可用值： • **停用**表示不使用TLS加密。預設選擇該值。 • **啟用**表示使用加密，但憑證未經驗證。 • **使用驗證**表示使用加密並驗證憑證是否使用KUMA根憑證簽署。KUMA的根憑證和金鑰在程式安裝期間自動建立，並儲存在KUMA Core伺服器的目錄/opt/kaspersky/kuma/core/certificates/中。 過時的加密模式，已棄用。將在KUMA的未來版本中移除。 • **自訂 PFX**是指使用PFX密鑰進行TLS加密。您必須使用PKCS#12容器格式的私鑰生成PFX憑證，然後將PFX憑證作為PFX密鑰上傳到KUMA網頁介面。如果選擇此值，請在「PFX密鑰」下拉清單中指定一個由憑證授權單位簽署的PFX憑證。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇「新建」。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立PFX密鑰？** *若要建立PFX密鑰：* 1. 在**名稱**欄位中，輸入PFX密鑰的名稱。 2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。 3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。 4. 按一下**建立**按鈕。 PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。 • **具有用戶端身分驗證的自訂PFX**是指使用PFX金鑰進行TLS加密。在此模式下，用戶端將使用憑證進行身份驗證。 您必須使用PKCS#12容器格式的私鑰生成PFX憑證，然後將PFX憑證作為PFX密鑰上傳到KUMA網頁介面。如果選擇此值，請在「PFX密鑰」下拉清單中指定一個由憑證授權單位簽署的PFX憑證。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇「新建」。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立PFX密鑰？** *若要建立PFX密鑰：* 1. 在**名稱**欄位中，輸入PFX密鑰的名稱。 2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。 3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。 4. 按一下**建立**按鈕。 PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。

SQL類型

sql類型的連接器用於查詢資料庫。KUMA支援多種類型的資料庫。

支援的資料庫類型

此程式支援以下類型的SQL資料庫：

- SQLite
- MSSQL
- MySQL
- PostgreSQL
- Cockroach

- Oracle
- Firebird

建立**sql**類型的連接器時，必須指定一般連接器設定和個別資料庫連線設定。下表描述了**sql**類型連接器的設定。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
類型	連接器類型：**sql**。 必需設定。
標記	資源搜尋標籤。 可選設定。
預設查詢	連線至資料庫時執行的 SQL 查詢。 必需設定。
每次傳送請求時都重新連線到資料庫	此切換開關會啟用連接器在每次傳送查詢時重新連線至資料庫。預設情況下，切換開關處於關閉狀態。
輪詢間隔，秒	執行 SQL 查詢的間隔時間，以秒為單位。預設值是 10 秒。

設定	描述
連線	此群組中的設定取決於為連線選取的資料庫類型： MySQL Postgres SQLite3 Oracle Firebird ClickHouse ODBC • **資料庫種類**是要連線的資料庫類型。選擇資料庫類型時，**URL** 欄位中會顯示與通訊協定對應的前綴。例如，對於 **ClickHouse** 資料庫，**URL** 欄位包含 `clickhouse://` 前綴。 • **獨立密鑰**核取方塊允許檢視連線資訊。如果您選取了**獨立密鑰**核取方塊，則認證資料會在 **密碼** 欄位中指定，而連線字串則會輸入到 **URL** 欄位中，且不指定使用者的密碼。 • 如果您已選取 **獨立密鑰** **核取方塊，則 URL 是連線 URL。**這樣一來，如果您用於連線的使用者帳戶密碼變更，您可以檢視連線資訊，而無需重新建立大量連線。 建立連線時，如果在 URL 中指定連線資訊，則包含特殊字元的認證資料字串可能無法正確處理。如果在建立連線時發生錯誤，但您確定指定的設定正確，請以百分比編碼輸入特殊字元。 **特殊字元代碼** ! # $ % & ' ( ) * + %21 %23 %24 %25 %26 %27 %28 %29 %2A %2B . / : ; = ? @ [ ] \ %2C %2F %3A %3B %3D %3F %40 %5B %5D %5C 用於存取SQL資料庫的密碼不支援以下特殊字元：空格、`[`、`]`、`:`、`/`、`#`、`%`、`\` 如果您已選取**獨立密鑰**核取方塊，則不需要使用任何特殊字元代碼。 在**使用密鑰中的 URL**下拉式清單中，您可以選擇現有 URL 或建立新的 URL。若要建立新 URL，請選擇**新建**。 若要編輯現有 URL 的設定，請點選其旁邊的鉛筆圖示。 • **密鑰** 是儲存連線到資料庫所用 URL 清單的 URL 密鑰。如果選取了**獨立密鑰**核取方塊，則會顯示此欄位。 • **身分直欄**是包含表格每行 ID 的直欄名稱。 必需設定。 • **身分種子**是身分直欄中的值，用於判斷要從 SQL 表格的哪一列開始讀取資料。 • **查詢**是取代預設 SQL 查詢執行的其他 SQL 查詢。 • **輪詢間隔，秒**是 SQL 查詢執行間隔，以秒為單位。指定的間隔將取代連接器的預設間隔。預設值是 10 秒。 您可以新增多個連線或刪除連線。若要新增連線，請點選**+ 新增連線**按鈕。若要刪除連線，請點選其旁邊的刪除圖示。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。
字元編碼	字符編碼。預設值是**UTF-8**。 KUMA將SQL回應轉換為UTF-8編碼。您可以將SQL伺服器設定為以UTF-8編碼傳送回應，或在KUMA端變更傳入訊息的編碼。

在單一連接器中，您可以為多個受支援的資料庫**建立連線**。若無法啟動具有 **sql** 類型連接器的收集器，請檢查 /opt/kaspersky/kuma/collector/<收集器 ID>/sql/state-<檔案 ID> 狀態檔案是否為空。如果狀態檔案為空，請將其刪除並重新啟動收集器。

若要為多個SQL資料庫建立連線：

1. 按一下**新增連線**按鈕。
2. 指定**URL** 、**身分直欄**、**身分種子**、**查詢**和**輪詢間隔（秒）**值。
3. 對每個所需的連線重複步驟1-2。

支援的SQL類型及其特定使用功能

支援以下SQL類型：

- MSSQL
  例如：
  - `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}`

  我們建議使用此 URL 變體。
  - `sqlserver://{user}:{password}@{server}?database={database}`

  `@p1` 字元在 SQL 查詢中用作佔位符。

  > 如果要使用網域帳戶憑據進行連線，請以 `< domain >%5C< user >` 格式指定帳戶名稱。例如：`sqlserver://domain%5Cuser:password@ksc.example.com:1433/SQLEXPRESS?database=KAV`。

- MySQL/MariaDB
  例如：
  `mysql://{user}:{password}@tcp({server}:{port})/{database}`
  `?` 字元在 SQL 查詢中用作佔位符。

- PostgreSQL
  例如：`postgres://{user}:{password}@{server}/{database}?sslmode=disable`
  `$1` 字元在 SQL 查詢中用作佔位符。

- CockroachDB
  例如：
  `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`
  `$1` 字元在 SQL 查詢中用作佔位符。

- SQLite3
  例如：
  `sqlite3://file:{file_path}`
  問號 (`?`) 在 SQL 查詢中用作佔位符。
  在查詢 SQLite3 時，若 ID 的初始值為 datetime 格式，必須在 SQL 查詢中新增使用 `sqlite datetime` 函式的日期轉換。例如：
  `select * from connections where datetime(login_time) > datetime(?, 'utc') order by login_time`
  在此範例中，`connections` 為 SQLite 資料表，而變數 `?` 的值取自 **身分種子** 欄位，且必須以 `{< date >}T{< time >}Z` 格式指定，例如 `2021-01-01T00:10:00Z)`。

- Oracle DB
  使用「oracle」驅動程式的密鑰範例 URL：
  `oracle://{user}:{password}@{server}:{port}/{service_name}`
  `oracle://{user}:{password}@{server}:{port}/?SID={SID_VALUE}`

如果查詢執行時間超過 30 秒，oracle 驅動程式會中止 SQL 請求，並且收集器記錄檔中會出現以下錯誤：**user requested cancel of current operation**。若要延長 SQL 查詢的執行時間，請在連線字串中指定 **timeout** 參數的值（以秒為單位），例如：

```
oracle://{user}:{password}@{server}:{port}/{service_name}?timeout=300
```

其中，SQL 變數 `:val` 用作預留位置。

查詢 Oracle DB 時，若身分種子採用 datetime 格式，則必須考慮資料庫中該欄位的類型，並在必要時於 SQL 查詢中新增時間字串轉換，以確保 SQL 連接器正常運作。例如，如果資料庫中的 `Connections` 資料表具有 `login_time` 欄位，則可進行下列轉換：

- 如果 **login_time** 欄位的類型為 TIMESTAMP，則依據資料庫設定，**login_time** 欄位可能包含 `YYYY-MM-DD HH24:MI:SS` 格式的值，例如 `2021-01-01 00:00:00`。在此情況下，您需要在 **身分種子** 欄位中指定 `2021-01-01T00:00:00Z`，並在 SQL 查詢中使用 `to_timestamp` 函式執行轉換，例如：

  ```
  select * from connections where login_time > to_timestamp(:val, 'YYYY-MM-DD"T"HH24:MI:SS"Z"')
  ```

- 如果 **login_time** 欄位的類型為 TIMESTAMP WITH TIME ZONE，則依據資料庫設定，**login_time** 欄位可能包含 `YYYY-MM-DD"T"HH24:MI:SSTZH:TZM` 格式的值（例如 `2021-01-01T00:00:00+03:00`）。在此情況下，您需要在身分種子欄位中指定 `2021-01-01T00:00:00+03:00`，並在 SQL 查詢中使用 `to_timestamp_tz` 函式執行轉換，例如：

  ```
  select * from connections_tz where login_time > to_timestamp_tz(:val, 'YYYY-MM-DD"T"HH24:MI:SSTZH:TZM')
  ```

  如需有關 `to_timestamp` 和 `to_timestamp_tz` 函式的詳細資訊，請參閱 Oracle 官方文件。

若要與Oracle DB交互，必須安裝libaio1 Astra Linux套件。

- Firebird® SQL

  例如：

  ```
  firebirdsql://{user}:{password}@{server}:{port}/{database}
  ```

  問號 (`?`) 在 SQL 查詢中用作佔位符。

  如果在 Windows 上連線 Firebird 時出現問題，請使用資料庫檔案的完整路徑，例如：

  ```
  firebirdsql://{user}:{password}@{server}:{port}/C:\Users\user\firebird\db.FDB
  ```

- ClickHouse

  例如：

  ```
  clickhouse://{user}:{password}@{server}:{port}/{database}
  ```

  問號 (`?`) 在 SQL 查詢中用作佔位符。

  KUMA 支援下列資料類型：

  - 可轉換為字串的資料（例如字串、數值和 BLOB）會以字串形式顯示。
  - 陣列和映射會以 JSON 格式顯示，或透過內建的 `go fmt.Sprintf("%v",v)` 函式以最佳方式顯示。

  有兩種連線至 ClickHouse 的方法：

  - 不使用憑證，透過輸入 URL：`clickhouse://host:port/database`
  - 使用憑證，透過輸入 URL：`clickhouse://user:password@host:port/database`

使用 TLS 加密時，連接器預設僅在連接埠 9440 上運作。如果未使用 TLS 加密，連接器預設僅透過連接埠 9000 與 ClickHouse 搭配運作。

連接器無法透過 HTTP 運作。

如果 ClickHouse 伺服器上已設定 TLS 加密模式，而您在連接器設定的 **TLS 模式** 下拉式清單中選取 **已停用**，或反之亦然，則無法建立資料庫連線。

TLS 模式 只會在指定 ClickHouse 驅動程式時使用。

如果要連線到 KUMA ClickHouse，請在 **SQL** 連接器設定中指定 **PublicPKI** 密鑰類型，其中包含 base64 編碼的 PEM 私密金鑰和公開金鑰。

在 ClickHouse 連線類型的 **SQL** 連接器參數中，您需要在 **TLS 模式** 下拉式清單中選取 **已停用**。如果使用憑證進行驗證，則不得指定此值。如果您在 **TLS 模式** 下拉式清單中選取 **自訂 CA**，則需要在 **密鑰** 欄位中指定「certificate」類型密鑰的 ID。您還需要在 **授權類型** 下拉式清單中選取下列其中一個值：

- **已禁用** 。如果選取此值，您需要將 **密鑰** 欄位留空。
- **Plain**。如果已選取 **獨立密鑰** 核取方塊，並在 **密鑰** 欄位中指定「憑據」類型密鑰的 ID，請選取此值。
- **PublicPKI**。如果已選取 **獨立密鑰** 核取方塊，並在 **密鑰** 欄位中指定 PublicPKI 類型密鑰的 ID，請選取此值。

如果 ID 的初始值包含時間指示（ `datetime` ），則在查詢中必須使用時間轉換變數（ `parseDateTimeBestEffort` ）。例如，如果時間指定為 `2021-01-01 00:10:00`，則可以使用下列查詢：

```
select connections, username, host, login_time from connections where login_time > parseDateTimeBestEffort(?) order by login_time
```

- ODBC

  例如：

  `odbc://{server}:{port}/{database}`：如果您在配置連線設定時選取了 **獨立密鑰** 核取方塊。

  `odbc://{server}:{port}/{database}?params1=value1&params2=value2`：如果您需要指定所有連線參數。

  問號 (`?`) 在 SQL 查詢中用作佔位符。

  當收集器部署在 Kubernetes 中時，不支援 ODBC。

  如果您使用 ODBC，則需要為 **ODBC 驅動程式檔案名稱** 設定指定 ODBC 資料庫驅動程式的名稱。然後，您需要將驅動程式檔案儲存在 `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` 目錄中。

  解決方案使用 ODBC Manager 系統公用程式 2.3.14 版來管理 ODBC 驅動程式和資料庫連線。您需要使用與此版本的系統公用程式相容的 ODBC 驅動程式。

指定 ODBC 資料庫驅動程式的名稱時，請考慮下列事項：

- 如果驅動程式具有相依性，您需要將這些相依項儲存在 `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` 或 `/opt/kaspersky/kuma/collector/<uuid_of_collector>/` 目錄中（如果驅動程式有此要求）。
- 此設定區分大小寫。
- 指定路徑時，可以使用特殊字元。

ODBC 資料庫驅動程式名稱範例

```
psqlodbcw.so
```

若要在現有收集器中使用 ODBC SQL 連接器，將解決方案從 4.2 版升級後，您需要解除安裝，然後重新安裝收集器。這可讓您取得 ODBC 連接器正確運作所需的所有環境變數值。

使用 ODBC 驅動程式設定 SQL 連接器的範例

若要設定連接器以搭配 ODBC 驅動程式運作（以 PostgreSQL 和 Astra Linux 的 ODBC 驅動程式為例）：

1. 檢查您的資料庫是否有可用的 ODBC 驅動程式。如果有此類驅動程式，請在線上查找該驅動程式的 .so 副檔名檔案名稱。
2. 在 **監控** → **資源和服務** → **連接器** 區段中，建立 SQL 連接器；在 **資料庫種類** 欄位中，選取 **ODBC**。
3. 填寫新連接器的所有必填欄位，方法是在 **ODBC 驅動程式檔案名稱** 欄位中指定 ODBC 驅動程式的名稱。

   如有必要，您可以在使用指定的連接器安裝收集器後變更驅動程式名稱。
4. 在主機上安裝含有 SQL 連接器的收集器。
5. 下載適當的 .so 檔案。對於 PostgreSQL，您可以使用以下命令下載此檔案：

   ```
   apt download odbc-postgresql
   ```

   解決方案會下載適用於 Astra Linux 的 `ibpq5_15.17-astra.se2.3r2_amd64.deb` 套件。
6. 請執行下列操作：

   a. 執行以下命令解壓縮 `ibpq5_15.17-astra.se2.3r2_amd64.deb` 套件：

   ```
   ar x libpq5_15.17-astra.se2.3r2_amd64.deb
   ```

   b. 執行以下命令解壓縮 `data.tar.xz` 壓縮檔案：

   ```
   tar -xf data.tar.xz
   ```
7. 在解出的檔案中，執行以下命令尋找 .so 檔案：

   ```
   find . -name ".so"
   ```

8. 執行以下命令，將 PostgreSQL ODBC 驅動程式複製到收集器目錄內的 `driver` 目錄：

```
cp ./usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so
```

9. 執行以下命令，確認主機上已滿足所有 ODBC 驅動程式相依性：

```
LD_LIBRARY_PATH="/opt/kaspersky/kuma/collector/<ID>/deps/odbc:/opt/kaspersky/kuma/collector/<ID>/driver"
ldd /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so | grep "not found"
```

其中 `<ID>` 是已安裝收集器的 ID。

如果命令顯示 `libpq.so.5 => not found`，您還需要下載 `libpq.so.5` 相依性。若使用 Astra Linux，您也可以執行以下命令完成此操作：

```
apt download libpq5
```

之後，解開 deb 套件並搜尋 .so 檔案。將找到的 .so 檔案移至收集器資料夾 (`cp ./usr/lib/x86_64-linux-gnu/libpq.so.5.15 /opt/kaspersky/kuma/collector/<ID>/driver/libpq.so.5`) 中的 `driver` 目錄。

10. 重新檢查主機上的所有 ODBC 驅動程式相依性。此外，請確定收集器的 `driver` 目錄 (`/opt/kaspersky/kuma/` collector/<ID>/driver/psqlodbcw.so) 中的驅動程式檔案名稱，與設定檔中的檔案名稱相符。

為防止發生遺漏相依性相關錯誤，您可以將 `- Environment=LD_DEBUG=libs` 這一行新增至收集器的 systemd 檔案，並執行以下命令：

```
systemctl daemon-reload
```

然後重新啟動收集器；`journalctl` 會顯示 ODBC 驅動程式搜尋相依性的相關資訊。

每種 ODBC 驅動程式都有其呈現遺漏相依性相關資訊的特殊方式。例如，MsSQL ODBC 驅動程式會在 `driver` 目錄的上一層尋找相依性。您需要將遺漏的 `share` 資料夾儲存在 `/opt/kaspersky/kuma/collector/<ID>` 中，而不是 `driver` 目錄中。視 ODBC 驅動程式而定，指定 URL 時也可能會有一些特殊情況。例如，對於 Oracle ODBC 驅動程式，您需要在連接器設定檔中以 `odbc://?DBQ=//{server}:{port}/{database}` 格式指定 URL (使用者帳戶需另行指定)。

> 設定 ODBC 驅動程式時，建議遵循特定驅動程式的文件。

11. 重新啟動收集器。

SQL 查詢支援對資料庫資訊的順序請求。例如，如果您在 **查詢** 欄位中輸入 `select * from <資料表名稱> where id > <預留位置>`，則第一次查詢該資料表時，會將 **識別種子** 欄位的值用作預留位置值。此外，使用 SQL 連接器的服務會儲存最後讀取項目的 ID，並且該項目的 ID 將用作下次查詢資料庫時的佔位符值。

> 建議將 `order by` 命令新增至查詢字串，後接排序欄位。例如，`select * from table_name where id > ? order by id`。

SQL請求範例

SQLite、Firebird—`select * from table_name where id > ?`

MSSQL—`select * from table_name where id > @p1`

MySQL—`select * from table_name where id > ?`

PostgreSQL、Cockroach—`select * from table_name where id > $1`

Oracle—`select * from table_name where id > :val`

檔案類型

檔案類型用於從任何文字檔案中檢索資料。檔案中的一個字串被視為一個事件。字串分隔符號：\n。此類連接器適用於Linux代理程式和Windows代理程式。

要讀取Windows檔案，您需要建立一個「檔案」類型的連接器，並在Windows上手動安裝代理程式。在一個Windows代理程式中，您可以設定多個不同類型的連線，但只能有一個「檔案」類型的連線。Windows代理程式不得讀取其安裝資料夾中的檔案。即使使用 FAT 檔案系統，此連接器也能正常運作。如果磁碟進行重組，連接器會重新讀取所有檔案，因為所有檔案的 inode 都會重設。

不建議使用管理員帳戶執行代理。代理的使用者帳戶必須具備資料夾和檔案的讀取權限。不建議在重要系統上安裝代理。建議傳送事件記錄，並由專用裝置上的代理讀取。

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填） - 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型，**檔案**。
  - **檔案路徑**（必填）— 要互動之檔案的完整路徑。例如，`/var/log/*som?[1-9].log or c:\folder\logs.*.` 不允許使用下列路徑：
    - `` `(?i)^[a-zA-Z]:\\Program Files` ``
    - `` `(?i)^[a-zA-Z]:\\Program Files \(x86\)` ``
    - `` `(?i)^[a-zA-Z]:\\Windows` ``
    - `` `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` ``

    檔案和資料夾遮罩範本

    遮罩：
    - '*'—比對任意字元序列。
    - '[' ['^'] { 字元範圍 } ']'—字元類別（不得留空）。
    - '?'—比對任意單一字元。

    字元範圍：
    - [0-9]—數字；
    - [a-zA-Z]—拉丁字母字元。

例如：

- /var/log/*som?[1-9].log
- /mnt/dns_logs/*/dns.log
- /mnt/proxy/access*.log

在檔案路徑中使用前綴時的限制

指定檔案路徑時不能使用的前綴：

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*

- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。

檔案位於下列路徑：

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

透過遮罩限制要監視的檔案數量

Core 的 max_user_watches 設定可限制同時透過遮罩監視的檔案數量。若要檢視設定值，請執行以下命令：

```
cat /proc/sys/fs/inotify/max_user_watches
```

如果要監視的檔案數量超過 max_user_watches 設定值，收集器將無法再從檔案讀取任何事件，並在收集器記錄中寫入以下錯誤：

```
Failed to add files for watching {"error": "no space left on device"}
```

為確保收集器持續正常運作，您可以設定適當的檔案輪替方式，使檔案數量不超過 max_user_watches 設定值，或提高 max_user_watches 設定值。

若要提高設定值：

```
sysctl fs.inotify.max_user_watches=<number of files>
```

```
sysctl -p
```

您也可以將 max_user_watches 設定值加入 sysctl.conf，以確保該值永久保留。

提高 max_user_watches 設定值後，收集器便會恢復正常運作。

- **Auditd**是將從連接器收到的auditd日誌事件記錄分組為單一事件的機制的切換開關。Auditd 僅支援 \n 分隔符號。若啟用切換開關，**分隔符號**欄位將無法使用。如果在代理連接器中啟用了**Auditd**切換開關，則必須在代理程式向其傳送事件的收集器的連接器中設定\n分隔符號。
- **適用於Windows**是一個切換開關，開啟後將允許從Windows代理程式接收Windows事件日誌事件。在這種情況下，必須關閉**Auditd**開關。預設情況下，**適用於Windows**切換開關處於關閉狀態。
- **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。
  - **緩衝區大小**設定用於指定在將事件傳送到儲存或進一步處理之前，用於在RAM中累積事件的緩衝區大小（以位元組為單位）。

    預設值：1048576位元組（1MB）。

可能值：小於或等於67108864位元組（64MB）的正整數。

- **處理程式數量**用於設定處理佇列的服務數量。您可以使用下列公式確定處理程序的數量：(<CPU核心數>/2) + 2。

- **輪詢間隔（毫秒）**用於設定連接器重新讀取包含檔案的目錄的間隔。該值以毫秒為單位。只有當檔案沒有變更時，連接器才會等待指定的時間。如果檔案被連續修改，且輪詢間隔=5000毫秒，則不會觀察到重新讀取目錄中檔案的5秒間隔，而是連續重新讀取。如果檔案沒有更改，連接器將等待5秒。如果在網頁介面中設定了0，則使用預設值700毫秒。我們建議將 **輪詢間隔（毫秒）**（毫秒）設定為至少 **事件緩衝 TTL** 的值。否則，**Auditd**選項可能會受到不利影響。

- **字元編碼** 設定可指定字元編碼。預設值是UTF-8。

- **事件緩衝TTL**是緩衝區的生存時間，用於將記錄分組為單一auditd事件。只有啟用了**Auditd**切換開關，此欄位才可用。倒數計時從收到第一個事件行時開始，或在上一個TTL過期後立即開始。可能值：700毫秒到3000毫秒。預設值是2000毫秒。

- **傳輸標頭**— 對於auditd事件，您必須指定一個規則運算式來辨識auditd日誌的各個部分。您可以使用預設值或加以編輯。規則運算式必須包含record_type_name、record_type_value和event_sequence_number群組。如果多行auditd事件包含前綴，則第一個記錄將保留該前綴，而後續條目將丟棄該前綴。

  您可以透過點擊**重設為預設值**來恢復到原始值。

1c-xml類型

1c-xml類型用於從1C應用程式註冊日誌中檢索資料。當連接器處理多行事件時，它會將其轉換為單行事件。此類型的連接器適用於Linux代理程式。

建立此類型的連接器時，請指定以下設定的值：

- **基本設定**頁籤：

  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。

  - **租用戶**（必填）- 擁有該資源的租用戶名稱。

  - **類型**（必要）— 連接器類型，**1c-xml**。

  - **URL**（必要）—包含您需要互動之檔案的目錄完整路徑。例如，`/var/log/1c/logs/`。

    在檔案路徑中使用前綴時的限制

    指定檔案路徑時不能使用的前綴：

    - `/*`
    - `/bin`
    - `/boot`
    - `/dev`
    - `/etc`
    - `/home`

- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。

檔案位於下列路徑：

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/metrics/log/

- **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **緩衝區大小**設定用於指定在將事件傳送到儲存或進一步處理之前，用於在RAM中累積事件的緩衝區大小（以位元組為單位）。

預設值：1048576位元組（1MB）。

可能值：小於或等於67108864位元組（64MB）的正整數。

- **輪詢間隔（毫秒）**用於設定連接器重新讀取包含檔案的目錄的間隔。該值以毫秒為單位。只有當檔案沒有變更時，連接器才會等待指定的時間。如果檔案被連續修改，且輪詢間隔=5000毫秒，則不會觀察到重新讀取目錄中檔案的5秒間隔，而是連續重新讀取。如果檔案沒有更改，連接器將等待5秒。如果在網頁介面中設定了0，則使用預設值700毫秒。

- **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

連接器操作圖：

1. 系統會在指定目錄內搜尋包含1C日誌且副檔名為XML的檔案。日誌可手動放置在目錄中，也可使用以 1C 語言編寫的應用程式放置，例如使用 `DownloadRegistrationLog()` 函數。連接器僅支援以這種方式接收的記錄。有關如何取得1C記錄的更多資訊，請參閱官方1C說明文件。

2. 檔案依上次修改時間升序排序。上次讀取之前修改的所有檔案都將被丟棄。

   已處理檔案的相關資訊儲存在 /<收集器工作目錄>/1c_xml_connector/state.ini 檔案中，格式如下：`offset=<number>\ndev=<number>\ninode=<number>`。

3. 事件在每個未讀檔案中定義。

4. 檔案中的事件被逐一處理。多行事件將轉換為單行事件。

連接器限制：

- Windows作業系統不支援安裝帶有1c-xml連接器的收集器。要設定1C日誌檔案的檔案傳輸以供KUMA收集器處理：

  1. 在Windows伺服器上，授予包含1C日誌檔案的資料夾的網路讀取權限。

  2. 在Linux伺服器上，將包含1C日誌檔案的共用資料夾掛載到Windows伺服器上（請參閱支援的作業系統清單）。

  3. 在Linux伺服器上，安裝要從已掛載的共用資料夾處理1C日誌檔案的收集器。

- 不會讀取事件格式不正確的檔案。例如，如果檔案中的事件標籤是俄語，收集器就不會讀取此類事件。

包含事件的正確XML檔案範例。

```
<?xml version="1.0" encoding="UTF-8"?>
<v8e:EventLog xmlns:v8e="http://v8.1c.ru/eventLog"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <v8e:Event>
                <v8e:Level>Information</v8e:Level>
                <v8e:Date>2022-12-07T01:55:44+03:00</v8e:Date>
                <v8e:ApplicationName>generator.go</v8e:ApplicationName>

<v8e:ApplicationPresentation>generator.go</v8e:ApplicationPresentation>
                <v8e:Event>Test event type: Count test</v8e:Event>
                <v8e:EventPresentation></v8e:EventPresentation>
                <v8e:User>abcd_1234</v8e:User>
                <v8e:UserName>TestUser</v8e:UserName>
                <v8e:Computer>Test OC</v8e:Computer>
                <v8e:Metadata></v8e:Metadata>
                <v8e:MetadataPresentation></v8e:MetadataPresentation>
                <v8e:Comment></v8e:Comment>
                <v8e:Data>
                        <v8e:Name></v8e:Name>
                        <v8e:CurrentOSUser></v8e:CurrentOSUser>
                </v8e:Data>
                <v8e:DataPresentation></v8e:DataPresentation>
                <v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus>
                <v8e:TransactionID></v8e:TransactionID>
                <v8e:Connection>0</v8e:Connection>
                <v8e:Session></v8e:Session>
                <v8e:ServerName>kuma-test</v8e:ServerName>
                <v8e:Port>80</v8e:Port>
                <v8e:SyncPort>0</v8e:SyncPort>
        </v8e:Event>
</v8e:EventLog>
```

已處理事件的範例。

```
<v8e:Event><v8e:Level>Information</v8e:Level><v8e:Date>2022-12-
07T01:55:44+03:00</v8e:Date><v8e:ApplicationName>generator.go</v8e:ApplicationName><v8e:ApplicationPresentation>generator.go
</v8e:ApplicationPresentation><v8e:Event>Test event type: Count
test</v8e:Event><v8e:EventPresentation></v8e:EventPresentation><v8e:User>abcd_1234</v8e:User><v8e:UserName>TestUser</v8e:Use
rName><v8e:Computer>Test
OC</v8e:Computer><v8e:Metadata></v8e:Metadata><v8e:MetadataPresentation></v8e:MetadataPresentation><v8e:Comment></v8e:Commen
t><v8e:Data><v8e:Name></v8e:Name><v8e:CurrentOSUser></v8e:CurrentOSUser></v8e:Data><v8e:DataPresentation></v8e:DataPresentat
ion><v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus><v8e:TransactionID></v8e:TransactionID><v8e:Connection>0</v8
e:Connection><v8e:Session></v8e:Session><v8e:ServerName>kuma-
test</v8e:ServerName><v8e:Port>80</v8e:Port><v8e:SyncPort>0</v8e:SyncPort></v8e:Event>
```

- 如果連接器讀取的檔案中充滿了新事件，且此檔案不是目錄中讀取的最後一個檔案，則會重新處理該檔案中的所有事件。

1c-log類型

1c-log類型用於從1C應用程式技術日誌中檢索資料。字串分隔符號：\n。連接器僅接受多行事件記錄的第一行。此類型的連接器適用於Linux代理程式。

建立此類型的連接器時，請指定以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必需）— 連接器類型， **1c-log** 。
  - **URL** （必要）—包含您需要互動之檔案的目錄完整路徑。例如， `/var/log/1c/logs/` 。

    在檔案路徑中使用前綴時的限制

指定檔案路徑時不能使用的前綴：

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。

檔案位於下列路徑：

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

- **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **緩衝區大小**設定用於指定在將事件傳送到儲存或進一步處理之前，用於在RAM中累積事件的緩衝區大小（以位元組為單位）。

    預設值：1048576位元組（1MB）。

    可能值：小於或等於67108864位元組（64MB）的正整數。
  - **輪詢間隔（毫秒）**用於設定連接器重新讀取包含檔案的目錄的間隔。該值以毫秒為單位。只有當檔案沒有變更時，連接器才會等待指定的時間。如果檔案被連續修改，且輪詢間隔=5000毫秒，則不會觀察到重新讀取目錄中檔案的5秒間隔，而是連續重新讀取。如果檔案沒有更改，連接器將等待5秒。如果在網頁介面中設定了0，則使用預設值700毫秒。
  - **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

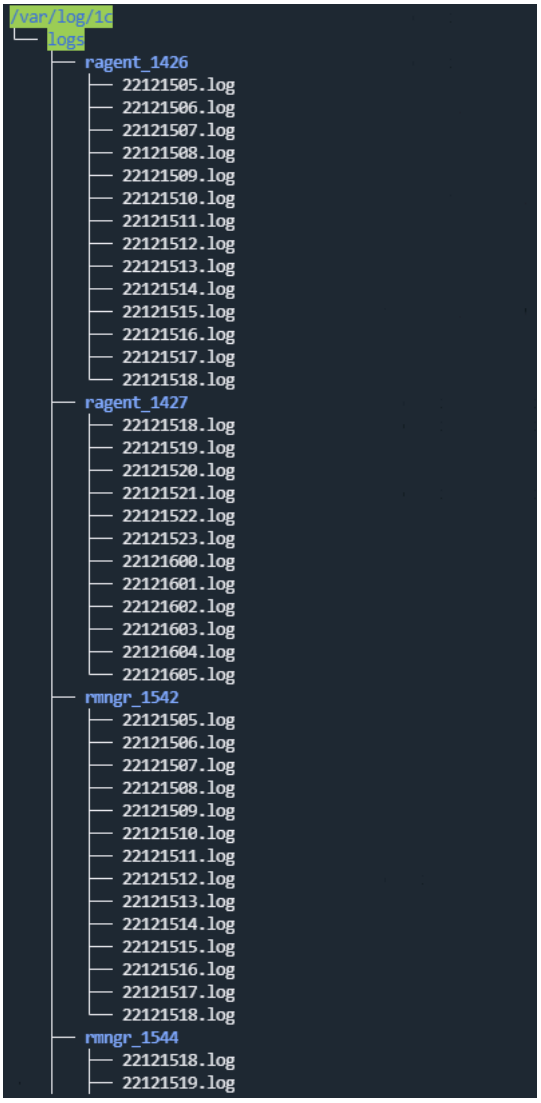
連接器操作圖：

1. 搜尋所有1C技術日誌檔案。

   日誌檔案需求：

   - 帶有 LOG 副檔名的檔案會在日誌目錄（預設為 `/var/log/1c/logs/` ）中建立，且每個處理程序都有專屬子目錄。

支援的1C技術日誌結構範例



- 事件記錄到檔案中，記錄時間為一小時；之後，將建立下一個日誌檔案。
- 檔案名稱格式如下：`<YY><MM><DD><HH>.log`。例如，`22111418.log` 是 2022 年 11 月 14 日 18:00 建立的檔案。
- 每個事件都以以下格式的事件時間開頭：<mm>:<ss>.<microseconds>-<duration_in_microseconds>。

2. 已處理的檔案將被丟棄。

   已處理檔案的相關資訊儲存在檔案/<連接器工作目錄>/1c_log_connector/state.json中。

3. 新事件開始處理，事件時間轉換為RFC3339格式。

4. 隊列中的下一個檔案將被處理。

連接器限制：

- Windows作業系統不支援安裝具有1c-log連接器的收集器。要設定1C日誌檔案的檔案傳輸以供KUMA收集器處理：

  1. 在Windows伺服器上，授予包含1C日誌檔案的資料夾的網路讀取權限。
  2. 在Linux伺服器上，將包含1C日誌檔案的共用資料夾掛載到Windows伺服器上（請參閱支援的作業系統清單）。
  3. 在Linux伺服器上，安裝要從已掛載的共用資料夾處理1C日誌檔案的收集器。

- 僅處理多行事件記錄的第一行。
- 標準化器僅處理以下類型的事件：
  - ADMIN
  - ATTN
  - CALL
  - CLSTR
  - CONN
  - DBMSSQL
  - DBMSSQLCONN
  - DBV8DBENG
  - EXCP
  - EXCPCNTX
  - HASP
  - LEAKS
  - LIC
  - MEM
  - PROC
  - SCALL
  - SCOM
  - SDBL
  - SESN
  - SINTEG

- SRVC
- TLOCK
- TTIMEOUT
- VRSREQUEST
- VRSRESPONSE

二極體類型

用於透過資料二極體傳輸事件。

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型，**二極體**。
  - **資料二極體目的地目錄**（必填）— KUMA收集器伺服器目錄的完整路徑，資料二極體將包含來自隔離網段的事件的檔案移至該目錄。連接器讀取這些檔案後，將從目錄中刪除這些檔案。該路徑最多可包含255個Unicode字元。

    在路徑中使用前綴的限制

    指定檔案路徑時不能使用的前綴：

    - `/*`
    - `/bin`
    - `/boot`
    - `/dev`
    - `/etc`
    - `/home`
    - `/lib`
    - `/lib64`
    - `/proc`
    - `/root`
    - `/run`
    - `/sys`

- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。

檔案位於下列路徑：

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/metrics/log/

- **分隔符號**用於指定代表事件之間分隔符號的字元。可用值：\n、\t、\0。若未指定分隔符號（選取的值為空），則預設值為 \n。

  此設定必須與用於透過資料二極體中繼來自隔離網段的事件的連接器和目標資源相符。

- **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **工作線程**— 處理請求佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
  - **輪詢間隔，秒**— 從包含來自資料二極體的事件的目錄讀取檔案的頻率。預設值是2。時間以秒為單位指定。
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **壓縮**- 您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。

    此設定必須與用於透過資料二極體中繼來自隔離網段的事件的連接器和目標資源相符。
  - **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

Ftp類型

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填） - 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型， **ftp**。
  - **URL**（必填）—檔案或檔案遮罩的實際 URL，以「ftp:// 」開頭。對於檔案遮罩，您可以使用 * ? [...]。
    檔案遮罩範本

    遮罩：

    - '*'—比對任意字元序列。
    - '[' ['^'] { 字元範圍 } ']'—字元類別（不得留空）。
    - '?'—比對任意單一字元。

    字元範圍：

    - [0-9]—數字；
    - [a-zA-Z]—拉丁字母字元。

    例如：

    - /var/log/*som?[1-9].log
    - /mnt/dns_logs/*/dns.log
    - /mnt/proxy/access*.log

    如果URL不包含FTP伺服器端口，則插入連接埠21。
  - **URL 憑據**— 用於指定FTP伺服器的使用者名稱和密碼。如果沒有使用者名稱和密碼，則該行保留為空。
  - **描述** — 資源描述：最多4,000個Unicode字元。
- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

Sftp類型

sftp 類型的連接器用於在使用 Windows 和 Linux 代理時，透過安全檔案傳輸通訊協定 (SFTP) 取得資料。

下表描述了**sftp**類型連接器的設定。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
類型	連接器類型：**sftp**。 必需設定。
標記	資源搜尋標籤。 可選設定。
URL	以 `'sftp://'` 配置開頭的日誌檔案 URL 或檔案遮罩，例如 `sftp://example.ru:22/path/to/file.log`。您可以將 `* ? [...]` 用於檔案遮罩。 **檔案遮罩範本** 遮罩： • '*'—比對任意字元序列。 • '[' ['^'] { 字元範圍 } ']'—字元類別（不得留空）。 • '?'—比對任意單一字元。 字元範圍： • [0-9]—數字； • [a-zA-Z]—拉丁字母字元。 例如： • /var/log/*som?[1-9].log • /mnt/dns_logs/*/dns.log • /mnt/proxy/access*.log 如果 URL 不包含 SFTP 伺服器的連接埠號碼，則會自動指定連接埠 `22`。 必需設定。

SSH 伺服器公開金鑰	建立 SSH 連線時用來驗證 SFTP 伺服器的公開金鑰。您可以指定多個不同類型的金鑰，連接器會自動選取適當的金鑰。
	格式：`<key_type> <base64-value>`
	金鑰範例：ssh-ed25519 ABCD...
	在伺服器上，公開金鑰儲存在以下路徑：
	`/etc/ssh/ssh_host_*_key.pub`
	您也可以執行以下命令來取得公開金鑰：
	`ssh-keyscan [-p port] [-t type] [host | addrlist namelist]`
	範例命令：
	`ssh-keyscan example.com`
	`ssh-keyscan -p 2222 -t rsa,ed25519 example.com`
	必需設定。

設定	描述
密鑰	儲存用於連線至 SFTP 伺服器之憑證的密鑰。支援 **憑證**和 **SSH 私密金鑰**類型的密鑰。此密鑰必須包含使用者名稱與密碼，或 SSH 私密金鑰。如果您不需要憑證即可連線至 SFTP 伺服器，請將使用者名稱和密碼欄位留空。 您可以選擇現有密鑰或建立新密鑰。若要建立新密鑰，請選擇**新建**。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立密鑰？** *若要建立密鑰：* 1. 在**名稱**欄位中，輸入密鑰的名稱。 2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。 3. 如有必要，在**描述**欄位中輸入密鑰的描述。 4. 點擊**建立**按鈕。 密鑰將會新增並顯示在**密鑰**下拉清單中。 必需設定。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。
字元編碼	從 SFTP 伺服器接收之檔案的編碼。預設編碼為 UTF-8。 可選設定。

smb類型

smb 類型的連接器用於在使用 Linux 代理時，透過 SMB（Server Message Block）通訊協定接收資料。下表說明 **smb** 類型連接器的可用設定。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
類型	連接器類型：**smb**。 必需設定。
標記	資源搜尋標籤。 可選設定。
URL	以下其中一種格式的遠端目錄路徑： • `smb://< ip_address 或 host_name >:< port >/< shared_resource_name >` • `smb://< ip_address 或 host_name >:< port >/< shared_resource_name >/< directory_path >` KUMA 只會從路徑中最後一個目錄內的檔案取得資訊。假設您指定下列路徑： `smb://< ip_address 或 host_name >:< port >/< shared_resource_name >/< directory1 >/< directory2 >` 在此情況下，KUMA 只會從 directory2 中的檔案取得資訊。如果 directory2 有更深層的子目錄，將不會讀取這些子目錄中的檔案。 如果未指定連接埠，KUMA 會自動使用連接埠 445。 必需設定。

設定	描述
檔案名稱遮罩	用來篩選包含事件之檔案的遮罩。可接受下列萬用字元：「*」、「?」、「[...]」。 範例：*.json 必需設定。
密鑰	儲存用於連線到 SMB 伺服器之憑證的密鑰。支援 **憑證** 類型的密鑰。使用 NTLMv2 通訊協定進行身分驗證。 您可以選擇現有密鑰或建立新密鑰。若要建立新密鑰，請選擇**新建**。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立密鑰？** *若要建立密鑰：* 1. 在**名稱**欄位中，輸入密鑰的名稱。 2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。 3. 如有必要，在**描述**欄位中輸入密鑰的描述。 4. 點擊**建立**按鈕。 密鑰將會新增並顯示在**密鑰**下拉清單中。 必需設定。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。
緩衝區大小	用於在將事件傳送至伺服器RAM進行進一步處理或儲存之前，先在伺服器RAM中彙總事件的緩衝區大小（以位元組為單位）。該值必須為正整數。 最小值為 16。 最大值：67,108,864 (64 MB)。 預設緩衝區大小：1,048,576 (1 MB)；在介面中顯示為 **自動**。
服務處理數量。	服務可以同時執行以並行處理回應規則的事件處理器數量。 該值必須為不超過999的正整數。
輪詢間隔（毫秒）	連接器重新讀取目錄中檔案的間隔時間（以毫秒為單位）。預設值為`0`。使用此值，連接器會每隔 700 毫秒重新讀取目錄中的檔案。
字元編碼	從 SMB 伺服器接收的檔案的編碼。預設編碼為 UTF-8。 必需設定。

Nfs類型

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填） - 擁有該資源的租用戶名稱。
- **類型**（必要）— 連接器類型， **nfs** 。
- **URL**（必填）—遠端資料夾的路徑，格式為 nfs://host/path。
- **檔案名稱遮罩**（必填）— 用於篩選包含事件之檔案的遮罩。可使用遮罩"*"、"?"、"[...]"。

- **輪詢間隔，秒**— 輪詢間隔。在此時間間隔後從遠端系統重新讀取檔案。時間以秒為單位指定。預設值是0。
- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
- **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

vmware類型

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）- 擁有該資源的租用戶名稱。
- **類型**（必填）— 連接器類型，**vmware**。
- **URL**（必填）— VMware API可用的URL。URL必須包含主機和連接埠。只能指定一個URL。
- **VMware 憑據**（必填）— 儲存用於連線到VMware API的使用者名稱和密碼的密鑰。
- **用戶端逾時時間**是指在發出新請求之前，在請求未返回事件之後等待的時間。時間以秒為單位指定。預設值是 5 秒。如果指定為 0，則使用預設值。
- **最大事件數量**— 一次請求中從VMware API請求的事件數。預設值是100。最大值是1000。
- **開始時間戳記**— 您要從VMware API讀取事件的開始日期和時間。預設值是收集器啟動的時間。如果在收集器停止後啟動，則從上次儲存的日期開始讀取事件。

進階設定頁籤：

- **調試**— 一個切換開關，用於指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。
- **字元編碼**—指定字元編碼格式。預設值是UTF-8。
- **TLS模式** — 使用PEM x509格式憑證的TLS加密模式：
  - **停用**（預設）—不使用TLS加密。
  - **啟用**表示使用加密，但不驗證憑證。
  - **自訂CA** — 此選項要求您向收集器新增具有憑證的密鑰。非自簽署憑證。伺服器的憑證必須使用收集器設定中指定的憑證進行簽署。
- **自訂CA**（如果為TLS模式設定選擇了**自訂CA**，則必填）是儲存憑證的密鑰。

Wmi類型

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必填）- 連接器類型， **wmi** 。
  - **URL** （必填）- 正在建立的收集器 URL，例如： `kuma-collector.example.com:7221` 。

    使用Windows Management Instrumentation建立用於接收資料的收集器會自動建立一個代理程式，該代理程式在遠端裝置上接收必要的資料，並將這些資料轉發到收集器服務。您必須在**URL**中指定此收集器的位址。如果您已經知道計劃在哪台伺服器上安裝該服務，則可以事先知道URL。但是，也可以在安裝精靈完成後，透過從**資源→活動服務**部分複製URL資料來填寫此欄位。
  - **描述** — 資源描述：最多4,000個Unicode字元。
  - **預設憑據**— 無需選擇任何值的下拉清單。必須在**遠端主機**表中提供用於連接主機的帳戶憑據（請參閱下文）。
  - **遠端主機**表列出了您可以連線到的遠端Windows資產。可用直欄：
    - **主機**（必填）是要從中接收資料之裝置的IP位址或名稱。例如， `machine-1` 。
    - **網域**（必填）— 遠端裝置所屬網域的名稱。例如， `example.com` 。
    - **記錄類型**— 用於選擇需要檢索的Windows日誌名稱的下拉清單。預設情況下，清單中僅顯示預先設定的日誌，但您可以透過在**Windows日誌**欄位中輸入其名稱，然後按**ENTER鍵**，將自訂日誌新增至清單中。為了正確處理自訂日誌，KUMA服務和資源組態可能需要進行額外變更。

      預設可用的日誌包括：
      - 應用程式
      - 轉發的事件
      - 安全性
      - 系統
      - 硬體事件

如果WMI連線至少使用一個名稱不正確的日誌，則使用該連接器的代理程式不會接收來自此連線內所有日誌的事件，即使其他日誌的名稱指定正確。所有日誌名稱均指定正確的WMI代理連線將正常運作。

- **密鑰** — 用於存取具有讀取記錄權限的遠端Windows資產的帳戶憑據。如果將此欄位留空，則使用**預設憑據**下拉清單中所選的密鑰中的憑證。必須指定密鑰中的登入名稱而不指定網域。用於存取主機的域值取自**遠端主機**表的遠端主機直欄。

  您可以從下拉清單中選擇密鑰資源，或透過點選加號圖示 (+) 建立一個密鑰資源。可以透過點選鉛筆圖示 (✎) 來變更所選密鑰。

- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

從遠端裝置接收事件

從託管KUMA代理程式的遠端Windows裝置接收事件的條件：

- 要在遠端裝置上啟動KUMA代理程式，您必須使用具有**作為服務登入**權限的帳戶。
- 若要接收來自KUMA代理程式的事件，您必須使用具有事件日誌讀取器權限的帳戶。對於網域伺服器，可以建立一個這樣的使用者帳戶，以便使用群組政策將其讀取日誌的權限指派給網域中的所有伺服器和工作站。
- 必須在遠端Windows裝置上開啟TCP連接埠135、445和49152-65535。
- 您必須在遠端電腦上執行以下服務：
  - 遠端過程呼叫（RpcS）
  - RPC Endpoint Mapper (RpcEptMapper)

Wec類型

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型， **wec** 。
  - **URL**（必填）- 正在建立的收集器 URL，例如：`kuma-collector.example.com:7221`。

    建立使用Windows事件收集器接收資料的收集器會自動建立一個代理程式，該代理程式在遠端裝置上接收必要的資料並將該資料轉發到收集器服務。您必須在**URL**中指定此收集器的位址。如果您已經知道計劃在哪台伺服器上安裝該服務，則可以事先知道URL。但是，也可以在安裝精靈完成後，透過從**資源→活動服務**部分複製URL資料來填寫此欄位。
  - **描述** — 資源描述：最多4,000個Unicode字元。

- **Windows日誌**（必要）— 從此下拉清單中選擇要檢索的Windows日誌的名稱。預設情況下，清單中僅顯示預先設定的日誌，但您可以透過在**Windows日誌**欄位中輸入其名稱，然後按**ENTER鍵**，將自訂日誌新增至清單中。為了正確處理自訂日誌，KUMA服務和資源組態可能需要進行額外變更。

  預先設定的日誌：

  - 應用程式
  - 轉發的事件
  - 安全性
  - 系統
  - 硬體事件

  如果至少一個日誌的名稱指定不正確，則使用連接器的代理程式不會從任何日誌接收事件，即使其他日誌的名稱正確。

- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

若要在遠端裝置上啟動KUMA代理程式，必須使用具有「作為服務登入」權限的服務帳戶。若要從作業系統日誌接收事件，服務使用者帳戶也必須具有事件日誌讀取器的權限。

您可以建立一個具有「以服務身分登入」和「事件日誌讀取器」權限的使用者帳戶，然後使用群組原則擴充此帳戶的權限，以便將日誌讀取到網域中的所有伺服器和工作站。

我們建議您停用服務帳戶的互動式登入。

SNMP 類型

若要處理透過SNMP接收的事件，您必須使用json標準化器。

它適用於Windows和Linux代理程式。支援的協定版本：

- snmpV1
- snmpV2
- snmpV3

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。

- **類型**（必填）— 連接器類型，**snmp**。
- **SNMP 版本**（必填）— 此下拉清單可讓您選擇要使用的協定版本。
- **主機**（必填）— 主機名稱或其IP位址。可用格式：主機名稱、IPv4、IPv6。
- **連接埠**（必填）— 用於連線到主機的連接埠。通常使用161或162。

SNMP 版本、**主機**和**連接埠**設定定義與SNMP資源的一個連線。您可以透過點擊**SNMP 資源**按鈕新增連線，從而在一個連接器中建立多個這樣的連線。您可以透過點擊垃圾桶圖示（ ）來刪除連線。

- **密鑰**（必需）— 用於選擇密鑰的下拉列表，該密鑰用於儲存透過簡易網路管理通訊協定 (SNMP) 進行連接的憑據。密鑰類型必須與SNMP版本相符。如果需要，可以透過點擊加號圖示（ ）在連接器建立視窗中建立密鑰。可以透過點擊鉛筆圖示（ ）來變更所選密鑰。
- **來源資料** - 一個表格，您可以在其中指定接收資料的命名規則，並根據這些規則將OID（物件識別碼）轉換為標準化器可以互動的鍵。可用的表格直欄：
  - **參數名稱**（必填）— 資料類型的任意名稱。例如，`Site name`或`Site uptime`。
  - **OID**（必填）— 唯一識別碼，用於確定在事件來源中尋找所需資料的位置。例如，`1.3.6.1.2.1.1.5`。
  - **鍵**（必填）— 向資產傳送請求後，針對所請求設定值傳回的唯一識別碼。例如，`sysName`。在標準化資料時可以存取此鍵。
  - **MAC位址**— 如果啟用此功能，KUMA會正確解碼資料，其中OID包含OctetString格式的MAC位址資訊。解碼後， MAC位址將轉換為XX:XX:XX:XX:XX:XX格式的字串值。
- **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是`UTF-8`。
  - **偵錯**— 切換開關，可讓您指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。

SNMP 陷阱類型

snmp-trap連接器用於代理程式和收集器中，以被動接收SNMP陷阱訊息。連接器透過將SNMP物件ID對應到臨時鍵來接收並準備訊息以進行標準化。然後，訊息被傳遞給JSON標準化器，在那裡臨時鍵被對應到KUMA欄位並產生事件。

若要處理透過SNMP接收的事件，您必須使用json標準化器。

它適用於Windows和Linux代理程式。支援的協定版本：

- snmpV1
- snmpV2

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型， **snmp-trap**。
  - **SNMP 版本**（必填）— 在此下拉清單中，選擇要使用的協定版本：**snmpV1**或**snmpV2**。

    例如，Windows預設使用**snmpV2**版本。

  - **URL**（必填）– SNMP陷阱訊息的URL。可用格式：主機名稱:連接埠、IPv4:連接埠、IPv6:連接埠、:連接埠。

  SNMP 版本和**URL**參數定義了用於接收SNMP陷阱的連線。您可以透過點擊**SNMP 資源**按鈕新增連線，從而在一個連接器中建立多個這樣的連線。您可以透過點擊 ✕ 按鈕來刪除連線。

  - **來源資料**— 一個表，您可以在其中指定接收資料的命名規則，根據該規則，OID（物件識別碼）將轉換為標準化器可以互動的鍵。

    您可以按一下**套用 WinEventLog 的 OID**，以使用到達WinEventLog日誌的OID值的對應填入表。如果需要在傳入事件中確定並標準化更多資料，請在表中新增包含OID物件及其鍵的行。

    可用的表格直欄：

    - **參數名稱** — 資料類型的任意名稱。例如，`Site name`或`Site uptime`。
    - **OID**（必填）— 唯一識別碼，用於確定在事件來源中尋找所需資料的位置。例如，`1.3.6.1.2.1.1.1`。
    - **鍵**（必填）— 向資產傳送請求後，針對所請求設定值傳回的唯一識別碼。例如，`sysDescr`。在標準化資料時可以存取此鍵。
    - **MAC位址**— 如果啟用此功能，KUMA會正確解碼資料，其中OID包含OctetString格式的MAC位址資訊。解碼後， MAC位址將轉換為XX:XX:XX:XX:XX:XX格式的字串值。

    資料根據允許清單原則處理：表中未指定的物件不會傳送到標準化器進行進一步處理。

  - **描述** — 資源描述：最多4,000個Unicode字元。
- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是`UTF-8`。從俄文本地化版本 Windows 接收 snmp-trap 事件時，若事件中出現無效字元，建議將 snmp-trap 連接器的字元編碼變更為 Windows 1251。
  - **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

設定Windows的SNMP陷阱訊息來源

設定Windows裝置以將SNMP陷阱訊息傳送至KUMA收集器涉及下列步驟：

1. **設定和啟動SNMP和SNMP陷阱服務**
2. **設定事件到陷阱轉換器服務**

KUMA收集器必須接收來自SNMP陷阱訊息源的事件，它使用snmp陷阱類型的連接器和json標準化器。

設定和啟動SNMP和SNMP陷阱服務

若要在Windows 10中設定和啟動SNMP和SNMP陷阱服務：

1. 開啟**設定→應用程式應用程式和功能可選功能→新增功能→簡易網路管理通訊協定（SNMP）**，然後點擊**安裝**。
2. 等待安裝完成並重新啟動電腦。
3. 確保SNMP服務正在執行中。如果以下任何服務未執行，請啟用它們：
   - **服務→ SNMP服務**。
   - **服務→ SNMP陷阱**。
4. 右鍵點擊**服務→SNMP服務**，然後在快顯選單中選擇**內容**。指定下列設定：
   - 在**登入**標籤上，選取**本機系統帳戶**核取方塊。
   - 在**代理**索引標籤上，填寫**聯絡人**（例如，指定 `User-win10`）與「位置」（例如，指定 `detroit`）欄位。
   - 在**陷阱**頁籤上：
     - 在**社群名稱**欄位中，輸入**社群公用**，然後按一下**新增至清單** 。
     - 在**陷阱目標**欄位中，按一下**新增**，指定部署了等待SNMP事件的收集器的KUMA伺服器的IP位址或主機，然後按一下**新增** 。
   - 在**安全性**頁籤上：
     - 選取**傳送身份驗證陷阱**核取方塊。
     - 在**接受的社群名稱**表中，按一下**新增**，輸入**社群名稱公用**並將**讀寫**指定為**社群權限**。
     - 選取**接受來自任何主機的SNMP封包**核取方塊。
5. 點擊**套用**並確認您的選擇。
6. 右鍵點選**服務→ SNMP 服務**並選擇**重新啟動**。

若要在Windows XP中設定和啟動SNMP和SNMP陷阱服務：

1. 開啟**開始→主控台窗格→新增或移除程式→新增/刪除Windows元件→管理和監控工具→詳細資訊**。
2. 選擇**簡易網路管理通訊協定**和**WMI SNMP提供者**，然後按一下**確定→下一步**。
3. 等待安裝完成並重新啟動電腦。

4. 確保SNMP服務正在執行中。如果以下任何服務未執行，請透過將**啟動類型**設為**自動**來啟用它們：

   - **服務→ SNMP服務**。
   - **服務→ SNMP陷阱**。

5. 右鍵點擊**服務→SNMP服務**，然後在快顯選單中選擇**內容**。指定下列設定：

   - 在**登入**標籤上，選取**本機系統帳戶**核取方塊。
   - 在**代理**索引標籤上，填寫**聯絡人**（例如，指定 `User-win10`）與「位置」（例如，指定 `detroit`）欄位。
   - 在**陷阱**頁籤上：
     - 在**社群名稱**欄位中，輸入**社群公用**，然後按一下**新增至清單** 。
     - 在**陷阱目標**欄位中，按一下**新增**，指定部署了等待SNMP事件的收集器的KUMA伺服器的IP位址或主機，然後按一下**新增** 。
   - 在**安全性**頁籤上：
     - 選取**傳送身份驗證陷阱**核取方塊。
     - 在**接受的社群名稱**表中，按一下**新增**，輸入**社群名稱公用**並將**讀寫**指定為**社群權限**。
     - 選取**接受來自任何主機的SNMP封包**核取方塊。

6. 點擊**套用**並確認您的選擇。

7. 右鍵點選**服務→ SNMP 服務**並選擇**重新啟動**。

變更SNMP陷阱服務的連接埠

如有必要，您可以變更SNMP陷阱服務連接埠。

若要變更SNMP陷阱服務的連接埠：

1. 開啟C:\Windows\System32\drivers\etc資料夾。
2. 以管理員身分在記事本中開啟**服務**檔案。
3. 在檔案的**服務名稱**部分，指定為**SNMP陷阱**服務新增至KUMA收集器的snmp-trap連接器連接埠。
4. 儲存檔案。
5. 開啟主控台窗格並選擇**管理工具→服務**。
6. 右鍵點擊**SNMP服務**並選擇**重新啟動**。

設定事件到陷阱轉換器服務

若要設定將Windows事件轉換為SNMP陷阱訊息的事件到陷阱轉換器服務：

1. 在命令列中輸入 `evntwin`，然後按 **Enter** 鍵。
2. 在**組態類型**下，選擇**自訂**，然後按一下**編輯**按鈕。
3. 在**事件來源**設定群組中，按一下**新增**按鈕以尋找並新增要傳送至安裝了SNMP陷阱連接器的KUMA收集器的事件。
4. 點選**設定**按鈕，在開啟的視窗中，選取**不套用節流**核取方塊，然後點選**確定**。
5. 點擊**套用**並確認您的選擇。

elastic類型

保證支援Elasticsearch 7.0.0。

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填）- 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型，**elastic**。
  - **URL**（必填）— Elasticsearch伺服器的有效URL。
  - **Elastic 憑據**（必填）是一個下拉清單，您可以在其中選擇儲存用於連線到Elasticsearch伺服器的憑據的密鑰。
  - **Elastic 指紋** — 用於選取祕密的下拉式清單，其中存放兩類祕密：用於連線到 Elasticsearch 伺服器的 `fingerprint` 類型祕密，以及用於使用 CA 憑證的 `certificate` 類型祕密。
  - **索引**（必填）— Elasticsearch中的索引名稱。
  - **查詢**（必填）— 用於 Elasticsearch 的查詢。建議在查詢中指定 `size` 參數，以防止 KUMA 與 Elasticsearch 出現效能問題。

    查詢範例：

    ```
    "query" : { "match_all" : {} },"size" : 25
    ```
  - **排序**（必填）— 排序順序。可能的值：asc、desc.
  - **輪詢間隔（秒）** — 如果上一次查詢未傳回任何事件，則向Elasticsearch伺服器發出查詢的間隔（以秒為單位）。如果請求時Elasticsearch包含事件，則連接器將接收事件，直到從Elasticsearch接收到所有可用事件為止。
  - **描述** — 資源描述：最多4,000個Unicode字元。

- **進階設定**頁籤：
  - **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
  - **偵錯**— 可讓您指定是否必須啟用資源日誌記錄的切換開關。預設情況下，此切換開關處於**已停用**位置。

etw類型

建立此類連接器時，需要定義以下設定的值：

- **基本設定**頁籤：
  - **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
  - **租用戶**（必填） - 擁有該資源的租用戶名稱。
  - **類型**（必填）— 連接器類型，**etw**。
  - **URL**（必填）—DNS伺服器的有效URL。
  - **工作階段名稱**（必填）—您只能指定一個會話名稱，該名稱對應於 Microsoft-Windows-DNSServer ETW提供者{EB79061A-A566-4698-9119-3ED2807060E7}。
  - **擷取事件資訊** - 如果切換開關關閉，則會提取無需從磁碟下載協力廠商元資料即可擷取的最小事件資訊集。這種方法有助於節省執行代理程式的電腦上的CPU資源。預設情況下，將擷取有關該事件的所有資料。
  - **擷取事件內容**— 如果此開關關閉，則不會擷取事件內容，這有助於節省執行代理程式的電腦上的CPU使用率。預設情況下，會擷取事件內容。只有在**擷取事件內容**開關開啟時，才能使用**擷取事件資訊**開關。
  - **描述** — 資源描述：最多4,000個Unicode字元。
- **進階設定**頁籤：
  - **調試**— 一個切換開關，用於指定是否必須啟用資源日誌記錄。預設情況下，此切換開關處於**已停用**位置。
  - **字元編碼**— 用於指定來源編碼（UTF-8）。我們建議僅當標準化事件的欄位中顯示亂碼時才編輯此設定。預設情況下，不指定值。
  - **TLS模式** — 使用PEM x509格式憑證的TLS加密模式：
    - **停用**（預設）— 不使用TLS加密。
    - **啟用**— 使用加密但不進行憑證驗證。
    - **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA的根憑證和金鑰在程式安裝期間自動創建，並儲存在KUMA Core伺服器的資料夾/opt/kaspersky/kuma/core/certificates/中。
  - **壓縮**- 您可以使用Snappy壓縮。預設情況下，壓縮是停用的。

universalAPI類型

universalAPI類型的連接器用於從任何支援JSON回應的REST API接收資料。

這種連接器類型僅適用於可透過使用者介面進行設定的REST API。這些連接器始終使用**JSON**規範化器。一個連接器只能建立一個連線。一個連線只能設定一個URL。

universalAPI連接器僅支援包含一個巢狀層級的JSON結構中收集事件。如果回應結構包含巢狀清單（例如，一個物件清單，其中每個物件包含另一個物件清單），則連接器不支援從此類清單中收集事件。在這種情況下，我們建議收集頂層資料並在規範化器層級處理巢狀結構。

執行收集器後，您可以透過分析其日誌來測試與來源的連線。如果連線出現問題或有授權問題，收集器將在**資源和服務→活動服務**部分以黃色狀態顯示。

> **universalAPI**連接器不會取代其他現有的API連接器，例如**office365**。

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**— 資源的唯一名稱。名稱的最大長度：128個Unicode字元。必需設定。
- **租用戶**— 擁有資源的租用戶的名稱。必需設定。
- **類型**—連接器的類型，**universalAPI** 。必需設定。
- **標籤**—用于資源搜尋。
- **描述**— 資源的描述。描述的最大長度為4000個Unicode字元。
- REST API伺服器的**URL**。您無需指定連線協定（http或https）。系統會根據tlsMode設定自動推斷。您只能指定一個URL。必需設定。
- 指定URL的**請求間隔（秒）**。輸入60到3600之間的數字（即1分鐘到60分鐘）。預設值是 3600。
- 用於API請求的**HTTP 方法**。可用值：
  - **GET**
  - **POST**
  - **PUT**
  - **DELETE**

  必需設定。
- 用於連線到API的**授權**方法。以下授權方法可用：
  - **已停用**。無需授權。
  - **Plain**。登入名稱和密碼授權。您需要使用**憑據**類型的金鑰。
  - **權杖**。權杖授權。您需要使用**權杖**類型的密鑰。

  如需詳細資訊，請參閱金鑰一節。
  預設值是**已停用**。

如果在**進階設定**頁籤中，**TLS模式**欄位設定為**自訂PFX**，則**授權**欄位不可用。

- 如果**密鑰 ID**欄位設定為**授權**，則**Plain**欄位可用。您需要選取**憑據**類型的金鑰。必需設定。
- 如果**授權**欄位設定為授權，則**權杖**欄位可用。您需要選取**權杖**類型的密鑰。必需設定。
- 如果**權杖名稱**欄位設定為**權杖**，則**授權**欄位可用。可用值：
  - **Bearer**
  - **OAuth**

  您也可以手動指定名稱。必需設定。
- **查詢正文**是HTTP請求的正文。您也可以使用變數：`$token`、`$username`、`$password`、`$identityValue`。如果啟用了迭代功能，並且狀態具有迭代金鑰，則會自動將其取代到請求參數中。
- **JSONPath 格式的資料路徑**是指API回應結構中指向物件或物件清單的資料路徑。路徑以JSONPath格式指定（例如，`$.data`、`$.data.edges[0].node.event`、`$.data.edges[*].node.event`）。`$`字元會自動替換到欄位中，您無需輸入。必需設定。
- **識別欄位**切換開關啟用了選擇事件的唯一ID。預設情況下，切換開關是關閉的。
- 如果選取**JSONPath 格式的欄位路徑**核取方塊，則**識別欄位**可用。API回應元素結構中ID欄位的路徑以JSONPath格式指定（例如，`$.id`）。`$`字元會自動替換到欄位中，您無需輸入。必需設定。
- 如果啟用了**識別欄位**切換開關，則識別欄位欄位可用。選擇事件的ID欄位的類型。可用值：
  - **int**
  - **float**
  - **字串**
  - **date**

  在內部，該值以毫秒為單位儲存為時間戳記。必需設定。
- 如果**類型**欄位設定為**日期格式**，則**date**欄位可用。日期格式可以包括日期、時間、秒的小數部分和時區，例如：`YYYY-MM-DDTHH:mm:ssX`。使用指定的格式：
  - 用於解析ID的初始值。
  - 用於解析REST API回應中的ID值。如果日期格式包含時區，則以指定的時區處理該值。如果日期格式不包含時區，則以UTC時間處理該值。
  - 用於產生查詢參數的日期字串（例如，`queryParams`、`headers`、`body` 中的 `$identityValue`）。如果日期格式包含時區，則字串將以伺服器的時區產生。如果日期格式不包含時區，則字串將以UTC時間產生。
- 如果啟用了**初始值**切換開關，則**識別欄位**欄位可用。識別種子以字串形式指定，其格式與所選**類型**相對應。對於**date**類型，您需要以**日期格式**欄位中指定的格式指定值。此值可以包含Unicode字元。最小長度為1個字元。
- **迭代參數**切換開關啟用用於具有分階段資料輸出的API的迭代模式。預設情況下，切換開關是關閉的。

- **JSONPath 格式的迭代索引鍵欄位路徑**是API回應元素結構中迭代金鑰欄位的JSONPath格式路徑。`$`字元會自動插入到欄位中。必需設定。

- **迭代模式下的請求間隔（秒）**是指迭代模式下的URL輪詢間隔，單位為秒。預設值是 `60`。

- **迭代索引鍵的 URL 參數**是指向API發出請求時傳遞迭代金鑰的URL參數名稱。

- **可選查詢參數**是`map[string][]string`格式的附加請求參數。您也可以使用變數：`$token`、`$username`、`$password`、`$identityValue`。若要新增參數，請按一下**+新增**按鈕，然後填寫**金鑰**和**值**欄位。若要刪除參數，請選取其旁邊的核取方塊，然後按一下**刪除**。

- **查詢標頭**是`map[string][]string`格式的可選HTTP請求標頭。您也可以使用變數：`$token`、`$username`、`$password`、`$identityValue`。若要新增參數，請按一下**+新增**按鈕，然後填寫**金鑰**和**值**欄位。若要刪除參數，請選取其旁邊的核取方塊，然後按一下**刪除**。

- **其他欄位**是以`map[string][]string`格式新增到每個資料元素的欄位。若要新增欄位，請按一下**+新增**按鈕，然後填入**欄位名稱**和**JSONPath**欄位。若要刪除欄位，請選取其旁邊的核取方塊，然後按一下**刪除**。

進階設定頁籤：

- **偵錯**切換開關為連接器啟用了偵錯模式。預設情況下，切換開關是關閉的。

- **字元編碼**。預設值是**UTF-8**。

- **代理**指定連線到API時所需的代理伺服器設定（如果需要）。您可以選擇可用的代理伺服器之一或建立一個新的代理伺服器。

- **TLS模式**。使用TLS加密時，您無法在基本設定**基本設定URL**欄位中指定IP位址。可用值：

  - **停用**表示不使用TLS加密。預設選擇該值。

  - **啟用**表示使用加密，但憑證未經驗證。

  - **自訂CA**啟用TLS加密，並驗證由憑證授權單位簽署的憑證。如果選擇此值，請在**自訂CA**下拉清單中，指定由憑證授權單位簽署的憑證所對應的密鑰。您可以選擇現有密鑰或建立新密鑰。若要建立新密鑰，請選擇**新建**。

    若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。

    如何建立由憑證授權單位簽署的憑證？

    您可以在KUMA Core伺服器上建立CA簽署的憑證（以下命令範例使用OpenSSL）。

    若要建立由憑證授權單位簽署的憑證：

    1. 產生憑證授權單位要使用的金鑰，例如：

       ```
       openssl genrsa -out ca.key 2048
       ```

    2. 為產生的金鑰建立憑證，例如：

       ```
       openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<憑證授權單位的通用主機名稱>" -out ca.crt
       ```

    3. 建立私鑰並要求憑證授權單位對其進行簽署，例如：

       ```
       openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<KUMA 伺服器的通用主機名稱>" -out server.csr
       ```

4. 建立由憑證授權單位簽署的憑證。您需在 `subjectAltName` 變數中包含為其建立憑證之伺服器的網域名稱或 IP 位址，例如：

   ```
   openssl x509 -req -extfile <(printf
   "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in
   server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
   ```

5. 在 Open Single Management Platform 網頁介面中，將建立的 `server.crt` 憑證上傳至 **憑證** 類型的機密項目，然後在 **自訂 CA** 下拉式清單中選取該 **憑證** 類型的機密項目。

- **自訂 PFX**可使用 PFX 密鑰啟用 TLS 加密。您必須產生一個含有私密金鑰且採用 PKCS#12 容器格式的 PFX 憑證，然後將該 PFX 憑證作為 PFX 密鑰上傳至 OSMP 主控台。如果選擇此值，請在**自訂PFX**下拉清單中指定由憑證授權單位簽署的憑證的PFX密鑰。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇**新建**。

  若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。

  如何建立PFX密鑰？

  若要建立PFX密鑰：

  1. 在**名稱**欄位中，輸入PFX密鑰的名稱。
  2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。
  3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。
  4. 按一下**建立**按鈕。

     PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。

- **請求逾時時間（秒）**是指等待API請求回應的時間，以秒為單位。預設回應逾時時間為30秒。
- **請求重試次數**是指發生錯誤時重複嘗試發出請求的次數。預設值是 `1`。
- **重試間隔（秒）**是指請求重試之間的間隔，以秒為單位。預設值是 `0`。

promtail類型

Promtail連接器用於從OSMP元件傳輸稽核事件。

建立此類連接器時，需要定義以下設定的值：

基本設定頁籤：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）- 擁有該資源的租用戶名稱。
- **類型**（必填）— 連接器類型，promtail。

- **URL**（必填）—您需要連線的URL。可用格式：主機名稱:連接埠、IPv4:連接埠、IPv6:連接埠、:連接埠。

  您可以以下列格式指定IPv6位址：`[<IPv6 address>%<interface>:<port number>`，例如`[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。您可以新增多個URL或刪除URL。如果URL欄位包含製表符或空格，KUMA不允許儲存資源或服務。若要新增URL，請按一下**+ 新增**按鈕。若要刪除URL，請按一下其旁邊的刪除 × 圖示。

- **描述** — 資源描述：最多4,000個Unicode字元。

進階設定頁籤：

- **調試**— 一個切換開關，用於指定是否必須啟用資源日誌記錄。預設情況下，切換開關是關閉的。
- **字元編碼** 設定可指定字元編碼。預設值是UTF-8。
- **TLS模式** — 使用PEM x509格式憑證的TLS加密模式：
  - **停用**（預設）—不使用TLS加密。
  - **啟用**— 使用加密但不進行憑證驗證。
  - **使用驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA的根憑證和金鑰在程式安裝期間自動建立，並儲存在KUMA Core伺服器的資料夾/opt/kaspersky/kuma/core/certificates/中。
  - **自訂PFX** — 使用加密。選擇此選項後，必須在外部憑證授權單位中使用PKCS#12容器格式的私鑰產生憑證。然後，必須將憑證從金鑰庫匯出，並將其作為PFX密鑰上傳到KUMA主控台。**新增PFX密鑰**。

    若要建立PFX密鑰：

    1. 在**名稱**欄位中，輸入PFX密鑰的名稱。
    2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。
    3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。
    4. 按一下**建立**按鈕。

    PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。

    使用TLS時，無法將IP位址指定為URL。
  - **具有用戶端身分驗證的自訂PFX**是指使用PFX金鑰進行TLS加密。在此模式下，用戶端將使用憑證進行身份驗證。

    您必須使用PKCS#12容器格式的私鑰生成PFX憑證，然後將PFX憑證作為PFX密鑰上傳到KUMA網頁介面。如果選擇此值，請在「PFX密鑰」下拉清單中指定一個由憑證授權單位簽署的PFX憑證。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇**新建**。

    若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。

http-streaming 類型

http-streaming 類型的連接器用於在搭配 Windows 和 Linux 代理運作時，透過 HTTP 接收事件。

連接器接受 HTTP 請求，並依下列方式處理請求主體：讀取請求主體（並視需要解壓縮）、將主體分割成事件，再逐一傳送事件進行處理。這種處理方式有助於減少記憶體用量，但當事件來自少數來源且密集度很高時，連接器的效能可能會降低。

http-streaming 類型連接器的設定如下表所述。

基本設定頁籤

設定	描述
名稱	連接器的唯一名稱。名稱的長度上限為 128 個 Unicode 字元。 必需設定。
租用戶	擁有連接器的租用戶名稱。 必需設定。
類型	連接器類型：**http-streaming**。 必需設定。
標記	用於搜尋連接器的標記。 可選設定。
URL	URL（必需）—您需要連線的 URL。您可以按以下格式之一輸入URL： • < 主機名稱 >:< 連接埠號碼 > • < IPv4 位址 >:< 連接埠號碼 > • < IPv6 位址 >:< 連接埠號碼 > 若要將事件來源中的資料傳送到連接器，指定的URL必須以`/input`結尾。 必需設定。
分隔符號	標記事件之間邊界的字元： • **\n** • **\t** • **\0** 如果您未在此下拉清單中選擇值，則預設選擇空值。在這種情況下，連接器不會將一個事件拆分成多個事件，而是原封不動地將其傳遞給規範化器。
緩衝區大小	設定單一事件的大小上限（以位元組為單位）。事件大小上限為 1 位元組。 如果 HTTP 要求本文中沒有分隔符號，則整個要求本文會被視為一個事件。在這種情況下，緩衝區大小必須大於要求本文的大小。 我們建議根據最大事件的大小（而非一批事件的大小）設定緩衝區大小，並保留至少 2 位元組的安全餘裕。 預設值：4096 位元組（4 KB）。最大值：67108864 位元組（64 MB）。 如果設定為 0，則使用預設值。
描述	連接器的描述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
偵錯	此切換開關可啟用或停用資源的記錄功能。預設情況下，切換開關是關閉的。
字元編碼	字符編碼。預設值是UTF-8。

設定	描述
TLS模式	TLS加密模式。使用TLS加密時，您無法在**基本設定**的基本設定欄位中指定IP位址。可用值： • **停用**表示不使用TLS加密。預設選擇該值。 • **啟用**表示使用加密，但憑證未經驗證。 • **自訂 PFX**是指使用PFX密鑰進行TLS加密。您必須使用PKCS#12容器格式的私鑰生成PFX憑證，然後將PFX憑證作為PFX密鑰上傳到KUMA網頁介面。如果您選擇此值，請在**使用用戶端驗證的自訂PFX**下拉式清單中，指定包含由憑證授權單位簽署之憑證的PFX密鑰。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇**新建**。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立PFX密鑰？** *若要建立PFX密鑰：* 1. 在**名稱**欄位中，輸入PFX密鑰的名稱。 2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。 3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。 4. 按一下**建立**按鈕。 PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。 • **具有用戶端身分驗證的自訂PFX**是指使用PFX金鑰進行TLS加密。在此模式下，用戶端將使用憑證進行身份驗證。 您必須使用PKCS#12容器格式的私鑰生成PFX憑證，然後將PFX憑證作為PFX密鑰上傳到KUMA網頁介面。如果您選擇此值，請在**使用用戶端驗證的自訂PFX**下拉式清單中，指定包含由憑證授權單位簽署之憑證的PFX密鑰。您可以選擇現有的PFX密鑰或建立新的PFX密鑰。若要建立新的PFX密鑰，請選擇**新建**。 若要編輯現有密鑰的設定，請點選其旁邊的鉛筆圖示。 **如何建立PFX密鑰？** *若要建立PFX密鑰：* 1. 在**名稱**欄位中，輸入PFX密鑰的名稱。 2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。 3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。 4. 按一下**建立**按鈕。 PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。
佇列中的傳入請求數量	連接器可同時處理的 HTTP 請求數上限。 達到指定的限制時，新的 HTTP 請求會遭到拒絕，並傳回代碼 `429 Too Many Requests`。遭拒絕的請求本文不會被處理。 實際同時處理的請求數量取決於此設定的值，以及收集器上透過**工作程序**設定所指定的工作程序數量。 預設值是 32768。最大值是65535。 如果設定為 0，則使用預設值。 增加此值可同時處理更多請求，但可能會增加記憶體使用量。

預定義連接器

下表所列的連接器包含在OSMP分發套件中。

預定義連接器

連接器名稱	註解
[OOTB] Continent SQL	從Continent硬體和軟體加密系統的資料庫中取得事件。 要使用它，您必須設定相應密鑰類型的設定。
[OOTB] InfoWatch Trafic Monitor SQL	從InfoWatch Traffic Monitor系統的資料庫中取得事件。 要使用它，您必須設定對應密鑰類型的設定。
[OOTB] KSC MSSQL	從卡巴斯基安全管理中心應用程式的MS SQL資料庫中取得事件。 要使用它，您必須設定對應密鑰類型的設定。
[OOTB] KSC MySQL	從卡巴斯基安全管理中心應用程式的MySQL資料庫中取得事件。 要使用它，您必須設定對應密鑰類型的設定。

[OOTB] KSC PostgreSQL	從卡巴斯基安全管理中心15.0應用程式的PostgreSQL資料庫中取得事件。 要使用它，您必須設定對應密鑰類型的設定。
[OOTB] Oracle Audit Trail SQL	從Oracle資料庫取得稽核事件。 要使用它，您必須設定對應密鑰類型的設定。
[OOTB] SecretNet SQL	從SecretNet SQL資料庫中取得事件。 要使用它，您必須設定對應密鑰類型的設定。

目標

目標定義了用於傳送標準化事件的網路設定。收集器和管理器使用目標來描述將已處理事件傳送到的位置。通常，目標點是關聯器和儲存體。

目標的設定在兩個頁籤上設定：**基本設定**和**進階設定**。可用的設定取決於所選的目標類型：

- **內部** — 用於使用「內部」協定從KUMA服務接收資料。
- **nats-jetstream** — 用於NATS通訊。
- **tcp** — 用於TCP通訊。
- **udp** — 用於透過UDP通訊。
- **http** —用於HTTP通訊。
- **二極體** —用於使用資料二極體傳輸事件。
- **kafka** — 用於Kafka通訊。
- **檔案** — 用於寫入檔案。
- **儲存體** — 用於將資料傳輸到儲存體。
- **關聯器** — 用於將資料傳輸到關聯器。
- **事件路由器** — 用於將事件傳送至事件路由器。

目標，內部類型

內部類型的目標用於透過「內部」協定接收來自 KUMA 服務的資料。您可以使用內部協定傳輸以下資料：

- 內部資料，例如事件路由。
- 檔案屬性。如果您在建立收集器期間，於安裝的傳輸步驟指定了檔案類型的連接器、1c-xml或1c-log，則可在事件剖析步驟的**對應**表格中，使用 KUMA 事件欄位傳遞收集器所處理檔案的名稱或其路徑。為此，請在**來源**直欄中，指定下列值之一：
  - `$kuma_fileSourceName` 表示在 KUMA 事件欄位中傳遞正由收集器處理的檔案名稱。
  - `$kuma_fileSourcePath` 表示在 KUMA 事件欄位中傳遞正由收集器處理的檔案路徑。

當您使用**檔案**、**1c-xml**或**1c-log**連接器時，標準化器中的新變數僅適用於**內部類型的目標**。

- 事件傳送到事件路由器。事件路由器只能透過「內部」協定接收事件，因此在向事件路由器傳送事件時，您只能使用**內部**目標。

下表描述了**內部**類型目標的設定。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
州	此切換開關用於啟用向目標傳送事件的功能。此切換開關預設為開啟。
類型	目標類型：**內部**。 必需設定。
網址	URL（必填）—您需要連線的 URL。現支援以下URL格式： • `<` 主機名稱 `>:<` 連接埠號碼 `>` • `< IPv4` 位址 `>:<` 連接埠號碼 `>` • `< IPv6` 位址 `>:<` 連接埠號碼 `>` 您可以使用以下格式指定 IPv6 位址：`[< IPv6` 位址 `>%<` 介面 `>:<` 連接埠號碼 `>`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以新增多個 URL，也可以移除 URL。如果URL欄位包含製表符或空格，KUMA不允許儲存資源或服務。若要新增URL，請按一下**+ 新增**按鈕。若要刪除URL，請按一下其旁邊的刪除✕圖示。 必需設定。
標記	資源搜尋標籤。 可選設定。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
緩衝區大小	用於在將事件傳送至伺服器RAM進行進一步處理或儲存之前，先在伺服器RAM中彙總事件的緩衝區大小（以位元組為單位）。該值必須為正整數。預設緩衝區大小：67,108,864（64MB），在介面中顯示為0。
緩衝區排清間隔	向目標傳送事件的間隔（以秒為單位）。預設值為1秒。
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。預設值：10GB，在介面中顯示為0。
事件處理器	服務可以同時執行以並行處理回應規則的事件處理器數量。 該值必須為不超過999的正整數。
代理伺服器	目標的代理伺服器。您可以選擇現有代理伺服器或建立新的代理伺服器。若要建立新的代理伺服器，請選擇**新建**。 如果要編輯現有代理伺服器的設定，請點選其旁邊的鉛筆🖉圖示。

設定	描述
URL選擇政策	如果您在**基本設定**頁籤的基本設定欄位中新增了多個URL，則此方法用於確定事件必須先傳送到哪些URL： • **任意**表示只要URL接受事件，事件就會傳送到隨機選擇的可用URL。如果該URL不可用，則事件會傳送到另一個隨機選擇的可用URL。預設選擇該值。 • **優先**表示事件會傳送到第一個新增的URL。如果該URL不可用，則事件會傳送到下一個已新增的可用URL。如果第一個新增的URL再次可用，則事件會再次傳送到第一個新增的URL。 • **輪詢**表示事件會在可用URL之間均勻分配。此方法無法保證事件在URL之間均勻分配，因為緩衝區可能會溢位或事件可能會傳送到目標位置。您可以在**緩衝區大小限制**欄位中以位元組為單位指定緩衝區大小；您也可以在**緩衝區重新整理間隔**欄位中以秒為單位指定向目標位置傳送事件的間隔。
健康檢查超時	檢查目標執行狀況的間隔（以秒為單位）。
磁碟緩衝區已停用	此切換開關用於啟用磁碟緩衝區。切換開關預設為開啟。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。您可以在**磁碟緩衝區大小限制**欄位中指定磁碟緩衝區的大小。如果磁碟緩衝區空間不足，新的標準化事件將覆蓋舊的標準化事件，從最早的事件開始。
逾時時間	目標等待其他服務或元件回應的時間（以秒為單位）。
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。

設定	描述
篩選器	用於決定資源必須處理哪些事件的篩選器。您可以選擇現有篩選條件或建立新篩選條件。若要建立新篩選器，請選擇**新建**。 若要編輯現有篩選器的設定，請點選其旁邊的鉛筆圖示。 **如何建立篩選器？** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

設定	描述

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

Nats-jetstream 類型

nats-jetstream類型用於NATS通訊。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型，**nats-jetstream**。
URL	必需設定。 要連線的URL。
主題	必需設定。 NATS訊息的主題。必須包含Unicode字元。
分隔符號	指定一個用於界定一個事件結束而另一個事件開始的字元。預設使用 \n。

設定	描述
授權	連線到指定URL時的授權類型可能的值： • 預設值是**停用**。 • **純文字**：如果選擇此選項，則必須指示包含使用者帳戶憑證的密鑰，以便在連線到連接器時進行授權。 **新增密鑰** *若要建立密鑰：* 1. 在**名稱**欄位中，輸入密鑰的名稱。 2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。 3. 如有必要，在**描述**欄位中輸入密鑰的描述。 4. 按一下**建立**按鈕。 密鑰將會新增並顯示在**密鑰**下拉清單中。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
壓縮	您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。
叢集 ID	NATS叢集的ID。
輸出格式	將事件傳送到外部目標的格式。可用值： • JSON • CEF 如果選擇CEF格式，則傳送的事件包含CEF標頭和僅非空白欄位。

設定	描述

TLS模式	使用TLS加密。可用值：
	• **已停用** (預設) 表示不使用 TLS 加密。
	• **啟用**表示使用加密，但不驗證憑證。
	• **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA 的根憑證和金鑰會在程式安裝期間自動建立，並儲存在 KUMA Core 伺服器的 /opt/kaspersky/kuma/core/certificates/ 資料夾中。
	• **自訂CA**表示使用加密並驗證憑證是否由憑證授權單位簽署。包含憑證的密鑰可從**自訂CA**下拉清單中選擇，選擇此選項後會顯示該清單。
	建立由憑證授權單位簽署的憑證。
	您可以在KUMA Core伺服器上建立CA簽署的憑證（以下命令範例使用OpenSSL）。
	若要建立由憑證授權單位簽署的憑證：
	1. 產生憑證授權單位要使用的金鑰，例如：
	`openssl genrsa -out ca.key 2048`
	2. 為產生的金鑰建立憑證，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 憑證授權單位的通用主機名稱 >" -out ca.crt`
	3. 建立私鑰並要求憑證授權單位對其進行簽署，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 伺服器的通用主機名稱 >" -out server.csr`
	4. 建立由憑證授權單位簽署的憑證。您需在 `subjectAltName` 變數中包含為其建立憑證之伺服器的網域名稱或 IP 位址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform 網頁介面中，將建立的 `server.crt` 憑證上傳至 **憑證** 類型的機密項目，然後在 **自訂 CA** 下拉式清單中選取該 **憑證** 類型的機密項目。
	使用TLS時，無法將IP位址指定為URL。

分隔符號	在下拉式清單中，可選取字元來標記事件之間的邊界。預設使用 `\n`。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在**篩選器**部分，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

Tcp類型

tcp類型用於TCP通訊。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型， **tcp** 。
URL	必需設定。 要連線的URL。可用格式： `host:port` 、 `IPv4:port` 、 `:port` 。 IPv6 位址也受支援。使用 IPv6 位址時，還必須以 `[address%interface]:port` 格式指定介面。 例如， `[fe80::5054:ff:fe4d:ba0c%eth0]:4222` ）。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
壓縮	您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。
逾時時間	等待來自另一個服務或元件的回應時間（以秒為單位）。 預設值為 `30` 。
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。

設定	描述
輸出格式	將事件傳送到外部目標的格式。可用值： • JSON • CEF 如果選擇CEF格式，則傳送的事件包含CEF標頭和僅非空白欄位。
TLS模式	使用pem x509格式的憑證的TLS加密模式。可用值： • **停用**表示不使用TLS加密。預設值。 • **啟用**– 使用加密但不進行憑證驗證。 • **自訂CA**表示使用加密，並驗證您提供的憑證檔案。選擇此值後，將顯示**自訂CA**附加參數。使用此參數指定憑證。 • **自訂PFX**表示使用加密，並驗證您提供的PFX格式憑證。選擇此值後，將顯示**PFX金鑰**附加參數。使用此參數指定憑證。 使用TLS時，無法將IP位址指定為URL。
自訂CA	此欄位可讓您選擇包含憑證檔案的憑證類型金鑰。您可以選擇現有密鑰或新建密鑰。若要建立新金鑰，請選擇**建立**值，然後在開啟的視窗中上傳TLS憑證檔案。
新增PFX密鑰	此欄位可讓您選擇包含憑證檔案的PFX類型金鑰。您可以選擇現有密鑰或新建密鑰。若要建立新金鑰，請選擇**建立**值，然後在開啟的視窗中上傳包含TLS憑證的 PFX 檔案。
分隔符號	在下拉式清單中，可選取字元來標記事件之間的邊界。預設使用 `\n`。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在此部分中，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

udp類型

udp類型的目標用於UDP通訊。下表描述了**udp**類型目標的設定。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
州	此切換開關用於啟用向目標傳送事件的功能。此切換開關預設為開啟。
類型	目標類型：**udp**。 必需設定。
網址	URL（必填）—您需要連線的 URL。現支援以下URL格式： • `< 主機名稱 >:< 連接埠號碼 >` • `< IPv4 位址 >:< 連接埠號碼 >` • `< IPv6 位址 >:< 連接埠號碼 >` 您可以使用以下格式指定 IPv6 位址：`[< IPv6 位址 >%< 介面 >:< 連接埠號碼 >`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以新增多個 URL，也可以移除 URL。如果**URL**欄位包含製表符或空格，則無法儲存資源或服務。若要新增URL，請按一下**+ 新增**按鈕。若要刪除URL，請按一下其旁邊的刪除✕圖示。 必需設定。
標記	資源搜尋標籤。 可選設定。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
緩衝區大小	用於在將事件傳送至伺服器RAM進行進一步處理或儲存之前，先在伺服器RAM中彙總事件的緩衝區大小（以位元組為單位）。該值必須為正整數。預設緩衝區大小：67,108,864（64MB），在介面中顯示為0。
緩衝區排清間隔	向目標傳送事件的間隔（以秒為單位）。預設值為1秒。

設定	描述
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。預設值：10GB，在介面中顯示為0。
事件處理器	服務可以同時執行以並行處理回應規則的事件處理器數量。 該值必須為不超過999的正整數。
輸出格式	事件傳送到目標的格式： • **JSON**。 • **CEF**。如果選擇該值，則傳送的事件包含CEF標頭和僅非空白欄位。 • **Syslog-CEF**
TLS模式	TLS加密模式。使用TLS加密時，您無法在基本設定**基本設定URL**欄位中指定IP位址。可用值： • **停用**表示不使用TLS加密。預設選擇該值。 • **啟用**表示使用加密，但憑證未經驗證。 • **使用驗證**表示使用加密並驗證憑證是否使用KUMA根憑證簽署。KUMA的根憑證和金鑰在程式安裝期間自動建立，並儲存在KUMA Core伺服器的目錄/opt/kaspersky/kuma/core/certificates/中。 過時的加密模式，已棄用。
壓縮	用於設定Snappy壓縮的下拉清單： • **已停用**。預設選擇該值。 • **使用Snappy**。
URL選擇政策	如果您在**基本設定**頁籤的基本設定欄位中新增了多個URL，則此方法用於確定事件必須先傳送到哪些URL： • **任意**表示只要URL接受事件，事件就會傳送到隨機選擇的可用URL。如果該URL不可用，則事件會傳送到另一個隨機選擇的可用URL。預設選擇該值。 • **優先**表示事件會傳送到第一個新增的URL。如果該URL不可用，則事件會傳送到下一個已新增的可用URL。如果第一個新增的URL再次可用，則事件會再次傳送到第一個新增的URL。 • **輪詢**表示事件會在可用URL之間均勻分配。此方法無法保證事件在URL之間均勻分配，因為緩衝區可能會溢位或事件可能會傳送到目標位置。您可以在**緩衝區大小限制**欄位中以位元組為單位指定緩衝區大小；您也可以在**緩衝區重新整理間隔**欄位中以秒為單位指定向目標位置傳送事件的間隔。
分隔符號	標記事件之間邊界的字元： • **\n** • **\t** • **\0** 如果您未在此下拉清單中選擇值，則預設選擇空值。在這種情況下，連接器不會將一個事件拆分成多個事件，而是原封不動地將其傳遞給規範化器。
磁碟緩衝區已停用	此切換開關用於啟用磁碟緩衝區。切換開關預設為開啟。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。您可以在**磁碟緩衝區大小限制**欄位中指定磁碟緩衝區的大小。如果磁碟緩衝區空間不足，新的標準化事件將覆蓋舊的標準化事件，從最早的事件開始。
逾時時間	目標等待其他服務或元件回應的時間（以秒為單位）。
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。

設定	描述
篩選器	用於決定資源必須處理哪些事件的篩選器。您可以選擇現有的篩選器或建立新的篩選器。若要建立新篩選器，請選擇**新建**。 若要編輯現有篩選器的設定，請點選其旁邊的鉛筆圖示。 **如何建立篩選器？** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

設定	描述

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

Http類型

http類型用於HTTP通訊。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型， **http** 。
URL	必需設定。 要連線的URL。 可用格式： `host:port` 、 `IPv4:port` 、 `:port` 。 IPv6 位址也受支援，不過使用時，您也必須指定介面： `[address%interface]:port` 。 範例： `[fe80::5054:ff:fe4d:ba0c%eth0]:4222` ）。

設定	描述
授權	連線到指定URL時的授權類型可能的值： • 預設值是**停用**。 • **plain** — 如果選擇此選項，則必須指示包含使用者帳戶憑證的密鑰，以便在連線到連接器時進行授權。 **新增密鑰** *若要建立密鑰：* 1. 在**名稱**欄位中，輸入密鑰的名稱。 2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。 3. 如有必要，在**描述**欄位中輸入密鑰的描述。 4. 按一下**建立**按鈕。 密鑰將會新增並顯示在**密鑰**下拉清單中。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
壓縮	您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。
逾時時間	等待來自另一個服務或元件的回應時間（以秒為單位）。 預設值為 `30`。
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。
輸出格式	將事件傳送到外部目標的格式。可用值： • JSON • CEF 如果選擇CEF格式，則傳送的事件包含CEF標頭和僅非空白欄位。

設定	描述

TLS模式	使用TLS加密。可用值：
	• **已停用** (預設) 表示不使用 TLS 加密。
	• **啟用**表示使用加密，但不驗證憑證。
	• **附驗證**– 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA 的根憑證和金鑰會在程式安裝期間自動建立，並儲存在 KUMA Core 伺服器的 /opt/kaspersky/kuma/core/certificates/ 資料夾中。
	• **自訂CA**表示使用加密並驗證憑證是否由憑證授權單位簽署。包含憑證的密鑰可從**自訂CA**下拉清單中選擇，選擇此選項後會顯示該清單。
	建立由憑證授權單位簽署的憑證。
	您可以在KUMA Core伺服器上建立CA簽署的憑證（以下命令範例使用OpenSSL）。
	若要建立由憑證授權單位簽署的憑證：
	1. 產生憑證授權單位要使用的金鑰，例如：
	`openssl genrsa -out ca.key 2048`
	2. 為產生的金鑰建立憑證，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 憑證授權單位的通用主機名稱 >" -out ca.crt`
	3. 建立私鑰並要求憑證授權單位對其進行簽署，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 伺服器的通用主機名稱 >" -out server.csr`
	4. 建立由憑證授權單位簽署的憑證。您需在 `subjectAltName` 變數中包含為其建立憑證之伺服器的網域名稱或 IP 位址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform 網頁介面中，將建立的 `server.crt` 憑證上傳至 **憑證** 類型的機密項目，然後在 **自訂 CA** 下拉式清單中選取該 **憑證** 類型的機密項目。
	使用TLS時，無法將IP位址指定為URL。

URL選擇政策	如果您指定了多個URL，您可以從下拉清單中選擇決定將事件傳送到哪個URL的方法。可用值： • **任何**。只要其中一個可用的URL可以接收事件，事件就會傳送到該URL。如果連線中斷（例如，接收節點斷開連線），則會選擇其他URL作為事件目標。 • **第一優先**。事件將會傳送到已新增位址清單中的第一個URL。如果該URL不可用，事件將依序傳送到下一個可用節點。當第一個URL再次可用時，事件將再次開始傳送到此URL。 • **均衡**意味著包含事件的套件均勻分發在清單中可用的URL中。由於封包是在目標緩衝區溢位或排清計時器上傳送的，因此此URL選擇政策無法保證事件均勻分佈到目標。
分隔符號	在下拉式清單中，可選取字元來標記事件之間的邊界。預設使用 \n。
路徑	必須為URL請求新增的路徑。例如，指定路徑 `/input` 並為 URL 輸入 `10.10.10.10`，目的地將傳送對 `10.10.10.10/input` 的請求。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	正在處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
健康檢查路徑	用於傳送請求以獲取有關目標資源所連線到的系統的健康資訊的URL。
健康檢查超時	健康檢查的頻率（以秒為單位）。
健康檢查已停用	停用健康檢查的核取方塊。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在**篩選器**部分，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

二極體類型

二極體類型用於透過資料二極體傳輸事件。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型，**二極體**。

設定	描述
資料二極體來源目錄	必需設定。 資料二極體從中移動事件的目錄。該路徑最多可包含255個Unicode字元。 **在Windows伺服器上的路徑中使用前綴時的限制** 在Windows伺服器上，必須指定目錄的絕對路徑。不能使用名稱與下列規則運算式相符的目錄： • ^[a-zA-Z]:\\Program Files • ^[a-zA-Z]:\\Program Files \(x86\) • ^[a-zA-Z]:\\Windows • ^[a-zA-Z]:\\Program Files\\Kaspersky Lab\\KUMA **在Linux伺服器上的路徑中使用前綴時的限制** 指定檔案路徑時不能使用的前綴： • /* • /bin • /boot • /dev • /etc • /home • /lib • /lib64 • /proc • /root • /run • /sys • /tmp • /usr/* • /usr/bin/ • /usr/local/* • /usr/local/sbin/ • /usr/local/bin/ • /usr/sbin/ • /usr/lib/ • /usr/lib64/ • /var/* • /var/lib/ • /var/run/ • /opt/kaspersky/kuma/ 系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。 檔案位於下列路徑： • /opt/kaspersky/kuma/clickhouse/logs/ • /opt/kaspersky/kuma/metrics/log/

設定	描述
暫存目錄	準備將事件傳輸到資料二極體的目錄。 當發生逾時（預設為10秒）或緩衝區溢位時，事件會儲存在檔案中。準備好的檔案將會移動到**資料二極體來源目錄**欄位中指定的目錄。檔案內容的校驗和（SHA256）用作包含事件的檔案名稱。 暫存目錄必須與資料二極體來源目錄不同。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
壓縮	您可以使用Snappy壓縮。預設情況下，壓縮是**停用的**。 此設定必須與用於透過資料二極體中繼來自隔離網段的事件的連接器和目標資源相符。
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。
分隔符號	在下拉式清單中，可選取字元來標記事件之間的邊界。預設使用 `\n`。 此設定必須與用於透過資料二極體中繼來自隔離網段的事件的連接器和目標資源相符。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。

設定	描述
篩選器	在**篩選器**部分，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

Kafka類型

Kafka類型用於Kafka通訊。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型，**kafka**。
URL	必需設定。 要連線的URL。可用格式： `host:port` 、 `IPv4:port` 、 `:port` 。IPv6 位址也受支援，不過使用時，您也必須指定介面： `[address%interface]:port` 。 範例： `[fe80::5054:ff:fe4d:ba0c%eth0]:4222)` 。 您可以透過點擊URL按鈕來新增多個位址。
主題	必需設定。 Kafka訊息的主題。必須包含以下1到255個字元：a–z、A–Z、0–9、「.」、「_」、「-」。
分隔符號	指定一個用於界定一個事件結束而另一個事件開始的字元。預設使用 `\n` 。

設定	描述
授權	連線到指定URL時的授權類型可能的值： • 預設值是**停用**。 • **PFX** — 必須在外部憑證授權單位中使用PKCS#12容器格式的私鑰產生憑證。然後，必須將憑證從金鑰庫匯出，並將其作為PFX密鑰上傳到KUMA主控台。 • **新增PFX密鑰** *若要建立PFX密鑰：* 1. 在**名稱**欄位中，輸入PFX密鑰的名稱。 2. 按一下**上傳PFX**，然後選擇使用私鑰匯出PFX檔案的PKCS#12容器檔案。 3. 在**密碼**欄位中，輸入在PFX匯出精靈中設定的PFX檔案的密碼。 4. 按一下**建立**按鈕。 PFX密鑰隨即建立並顯示在**PFX 密鑰**下拉清單中。 • **純文字**—您必須指定包含使用者帳戶憑證的密鑰，以便在連線到連接器時進行授權。 **新增密鑰** *若要建立密鑰：* 1. 在**名稱**欄位中，輸入密鑰的名稱。 2. 在**使用者**和**密碼**欄位中，輸入代理程式將用於連線到連接器的使用者帳戶的憑據。 3. 如有必要，在**描述**欄位中輸入密鑰的描述。 4. 按一下**建立**按鈕。 密鑰將會新增並顯示在**密鑰**下拉清單中。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。
逾時時間	等待來自另一個服務或元件的回應時間（以秒為單位）。 預設值為 `30`。
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。
輸出格式	將事件傳送到外部目標的格式。可用值： • JSON • CEF 如果選擇CEF格式，則傳送的事件包含CEF標頭和僅非空白欄位。

設定	描述

TLS模式	使用TLS加密。可用值：
	• **停用**（預設）表示不使用TLS加密。
	• **啟用**— 使用加密但不進行憑證驗證。
	• **附驗證**— 使用加密並驗證憑證是否使用KUMA根憑證簽名。KUMA 的根憑證和金鑰會在程式安裝期間自動建立，並儲存在 KUMA Core 伺服器的 /opt/kaspersky/kuma/core/certificates/ 資料夾中。
	• **自訂CA**表示使用加密並驗證憑證是否由憑證授權單位簽署。包含憑證的密鑰可從**自訂CA**下拉清單中選擇，選擇此選項後會顯示該清單。
	建立由憑證授權單位簽署的憑證。
	您可以在KUMA Core伺服器上建立CA簽署的憑證（以下命令範例使用OpenSSL）。
	若要建立由憑證授權單位簽署的憑證：
	1. 產生憑證授權單位要使用的金鑰，例如：
	`openssl genrsa -out ca.key 2048`
	2. 為產生的金鑰建立憑證，例如：
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=< 憑證授權單位的通用主機名稱 >" -out ca.crt`
	3. 建立私鑰並要求憑證授權單位對其進行簽署，例如：
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=< KUMA 伺服器的通用主機名稱 >" -out server.csr`
	4. 建立由憑證授權單位簽署的憑證。您需在 `subjectAltName` 變數中包含為其建立憑證之伺服器的網域名稱或 IP 位址，例如：
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. 在 Open Single Management Platform 網頁介面中，將建立的 `server.crt` 憑證上傳至 **憑證** 類型的機密項目，然後在 **自訂 CA** 下拉式清單中選取該 **憑證** 類型的機密項目。
	使用TLS時，無法將IP位址指定為URL。

分隔符號	在下拉式清單中，可選取字元來標記事件之間的邊界。預設使用 `\n`。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在此部分中，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

檔案類型

檔案類型用於將資料寫入檔案。

> 如果刪除服務中使用的「檔案」類型的目標，則必須重新啟動該服務。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型，**檔案**。

設定	描述
URL	必需設定。 必須寫入事件的檔案的路徑。 **在檔案路徑中使用前綴時的限制** 指定檔案路徑時不能使用的前綴： • /* • /bin • /boot • /dev • /etc • /home • /lib • /lib64 • /proc • /root • /run • /sys • /tmp • /usr/* • /usr/bin/ • /usr/local/* • /usr/local/sbin/ • /usr/local/bin/ • /usr/sbin/ • /usr/lib/ • /usr/lib64/ • /var/* • /var/lib/ • /var/run/ • /opt/kaspersky/kuma/ 系統使用這些前綴作為規則運算式來檢查路徑。前綴中的*字元符合任何字元序列，如果路徑本身不是有效路徑的一部分，則不得手動指定該字元。 檔案位於下列路徑： • /opt/kaspersky/kuma/clickhouse/logs/ • /opt/kaspersky/kuma/metrics/log/
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。
分隔符號	在下拉式清單中，可選取字元來標記事件之間的邊界。預設使用 \n。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
輸出格式	將事件傳送到外部目標的格式。可用值： • JSON • CEF 如果選擇CEF格式，則傳送的事件包含CEF標題和僅非空白欄位。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在**篩選器**部分，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

儲存體類型：

儲存體類型用於將資料傳輸到儲存體。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型，**儲存體**。
URL	必需設定。 要連線的URL。可用格式：`host:port`、`IPv4:port`、`:port`。IPv6 位址也受支援，不過使用時，您也必須指定介面：`[address%interface]:port`。 範例：`[fe80::5054:ff:fe4d:ba0c%eth0]:4222`)。 您可以透過點擊**URL**按鈕來新增多個位址。 **URL**欄位支援透過FQDN、IP位址和名稱搜尋服務。搜尋字串格式： • `<Search value>` — 透過 FQDN、IP 位址和服務名稱執行搜尋。 • `<First search value ending in one or more digits>:<second search value>` — 第一個值用於依服務的 FQDN 或 IP 位址搜尋，第二個值用於依連接埠搜尋。 • `:<value>` — 透過連接埠執行搜尋。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
代理伺服器	用於選擇代理伺服器的下拉清單。
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。

設定	描述
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。
URL選擇政策	下拉清單，如果指定了多個URL，您可以在其中選擇一種方法來確定將事件傳送到哪個URL： • **任何**。只要其中一個可用的URL可以接收事件，事件就會傳送到該URL。如果連線中斷（例如，接收節點斷開連線），則會選擇其他URL作為事件目標。 • **第一優先**。事件將會傳送到已新增位址清單中的第一個URL。如果該URL不可用，事件將依序傳送到下一個可用節點。當第一個URL再次可用時，事件將再次開始傳送到此URL。 • **均衡**意味著包含事件的套件均勻分發在清單中可用的URL中。由於封包是在目標緩衝區溢位或排清計時器上傳送的，因此此URL選擇政策無法保證事件均勻分佈到目標。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
健康檢查超時	健康檢查的頻率（以秒為單位）。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在此部分中，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

關聯器類型

關聯器類型用於將資料傳輸到關聯器。

基本設定頁籤

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
狀態切換開關	在必須將事件傳送到目標時使用。 預設情況下，啟用傳送事件。
類型	必需設定。 目標類型，**關聯器**。
URL	必需設定。 要連線的URL。可用格式：`host:port`、`IPv4:port`、`:port`。IPv6 位址也受支援，不過使用時，您也必須指定介面：`[address%interface]:port`。 範例：`[fe80::5054:ff:fe4d:ba0c%eth0]:4222`)。 您可以透過點擊**URL**按鈕來新增多個位址。 **URL**欄位支援透過FQDN、IP位址和名稱搜尋服務。搜尋字串格式： • `<Search value>` — 透過 FQDN、IP 位址和服務名稱執行搜尋。 • `<First search value ending in one or more digits>:<second search value>` — 第一個值用於依服務的 FQDN 或 IP 位址搜尋，第二個值用於依連接埠搜尋。 • `:<value>` — 透過連接埠執行搜尋。
描述	資源描述：最多4,000個Unicode字元。

進階設定頁籤

設定	描述
代理伺服器	用於選擇代理伺服器的下拉清單。
緩衝區大小	設定緩衝區的大小。 預設值為1KB，最大值為64MB。

設定	描述
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。 預設值為10GB。
URL選擇政策	下拉清單，如果指定了多個URL，您可以在其中選擇一種方法來確定將事件傳送到哪個URL： • **任何**。只要其中一個可用的URL可以接收事件，事件就會傳送到該URL。如果連線中斷（例如，接收節點斷開連線），則會選擇其他URL作為事件目標。 • **第一優先**。事件將會傳送到已新增位址清單中的第一個URL。如果該URL不可用，事件將依序傳送到下一個可用節點。當第一個URL再次可用時，事件將再次開始傳送到此URL。 • **均衡**意味著包含事件的套件均勻分發在清單中可用的URL中。由於封包是在目標緩衝區溢位或排清計時器上傳送的，因此此URL選擇政策無法保證事件均勻分佈到目標。
緩衝區排清間隔	將資料批次傳送至目標的時間間隔（以秒為單位）。預設值為 `1 second`。
處理程式數量	此欄位用於設定處理佇列的服務數量。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
健康檢查超時	健康檢查的頻率（以秒為單位）。
除錯	此切換開關可讓您指定是否必須啟用資源日誌記錄。預設值是**停用**。
磁碟緩衝區已停用	下拉清單可讓您啟用或停用磁碟緩衝區。預設情況下已啟用該選項。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。分配的磁碟空間容量受**磁碟緩衝區大小限制**設定的值的限制。 如果分配給磁碟緩衝區的磁碟空間已耗盡，則事件將如下輪換：新事件替換寫入緩衝區的最舊事件。

設定	描述
篩選器	在**篩選器**部分，您可以指定用於識別必須由資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

目標，事件路由器類型

eventRouter 類型的目標用於將事件傳送至事件路由器。**事件路由器**類型的目標設定如下表所示。

基本設定頁籤

設定	描述
名稱	資源的唯一名稱。名稱的最大長度：128個Unicode字元。 必需設定。
租用戶	擁有資源的租用戶名稱。 必需設定。
州	此切換開關用於啟用向目標傳送事件的功能。此切換開關預設為開啟。
類型	目標類型：**事件路由器**。 必需設定。
網址	URL（必填）—您需要連線的 URL。現支援以下URL格式： • `< 主機名稱 >:< 連接埠號碼 >` • `< IPv4 位址 >:< 連接埠號碼 >` • `< IPv6 位址 >:< 連接埠號碼 >` 您可以使用以下格式指定 IPv6 位址：`[< IPv6 位址 >%< 介面 >:< 連接埠號碼 >`，例如 `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`。 您可以新增多個 URL，也可以移除 URL。如果URL欄位包含製表符或空格，KUMA不允許儲存資源或服務。若要新增URL，請按一下**+新增**按鈕。若要刪除URL，請按一下其旁邊的刪除✕圖示。 必需設定。
標記	資源搜尋標籤。 可選設定。
描述	資源的敘述。描述的最大長度為4000個Unicode字元。

進階設定頁籤

設定	描述
緩衝區大小	用於在將事件傳送至伺服器RAM進行進一步處理或儲存之前，先在伺服器RAM中彙總事件的緩衝區大小（以位元組為單位）。該值必須為正整數。預設緩衝區大小：67,108,864（64MB），在介面中顯示為0。
緩衝區排清間隔	向目標傳送事件的間隔（以秒為單位）。預設值為1秒。

設定	描述
磁碟緩衝區大小限制	磁碟緩衝區的大小（以位元組為單位）。預設值：10GB，在介面中顯示為0。
事件處理器	服務可以同時執行以並行處理回應規則的事件處理器數量。 該值必須為不超過999的正整數。
代理伺服器	目標的代理伺服器。您可以選擇現有代理伺服器或建立新的代理伺服器。若要建立新的代理伺服器，請選擇**新建**。 如果要編輯現有代理伺服器的設定，請點選其旁邊的鉛筆圖示。
URL選擇政策	如果您在**基本設定**頁籤的基本設定欄位中新增了多個URL，則此方法用於確定事件必須先傳送到哪些URL： • **任意**表示只要URL接受事件，事件就會傳送到隨機選擇的可用URL。如果該URL不可用，則事件會傳送到另一個隨機選擇的可用URL。預設選擇該值。 • **優先**表示事件會傳送到第一個新增的URL。如果該URL不可用，則事件會傳送到下一個已新增的可用URL。如果第一個新增的URL再次可用，則事件會再次傳送到第一個新增的URL。 • **輪詢**表示事件會在可用URL之間均勻分配。此方法無法保證事件在URL之間均勻分配，因為緩衝區可能會溢位或事件可能會傳送到目標位置。您可以在**緩衝區大小限制**欄位中以位元組為單位指定緩衝區大小；您也可以在**緩衝區重新整理間隔**欄位中以秒為單位指定向目標位置傳送事件的間隔。
健康檢查超時	檢查目標執行狀況的間隔（以秒為單位）。
磁碟緩衝區已停用	此切換開關用於啟用磁碟緩衝區。切換開關預設為開啟。 如果收集器無法將標準化事件傳送到目標，則使用磁碟緩衝區。您可以在**磁碟緩衝區大小限制**欄位中指定磁碟緩衝區的大小。如果磁碟緩衝區空間不足，新的標準化事件將覆蓋舊的標準化事件，從最早的事件開始。
逾時時間	目標等待其他服務或元件回應的時間（以秒為單位）。
偵錯	此開關會啟用資源記錄。預設情況下，切換開關是關閉的。

設定	描述
篩選器	用於決定資源必須處理哪些事件的篩選器。您可以選擇現有篩選條件或建立新篩選條件。若要建立新篩選器，請選擇**新建**。 若要編輯現有篩選器的設定，請點選其旁邊的鉛筆圖示。 **如何建立篩選器？** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect**檢查右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

設定	描述

服務頁籤

此頁籤僅在管理目標設定時顯示，用於關聯至服務，也就是收集器、關聯器和事件路由器。

若要將目標關聯至服務，請點選**關聯至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個服務，然後按一下**確定**。目標隨即與所選服務相關聯。

如有必要，您可以將目標與服務取消關聯。若要執行此操作，請選取服務旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

預定義目標

下表所列的目標包含在OSMP分發套件中。

預定義目標

目標名稱	描述
[OOTB] 關聯器	將事件傳送到關聯器。
[OOTB] 儲存體	將事件傳送到儲存體。

篩選器

篩選器可讓您依指定條件選擇事件。

收集器服務使用篩選器來選擇要傳送到KUMA的事件。也就是說，符合篩選條件的事件將會被傳送到KUMA進行進一步處理。

篩選器可用於以下KUMA服務和功能：

- 收集器。
- 關聯器。
- 儲存。
- KUMA代理程式。
- 關聯規則。
- 擴充規則。
- 彙總規則。
- 目標。

- 回應規則。
- 分段規則。

您可以使用獨立篩選器或內建篩選器，這些篩選器儲存在建立它們的服務或資源中。

對於這些資源，您可以在除**描述**欄位之外的所有輸入欄位中啟用控制字元的顯示。

篩選器的可用設定：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。內聯篩選器在其他資源或服務中建立，沒有名稱。
- **租用戶**（必填）- 擁有該資源的租用戶名稱。
- 描述 — 最多4,000個Unicode字元，用於描述篩選器。
- **條件**設定群組允許您透過建立篩選器條件和篩選器群組，或新增現有篩選器來制定篩選條件。

  若要建立篩選條件，您可以使用*建構器模式*或*原始碼模式*。預設情況下，使用建構器模式。

  在建構器模式下，您可以從下拉清單中選擇篩選條件和運算子來建立或編輯篩選條件。

  在原始碼模式下，您可以使用文字命令建立和編輯搜尋查詢。

  建立篩選條件時，您可以在模式之間自由切換。若要切換到原始碼模式，請按一下**代碼**按鈕。在模式之間切換時，已建立的條件篩選器將被保留。如果將建立的篩選器連結到資源後，則**代碼**頁籤上未顯示篩選器代碼，請轉至**建構器**頁籤，然後返回**代碼**頁籤。將顯示篩選器代碼。

在建構器模式下建立條件

您可以透過點選下列按鈕在建構器模式下建立篩選條件：

- **新增條件**會新增一個字串，其中包含用於定義條件的欄位。
- **新增群組**會新增一組篩選器。群組運算子可以在**AND** 、 **OR**和**NOT**之間切換。您可以將群組、條件和現有篩選器新增至篩選器群組。**NOT**子群組中的條件與**AND**運算子組合。

若要替換已建立條件中的運算子，請按一下要替換的運算子，然後從下拉清單中選擇新的運算子。

若要刪除已建立條件中的運算子，請按一下要刪除的運算子，然後按**退格鍵** 。

若要變更篩選條件的順序，請按一下 ⣿ 並將條件拖曳到新位置。

可以透過按一下 ✕ 按鈕刪除條件、群組和篩選器。

條件設定：

- **當**（必要）- 在此下拉清單中，您可以指定是否使用運算子的反函式。
- **左運算元**和**右運算元**（必填）- 用於指定運算子將處理的值。可用的類型取決於選定的運算子。

篩選器的運算元

- **事件欄位** - 用於將事件欄位的值指派給運算元。進階設定：
  - **事件欄位**（必填） - 此下拉清單用於選取要從中擷取運算元值的欄位。
- **活動清單** - 用於將活動清單記錄的值指派給運算元。進階設定：
  - **活動清單**（必填） - 此下拉清單用於選取活動清單。
  - **金鑰欄位**（必填） - 這是用於建立活動清單項目，並作為該項目金鑰的事件欄位清單。
  - **欄位**（除非選取 **inActiveList** 操作員，否則為必填） - 用於輸入要從中擷取運算元值的活動清單欄位名稱。
- **上下文表** - 用於將上下文表的值指派給運算元。進階設定：
  - **上下文表名稱**（必填） - 此下拉清單用於選取上下文表。
  - **金鑰欄位**（必填） - 用於建立上下文表記錄，並作為該記錄金鑰的事件欄位或區域變數清單。
  - **欄位** - 用於輸入要從中擷取運算元值的上下文表欄位名稱。
  - **索引** - 用於輸入要從中擷取運算元值的表格清單欄位索引。
- **字典** - 用於將字典資源的值指派給運算元。進階設定：
  - **字典**（必填） - 此下拉清單用於選取字典。
  - **金鑰欄位**（必填） - 這是用於組成字典值金鑰的事件欄位清單。
- **常數** - 用於將自訂值指派給運算元。進階設定：
  - **值**（必填） - 在此輸入要指派給運算元的常數。
- **表格** - 用於將多個自訂值指派給運算元。進階設定：
  - **字典**（必填） - 此下拉清單用於選取**表格**類型的字典。
  - **金鑰欄位**（必填） - 這是用於組成字典值金鑰的事件欄位清單。
- **清單** - 用於將多個自訂值指派給運算元。進階設定：
  - **值**（必填） - 在此輸入要指派給運算元的常數清單。在欄位中鍵入值並按**回車鍵**時，該值將會新增至清單中，您可以輸入新值。
- **TI** - 用於從事件中讀取 CyberTrace 威脅情報 (TI) 資料。進階設定：
  - **資訊來源**（必填） - 此欄位用於指定 CyberTrace 威脅類別。
  - **金鑰欄位**（必填） - 此下拉清單用於選取包含 CyberTrace 威脅指標的事件欄位。
  - **欄位**（必填） - 此欄位用於指定包含威脅指標的 CyberTrace 資訊來源欄位。

- **運算子**（必填）—用於選擇條件運算子。

在此下拉清單中，如果運算子應忽略值的大小寫，則可以選取**大小寫不相符**核取方塊。如果選取了**inSubnet**、**inActiveList**、**inCategory**、**InActiveDirectoryGroup**、**hasBit**、**inDictionary**運算子，則忽略此核取方塊。預設情況下，此核取方塊已清除。

篩選器運算子

- **=** — 左運算元等於右運算元。
- **<** — 左運算元小於右運算元。
- **<=** — 左運算元小於或等於右運算元。
- **>** — 左運算元大於右運算元。
- **>=** — 左運算元大於或等於右運算元。
- **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
- **contains** — 左運算元包含右運算元的值。
- **startsWith** — 左運算元以右運算元的某個值開頭。
- **endsWith** — 左運算元以右運算元的某個值末端。
- **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

可用的運算元種類取決於運算元是左 (L) 還是右 (R)。

左 (L) 和右 (R) 運算元類型

運算子	事件欄位類型	活動清單類型	字典類型	快顯表單類型	表類型	TI類型	常數類型	清單類型
=	L,R	L,R	L,R	L,R	L,R	L,R	R	R
>	L,R	L,R	L,R	L,R（僅在依索引查詢表格值時）。	L,R	L	R	—
>=	L,R	L,R	L,R	L,R（僅在依索引查詢表格值時）。	L,R	L	R	—
<	L,R	L,R	L,R	L,R（僅在依索引查詢表格值時）。	L,R	L	R	—
<=	L,R	L,R	L,R	L,R（僅在依索引查詢表格值時）。	L,R	L	R	—
inSubnet	L,R	L,R	L,R	L,R	L,R	L,R	R	R
contains	L,R	L,R	L,R	L,R	L,R	L,R	R	R
startsWith	L,R	L,R	L,R	L,R	L,R	L,R	R	R
結束於	L,R	L,R	L,R	L,R	L,R	L,R	R	R
相符	L	L	L	L	L	L	R	R
hasVulnerability	L	L	L	L	L	—	—	—
hasBit	L	L	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—	—	—
inDictionary	—	—	—	—	—	—	—	—
inCategory	L	L	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—	—	—
inActiveDirectoryGroup	L	L	L	L	L	—	R	R
TIDetect	—	—	—	—	—	—	—	—

您可以使用熱鍵來管理篩選器。下表介紹了熱鍵。

熱鍵及其功能

熱鍵	功能
e	喚出事件欄位篩選器
d	喚出字典欄位篩選器
a	喚出活動清單欄位篩選器
c	喚出快顯表單欄位篩選器
t	喚出表格欄位篩選器
f	喚出篩選器
t+i	喚出使用TI的篩選器
Ctrl+Enter	完成編輯條件

`string`、`number` 或 `float` 類型的延伸事件結構描述欄位，其使用方式與 KUMA 事件結構描述的欄位相同。

在使用 `Array of strings`、`Array of numbers` 和 `Array of floats` 類型的延伸事件結構描述欄位進行篩選時，您可以使用以下操作：

- 若陣列中存在指定的子字串，`contains` 操作會傳回 `True`，否則會傳回 `False`。
- `match` 操作會將字串與規則運算式進行比對。
- `intersec` 操作。

在使用 `Array of numbers` 和 `Array of floats` 類型的延伸事件結構描述欄位進行篩選時，您可以使用以下比較操作：`<`、`>`、`=`、`>=`、`<=`。

若要在篩選器中引用陣列的特定元素，可以使用下列語法：`NA.<` 陣列名稱 `>.<` 元素索引 `>`

陣列以0為基礎。

範例：

`NA.ArrayOne.0` — 存取 ArrayOne 整數陣列的第一個元素。

`FA.ArrayTwo.2` — 存取 ArrayTwo 浮點數陣列的第三個元素。

在原始碼模式下建立條件

代碼編輯器模式可讓您快速編輯條件、選擇和複製代碼區塊。

在建構器的右側，您可以找到導航器，它允許您導航篩選器代碼。

系統會自動在 **AND**、**OR**、**NOT** 邏輯操作員處，或在分隔值清單中各項目的逗號處換行。

篩選器中使用的資源名稱是自動指定的。包含連結資源名稱的欄位無法編輯。如果您沒有**存取共享資源**，則共用資源類別的名稱不會顯示在篩選器中。

下表所列的篩選器包含在OSMP分發套件中。

預定義篩選器

篩選器名稱	描述
[OOTB][AD] 一個成員被新增到安全性全域群組（4728）	選擇將使用者新增至Active Directory安全性全域群組的事件。
[OOTB][AD] 一個成員被新增到安全性通用群組（4756）	選擇將使用者新增至Active Directory安全性通用群組的事件。
[OOTB][AD] 一個成員被從安全性全域群組中刪除（4729）	選擇從Active Directory安全性全域群組中刪除使用者的事件。
[OOTB][AD] 一個成員被從安全性通用群組中刪除（4757）	選擇從Active Directory安全性通用群組中刪除使用者的事件。
[OOTB][AD] 帳戶已建立	選擇Windows使用者帳戶建立事件。
[OOTB][AD] 帳戶已刪除	選擇Windows使用者帳戶刪除事件。
[OOTB][AD] 帳號登入失敗 (4625)	選擇Windows登入失敗事件。
[OOTB][AD] Kerberos身分驗證成功 (4624, 4768, 4769, 4770)	選擇成功的Windows登入事件以及在網域控制器上記錄的ID為 4769、4770的事件。
[OOTB][AD][Technical] 4768。已請求TGT	選擇ID為4768的Microsoft Windows事件。
[OOTB][Net] 可能的連接埠掃描	選擇可能指示連接埠掃描的事件。
[OOTB][SSH] 接受的密碼	選擇使用密碼成功建立SSH連線的事件。
[OOTB][SSH] 失敗的密碼	選擇使用密碼透過SSH連線的嘗試。

活動清單

活動清單是KUMA關聯器用來依關聯規則分析事件的儲存貯體。

例如，對於信譽不佳的IP位址清單，您可以：

1. 建立操作類型的關聯規則，並將這些IP位址新增至活動清單中。
2. 建立標準類型的關聯規則，並將活動清單指定為篩選條件。
3. 使用此規則建立關聯器。
   在這種情況下，KUMA選擇活動清單中包含IP地址的所有事件，並建立關聯事件。

您可以使用簡單類型的相關性規則自動填充活動清單，或匯入包含活動清單資料的檔案。

您可以新增、複製或刪除活動清單。

活動清單可用於以下KUMA服務和功能：

- 關聯規則。
- 儀表板。

不同的關聯器可以使用相同的活動清單。但是，每個關聯器都會建立一個單獨的活動清單實體。因此，即使活動清單具有相同的名稱和ID，不同關聯器使用的活動清單的內容也會有所不同。

只有基於關聯器關聯規則的資料才會加入到活動清單中。

您可以在活動關聯器表中新增、編輯、複製、刪除和匯出記錄。

在關聯過程中，從活動清單中刪除條目時，會在關聯器中產生服務事件。這些事件僅存在於關聯器中，不會重新導向到其他目標。可以設定關聯規則來追蹤這些事件，以便使用它們來識別威脅。下面描述了用於從活動清單中刪除條目的服務事件欄位。

事件欄位	值或注釋
`ID`	事件識別器
`Timestamp`	刪除過期條目的時間
`Name`	`"active list record expired"`
`DeviceVendor`	`"Kaspersky"`
`DeviceProduct`	`"KUMA"`
`ServiceID`	關聯器ID
`ServiceName`	關聯器名稱
`DeviceExternalID`	活動清單ID
`DevicePayloadID`	過期條目的鍵
`BaseEventCount`	已刪除條目的更新數增加了一個
`S.<active list field>`	活動清單中丟棄的條目，格式如下： S.<活動清單欄位> = <活動清單欄位的值>

檢視活動清單表

若要檢視關聯器活動清單表：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。

將顯示**關聯器活動清單**表。

此表包含以下資料：

- **名稱**– 關聯器清單的名稱。
- **記錄**– 活動清單包含的記錄數。
- **磁碟佔用大小**– 活動清單的大小。
- **目錄**– KUMA Core伺服器上活動清單的路徑。

新增活動清單

若要新增活動清單：

1. 在主功能表中，轉至**監控 → 資源 → 活動清單**。
2. 點選**新增活動清單**按鈕。
3. 請執行下列操作：
   a. 在**名稱**欄位中，輸入活動清單的名稱。
   b. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。
   c. 在**TTL**欄位中，指定新增至活動清單的記錄儲存在其中的時間。
   指定時間到期時，記錄將被刪除。時間以秒為單位指定。
   預設值是0。如果該欄位的值為0，則記錄將保留36,000天（約100年）。
   d. 在**描述**欄位中，輸入任何其他資訊。
   最多可以使用4,000個Unicode字元。
   該欄位是可選的。
4. 按一下**儲存**按鈕。

活動清單已新增。

檢視活動清單的設定

若要檢視活動清單的設定：

1. 在主功能表中，轉至**監控 → 資源 → 活動清單**。
2. 在**名稱**列中，選擇要檢視其設定的活動清單。

這將開啟活動清單設定視窗。它顯示以下資訊：

- **ID** – 選定活動清單的識別碼。
- **名稱**– 資源的唯一名稱。
- **租用戶**– 擁有資源的租用戶的名稱。
- **TTL** – 新增至活動清單的記錄將在此時間段內儲存。時間以秒為單位指定。
- **描述**– 有關資源的任何其他資訊。

變更活動清單的設定

若要變更活動清單的設定：

1. 在主功能表中，轉至**監控 → 資源 → 活動清單**。
2. 在**名稱**欄位中，選擇要變更其設定的活動清單。
3. 指定以下參數的值：
   - **名稱**– 資源的唯一名稱。
   - **TTL** – 新增至活動清單的記錄將在此時間段內儲存。時間以秒為單位指定。
     如果該欄位設為0，則記錄將無限期儲存。
   - **描述**– 有關資源的任何其他資訊。

> **ID**和**租用戶**欄位不可編輯。

複製活動清單的設定

若要複製活動清單：

1. 在主功能表中，轉至**監控 → 資源 → 活動清單**。
2. 選取您要複製的活動清單旁邊的核取方塊。

3. 按一下**複製**。
4. 指定需要的設定：
5. 按一下**儲存**按鈕。

活動列表即被複製。

刪除活動清單

若要刪除活動清單：

1. 在主功能表中，轉至**監控 → 資源 → 活動清單**。
2. 選取您要刪除的活動清單旁邊的核取方塊。
   若要刪除所有列表，請選取**名稱**列旁邊的核取方塊。

   > 必須至少選取一個核取方塊。

3. 點擊**刪除**按鈕。
4. 點擊**確定**。

活動清單即被刪除。

檢視活動清單中的記錄

若要檢視活動清單中的記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。
5. 在**名稱**列中，選擇所需的活動清單。

系統將開啟所選清單的記錄表。

此表包含以下資料：

- **鍵**– 記錄鍵的值。
- **記錄重複**– 此記錄在事件中被提及的總次數以及將活動清單匯入KUMA時下載相同記錄的總次數。

- **到期日**– 必須刪除記錄的日期和時間。
  如果在建立活動清單時**TTL**欄位的值為0，則此活動清單的記錄將保留36,000天（約100年）。
- **建立時間**– 建立活動清單的時間。
- **更新時間**– 活動清單的最後更新時間。

搜尋活動清單中的記錄

若要搜尋活動清單中的記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。
5. 在**名稱**直欄中，選擇所需的活動清單。
   將會開啟一個視窗，其中包含所選清單的記錄。
6. 在**搜尋**欄位中，輸入記錄鍵值或鍵中的幾個字元。

活動清單的記錄表僅顯示鍵包含輸入字元的記錄。

將記錄新增至活動清單

若要將記錄新增至活動清單：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取所需關聯器旁邊的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。
5. 在**名稱**直欄中，選擇所需的活動清單。
   將會開啟一個視窗，其中包含所選清單的記錄。
6. 按一下**新增**按鈕。
   建立記錄視窗將會開啟。
7. 指定以下參數的值：
   a. 在**鍵**欄位中，輸入記錄的名稱。
      您可以指定多個值，並以「|」字元分隔。

鍵欄位不能為空。如果未填寫該欄位，KUMA在嘗試儲存變更時將傳回錯誤。

b. 在**值**欄位中，指定**欄位**列中欄位的值。

KUMA從與活動清單關聯的關聯規則中取得欄位名稱。這些名稱不可編輯。如有必要，您可以刪除這些欄位。

c. 點擊新增元素按鈕以**新增元素**。

d. 在**欄位**列中，指定欄位名稱。

該名稱必須符合以下要求：

- 是唯一的。
- 不包含頁籤字元。
- 不包含底線字元外的特殊字元。
- 最大字元數是128。

名稱不能以底線字元開頭，且只能包含數字。

e. 在**值**直欄中，指定此欄位的值。

必須符合以下要求：

- 不包含頁籤字元。
- 不包含底線字元外的特殊字元。
- 最大字元數是1024。

該欄位是可選的。

8. 按一下**儲存**按鈕。

記錄已新增。儲存後，活動清單中的記錄將依字母順序排序。

複製活動清單中的記錄

若要複製活動清單中的記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。

將顯示**關聯器活動清單**表。

5. 在**名稱**直欄中，選擇所需的活動清單。
   將會開啟一個視窗，其中包含所選清單的記錄。
6. 選取您要複製的記錄旁邊的核取方塊。
7. 按一下**複製**。
8. 指定需要的設定：

   鍵欄位不能為空。如果未填寫該欄位，KUMA在嘗試儲存變更時將傳回錯誤。

   對於先前已新增至活動清單的記錄，無法編輯**欄位**直欄中的欄位名稱。您只能變更編輯時新增的記錄的名稱。名稱不能以底線字元開頭，且只能包含數字。

9. 按一下**儲存**按鈕。

記錄已複製。儲存後，活動清單中的記錄將依字母順序排序。

變更活動清單中的記錄

若要編輯活動清單中的記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。
5. 在**名稱**直欄中，選擇所需的活動清單。
   將會開啟一個視窗，其中包含所選清單的記錄。
6. 按一下**鍵**直欄中的記錄名稱。
7. 指定所需的值。
8. 按一下**儲存**按鈕。

此記錄將被覆蓋。儲存後，活動清單中的記錄將依字母順序排序。

編輯記錄時的限制：

- 記錄名稱不可編輯。您可以透過匯入具有不同名稱的相同資料來變更它。
- 對於先前已新增至活動清單的記錄，無法編輯**欄位**直欄中的欄位名稱。您只能變更編輯時新增的記錄的名稱。名稱不能以底線字元開頭，且只能包含數字。

- **值**列中的值必須滿足以下要求：
  - 不包含西里爾字元。
  - 不包含空格或製表符。
  - 不包含底線字元外的特殊字元。
  - 最大字元數是128。

刪除活動清單中的記錄

若要刪除活動清單中的記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。
5. 在**名稱**直欄中，選擇所需的活動清單。
   將會開啟一個視窗，其中包含所選清單的記錄。
6. 選取您要刪除的記錄旁邊的核取方塊。
   若要刪除所有記錄，請選取**鍵**直欄旁邊的核取方塊。

   > 必須至少選取一個核取方塊。

7. 點擊**刪除**按鈕。
8. 點擊**確定**。

記錄將被刪除。

將資料匯入活動清單

若要匯入活動清單：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。

5. 將滑鼠游標停在所需活動清單的行上。
6. 點選活動清單名稱左側的...。
7. 選擇**匯入**。
   將開啟活動清單匯入視窗。
8. 在**檔案**欄位中選擇要匯入的檔案。
9. 在**格式**下拉清單中，選擇檔案的格式：
   - **csv**
   - **tsv**
   - **internal**
10. 在**鍵欄位**下，輸入包含活動清單記錄鍵的直欄的名稱。
11. 點擊**匯入**按鈕。

檔案中的資料將會匯入活動清單中。先前清單中包含的記錄將被儲存。

從檔案匯入的資料不會檢查是否有無效字元。如果在小工具中使用此資料，則當資料中存在無效字元時，小工具將無法正確顯示。

匯出活動清單資料

若要匯出活動清單：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 選取要檢視其活動清單之關聯器旁的核取方塊。
4. 按一下**前往有效清單**按鈕。
   將顯示**關聯器活動清單**表。
5. 將滑鼠游標停在所需活動清單的行上。
6. 按一下所需活動清單左側的...。
7. 按一下**匯出**按鈕。

使用瀏覽器設定下載JSON格式的活動清單。下載檔案的名稱反映了活動清單的名稱。

預定義活動清單

下表所列的活動清單包含在OSMP分發套件中。

活動清單名稱	描述
[OOTB][AD] 最終使用者技術支援帳戶	此活動清單用作「[OOTB][AD] 在多部主機上使用相同使用者帳戶成功驗證」關聯規則的篩選器。技術支援人員的帳戶可以新增到活動清單中。記錄不會從活動清單中刪除。
[OOTB][AD] 已請求TGT的清單。事件ID 4768	此活動清單由「[OOTB][AD][Technical] 4768.已請求 TGT」規則填入，此活動清單也用於「[OOTB][AD] 未使用 TGT 即授予 TGS（黃金票證）」規則的選擇器中。記錄在記錄10小時後從清單中刪除。
[OOTB][AD] 敏感群組清單	此活動清單用作「[OOTB][AD] 敏感群組的成員資格已修改」關聯規則的篩選器。必須監視其成員身分的關鍵網域群組可以新增到活動清單中。記錄不會從活動清單中刪除。
[OOTB][Linux] 受損的主機	此活動清單由[OOTB] 潛在受損Linux主機成功暴力破解規則填入。記錄將在記錄24小時後從清單中刪除。

字典

描述

字典是儲存可供其他KUMA資源和服務使用的資料的資源。

字典可用於以下KUMA服務和功能：

- 收集器。
- 關聯規則。
- 標準化器。

可用設定：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填） - 擁有該資源的租用戶名稱。
- **描述**— 最多4,000個Unicode字符，用於描述資源。
- **類型**（必填）— 字典類型。所選類型決定了字典可包含的資料格式：
  - 您可以為**字典**類型新增鍵值對。
    建議不要向此類型的字典添加超過50,000個條目。

    > 在字典中新增具有相同鍵的行時，每個新行都會覆蓋具有相同鍵的現有行。這意味著字典中只會新增一行。

  - 可以將複雜表格形式的資料新增至**表格**類型。您可以使用REST API與此類型的字典進行互動。
- **值**設定區塊 — 包含字典資料表：

對於**字典**類型，此區塊顯示**鍵-值**對的清單。您可以點選 + 按鈕在表格中新增一行。您可以透過點選將滑鼠游標停留在某一行時出現的 × 按鈕來刪除行。在**鍵**欄位中，您可以選擇指定一個唯一值：最多128個Unicode字元，第一個字元不能是$。在**值**欄位中，您可以選擇指定一個值：最多255個Unicode字元，第一個字元不能是$。您可以新增一個或多個**鍵-值**對。

- 對於**表格**類型，此區塊顯示一個包含資料的表格。您可以點選 + 按鈕在表格中新增行和列。您可以透過點選將滑鼠游標停留在某一行或某個列標頭上時顯示的 × 按鈕來刪除行和列。列標頭可以編輯。

如果字典包含超過5,000個條目，則它們不會顯示在KUMA主控台中。若要查看此類字典的內容，必須將內容匯出為CSV格式。如果您編輯CSV檔案並將其匯入回KUMA，字典就會更新。

匯入和匯出字典

您可以透過按一下**匯入CSV**或**匯出CSV**按鈕以CSV格式（UTF-8編碼）匯入或匯出字典資料。

CSV檔案的格式取決於字典類型：

- **字典**類型：

  ```
  {KEY},{VALUE}\n
  ```

- **表格**類型：

  ```
  {Column header 1}, {Column header N}, {Column header N+1}\n
  {Key1}, {ValueN}, {ValueN+1}\n
  {Key2}, {ValueN}, {ValueN+1}\n
  ```

  CSV檔案和字典的鍵都必須是唯一的。在表格中，鍵在第一直欄中指定。必須包含1至255個Unicode字元。值必須包含0到256個Unicode字元。

在匯入過程中，字典的內容將被匯入的檔案覆蓋。匯入字典時，資源名稱也會變更以反映匯入檔案的名稱。

如果鍵或值包含逗號或引號字元（, 和 "），則匯出時會將它們括在引號 (") 中。此外，引號字元 (") 會被額外的引號 (") 遮蔽。

如果在匯入的檔案中偵測到不正確的行（例如，無效的分隔符號），則在匯入字典時將忽略這些行，並且在匯入表時匯入進程將中斷。

透過API與字典互動

您可以使用REST API讀取**表格**類型字典的內容。即使這些資源正在由活動服務使用，您也可以修改它們。例如，這可讓您使用從協力廠商應用程式匯出的動態變更表中的資料設定事件擴充功能。

預定義字典

下表所列的字典包含在OSMP分發套件中。

字典名稱	類型	描述
[OOTB] Ahnlab。嚴重等級	字典	包含優先權ID與其名稱之間的對應關係表。
[OOTB] Ahnlab。SeverityOperational	字典	包含SeverityOperational參數的值和對應的描述。
[OOTB] Ahnlab。VendorAction	字典	包含正在執行的操作的ID與其名稱之間的對應關係表。
[OOTB] Cisco ISE 訊息代碼	字典	包含 Cisco ISE 事件代碼及其對應的名稱。
[OOTB] DNS。操作碼	字典	包含DNS操作的十進位操作碼與其IANA註冊描述之間的對應關係表。
[OOTB] IANAProtocolNumbers	字典	包含IANA註冊的傳輸協定（TCP、UDP）的連接埠號碼及其對應的服務名稱。
[OOTB] Juniper - JUNOS	字典	包含JUNOS事件ID及其對應的描述。
[OOTB] KEDR。帳戶類型	字典	包含使用者帳戶類型的ID及其對應的類型名稱。
[OOTB] KEDR。檔案屬性	字典	包含檔案系統儲存的檔案屬性的ID及其對應的描述。
[OOTB] KEDR。檔案操作類型	字典	包含來自KATA API的檔案操作的ID及其對應的操作名稱。
[OOTB] KEDR。檔案類型	字典	包含來自KATA API的修改的檔案ID及其對應的檔案類型描述。
[OOTB] KEDR。完整性等級	字典	包含Microsoft Windows完整性等級參數的SID及其對應的描述。
[OOTB] KEDR。登錄檔操作類型	字典	包含來自KATA API的登錄檔操作的ID及其對應的值。
[OOTB] Linux。Sycall類型	字典	包含Linux呼叫ID及其對應的名稱。
[OOTB] MariaDB錯誤代碼	字典	字典包含MariaDB錯誤代碼，並由 [OOTB] MariaDB Audit Plugin syslog標準化器用來擴充事件。
[Deprecated][OOTB] Microsoft SQL Server代碼	字典	包含MS SQL Server錯誤ID及其對應的描述。
[OOTB] MS DHCP事件ID描述	字典	包含Microsoft Windows DHCP伺服器事件ID及其對應的描述。
[OOTB] S-Terra。字典MSG ID到名稱	字典	包含S-Terra裝置事件的ID及其對應的事件名稱。
[OOTB] S-Terra。MSG_ID到嚴重等級	字典	包含S-Terra裝置事件的ID及其對應的嚴重等級值。
[OOTB] Syslog優先順序到設施和嚴重等級	table	該表包含**優先順序**值以及相應的**設施和嚴重等級**欄位值。
[OOTB] VipNet Coordinator Syslog Direction	字典	包含ViPNet Coordinator中用於指定方向的方向ID（特殊字元序列）及其對應的值。
[OOTB] Wallix EventClassId - 裝置操作	字典	包含Wallix AdminBastion事件ID及其對應的描述。
[OOTB] Windows.Codes (4738)	字典	包含MS Windows稽核事件中存在的操作代碼，ID為4738及其對應的名稱。
[OOTB] Windows.Codes (4719)	字典	包含MS Windows稽核事件中存在的操作代碼，ID為4719及其對應的名稱。
[OOTB] Windows.Codes (4663)	字典	包含MS Windows稽核事件中存在的操作代碼，ID為4663及其對應的名稱。
[OOTB] Windows.Codes (4662)	字典	包含MS Windows稽核事件中存在的操作代碼，ID為4662及其對應的名稱。
[OOTB] Windows.事件ID和事件名稱對應	字典	包含Windows事件ID及其對應的事件名稱。
[OOTB] Windows.失敗代碼 (4625)	字典	包含來自Microsoft Windows事件4625的**失敗資訊\狀態**和**失敗資訊\子狀態**欄位的ID及其對應的描述。
[OOTB] Windows.模擬層級 (4624)	字典	包含來自Microsoft Windows事件 4624 的**模擬層級**欄位的ID及其對應的描述。
[OOTB] Windows.KRB結果代碼	字典	包含Kerberos v5錯誤代碼及其對應的描述。
[OOTB] Windows.登入類型（Windows所有事件）	字典	包含使用者登入類型的ID及其對應的名稱。
[OOTB] Windows_終端伺服器。事件ID和事件名稱對應	字典	包含Microsoft終端伺服器事件ID及其對應的名稱。
[OOTB] Windows.驗證憑證。錯誤代碼	字典	包含使用者登入類型的ID及其對應的名稱。
[OOTB] VipNet Coordinator Syslog方向	字典	包含ViPNet Coordinator中用於指定方向的方向ID（特殊字元序列）及其對應的值。
[OOTB] Syslog優先順序到設施和嚴重等級	table	包含優先順序以及對應的設施和嚴重等級欄位值。

密鑰

密鑰用於安全地儲存敏感資訊，例如KUMA必須使用使用者名稱和密碼才能與外部服務互動。如果密鑰儲存了使用者登入名稱和密碼等帳戶資料，則當收集器連線到事件來源時，密鑰中指定的使用者帳戶可能會根據事件來源系統中設定的密碼政策被封鎖。

密鑰可用於以下KUMA服務和功能：

- 收集器（使用TLS加密時）。
- 連接器（使用TLS加密時）。
- 目標（使用TLS加密或授權時）。
- 代理伺服器。

可用設定：

- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填） - 擁有該資源的租用戶名稱。
- **類型**（必填） - 密鑰類型。

  在下拉清單中選擇類型時，也會出現用於設定此密鑰類型的參數。這些參數如下所述。
- **描述**—最多4,000個Unicode字元。

根據密鑰類型，有不同的欄位可用。您可以選取以下密鑰類型之一：

- **憑據** - 此類密鑰用於儲存連線到外部服務（例如SMTP伺服器）所需的帳戶憑據。如果選擇此類密鑰，則必須填寫**使用者**和**密碼**欄位。如果**密鑰**資源使用「憑據」類型將收集器連線到事件來源（例如資料庫管理系統），則密鑰中指定的使用者帳戶可能會根據事件來源系統中設定的密碼政策被封鎖。

  變更先前儲存的憑據類型密鑰時，使用者名稱和密碼欄位會顯示為空白。這些欄位的值會保留，您無需再次輸入。
- **權杖** - 此類密鑰用於儲存API請求的權杖。例如，在連線到IRP系統時使用權杖。如果您選擇此類型的密鑰，則必須填寫**權杖**欄位。
- **ktl**—此類密鑰用於儲存Kaspersky Threat Intelligence Portal網站帳戶憑據。如果您選擇此類型的密鑰，則必須填寫以下欄位：
  - **使用者**和**密碼**（必填欄位）—您的Kaspersky Threat Intelligence Portal網站帳戶的使用者名稱和密碼。
  - **PFX檔案**（必填）— 允許您上傳Kaspersky Threat Intelligence Portal網站憑證金鑰。
  - **PFX密碼**（必填）— 用於存取Kaspersky Threat Intelligence Portal網站憑證金鑰的密碼。
- **urls** — 此類密鑰用於儲存連線到SQL資料庫和代理伺服器的URL。在**描述**欄位中，您必須提供使用**urls**類型密鑰的連線的描述。

  您可以指定以下格式的URL：主機名稱:連接埠、IPv4:連接埠、IPv6:連接埠、:連接埠。

- **pfx** — 此類密鑰用於匯入包含憑證的PFX檔案。如果您選擇此類型的密鑰，則必須填寫以下欄位：
  - **PFX檔案**（必要）— 用於上傳PFX檔案。該檔案必須包含憑證和金鑰。PFX檔案可能包含用於伺服器憑證驗證的CA簽署憑證。
  - **PFX密碼**（必要）— 用於輸入存取憑證金鑰的密碼。
- **kata/edr** — 此類密鑰用於儲存連線到Kaspersky Endpoint Detection and Response伺服器時所需的憑證檔案和私鑰。如果您選擇此類型的密鑰，則必須上傳下列檔案：
  - 憑證檔案 - KUMA伺服器憑證。

    該檔案必須為PEM格式。您只能上傳一個憑證檔案。
  - 用於加密連線的私鑰 - KUMA伺服器RSA金鑰。

    該金鑰必須沒有密碼，但附有PRIVATE KEY標頭。您只能上傳一個金鑰檔案。

    > 您可以透過點擊 ⬇ 按鈕產生憑證和金鑰檔案。
- **snmpV1**—此類密鑰用於儲存透過簡易網路管理通訊協定進行互動時所需的 **社群** 值（例如，`public` 或 `private`）。
- **snmpV3** — 此類密鑰用於儲存透過簡易網路管理通訊協定進行互動所需的資料。如果您選擇此類型的密鑰，則必須填寫以下欄位：
  - **使用者**— 沒有網域的使用者名稱。
  - **安全等級**— 使用者的安全等級。
    - **NoAuthNoPriv** — 轉發訊息時無需身份驗證，也不確保機密性。
    - **AuthNoPriv** — 轉發訊息時需要身份驗證，但不確保機密性。
    - **AuthPriv** — 轉發訊息時需要驗證並確保機密性。

    根據所選的安全等級，可能會顯示其他設定。
  - **密碼**— SNMP使用者身份驗證密碼。選擇**AuthNoPriv**或**AuthPriv**安全等級時，此欄位可用。
  - **身分驗證通訊協定**— 以下協定可用：MD5、SHA、SHA224、SHA256、SHA384、SHA512。選擇**AuthNoPriv**或**AuthPriv**安全等級時，此欄位可用。
  - **私密通訊協定**— 用於加密訊息的協定。可用協定：DES、AES。選擇**AuthPriv**安全等級時，此欄位可用。
  - **私密密碼**— 建立SNMP使用者時設定的加密密碼。選擇**AuthPriv**安全等級時，此欄位可用。
- **憑證**— 此類密鑰用於儲存憑證檔案。點擊**上傳憑證檔案**按鈕即可將檔案上傳到資源。支援Base64格式的X.509憑證公鑰。
- **SSH 私密金鑰**—此類密鑰用於SFTP 連接器，以連接 SFTP 伺服器。如果選擇此類密鑰，您必須指定使用者名稱和包含SSH私密金鑰的檔案。

預定義密鑰

下表所列的密鑰包含在OSMP分發套件中。

預定義密鑰

密鑰名稱	描述
[OOTB] Continent SQL連線	儲存用於連線到APKSh Kontinent資料庫的機密資料和設定。要使用它，您必須指定資料庫的登入名稱和密碼。
[OOTB] KSC MSSQL連線	儲存用於連線到卡巴斯基安全管理中心（KSC）的MS SQL資料庫的機密資料和設定。要使用它，您必須指定資料庫的登入名稱和密碼。
[OOTB] KSC MySQL連線	儲存用於連線到卡巴斯基安全管理中心（KSC）的MySQL資料庫的機密資料和設定。要使用它，您必須指定資料庫的登入名稱和密碼。
[OOTB] Oracle Audit Trail SQL連線	儲存用於連線到Oracle資料庫的機密資料和設定。要使用它，您必須指定資料庫的登入名稱和密碼。
[OOTB] SecretNet SQL連線	儲存機密資料和設定，用於連線到SecretNet系統的MS SQL資料庫。要使用它，您必須指定資料庫的登入名稱和密碼。

快顯表單

*快顯表單*是資料陣列的容器，KUMA關聯器使用它根據關聯規則分析事件。您可以在**監控 → 資源**部分建立快顯表單。快顯表單資料僅儲存在使用關聯規則中的篩選器或操作新增它的關聯器中。

您可以使用「簡單」和「作業」類型的關聯規則自動填入快顯表單，也可以匯入包含快顯表單資料的檔案。

您可以新增、複製和刪除快顯表單，以及編輯其設定。

快顯表單可用於下列KUMA服務和功能：

- 關聯規則。
- 儀表板。

同一個快顯表單可用於多個關聯器。但是，每個關聯器都會建立一個單獨的快顯表單實體。因此，即使快顯表單具有相同的名稱和ID，不同關聯器使用的快顯表單的內容也是不同的。

只有基於關聯器關聯規則的資料才會加入到快顯表單中。

您可以在關聯器的快顯表單中新增、編輯、刪除、匯入和匯出記錄。

在關聯過程中，當從快顯表單中刪除條目時，關聯器中會產生服務事件。這些事件僅存在於關聯器中，不會重新導向到其他目標。服務事件會被傳送，由使用快顯表單的關聯器的關聯規則進行處理。可以設定關聯規則來追蹤這些事件，以便使用它們來辨識威脅。

用於從快顯表單中刪除條目的服務事件欄位如下所述。

事件欄位	值或注釋
ID	事件ID

Timestamp	刪除過期條目的時間
Name	"context table record expired"
DeviceVendor	"Kaspersky"
DeviceProduct	"KUMA"
ServiceID	關聯器ID
ServiceName	關聯器名稱
DeviceExternalID	快顯表單ID
DevicePayloadID	過期條目的鍵
BaseEventCount	已刪除條目的更新次數加一
FileName	快顯表單的名稱。
S.< 快顯表單欄位 > SA.< 快顯表單欄位 > N.< 快顯表單欄位 > NA.< 快顯表單欄位 > F.< 快顯表單欄位 > FA.< 快顯表單欄位 >	根據從快顯表單中刪除的條目的類型，刪除的快顯表單條目會記錄在對應類型的事件中： 例如，S.< 快顯表單欄位 > = < 快顯表單欄位值 > SA.< 快顯表單欄位 > = < 快顯表單欄位值陣列 > 布林類型的快顯表單記錄具有以下格式： S.< 快顯表單欄位 > = true/false SA.< 情境資料表欄位 > = false,true,false

檢視快顯表單清單

若要檢視關聯器的快顯表單清單：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 在要檢視其快顯表單的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。

   關聯器背景脈絡表格清單隨即顯示。

此表包含以下資料：

- **名稱**— 快顯表單的名稱。
- **磁碟大小**— 快顯表單的大小。
- **目錄**— KUMA關聯器伺服器上快顯表單的路徑。

新增快顯表單

若要新增快顯表單：

1. 在主功能表中，轉至**監控 → 資源 → 快顯表單**。
2. 在**快顯表單**視窗中，按一下**新增**。
   這將開啟**建立背景脈絡表格**視窗。

3. 在**名稱**欄位中，輸入快顯表單的名稱。

4. 在**租用戶**下拉清單中，選擇擁有該資源的租用戶。

5. 在**TTL**欄位中，指定新增至快顯表單的記錄儲存在其中的時間。

   指定時間到期時，記錄將被刪除。時間以秒為單位指定。最大值為`31536000`（1年）。

   預設值為`0`。若該欄位的值為0，記錄將無限期儲存。

6. 在**描述**欄位中，輸入任何其他資訊。

   最多可以使用4,000個Unicode字元。

   該欄位是可選的。

7. 在**結構描述**部分中，指定快顯表單具有哪些欄位以及這些欄位的資料類型。

   根據資料類型，欄位可能是或可能不是鍵欄位。表中至少有一個欄位必須是鍵欄位。所有欄位的名稱必須是唯一的。

   若要新增表格行，請按一下**新增**並填寫表格欄位：

   a. 在**名稱**欄位中，輸入欄位的名稱。最大長度為128個字元。

   b. 在**類型**下拉清單中，選擇欄位的資料類型。

   可能的欄位資料類型

   快顯表單欄位的可能資料類型

欄位資料類型	可以是鍵欄位	註解
整數	是	—
浮點	是	—
字串	是	—
布林值	是	—
時間戳記	是	對於此類欄位，會檢查欄位值是否大於或等於零。不提供其他操作。
IP位址	是	對於此類欄位，會檢查欄位值是否與IPv4、IPv6格式相對應。不提供其他操作。
整數清單	否	—
浮點數清單	否	—
字串清單	否	—
布林清單	否	—
時間戳記清單	否	對於此類欄位，會檢查清單中的每個項目是否大於或等於零。不提供其他操作。
IP清單	否	對於此類欄位，會檢查清單中的每個項目是否與IPv4、IPv6格式相對應。不提供其他操作。

   c. 如果要將欄位設為鍵欄位，請選取**鍵欄位**核取方塊。

   一個表格可以有多個鍵欄位。鍵欄位在建立快顯表單時選擇，唯一地辨識表條目且不能更改。

   如果快顯表單具有多個鍵欄位，則每個表條目由多個欄位唯一辨識（複合鍵）。

8. 新增所需數量的快顯表單行。

> 儲存快顯表單後，結構描述將無法變更。

9. 按一下**儲存**按鈕。

快顯表單已新增。

檢視快顯表單設定

若要檢視快顯表單設定：

1. 在主功能表中，轉至**監控 → 資源 → 快顯表單**。
2. 在**快顯表單**視窗的清單中，選擇要檢視其設定的快顯表單。

這將開啟快顯表單設定視窗。它顯示以下資訊：

- **名稱**— 資源的唯一名稱。
- **租用戶**— 擁有資源的租用戶的名稱。
- **TTL** — 新增到快顯表單的記錄在此期間儲存在其中。時間以秒為單位指定。
- **描述**— 有關資源的任何其他資訊。
- **架構**是欄位及其資料類型的有序清單，其中標記了鍵欄位。

編輯快顯表單設定

若要編輯快顯表單設定：

1. 在主功能表中，轉至**監控 → 資源 → 快顯表單**。
2. 在**快顯表單**視窗的清單中，選擇要編輯其設定的快顯表單。
3. 指定以下參數的值：
   - **名稱**— 資源的唯一名稱。
   - **TTL** — 新增到快顯表單的記錄在此期間儲存在其中。時間以秒為單位指定。
   - **描述**— 有關資源的任何其他資訊。
   - **架構**是欄位及其資料類型的有序清單，其中標記了鍵欄位。如果關聯規則中未使用快顯表單，則可以編輯欄位清單。

     如果要編輯關聯規則中已使用的快顯表單中的結構描述，請依照下列步驟操作。

   租用戶欄位不可編輯。
4. 按一下**儲存**按鈕。

若要編輯關聯器先前使用的快顯表單的設定：

1. 從表中匯出資料。
2. 複製並儲存關聯器磁碟上包含表資料的檔案的路徑。此路徑在**關聯器快顯表單**視窗的關聯器背景脈絡表格直欄中指定。稍後您將需要此路徑從關聯器磁碟中刪除檔案。
3. 從關聯器中刪除快顯表單。
4. 根據需要編輯快線表單設定。
5. 刪除關聯器磁碟上位於步驟2中的路徑的包含表格資料的檔案。
6. 將您在其中編輯設定的快顯表單新增至關聯器。
7. 若要重新啟動關聯器，請在**資源→活動服務**部分的服務清單中，選取相關關聯器旁的核取方塊，按一下工具列上的三個點圖示，然後在顯示的功能表中選擇**重新啟動**。
8. 調整匯出表中的欄位（請參閱步驟1），使其與步驟6中上傳到關聯器的資料表的欄位相符。
9. 將調整後的資料匯入快顯表單。

複製快顯表單設定

若要複製快顯表單：

1. 在主功能表中，轉至**監控 → 資源 → 快顯表單**。
2. 選取您要複製的快顯表單旁邊的核取方塊。
3. 按一下**複製**。
4. 指定需要的設定：
5. 按一下**儲存**按鈕。

快顯表單隨即複製。

刪除快顯表單

您只能刪除未在任何關聯器中使用的快顯表單。

若要刪除快顯表單：

1. 在主功能表中，轉至**監控 → 資源 → 快顯表單**。
2. 選取您要刪除的快顯表單旁邊的核取方塊。

   若要刪除所有快顯表單，請選取**名稱**直欄旁的核取方塊。

> 必須至少選取一個核取方塊。

3. 點擊**刪除**按鈕。
4. 點擊**確定**。

快顯表單被刪除。

檢視快顯表單記錄

若要檢視快顯表單記錄清單：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 在要檢視其快顯表單的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。

   這將開啟**關聯器背景脈絡表格**視窗。
4. 在**名稱**直欄中，選擇相關的快顯表單。

將顯示所選快顯表單的記錄清單。

清單包含以下資料：

- **鍵**是記錄的複合鍵。它由一個或多個鍵欄位的值組成，以「|」字元分隔。如果其中一個鍵欄位值不存在，則仍顯示分隔符號。

  例如，記錄金鑰由三個欄位組成：`DestinationAddress`、`DestinationPort` 和 `SourceUserName`。如果最後兩個欄位不包含值，則記錄金鑰顯示如下：`43.65.76.98| |` 。
- **記錄重複次數**是該記錄在事件中被提及的總次數，以及將快顯表單匯入KUMA時下載相同記錄的總次數。
- **到期日**– 必須刪除記錄的日期和時間。

  如果建立快顯表單時**TTL**欄位的值為0，則該快顯表單的記錄將保留36,000天（約100年）。
- **已更新**是快顯表單更新的日期和時間。

搜尋快顯表單記錄

若要在快顯表單中找尋記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 在要在其快顯表單中找尋記錄的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。

   這將開啟**關聯器背景脈絡表格**視窗。

4. 在**名稱**直欄中，選擇您的快顯表單。

   這將開啟一個視窗，其中包含選定的快顯表單的記錄。

5. 在**搜尋**欄位中，輸入記錄鍵值或鍵中的幾個字元。

   快顯表單記錄清單僅顯示鍵包含輸入字元的記錄。

如果您的搜尋查詢與鍵值為空的記錄相符，則**儀表板**上的小工具中會顯示文字<未找到>。我們建議您指明搜尋查詢的條件。

新增快顯表單

若要將記錄新增至快顯表單：

1. 在主功能表中，轉至**監控 → 資源**。

2. 在**服務**部分中，按一下**活動服務**按鈕。

3. 在要向其快顯表單中新增記錄的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。

   這將開啟**關聯器背景脈絡表格**視窗。

4. 在**名稱**直欄中，選擇相關的快顯表單。

   將顯示所選快顯表單的記錄清單。

5. 按一下**新增**按鈕。

   建立記錄視窗將會開啟。

6. 在**值**欄位中，指定**欄位**直欄中欄位的值。

   KUMA從與快顯表單相關的關聯規則中取得欄位名稱。這些名稱不可編輯。欄位清單也無法編輯。

   如果您未指定某些欄位值，則缺少的欄位（包括鍵欄位）將填入預設值。記錄鍵由完整的欄位集決定，並將記錄新增至表中。如果表中已存在相同的鍵，則會顯示錯誤。

   預設欄位值清單

欄位類型	預設值
整數	0
浮點	0.0
字串	""
布林值	false
IP位址	"0.0.0.0"
時間戳記	0
整數清單	[]
浮點清單	[]
字串清單	[]
布林清單	[]

時間戳記清單	[]
IP清單	[]

7. 按一下**儲存**按鈕。

記錄已新增。

編輯快顯表單記錄

若要編輯快顯表單中的記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。
3. 在要編輯快顯表單的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。
   這將開啟**關聯器背景脈絡表格**視窗。
4. 在**名稱**直欄中，選擇相關的快顯表單。
   將顯示所選快顯表單的記錄清單。
5. 點擊您要編輯的記錄行。
6. 在**值**直欄中指定您的值。
7. 按一下**儲存**按鈕。

此記錄將被覆蓋。

編輯記錄時的限制：

- 記錄的鍵欄位值無法編輯。您可以透過匯出和匯入記錄來更改它。
- **欄位**直欄中的欄位名稱無法編輯。
- **值**直欄中的值必須滿足以下要求：
  - 對於**時間戳記**和**時間戳記清單**類型的字段，其值大於或等於 0。
  - 對於**IP位址**和**IP清單**類型的欄位，其值必須為IPv4或IPv6格式。
  - 對於**布林值**欄位，其值必須為**true**或布林值。

刪除快顯表單記錄

若要從快顯表單中刪除記錄：

1. 在主功能表中，轉至**監控 → 資源**。
2. 在**服務**部分中，按一下**活動服務**按鈕。

3. 在要從其快顯表單中刪除記錄的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。
   這將開啟**關聯器背景脈絡表格**視窗。

4. 在**名稱**直欄中，選擇相關的快顯表單。
   將顯示所選快顯表單的記錄清單。

5. 選取您要刪除的記錄旁邊的核取方塊。
   若要刪除所有記錄，請選取**鍵**直欄旁邊的核取方塊。

   > 必須至少選取一個核取方塊。

6. 點擊**刪除**按鈕。

7. 點擊**確定**。

記錄將被刪除。

將資料匯入快顯表單

若要將資料匯入快顯表單：

1. 在主功能表中，轉至**監控 → 資源**。

2. 在**服務**部分中，按一下**活動服務**按鈕。

3. 在要從其快顯表單匯入資料的關聯器的快顯表單中，選擇**前往背景脈絡表格頁面**。
   這將開啟**關聯器背景脈絡表格**視窗。

4. 選取快顯表單旁邊的核取方塊，然後按一下**匯入**。
   這將開啟快顯表單資料匯入視窗。

5. 點選**新增** ，然後選擇要匯入的檔案。

6. 在**格式**下拉清單中，選擇檔案的格式：

   - **csv**
   - **tsv**
   - **internal**

7. 點擊**匯入**按鈕。

檔案中的資料將會匯入到快顯表單中。快顯表單中先前存在的記錄將被保留。

匯入時，KUMA會檢查每個記錄鍵的唯一性。如果記錄已存在，則其欄位將填入新值，新值是透過將先前的值與匯入記錄的欄位值合併而獲得的。

如果快顯表單中不存在記錄，則建立新記錄。

從檔案匯入的資料不會檢查是否有無效字元。如果在小工具中使用此資料，則當資料中存在無效字元時，小工具將無法正確顯示。

從快顯表單匯出資料

若要從快顯表單匯出資料：

1. 在主應用程式視窗中，前往**資源和服務 →活動服務**部分。
2. 選擇要匯出其快顯表單的關聯器，然後在工具列或功能表（⋮）中，點選**前往背景脈絡表格頁面**。
   這將開啟**關聯器背景脈絡表格**視窗。
3. 選取您要複製的快顯表單旁邊的核取方塊。
   您不能同時匯出多個快顯表單。每個表格都必須單獨匯出。
4. 點選**匯出**按鈕，然後從**格式**下拉清單中選擇一種格式：
   - **internal**
     快顯表單以JSON格式會出。
   - **csv**
   - **tsv**
5. 按一下**匯出**按鈕。

快顯表單將以所選格式下載到您的裝置。匯出檔案的名稱遵循以下範本：<快顯表單名稱>_<匯出日期（YYYY-MM-DD）>_<匯出時間（HH-MM-SS）>。檔案中的匯出資料按**鍵**欄位排序。

以JSON（**內部**）格式匯出時：

- 檔案中欄位的順序未定義。
- 陣列類型的欄位會以值陣列的形式匯出到檔案，例如：`["val1","val2","val3","val4"]`。
- **時間戳記**類型欄位中的日期和時間格式取決於所選的應用程式介面語言：
  - 俄文：DD.MM.YYYY HH:MM:SS，例如：`18.02.2025 16:09:58`
  - 英文：YYYY-MM-DD HH:MM:SS，例如：`2025.02.18 16:09:58`

以CSV和TSV格式匯出時：

- 檔案的第一行包含欄位名稱，後續行包含資料。
- 在CSV格式中，逗號用作欄位分隔符號；在TSV格式中，製表符用作欄位分隔符號。

您也可以在上下文表設定視窗中，將資料匯出至上下文表。

關聯規則

關聯規則用於識別已處理事件的特定序列，並在識別後採取某些操作，例如建立關聯事件/警示或與活動清單互動。

關聯規則可用於以下KUMA服務和功能：

- 關聯器。
- 通知規則。
- 分段規則的連結。
- 回溯掃瞄。

可用的關聯規則設定取決於所選類型。關聯規則的類型：

- 標準- 用於尋找多個事件之間的關聯。此類資源可以建立關聯事件。

  此規則類型用於確定複雜的關聯模式。對於較簡單的模式，您應該使用其他需要較少資源來操作的關聯規則類型。

- 簡單- 用於在發現某個事件時建立關聯事件。
- 操作— 用於與活動清單和快顯表單相關的操作。此規則類型無法建立關聯事件。
- 週期性—用於根據定期分析的累積資料偵測異常使用者活動。當兩個指標超過閾值時，即偵測到異常：**相對分數**和標準分數（**Z分數**）。

  此類規則僅在使用correlator-ng關聯器時可用。無法在OSMP主控台中建立此類規則。

  變更correlator-ng組態時，您可能需要刪除correlation/和containers/目錄。刪除這些目錄會導致所有彙總的關聯器資料遺失，包括統計資料、關聯規則儲存桶、活動清單和快顯表單。

對於這些資源，您可以在除**描述**欄位之外的所有輸入欄位中啟用控制字元的顯示。

如果在關聯器中使用了關聯規則，並且基於該規則建立了警示，則即使重新啟動關聯器服務，對關聯規則的任何變更都不會導致現有警示的變更。例如，如果變更了關聯規則的名稱，則警示的名稱將保持不變。如果關閉現有警示，則會建立一個新警示，並且該新警示將考慮關聯規則所做的變更。

標準關聯規則

標準關聯規則用於識別已處理事件中的複雜模式。

模式搜尋是透過使用儲存貯體進行的

*儲存貯體*是一個資料容器，關聯規則資源使用它來決定是否應該建立關聯事件。它具有以下功能：

- 將關聯規則資源設定中**選擇器**群組中的篩選器相符的事件分組在一起。事件根據使用者在**相同欄位**欄位中選擇的欄位進行分組。
- 確定關聯規則應在何時觸發，從而影響儲存貯體中分組的事件。
- 執行在設定的**操作**群組中所選的操作。
- 建立關聯事件。

儲存貯體的可用狀態：

- `Empty` — 儲存貯體中沒有任何事件。這僅在由關聯規則觸發建立時才會發生。
- `Partial Match` — 儲存貯體中有一些預期事件（復原事件不列入計算）。
- `Full Match` — 儲存貯體包含所有預期事件（復原事件不列入計算）。滿足此條件時：
  - 關聯規則觸發器
  - 從儲存貯體中清除事件
  - 儲存貯體的觸發計數器會更新
  - 儲存貯體的狀態變為 `Empty`
- `False Match` — 儲存貯體的此狀態可於以下情況出現：
  - 已達成 `Full Match` 狀態，但聯接篩選器傳回 false 時。
  - 選取**復原**核取方塊並收到復原事件時。

  滿足此條件時，關聯規則不會觸發。事件從儲存貯體中清除，觸發計數器隨之更新，儲存貯體狀態變為 `Empty`。

關聯規則視窗包含以下頁籤：

- **一般**— 用於指定關聯規則的主要設定。在此頁籤上，您可以選擇關聯規則的類型。
- **選擇器**— 用於定義已處理的事件必須滿足的條件才能觸發關聯規則。可用的設定因所選規則類型而異。
- **操作**— 用於設定在**選擇器**設定區塊中配置的條件滿足時啟動的觸發器。關聯規則資源必須至少有一個觸發器。可用的設定因所選規則類型而異。
- **關聯器**— 用於連結關聯器。僅適用於已建立且可編輯的關聯規則。

一般頁籤

- **卡巴斯基儲存庫中的資源版本** - 資源版本號。此欄位不可編輯。僅適用於卡巴斯基提供的資源，並用於管理資源更新。
- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。

- **租用戶**（必填）— 擁有關聯規則的租用戶。
- **類型**（必填）— 用於選擇關聯規則類型的下拉清單。如果要建立標準關聯規則，請選擇**標準** 。
- **相同欄位**（必填） - 應分組到儲存貯體中的事件欄位。所選欄位值的雜湊值將用作儲存貯體的金鑰。如果選擇器（請參閱下文）觸發，所選欄位將複製到關聯事件中。

  如果關聯規則的不同選擇器使用在事件中具有不同值的欄位，請勿在**相同欄位**部分中指定這些欄位。
- **唯一欄位** - 應傳送到儲存貯體的事件欄位。如果設定了此參數，則儲存貯體將僅接收唯一事件。所選欄位值的雜湊值將用作儲存貯體的金鑰。

  > 您可以在**相同欄位**和**唯一欄位**部分中使用局部變數。要存取變數，其名稱必須以「$」字元開頭。
  > 有關在這些部分中使用局部變數的範例，請參閱 KUMA 提供的規則：R403_從停用防護的主機或過時的病毒資料庫存取惡意的資源。

- **觸發率限制**— 每秒可觸發關聯規則的最大次數。預設值是100。

  > 若採用複雜模式偵測邏輯的關聯規則未被觸發，原因可能在於KUMA中用於規則觸發計數的特定方法。此種情況下，可嘗試將**觸發率限制**的值提高至`1000000`（例如）。

- **視窗，秒**（必填） - 儲存貯體使用期，以秒為單位。預設值：86,400秒（24小時）。此計時器在儲存貯體建立時（即收到第一個事件時）啟動。使用期不會更新，到期後，將啟動**操作**設定群組中的**逾時**觸發器並刪除儲存貯體。在儲存貯體的使用期內，**在每個閾值上觸發**和**在後續閾值上觸發**觸發器可以多次啟動。
- **基本事件保留政策** - 此下拉清單用於指定必須儲存在關聯事件中的基本事件：
  - **第一個**（預設值） - 此選項用於儲存觸發關聯事件所建立的事件集合中的第一個基本事件。
  - **最後一個** - 此選項用於儲存觸發關聯事件所建立的事件集合中的最後一個基本事件。
  - **所有** - 此選項用於儲存觸發關聯事件所建立的事件集合中的所有基本事件。
- **優先順序** — 用於判定關聯規則重要性的基礎係數。預設值是**低**。
- **排序依據** - 在此下拉清單中，您可以選擇關聯規則選擇器將用於追蹤情況變化的事件欄位。例如，如果您想要設定一個關聯規則，使其在多種類型的事件連續發生時觸發，這將非常有用。
- **描述**— 資源的描述。最多4,000個Unicode字元。

選擇器頁籤

標準類型的規則可以包含多個選擇器。您可以點選**新增選擇器**按鈕新增選擇器，也可以點選**刪除選擇器**按鈕刪除選擇器。可以透過點選 ⣿ 按鈕來移動選擇器。

對於每個選擇器，以下兩個頁籤可用：**設定**和**局部變數**。

設定頁籤包含以下設定：

- **別名**（必需）- 滿足選擇器條件的事件群組的唯一名稱。必須包含1至255個Unicode字元。
- **選擇器閾值（事件數）**（必要）— 選擇器必須接收才能觸發的事件數。預設值是1。
- **篩選器**（必填）— 用於設定決定應觸發選擇器的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。

  在資源中建立篩選器

  KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

  若要建立篩選器：

  1. 在**篩選器**下拉清單中，選擇**新建**。
  2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
  3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。
  4. 在**條件**下，指定事件必須滿足的條件：
     a. 點擊**新增條件**按鈕。
     b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。
     c. 在**運算子**下拉清單中，選擇一個運算子。

     篩選器運算子

     - **=** — 左運算元等於右運算元。
     - **<** — 左運算元小於右運算元。
     - **<=** — 左運算元小於或等於右運算元。
     - **>** — 左運算元大於右運算元。
     - **>=** — 左運算元大於或等於右運算元。
     - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
     - **contains** — 左運算元包含右運算元的值。
     - **startsWith** — 左運算元以右運算元的某個值開頭。
     - **endsWith** — 左運算元以右運算元的某個值末端。
     - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。

- **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

  待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

  若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。

- **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

  如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。

- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。

- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。

- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。

- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。

- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。

- **inContextTable**檢查指定快顯表單中條目的存在情況。

- **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

基於「額外」事件欄位資料的篩選：

基於**額外**事件欄位資料的篩選器條件：

- 條件 —**如果**。
- 左運算元 —**事件欄位**。
- 在此事件欄位中，您可以指定以下其中一個值：
  - **Extra**欄位。
  - Extra 欄位中的值，格式如下：

    `Extra.<field name>`

    例如，`Extra.app`。

這種類型的值需手動指定。

- 寫入**Extra**欄位的陣列值須符合以下格式：

  `Extra.<field name>.<array element>`

  例如，`Extra.array.0`。

  陣列中的值從0開始編號。

  這種類型的值需手動指定。

  若要使用 Extra 欄位中深度為 3 或更深層的值，請使用反引號 ``。例如，`Extra.lev1.lev2.lev3`。

- 運算子 — =。
- 右運算元 —**常數**。
- 值 — 您需要用來篩選事件的值。

關聯規則的選擇器篩選器中指定的條件順序非常重要，它會影響系統效能。我們建議將最獨特的條件放在選擇器篩選器的第一位。

請考慮兩個在Microsoft Windows中選擇成功驗證事件的選擇器篩選器範例。

選擇器篩選器1：

條件1。DeviceProduct = Microsoft Windows

條件2。DeviceEventClassID = 4624

選擇器篩選器2：

條件1。DeviceEventClassID = 4624

條件2。DeviceProduct = Microsoft Windows

選擇器篩選器2中的條件順序更可取，因為它對系統造成的負載較小。

- **復原**— 如果從選擇器接收到一定數量的事件，關聯規則不得觸發，則必須選取此核取方塊。預設情況下，此核取方塊已清除。

選擇**局部變數**頁籤，然後按一下**新增變數**以宣告要在此關聯規則限制內使用的變數。

在關聯規則的選擇器中，可以使用符合RE2標準的規則運算式。

與其他操作相比，在關聯規則中使用規則運算式的計算量很大。因此，在設計關聯規則時，我們建議將規則運算式的使用限制在必要的最小值，並使用其他可用的操作。

要使用規則運算式，必須使用 `match` 比較運算子。規則運算式必須置於常數中。在規則運算式中使用擷取群組為可選操作。要觸發關聯規則，與規則運算式相符的欄位文字必須與該規則運算式完全相符。

如需瞭解語法入門，以及選擇器中使用規則運算式的關聯規則範例，請查看 KUMA 隨附的下列規則：

- R105_04_可疑的PowerShell命令。可疑的混淆。
- R333_在自動運行資料夾中建立可疑的檔案。

操作頁籤

標準類型的規則可以有多個觸發器。

- **在首個閾值上觸發**– 當儲存貯體在其使用期內註冊選擇器首次觸發時，此觸發器會啟動。
- **在後續閾值上觸發** – 當儲存貯體在其使用期內註冊選擇器第二次及所有後續觸發時，此觸發器會啟動。
- **在每個閾值上觸發**– 每次儲存貯體註冊選擇器觸發時，此觸發器都會啟動。
- **逾時**– 此觸發器在儲存貯體的使用期結束時激活，並透過選取**復原**核取方塊連結到選擇器。換句話說，如果關聯規則偵測到的情況未在定義的時間內解決，則會啟動此觸發器。

每個觸發器都表示為一組設定，其中包含以下可用參數：

- **輸出**––如果選中此核取方塊，關聯事件將被傳送進行後處理：用於關聯規則之外的外部擴充、回應以及傳送至目標。
- **迴圈到關聯器**– 如果選取此核取方塊，則建立的關聯事件由目前關聯器的規則鏈處理。這允許分層關聯。

  如果設定了**輸出**和**迴圈到關聯器**核取方塊，則關聯規則首先被傳送到後處理，然後再傳送到目前關聯規則的選擇器。
- **不建立警示**– 如果選取此核取方塊，則觸發此關聯規則時不會建立警示。如果您不想在觸發關聯規則時建立警示，但仍想將關聯事件傳送到儲存體，請選取**輸出**和**不觸發警示**核取方塊。如果僅選取**不觸發警示**核取方塊，則關聯事件不會儲存在儲存體中。
- 在**擴充**下，您可以使用擴充規則修改關聯事件的欄位。這些擴充規則儲存在建立它們的關聯規則中。您可以建立多個擴充規則。透過分別點選**新增擴充**或**移除資料補足**按鈕，可以新增或刪除擴充規則。
  - **來源類型**– 您可以在下拉清單中選擇擴充的類型。根據所選類型，可能會顯示其他也需要填寫的進階設定。

    可用的擴充類型：
    - **常數**

      當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定：
      - 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。
      - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

      若針對 `String`、`Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。

      若針對 `Array of strings`、`Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。
    - **字典**

      如果需要從字典類型的**字典**中新增值，則使用此類擴充。

      在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。

如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。

例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。

如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。

例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。

- **表格**

  如果您需要從表格類型的**字典**中新增值，請使用此類擴充。

  在**字典名稱**下拉清單中選擇此擴充類型後，請選擇用於提供值的字典。在**鍵欄位**設定群組中，按一下**新增欄位**按鈕以選擇其值用於選擇字典條目的事件欄位。

  在**對應**表中，設定用於提供資料的字典欄位和用於接收資料的事件欄位：

  - 在**字典欄位**直欄中，選擇字典欄位。可用欄位取決於所選的字典資源。
  - 在 **KUMA 欄位**直欄中，選取要寫入值的事件欄位。對於某些選取的欄位（`*custom*` 與 `*flex*`），您可以在**標籤**直欄中，為寫入其中的資料指定名稱。

  可以透過點選**新增元素**按鈕來新增表格行。可以透過按一下✕按鈕來刪除直欄。

- **事件**

  當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定：

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。
  - 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。
  - 按一下🔧按鈕會開啟**轉換**視窗，您可以在其中使用**新增轉換**按鈕建立規則，在將原始資料寫入 KUMA 事件欄位前對其進行修改。

    可用的轉換

    轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

    可用轉換類型：

    - **小寫** — 用於將值的所有字元變為小寫
    - **大寫** — 用於將值的所有字元變為大寫
    - **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。
    - **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。

- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。
- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。
- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。
- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

當您使用事件擴充功能，且在 **來源類型** 設定中選取 **事件**，並使用延伸事件結構描述的欄位作為引數時，須注意以下特殊事項：

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `String` 類型的欄位，則值會以 TSV 格式寫入目標欄位。

  範例：SA.StringArray 延伸事件結構描述欄位包含以下值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 DeviceCustomString1 事件結構描述欄位。操作結果為：DeviceCustomString1 欄位包含 ["string1", "string2", "string3"]。

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `Array of strings` 類型的欄位，則來源欄位的值會附加至目標欄位的值，並存入目標欄位，以逗號 (",") 作為分隔符號。

  範例：延伸事件結構描述欄位 SA.StringArrayOne 包含值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 SA.StringArrayTwo 事件結構描述欄位。操作結果為：SA.StringArrayTwo 欄位包含 "string1"、"string2"、"string3"。

- **範本**

  當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

  - 在 **範本**欄位中，輸入 Go 範本。

    事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。

    範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

  若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

  如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

  範例：

  {{.SA.StringArrayOne}}

  範例：

  {{- range $index, $element := .SA.StringArrayOne -}}

  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **偵錯**— 您可以使用此切換開關來啟用服務操作的日誌記錄。

- **描述**— 資源的描述。最多4,000個Unicode字元。

- **分類** – 用於變更事件中指示的資產類別。可以有多個分類規則。您可以透過點選**新增分類**或**移除分類**按鈕來新增或刪除它們。只能將響應式類別新增至資產或從資產中刪除。

  - **操作**– 此下拉清單用於選擇要對類別執行的操作：

    - **新增**– 將類別指派給資產。

    - **刪除**– 將資產與類別解除綁定。

  - **事件欄位**– 指示需要操作的資產的事件欄位。

  - **類別 ID** – 下拉清單顯示類別樹，您可以在其中選擇要對其執行動作的類別。按一下此行可延伸清單。

- **活動清單更新**設定群組 – 用於指派活動清單一個或多個操作的觸發器。您可以點選**新增活動清單操作**和**刪除活動清單操作**按鈕分別新增或刪除活動清單操作。

  可用設定：

  - **名稱**（必要）– 此下拉清單用於選擇活動清單資源。

  - **操作**（必要）– 此下拉清單用於選擇必須執行的操作：

    - **求和**– 將常數、關聯事件欄位的值或局部變數的值新增至活動清單的值。

    - **取得**– 取得活動清單項目並將選定欄位的值寫入關聯事件。

    - **設定**– 透過建立新的或更新現有的活動清單條目，將關聯事件的選定欄位的值寫入活動清單。更新活動清單條目時，資料將合併，並且僅覆蓋指定的欄位。

    - **刪除**– 刪除活動清單條目。

  - **鍵欄位**（必填）- 這是用於建立活動清單條目的事件欄位清單。它也用作活動清單條目的鍵。

    > 活動清單條目的鍵取決於可用欄位，而不取決於它們在KUMA主控台中的顯示順序。

  - **對應**（ **取得**和**設定**操作必填）- 用於將活動清單欄位與事件欄位進行對應。可以設定多個對應規則。

    - 左側欄位用於指定活動清單欄位。

      > 此欄位不得僅包含特殊字元或數字。

    - 中間下拉清單用於選擇事件欄位。

    - 選擇**設定**操作時，右側欄位可用於為活動清單欄位指派常數。

    - 在快顯表單更新下，您可以為一個或多個快顯表單操作指派觸發器。您可以按一下**新增背景脈絡表格操作**或**刪除背景脈絡表格操作**來新增或刪除快顯表單操作。

    - 可用設定：

    - 名稱（必填）- 此下拉清單用於選擇快顯表單資源。

    - 操作（必填）- 此下拉清單用於選擇必須執行的操作。

- 求和 - 將常數、關聯事件欄位的值或局部變數的值加到快顯表單的值中。此操作僅適用於數字和浮點類型的欄位。

- 設定 - 透過建立新的或更新現有的快顯表單條目，將關聯事件的選定欄位的值寫入快顯表單。更新快顯表單條目時，資料將合併，並且僅覆蓋指定的欄位。

- 取得—取得快顯表單的欄位，並將指定欄位的值寫入關聯事件。布林類型的表欄位和布林值清單不包括在對應中，因為事件不包含布林欄位。

- 合併—將關聯事件欄位、局部變數或常數的值附加到快顯表單欄位的目前值。

- 刪除—刪除快顯表單條目。

- 鍵欄位（必填）—這是用於建立快顯表單條目的事件欄位清單。它也用作快顯表單條目的鍵。作為鍵欄位，您可以指定在**選擇器**頁籤上宣告的事件欄位或局部變數。

- 快顯表單條目的複合鍵僅取決於欄位的值，而不取決於它們在KUMA主控台中的顯示順序。

- 對應（除**刪除**之外的所有操作都需要）—用於將快顯表單欄位對應到事件欄位或變數。可以設定多個對應規則。您可以多次指定相同的快顯表單欄位。

- 左側欄位用於指定快顯表單欄位。

- 此欄位不得包含對應中已使用的欄位名稱、頁籤字元、特殊字元或僅包含數字。最大字元數是128。名稱不能以底線字元開頭。

- 中間下拉清單用於選擇事件欄位或局部變數。

- 如果選擇了**設定**操作，則右側欄位可用於將常數指派給快顯表單欄位。例如，**合併**或**求和**。最大字元數是1,024。

關聯器頁籤

- **新增**— 用於編輯已建立的關聯規則。您可以按一下**新增**開啟**關聯器**視窗，然後從清單中選擇一個關聯器。按一下**確定**後，規則將連結到選定的關聯器。您可以同時選擇多個關聯器。規則將會新增到執行佇列的末尾。如果要在執行佇列中上移規則，請轉至**資源 - 關聯器 -** <選定的關聯器> **- 編輯關聯器 - 關聯**，選取關聯規則旁的核取方塊，然後點擊**上移**或**下移**按鈕來根據需要重新排序規則。

- **刪除**— 用於取消關聯規則與關聯器的連結。

簡單關聯規則

簡單關聯規則用於定義簡單的事件序列。

關聯規則視窗包含下列設定頁籤：

- **一般**— 用於指定關聯規則的主要設定。在此頁籤上，您可以選擇關聯規則的類型。

- **選擇器**— 用於定義已處理的事件必須滿足的條件才能觸發關聯規則。可用的設定因所選規則類型而異。

- **操作**— 用於設定在**選擇器**設定區塊中配置的條件滿足時啟動的觸發器。關聯規則必須至少包含一個觸發器。可用的設定因所選規則類型而異。
- **關聯器**— 用於連結關聯器。僅適用於已建立且可編輯的關聯規則。

一般頁籤

- **卡巴斯基儲存庫中的資源版本** - 資源版本號。此欄位不可編輯。僅適用於卡巴斯基提供的資源，並用於管理資源更新。
- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）— 擁有關聯規則的租用戶。
- **類型**（必填）— 用於選擇關聯規則類型的下拉清單。如果要建立簡單的關聯規則，請選擇**簡單**。
- **傳播欄位**（必填）— 用於事件選擇的事件欄位。如果觸發選擇器（見下文），這些欄位將寫入關聯事件。
- **觸發率限制**— 每秒可觸發關聯規則的最大次數。預設值是100。

  若採用複雜模式偵測邏輯的關聯規則未被觸發，原因可能在於KUMA中用於規則觸發計數的特定方法。此種情況下，可嘗試將**觸發率限制**的值提高至`1000000`（例如）。

- **優先順序** — 用於判定關聯規則重要性的基礎係數。預設值是`Low`。
- **描述**— 資源的描述。最多4,000個Unicode字元。

選擇器頁籤

簡單類型的規則只能有一個選擇器，其**設定**和**局部變數**頁籤可用。

設定頁籤包含具有**篩選器**設定群組的設定：

- **篩選器**（必填）— 用於設定決定應觸發選擇器的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。

  在資源中建立篩選器

  KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

  若要建立篩選器：

  1. 在**篩選器**下拉清單中，選擇**新建**。
  2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。

3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。

4. 在**條件**下，指定事件必須滿足的條件：

   a. 點擊**新增條件**按鈕。

   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。

   c. 在**運算子**下拉清單中，選擇一個運算子。

   篩選器運算子

   - **=** — 左運算元等於右運算元。
   - **<** — 左運算元小於右運算元。
   - **<=** — 左運算元小於或等於右運算元。
   - **>** — 左運算元大於右運算元。
   - **>=** — 左運算元大於或等於右運算元。
   - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
   - **contains** — 左運算元包含右運算元的值。
   - **startsWith** — 左運算元以右運算元的某個值開頭。
   - **endsWith** — 左運算元以右運算元的某個值末端。
   - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
   - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

     待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

     若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
   - **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

     如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
   - **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
   - **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
   - **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
   - **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。

- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。

- **inContextTable**檢查指定快顯表單中條目的存在情況。

- **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

基於「額外」事件欄位資料的篩選：

基於**額外**事件欄位資料的篩選器條件：

- 條件 —**如果**。
- 左運算元 —**事件欄位**。
- 在此事件欄位中，您可以指定以下其中一個值：
  - **Extra**欄位。
  - Extra 欄位中的值，格式如下：

    `Extra.<field name>`

    例如，`Extra.app`。

    這種類型的值需手動指定。

  - 寫入**Extra**欄位的陣列值須符合以下格式：

    `Extra.<field name>.<array element>`

    例如，`Extra.array.0`。

    陣列中的值從0開始編號。

    這種類型的值需手動指定。

    若要使用 Extra 欄位中深度為 3 或更深層的值，請使用反引號 ``。例如，`Extra.lev1.lev2.lev3`。
- 運算子 — =。
- 右運算元 —**常數**。
- 值 — 您需要用來篩選事件的值。

關聯規則的選擇器篩選器中指定的條件順序非常重要，它會影響系統效能。我們建議將最獨特的條件放在選擇器篩選器的第一位。

請考慮兩個在Microsoft Windows中選擇成功驗證事件的選擇器篩選器範例。

選擇器篩選器1：

條件1。DeviceProduct = Microsoft Windows

條件2。DeviceEventClassID = 4624

選擇器篩選器2：

條件1。DeviceEventClassID = 4624

條件2。DeviceProduct = Microsoft Windows

選擇器篩選器2中的條件順序更可取，因為它對系統造成的負載較小。

選擇**局部變數**頁籤，然後按一下**新增變數**以宣告要在此關聯規則限制內使用的變數。

操作頁籤

簡單類型的規則只能有一個觸發器：**在每個事件上**。每次選擇器觸發時都會啟動它。

觸發器的可用參數：

- **輸出**— 如果選取此核取方塊，則會將關聯事件傳送以進行後處理：用於擴充、回應和傳送至目標。
- **迴圈到關聯器**— 如果選取此核取方塊，則建立的關聯事件由目前關聯器的規則鏈處理。這允許分層關聯。

  如果設定了**輸出**和**迴圈到關聯器**核取方塊，則關聯規則首先被傳送到後處理，然後再傳送到目前關聯規則的選擇器。
- **不建立警示**— 如果選取此核取方塊，則觸發此關聯規則時不會建立警示。如果您不想在觸發關聯規則時建立警示，但仍想將關聯事件傳送到儲存體，請選取**輸出**和**不觸發警示**核取方塊。如果僅選取**不觸發警示**核取方塊，則關聯事件不會儲存在儲存體中。
- **擴充**設定群組 — 您可以使用擴充規則修改關聯事件的欄位。這些擴充規則儲存在建立它們的關聯規則中。您可以建立多個擴充規則。透過分別點選**新增擴充**或**移除資料補足**按鈕，可以新增或刪除擴充規則。

  - **來源類型**— 您可以在下拉清單中選擇擴充的類型。根據所選類型，可能會顯示其他也需要填寫的進階設定。

    可用的擴充類型：

    - **常數**

      當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定：

      - 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。
      - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

      若針對 `String`、`Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。

      若針對 `Array of strings`、`Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。

- **字典**

  如果需要從字典類型的**字典**中新增值，則使用此類擴充。

  在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。

  如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。

  例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。

  如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。

  例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。

- **表格**

  如果您需要從表格類型的**字典**中新增值，請使用此類擴充。

  在**字典名稱**下拉清單中選擇此擴充類型後，請選擇用於提供值的字典。在**鍵欄位**設定群組中，按一下**新增欄位**按鈕以選擇其值用於選擇字典條目的事件欄位。

  在**對應**表中，設定用於提供資料的字典欄位和用於接收資料的事件欄位：

  - 在**字典欄位**直欄中，選擇字典欄位。可用欄位取決於所選的字典資源。
  - 在 **KUMA 欄位**直欄中，選取要寫入值的事件欄位。對於某些選取的欄位（`*custom*` 與 `*flex*`），您可以在**標籤**直欄中，為寫入其中的資料指定名稱。

  可以透過點選**新增元素**按鈕來新增表格行。可以透過按一下✕按鈕來刪除直欄。

- **事件**

  當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定：

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。
  - 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。
  - 按一下🔧按鈕會開啟**轉換**視窗，您可以在其中使用**新增轉換**按鈕建立規則，在將原始資料寫入 KUMA 事件欄位前對其進行修改。

    可用的轉換

    轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。

    可用轉換類型：

    - **小寫** — 用於將值的所有字元變為小寫
    - **大寫** — 用於將值的所有字元變為大寫

- **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。

- **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。

- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：

  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。

  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。

- **修剪**—用於同時從值的開頭和結尾移除 **字元** 欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將 `Micromon` 值的 **修剪** 轉換套用至 `Microsoft-Windows-Sysmon`，結果為 `soft-Windows-Sys`。

- **追加**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的結尾。選擇此轉換類型時，將出現此欄位。

- **前置**—用於將 **常數** 欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。

- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。

  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。

  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。

- 將編碼字串轉換為文字：

  - **decodeHexString** —用於將HEX字串轉換為文字。

  - **decodeBase64String** —用於將Base64字串轉換為文字。

  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。

  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。

  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。

- **hexToDecimal** 會將十六進位數值轉換為其十進位表示形式。此轉換會套用至包含十六進位值（如果存在，則包括 0x 前置詞）的字串或數值欄位，並將結果以整數形式儲存在目標 KUMA 事件欄位中。此轉換會傳回一個十進位數字。例如，值 0x00FF 會轉換為 255。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

當您使用事件擴充功能，且在 **來源類型** 設定中選取 **事件**，並使用延伸事件結構描述的欄位作為引數時，須注意以下特殊事項：

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `String` 類型的欄位，則值會以 TSV 格式寫入目標欄位。

  範例：SA.StringArray 延伸事件結構描述欄位包含以下值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 DeviceCustomString1 事件結構描述欄位。操作結果為：DeviceCustomString1 欄位包含 ["string1", "string2", "string3"]。

- 如果來源欄位是 `Array of strings` 類型的欄位，而目標欄位是 `Array of strings` 類型的欄位，則來源欄位的值會附加至目標欄位的值，並存入目標欄位，以逗號 (",") 作為分隔符號。

  範例：延伸事件結構描述欄位 SA.StringArrayOne 包含值："string1"、"string2"、"string3"。事件擴充操作已執行完畢。操作結果會寫入 SA.StringArrayTwo 事件結構描述欄位。操作結果為：SA.StringArrayTwo 欄位包含 "string1"、"string2"、"string3"。

- **範本**

  當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

  - 在 **範本**欄位中，輸入 Go 範本。

    事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。

    範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。

  - 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

  若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

  如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

  範例：

  {{.SA.StringArrayOne}}

  範例：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **偵錯**— 您可以使用此切換開關來啟用服務操作的日誌記錄。
- **描述**— 資源的描述。最多4,000個Unicode字元。
- **篩選器**設定區塊 — 讓您選擇要轉發哪些事件進行擴充。組態如上所述執行。

- **分類** — 用於變更事件中指示的資產類別。可以有多個分類規則。您可以透過點選**新增分類**或**移除分類**按鈕來新增或刪除它們。只能將響應式類別新增至資產或從資產中刪除。
  - **操作**— 此下拉清單用於選擇要對類別執行的操作：
    - **新增**— 將類別指派給資產。
    - **刪除**— 將資產與類別解除綁定。
  - **事件欄位**— 指示需要操作的資產的事件欄位。
  - **類別 ID** — 下拉清單顯示類別樹，您可以在其中選擇要對其執行動作的類別。按一下此行可延伸清單。
- **活動清單更新**設定群組 — 用於指派活動清單一個或多個操作的觸發器。您可以點選**新增活動清單操作**和**刪除活動清單操作**按鈕分別新增或刪除活動清單操作。

  可用設定：
  - **名稱**（必要）— 此下拉清單用於選擇活動清單。
  - **操作**（必要）— 此下拉清單用於選擇必須執行的操作：
    - **求和**— 將常數、關聯事件欄位的值或局部變數的值新增至活動清單的值。
    - **取得**— 取得活動清單項目並將選定欄位的值寫入關聯事件。
    - **設定**— 透過建立新的或更新現有的活動清單條目，將關聯事件的選定欄位的值寫入活動清單。更新活動清單條目時，資料將合併，並且僅覆蓋指定的欄位。
    - **取得**— 取得活動清單項目並將選定欄位的值寫入關聯事件。
    - **刪除**— 刪除活動清單條目。
  - **鍵欄位**（必填）- 這是用於建立活動清單條目的事件欄位清單。它也用作活動清單條目的鍵。

    > 活動清單條目的鍵取決於可用欄位，而不取決於它們在KUMA主控台中的顯示順序。

  - **對應**（**取得**和**設定**操作必填）- 用於將活動清單欄位與事件欄位進行對應。可以設定多個對應規則。
    - 左側欄位用於指定活動清單欄位。

      > 此欄位不得僅包含特殊字元或數字。

- 中間下拉清單用於選擇事件欄位。
- 選擇**設定**操作時，右側欄位可用於為活動清單欄位指派常數。

- 在快顯表單更新下，您可以為一個或多個快顯表單操作指派觸發器。您可以按一下**新增背景脈絡表格操作**或**刪除背景脈絡表格操作**來新增或刪除快顯表單操作。
- 可用設定：
- 名稱（必填）- 此下拉清單用於選擇快顯表單資源。
- 操作（必填）- 此下拉清單用於選擇必須執行的操作。
- 求和 - 將常數、關聯事件欄位的值或局部變數的值加到快顯表單的值中。此操作僅適用於數字和浮點類型的欄位。
- 設定 - 透過建立新的或更新現有的快顯表單條目，將關聯事件的選定欄位的值寫入快顯表單。更新快顯表單條目時，資料將合併，並且僅覆蓋指定的欄位。
- 取得—取得快顯表單的欄位，並將指定欄位的值寫入關聯事件。布林類型的表欄位和布林值清單不包括在對應中，因為事件不包含布林欄位。
- 合併—將關聯事件欄位、局部變數或常數的值附加到快顯表單欄位的目前值。
- 刪除—刪除快顯表單條目。
- 鍵欄位（必填）—這是用於建立快顯表單條目的事件欄位清單。它也用作快顯表單條目的鍵。作為鍵欄位，您可以指定在**選擇器**頁籤上宣告的事件欄位或局部變數。
- 快顯表單條目的複合鍵僅取決於欄位的值，而不取決於它們在KUMA主控台中的顯示順序。
- 對應（除**刪除**之外的所有操作都需要）—用於將快顯表單欄位對應到事件欄位或變數。可以設定多個對應規則。您可以多次指定相同的快顯表單欄位。
- 左側欄位用於指定快顯表單欄位。
- 此欄位不得包含對應中已使用的欄位名稱、頁籤字元、特殊字元或僅包含數字。最大字元數是128。名稱不能以底線字元開頭。
- 中間下拉清單用於選擇事件欄位或局部變數。
- 如果選擇了**設定**操作，則右側欄位可用於將常數指派給快顯表單欄位。例如，**合併**或**求和**。最大字元數是1,024。

關聯器頁籤

- **新增**— 用於編輯已建立的關聯規則。您可以按一下**新增**開啟**關聯器**視窗，然後從清單中選擇一個關聯器。按一下**確定**後，規則將連結到選定的關聯器。您可以同時選擇多個關聯器。規則將會新增到執行佇列的末尾。如果要在執行佇列中上移規則，請轉至**資源 - 關聯器 -** <選定的關聯器> **- 編輯關聯器 - 關聯**，選取關聯規則旁的核取方塊，然後點擊上移或下移按鈕來根據需要重新排序規則。
- **刪除**— 用於取消關聯規則與關聯器的連結。

操作關聯規則

操作關聯規則用於處理活動清單。

關聯規則視窗包含以下頁籤：

- **一般**— 用於指定關聯規則的主要設定。在此頁籤上，您可以選擇關聯規則的類型。
- **選擇器**— 用於定義已處理的事件必須滿足的條件才能觸發關聯規則。可用的設定因所選規則類型而異。
- **操作**— 用於設定在**選擇器**設定區塊中配置的條件滿足時啟動的觸發器。關聯規則必須至少包含一個觸發器。可用的設定因所選規則類型而異。
- **關聯器**— 用於連結關聯器。僅適用於已建立且可編輯的關聯規則。

一般頁籤

- **卡巴斯基儲存庫中的資源版本** - 資源版本號。此欄位不可編輯。僅適用於卡巴斯基提供的資源，並用於管理資源更新。
- **名稱**（必要）—此類資源的唯一名稱。必須包含1至255個Unicode字元。
- **租用戶**（必填）— 擁有關聯規則的租用戶。
- **類型**（必填）— 用於選擇關聯規則類型的下拉清單。如果要建立操作關聯規則，請選擇**操作**。
- **觸發率限制**— 每秒可觸發關聯規則的最大次數。預設值是100。

  若採用複雜模式偵測邏輯的關聯規則未被觸發，原因可能在於KUMA中用於規則觸發計數的特定方法。此種情況下，可嘗試將**觸發率限制**的值提高至`1000000`（例如）。

- **描述**— 資源的描述。最多4,000個Unicode字元。

選擇器頁籤

操作類型的規則只能有一個選擇器，**設定**和**局部變數**頁籤可用於此選擇器。

設定頁籤包含具有**篩選器**設定群組的設定：

- **篩選器**（必填）— 用於設定決定應觸發選擇器的事件的條件。您可以從下拉清單中選擇現有篩選器，或建立新的篩選器。

  在資源中建立篩選器

KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

若要建立篩選器：

1. 在**篩選器**下拉清單中，選擇**新建**。
2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。
4. 在**條件**下，指定事件必須滿足的條件：
   a. 點擊**新增條件**按鈕。
   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。
   c. 在**運算子**下拉清單中，選擇一個運算子。

   篩選器運算子

   - **=** — 左運算元等於右運算元。
   - **<** — 左運算元小於右運算元。
   - **<=** — 左運算元小於或等於右運算元。
   - **>** — 左運算元大於右運算元。
   - **>=** — 左運算元大於或等於右運算元。
   - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
   - **contains** — 左運算元包含右運算元的值。
   - **startsWith** — 左運算元以右運算元的某個值開頭。
   - **endsWith** — 左運算元以右運算元的某個值末端。
   - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
   - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。

     待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。

     若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
   - **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。

     如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。

- **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
- **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
- **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
- **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
- **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
- **inContextTable**檢查指定快顯表單中條目的存在情況。
- **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、 **InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。

e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

您可以新增多個條件或一組條件。

5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、 **or**、**not**）。

6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

基於「額外」事件欄位資料的篩選：

基於**額外**事件欄位資料的篩選器條件：

- 條件 —**如果**。
- 左運算元 —**事件欄位**。
- 在此事件欄位中，您可以指定以下其中一個值：
  - **Extra**欄位。
  - Extra 欄位中的值，格式如下：

    `Extra.<field name>`

    例如，`Extra.app`。

    這種類型的值需手動指定。
  - 寫入**Extra**欄位的陣列值須符合以下格式：

    `Extra.<field name>.<array element>`

    例如，`Extra.array.0`。

    陣列中的值從0開始編號。

    這種類型的值需手動指定。

若要使用 Extra 欄位中深度為 3 或更深層的值，請使用反引號 ``。例如，`Extra.lev1.lev2.lev3`。

- 運算子 — =。
- 右運算元 —**常數**。
- 值 — 您需要用來篩選事件的值。

在**局部變數**頁籤上，按一下**新增變數**以宣告要在此關聯規則限制內使用的變數。

操作頁籤

操作類型的規則只能有一個觸發器：**在每個事件上**。每次選擇器觸發時都會啟動它。

觸發器的可用參數：

- **活動清單更新**設定群組 — 用於為一或多個使用活動清單的操作指派觸發器。您可以點選**新增活動清單操作**和**刪除活動清單操作**按鈕分別新增或刪除活動清單操作。

  可用設定：

  - **名稱**（必要）— 此下拉清單用於選擇活動清單。
  - **操作**（必要）— 此下拉清單用於選擇必須執行的操作：
    - **求和**— 將常數、關聯事件欄位的值或局部變數的值新增至活動清單的值。
    - **設定**— 透過建立新的或更新現有的活動清單條目，將關聯事件的選定欄位的值寫入活動清單。更新活動清單條目時，資料將合併，並且僅覆蓋指定的欄位。
    - **刪除**— 刪除活動清單條目。
  - **鍵欄位**（必填） - 這是用於建立活動清單條目的事件欄位清單。它也用作活動清單條目的鍵。

    > 活動清單條目的鍵取決於可用欄位，而不取決於它們在KUMA主控台中的顯示順序。

  - **對應**（**設定**操作必填）—用於將活動清單欄位與事件欄位對應。可以設定多個對應規則。
    - 左側欄位用於指定活動清單欄位。

      > 此欄位不得僅包含特殊字元或數字。

    - 中間下拉清單用於選擇事件欄位。
    - 選擇**設定**操作時，右側欄位可用於為活動清單欄位指派常數。
- 在**快顯表單更新**下，您可以為一個或多個快顯表單操作指派觸發器。您可以按一下**新增背景脈絡表格操作**或**刪除背景脈絡表格操作**來新增或刪除快顯表單操作。

可用設定：

- **名稱**（必填）—此下拉清單用於選擇快顯表單資源。
- **操作**（必填）—此下拉清單用於選擇必須執行的操作。
  - **求和**—將常數、關聯事件欄位的值或局部變數的值加到快顯表單的值中。此操作僅適用於數字和浮點類型的欄位。
  - **設定**—透過建立新的或更新現有的快顯表單條目，將關聯事件的選定欄位的值寫入快顯表單。更新快顯表單條目時，資料將合併，並且僅覆蓋指定的欄位。
  - **合併**—將關聯事件欄位、局部變數或常數的值附加到快顯表單欄位的目前值。
  - **刪除**—刪除快顯表單條目。
- **鍵欄位**（必填）—這是用於建立快顯表單條目的事件欄位清單。它也用作快顯表單條目的鍵。作為金鑰欄位，您可以指定事件欄位或在「選取器」索引標籤上宣告的區域變數。

  > 快顯表單條目的複合鍵僅取決於欄位的值，而不取決於它們在KUMA主控台中的顯示順序。

- **對應**（除**刪除**外的所有操作都需要）— 用於將情境表欄位對應到事件欄位或變數。可以設定多個對應規則。您可以多次指定相同的快顯表單欄位。
  - 左側欄位用於指定快顯表單欄位。

    此欄位不得包含對應中已使用的欄位名稱、頁籤字元、特殊字元或僅包含數字。最大字元數是128。名稱不能以底線字元開頭。
  - 中間下拉清單用於選擇事件欄位或局部變數。
  - 您可以使用右側欄位將常數指派給快顯表單欄位。最大字元數是1,024。

關聯器頁籤

- **新增**— 用於編輯已建立的關聯規則。您可以按一下**新增**開啟**關聯器**視窗，然後從清單中選擇一個關聯器。按一下**確定**後，規則將連結到選定的關聯器。您可以同時選擇多個關聯器。規則將會新增到執行佇列的末尾。如果要在執行佇列中上移規則，請轉至**資源 - 關聯器 -** <選定的關聯器> **- 編輯關聯器 - 關聯**，選取關聯規則旁的核取方塊，然後點擊上移或下移按鈕來根據需要重新排序規則。
- **刪除**— 用於取消關聯規則與關聯器的連結。

關聯器中的變數

如果追蹤事件欄位、活動清單或字典中的值不足以涵蓋某些特定的安全場景，則可以使用全域和局部*變數*。您可以使用它們透過實作複雜的威脅偵測邏輯對關聯器收到的值執行各種操作。可以在關聯器（*全域變數*）或關聯規則（*局部變數*）中宣告變數，方法是向它們指派一個函式，然後從關聯規則中查詢它們，就好像它們是普通的事件欄位一樣，並在回應中接收觸發的函式結果。

變數的使用範圍：

- 在關聯規則中搜尋分組欄位值或唯一欄位值時。
- 在關聯規則選擇器中，於用來判斷是否應觸發關聯規則的條件篩選器內。
- 在擴充關聯事件時。將**事件**選為來源類型。
- 使用值填入活動清單時。

可以像查詢事件欄位一樣查詢變數，只需在其名稱前加上「$」字元。

相同和唯一欄位中的局部變數

您可以在「標準」類型關聯規則的**相同欄位**和**唯一欄位**部分中使用局部變數。要使用局部變量，其名稱前面必須帶有「$」字元。

有關在**相同欄位**和**唯一欄位**部分中使用局部變數的範例，請參閱KUMA提供的規則：R403_從停用防護的主機或過時的病毒資料庫存取惡意資源。

選擇器中的局部變數

若要在選擇器中使用局部變數：

1. 將局部變數新增至規則。
2. 在**關聯規則**視窗中，轉到**常規**頁籤，然後將建立的局部變數新增至**相同欄位**部分。在局部變數名稱前加上「$」字元。
3. 在**關聯規則**視窗中，請轉至**選擇器**頁籤，選擇現有篩選器或建立新篩選器，然後按一下**新增條件** 。
4. 將**事件欄位**選為運算元。
5. 選擇局部變數作為事件欄位值，並在變數名稱前加上「$」字元。
6. 指定其餘篩選器設定。
7. 按一下**儲存**按鈕。

有關使用局部變數的範例，請參閱KUMA提供的規則：R403_從停用防護的主機或過時的病毒資料庫存取惡意資源。

事件擴充中的局部變數

您可以使用「標準」和「簡單」關聯規則來用局部變數擴充事件。

使用文字和數字進行擴充

您可以使用文字（字串）擴充事件。為此，您可以使用修改字串的函式：to_lower、to_upper、str_join、append、prepend、substring、tr、replace、str_join。

您可以使用數字擴充事件。為此，您可以使用以下函式：加法（「+」）、減法（「-」）、乘法（「*」）、除法（「/」）、round、ceil、floor、abs、pow。

您也可以使用規則運算式來管理局部變數中的資料。

與其他操作相比，在關聯規則中使用規則運算式在運算上非常耗費資源。因此，在設計關聯規則時，我們建議將規則運算式的使用限制在必要的最小值，並使用其他可用的操作。

時間戳擴充

您可以使用時間戳（日期和時間）擴充事件。為此，您可以使用允許您取得或修改時間戳記的函式：now、extract_from_timestamp、parse_timestamp、format_timestamp、truncate_timestamp、time_diff。

使用活動清單和表格的函式

您可以使用局部變數以及來自活動清單和表格的資料來擴充事件。

若要使用活動清單的資料來豐富事件，請使用active_list和 active_list_dyn函式。

若要使用來自表格的資料來擴充事件，請使用table_dict和dict函式。

您可以使用局部變數中的「conditional」函式建立條件語句。這樣，變數可以根據收到的待處理資料傳回其中一個值。

使用局部變數擴充事件

若要使用局部變數擴充事件：

1. 將局部變數新增至規則。
2. 在**關聯規則**視窗中，轉到**常規**頁籤，然後將建立的局部變數新增至**相同欄位**部分。在局部變數名稱前加上「$」字元。
3. 在**關聯規則**視窗中，轉到**操作**頁籤，然後在**擴充**功能下的**來源類型**下拉列表中，選擇**事件**。
4. 從**目標欄位**下拉清單中，選擇要將局部變數的值傳遞給的KUMA事件欄位。
5. 從**來源欄位**下拉清單中，選擇一個局部變數。在局部變數名稱前加上「$」字元。
6. 指定其餘規則設定。
7. 按一下**儲存**按鈕。

活動清單擴充中的局部變數

您可以使用局部變數來擴充活動清單。

若要使用局部變數擴充活動清單：

1. 將局部變數新增至規則。
2. 在**關聯規則**視窗中，轉到**常規**頁籤，然後將建立的局部變數新增至**相同欄位**部分。在局部變數名稱前加上「$」字元。

3. 在**關聯規則**視窗中，轉至**操作**頁籤，在**活動清單更新**下，將局部變數新增至**鍵欄位**欄位。在局部變數名稱前加上「$」字元。

4. 在**對應**下，指定事件欄位和活動清單欄位之間的對應關係。

5. 按一下**儲存**按鈕。

變數的內容

局部變數和全域變數

全域變數的內容與局部變數的內容不同。

全域變數：

- 全域變數在關聯器層級宣告，並且僅在該關聯器的範圍內套用。
- 可以從關聯器中指定的所有關聯規則中查詢關聯器的全域變數。
- 在標準關聯規則中，同一個全域變數在每個選擇器中可以取不同的值。
- 無法在不同的關聯器之間傳輸全域變數。

局部變數：

- 局部變數在關聯規則層級宣告，並且僅在該規則的限制範圍內應用。
- 在標準關聯規則中，局部變數的範圍僅由宣告該變數的選擇器組成。
- 局部變數可以在任何類型的關聯規則中宣告。
- 局部變數不能在規則或選擇器之間傳輸。
- 局部變數不能用作全域變數。

各種關聯規則中使用的變數

- 在**操作**關聯規則的**操作**頁籤上，您可以指定此規則中可用或宣告的所有變數。
- 在**標準**關聯規則的**操作**頁籤上，您只能在**一般**頁籤的**相同欄位**欄位中提供這些規則中指定的變數。
- 在**簡單**關聯規則的**操作**頁籤上，您只能在**一般**頁籤上的**繼承欄位**欄位中提供這些規則中指定的變數。

變數的需求

當新增變數函式時，必須先指定函式的名稱，然後在括號中列出其參數。基本數學運算（加、減、乘、除）是此需求的例外。使用這些運算時，括號用於指定運算的嚴重等級。

函式名稱的要求：

- 在關聯器內必須是唯一的。
- 必須包含1至255個Unicode字元。
- 不能以字元「$」開頭。
- 必須以駝峰式大小寫命名。

指定變數函式時的特殊注意事項：

- 參數的順序很重要。
- 參數以逗號分隔：**,**。
- 字串參數以單引號傳遞：**'**。
- 事件欄位名稱和變數在指定時不帶引號。
- 將變數作為參數查詢時，請在其名稱前新增 **$** 字元。
- 您不需要在參數之間新增空格。
- 在所有可以使用變數作為參數的函式中，都可以建立巢狀函式。

變數的函式

使用活動清單和字典的操作

active_list and active_list_dyn

這些函式允許您從活動清單中接收資訊，併為活動清單和金鑰動態生成欄位名稱。

您必須依以下順序指定參數：

1. 活動列表名稱。
2. 傳回活動清單欄位名稱的運算式
3. 一個或多個運算式，其結果構成金鑰

使用範例	結果
`active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2), to_lower(DeviceCustomString1))`	獲取活動清單的欄位值。

使用此函式可從變數中存取共享租用戶的活動清單。為此，請在作用中清單的名稱後新增尾碼 @Shared（區分大小寫）。例如，active_list('exampleActiveList@Shared', 'score', SourceAddress, SourceUserName)。

table_dict

獲取有關表格型別字典中指定列的值的資訊。

您必須依以下順序指定參數：

1. 字典名稱
2. 字典資料行名稱
3. 一或多個運算式，其結果構成字典字串金鑰

使用範例	結果
`table_dict('exampleTableDict', 'office', SourceUserName)`	從 `exampleTableDict` 字典中，取得金鑰為 `SourceUserName` 的行在 `office` 列中的資料。
`table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))`	從 `exampleTableDict` 字典中，取得複合金鑰字串所對應的行在 `office` 列中的資料，該複合金鑰字串由 `SourceAddress` 欄位值和 `SourceUserName` 欄位的小寫值組成。

使用此函式可從變數中存取共享租用戶的字典。為此，請在活動清單的名稱後新增 `@Shared` 尾碼（區分大小寫）。例如，`table_dict('exampleTableDict@Shared', 'office', SourceUserName)`。

dict

獲取有關字典型別字典的指定列中值的資訊。

您必須依以下順序指定參數：

1. 字典名稱
2. 一個或多個運算式，其結果用於產生字典行金鑰

使用範例	結果
`dict('exampleDictionary', SourceAddress)`	從 `exampleDictionary` 中，取得金鑰為 `SourceAddress` 的行中的資料。
`dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))`	從 `exampleDictionary` 中取得資料，使用由 `SourceAddress` 欄位值和 `SourceUserName` 欄位的小寫值組成的複合金鑰字串。

使用此函式可從變數中存取共享租用戶的字典。為此，請在活動清單的名稱後新增 `@Shared` 尾碼（區分大小寫）。例如，`dict('exampleDictionary@Shared', SourceAddress)`。

使用快顯表單的操作

context_table

傳回基本類型（例如，整數、整數陣列）中指定欄位的值。

您必須依以下順序指定參數：

1. 快顯表單的名稱。必須指定名稱。
2. 傳回快顯表單的欄位名稱的運算式。
3. 傳回快顯表單的鍵欄位1名稱的運算式。
4. 傳回快顯表單的鍵欄位1值的運算式。

此函式必須至少包含4個參數。

使用範例	結果
`context_table('tbl1', 'list_field1', 'key1', 'key1_val')`	`Get the value of the specified field. If the context table or context table field does not exist, an empty string is returned.`

len

傳回字串或陣列的長度。

如果傳遞的陣列屬於以下類型之一，則該函式傳回陣列的長度：

- 整數陣列
- 浮點陣列
- 字串陣列
- 布林陣列

如果傳遞了不同類型的陣列，則陣列的資料將轉換為字串類型，並且該函式會傳回結果字串的長度。

使用範例
`len(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`len(DeviceCustomString1)`

distinct_items

傳回陣列中唯一元素的清單。

如果傳遞的陣列屬於以下類型之一，則函式傳回陣列的唯一元素清單：

- 整數陣列
- 浮點陣列
- 字串陣列
- 布林陣列

如果傳遞了不同類型的陣列，則陣列的資料將轉換為字串類型，並且該函式會傳回由原始字串中唯一字元組成的字串。

使用範例
`distinct_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))`
`distinct_items(DeviceCustomString1)`

sort_items

傳回陣列元素的排序清單。

您必須依以下順序指定參數：

1. 傳回排序物件的運算式
2. 排序順序 可能的值： `asc`、`desc`。若未指定參數，則預設值為 `asc`。

如果傳遞的陣列屬於下列類型之一，則函式傳回陣列的排序元素清單：

- 整數陣列
- 浮點陣列
- 字串陣列

對於布林陣列，該函式會依原始順序傳回陣列元素清單。

如果傳遞了不同類型的陣列，則陣列的資料將轉換為字串類型，並且該函式會傳回排序後的字串。

使用範例
`sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')`
`sort_items(DeviceCustomString1)`

item

如果傳遞的是整數、浮點數、字串或布林值陣列，則傳回具有指定索引的陣列元素或具有指定索引的字串的字元。

您必須依以下順序指定參數：

1. 傳回索引物件的運算式
2. 傳回元素或字元索引的運算式

此函式必須至少包含2個參數。

如果索引在陣列範圍內且傳遞的陣列屬於下列類型之一，則函式會傳回具有指定索引的陣列元素或具有指定索引的字串字元：

- 整數陣列
- 浮點陣列
- 字串陣列
- 布林陣列

如果傳遞了不同類型的陣列且索引在陣列範圍內，則資料將轉換為字串類型，並且函式傳回具有指定索引的字串字元。如果傳遞了不同類型的陣列並且索引超出了陣列範圍，則函式會傳回空字串。

使用範例
`item(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 1)`
`item(DeviceCustomString1, 0)`

to_lower

將字串中的字元轉換為小寫。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

字串可以作為字串、欄位名稱或變數傳遞。

使用範例
`to_lower(SourceUserName)`
`to_lower('SomeText')`
`to_lower($otherVariable)`

to_upper

將字串中的字元轉換為大寫。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。字串可以作為字串、欄位名稱或變數傳遞。

使用範例
`to_upper(SourceUserName)`
`to_upper('SomeText')`
`to_upper($otherVariable)`

append

在字串末尾新增字元。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 新增字串

字串可以作為字串、欄位名稱或變數傳遞。

使用範例	使用結果
`append(Message, '123')`	字串 `123` 被新增至來自 `Message` 欄位的此字串末尾。
`append($otherVariable, 'text')`	字串 `text` 被新增至來自變數 `otherVariable` 的此字串末尾。
`append(Message, $otherVariable)`	來自 `otherVariable` 的字串被新增至來自 `Message` 欄位的此字串末尾。

prepend

在字串開頭新增字元。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 新增字串

字串可以作為字串、欄位名稱或變數傳遞。

使用範例	使用結果
`prepend(Message, '123')`	字串 `123` 被新增至來自 `Message` 欄位的此字串開頭。
`prepend($otherVariable, 'text')`	字串 `text` 被新增至來自 `otherVariable` 的此字串開頭。
`prepend(Message, $otherVariable)`	來自 `otherVariable` 的字串被新增至來自 `Message` 欄位的此字串開頭。

substring

傳回字串中的子字串。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 子字串起始位置（自然數或0）。
3. 子字串結束位置（選用）。

字串可以作為字串、欄位名稱或變數傳遞。如果位置編號大於原始資料字串長度，則傳回空字串。

使用範例	使用結果
`substring(Message, 2)`	傳回來自 `Message` 欄位的字串的一部分：從第 3 個字元到末尾。
`substring($otherVariable, 2, 5)`	傳回來自 `otherVariable` 變數的字串的一部分：3 至 6 個字元。
`substring(Message, 0, len(Message) - 1)`	傳回來自 `Message` 欄位的完整字串，但排除最後一個字元。

index_of

`index_of` 函式會傳回字元或子字串在字串中的位元組偏移量；字串中第一個字元的索引值為 0。若函式沒有找到子字串，則會傳回負值。

如果字串包含非ASCII字符，則傳回的位元組偏移量將與要搜尋的子字串前面的字元數不對應。

此函式接受以下參數：

- 作為來源資料、事件欄位、其他變數或常數
- 局部變數中可用的任何運算式。

若要使用此函式，必須按以下順序指定參數：

1. 要尋找其位置的字元或子字串。
2. 要搜尋的字串。

使用範例	使用結果
`index_of('@', SourceUserName)`	此函式會在 `SourceUserName` 欄位中尋找 `@` 字元。`SourceUserName` 欄位包含 `user@example.com` 字串。 Result = 4. 此函式傳回字串中第一次出現的字元的索引。字串中第一個字元的索引為0。

`index_of('m', SourceUserName)`	此函式會在 `SourceUserName` 欄位中尋找 `m` 字元。`SourceUserName` 欄位包含 `user@example.com` 字串。 Result = 8. 此函式傳回字串中第一次出現的字元的索引。字串中第一個字元的索引為0。

last_index_of

`last_index_of` 函式會傳回字元或子字串在字串中最後一次出現的位置；字串中的第一個字元索引值為 0。若函式沒有找到子字串，則會傳回 -9223372036854775808。

此函式接受以下參數：

- 作為來源資料、事件欄位、其他變數或常數
- 局部變數中可用的任何運算式。

若要使用此函式，必須按以下順序指定參數：

1. 要尋找其位置的字元或子字串。
2. 要搜尋的字串。

使用範例	使用結果
`last_index_of('m', SourceUserName)`	此函式會在 `SourceUserName` 欄位中尋找 `m` 字元。`SourceUserName` 欄位包含 `user@example.com` 字串。 Result = 15. 此函式傳回字串中最後一次出現的字元的索引。字串中第一個字元的索引為0。

tr

從字串的開頭和結尾刪除指定的字元。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 要從原始字串的開頭和結尾刪除的子字串（選用）

字串可以作為字串、欄位名稱或變數傳遞。如果不指定要刪除的字串，則會從原始字串的首尾刪除空格。

使用範例	使用結果
`tr(Message)`	已從 `Message` 欄位中字串的開頭和結尾移除空格。
`tr($otherVariable, '_')`	如果 `otherVariable` 變數的值為 `_test_`，則會傳回字串 `_test_`。
`tr(Message, '@example.com')`	如果 `Message` 事件欄位包含字串 `user@example.com`，則會傳回字串 `user`。

取代

將字串中所有出現的字元序列 A 取代為字元序列 B。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 搜尋字串：要替換的字元序列。
3. 替換字串：用於替換搜尋字串的字元序列。

字串可以作為運算式傳遞。

使用範例	使用結果
`replace(Name, 'UserA', 'UserB')`	傳回來自 `Name` 事件欄位的字串，其中出現的所有 `UserA` 皆替換為 `UserB`。
`replace($otherVariable, ' text ', '_text_')`	傳回來自 `otherVariable` 的字串，其中出現的所有 `' text'` 皆替換為 `'_text_'`。

regexp_replace

將符合規則運算式的字元序列，替換為包含規則運算式擷取群組的字元序列。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 搜尋字串：規則運算式。
3. 替換字串：用於替換搜尋字串的字元序列，以及規則運算式擷取群組的ID。字串可以作為運算式傳遞。

字串可以作為字串、欄位名稱或變數傳遞。可以使用未命名的擷取群組。

在變數函式使用的規則運算式中，每個反斜線字元必須額外進行跳脫處理。例如，必須使用 `^example\\\\`，而不是規則運算式 `^example\\`。

使用範例	使用結果
`regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')`	傳回來自 `SourceAddress` 事件欄位的字串，其中文字 `newIP` 會插入到 IP 位址之前。此外，位址的最後幾位數字將被替換為 `10`。

regexp_capture

從原始字串中取得符合規則運算式條件的結果。支援標準欄位以及 `string` 類型的延伸事件結構描述欄位。

您必須依以下順序指定參數：

1. 原始字串
2. 搜尋字串：規則運算式。

字串可以作為字串、欄位名稱或變數傳遞。可以使用未命名的擷取群組。

在變數函式使用的規則運算式中，每個反斜線字元必須額外進行跳脫處理。例如，必須使用 `^example\\\\`，而不是規則運算式 `^example\\`。

使用範例	範例值	使用結果
`regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})')`	`Message = 'Access from 192.168.1.1 session 1'` `Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'`	`'192.168.1.1'` `'45.45.45.45'`

範本

傳回函式中指定的字串，其中變數會替換為其值。可以透過以下方式傳遞用於替換的變數：

- 在字串內。
- 在字串後面。此種情況下，您必須在字串內以 `{{index.<n>}}` 標記法指定變數，其中 <n> 代表字串之後傳遞的變數索引值。索引值以0為基礎。

使用範例
`template('Very long text with values of rule={{.DeviceCustomString1}} and {{.Name}} event fields, as well as values of {{index.0}} and {{index.1}} local variables and then {{index.2}}', $var1, $var2, $var10)`

使用時間戳的操作

Now函式

獲取epoch格式的時間戳。無需參數即可運作。

使用範例
`now()`

extract_from_timestamp

從時間戳epoch格式的欄位和變數中獲取原子時間表示（年、月、日、時、分、秒、星期幾）。

必須依照以下順序指定參數：

1. 時間戳類型的事件欄位或變數。
2. 原子時間表示的表示法。此參數區分大小寫。

原子時間表示法的可能變體：

- y表示數字格式的年份。
- M表示數字格式的月份。
- d表示月份中的日期。
- wd表示星期幾：星期一、星期二、星期三、星期四、星期五、星期六、星期日。
- h表示小時，24小時制。
- m表示分鐘。
- s表示秒。

3. 時區標示（選用）。

   參數可以指定為字串（例如 `Europe/Moscow`），或指定為變數（`$timezone`）。變數必須在關聯規則的局部變數中宣告。變數的值必須包含時區的字串識別碼。也允許使用從其他變數和字典值派生的變數。

   如果未指定此參數，則以UTC格式計算時間。

使用範例
`extract_from_timestamp(Timestamp, 'wd')`
`extract_from_timestamp(Timestamp, 'h')`
`extract_from_timestamp($otherVariable, 'h')`
`extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')`
`extract_from_timestamp(Timestamp, 'h', $timezone)`

使用範例：使用從字典中取得的變數

`$key_timezone = 'timezone'`
 	
`$timezone = dict('UEBA.Timezone', $key_timezone)`
 	
`extract_from_timestamp(EndTime, 'h', $timezone)`

在此範例中，`$timezone` 變數衍生自另一個變數和字典值，並用作 `timezone` 參數。

parse_timestamp

將時間從 RFC3339 格式（例如 `2022-05-24 00:00:00`、`2022-05-24 00:00:00+0300`）轉換為 epoch 格式。

使用範例
`parse_timestamp(Message)`
`parse_timestamp($otherVariable)`

format_timestamp

將時間從epoch格式轉換為RFC3339格式。

必須依照以下順序指定參數：

1. 時間戳類型的事件欄位或變數。
2. 時間格式表示法：RFC3339。
3. （可選）時區表示法。如果未指定此參數，則以UTC格式計算時間。

使用範例
`format_timestamp(Timestamp, 'RFC3339')`
`format_timestamp($otherVariable, 'RFC3339')`
`format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')`

truncate_timestamp

以epoch格式舍入時間。舍入後，以epoch格式返回時間。時間向下舍入。

必須依照以下順序指定參數：

1. 時間戳類型的事件欄位或變數。
2. 舍入參數：
   - 1s向下舍入到秒。
   - 1m向下舍入到分鐘。
   - 1h向下舍入到小時。
   - 24h向下舍入到天。
3. 時區標示（選用）。如果未指定此參數，則以UTC格式計算時間。

使用範例	舍入值範例	使用結果
`truncate_timestamp(Timestamp, '1m')`	1654631774175 (2022年6月7日 19:56:14.175)	1654631760000 (2022年6月7日 19:56:00)
`truncate_timestamp($otherVariable, '1h')`	1654631774175 (2022年6月7日 19:56:14.175)	1654628400000 (2022年6月7日 19:00:00)
`truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')`	1654631774175 (2022年6月7日 19:56:14.175)	1654560000000 (2022年6月7日 0:00:00)

time_diff

以epoch格式獲取兩個時間戳之間的時間間隔。

必須依照以下順序指定參數：

1. 間隔結束時間。時間戳類型的事件欄位或變數。
2. 間隔開始時間。時間戳類型的事件欄位或變數。

3. 時間間隔表示法：

- ms表示毫秒。
- s表示秒。
- m表示分鐘。
- h表示小時。
- d表示天。

使用範例
`time_diff(EndTime, StartTime, 's')`
`time_diff($otherVariable, Timestamp, 'h')`
`time_diff(Timestamp, DeviceReceiptTime, 'd')`

數學運算

這些由基本數學運算和函式組成。

基本數學運算

支援延伸事件結構的整數和浮點欄位。

運算：

- 加法
- 減法
- 乘法
- 除法
- 模除

括號決定操作順序

可用的參數：

- 數字事件欄位
- 數字變數
- 實數
  模除時，只能使用自然數作為參數。

使用限制：

- 除以零返回零。
- 對數字和字串執行數學運算時，傳回的數字維持不變。例如，1+abc返回1。

- 傳回運算結果的整數不帶點。

使用範例 (Type=3; otherVariable=2; Message=text)	使用結果
Type + 1	4
$otherVariable - Type	-1
2 * 2.5	5
2 / 0	0
Type * Message	0
(Type + 2) * 2	10
Type % $otherVariable	1

round

舍入數字。支援延伸事件結構的整數和浮點欄位。

可用參數：

- 數字事件欄位
- 數字變數
- 數字常數

使用範例 (DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)	使用結果
round(DeviceCustomFloatingPoint1)	8
round(DeviceCustomFloatingPoint2)	8
round($otherVariable)	7

ceil

向上舍入數字。支援延伸事件結構的整數和浮點欄位。

可用參數：

- 數字事件欄位
- 數字變數
- 數字常數

使用範例 (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	使用結果
ceil(DeviceCustomFloatingPoint1)	8
ceil($otherVariable)	9

floor

向下舍入數字。支援延伸事件結構的整數和浮點欄位。

可用參數：

- 數字事件欄位
- 數字變數
- 數字常數

使用範例 (DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)	使用結果
floor(DeviceCustomFloatingPoint1)	7
floor($otherVariable)	8

abs

獲取數字的模數。支援延伸事件結構的整數和浮點欄位。

可用參數：

- 數字事件欄位
- 數字變數
- 數字常數

使用範例 (DeviceCustomNumber1=-7; otherVariable=-2)	使用結果
abs(DeviceCustomFloatingPoint1)	7
abs($otherVariable)	2

pow

對數字求冪。支援延伸事件結構的整數和浮點欄位。

必須依照以下順序指定參數：

1. 底數—實數。
2. 指數 — 自然數。

可用的參數：

- 數字事件欄位
- 數字變數
- 數字常數

使用範例
pow(DeviceCustomNumber1, DeviceCustomNumber2)
pow($otherVariable, DeviceCustomNumber1)

str_join

使用分隔符號將多個字串合併為一個。支援延伸事件結構的整數和浮點欄位。

必須依照以下順序指定參數：

1. 分隔符號。字串。
2. 字串1、字串2、字串N。至少2個運算式。

使用範例	使用結果
`str_join('|', to_lower(Name), to_upper(Name), Name)`	字串。

條件式

如果滿足條件，則取得一個值，如果不滿足條件，則取得另一個值。支援延伸事件結構的整數和浮點欄位。

必須依照以下順序指定參數：

1. 條件。字串。語法類似SQL中Where語句的條件。您可以在條件中使用KUMA變數的函式以及對其他變數的參考。
2. 滿足條件時的值。運算式。
3. 不滿足條件時的值。運算式。

支援的運算子：

- AND
- OR
- NOT
- =
- !=
- <
- <=
- >
- >=
- LIKE（傳遞 RE2 規則運算式，而非 SQL 運算式）
- ILIKE（傳遞 RE2 規則運算式，而非 SQL 運算式）
- BETWEEN
- IN
- IS NULL（檢查是否有空值，例如 0 或空字串）

使用範例（值取決於參數2和參數3）
conditional('SourceUserName = \\'root\\' AND DestinationUserName = SourceUserName', 'match', 'no match')
conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no match')
conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no match')

延伸事件結構模式欄位的運作

對於 **string** 類型的延伸事件結構模式欄位，支援以下操作：

- `len`
- `to_lower`
- `to_upper`
- `append`
- `prepend`
- `substring`
- `tr`
- `replace`
- `regexp_replace`
- `regexp_capture`

對於整數或浮點類型的延伸事件結構描述欄位，支援以下幾種操作：

- 基本數學運算：
- `round`
- `ceil`
- `floor`
- `abs`
- `pow`
- `str_join`
- `conditional`

對於 **array of integers**、**array of floats** 和 **array of strings** 類型的延伸事件結構描述欄位，KUMA 支援以下函式：

- 取得陣列的第 i 個元素。範例：**item(<type>.someStringArray)**。
- 取得值陣列。範例：**<type>.someStringArray**。傳回 **["string1", "string2", "string3"]**。

- 取得陣列中的元素計數。範例：`len(<type>.someStringArray)`。傳回 `["string1", "string2"]`。
- 從陣列中取得唯一元素。範例：`distinct_items(<type>.someStringArray)`。
- 產生陣列元素的TSV字串。範例：`to_string(<type>.someStringArray)`。
- 對陣列元素進行排序。範例：`sort_items(<type>.someStringArray)`。
  在範例中，必須以陣列類型替換 `<type>`：NA 代表整數陣列，FA 代表浮點數陣列，SA 代表字串陣列。

對於 `array of integers` 和 `array of floats` 類型的欄位，支援以下函式：

- `math_min` — 傳回陣列中的最小元素。範例：`math_min(NA.NumberArray)`、`math_min(FA.FloatArray)`。
- `math_max` 傳回陣列中的最大元素。範例：`math_max(NA.NumberArray)`、`math_max(FA.FloatArray)`。
- `math_avg` — 傳回陣列的平均值。範例：`math_avg(NA.NumberArray)`、`math_avg(FA.FloatArray)`。

宣告變數

要宣告變數，必須將它們新增至關聯器或關聯規則中。

若要將全域變數新增至現有的關聯器：

1. 在主功能表中，轉至**監控 → 資源 → 關聯器**。
2. 選擇相關關聯器的資源集。
   將開啟關聯器安裝精靈。
3. 選擇安裝精靈中的**全域變數**步驟。
4. 請按一下**新增變數**按鈕並指定以下參數：
5. 在**變數**視窗中，輸入變數的名稱。
   變數命名需求
   - 在關聯器內必須是唯一的。
   - 必須包含1至255個Unicode字元。
   - 不能以字元「$」開頭。
   - 必須以駝峰式大小寫命名。
   - 在**值**視窗中，輸入變數函式。
     變數函式描述。

   可以新增多個變數。新增的變數可以使用✕圖示進行編輯或刪除。
6. 選擇安裝精靈的**安裝驗證**步驟，然後按一下**儲存**。

全域變數將新增至關聯器。它可以像事件欄位一樣透過在變數名稱前插入「$」字元進行查詢。重新啟動關聯器服務後，該變數將用於關聯。

若要將局部變數新增至現有的關聯規則：

1. 在主功能表中，轉至**監控 → 資源 → 關聯規則**。
2. 選擇相關的關聯規則。

   規則設定視窗隨即開啟。也可以透過繼續執行安裝精靈的**關聯**步驟，從新增關聯規則的關聯中開啟關聯規則的參數。
3. 按一下**選取器**索引標籤。
4. 在選擇器中，開啟**局部變數**頁籤，按一下**新增變數**按鈕並指定以下參數：

   - 在**變數**視窗中，輸入變數的名稱。

     變數命名需求

     - 在關聯器內必須是唯一的。
     - 必須包含1至255個Unicode字元。
     - 不能以字元「$」開頭。
     - 必須以駝峰式大小寫命名。
   - 在**值**視窗中，輸入變數函式。

     變數函式描述。

   可以新增多個變數。新增的變數可以使用✕圖示進行編輯或刪除。

   對於標準關聯規則，對每個要宣告變數的選擇器重複此步驟。
5. 按一下**儲存**按鈕。

   局部變數已新增至關聯規則。它可以像事件欄位一樣透過在變數名稱前插入「$」字元進行查詢。重新啟動關聯器服務後，該變數將用於關聯。

新增的變數可以編輯或刪除。如果關聯規則查詢未宣告的變數（例如，如果其名稱已變更），則會傳回空字串。

若要更改變數的名稱，則需要在使用它的所有關聯規則中手動更改此變數的名稱。

預定義關聯規則

OSMP分發套件包含下表中所列的關聯規則。

預定義關聯規則

關聯規則名稱	描述
[OOTB] KATA警示	用於擴充KATA事件。
[OOTB] 成功的暴力破解	在多次身份驗證嘗試失敗後檢測到成功的身份驗證嘗試時觸發。此規則基於sshd守護進程事件運行。
[OOTB][AD] 短時間內建立和刪除的帳戶	偵測在Microsoft Windows主機上建立和隨後刪除帳戶的實例。
[OOTB][AD] 帳號從不同主機登入失敗	偵測在不同主機上多次身分驗證失敗的情況。

[OOTB][AD] 無需TGT（黃金票證）即可授予TGS	偵測可疑的黃金票證類型的攻擊。此規則基於Microsoft Windows事件運行。
[OOTB][AD][Technical] 4768。已請求TGT	用於填充活動清單的技術規則是[OOTB][AD]已請求TGT清單。事件ID 4768。此規則基於Microsoft Windows事件運行。
[OOTB][AD] 敏感群組的成員資格已修改	基於Microsoft Windows事件運行。
[OOTB][AD] 多個帳戶從相同主機登入失敗	在同一台主機上從不同帳戶偵測到多次身分驗證失敗後觸發。
[OOTB][AD] 可能的Kerberoasting攻擊	偵測可疑的Kerberoasting類型的攻擊。此規則基於Microsoft Windows事件運行。
[OOTB][AD] 在多個主機上使用相同帳戶成功進行身分驗證	偵測在相同帳戶下與不同主機的連線。此規則基於Microsoft Windows事件運行。
[OOTB][AD] 短時間內在群組中新增和刪除的帳戶	偵測將使用者新增至群組並隨後刪除。此規則基於Microsoft Windows事件運行。
[OOTB][Net] 可能的連接埠掃描	偵測可疑的連接埠掃描。此規則基於Netflow、Ipfix事件運行。
[OOTB] EDR IOA警示	監控EDR事件，並在偵測到具有已觸發IOA規則特徵且標記為警示的EDR事件時建立警示。
[OOTB] EDR IOA SB警示	監控EDR事件，並在偵測到從自動沙盒掃描收到的EDR事件時建立警示。
[OOTB] OSMP掃描器偵測	監控IRP元件產生的安全性稽核事件，並在收到下列類型之一的事件時建立警示：「YARA掃描主機」、「沙盒偵測」、「反惡意軟體偵測」、「IOC掃描主機」、「YARA掃描伺服器」。
[OOTB] KEDR事件監控	稽核事件，並在事件來源監控政策觸發時建立警示。
[OOTB] 使用相同帳戶多次嘗試登入OSMP主控台	偵測使用相同帳戶登入OSMP主控台的嘗試，如果發生三次身分驗證失敗，則產生警示。

為關聯規則新增暫時排除清單

沒有權限在 OSMP 主控台中編輯關聯規則的使用者，可以建立暫時排除清單（例如，在管理警示時為誤報建立排除項目）。擁有編輯關聯規則權限的使用者可以將排除項目新增至規則，並將其從暫時清單中移除。

若要在管理警示時將排除項目新增至關聯規則：

1. 前往 **警示** 區段並選取警示。
2. 按一下 **在事件中尋找** 按鈕。

   警示的事件會顯示在事件頁面上。
3. 開啟關聯事件。

   這會開啟事件卡片，其中每個欄位都有一個 ⌄（箭頭）按鈕，可讓您新增排除項目。
4. 按一下 ⌄ 按鈕，然後選取 **新增至排除項目**。

   系統會顯示側邊欄，其中包含以下欄位：**關聯規則**、**排除項目**、**警示**、**註解**。
5. 點擊**建立**按鈕。

   排除規則已新增。

排除項目已新增至暫時清單。任何擁有讀取關聯規則權限的人都可以存取此清單：在 **資源 → 關聯規則** 區段中，按一下規則清單工具列中的 **排除項目清單** 按鈕。如果要檢視特定規則的排除項目，請開啟該規則的卡片，然後選取 **排除項目** 索引標籤。

排除清單包含具有以下參數的項目：

- `Exclusion`
  排除條件。
- `Correlation rule`
  關聯規則的名稱。
- `Alert`
  新增排除項目的來源警示名稱。
- `Tenant`
  規則和排除項目適用的租用戶。
- `Condition`
  根據關聯事件的所選欄位自動產生。
- `Creation date`
  新增排除項目的日期和時間。
- `Expires`

排除項目將自動從清單中移除的日期和時間。

- `Created by`
  新增排除項目的使用者名稱。
- `Comment`

新增排除項目後，依預設，關聯規則會將該排除項目納入考量 7 天。在**選項 → 一般**區段中，您可以編輯**核心屬性**區段中的`corr_rule_exclusion_ttl_hours`參數，以設定排除項目的有效期限。您可以以小時和天數設定排除項目的有效期限。最小值為 1 小時，最大值為 365 天。此設定僅適用於具有主管理員角色的使用者。

若要將基礎事件中的欄位傳播至關聯事件，必須在關聯規則卡片的**一般**索引標籤上，於**傳播的欄位**欄位中指定這些欄位。如果基礎事件的欄位未對應至關聯事件，則無法將這些欄位新增至排除項目。

若要從關聯規則中移除排除項目：

1. 前往**資源 → 關聯規則**區段。
2. 在規則清單的工具列中，按一下**排除項目清單**按鈕。
   這會開啟包含排除項目清單的視窗。
3. 選取您要刪除的排除項目，然後按一下**刪除**按鈕。

例外已從關聯規則中刪除。

KUMA 會在每次建立或刪除例外時產生稽核事件。您可以在**事件詳細資料**視窗中檢視事件設定的變更。

Sigma 規則轉換器

Sigma 規則轉換器會將關聯規則轉換為 OSMP 支援的格式，並方便匯入簡單規則，再由分析師加以完善。

支援 Sigma 規則轉換器的作業系統清單列於「軟體需求」區段。

若要使用 Sigma 規則轉換器轉換關聯規則，請依照下列步驟操作：

1. 安裝 Sigma 規則轉換器。以下安裝選項可供使用：

   - **使用 Docker 和 Bash 安裝 Sigma 規則轉換器**

     此安裝方法適用於在本機安裝轉換器網頁介面。

     安裝需要最新版本的 Bash 和 Docker。如需部署 Bash 和 Docker 的詳細資訊，請參閱官方文件。

     不支援 Astra Linux 1.7。

     若要執行安裝：

     1. 進入壓縮檔案解壓縮後的目錄，並執行下列其中一個命令：

        - 若要將轉換器安裝在位址為下列內容的主機上：

          `0.0.0.0:8000`
          執行以下命令：

          ```
          ./run.sh
          ```

        - 若要將轉換器安裝在位址為下列內容的主機上：

          `0.0.0.0:8888`
          執行以下命令：

          ```
          ./run.sh <port>
          ```

          其中：

          <port> 是連接埠（預設連接埠為 `8000`）。

        - 若要將轉換器安裝在位址為下列內容的主機上：

          `127.0.0.1:9999`
          執行以下命令：

          ```
          ./run.sh <IP address>:<port>
          ```

          其中：

- 預設情況下，<IP address> 是接聽介面的 IP 位址

  `0.0.0.0`
  。指定

  `127.0.0.1`
  僅在本機介面上執行。

- <port> 是連接埠。

轉換器隨即安裝。

- **在允許執行 Docker 映像檔的環境中安裝 Sigma 規則轉換器**

  此安裝方法使用提供的容器，可讓您建立 systemd 服務，並使用 Kubernetes 部署網頁介面。

  任何容器化工具皆可：docker、podman、cri-o。安裝程序包括下載容器映像檔，然後指定連接埠並執行該映像檔。

  若要使用 podman 安裝轉換器：

  1. 下載容器映像檔：

     ```
     podman load --input "kuma-sigma-converter-x.x.x.tar
     ```

  2. 以下列方式之一執行映像檔：

     - 執行直到按下 Ctrl+C 為止：

       ```
       podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm -it kuma-sigma-converter:x.x.x
       ```

     - 在背景執行：

       ```
       podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm kuma-sigma-converter:x.x.x
       ```

  轉換器隨即安裝。

- **使用 Python 3.10 或更新版本安裝 Sigma 規則轉換器**

  此安裝方法最為靈活，適合經驗豐富的使用者，因為它可讓您根據特定需求調整轉換器。與其他方法不同，此方法需要網際網路連線才能下載 Python 套件。

  若要安裝轉換器：

  1. 請確定您已安裝 Python 3.10 或更新版本。

  2. 安裝 poetry 以管理 Python 相依性。若為 Ubuntu 或 Debian，您可以使用套件管理員：

     ```
     sudo apt-get update
     sudo apt install pipx
     pipx install poetry
     ```

  3. 使用 poetry 設定並執行 Sigma 規則轉換器的 Web 介面：

     ```
     cd sigconverter.io
     poetry install
     ```

```
poetry run ./run.py
```

4. 在瀏覽器中，瀏覽至安裝 Sigma 規則轉換器 Web 介面的主機。若為本機安裝，位址為 http://127.0.0.1:8000 或 http://0.0.0.0:8000。

5. 如有需要，您可以指定 `HOST` 和 `PORT` 環境變數以設定監聽介面並指定連接埠號碼。

轉換器隨即安裝。

Sigma 規則轉換器是 pySigma 架構的外掛程式，這表示它

pySigma-backend-kuma

可以與其他標準 Sigma 工具搭配使用，而不只是自訂版本
sigconverter.io

。例如：
sigma-cli 是具有命令列介面的轉換器。

sigconverter.io 是原始的通用 Web 介面。

以下是以原始碼提供之函式庫的 README 檔案：

src/pySigma/README.md—適用於業界標準 Sigma 轉換架構與函式庫。

src/pySigma-backend-kuma/README.md—適用於為 pySigma 實作 OSMP 篩選器及查詢轉換的外掛程式。

src/sigconverter.io/README.md—Web 使用者介面。

安裝後，登入轉換器的 Web 介面。

2. 視需要在 Sigma 規則轉換器中調整關聯規則，並將調整後的規則複製或匯入 OSMP。

3. 重新啟動關聯器以套用變更。

您調整後的關聯已套用至關聯器。

準備 Sigma 規則

若要將 Sigma 規則轉換為關聯規則：

1. 修改規則之前，請確認符合下列要求：

   - 預先定義的正規化器會針對包含使用者名稱、主機名稱和程序名稱的欄位使用事件擴充 `to lower case`，因此建議在來源 Sigma 規則中將相關欄位轉換為小寫。
   - 不建議在 `contains` 條件及類似項目中撰寫註解或其他資訊。如果需要保留註解，建議使用 `#` 字元；這類註解不會影響條件。
   - 規則必須以 `title` 一字開頭，且前面不得有連字號。

2. 從 OSMP Web 介面複製您要編輯的關聯規則，將其轉換為 YML 格式，然後貼到轉換器的 **rule.yml** 索引標籤中。視需要在下拉式清單中選取設定。視需要修正任何錯誤。

3. 在 Sigma 規則轉換器的 **後端** 欄位中，選取 **kuma**；在 **格式** 欄位中，選取 **default**，並將 **管線** 欄位留空。
以下值可用：

- 後端：kuma，格式：default—未經格式化、可直接執行的 SQL 查詢。
- 後端：kuma，格式：SQL_formatted—經格式化、可直接執行的 SQL 查詢。
- 後端：kuma_filter，格式：default—可直接用於關聯規則的選擇器。
- 後端：kuma_filter，格式：correlation—JSON 格式、可直接匯入的關聯規則。若要執行匯入，您可以使用 REST API 方法 /xdr/api/v3/kuma/resources/{kind}/create，並指定 tenantID 以及要匯入的租用戶名稱。

4. 前往轉換器的 **custom_pipeline.yml** 索引標籤，並將針對 pySigma 調整的範例字典複製到該索引標籤。
針對 pySigma 調整的範例字典

Windows process_creation 對應

product: windows

category: process_creation

DeviceEventClassID = 4688

Windows sysmon EVENT=11 對應

product: windows

service: Sysmon

EventID = 11

Windows 安全性

product: windows

service: security

EventID = 4624|4662|4104|4698

```
name: KUMA windows
priority: 30
transformations:
### Windows process_creation mapping
  - id: MAPPING_logsource_windows_process_creation
    type: field_name_mapping
    mapping:
      ParentImage: SourceProcessName
      Image: DestinationProcessName
      CommandLine: DeviceCustomString4
    rule_conditions:
      - type: logsource
        product: windows
        category: process_creation
  - id: DEFAULT_FOR_logsource_windows_process_creation
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
```

```
      DeviceProduct: Windows
      DeviceEventClassID: '4688'
    rule_conditions:
       - type: logsource
         product: windows
         category: process_creation
### Windows sysmon EventID=11 mapping
  - id: DEFAULT_FOR_logsource_windows_sysmon
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Sysmon
    rule_conditions:
       - type: logsource
         product: windows
         service: Sysmon
  - id: MAPPING_logsource_windows_sysmon
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Image: OldFilePath
      CommandLine: DeviceCustomString4
      TargetFilename: FilePath
    rule_conditions:
      - type: logsource
        product: windows
        service: Sysmon
### Windows security mapping
  - id: DEFAULT_FOR_logsource_windows_security
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
    rule_conditions:
       - type: logsource
         product: windows
         service: security
  - id: DEFAULT_MAPPING_FOR_logsource_windows_security
    type: field_name_mapping
    mapping:
      Computer: DestinationHostName
      LogonID: FlexString1
    rule_conditions:
       - type: logsource
         product: windows
         service: security
  - id: 4624_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      LogonType: DeviceCustomNumber1
      SourceIP: SourceAddress
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4624
  - id: 4662_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Properties: FilePermission
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4662
  - id: 4104_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      ScriptBlockText: Message
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4104
  - id: 4698_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      TaskName: SourceProcessName
    rule_conditions:
      - type: contains_detection_item
```

```
        field: "EventID"
        value: '4698'
```

轉換後的規則會顯示在 **查詢** 索引標籤上。轉換結果是 SQL 查詢的 `WHERE` 子句。

如果最終結果是查詢或篩選器，您可以將其複製到 OSMP。若要在 OSMP 中使用規則，您可以逐一將規則匯入 OSMP。

支援的 Sigma 規則轉換範例

支援的 Sigma 規則轉換範例

Sigma 規則	對應至 OSMP 物件	
title: Generic-DCSync Execution id: 9107f781-c984-436a-8093-1aaa64c70c49 description: Detects access to DC with "DS-Replication-Get-Changes" or "DS-Replication-Get-Changes-All" rights author: Kaspersky status: stable modified: 2023-08-02 tags: - attack.credential_access - attack.t1003.006 logsource: product: windows service: security detection: selection1: EventID: 4662 Properties|contains: - 'DS-Replication-Get-Changes' - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' selection2: EventID: 4624 LogonType: 3 filter: EventID: 4624 LogonType: 3 SourceIP: - '<ip address of DC servers>' timeframe: 1m condition: selection1 or (selection2 and not filter) | count(EventID) by Computer,LogonID = 2 fields: - SourceIP - Computer - LogonID - Username - Properties falsepositives: - Unknown level: high	「Microsoft 產品」正規化工具 tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows selection1: DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '' selection2 DeviceEventClassID=4624 DeviceCustomNumber1 = 3 filter DeviceEventClassID=4624 DeviceCustomNumber1 = 3 SourceAddress = <IP> condition: DeviceVendor = Microsoft AND DeviceProduct = Windows AND ((DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '') OR ((DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3) NOT (DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3 AND SourceAddress = <IP>))) everything inside Count() Put EventID in Unique fields, everything after 'by' Computer → DestinationHostName LogonID → FlexString1 put in Aggregation fields, everything after '=' or '>' 2 put in threshold. timeframe put in time window	這是含有關聯的關則。目前僅部分支移除管線符號，便脅搜尋所用的 SQI

Sigma 規則	對應至 OSMP 物件	
title: Lsass Dump via LOLBin id: 2fe9cd33-d7f1-4d52-ab11-e40cb359ad02 description: detects lsass dump via lolbins such as procdump.exe, dotnet-dump.exe, dumpminitool.exe references: - https://twitter.com/bohops/status/1635288066909966338 - https://twitter.com/mrd0x/status/1511415432888131586 modified: 2023-07-18 author: Kaspersky status: stable tags: - attack.credential_access - attack.t1003.001 logsource: product: windows category: process_creation detection: selection_procdump: Image|endswith: - '\procdump.exe' - '\procdump64.exe' CommandLine|contains: 'lsass' selection_dotnet: Image|endswith: '\dotnet-dump.exe' CommandLine: ' collect ' selection_dumpminitool: Image|endswith: '\dumpminitool.exe' condition: 1 of selection* falsepositives: - Unknown level: high	轉換方式與表格第 3 列的規則相同。 差異：'selection* 的條件 1' 中的條件是其中一個命名集合。	DeviceVendor=' DeviceProduct= DeviceEventCla (((Desti '\\procdump.ex '\\procdump64. 'lsass') OR (Destinati dump.exe' AND De) OR Destinati '\\dumpminitoo)
title: Generic-Clearing Windows Event Logs via Command Line id: a903492e-da40-4ab4-a92d-306a4799d973 description: Detects Clear Windows Event Logs via Command Line author: Kaspersky status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1070.001 logsource: product: windows category: process_creation detection: selection1: Image|endswith: '\wevtutil.exe' CommandLine|contains: - ' cl ' - 'clear' selection2: Image|endswith: - '\powershell.exe' - '\powershell_ise.exe' - '\pwsh.exe' CommandLine|contains: - 'Clear-EventLog' - 'Remove-EventLog' selection3: Image|endswith: '\wmic.exe' CommandLine|contains: - 'ClearEventLog' condition: 1 of them falsepositives: - Legitimate System Administrator actions level: high	"Microsoft products" normalizer tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows DeviceEventClassID=4688 selection1: DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" Selection2 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" selection3 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" condition DeviceVendor = Microsoft AND DeviceProduct = Windows AND DeviceEventClassID=4688 AND ((DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains ""))) identical fields - specify the fields from the condition, except Name, deviceProduct, deviceVendor	DeviceVendor=' DeviceProduct= DeviceEventCla ((Destinati '\\wevtutil.ex (Devic DeviceCustomSt) OR ((Destin '\\powershell. Des '\\powershell\ '\\pwsh.exe') A (Device EventLog' OR D 'Remove-EventL) OR (Destinatio AND DeviceC 'ClearEventLog)

Sigma 規則	對應至 OSMP 物件	
title: 0021-0002.1204.003 Execution - PowerExchangeDropper description: Detect the dropping of PowerExchange components. status: experimental logsource: product: windows service: Sysmon detection: selection1: EventID: 11 selection2: TargetFilename|contains: - 'c:\users\public\microsoftedge\autosave.exe' - 'c:\users\public\microsoftedge\wsdl.ps1' selection3: Image|endswith: "brochure.exe" condition: selection1 and selection2 and selection3 falsepositives: - Unknown level: high	Based on: Normalizer 11 of Sysmon event. title → name author → description description→ description status → description logsource DeviceVendor = Microsoft DeviceProduct = Sysmon selection1 DeviceEventClassID=11 selection2 FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '' if the file path contains * format in regexp selection3 OldFilePath endswith "" condition: DeviceVendor = Microsoft AND DeviceProduct = Sysmon AND (DeviceEventClassID=11) AND (FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '') AND (OldFilePath endswith "") identical fields—specify the fields from the condition, except Name, deviceProduct, deviceVendor level →severity falsepositive → Description	DeviceVendor=' DeviceProduct= DeviceEventCla (FilePath con 'c:\\users\\pu OR FilePath c 'c:\\users\\pu) AND OldFilePath en
標題：已加入網域主機探索 description: Detect an attacker enumerating domain-joined machines using PowerShell. status: stable logsource: product: windows service: security detection: selection: EventID: 4104 ScriptBlockText|contains|all： - 'System.DirectoryServices.DirectorySearcher' - 'Properties.operatingsystem' condition: selection falsepositives: - "Administrative scripts or tools like Vulnerability Scanners" level: medium	ScriptBlockText → Message	

Sigma 規則	對應至 OSMP 物件	
title: 0022-0002.1053.005 Execution - PowerExchange Task description: Detect the creation of a scheduled task by PowerExchange. status: experimental logsource: product: windows service: security detection: selection: EventID： - '4698' TaskName|contains: - 'MicrosoftEdgeUpdateService' condition: selection falsepositives: - Unknown level: medium	TaskName → SourceProcessName	

Sigma 規則	對應至 OSMP 物件	
title: Created Windows Shell from Critical Windows Process description: Anomaly behavior critical windows process status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1036 logsource: product: windows category: process_creation detection: selection: ParentImage|endswith: - '\searchindexer.exe' - '\lsaiso.exe' - '\lsm.exe' - '\spoolsv.exe' - '\wininit.exe' - '\smss.exe' - '\csrss.exe' - '\lsass.exe' - '\services.exe' - '\winlogon.exe' Image|endswith: - '\powershell_ise.exe' - '\cmstp.exe' - '\appvlp.exe' - '\mftrace.exe' - '\scriptrunner.exe' - '\forfiles.exe' - '\msiexec.exe' - '\rundll32.exe' - '\mshta.exe' - '\hh.exe' - '\wmic.exe' - '\regsvr32.exe' - '\scrcons.exe' - '\bash.exe' - '\sh.exe' - '\cscript.exe' - '\wscript.exe' - '\powershell.exe' - '\cmd.exe' condition: selection falsepositives: - Unknown level: high	ParentImage → SourceProcessName	

MITRE ATT&CK框架涵蓋範圍

若要透過關聯規則評估MITRE ATT&CK框架的涵蓋範圍，請執行以下操作：

1. 從官方MITRE ATT&CK儲存庫下載MITRE技術清單並將其匯入KUMA。
2. 將MITRE技術對應到關聯規則。
3. 將關聯規則匯出到MITRE ATT&CK Navigator。

這樣，您就可以直觀地評估MITRE ATT&CK框架的涵蓋範圍。

匯入MITRE技術清單

只有擁有主管理員角色的使用者才能匯入MITRE技術清單。

若要匯入MITRE ATT&CK技術清單：

1. 請從GitHub入口網站下載MITRE ATT&CK技術清單。

   > KUMA僅支援MITRE ATT&CK技術清單14.1版本。

2. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。
   這將開啟KUMA設定視窗。
3. 在**其他**下，按一下**常見**。
4. 在**MITRE技術清單設定**中，按一下**從檔案匯入**。
   檔案選擇視窗隨即開啟。
5. 選擇已下載的MITRE ATT&CK技術清單，然後按一下**開啟**。

MITRE ATT&CK技術清單隨即匯入到KUMA中。點擊**檢視清單**即可查看已匯入的技術清單以及MITRE ATT&CK技術清單的版本。

將MITRE技術對應到關聯規則

若要將MITRE ATT&CK技術對應到關聯規則：

1. 在主功能表中，轉至**監控 → 資源 → 關聯規則**。
2. 請按一下關聯規則的名稱來開啟關聯規則編輯視窗。
   這將開啟關聯規則編輯視窗。

3. 在**一般**頁籤上，按一下**MITRE技術**欄位來開啟可用技術清單。為了方便搜索，我們提供了一個篩選器，您可以在其中輸入技術名稱或技術/策略的ID。一個或多個MITRE ATT&CK技術可用於連結到關聯規則。

4. 按一下**儲存**按鈕。

MITRE ATT&CK技術隨即對應到關聯規則。在KUMA主控台的**監控 → 資源 → 關聯規則**部分，已編輯規則的**MITRE技術**直欄會顯示所選技術的ID。將滑鼠游標停留在ID上時，會顯示技術的完整名稱，包括技術ID和策略。

將關聯規則匯出到MITRE ATT&CK Navigator

若要將關聯規則與已對應的MITRE技術匯出至MITRE ATT&CK Navigator：

1. 在主功能表中，轉至**監控 → 資源 → 關聯規則**。

2. 點選右上角的省略号按鈕（ ... ）。

3. 在下拉清單中，按一下**匯出到MITRE ATT&CK Navigator**。

4. 在開啟的視窗中，選取您需要匯出的關聯規則。

5. 點擊**確定**。
   一個包含匯出規則的檔案隨即下載到您的電腦。

6. 將檔案從您的電腦上傳到MITRE ATT&CK Navigator來評估MITRE ATT&CK框架的涵蓋範圍。

您可以評估MITRE ATT&CK框架的涵蓋範圍。

彙總規則

彙總規則可讓您組合相同類型的重複事件，並將其替換為一個公共事件。彙總規則支援標準KUMA事件結構描述的欄位以及擴充事件架構的欄位。透過這種方式，您可以減少傳送到儲存體和/或關聯器的類似事件的數量，減少服務負載，節省資料儲存空間和產品授權配額 (EPS)。當達到時間或事件數量閾值（以先發生者為準）時，將建立彙總事件。

對於彙總規則，您可以設定篩選器並將其僅套用於符合指定條件的事件。

您可以在**監控 → 資源 → 彙總規則**下設定彙總規則，然後從收集器設定的下拉清單中選擇已建立的彙總規則。您也可以直接在收集器設定中設定彙總規則。

可用的彙總規則設定

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
閾值	事件數量的閾值。在累積了指定數量的具有相同欄位的事件後，收集器會建立一個彙總事件並開始為下一個彙總事件累積事件。預設值是 `100`。
觸發後規則有效期	必需設定。 時間閾值，以秒為單位。在指定時間到期時，基礎事件的累積停止，收集器會建立一個彙總事件並開始取得下一個彙總事件的事件。預設值是 `60`。

設定	描述
描述	資源描述：最多4,000個Unicode字元。
相同欄位	必需設定。 此下拉清單列出了必須具有相同值的標準化事件的欄位。例如，對於網路事件，您可以使用SourceAddress、DestinationAddress和 DestinationPort欄位。在彙總事件中，這些欄位將使用基礎事件的值進行填入。
唯一欄位	此下拉清單列出了必須在彙總事件中儲存其值範圍的欄位。例如，如果在**唯一欄位**下而不是**相同欄位**下指定了DestinationPort欄位，則彙總事件將組合各種連接埠的基本連線事件，並且彙總事件的DestinationPort欄位包含所有已建立連線的連接埠的清單。
總和欄位	在此下拉清單中，您可以選擇在彙總期間將值相加並寫入彙總事件的同名欄位的欄位。

設定	描述
篩選器	一組設定，您可以在其中指定識別必須由此資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，也可以**建立**新篩選器。 在彙總規則中，請勿使用具有**TI**運算元或**TIDetect**、**inActiveDirectoryGroup**或**hasVulnerability**運算子的篩選器。可以使用**inActiveDirectoryGroup**運算子的Active Directory欄位將在擴充階段（執行彙總規則之後）顯示。 **在資源中建立過濾器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。

設定	描述
	5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

只有在編輯已建立的彙總規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到收集器。

若要將彙總規則關聯到收集器，請按一下**連結至服務**按鈕→**連結至收集器**。這將開啟一個視窗；在該視窗中，選擇一個或多個收集器，然後按一下**確定**。彙總規則與選定的收集器相關聯，並根據其組態套用。

如有必要，您可以將彙總規則與收集器取消關聯。若要執行此操作，請選取收集器旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

預定義彙總規則

OSMP分發套件包含下表所列的彙總規則。

彙總規則名稱	描述
[OOTB] Netflow 9	此規則在100個事件或10秒後觸發。 事件依以下欄位彙總： • DestinationAddress • DestinationPort • SourceAddress • TransportProtocol • DeviceVendor • DeviceProduct DeviceCustomString1和BytesIn欄位相加。

擴充規則

*事件擴充*涉及為事件添加可用於識別和調查事件的資訊。

擴充規則可讓您透過轉換欄位中已有的資料或查詢外部系統的資料來新增補充資料至事件欄位。例如，假設事件中記錄了使用者名稱。您可以使用擴充規則將此使用者的部門、職位和經理的資訊新增至事件欄位。

擴充規則可用於下列KUMA服務和功能：

- 收集器。
- 關聯器。
- 標準化器。

可用的擴充規則設定列於下表。

基本設定頁籤

設定	描述

來源類型	必需設定。 用於選擇傳入事件類型的下拉清單。根據所選類型，將顯示以下其他設定： • **常數** 當需要將常數新增至事件欄位時，請使用此類擴充。此類擴充的設定： • 在 **常數** 欄位中，指定要新增至事件欄位的值。此值不得超過 255 個 Unicode 字元。如果將此欄位留空，現有事件欄位的值將被清除。 • 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。 若針對 `String` 、 `Number` 或 `Float` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至該欄位。 若針對 `Array of strings` 、 `Array of numbers` 或 `Array of floats` 類型的擴展結構描述欄位使用事件擴充函式，並搭配常數，則該常數會被新增至陣列的元素。 • **字典** 如果需要從字典類型的**字典**中新增值，則使用此類擴充。 在**字典名稱**下拉清單中選擇此類型時，您必須選擇用於提供值的字典。在**鍵欄位**設定區塊中，按一下**新增欄位**按鈕，然後選擇其值將用於選擇字典條目的事件欄位。 如果使用事件擴充，將「來源類型」設定選為「字典」，並在「金鑰擴充欄位」設定中指定陣列欄位，則當陣列作為字典金鑰傳遞時，會依照 TSV 格式中單一值的序列化規則，將陣列序列化為字串。 例如：「金鑰擴充欄位」設定使用 SA.StringArrayOne 擴展結構描述欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」。以下值會作為金鑰傳遞至字典：['a','b','c']。 如果「金鑰擴充欄位」設定使用擴展結構描述的陣列欄位和一般事件結構描述欄位，查詢字典時，欄位值會以「|」字元分隔。 例如：「金鑰擴充欄位」設定使用兩個欄位：SA.StringArrayOne 擴展結構描述欄位和 Code 欄位。SA.StringArrayOne 擴展結構描述欄位包含 3 個元素：「a」、「b」和「c」；Code 字串欄位包含字元序列「myCode」。以下值會作為金鑰傳遞至字典：['a','b','c']|myCode。 • **表格** 如果您需要從表格類型的**字典**中新增值，請使用此類擴充。 在**字典名稱**下拉清單中選擇此擴充類型後，請選擇用於提供值的字典。在**鍵欄位**設定群組中，按一下**新增欄位**按鈕以選擇其值用於選擇字典條目的事件欄位。 在**對應**表中，設定用於提供資料的字典欄位和用於接收資料的事件欄位： • 在**字典欄位**直欄中，選擇字典欄位。可用欄位取決於所選的字典資源。 • 在 **KUMA 欄位**直欄中，選取要寫入值的事件欄位。對於某些選取的欄位（ `*custom*` 與 `*flex*` ），您可以在**標籤**直欄中，為寫入其中的資料指定名稱。 可以透過點選**新增元素**按鈕來新增表格行。可以透過按一下✕按鈕來刪除直欄。 • **事件** 當需要將值從另一個事件欄位寫入目前事件欄位時，將使用此類擴充。此類擴充的設定： • 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。 • 在**來源欄位**下拉清單中，選擇要將其值寫入目標欄位的事件欄位。 • 在**轉換**下，您可以建立規則，以便在將原始資料寫入 KUMA 事件欄位之前修改資料。可以從下拉清單中選擇轉換類型。您可以使用**新增轉換**和**刪除轉換**按鈕分別新增或刪除轉換。轉換的順序很重要。 **可用的轉換** 轉換是在將值寫入事件欄位之前可以套用於該值的變更。從下拉清單中選擇轉換類型。 可用轉換類型： • **熵**用於使用資訊熵計算函式轉換來源欄位的值，並將轉換結果放置在浮點類型的目標欄位中。轉換結果是一個數字。計算資訊熵可以偵測DNS隧道或洩漏的密碼，例如，當使用者輸入密碼而不是登入名稱時，該密碼會以純文字形式記錄。 • **小寫** — 用於將值的所有字元變為小寫 • **大寫** — 用於將值的所有字元變為大寫 • **regexp** — 用於使用規則運算式RE2轉換值。選擇此轉換類型時，欄位將出現在應新增規則運算式的位置。 • **子字串**—用於擷取在**開始**和**結束**欄位中指定的位置範圍內的字元。選擇此轉換類型時，將出現這些欄位。

- **替換** — 用於將指定的字元序列替換為其他字元序列。選擇此轉換類型時，將出現新欄位：
  - **替換字元** — 您可以在此欄位中指定應替換的字元序列。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- **trim** —用於同時從值的開始和結束位置刪除「字元」欄位中指定的字元。選擇此轉換類型時，將出現此欄位。例如，將Micromon值套用至Microsoft-Windows-Sysmon的trim轉換會導致soft-Windows-Sys。
- **append** 用於將「常數」欄位中指定的字元新增至事件欄位值的末端。選擇此轉換類型時，將出現此欄位。
- **prepend** —用於將「常數」欄位中指定的字元新增至事件欄位值的開頭。選擇此轉換類型時，將出現此欄位。
- **使用規則運算式替換**— 用於將RE2規則運算式的結果替換為字元序列。
  - **運算式**— 在此欄位中，您可以指定要替換結果的規則運算式。
  - **使用字元** — 您可以在此欄位中指定應使用的字元序列而非已替換的字元。
- 將編碼字串轉換為文字：
  - **decodeHexString** —用於將HEX字串轉換為文字。
  - **decodeBase64String** —用於將Base64字串轉換為文字。
  - **decodeBase64URLString** —用於將Base64url字串轉換為文字。

  轉換損壞的字串或發生轉換錯誤時，損壞的資料可能會寫入事件欄位。
  在事件擴充期間，如果編碼字串的長度超過了標準化事件欄位的大小，則字串會被截斷並且不會被解碼。
  如果解碼字串的長度超過了要寫入解碼值的事件欄位的大小，則該字串將被截斷以適應事件欄位的大小。

使用延伸事件結構描述時的轉換

是否可以使用轉換取決於所使用的延伸事件結構描述欄位的類型：

- 對於 `String` 類型的附加欄位，所有轉換類型皆可用。
- 對於 `Number` 與 `Float` 類型的欄位，以下轉換類型皆可用：regexp、substring、replace、trim、append、prepend、replaceWithRegexp、decodeHexString、decodeBase64String、decodeBase64URLString。
- 對於 `Array of strings`、`Array of numbers` 與 `Array of floats` 類型的欄位，以下轉換類型皆可用：append、prepend。

- **範本**

當您需要將透過處理 Go 範本取得的值寫入事件欄位時，請使用此類擴充。此類擴充的設定：

- 在 **範本**欄位中，輸入 Go 範本。
  事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是必須將其值傳遞給指令碼的事件欄位名稱。
  範例：`Attack on {{.DestinationAddress}} from {{.SourceAddress}}`。
- 在**目標欄位**下拉清單中，選擇要將資料寫入的KUMA事件欄位。

若要將範本中陣列欄位的資料轉換為 TSV 格式，請使用 toString 函數，例如：

如果您使用事件擴充，並在 **來源類型** 設定中選取 **範本** 類型，且目標欄位的類型為 `String`、來源欄位是包含字串陣列的延伸事件結構描述欄位，則可以使用以下任一範例作為範本。

範例：

{{.SA.StringArrayOne}}

範例：

{{- range $index, $element := .SA.StringArrayOne -}}

{{- if $index}}, {{end}}"{{$element}}"{{- end -}}

- **dns**

此類擴充用於向私人網路DNS伺服器傳送請求，以將IP位址轉換為網域名稱或反之亦然。IP 位址只會針對以下私人位址轉換為 DNS 名稱：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、100.64.0.0/10、fd00::/8。

下表說明此類擴充的設定。

「dns」擴充類型的參數

設定	描述
網址	要傳送請求的 DNS 伺服器 URL。 您可以使用 **新增 URL** 按鈕指定多個 URL。 如果未指定 **URL** 設定，KUMA 會從本機的 `/etc/resolv.conf` 檔案取得 DNS 伺服器清單。在這種情況下，您需要啟用 **遞迴查詢** 選項。否則將不會執行擴充。
每秒請求數	每秒傳送至 DNS 伺服器的查詢數上限。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
工作模組	服務可以同時執行以並行處理回應規則的事件處理器數量。請指定介於 0 到 999 之間的正整數。如果指定 0，則使用邏輯 CPU 核心數。預設值為 `1`。
資料補足佇列中的最大事件數量	重新提交佇列可容納的事件數上限。預設值為 `1,000,000`。
逾時時間	等待 DNS 伺服器回應的時間（以秒為單位）。預設值為 `5`。
DNS 模式覆寫	使用的解析方法： • **僅轉發 DNS**會將網域名稱解析為 IP 位址。 • **僅反向 DNS**會將 IP 位址解析為網域名稱。 • **轉發並反向 DNS**會將網域名稱解析為 IP 位址，或將 IP 位址解析為網域名稱。
快取存續時間	快取中儲存的值的存活時間（以秒為單位）。預設值為 `60` 秒。
已停用快取	您可以使用此設定啟用或停用快取。預設情況下啟用快取。
已停用快取重新整理	如果啟用快取更新，當快取的 TTL 到期時，收集器會再次向 DNS 伺服器傳送請求，以更新快取中儲存的資料。此設定僅在啟用快取時可用。預設會啟用快取更新。
遞迴查詢	允許收集器向權威 DNS 伺服器傳送遞迴查詢，以擴充資料。預設值是**停用**。

- **cybertrace**

  此類擴充用於將CyberTrace資料流中的資訊新增至事件欄位。

  可用設定：

  - **URL**（必填）- 在此欄位中，您可以指定要傳送請求的CyberTrace伺服器的URL。
  - **連線數**– KUMA可以同時與CyberTrace伺服器建立的最大連線數。預設情況下，此值等於KUMA Core伺服器的vCPU數量。
  - **RPS** – 每秒傳送至伺服器的最大請求數。預設值是 `1000`。
  - **逾時** – 等待CyberTrace伺服器回應的時間長度（以秒為單位）。預設值為 `30`。
  - **對應**（必要）– 此設定區塊包含用於將KUMA事件欄位對應到 CyberTrace指標類型的對應表。**KUMA 欄位**欄會顯示 KUMA 事件欄位的名稱，而 **CyberTrace 指標**欄會顯示 CyberTrace 指標的類型。
    可用的CyberTrace指標類型：
    - **ip**
    - **網址**
    - **雜湊值**

    在對應表中，您必須提供至少一個字串。您可以點擊**新增行**按鈕新增字串，也可以點擊 ✕ 按鈕刪除字串。

- **cybertrace-http**

  此類擴充功能用於使用REST API將CyberTrace資料流中的資訊新增至事件欄位。

  可用設定：

  - **URL**（必填）- 在此欄位中，您可以指定要傳送請求的CyberTrace伺服器的URL。
  - **密鑰**（必填）是一個下拉清單，您可以在其中選擇儲存連接憑證的金鑰。
  - **逾時** – 等待CyberTrace伺服器回應的時間長度（以秒為單位）。預設值是30。
  - **鍵欄位**（必填）是用於使用CyberTrace資料擴充事件的事件欄位清單。
  - **擴充佇列中的最大事件數**– 擴充佇列中儲存的用於重新傳送的最大事件數。預設值是1000000000。從CyberTrace伺服器接收的事件達到100萬個後，將停止擴充事件，直到接收到的事件數量減少到50萬個以下。

  > 當佇列數字達到100萬個接收事件時，事件擴充將停止，且事件將以未擴充狀態記錄在儲存體中，直到佇列數字變為少於50萬個事件。

- **時區**

  此類擴充在收集器和關聯器中用於為事件指派特定的時區。在搜尋發生在異常時間（例如夜間）的事件時，時區資訊可能很有用。

選擇此類擴充時，必須從**時區**下拉清單中選擇所需的時區。

請確保託管擴充利用服務的伺服器已設定正確的時區。例如，您可以使用 `timedatectl list-timezones` 命令執行此操作，該命令會顯示伺服器上已設定的所有時區。有關設定時區的詳細資訊，請參閱相應的作業系統說明文件。

當事件進行擴充處理時，所選時區相對於協調世界時 (UTC) 的時間偏移量，會以`+-hh:mm`格式寫入DeviceTimeZone事件欄位。例如，若選取 **Asia/Yekaterinburg** 時區，則會將值 `+05:00` 寫入 DeviceTimeZone 欄位。若經擴充處理的事件在 DeviceTimeZone 欄位中已有值，該值將被覆蓋。

預設情況下，如果未在正在處理的事件中指定時區，且未配置按時區擴充規則，則為事件指派處理事件的服務（收集器或關聯器）所在伺服器的時區。如果伺服器時間發生變化，則必須重新啟動服務。

擴充DeviceTimeZone欄位時允許的時間格式

在收集器中處理傳入的原始事件時，下列時間格式可自動轉換為+-hh:mm格式：

已處理事件中的時間格式	範例
+-hh:mm	-07:00
+-hhmm	-0700
+-hh	-07

若 `DeviceTimeZone` 欄位中的日期格式與上述格式不符，當事件使用時區資訊進行擴充處理時，系統會將收集器伺服器的時區寫入該欄位。您可以為非標準時間格式建立自訂的標準化規則。

- **地理資料**

此類擴充用於將IP地理資料新增至事件位址。了解有關將IP位址連結到地理資料的更多資訊。

選取此類型時，在**將地理資料對應到事件欄位**下，您必須指定要從哪個事件欄位讀取IP位址、選取所需的地理資料屬性，並定義要將地理資料寫入哪些事件欄位：

1. 在**具有IP位址的事件欄位**下拉清單中，選擇從中讀取IP位址的事件欄位。上傳到KUMA的地理資料與此IP位址相符。

   您可以使用**新增具有IP位址的事件欄位**按鈕來指定需要擴充地理資料的多個具有IP位址的事件欄位。您可以透過點擊**刪除具有IP位址的事件欄位**按鈕來刪除以這種方式新增的事件欄位。

   當選取`SourceAddress`、`DestinationAddress`和`DeviceAddress`事件欄位時，**套用預設對應**按鈕將可供使用。您可以按一下此按鈕，新增地理資料屬性與事件欄位的預先設定的對應配對。

2. 對於需要從中讀取IP位址的每個事件欄位，選擇地理資料的類型以及要將地理資料寫入的事件欄位。

   您可以使用**新增地理資料屬性**按鈕為**地理資料屬性-要寫入的事件欄位**新增欄位對。您也可以為一個IP位址設定不同類型的地理資料，以便將其寫入不同的事件欄位。若要刪除欄位對，請按一下 ❌。

   - 在**地理資料屬性**欄位中，選擇應將與讀取的IP位址對應的地理資料寫入事件。可用的地理資料屬性：**國家**、**地區**、**城市**、**經度**、**緯度**。
   - 在**要寫入的事件欄位**中，選擇必須將所選地理資料屬性寫入的事件欄位。

   您可以將相同的地理資料屬性寫入不同的事件欄位。如果設定要寫入相同事件欄位的多個地理資料屬性，則事件將使用序列中的最後一個對應進行擴充。

名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
偵錯	您可以使用此切換開關啟用服務運作的日誌記錄。預設情況下，日誌記錄處於停用狀態。
描述	資源描述：最多4,000個Unicode字元。

篩選器

一組設定，您可以在其中指定識別必須由此資源處理的事件的條件。您可以從下拉清單中選擇現有篩選器，也可以**建立**新篩選器。

在資源中建立篩選器

KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。

若要建立篩選器：

1. 在**篩選器**下拉清單中，選擇**新建**。
2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。
3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。
4. 在**條件**下，指定事件必須滿足的條件：
   a. 點擊**新增條件**按鈕。
   b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。
   c. 在**運算子**下拉清單中，選擇一個運算子。

   篩選器運算子

   - **=** — 左運算元等於右運算元。
   - **<** — 左運算元小於右運算元。
   - **<=** — 左運算元小於或等於右運算元。
   - **>** — 左運算元大於右運算元。
   - **>=** — 左運算元大於或等於右運算元。
   - **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。
   - **contains** — 左運算元包含右運算元的值。
   - **startsWith** — 左運算元以右運算元的某個值開頭。
   - **endsWith** — 左運算元以右運算元的某個值末端。
   - **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。
   - **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。
     待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。
     若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。
   - **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。
     如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。
   - **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。
   - **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。
   - **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。
   - **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。
   - **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。
   - **inContextTable**檢查指定快顯表單中條目的存在情況。
   - **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。

   d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。
   e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。

   您可以新增多個條件或一組條件。
5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。
6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

只有在編輯已建立的擴充規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到服務，即關聯器和收集器。

若要將擴充規則關聯到收集器或關聯器，請按一下**連結至服務**按鈕→**關聯至<服務名稱>**。這將開啟一個視窗；在該視窗中，選擇一個或多個關聯器或收集器，然後按一下**確定**。擴充規則與選定的服務相關聯，並根據其組態套用。

如有必要，您可以將彙總規則與服務取消關聯。若要執行此操作，請選取關聯器或收集器旁的核取方塊，按一下**刪除**，然後確認與服務取消關聯。

預定義擴充規則

OSMP分發套件包含下表所列的擴充規則。

預定義擴充規則

擴充規則名稱	描述
[OOTB] KATA警示	用於以警示的超連結形式擴充從KATA收到的事件。超連結放在DeviceExternalId欄位中。

回應規則

回應規則可讓您啟動卡巴斯基安全管理中心工作的自動運作、Kaspersky Endpoint Detection and Response and Response、KICS for Networks、Active Directory的威脅回應操作以及針對特定事件執行自訂指令碼。

與相關程序整合後，可依照回應規則自動執行卡巴斯基安全管理中心工作、Kaspersky Endpoint Detection and Response工作以及KICS for Networks和Active Directory工作。

您可以在**監控 → 資源 → 回應規則**下設定回應規則，然後從關聯器設定中的下拉清單中選擇已建立的回應規則。您也可以直接在關聯器設定中設定回應規則。

卡巴斯基安全管理中心的回應規則

您可以設定回應規則，以自動啟動卡巴斯基安全中心資產的病毒掃描和更新工作。

在建立和編輯卡巴斯基安全管理中心的回應規則時，您需要定義以下設定的值。

一般頁籤

回應規則設定

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
類型	必需設定，如果KUMA與卡巴斯基安全管理中心整合則可用。 回應規則**osmptasks** 。
Open Single Management Platform工作	必需設定。 待執行之卡巴斯基安全管理中心工作的名稱。工作必須預先建立，且其名稱必須以「 `KUMA` 」開頭。例如， `KUMA antivirus check` （不區分大小寫且不帶引號）。 您可以使用KUMA執行以下類型的卡巴斯基安全管理中心工作： • 更新 • 病毒掃描
事件欄位	必需設定。 定義應為其啟動卡巴斯基安全管理中心工作的資產的事件欄位。可能的值： • SourceAssetID • DestinationAssetID • DeviceAssetID
工作線程	服務可以同時執行的進程數。預設情況下，工作線程數量與安裝服務的伺服器上的虛擬處理器數量相同。
描述	回應規則的描述。您最多可以新增4,000個Unicode字元。

設定	描述
篩選器	用於定義使用回應規則處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

設定	描述

要向卡巴斯基安全管理中心傳送請求，您必須確保卡巴斯基安全管理中心透過UDP協議可用。

如果回應規則由共用租用戶擁有，則主要租用戶所連線之卡巴斯基安全管理中心伺服器中的工作，會顯示為可供選擇的卡巴斯基安全管理中心工作。

如果回應規則選擇了租用戶連線到的卡巴斯基安全管理中心伺服器中沒有的工作，則不會針對此租用戶的資產執行該工作。例如，當兩個租用戶使用同一個關聯器時，就可能發生這種情況。

服務頁籤

只有在編輯已建立的回應規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到關聯器。

若要將回應規則關聯至關聯器，請點選**關聯至服務**按鈕→**關聯至關聯器**。這將開啟一個視窗；在該視窗中，選擇一個或多個關聯器，然後按一下**確定**。回應規則與選定的關聯器相關聯，並根據其組態套用。

如有必要，您可以將回應規則與服務取消關聯。若要執行此操作，請選取相關關聯器旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

自訂指令碼的回應規則

您可以建立一個指令碼，其中包含在偵測到選定事件時在KUMA伺服器上執行的命令，並配置回應規則以自動執行此指令碼。在這種情況下，程式將在收到與回應規則相符的事件時執行該指令碼。

指令碼檔案儲存於安裝了使用回應資源之關聯器服務的伺服器上：/opt/kaspersky/kuma/correlator/<關聯器ID>/scripts。此伺服器的 kuma 使用者需要有執行該指令碼的權限。

在建立和編輯自訂指令碼的回應規則時，需要定義以下參數的值。

一般頁籤

回應規則設定

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
類型	必需設定。 回應規則類型，**指令碼**。
逾時時間	分配給指令碼完成的秒數。如果超過此時間量，指令碼將終止。

設定	描述
指令碼名稱	必需設定。 指令碼檔案的名稱。 如果回應資源已附加到關聯器服務，但/opt/kaspersky/kuma/correlator/<關聯器ID>/scripts資料夾中沒有指令碼檔案，則關聯器將無法運作。
指令碼引數	必須傳遞給指令碼的引數或事件欄位值。 如果指令碼包含對檔案執行的操作，則應指定這些檔案的絕對路徑。 參數可以用引號 (") 括起來。 事件欄位名稱會以 `{{.EventField}}` 格式傳遞，其中 `EventField` 是其值必須傳遞至指令碼的事件欄位名稱。 範例： `-n "\"usr\": {{.SourceUserName}}"`
工作線程	服務可以同時執行的進程數。預設情況下，工作線程數量與安裝服務的伺服器上的虛擬處理器數量相同。
描述	資源的敘述。您最多可以新增4,000個Unicode字元。

設定	描述
篩選器	用於定義使用回應規則處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

只有在編輯已建立的回應規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到關聯器。

若要將回應規則關聯至關聯器，請點選**關聯至服務**按鈕→**關聯至關聯器**。這將開啟一個視窗；在該視窗中，選擇一個或多個關聯器，然後按一下**確定**。回應規則與選定的關聯器相關聯，並根據其組態套用。

如有必要，您可以將回應規則與服務取消關聯。若要執行此操作，請選取相關關聯器旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

KICS for Networks的回應規則

您可以設定回應規則以自動觸發對KICS for Networks資產的回應操作。例如，您可以在KICS for Networks中變更資產狀態。

在建立和編輯KICS for Networks的回應規則時，您需要定義以下設定的值。

一般頁籤

回應規則設定

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
類型	必需設定。 回應規則類型， **kics** 。
事件欄位	必需設定。 指定必須執行回應操作的資產的事件欄位。可能的值： • SourceAssetID • DestinationAssetID • DeviceAssetID
KICS for Networks工作	收到與篩選器相符的資料時要執行的回應操作。可用的回應操作類型如下： • **將資產狀態變更為已授權**。 • **將資產狀態變更為未授權**。 當觸發回應規則時，KUMA將向KICS for Networks傳送API請求，以將指定裝置的狀態變更為**已授權**或**未授權**。
工作線程	服務可以同時執行的進程數。預設情況下，工作線程數量與安裝服務的伺服器上的虛擬處理器數量相同。
描述	資源的敘述。您最多可以新增4,000個Unicode字元。

設定	描述
篩選器	用於定義使用回應規則處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

只有在編輯已建立的回應規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到關聯器。

若要將回應規則關聯至關聯器，請點選**關聯至服務**按鈕→**關聯至關聯器**。這將開啟一個視窗；在該視窗中，選擇一個或多個關聯器，然後按一下**確定**。回應規則與選定的關聯器相關聯，並根據其組態套用。

如有必要，您可以將回應規則與服務取消關聯。若要執行此操作，請選取相關關聯器旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

Kaspersky Endpoint Detection and Response的回應規則

您可以設定回應規則以自動觸發對Kaspersky Endpoint Detection and Response資產的回應操作。例如，您可以設定自動資產網路隔離。

在建立和編輯Kaspersky Endpoint Detection and Response的回應規則時，您需要為下列設定定義值。

一般頁籤

回應規則設定

設定	描述
事件欄位	必需設定。 指定必須執行回應操作的資產的事件欄位。可能的值： • SourceAssetID • DestinationAssetID • DeviceAssetID

設定	描述
工作類型	收到與篩選器相符的資料時要執行的回應操作。可用的回應操作類型如下： • 啟用網路隔離當選擇此類型的回應時，您需要為以下設定定義值： • **隔離逾時**— 資產的網路隔離處於活動狀態的小時數。您可以指定從1到9,999小時的數值。如有必要，您可以**新增網路隔離排除項**。 *若要新增網路隔離排除項：* a. 按一下**新增排除項**按鈕。 b. 選擇不得封鎖的網路流量方向： • 入站。 • 出站。 • 入站/出站。 c. 在**資產IP**欄位中，輸入不得封鎖其網路流量的資產的IP位址。 d. 如果您選擇了**入站**或**出站** ，請在**遠端連接埠**和**本機連接埠**欄位中指定連線連接埠。 e. 若要新增多個排除項，請點選**新增排除項** ，然後重複上述步驟以填寫**流量方向** 、 **資產IP** 、 **遠端連接埠**和**本機連接埠**欄位。 f. 如果要刪除排除項，請按一下相關排除項下的**刪除**按鈕。 將排除項新增至網路隔離規則時，Kaspersky Endpoint Detection and Response可能會在規則詳細資料中錯誤顯示連接埠值。這不會影響應用程式效能。有關查看網路隔離規則的更多詳細資訊，請參閱*Kaspersky Anti Targeted Attack Platform說明*。 • 停用網路隔離。 • 新增防護規則。選擇此類型的回應時，您需要為下列設定定義值： • **要從中擷取雜湊的事件欄位** - KUMA從中提取必須阻止執行的檔案的SHA256或MD5雜湊值的事件欄位。選定的事件欄位以及在**事件欄位**中選定的值必須新增到關聯規則的傳播欄位中。 • **檔案雜湊值#1**—要封鎖的檔案的SHA256或MD5雜湊值。 必須至少填寫上述其中一個欄位。 • 刪除防護規則。 • 啟動應用程式 選擇此類型的回應時，您需要為下列設定定義值： • **檔案路徑** - 要啟動的進程的檔案路徑。 • **命令列參數** - 要用於啟動檔案的參數。 • **工作目錄** - 啟動時檔案所在的目錄。 當為具有主管理員角色的使用者觸發回應規則時，程式主控台的**工作管理器**部分將顯示**執行程式**工作。在**工作表**的建立者欄中，此工作顯示為**排定的工作**。您可以檢視工作完成結果。 所有列出的操作都可以在具有Kaspersky Endpoint Agent for Windows的資產上執行。在具有Kaspersky Endpoint Agent for Linux的資產上，只能啟動該代理程式。 在軟體級別，使用Kaspersky Endpoint Kaspersky Endpoint Agent for Linux為資產建立阻止規則和網路隔離規則的能力是無限的。KUMA和Kaspersky Endpoint Detection and Response不提供任何有關這些規則應用失敗的通知。
工作線程	服務可以同時執行的進程數。預設情況下，工作線程數量與安裝服務的伺服器上的虛擬處理器數量相同。
描述	回應規則的描述。您最多可以新增4,000個Unicode字元。

設定	描述
篩選器	用於定義使用回應規則處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

只有在編輯已建立的回應規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到關聯器。

若要將回應規則關聯至關聯器，請點選**關聯至服務**按鈕→**關聯至關聯器**。這將開啟一個視窗；在該視窗中，選擇一個或多個關聯器，然後按一下**確定**。回應規則與選定的關聯器相關聯，並根據其組態套用。

如有必要，您可以將回應規則與服務取消關聯。若要執行此操作，請選取相關關聯器旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

Active Directory的回應規則

Active Directory的回應規則定義了觸發規則時要對帳戶執行的操作。

使用Active Directory建立和編輯回應規則時，請指定下列設定的值。

一般頁籤

回應規則設定

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。
類型	必需設定。 回應規則類型，**透過Active Directory回應**。
帳戶ID來源	從中取得Active Directory帳戶ID值的事件欄位。可能的值： • SourceAccountID • DestinationAccountID
AD命令	觸發回應規則時套用於帳戶的命令。 可用值： • **新增帳戶到群組** 若要將帳戶從/移至的Active Directory群組。 在必填欄位**可分辨名稱**中，您必須指定群組的完整路徑。 例如，CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。 一次操作中只能指定一個群組。 • **從群組中刪除帳戶** 若要將帳戶從/移至的Active Directory群組。 在必填欄位**可分辨名稱**中，您必須指定群組的完整路徑。 例如，CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。 一次操作中只能指定一個群組。 • 重設帳戶密碼 如果您的Active Directory網域允許選取**使用者無法變更密碼**核取方塊，則重設使用者帳戶密碼作為回應將導致使用者帳戶的要求衝突：使用者將無法進行身份驗證。網域管理員需要清除受影響使用者帳戶的核取方塊之一：**使用者無法變更密碼**或**使用者必須在下次登入時變更密碼**。 • 封鎖帳戶

設定	描述
篩選器	用於定義使用回應規則處理的事件的條件。您可以從下拉清單中選取現有的篩選器，或建立新的篩選器。 **在資源中建立篩選器** KUMA事件的所有欄位都有預設值。對於所有數值字段，預設值為0。對於所有字串字段，預設值為空字串。如果事件沒有某個字段，則該字段使用預設值。因此，即使事件本身不包含篩選器中指定的字段，該事件也可以觸發篩選器。例如，如果您在篩選器中指定 `DestinationPort <= 1024` 條件，但事件不包含 `DestinationPort` 字段，篩選器仍會被觸發，這是因為預設情況下 `DestinationPort = 0`。 *若要建立篩選器：* 1. 在**篩選器**下拉清單中，選擇**新建**。 2. 如果要將篩選器作為單獨的資源，請選取**儲存篩選器**核取方塊。在這種情況下，您將能夠在各種服務中使用已建立的篩選器。預設情況下，此核取方塊已清除。 3. 如果選擇了**儲存篩選器**核取方塊，請在**名稱**欄位中輸入已建立的篩選器資源的名稱。名稱的最大長度：128個Unicode字元。 4. 在**條件**下，指定事件必須滿足的條件： a. 點擊**新增條件**按鈕。 b. 在**左運算元**和**右運算元**下拉清單中，指定搜尋參數。根據在**右運算元**欄位中選取的資料來源，可能會顯示其他參數欄位，以識別要傳遞給篩選器的值。例如，當您選擇**活動清單**時，必須指定活動清單的名稱、輸入鍵和輸入鍵欄位。 c. 在**運算子**下拉清單中，選擇一個運算子。 **篩選器運算子** • **=** — 左運算元等於右運算元。 • **<** — 左運算元小於右運算元。 • **<=** — 左運算元小於或等於右運算元。 • **>** — 左運算元大於右運算元。 • **>=** — 左運算元大於或等於右運算元。 • **inSubnet** — 左運算元（IP位址）位於右運算元（子網路）的子網路中。 • **contains** — 左運算元包含右運算元的值。 • **startsWith** — 左運算元以右運算元的某個值開頭。 • **endsWith** — 左運算元以右運算元的某個值末端。 • **match** — 左運算元與運算元的規則運算式相符。使用RE2規則運算式。 • **hasBit**檢查左運算元（字串或數字）是否包含右運算元（常數或清單）中列出位置的位元。 待檢查的值將轉換為二進位並從右到左處理。將檢查字元，其索引指定為常數或清單。 若待檢查的值為字串，則會嘗試將其轉換為整數，並依照上述方式進行處理。如果字串無法轉換為數字，篩選器會傳回 `False`。 • **hasVulnerability**檢查左運算元是否包含具有右運算元中指定的弱點和弱點嚴重等級的資產。 如果沒有指定弱點的ID和嚴重等級，則當被檢查事件中的資產有任何弱點時，將觸發篩選器。 • **inActiveList**運算子只有一個運算元。其值在**鍵欄位**欄位中選擇，並與從活動清單下拉清單中選擇的活動清單中的項目進行比較。 • **inDictionary** 檢查指定的字典是否包含由選定事件欄位的連接值組成的鍵定義的條目。 • **inCategory** — 左運算元中的資產被分配了右運算元的至少一個資產類別。 • **inActiveDirectoryGroup** — 左運算元中的Active Directory帳號屬於右運算元中的其中一個Active Directory群組。 • **TIDetect**運算子用於透過CyberTrace Threat Intelligence（TI）資料來找尋事件。此運算子只能用於已使用CyberTrace Threat Intelligence資料完成擴充分析的事件。換句話說，它只能在目標選擇階段的收集器和關聯器中使用。 • **inContextTable**檢查指定快顯表單中條目的存在情況。 • **intersect** — 右運算元中指定的清單項目在左運算元中的存在情況。 d. 如果您希望運算子不區分大小寫，請選取**大小寫不相符**核取方塊。此核取方塊的選擇不適用於**InSubnet**、**InActiveList**、**InCategory**或**InActiveDirectoryGroup**運算子。預設情況下，此核取方塊已清除。 e. 如果要新增否定條件，請從**if**下拉清單中，選擇**若非**。 您可以新增多個條件或一組條件。 5. 如果您新增了多個條件或一組條件，請透過點選**AND**按鈕選擇選擇條件（**and**、**or**、**not**）。 6. 如果要新增從**選取篩選器**下拉清單中選擇的現有篩選器，請點擊**新增篩選器**按鈕。您可以透過點選 按鈕來檢視巢狀篩選器設定。

服務頁籤

只有在編輯已建立的回應規則的設定時才會顯示此頁籤；在此頁籤上，您可以將規則關聯到關聯器。

若要將回應規則關聯至關聯器，請點選**關聯至服務**按鈕→**關聯至關聯器**。這將開啟一個視窗；在該視窗中，選擇一個或多個關聯器，然後按一下**確定**。回應規則與選定的關聯器相關聯，並根據其組態套用。

如有必要，您可以將回應規則與服務取消關聯。若要執行此操作，請選取相關關聯器旁的核取方塊，按一下**刪除**，然後確認與該服務取消關聯。

資料收集和分析規則

資料探勘規則會分析儲存在 OSMP 資料庫中的事件，以偵測事件。

不同於串流關聯和回溯掃描，資料探勘規則會使用 SQL 查詢預先處理資料（包括使用 SQL 執行其他計算、分組及彙總），並依排程定期執行。正確設定資料探勘規則後，SIEM 可協助您偵測進階威脅。

若要管理此區段，您需要具備下列其中一種角色：主管理員、租用戶管理員、第 1 級分析師、第 2 級分析師。

當建立或編輯資料收集與分析規則時，您需要指定下表所列的設定。

資料探勘規則的設定

設定	描述
名稱	必需設定。 資源的唯一名稱。必須包含1至255個Unicode字元。
租用戶	必需設定。 擁有資源的租用戶名稱。 如果您只能存取一個租用戶，此欄位會自動填寫。如果您可以存取多個租用戶，則會填入可用租用戶清單中的第一個租用戶名稱。您可以從此清單中選擇任何租用戶。

SQL	必需設定。
	SQL 查詢必須包含搭配 LIMIT 的彙總函式及/或搭配 LIMIT 的資料分組。
	您必須使用介於 1 到 10,000 之間的 LIMIT 值。
	SQL 查詢範例
	• 僅包含彙總函式的查詢：
	`SELECT count(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
	• 僅包含資料分組的查詢：
	`SELECT SourceAddress, DeviceCustomFloatingPoint1 FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• 包含彙總函式和資料分組的查詢：
	`SELECT SourceAddress, sum(DeviceCustomFloatingPoint1) FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• 包含使用彙總函式之運算式的查詢：
	`SELECT stddevPop(DeviceCustomFloatingPoint1) + avg(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`

查詢間隔	必需設定。 執行 SQL 查詢的間隔時間。您可以指定以分鐘、小時和天為單位的間隔時間。最短間隔為 1 分鐘。 SQL 查詢的預設逾時時間等於您在此欄位中指定的間隔時間。 如果 SQL 查詢的執行時間超過逾時時間，則會發生錯誤。在此情況下，我們建議增加間隔時間。例如，如果間隔為 1 分鐘，而查詢需要 80 秒才能執行完畢，我們建議將間隔設定為至少 90 秒。

設定	描述
標記	可選設定。 資源搜尋標籤。
深度	可選設定。 用於在資料庫中搜尋事件之時間間隔下限的運算式。 若要從清單中選取值，或將深度指定為相對間隔，請將游標置於欄位中。例如，如果您要尋找從一小時前至今的所有事件，請將相對間隔設定為 now-1h。
描述	可選設定。 資料收集與分析規則的描述。
對應	將 SQL 查詢結果的欄位對應至 KUMA 事件的設定： **來源欄位**是 SQL 查詢結果中要轉換為 KUMA 事件的欄位。 **事件欄位**是 KUMA 事件的欄位。您可以將滑鼠游標置於此欄位中，以選取清單中的任一值。 **標籤**是以 `DeviceCustom*` 開頭之事件欄位的唯一自訂標籤。 您可以新增或刪除表格資料列。若要新增表格資料列，請按一下**新增對應**。若要刪除資料列，請選取資料列旁的核取方塊，然後按一下 按鈕。 如果您不想手動填寫欄位，可以按一下**從 SQL 更新對應**按鈕。欄位對應表會填入 SQL 查詢欄位的值，包括別名（如有）。例如，如果 SQL 查詢欄位的值為 `SourceAddress`，且此值與事件欄位的名稱相同，則此值會插入欄位對應表的**事件欄位**資料行中。 再次按一下**從 SQL 更新對應**按鈕不會重新整理表格，而是會將 SQL 查詢中的欄位再次新增至表格。

您可以透過下列任一方式建立資料收集和分析規則：

- 在**儀表板 → 資源和服務 → 資料探勘規則**區段中。

1. 在**儀表板 → *威脅搜尋***區段中。

*若要在**威脅搜尋**區段中建立資料收集和分析規則：*

1. 建立或產生 SQL 查詢，然後按一下 **建立資料探勘規則**按鈕。

   瀏覽器會開啟用於建立資料收集和分析規則的新分頁，其中已預先填入**SQL 查詢**和**深度**欄位。如果您未在 SQL 查詢中使用星號 (*)，欄位對應表也會自動填入。

2. 填寫必填欄位。

   如有需要，您可以變更**SQL 查詢期間**欄位中的值。

3. 儲存設定。

資料收集和分析規則已儲存，並可在**監控 → 資源和服務 → 資料收集和分析規則**區段中使用。若要套用資料探勘規則，您需要為其建立排程。

虛擬管理伺服器

虛擬管理伺服器（也稱為*虛擬伺服器*）是 Kaspersky Next XDR Expert 的元件，用於管理用戶端組織網路的病毒防護。

虛擬管理伺服器是從屬管理伺服器的一種特殊類型，與實體管理伺服器相比具有以下限制：

- 虛擬管理伺服器只能在主管理伺服器上建立。
- 虛擬管理伺服器依賴主管理伺服器的資料庫。虛擬管理伺服器不支援資料備份與還原任務，也不支援更新、掃描和下載任務。
- 虛擬管理伺服器不支援建立從屬管理伺服器（包括虛擬伺服器）。

另外虛擬管理伺服器具有以下限制：

- 在虛擬管理伺服器內容視窗中，能調整的區域是有限的。
- 若要在虛擬管理伺服器管理的用戶端裝置上遠端安裝 Kaspersky 應用程式，您必須確保已在其中一台用戶端裝置上安裝網路代理，以確保與虛擬管理伺服器的通訊。在第一次連線到虛擬管理伺服器時，該裝置會被自動分配為發佈點，並充當用戶端裝置與虛擬管理伺服器的連線閘道。
- 虛擬伺服器只能透過發佈點進行網路輪詢。
- 若要重新啟動發生故障的虛擬伺服器，Kaspersky Next XDR Expert 會重新啟動主管理伺服器及所有虛擬管理伺服器。
- 在虛擬伺服器上建立的使用者在管理伺服器上無法被分配到角色。

虛擬伺服器的管理員應擁有自己所管理的虛擬伺服器全部權限。

建構OSMP實例的層次結構

您可以將Open Single Management Platform（OSMP）實例排列成兩層層次結構，父實例位於頂端。這樣，您可以將父實例的設定分發給子實例，同時保持子實例的設定不變。

例如，使用者 A 和使用者 B 已部署 OSMP。每位使用者都有一個獨立的 OSMP 實例，並管理各自的 OSMP 控制台實例。

為了實現實例之間的資料交換，使用者A和使用者B必須將他們的實例排列成一個層次結構。為此，未來的子實例的使用者A會向未來的父實例發送連線請求，未來的父實例的使用者B核準該請求。

如有必要，您可以斷開子實例的連線。

建構層次結構後，實例中的實體會依下列方式在層次結構中進行管理：

- **管理伺服器**

  在實例的層次結構中，您必須手動指派從屬管理伺服器。

- **租用戶**

  子實例的租用戶層次結構建構於父實例的租用戶層次結構之中。子實例的租用戶設定和整合租用戶設定可以從子實例和父實例進行編輯。只能從實例實例租用戶設定和整合租用戶設定。

  在父實例上，您可以查看子實例的租用戶層次結構，建立、編輯和刪除子實例上的租用戶，但您無法刪除子實例的根租用戶。

- **資產（裝置）和資產類別**

  父實例和子實例的設定彼此獨立。如果對父實例進行更改，則變更不會套用到子實例，反之亦然。

  父實例的資產不會顯示在子實例中。在子實例中，可以檢視父實例的資產類別、將這些類別連結至子實例資產，以及對子實例的資產執行回應操作。例如，父實例和子實例中都有一個NNN資產類別。如果從子執行實例執行NNN類別的回應操作，則只有子實例的資產屬於該回應操作。但是，您無法編輯父實例類別，無法將這些類別指派給子實例裝置，也無法建立繼承類別的子類別。

  在父實例上，會顯示子實例的資產類別。選擇一個資產類別後，會顯示子實例的資產。您可以對子執行實例類別的資產執行回應操作。如果沒有與子實例建立連線，父實例的使用者可以啟動回應操作，該操作將在連接重新建立後在子實例裝置上執行。如果您從父實例中刪除一個類別，則該類別在子實例上會變成本機類別，並移至子實例根租用戶的「已分類資產」類別。如果某個資產類別已被KUMA資產使用，則無法刪除該類別。子實例的資產類別不能被父實例的KUMA資產使用。

- **使用者和使用者角色**

  所有使用者均由父實例管理。使用者和角色會從父實例複寫到子實例（admin 帳戶除外）。在子實例中，現有使用者將被刪除，使用者角色將保留，但不會複製到父實例。

  admin 帳戶是每個 OSMP 實例所獨有，不會在實例之間複寫。因此，無法使用父實例的 admin 帳戶執行下列操作：

  - 在父實例的**威脅搜尋**區段中管理子實例的事件
  - 從父實例檢視子實例的資源資訊
  - 從父實例檢視及管理子實例的服務

- **檔案**

  在子實例上執行回應操作後下載及取得的檔案，會顯示在父實例的檔案表中，並在**租用戶**欄位中顯示以下圖示：(8)。當您在父實例上開啟子實例檔案的詳細資料時，系統會將您重新導向至子實例，以便對該檔案執行進一步操作。

- **KUMA實體**

  - **事件**

    子實例事件儲存在子實例上，父實例事件儲存在父實例上。在父實例上，您可以搜尋子實例的事件。

  - **關聯規則和IOA規則**

    在建構層次結構後，IOA規則會轉換為KUMA關聯規則。

    在層次結構中使用關聯規則有以下幾種模式：

    - **本機**。如果關聯規則是在子實例上建立的，那麼它也在子實例上管理。如果關聯規則是從父實例繼承的，那麼在子實例上，您只能向關聯規則新增排除項，而不能編輯規則。

      關聯規則及其排除項僅適用於連線到子實例管理伺服器的裝置。

    - **通用**。這些關聯規則是在父實例上建立的。規則及其排除項將套用至您在設定規則設定時指定的子實例裝置。

  - **關聯規則中的排除項**

    新增到父實例關聯規則中的臨時排除項不會被繼承。在子實例上，您可以為繼承的關聯規則新增臨時排除項。篩選器會繼承關聯規則。

- **警示和事件**

  子實例的警示和事件會複製到父實例，並在子實例和父實例中同時顯示。父實例的警示和事件僅在父實例中顯示。在父實例上，您無法編輯、關聯和合併子實例的警示或事件。

  當刪除子實例上的警示或事件時，它們也會從父實例中刪除。

  警示和事件設定及其保留期間不會被繼承。如果保留期間到期，且子實例上的警示或事件被刪除，則相應的事件會被傳送到父事件，然後父實例上的警示或事件也會被刪除。

- **事件類型**、**工作流程**和**SLA**

  為避免資料不一致，事件類型、工作流程和SLA會作為一個整體複製到子實例。

  - **SLA**

    在子實例上，您無法建立SLA。嘗試從父實例檢視子實例的SLA時，系統會將您重新導向到子實例。

  - **工作流程**

    在子實例中，您可以建立工作流程，也可以檢視及套用從父實例繼承的工作流程。嘗試從父實例檢視子實例的工作流程時，系統會將您重新導向到子實例。在父實例上，您可以刪除父實例的工作流程；如果該工作流程在父實例上沒有連結的實體，則不再顯示該工作流程，並會在90天後完全刪除。您無法刪除具有連結實體的工作流程。

  - **事件類型**

    事件類型繼承自父實例，並預設為停用狀態。如果繼承了預設事件類型，則在子實例中，該事件類型將不再是預設類型。

    在子實例上，您可以建立新的事件類型，以及檢視和套用繼承的事件類型。您無法編輯繼承的事件類型。此外，您可以為繼承的事件類型和在子實例上本機建立的事件類型設定預設屬性。

- **彙總規則**

  手動建立的彙總規則會從父實例繼承。預先定義的彙總規則不會被繼承。

  在父實例上，您可以檢視子實例的所有彙總規則。編輯規則的權限取決於您的XDR角色。

  在子實例上，繼承的彙總規則會依照它們在父實例上的顯示順序顯示在規則表的頂部。預設情況下，繼承的規則處於停用狀態。您可以檢視、啟用和停用繼承的彙總規則。

  已啟用的彙總規則將根據其優先順序應用：規則在表中的位置越高，其優先順序越高。

- **區隔規則**

  手動建立的分段規則會從父實例繼承。預先定義的分段規則不會被繼承。

  在父實例上，您可以檢視子實例的所有分段規則。編輯規則的權限取決於您的XDR角色。

  在子實例上，繼承的分段規則會依照其在父實例上的顯示順序顯示在規則表的頂端。預設情況下，繼承的規則處於停用狀態。您可以檢視、啟用和停用繼承的分段規則。

  已啟用的分段規則將根據其優先順序應用：規則在表中的位置越高，其優先順序越高。

- **阻止規則**

  阻止規則繼承自父實例。

  在父實例上，您可以檢視和編輯子實例的阻止規則，以及將子實例規則套用至子實例的資產。您無法將子實例阻止規則套用至父實例的資產。

  在子實例上，您可以檢視從父實例繼承的阻止規則。您無法編輯這些規則，也無法在從父實例繼承的阻止規則中新增或刪除子實例資產。

- **YARA 和 IOC 規則**

  YARA規則和IOC規則清單是從父實例繼承的。

  在父實例上，您可以檢視和編輯子實例的規則，以及將子實例規則套用至子實例的資產。您無法將子實例規則套用至父實例的資產。

  在子實例上，您可以檢視從父實例繼承的YARA規則和IOC規則，但無法編輯這些規則。若要執行回應操作，您可以同時使用子實例的規則和從父實例繼承的規則。

- **沙盒規則**

  沙盒規則繼承自父實例。

  在父實例上，您可以檢視和編輯子實例沙盒規則，也可以將子實例規則套用至子實例資產。

  在子實例上，您可以查看從父實例繼承的沙盒規則，但您無法編輯這些規則。

- **常規程式**

  您可以從父實例在子實例上建立常規程式，並手動啟動用於子實例警示和事件的常規程式。

- **產品授權**

  產品授權管理和產品授權設定由各實例各自獨立處理，不會在實例階層中繼承。

  產品授權金鑰會分別新增至每個實例。您可以將同一個產品授權金鑰新增到所有實例中。

- **政策和工作**

  政策和工作繼承自父實例。

- KSN/KPSN設定、憑據和通知範本不會被繼承。

將子實例連線到父實例

未來子實例的使用者發送連線請求，未來父實例的使用者核准該請求。

兩位使用者都必須在各自的實例中擁有主管理員 XDR 角色。
如果您向在另一個層次結構中作為子實例的實例發送連線請求，該請求將被取消。
父實例最多可擁有 150 個子實例。

從子實例發送連線請求

若要發送連線請求：

1. 在未來的子實例上，在主功能表中，轉至**設定→租用戶**。
   螢幕上將顯示租用戶清單。
2. 在工具列上，點擊**請求連線**按鈕。
3. 在開啟的右側窗格中，執行以下操作：
   - 在**父實例的 API URL**欄位中，指定父實例公用 API 的位址，例如：`https://api.xdr-hier-1.kuma.example.com` 。
   - 在**父實例憑證指紋**中，指定父實例憑證的雜湊值。
     您可以點擊**獲取指紋**將父實例憑證的雜湊值插入到**父實例憑證指紋**中。如果父實例具有憑證鏈，Kaspersky Next XDR Expert將使用中間憑證。我們不建議您使用葉憑證，因為它的輪換頻率比中間憑證高。指定憑證輪替後，需要恢復實例層次結構。
   - 在**API 權杖**欄位中，指定用於外部整合的公用API權杖。

     API權杖必須事先在父實例上產生。
     設定權杖參數時，建構實例層次結構需要 GET:/api/hierman/v1/* 和 POST:/api/hierman/v1/* API 方法。
   - 如果必要，配置以下設定：
     - 在**子實例的 API URL**欄位中，指定子實例公用API的位址，例如：*https://api.xdr-hier-1.kuma.example.com*。
     - 在**選取要共用 SIEM 資源的租用戶**部分，選取要在父實例中顯示其SIEM資源的租用戶旁的核取方塊。

4. 點擊**請求**按鈕。
   窗格隨即關閉。

5. 在確認對話方塊，按一下**請求**。

確認對話方塊隨即關閉，螢幕上顯示**您的連線請求正待核准**狀態訊息。

父實例上的使用者核准或拒絕請求後，您會收到一封電子郵件通知，螢幕上顯示的狀態訊息也會隨之變更。

如果父實例上的使用者批准了請求，則子實例中會顯示父實例的ID和父實例租用戶的名稱。

核准來自父實例的連線請求

子實例的使用者傳送連線請求後，您會收到對應的電子郵件通知。

若要核准連線請求：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 在頁面頂部，按一下有關待處理連線請求的訊息中顯示的**檢視請求**連結。
3. 在開啟的**連線請求**窗格中，按一下要核准的請求的**批准**按鈕。
4. 在開啟的**核准連線請求**窗格中，執行以下操作：
   - 在**根租用戶名稱**欄位中，為要連線的子實例租用戶指定一個新名稱。
   - 在**根租用戶名稱**部分，從父實例的租用戶層次結構中，選擇一個租用戶作為子實例租用戶的父租用戶。
   - 點擊**批准**按鈕。
     窗格隨即關閉。

子實例將會被加入到父實例的租用戶層次結構中。螢幕上會顯示對應的訊息。

重新啟動子實例上的活動服務

子實例與父實例建立連線後，重新啟動子實例上的活動服務。之後，子實例的活動服務將顯示在父實例上。

結果

現在您可以如下管理子實例的租用戶樹：

- 檢視子實例租用戶樹
- 在子實例上建立租用戶

- 在子實例上編輯租用戶
- 從子實例中刪除租用戶（根租用戶為例外）
- 斷開子實例的連線

子實例的使用者只能檢視、編輯和刪除子實例的租用戶。

在 OSMP 實例階層中指派從屬管理伺服器

建立 OSMP 實例階層後，您必須藉由手動指派從屬管理伺服器，手動建立「主要/從屬」關係。

若要指派可透過 OSMP 主控台連線的從屬管理伺服器：

1. 在未來的主管理伺服器上，請確定連接埠 13000 可用於接收來自從屬管理伺服器的連線。
2. 在主功能表中，按一下管理伺服器名稱以開啟屬性視窗，然後按一下**管理伺服器**頁籤。
3. 選取您要向其新增管理伺服器的管理群組名稱旁邊的核取方塊。
4. 在功能表行中，點擊**連線從屬管理伺服器**。
   新增從屬管理伺服器精靈啟動。使用**下一步**按鈕進行精靈。
5. 指定未來從屬管理伺服器的連線設定：

   - **將主管理伺服器連線到 DMZ 中的從屬管理伺服器**

     如果從屬管理伺服器位於非武裝區 (DMZ)，選取該選項。

     如果選擇此選項，主管理伺服器將啟動與從屬管理伺服器的連線。否則，從屬管理伺服器將啟動與主管理伺服器的連線。

   - **從屬管理伺服器位址（可選）**

     指定從屬管理伺服器的 IP 位址或網域名稱。

     如果啟用了**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**選項，則需要此參數。

   - **從屬管理伺服器顯示名稱**

     從屬管理伺服器將顯示在層級的名稱。如果需要，您可以輸入 IP 位址作為名稱，也可以使用例如「群組 1 的從屬伺服器」之類的名稱。

   - **管理伺服器 SSL 連接埠號**

     指定主管理伺服器上的 SSL 埠號。預設埠號為 13000。

     連接埠 13000 用於根管理伺服器；此連接埠號碼無法變更。

   - **管理伺服器 API 連接埠**

     網頁主控台用於透過 OpenAPI 接收來自從屬管理伺服器之連線的連接埠號碼。預設埠號為 13299。

     在構建層級結構時，網頁主控台會連線至未來的從屬伺服器、請求憑據、擷取公開憑證，並執行初始設定。

管理伺服器的層級結構構建完成後，將不再使用連接埠 13299。管理伺服器將透過連接埠 13000 進行互動。

6. 指定未來從屬伺服器的憑證。

   如果已選取 **從屬管理伺服器位址（可選）** 參數，您必須按一下 **從從屬管理伺服器獲取** 按鈕以取得憑證，或按一下 **瀏覽憑證檔案** 並手動新增憑證。

7. 指定未來主伺服器的位址。

8. 若未來主管理伺服器的連線會透過代理伺服器執行，請選取**使用代理伺服器**核取方塊並指定連線設定。

9. 指定對未來從屬管理伺服器具有存取權限的使用者憑證。

10. 如果雙因素驗證已啟用並設定，請指定由身份驗證器應用程式產生的秘密金鑰。

11. 儲存設定。

12. 切換到未來從屬管理伺服器，並開啟其內容視窗。

13. 在**一般**索引標籤上，前往**管理伺服器階層**區段並執行下列操作：

    - 選取**此管理伺服器是階層中的從屬伺服器** 核取方塊。
    - 在**主管理伺服器位址**欄位中，指定未來主管理伺服器的網路名稱。
    - 按一下「瀏覽」，選取先前儲存且包含未來主管理伺服器憑證的檔案。
    - 如有需要，請選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**核取方塊。
    - 若未來主管理伺服器的連線會透過代理伺服器執行，請選取**使用代理伺服器**核取方塊並指定連線設定。

14. 儲存設定。

管理伺服器的「主管理伺服器/從屬管理伺服器」層次結構已建立。主管理伺服器開始使用連接埠 13000 從從屬管理伺服器接收連線。主管理伺服器的工作和政策被接收和套用。從屬管理伺服器顯示在主管理伺服器上，在新增其的管理群組中。

將子實例與父實例斷開連線

子實例與其父實例斷開連線後，您無法將子實例連接到另一個層次結構。

啟動與父實例斷開連線

若要斷開子實例的連線：

1. 在父實例的主功能表中，轉至**設定→租用戶**。

   螢幕上將顯示租用戶清單。

2. 選取要斷開連線的子實例根租用戶旁的核取方塊。

3. 在工具列中，按一下**中斷連線**按鈕，然後在顯示的確認對話方塊中，按一下**中斷連線**。

子實例隨即與父實例斷開連線，對應的訊息將顯示在螢幕上。子實例的使用者將收到電子郵件通知。

如果在斷開連線時子實例處於關閉狀態，則該實例將被強制斷開連線。無論如何，要完成斷開連線，請先打開子實例，然後按照以下說明將子實例與父實例斷開連線。

將實例斷開連線時，Kaspersky Next XDR Expert 會建立稽核事件 將 SCN 與 PCN 斷開連線。無論在斷開連線時子實例是處於開啟狀態還是關閉狀態，稽核事件都相同。

為了進行診斷，如果子實例在斷開連線時處於關閉狀態，Kaspersky Next XDR Expert 會將錯誤寫入 hierman 元件的日誌檔案，例如「在次要實例上斷開連線失敗」錯誤。使用稽核事件中`trace_id`欄位的值來查詢日誌檔案中的錯誤。

啟動與子實例斷開連線

若要斷開子實例的連線：

1. 在子實例的主功能中，轉至**設定→租用戶**。
螢幕上將顯示租用戶清單。

2. 選取要斷開連線的根租用戶旁的核取方塊。

3. 在工具列中，按一下**中斷連線**按鈕，然後在顯示的確認對話方塊中，按一下**中斷連線**。

子實例隨即與父實例斷開連線，對應的訊息將顯示在螢幕上。父實例的使用者將收到電子郵件通知。

斷開連線結果

由於子實例斷開連線，OSMP層次結構被破壞。

在父實例中：

- 斷開連線的實例的資源和設定將被刪除。
- 已複製到父實例的子實例資料現在已從父實例中刪除。

在子實例中：

- 父實例的資訊將被刪除，且父實例不會顯示在子實例租用戶層次結構中。
- 子實例租用戶層次結構的管理追溯到子實例。
- 身分和存取管理器仍以唯讀模式可用。
子實例的使用者仍可登入該實例，但不能執行任何其他操作（建立使用者、指派權限、變更密碼等）。
在子實例連線到層次結構之前，在該子實例上建立的使用者將從子實例中刪除。

- 如果從父實例繼承的實體在父實例上沒有關聯物件，則這些實體會立即從子實例中刪除。否則，該實體將不再顯示在子實例上，但仍以唯讀模式保留90天。該期間過後，資料將被刪除。
- 從父實例繼承的資產類別現在由子實例進行管理。
- 父實例管理的服務將被刪除。

層級結構中關聯規則的分發

OSMP 支援在組成層級結構的 OSMP 實例之間集中管理與分發關聯規則。

您可以在父 OSMP 實例上建立關聯規則，並自動將其分發到子實例。在 OSMP 的子實例上，繼承的關聯規則可供使用，但無法修改。若要進行變更，您需要建立繼承規則的本機副本（複製該關聯規則）。之後，變更只會套用至本機副本。由於資料夾名稱不同，OSMP 父實例和子實例上的資源路徑也不同；但是，資源本身及其包含的變更是同步的。

集中式管理可確保在具有多個 OSMP 實例的分散式基礎架構中統一使用關聯規則，降低規則維護成本，並支援一致的威脅偵測。

關鍵術語

*全域規則*是在OSMP父實例上建立並分發到子實例的關聯規則。

*本機規則*是在OSMP子實例上建立的規則。

*繼承的關聯器*是指OSMP子實例上的關聯器服務，它使用在父實例上建立的關聯器組態。

*繼承的資源*是指從層次結構中的OSMP父實例所取得的資源。

在您開始之前

若要讓規則繼承機制正常運作，必須滿足下列條件：

1. OSMP實例層級結構已設定。

   OSMP實例組織成一個層級結構，包含一個父實例和一個或多個子實例。

2. OSMP子實例已連線到OSMP父實例。

此功能可實現的操作

OSMP父實例可以執行下列操作：

- 建立全域關聯規則並將這些規則分發到OSMP子實例。
- 查看在OSMP子實例上建立的資源和服務。

以下操作位於活動服務部分：

- 新增服務
- 更新服務設定
- 重新啟動服務
- 刪除子實例的服務
- 查看服務事件
- 查看活動清單
- 查看快顯表單
- 查看部分
- 下載日誌和轉儲檔案
- 複製服務ID
- 複製叢集ID
- 重新設置憑證

OSMP子實例可以執行下列操作：

- 使用繼承的規則，但無法編輯它們
- 建立全域規則的本機副本

以下針對繼承服務的操作**活動服務**部分：

- 查看服務日誌
- 更新服務設定
- 查看服務組態

限制

對於OSMP子實例上繼承的關聯規則，規則無法編輯或刪除，無法變更連結到的服務，也無法修改關聯器設定。

要編輯繼承的關聯規則，需要在OSMP子實例上建立副本規則。

副本規則將成為可編輯的本機資源。

規則生命週期

更新父規則

全域規則修改後，變更不會自動分發。如需套用更改，您需要重新啟動關聯器服務或

更新服務設定。

之後，變更才會套用到OSMP子實例。

刪除父實例上的規則

如果在OSMP父實例上刪除全域規則，則OSMP子實例上繼承的規則不會自動刪除。繼承的規則會成為本機資源，OSMP子實例將獲得對該資源的完全權限。

複製規則

如果在OSMP子實例上複製全域規則，則會建立該規則的本機副本，OSMP子實例將取得對該副本的完全權限（讀取、寫入、刪除）。

匯出和匯入

可以將繼承的規則匯出或匯入到另一個OSMP實例。

匯入後，該規則將成為可編輯的本機資源。

連線暫時中斷

如果OSMP實例之間的連線暫時中斷，則會立即傳送最大64MB的資料包，更大的資料包將被拒絕並傳回錯誤。

連線恢復後，子實例將收到遺失的變更。

層級結構拆分

如果子實例從層級結構中分離出來，其繼承的服務和規則將變為本機規則，並可進行編輯和刪除。

使用案例

您可以執行以下操作：

- 將全域關聯器組態與全域關聯規則一起分發
- 分發全域關聯規則以供本機使用
- 在子實例上複製繼承的關聯規則
- 查看在OSMP子實例上建立的規則。

將全域關聯器組態與全域關聯規則一起分發

將全域規則作為繼承關聯器的一部分分發到OSMP子實例：

1. 在OSMP父實例上：
   a. 建立全域關聯規則：
      1. 轉至**資源和服務→關聯規則**區段。
      2. 建立關聯規則。
      3. 在關聯規則的設定中，啟用**在子節點上啟用繼承**切換開關。
      4. 在下拉清單中，指定要將規則分發到的一個或多個OSMP子實例的租用戶。
      5. 儲存關聯規則。

      建立的關聯規則必須關聯到關聯器服務。
   b. 建立將在OSMP子實例上繼承的關聯器服務，並關聯全域關聯規則：
      1. 轉至**資源和服務→關聯器**區段。
      2. 建立關聯器，並在安裝精靈的**常規**步驟中，啟用**在子節點上啟用繼承**切換開關。
      3. 在下拉清單中，指定要將關聯器組態分發到的一個或多個OSMP子實例租用戶。
      4. 在安裝精靈的**關聯**步驟中，關聯全域關聯規則。
      5. 儲存關聯器服務的設定。

      儲存設定後，關聯器服務的組態和全域關聯規則會儲存在OSMP父實例上，並傳播到OSMP子實例。關聯器服務的後續組態和安裝會在OSMP子實例上執行。

2. 在OSMP子實例上：

    a. 轉至**資源與服務→關聯器**區段，並在服務表中開啟繼承的關聯器服務。

        1. 在關聯器的安裝精靈的**路由**步驟中，指定目標位置：

        - 儲存事件和警示的儲存體。
        - OSMP父實例上的關聯器，用於進一步處理事件。

        1. 在**設定驗證**頁籤中，按一下**建立並儲存服務**。
        2. 複製**關聯器安裝建議**命令下的安裝命令，並在OSMP子實例的主機上安裝關聯器服務。

安裝完成後，在OSMP子實例上：

- 將建立關聯規則的副本；
- 將建立關聯的依賴資源；
- 將建立繼承的關聯器組態。即使關聯器內部使用的資源沒有單獨繼承，例如回應規則，它們也會被繼承。
- 關聯規則和關聯器服務的組態以讀取模式提供，並允許指定目標位置。
- 此服務將顯示在OSMP父實例的**活動服務**部分，並標示它是繼承的服務。
- 在OSMP父實例上所做的變更會自動向下繼承到子實例。

分發全域關聯規則供本機使用

將全域規則分發給OSMP子實例並將它們關聯到本機關聯器：

1. 在OSMP父實例上：

    a. 轉至**資源和服務→關聯規則**區段。

    b. 建立關聯規則。

    c. 在關聯規則的設定中，啟用**在子節點上啟用繼承**切換開關。

    d. 在下拉清單中，指定要將規則分發到的一個或多個OSMP子實例的租用戶。

    e. 請填寫其餘必填。

    f. 儲存此規則。
    建立的全域關聯規則會傳播到OSMP子實例。繼承的關聯規則必須關聯到關聯器服務。

2. 在OSMP子實例上：

    a. 轉至**資源和服務→關聯器**區段。

    b. 建立關聯器服務或開啟現有服務的設定。

c. 在關聯器的安裝精靈的**關聯**步驟中，將全域關聯規則關聯到本機關聯器服務。

d. 管理其餘必要的設定：

e. 在**設定驗證**步驟中，執行下列操作之一：

- 如果要建立關聯器，請按一下**儲存並建立服務**，然後使用產生的命令將服務安裝到OSMP子實例的主機上。
- 如果要更新活動關聯器的設定，請按一下**儲存並更新服務組態**。

安裝完成後，在OSMP子實例上：

- 將建立關聯規則的副本；
- 關聯器服務顯示在OSMP父實例的**活動服務**部分中，且可以檢視。
- 對OSMP父實例上的關聯規則所做的變更會自動向下繼承到整個層次結構中。

繼承的關聯規則是唯讀的。

如果需要編輯本機使用的規則，請複製關聯規則，並獨立於OSMP父實例使用本機副本。

複製繼承的關聯規則供本機使用

先決條件：

- OSMP實例層級結構已設定。
- OSMP子實例連線到父實例。
- 已在OSMP父實例上建立關聯規則。
- 全域關聯規則的繼承是在OSMP子實例上設定的。

要複製繼承的關聯規則以供本機使用：

1. 在OSMP子實例上，轉至**資源和服務→關聯規則**區段。
2. 在關聯規則表中，找到繼承的規則，並選取它旁邊的核取方塊。
3. 在工具列或選單中（⋮），點選**複製**。
4. 請輸入關聯規則的新名稱。
5. 儲存關聯規則的副本。
6. 開啟已建立的本機關聯規則副本。

7. 做必要的變更。
8. 保存關聯規則。

因此，OSMP子實例上的本機關聯規則副本將獨立於OSMP父實例，您可以編輯、刪除、匯出和變更本機副本的依賴資源。

限制：

複製後，對父規則所做的變更不會套用到本機副本，也不會同步。

查看在 OSMP 子實例中建立的資源和服務

先決條件：

- OSMP實例層級結構已設定。
- OSMP子實例已連線到OSMP父實例。
- 在OSMP子實例上建立資源或服務。

要查看在OSMP子實例上建立的資源：

1. 在OSMP父實例上，轉至**資源和服務→關聯規則**部分。
2. 開啟資源清單。
3. 查看可用的基本資訊：
   - ID。
   - 名稱。
   - 租用戶 ID
   - 租用戶名稱。
   - 遠端租用戶（OSMP子實例的租用戶）指示器
   - 規則類型
   - 最後更新（日期）
   - 標記
   - MITRE 技術。
   - 套件名稱（如果資源是透過卡巴斯基更新伺服器取得）
   - 描述

- 資源路徑

  父實例和子實例上的資料夾名稱不同，因此路徑也不同。但是，在適用的情況下，變更將進行同步。

要查看完整資訊，請打開關聯規則卡片。

若要檢視在OSMP子實例上建立的關聯器服務：

1. 在主應用程式視窗中，轉至**資源和服務→活動服務**區段。
2. 在服務清單中，開啟一項服務進行檢視。

因此，在OSMP父實例上：

- 此時會顯示子實例的資源和服務。
- 資源和服務為唯讀模式。
- 支援搜尋和篩選功能。
- 開啟資源卡時，關聯規則的完整資訊會直接從OSMP子實例載入。

以下涉及OSMP子實例資源的操作在OSMP父實例上無法使用：

- 複製
- 刪除
- 檢視依賴項清單
- 指派標籤
- 關聯至關聯器
- 指派和檢視排除項清單
- 檢視歷史版本
- 使用父實例關聯器中的資源

在階層中分發資源時的資料夾行為

資源會與分發時的資料夾路徑相關聯。如果您未手動重新命名或移動資料夾，路由將不會變更。OSMP 實例之間的資料夾結構變更不會同步。

在層次結構中分發資源時，適用以下規則：

1. 僅會傳輸包含至少一個分發資源的資料夾。
2. 資料夾會依其完整路徑在實例之間進行對應。
3. 資料夾 ID 不會傳輸：在目標實例上，資料夾建立時會使用新的 ID。

4. 匯入期間，現有資料夾結構不會被取代，而是會與匯入的資料夾結構合併。
5. 資料夾操作（建立、重新命名及移動）不會直接同步。只有在分發位於對應資料夾中的資源後，變更才會顯示。

建立資料夾

在子實例上建立的新資料夾，必須等到該資料夾中至少建立一個分發資源後，才會在父 OSMP 實例上顯示。

重新命名資料夾

重新命名資料夾不會自動更新其他 OSMP 實例上的資料夾結構。

重新命名後，預期會有以下行為：

- 在資料夾名稱變更前分發的資源，仍會與舊路徑相關聯。
- 重新命名後分發的資源會使用新路徑。

範例

初始狀態：

- 父實例：資料夾 A 包含資源 R1。
- R1 資源由子實例繼承。

變更：

- 在子實例上，資料夾 A 重新命名為 B。
- 在資料夾 B 中建立新資源 R2，並將其分發至父實例。

結果：

- 在父實例上，R1 位於資料夾 A 中；R2 位於資料夾 B 中。
- 在子實例上：R1 和 R2 位於資料夾 B 中。

每個資源都會與資源分發時存在的資料夾路徑相關聯。因此，為維持穩定的路由，建議不要手動重新命名或移動資料夾。

將 OSMP 實例組合成階層

本節說明如何將 OSMP 實例組合成階層。

1 先決條件

至少需要兩個 OSMP 實例：一個父實例和一個子實例。

本節將以下列網域名稱作為範例：

- 對於父實例：
  - 網頁介面：`console.edrparent.organization.acme`
  - API：`api.edrparent.organization.acme`
- 對於子實例：
  - 網頁介面：`console.edrchild1.organization.acme`
  - API：`api.edrchild1.organization.acme`
- 對於所有實例：
  - 必須透過連接埠 443 與每個實例的 IP 位址建立雙向通訊。
  - 父實例必須能夠存取子實例的 API 網域名稱，而所有子實例都必須能夠存取父實例的 API 網域。

2 準備父實例

1. 在即將作為父實例的實例主選單中，前往**設定** → **API 權杖**區段，然後按一下**新增權杖**按鈕。
2. 在**名稱**欄位中，輸入 API 權杖的名稱（例如 `edrparenthierarchy`）。
   完成與子節點的連線後，您可以撤銷此權杖。
3. 在**到期日**欄位中，指定權杖到期日。設定此日期時，請考量完成階層建置所需的最短時間（至少一天）。
4. 在**API 方法**部分，選取以下方法對應的核取方塊：
   - **GET:/api/hierman/v1/***
   - **POST:/api/hierman/v1/***
5. 按一下**產生**，然後按一下**複製並關閉**。
   API權杖隨即建立並複製到剪貼簿。請妥善保存，因為之後將無法複製。

6. 取得憑證的指紋，以驗證與實例的連線。若要執行此操作，請在瀏覽器中開啟父實例的 API 網域（`api.edrparent.organization.acme`），並檢視憑證詳細資訊。

   請確保指紋來自可信任的來源。檢查其 IP 位址，以確保網域未遭偽造。

3 每個子實例的步驟

1. 前往預定子實例的 Web 介面（在此範例中為`console.edrchild1.organization.acme`）。
2. 在主功能表中，轉至**設定** → **租用戶**。
3. 在工具列上，點擊**請求連線**按鈕。
4. 在開啟的右側窗格中，執行以下操作：
   - 在**父實例的 API URL**欄位中，指定父實例的 API 位址（在此範例中為`api.edrparent.organization.acme`）。
   - 在**父實例憑證指紋**中，指定父實例憑證的雜湊值。
   - 在**API 權杖**欄位中，指定先前在父實例中建立的 API權杖。
5. 點擊**請求**按鈕。

   如果所有欄位皆正確填寫，則會顯示*您的請求已發送*訊息。
6. 導覽至**父**實例（在此範例中為`console.edrparent.organization.acme`）。
7. 在主功能表中，轉至**設定** → **租用戶**。

   畫面會顯示*等待連線請求*訊息。如果訊息未顯示，請重新整理頁面。
8. 按一下**檢視請求**。

   這會開啟一個視窗，其中包含子實例的詳細資料。
9. 仔細檢查填寫的欄位和位址。尤其請注意**憑證指紋**欄位：必須透過子實例憑證的可信任來源驗證其值。檢查 IP 位址，確保網域（在此範例中為`api.edrchild1.organization.acme`）未遭到偽造。
10. 如果所有欄位皆正確填寫，請點擊**批准**按鈕。
11. 在開啟的**核准連線請求**窗格中，執行以下操作：
    - 在**根租用戶名稱**欄位中，為要連線的子實例租用戶指定一個新名稱。子實例的根租用戶會以此名稱在父實例中註冊。
    - 在**根租用戶名稱**部分，從父實例的租用戶層次結構中，選擇一個租用戶作為子實例租用戶的父租用戶。
    - 點擊**批准**按鈕。

      窗格隨即關閉。子實例將會被加入到父實例的租用戶層次結構中。畫面上會顯示*根租用戶已連線至實例*訊息。
12. 重新整理頁面後，您會在租用戶樹狀結構中看到一個包含子實例層次結構的新節點。

憑證輪替後修復實例層次結構

建置OSMP實例層次結構時，需要在父實例憑證的指紋欄位**父實例憑證指紋憑證**。指定憑證輪替後，憑證層次結構就會被打破。例如，這種情況可能由以下原因造成：

- 您是從先前的版本升級了Kaspersky Next XDR Expert，或是在同一主版本內進行了更新。
- 憑證到期後將自動替換。
- 您已手動替換憑證。

當層次結構被打破時，OSMP會將下列錯誤新增到hierman元件的日誌檔中：「鏈中沒有任何憑證符合預期的指紋」。

憑證輪替後修復實例層次結構：

1. 在OSMP父實例的管理員主機上，執行下列命令：

   ```
   ./kdt invoke hierman --action hiermanRepairTrust
   ```

2. 在層次結構中包含的OSMP子實例的管理員主機上執行相同的命令。

層次結構隨即修復。

與其他解決方案整合

與其他解決方案整合可讓您擴充Kaspersky Next XDR Expert的功能。

Kaspersky Next XDR Expert支援與以下卡巴斯基和協力廠商解決方案整合：

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal
- Kaspersky Anti-Targeted Attack Platform / Kaspersky Endpoint Detection and Response
- Active Directory
- UserGate
- Ideco NGFW
- Ideco UTM
- Redmine
- Check Point NGFW
- Sophos Firewall
- Continent 4
- SKDPU NT
- FortiGate
- Palo Alto NGFW

Kaspersky Next XDR Expert也支援100多個事件來源。有關受支援的事件來源的完整清單，請參閱受支援的事件來源部分。

可以為任何級別的租用戶指定整合設定。父整合設定將複製到子租用戶。您可以編輯複製的子整合設定，因為子設定和父設定不相關，子設定的變更不會影響父租用戶中的設定。

對於共用租用戶，您不需要配置整合設定。

如果需要停用整合，您可以在**設定→租用戶**中手動執行此操作。

當指定整合的租用戶被刪除時，與卡巴斯基解決方案的整合也會自動刪除。刪除資料的延遲最多為24小時。恢復整合設定不可用。

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform（以下也稱為 KASAP）是一個線上學習平台，讓使用者能夠在日常工作中學習資訊安全規則和相關威脅，並透過實際案例進行練習。

設定整合後，您可以在Kaspersky Next XDR Expert中執行以下工作：

- 為與警示和事件相關的使用者指派學習課程。
- 更改使用者學習群組。
- 檢視使用者參加的課程及其獲得的憑證資訊。

設定KASAP與KUMA的整合後，KASAP即視為已與Kaspersky Next XDR Expert整合。

設定KASAP與KUMA之間的整合之前，您需要在KASAP中建立授權令牌，並取得用於API請求的URL。

建立權杖

要授權從KUMA到KASAP的API請求，必須使用在KASAP中建立的令牌對請求進行簽署。

只有公司管理員可以建立令牌。

若要建立令牌：

1. 登入KASAP網頁介面。
2. 在**儀表板**部分，選擇**匯入和同步**部分，然後開啟**OpenAPI**頁籤。
3. 點擊**新建令牌**按鈕。
4. 在開啟的視窗中，選擇整合期間可用的令牌權限：
   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid
5. 點選**產生令牌**按鈕。
   產生的令牌將顯示在螢幕上。

6. 複製令牌並以任何方便的方式儲存。若要設定 KASAP 和 KUMA 之間的整合，需要此令牌。

令牌不會以開啟的表單形式儲存在KASAP系統中。關閉**建立令牌**視窗後，您將無法檢視該令牌。如果您關閉視窗而不複製令牌，則需要點擊**重新簽發令牌**按鈕，系統才會產生新的令牌。

簽發的令牌有效期為12個月。

獲得用於API請求的URL

此URL用於透過OpenAPI與KASAP進行互動。設定KASAP與KUMA整合時，必須指定此URL。

若要獲得KASAP中用於API請求的URL：

1. 登入KASAP網頁介面。
2. 在**儀表板**部分，選擇**匯入和同步**部分，然後開啟**OpenAPI**頁籤。
3. 在**OpenAPI URL**欄位中，複製URL，然後以任何方便的方式儲存。

與Kaspersky Threat Intelligence Portal整合

您必須設定與Kaspersky Threat Intelligence Portal（以下也稱為Kaspersky TIP）的整合，才能獲取可觀察物件的信譽資訊。

在進行設定前，您必須在 Kaspersky TIP 或 Kaspersky OpenTIP 上建立 API 請求的授權權杖。

若要設定Kaspersky Next XDR Expert與Kaspersky TIP之間的整合：

1. 在主功能表中，轉至**設定 → 租用戶**。
   螢幕上將顯示租用戶清單。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 轉至**設定**頁籤，然後選擇**Kaspersky TIP**部分。

如果您被分配了以下其中一個**XDR角色**：主管理員、租用戶管理員或SOC管理員，您可以編輯Kaspersky TIP部分。

4. 如果您在步驟2中選擇了根租用戶，則可以開啟**代理**切換按鈕，使用代理伺服器與Kaspersky TIP進行互動。
   代理伺服器在根管理伺服器內容中設定。
5. 在**快取存續時間**欄位中，指定快取儲存時間段和組件：天或小時。
   預設情況下，設定為7天。如果您未指定任何值，則快取儲存時間段不受限制。

您可以為所有連線設定快取儲存時間段。

6. 為以下其中一項服務開啟**整合**切換按鈕：

   - **Kaspersky TIP（通用存取）**

     新增授權令牌後，您將能夠從Kaspersky TIP獲取有關**警示**或事件詳情中可觀察物件頁籤中所列的下列可觀察物件類型：網域、URL、IP、MD5、SHA256。該資訊隨即在**擴充**列中更新。請求資料時會消耗配額。

   - **Kaspersky TIP（進階存取）**

     新增授權令牌後，您將能夠執行以下操作：

     - 從Kaspersky TIP獲取有關**警示**或事件詳細資訊中可觀察物件頁籤中列出的以下類型的可觀察物件的資訊：網域、URL、IP、MD5、SHA256。該資訊隨即在**擴充**列中更新。請求資料時會消耗配額。
     - 從Kaspersky TIP獲取有關警示或事件詳細資訊中**可觀察物件**頁籤中列出的以下類型的可觀察物件的資訊：網域、URL、IP、MD5、SHA256。此資訊隨即在**狀態更新**列中更新。請求資料時不會消耗配額。

7. 按一下**新增令牌**按鈕。

8. 在開啟的視窗中，輸入授權令牌，然後按一下**新增**按鈕。

   有關為API請求生成授權令牌的詳細資訊，請參閱Kaspersky TIP或Kaspersky OpenTIP說明。

   新增令牌後，您可以按一下**取代**按鈕，然後在開啟的視窗中輸入新令牌來變更它。如果令牌已過期，則可能需要執行此操作。

9. 按一下**儲存**按鈕。

設定與KATA/KEDR的整合

如果從 KEDR 7.1 遷移後，您擁有的端點代理程式不支援與Kaspersky Next XDR Expert 2.0或2.1整合，則您可能需要此說明。

Kaspersky Endpoint Detection and Response（以下也稱為 KEDR）是Kaspersky Anti Targeted Attack Platform（以下也稱為 KATA）的功能區塊，用於保護企業區域網路中的資產。

您可以配置Kaspersky Next XDR Expert與KATA/KEDR之間的整合，以管理連接到Kaspersky Endpoint Detection and Response伺服器的資產上的威脅回應操作。執行操作的命令由Kaspersky Endpoint Detection and Response伺服器接收，然後將這些命令轉發到安裝在資產上的Kaspersky Endpoint Agent。

若要設定Kaspersky Next XDR Expert與KATA/KEDR之間的整合：

1. 在主功能表中，轉至**設定 → 租用戶**。

   螢幕上將顯示租用戶清單。

2. 按一下所需政策的名稱。

   租用戶內容視窗隨即開啟。

3. 轉到**設定**頁籤，然後選擇**KATA/KEDR**部分。

> 如果您被指派了以下其中一個**XDR 角色**，則可以編輯KATA/KEDR部分：主管理員、租用戶管理員或SOC管理員。

4. 開啟**KATA整合**切換按鈕。

5. 按一下**新增連線**按鈕，然後在開啟的視窗中指定設定檔名稱。

   a. 在**IP 位址或主機名稱**欄位中，輸入以下其中一項內容：

   - 主機名稱
   - IPv4
   - IPv6

   b. 在**連接埠**欄位中，設定一個連接埠。

   c. 按一下**儲存**按鈕。

   視窗隨即關閉。

   若未建立連線，則會顯示錯誤訊息。

   如果新增連線成功，螢幕上會顯示對應的訊息。XDR ID、憑證和私密金鑰隨即產生並顯示在相應的欄位中。如有需要，您可以按一下**產生**按鈕產生新的憑證和私密金鑰。

   為確保連線成功建立，請按一下**檢查連線**按鈕。結果顯示在**連線狀態**參數中。

6. 按一下**儲存**按鈕以儲存變更。

   新增連線後，您可以點選對應的圖示進行編輯或刪除。您也可以透過執行步驟1至6來新增其他連線。

如果要接收有關Kaspersky Endpoint Detection and Response警示的訊息，則需要配置KUMA元件與KATA/KEDR之間的整合。

如果您尚未在所有受管主機上將端點安全應用程式升級至新版本，則在升級完成前，威脅回應動作仍會透過與 Kaspersky Anti Targeted Attack Platform (KATA) 的整合進行管理。在此情況下，事件回應平台會向 KATA 傳送請求，然後 KATA 會向端點安全應用程式傳送請求。

設定Kaspersky Next XDR Expert與指令碼啟動服務的整合

您可以透過外部系統在遠端用戶端裝置上啟動協力廠商指令碼，以回應警示和事件。若要啟用此選項，您必須設定環境以及Kaspersky Next XDR Expert與指令碼啟動服務之間的整合。

若要設定啟動協力廠商自訂指令碼的環境，您必須：

- 設定啟動協力廠商自訂指令碼的裝置。
- 設定Kaspersky Next XDR Expert與指令碼啟動服務之間的整合。
- 建立用於啟動指令碼的常規程式。

客戶提供對協力廠商自訂指令碼的存取權限並更新指令碼。

若要設定Kaspersky Next XDR Expert與指令碼啟動服務之間的整合：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
   螢幕上將顯示租用戶清單。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 轉到**設定**頁籤，然後在**自訂整合**部分中：
   - 開啟**自訂整合**切換按鈕。
   - 在**遠端主機驗證**部分，開啟**連線前驗證主機**切換按鈕，然後填寫**公開金鑰**欄位以在Kaspersky Next XDR Expert中啟用用戶端裝置驗證。
   - 在**遠端主機連線**部分，執行以下操作：
     - 填寫**IP位址或主機名稱**和**連接埠**欄位。
     - 選擇將用於與遠端裝置建立安全連線的**SSH驗證方法**：
       - **使用者名稱和密碼**。如果選擇此驗證方法，則下一步必須輸入使用者名稱和密碼。
       - **SSH金鑰**。如果選擇此驗證方法，則下一步必須輸入使用者名稱和SSH金鑰的私密部分。
     - 按一下**新增資料**按鈕。
4. 在開啟的視窗中，變更所需設定，然後按一下**儲存**按鈕。
   如果要編輯已儲存的資料，請按一下**取代**按鈕，在開啟的視窗中輸入新資料，然後儲存編輯。
   為確保連線成功建立，請按一下**檢查連線**按鈕。結果顯示在**連線狀態**參數中。
5. 按一下**儲存**按鈕以儲存變更。

Kaspersky Next XDR Expert與指令碼啟動服務之間的整合已設定。您可以透過啟動常規程式在遠端裝置上執行回應操作。

威脅偵測

Kaspersky Next XDR Expert 將警示和事件用作供分析師處理的工作項目。

如果符合以下條件，主選單中將顯示**警示**和**事件**部分：

- 您擁有Kaspersky Next XDR Expert的產品授權金鑰。
- 您已連線到OSMP主控台中的根管理伺服器。
- 您具有以下XDR角色之一：主管理員、租用戶管理員、初級分析師、一級分析師、二級分析師、 SOC管理員、與NCIRCC互動、核准人、稽核員。

搭配警示一起使用

本節包含有關警示、其內容、典型生命週期以及與事件連線的一般資訊。所提供的說明將幫助您分析警示表、根據生命週期的當前狀態變更警示屬性以及透過連結或取消連結將警示組合成事件。

若符合下列條件，則主選單中會顯示**警示**部分：

- 您擁有Kaspersky Next XDR Expert的產品授權金鑰。
- 您已連線到OSMP主控台中的根管理伺服器。
- 您具有以下XDR角色之一：主管理員、租用戶管理員、初級分析師、一級分析師、二級分析師、 SOC管理員、與NCIRCC互動、核准人、稽核員。

關於警示

*警示*是組織 IT 基礎架構中的事件，Kaspersky Next XDR Expert 將其標記為異常或可疑，且可能對組織 IT 基礎架構的安全性構成威脅。

當 EPP 應用程式（例如 Kaspersky Endpoint Security for Windows）偵測到基礎架構中符合偵測規則所定義條件的特定活動時，Kaspersky Next XDR Expert 會產生警示。

警示會在KUMA關聯事件發生後30秒內建立。如果您之前設定了通知模板，則會收到相應的電子郵件通知。

您也可以從一組事件中手動建立警示。

偵測後，Kaspersky Next XDR Expert 會將警示以待分析人員處理的工作項目形式新增至警示表。您無法刪除警示。您只能關閉警示。

事件只能指派給具有讀取和修改警示和事件之存取權限的分析人員。

您可以使用下列警報屬性將警示作為工作項目進行管理：

- **警示狀態**

  可能的值：**新增**、**調查中**、**已關閉**或**在事件中**。

  警示狀態顯示警示在其生命週期中的目前狀態。您可以根據需要變更狀態，但有以下例外：

  - 您無法將已關閉的警示返回**調查中**狀態。已關閉的警示只能返回到*新增*狀態，然後才能將狀態變更為**調查中**。
  - 您不能手動設定**在事件中**狀態。當警示連結到事件時，它們會獲得此狀態。
  - 您只能將連結的警示設定為**已關閉**狀態。若要設定**新增**或**調查中**狀態，您必須先取消警示與事件的連結。

- **警示嚴重等級。**

  可能的數值：**低**、**中**、**高**或**緊急**。

  警示嚴重等級顯示根據卡巴斯基經驗，此警示可能對電腦安全或企業LAN安全產生的影響。嚴重等級是自動定義的，不能手動變更。

- **警示受讓人**

  這是警示所有者，負責警示調查和處理的分析師。您可以隨時變更警示的受讓人。您無法變更已關閉警示的受讓人。

您可以將警示合併並連結到更大的工作項目（稱為*事件*）。您可以手動將警示連結到事件，也可以啟用規則來建立事件並自動連結警示。透過使用事件，分析師可以將多個警示作為一個問題進行調查。將目前未連結的警示連結到事件時，警示將失去其目前狀態並取得狀態**在事件中**。您可以將當前連結的警示連結到另一個事件。在這種情況下，將保留警示**在事件中**的狀態。您最多可以將200個警示連結到一個事件。

每個警示都有*警示詳情*，其中提供與該警示相關的所有資訊。您可以使用這些資訊來調查警示、追蹤警示之前的事件、檢視偵測產出物、受影響的資產或將警示連結到事件。

警示資料模型

警示的結構由包含值的欄位表示（參見下表）。某些欄位是物件或物件陣列，且具有自身的一組欄位（例如，`Assignee` 與 `Assets` 欄位）。

警示

欄位	值類型	必要	描述
`InternalID`	字串	是	內部警示ID，格式為UUID。欄位值可能與 `SourceID` 值相符。
`ID`	整數	是	短內部警示ID。
`TenantID`	字串	是	與警示相關的租用戶ID，採用UUID格式。
`CreatedAt`	字串	是	警示產生的日期和時間，採用RFC 3339格式。
`UpdatedAt`	字串	是	上次警示更改的日期和時間，採用RFC 3339格式。
`StatusChangedAt`	字串	否	上次警示狀態變更的日期和時間，採用RFC 3339格式。

Severity	字串	是	警示的嚴重等級。 可能的值： • critical • high • medium • low
IntegrationID	字串	是	整合在OSMP中的卡巴斯基應用程式管理外掛程式的ID。
IntegrationCompatibilityVersion	字串	是	整合在OSMP中的卡巴斯基應用程式管理外掛程式的版本。
SourceID	字串	否	整合元件中的唯一警示識別碼。
SourceCreatedAt	字串	否	整合元件中警示產生的日期和時間，採用RFC 3339格式。
FirstEventTime	字串	是	與警示相關的第一個遙測事件的日期和時間，採用RFC 3339格式。
LastEventTime	字串	是	與警示相關的最後一個遙測事件的日期和時間，採用RFC 3339格式。
DetectSource	字串	否	偵測並產生警示的元件。
DetectionTechnologies	字串陣列	否	觸發的偵測技術。
State	字串	是	警示狀態 可能的值： • new • inProgress • inIncident • closed
StatusResolution	字串	否	警示狀態的解決方案。 可能的值： • truePositive • falsePositive • lowPriority • merged
IncidentID	字串	否	與警示關聯的事件的內部ID。
IncidentLinkType	字串	否	將警示新增至事件的方式。 可能的值： • manual • auto
Assignee	Assignee 物件	否	警示指派給的運算子。
MITRETactics	MITRETactic 物件陣列	否	與警示中所有觸發的IOA規則相關的MITRE策略。
MITRETechniques	MITRETechnique 物件陣列	否	與警示中所有觸發的IOA規則相關的MITRE技術。
Observables	Observable 物件陣列	否	與警示相關的可觀察物件。
Assets	Asset 物件陣列	否	受警示影響的資產。
Rules	Rule 物件陣列	否	觸發的關聯規則，警示以此為基礎產生。
OriginalEvents	物件陣列	否	事件，警示以此為基礎生成。
ExternalRef	字串	是	連結到外部系統中的實體（例如，指向Jira票證的連結）。
Extra	物件	否	與警示相關的資料，採用JSON格式。這些資料是在事件轉換為警示時從託管的卡巴斯基應用程式中獲取的。此欄位不用於介面。
AdditionalData	物件	否	有關警示的附加資訊，採用JSON格式。此資訊可由使用者或常規程式填寫。
IsCII	布林值	是	指出受影響的資產（裝置或帳戶）是否為緊急資訊基礎設施物件的指標。

Name	字串	是	警示的名稱。
Attachments	UnkeyedAttachment 物件陣列	否	與事件相關的附件。

受讓人

欄位	值類型	必要	描述
ID	字串	是	指派警示的運算子的使用者帳戶ID。
Name	字串	是	指派警示的運算子的名稱。

MITRE策略

欄位	值類型	必要	描述
ID	字串	是	與警示中所有觸發的IOA規則相關的MITRE策略的ID。
Name	字串	是	與警示中所有觸發的IOA規則相關的MITRE策略的名稱。

MITRE技術

欄位	值類型	必要	描述
ID	字串	是	與警示中所有觸發的IOA規則相關的MITRE技術的ID。
Name	字串	是	與警示中所有觸發的IOA規則相關的MITRE技術的名稱。

可觀察物件

欄位	值類型	必要	描述
Type	字串	是	可觀察類型 可能的值： • ip • md5 • sha256 • url • domain • UserName • hostName
Value	字串	是	可觀察物件的值。
Details	字串	否	有關可觀察物件的附加資訊。

規則

欄位	值類型	必要	描述
ID	字串	是	觸發規則的ID。
Name	字串	否	觸發規則的名稱。
Severity	字串	否	觸發規則的嚴重等級。 可能的值： • critical • high • medium • low
Confidence	字串	否	觸發規則的信賴區間。 可能的值： • high • medium • low
Custom	布林值	否	指示警示基於自訂規則。

資產

欄位	值類型	必要	描述
Type	字串	是	受影響資產（裝置或帳戶）的類型。 可能的值： • host • user
ID	字串	是	受影響資產（裝置或帳戶）的ID。
Name	字串	否	與警示關聯的受影響裝置名稱（若 Type 設定為 host ）。 與事件關聯的受影響使用者帳戶的使用者名稱，警示會依據這些事件生成（若 Type 設定為 user ）。
IsAttacker	布林值	否	指示受影響資產（裝置或帳戶）是攻擊者。
IsVictim	布林值	否	指示受影響資產（裝置或帳戶）是受害者。
CIICategory	字串	否	作為緊急資訊基礎設施物件的受影響資產（裝置或帳戶）的重要性類別。 可能的值： • notCII • ciiWithoutCategory • ciiFirstCategory • ciiSecondCategory • ciiThirdCategory

無鍵附件

欄位	值類型	必要	描述
AttachmentID	字串	是	附件ID，格式為UUID。
Name	字串	是	附件名稱。
CreatedAt	字串	是	附件建立的日期和時間（UTC格式）。

`UpdatedAt`	字串	是	附件上次更改的日期和時間（UTC格式）。
`CreatedBy`	字串	是	指示受影響資產（裝置或帳戶）是受害者。
`Size`	整數	是	附件大小（以位元組為單位）。
`State`	字串	是	附件狀態，指示附件上傳是正在進行中、已完成還是因錯誤而中止。 可能的值： • `completed` • `error` • `uploading`
`Description`	字串	否	附件描述。
`StatusCode`	字串	否	向使用者顯示的狀態文字（例如，附件上傳失敗時顯示的錯誤訊息）。

檢視警示表

警示表顯示在 **監控 → 警示**區段中，並概略顯示 Kaspersky Next XDR Expert 中登錄的所有警示。預設情況下，該表顯示與您有存取權限的所有租用戶相關的警示。如有必要，您可以配置警示表。

若要設定警示表，請執行下列其中一項操作：

- 套用租用戶過濾器：
  a. 按一下**租用戶篩選器**設定旁邊的連結。
  租用戶篩選器隨即開啟。
  b. 選取所需事件旁邊的核取方塊。
- 使用以下方法之一篩選警示表中的資料：
  - 使用主篩選器：
    a. 按一下篩選器（ ）圖示。
    b. 在**篩選器**頁籤，在喚起的功能表中指定並套用篩選條件。
  - 篩選掉重新掃描的警示：
    a. 按一下**名稱**直欄的標頭。
    b. 選取**僅重新掃描的警示**或**排除重新掃描的警示**核取方塊。
  - 使用儲存格上下文篩選器可以快速新增的篩選條件：
    a. 找到包含要新增為篩選條件的值的儲存格。請注意，有些直欄沒有儲存格上下文篩選器。
    b. 按一下儲存格中的值。

c. 在開啟的清單中，執行以下操作之一：

- **新增至篩選器**中，將該值新增至篩選條件。
- **從篩選器中排除**，將該值從篩選條件中排除。
- **複製**，將該值複製到剪貼簿。

- 如果要隱藏或顯示某一直欄，請按一下設定（ ⚙ ）圖示，然後選擇所需的直欄。

警示表已配置並顯示您需要的資料。

警示表具有以下列：

- **已註冊**。警示添加到警示表的日期和時間。
- **已更新**。警示歷程記錄中上次變更的日期和時間。
- **警示ID**。警示的唯一 ID。
- **狀態**。警示的目前狀態。
- **事件連連結類型**將警示新增至事件的方式。
- **嚴重度**。警示的嚴重等級。
- **名稱**。警示的名稱。
- **偵測到的物件類別**。偵測到的物件的一個或多個類別。例如，當Kaspersky Next XDR Expert偵測到感染了Trojan-Downloader.JS.Cryptoload.ad病毒的檔案時，**偵測到的物件類別**欄位會顯示此警示的Trojan-Downloader.JS.Cryptoload.ad類別。
- **受影響的資產**。受警示影響的裝置和使用者。

  從資產新增至 OSMP 起，大約需要 2 分鐘，解決方案才能開始使用此資產擴充事件資訊。例如，如果在新增資產後兩分鐘內發生關聯事件，產生的警示中將不會顯示此資產。
- **已指派**。警示的當前受讓人。
- **可觀察物件**。偵測產出物，例如IP位址或檔案的MD5雜湊值。
- **詳細資訊**。警示的簡要摘要。
- **狀態已變更**。上次警示狀態變更的日期和時間。
- **租用戶**。偵測到警示的租用戶的名稱。
- **外部參考**。外部系統中的警示編號。
- **CII 物件**。顯示警示是否與 CII 物件相關資產相關聯的指標。
- **技術**。掃描過程中產生警示的模組或組件的名稱。

此直欄的可能值：

- IOA
- SB (Sandbox)
- AM（反惡意軟體引擎）。
- IOC
- YARA
- KUMA

IOA規則觸發的警示中事件彙總的特殊注意事項

如果 Kaspersky Next XDR Expert 建立由 IOA 規則觸發的警示，而同一天此主機或其他主機上的其他事件也觸發相同的 IOA 規則，Kaspersky Next XDR Expert 會將這些事件彙總至同一個警示中。如果警示已關閉，Kaspersky Next XDR Expert會將其重新開啟。事件彙總期間於次日00:00結束。

檢視警示詳情

警示詳情是介面中的一個頁面，其中包含與警示相關的所有信息，包括警示內容。

若要檢視警示詳情：

1. 在主功能表中，轉至**監控→ 警示**。
2. 在警示表中，按一下所需警示的ID。

   將顯示警示詳情。

如有必要，您可以透過按一下警示名稱旁邊的重新整理 (🔄) 圖示來重新整理警示詳情中的資訊。

警示詳情上部的工具列可讓您執行以下操作：

- 編輯**外部參考**欄位值
- 將警示分配給分析師
- 變更警示狀態
- 將警示連結到事件
- 取消警示與事件的連結
- 選取常規程式。
- 建立新事件並將警示連結到它

根據警示類型，警示詳情包含以下部分：

- **摘要**

  根據警示類型，摘要部分可能包含以下警示內容：

  - **分析師**。指派了警示的分析師。
  - **名稱**。警示的名稱。如果未指定警示名稱，則不顯示此欄位。
  - **租用戶**。偵測到警示的租用戶的名稱。
  - **資產**。與警示相關的使用者帳戶和裝置的數量。
  - **嚴重等級**。可能的數值：**低**、**中**、**高**或**緊急**。警示嚴重等級顯示根據卡巴斯基經驗，此警示可能對電腦安全或企業LAN安全產生的影響。
  - **規則**。觸發以檢測警示的規則。透過點擊規則名稱旁邊的省略號圖標，可以開啟快顯表單。使用此功能表可以了解有關規則的更多詳細信息，查找由相同規則檢測到的警示或事件，或在**威脅搜尋**中搜尋觸發規則的事件，以查找警示的第一個事件和最後一個事件之間的時間段。

    點擊功能表中的**轉到威脅搜尋**時，**威脅搜尋**區域將於同一索引標籤中開啟。區域標題會顯示您深入檢視至此處的來源警示 ID 和名稱。如果您想在新的瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住`Ctrl`金鑰，然後在功能表中點擊**轉到威脅搜尋**區域。

  - **已註冊**。警示添加到警示表的日期和時間。
  - **第一個事件**。與警示相關的第一個事件的日期和時間。
  - **最後一個事件**。與警示相關的最後一個事件的日期和時間。
  - **外部參考**。連結到外部系統中的實體（例如，指向Jira票證的連結）。您可以點擊頂部的**編輯**按鈕指定外部參考。如果警示是從Kaspersky Endpoint Detection and Response警示建立的，則欄位中將顯示指向此警示的連結。
  - **已連結到**。警示所連結到的事件。
  - **MITRE政策**。警示中偵測到的一個或多個政策。按一下MITRE政策名稱即可開啟右鍵功能表。使用快顯表單，您可以執行以下操作：
    - 按一下**在 Kaspersky TIP 中尋找**按鈕，即可在Kaspersky TIP中檢視MITRE策略的詳細資訊。
    - 按一下**在 MITRE ATTCK 中尋找**按鈕，即可在MITRE ATT&CK知識庫中檢視MITRE策略的詳細資訊。
    - 複製MITRE策略名稱。
  - **MITRE技術**。警示中偵測到的一種或多種技術。按一下MITRE技術名稱即可開啟右鍵功能表。使用快顯表單，您可以執行以下操作：
    - 按一下**在 Kaspersky TIP 中尋找**按鈕，即可在Kaspersky TIP中檢視MITRE技術的詳細資訊。
    - 按一下**在 MITRE ATTCK 中尋找**按鈕，即可在MITRE ATT&CK知識庫中檢視MITRE技術的詳細資訊。
    - 複製MITRE技術名稱。

- **關聯規則**。用於偵測威脅並建立警示的關聯規則。
- **IOA規則**。觸發的IOA規則用於偵測威脅並建立警示。按一下IOA規則名稱即可開啟快顯表單。使用快顯表單，您可以執行以下操作：
  - 按一下**開啟內容**按鈕，即可檢視該IOA規則的詳細資訊。
  - 按一下**轉到威脅搜尋**按鈕，即可檢視相關事件。

    您將被重定向到**威脅搜尋**部分，該部分僅顯示此IOA規則追蹤的事件。事件的預設顯示時間間隔為24小時。區域標題會顯示您深入檢視至此處的來源警示 ID 和名稱。
  - 尋找類似事件。
  - 按一下**在 Kaspersky TIP 中尋找**按鈕，即可在Kaspersky TIP中檢視IOA規則的詳細資訊。
  - 複製IOA規則名稱。
- **技術**。用於偵測威脅的偵測技術。
- **偵測來源**。偵測到的物件來源。例如，如果檔案從某個主機傳送到沙盒進行掃描，則該主機即為偵測來源。
- **附加資料**。有關警示的其他資訊。您只能使用常規程式編輯此欄位中的值。如果新增了值，則會顯示該欄位。

- **掃描結果**

  掃描結果部分包含有關已掃描檔案以及觸發警示的掃描結果的資訊。

- **IOC掃描結果**

  IOC掃描結果部分包含有關掃描期間觸發的IOC規則的資訊。

  點選IOC規則名稱，即可檢視該IOC規則的詳細資訊。

  點擊**掃描結果**列中的**檢視報告**，即可檢視掃描結果的詳細信息，包括網路和系統資訊、掃描過程中涉及的進程和檔案。

- **卡巴斯基沙盒掃描結果**

  卡巴斯基沙盒掃描結果部分包含有關沙盒中物件處理結果的信息，包括：
  - 偵測到的物件數量及其類型。
  - 擷取的檔案數量及其類型。
  - 偵測到的物件的雜湊值。

  點擊**匯出結果**，即可檢視沙盒中可用作業系統中物件處理結果的詳細資訊，包括：
  - 包含偵測統計資料的圖表。
  - 包含物件活動樹的圖表。
  - MITRE 戰術和技術（請參閱 MITRE ATT&CK 知識庫）。

- 作業系統中的可疑活動清單。
- 作業系統中檔案執行的螢幕截圖。
- 系統活動。
- 網路活動。

若要取得沙盒掃描結果視窗中的完整資訊，請在作業系統之間切換，並在**快速掃描模式**和**完整日誌記錄模式**之間切換。

- **YARA掃描結果**

  YARA掃描結果部分包含主機上YARA掃描結果的資訊。

  點選**掃描結果**欄位中的**檢視報告**，即可檢視掃描結果的詳細資訊。若要取得YARA掃描結果視窗中的完整資訊，請在**進程和記憶體轉儲** 、 **檔案**和**規則條件**頁籤之間切換。

- **已掃描檔案**

  在**已掃描檔案**部分，您可以找到有關已掃描檔案的資訊。若要了解有關在Kaspersky Threat Intelligence Portal上偵測到的檔案威脅的更多資訊，請點擊**判定**直欄中的威脅名稱。

- **詳細資訊**

  在**詳細資訊**部分中，您可以追蹤與警示相關的遙測事件。

  事件表顯示您透過SQL查詢定義的搜尋結果。

  事件表的工具列可讓您執行以下操作：

  - **下載事件**。您可以按一下此按鈕將相關事件的資訊下載為CSV檔案（UTF-8編碼）。
  - **在威脅搜尋中搜尋**。您可以按一下此按鈕開啟**威脅搜尋**部分。此部分可讓您搜尋與您有權存取的租用戶相關的所有事件，而不僅僅是與當前警示相關的事件。區域標題會顯示您深入檢視至此處的來源警示 ID 和名稱。

    依預設，此部分中開啟的事件表包含該警示第一個事件到最後一個事件之間的期間內發生的所有事件。例如，您可以執行搜尋查詢來尋找裝置受到影響的所有事件。

    在**威脅搜尋**部分，您可以手動將事件連結到警示。如果您發現某些事件與警示相關，但未自動連結到警示，此功能可能會有所幫助。有關詳情，請參閱將事件連結到警示或取消連結到警示的說明。

    您可以按一下**警示調查**，或按一下瀏覽器中的返回按鈕，返回事件詳細資料。
  - **從警示中取消連結**。您可以在表中選擇一個或多個事件，然後按一下此按鈕取消所選事件與警示的連結。

- **資產**

  在**資產**部分，您可以進行以下操作：

  - 檢視受警示影響或涉及的裝置和使用者。
  - 執行回應操作。為此，請選取資產旁的複選框，然後在**選擇回應操作**下拉清單中，選擇所需的回應操作。
  - 透過點擊**匯出到CSV**按鈕，將有關受影響資產的資訊匯出到CSV檔案。
  - 使用遠端終端連線到資產。為此，請點擊**開啟遠端終端**按鈕。

資產表包含以下列：

- **資產類型**

  可能的值：裝置或使用者。

- **資產名稱**

- **資產ID**

- **有跡象**

  可能的值：攻擊者或受害者。

- **授權狀態**

  此參數僅適用於裝置資產類型。裝置授權狀態由KICS for Networks定義。您可以透過對裝置套用相應的回應操作來變更授權狀態。

- **管理伺服器**

  管理裝置的管理伺服器。

- **管理群組**

  裝置所屬的管理群組。

- **類別**

  包含該資產的資產類別。

- **已歸檔**

  資產的歸檔狀態。可能的值： 是或否。

透過點選使用者名稱或裝置名稱，您可以：

- 檢視使用者或裝置內容。

  若要檢視與裝置相關的警示或事件列表，請在裝置內容視窗中按一下**顯示相關**按鈕，然後根據要檢視的內容選擇**警示**或**事件**。

- 在剪貼簿中複製使用者名稱或裝置名稱。

- 在其他警示中搜尋使用者名稱或裝置ID。

- 在其他事件中搜尋使用者名稱或裝置ID。

- 在**威脅搜尋**中搜尋使用者名稱或裝置ID，以尋找警示的第一個事件和最後一個事件之間的週期。

  點擊使用者名稱或裝置名稱後，在功能表中選取**轉到威脅搜尋**，**威脅搜尋**區域將於同一頁籤中開啟。區域標題會顯示您深入檢視至此處的來源警示 ID 和名稱。如果您想在新的瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住`Ctrl`金鑰，然後在功能表中點擊**轉到威脅搜尋**區域。

透過點選使用者ID或裝置ID，您可以：

- 檢視使用者或裝置內容。

  若要檢視與裝置相關的警示或事件列表，請在裝置內容視窗中按一下**顯示相關**按鈕，然後根據要檢視的內容選擇**警示**或**事件**。

- 在剪貼簿中複製使用者ID或裝置ID。
- 在其他警示中搜尋使用者ID或裝置ID。
- 在其他事件中搜尋使用者ID或裝置ID。
- 在**威脅搜尋**中搜尋警示的第一個事件和最後一個事件之間的週期。

  點擊使用者ID或裝置ID後，在功能表中選取**轉到威脅搜尋**，**威脅搜尋**區域將於同一索引標籤中開啟。區域標題會顯示您深入檢視至此處的來源警示 ID 和名稱。如果您想在新的瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住`Ctrl`金鑰，然後在功能表中點擊**轉到威脅搜尋**區域。

從資產新增至 OSMP 起，大約需要 2 分鐘，解決方案才能開始使用此資產擴充事件資訊。例如，如果在新增資產後兩分鐘內發生關聯事件，產生的警示中將不會顯示此資產。

- **檔案**

  檔案部分包含透過回應操作獲得的檔案或手動新增到此警示中的檔案。您可以上傳、下載、刪除與警示相關的檔案，或編輯檔案描述。

  您可以上傳任何擴展名的檔案。允許使用重複的檔案名稱。您可以在組態檔案中指定可附加到事件的最大檔案數量以及最大檔案總大小。

  預設限制：

  - 每個警示的檔案數量不能超過100個。
  - 每個警示的檔案總大小不得超過25MB。

  若要上傳檔案，請點擊**上傳**按鈕並選擇一個或多個檔案。如果您嘗試上傳的檔案超出限制，則會開啟**上傳檔案**窗格，其中顯示一則警告訊息。在此窗格中，您可以從上傳佇列中移除檔案，直到警告訊息消失，然後點擊**上傳**按鈕上傳檔案。如果您忽略警告訊息，上傳將會失敗，檔案清單將包含無法上傳的檔案，檔案名稱旁邊會顯示警告圖示。

  點擊**上傳**按鈕後，窗格會關閉，且上傳的檔案會同時顯示在警示詳情及主選單的**檔案**區段中的檔案表格內。上傳大檔案或多個檔案時，您必須重新整理表格，以便顯示新檔案。如果檔案正在上傳， **名稱或完整路徑**列會顯示載入指示器， **大小**欄位會顯示已上傳的檔案大小佔總檔案大小的比例。

  點擊檔案即可開啟**編輯檔案**窗格，其中顯示檔案詳情。在此窗格中，您可以編輯檔案描述。

  使用核取方塊選擇一個或多個檔案。選擇一個或多個檔案，然後點擊**下載**按鈕，以ZIP格式將其下載為存檔。此存檔受密碼*infected*保護。選擇一個或多個檔案，然後點擊**刪除**按鈕進行刪除。

  上傳、刪除檔案以及編輯檔案描述需要**警示和事件**功能區中的**寫入**權限。下載檔案需要**警示和事件**功能區中的**讀取**權限。

- **可觀察物件**

  在**可觀察物件**區段中，您可以：

  - 檢視與警示相關的可觀察物件。
  - 點擊**匯出至 CSV**按鈕，將相關可觀察物件的資訊匯出至 CSV 檔案。
  - 依據**值**欄中的資料搜尋可觀察物件表格。

    若要執行此操作，請開始在搜尋欄位中輸入所需可觀察物件的資料。如果**值**欄中沒有相符的可觀察物件值，則會顯示空白表格。

  可觀察物件可能包括：

  - MD5 hash
  - URL
  - 網域名稱
  - SHA256
  - 使用者名稱
  - 主機名稱
  - 本機IP位址
  - 遠端IP位址

    以下私有IP位址未包含在與警示相關的可觀察物件中：
    從10.0.0.0到10.255.255.255，子網路遮罩為255.0.0.0或/8
    從172.16.0.0到172.31.255.255，子網路遮罩為255.240.0.0或/12
    從192.168.0.0到192.168.255.255，子網路遮罩為255.255.0.0或/16
    從100.64.0.0到100.127.255.255，子網路遮罩為255.192.0.0或/10

    若要在可觀察物件中包含私有IP位址，請在管理員主機上執行下列命令：

    ```
    k0s kubectl -n irp set env deploy/transformer -c transformer
    OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
    ```

    ```
    k0s kubectl -n irp set env deploy/incident -c incident
    OSMP_FILTER_PRIVATE_IPS_DISABLED=true
    ```

  - 本機連接埠
  - 遠端連接埠
  - 系統進程ID

- 唯一PID
- 檔案全名

透過點選**值**列中的連結，您可以：

- 在**威脅搜尋**中搜尋警示的第一個事件和最後一個事件之間的可觀察物件值。

  點擊**值**欄位中的連結後，在功能表中選取**轉到威脅搜尋**，**威脅搜尋**區域將於同一索引標籤中開啟。區域標題會顯示您深入檢視至此處的來源警示 ID 和名稱。如果您想在新的瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住`Ctrl`金鑰，然後在功能表中點擊**轉到威脅搜尋**區域。

- 在其他警示中搜尋可觀察物件值。
- 在其他事件中搜尋可觀察物件值。
- 將可觀察物件值複製到剪貼簿。

此部分的工具列包含以下按鈕：

- **Kaspersky TIP 的請求狀態**。使用此按鈕可從卡巴斯基Kaspersky Threat Intelligence Portal（卡巴斯基TIP）取得所選可觀察物件的詳細資訊。取得後，**狀態更新**列中的資訊會更新。需要與Kaspersky Threat Intelligence Portal（進階存取權限）整合。
- **擴充來自 Kaspersky TIP 的資料**。使用此按鈕可從卡巴斯基TIP中取得所有列出的可觀察物件的詳細資訊。因此，**資料補足**列中的資訊會更新。使用**資料補足**列中的連結開啟有關可觀察物件的獲取的擴充詳細資訊。需要與Kaspersky Threat Intelligence Portal（進階存取權限）整合。
- **移動到隔離區**。使用此按鈕將檔案所在的裝置移至隔離區。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。
- **新增阻止規則**。使用此按鈕可新增阻止檔案運作的規則。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。
- **刪除阻止規則**。使用此按鈕可刪除封鎖檔案執行的規則。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。
- **終止處理程序**。使用此按鈕可終止與檔案關聯的進程。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。

- **類似已關閉警示**

  在**類似已關閉警示**部分，您可以檢視與目前警示具有相同受影響產出物的已關閉警示清單。受影響的產出物包括可觀察物件和受影響的裝置。類似已關閉警示可以幫助您調查當前警示。

  透過此列表，您可以評估當前警示與其他警示的相似度。相似度計算如下：

  相似度=M/T*100

  這裡，「M」表示目前警示和類似警示中符合的產出物數量，「T」表示目前警示中的產出物總數。

  如果相似度為100%，則目前警示與類似警示相比沒有任何新內容。如果相似度為0%，則目前警示和類似警示完全不同。相似度為0%的警示不會包含在清單中。

計算值將到四捨五入最接近的整數。如果相似度等於0%到1%之間的值，則應用程式不會將該值向下舍入為0%。在這種情況下，該值顯示為小於1%。

按一下警示ID可開啟警示詳情。

自訂類似已關閉警示清單

您可以使用以下選項自訂表格：

- 透過選擇已更新警示的週期來篩選警示。預設情況下，清單包含過去30天內已更新警示。
- 點選**列設定**圖示 (⚙)，然後選擇要顯示的列及其顯示順序。
- 按一下**篩選器**圖示 (▽)，然後選擇並設定要套用的篩選器。如果選擇多個篩選器，它們將透過邏輯「AND」運算子同時套用。
- 按一下列表頭，然後選擇排序選項。您可以依升序或降序對警示進行排序。

- **類似事件**

在**類似事件**部分，您可以檢視與目前警示具有相同受影響產出物的事件清單。受影響的產出物包括可觀察物件和受影響的裝置。類似事件可以幫助您判斷當前警示是否可能與現有事件相關聯。

透過該清單，您可以評估當前警示和事件的相似度。相似度計算如下：

相似度=M/T*100

其中，「M」表示目前警示與類似事件中匹配的產出物數量，「T」表示目前警示中產出物的總數。

如果相似度為100%，則目前警示與類似事件相比沒有任何新內容。如果相似度為0%，則目前警示與類似事件完全不同。相似度為0%的事件不包含在清單中。

計算值將到四捨五入最接近的整數。如果相似度等於0%到1%之間的值，則應用程式不會將該值向下舍入為0%。在這種情況下，該值顯示為小於1%。

按一下事件ID可開啟事件詳細資料。

自訂類似事件清單

您可以使用以下選項自訂表格：

- 透過選擇事件已更新的週期來篩選事件。預設情況下，清單包含過去30天內更新的事件。
- 按一下**列設定**圖示 (⚙)，然後選擇要顯示的列及其顯示順序。
- 按一下**篩選器**圖示 (▽)，然後選擇並設定要套用的篩選器。如果選擇多個篩選器，它們將透過邏輯「AND」運算子同時套用。
- 按一下列標頭，然後選擇排序選項。您可以按升序或降序對事件進行排序。

- **備註**

  在**備注**部分，您可以留下與警示相關的備注。例如，您可以輸入有關調查結果或變更警示內容（如警示受讓人或狀態）時的備注。

  若要儲存您的備注，請按**Enter** 。若要開始新行，請按**Shift+Enter** 。若要編輯或刪除您的備注，請使用右上角的按鈕。

  您只能在留下備註後的指定期間內編輯或刪除自己的備註。預設期間是 15 分鐘。

  如果您想變更此期間，請在管理員主機上執行以下命令：

  ```
  k0s kubectl -n irp set env deploy/comment -c comment
  OSMP_COMMENT_LOCK_AFTER_DURATION=Nx
  ```

  其中 `N` 是時間間隔，而 `x` 是測量單位：`h`（小時）或 `m`（分鐘）。

  其他用戶的備注無法修改或刪除。留下備注需要**警示和事件**功能區中的**寫入**權限。

- **歷程記錄**

  在**警示事件記錄**部分，您可以追蹤作為工作項目對警示所做的更改：

  - 變更警示狀態
  - 變更警示受讓人
  - 將警示連結到事件
  - 取消警示與事件的連結
  - 將檔案上傳到警示
  - 從警示中刪除檔案

  在**回應歷史**部分，您可以查看手動和常規程式回應操作的日誌。資源表包含以下列：

  - **時間**。事件發生的時間。
  - **啟動者**。啟動回應操作的使用者的名稱。
  - **事件**。事件敘述。
  - **回應參數**。回應操作中指定的回應操作參數。
  - **資產**。啟動回應操作的資產數量。您可以點選包含資產數量的連結來檢視資產詳情。
  - **動作狀態**。回應操作的執行狀態。此列可以顯示以下值：
    - **等待核准**– 等待核准啟動的回應操作。
    - **已啟動**– 回應操作正在執行中。
    - **成功**– 回應操作已完成，沒有錯誤或警告。
    - **警告**– 回應操作已完成，但有警告。
    - **錯誤**– 回應操作已完成，但有錯誤。
    - **已停止**– 由於使用者中斷了執行，回應操作已完成。

- **核准時間已過**– 由於啟動的核准時間已過，回應操作已完成。
- **被拒絕**– 由於使用者拒絕了啟動，回應操作已完成。

- **常規程式**。啟動回應操作的常規程式的名稱。您可以單擊連結以查看常規程式詳細資訊。
- **回應動作**。已執行的回應操作的名稱。
- **資產類型** 啟動回應操作所針對的資產類型。可能的值：**裝置**或**使用者**。
- **資產租用戶**。租用戶，即啟動回應操作的資產所有者。

將警示指派給分析師

作為工作項，可以將警示指派給SOC分析師或使用者群組，以進行檢查和可能的調查。如果您想要自動將警示指派給選定群組內的分析師，則可以將警示指派給使用者群組。有關詳情，請參閱設定警示和事件的自動指派。

您可以隨時變更活動警示的受讓人。您無法變更已關閉警示的受讓人。

> 警示只能指派給具有讀取和修改警示和事件存取權限的分析師和使用者群組。

若要指派一個或多個警示：

1. 在主功能表中，轉至**監控** → **警示**。
2. 選取您要安裝之更新旁邊的核取方塊。

   您必須僅選擇在同一租用戶中偵測到的警示。否則， **指派**按鈕將被停用。

   或者，您可以從警示詳情中將警示指派給分析師或使用者群組。若要開啟警示詳情，請按一下包含所需警示ID的連結。
3. 點選**指派**按鈕。
4. 在開啟的**指派給分析師**視窗中，選擇是否將警示指派給使用者或使用者群組。
5. 開始輸入分析師或使用者群組的名稱，然後從清單中選擇受讓人。

   如果要取消指派警示，請選擇**未分配** 。

   > 您可以為所有警示選擇**未分配**（狀態為**已關閉**的警示除外）。
6. 點選**指派**按鈕。

警示已指派。

您也可以使用常規程式來指派警示。

變更警示狀態

作為工作項，警示具有一種狀態，顯示警示在其生命週期中的當前狀態。

只有當您具有讀取和修改警示和事件的存取權限時，才可以變更您自己的警示或其他分析師的警示的狀態。

如果手動變更警示狀態，常規程式將不會自動啟動。您可以手動為此類警示啟動常規程式。

警示可以具有以下一種狀態：

- **新增**

  當 Kaspersky Next XDR Expert 登錄新的警示時，該警示的狀態為*新增*。您可以將狀態變更到*執行中*或*已關閉*。當您將狀態從*新增*變更為*已關閉*，且警示沒有受讓人時，警示將自動指派給您。

- **執行中**

  此狀態表示分析師已開始處理該警示。您可以將*進行中*狀態變更為*新增*或*已關閉*。

- **已關閉**

  確認為真的警示將被連結到事件，並在事件中進行調查。關閉事件時，連結的警示也會獲得*已關閉*狀態。您只能將未連結的警示作為誤報或低優先順序警示關閉。關閉警示時，您必須選擇解決方案。

  狀態*已關閉*只能變更為*新建*。若要將已關閉的警示還原為活動中狀態，請如下所示變更其狀態：*已關閉*→*新*→*進行中*。

  當您關閉連結到事件的警示時，警示將自動與事件取消連結。如果您要關閉的警示沒有受讓人，則警示將自動指派給關閉它的分析師。

- **在事件中**

  當警示連結到事件時，它們將獲得此狀態。此狀態無法手動選擇。只有已連結的警示才能設為*已關閉*狀態。若要將此狀態變更為*新建*或*進行中*，您必須先取消警示與事件的連結。

若要變更一個或多個警示的狀態：

1. 在主功能表中，轉至**監控→ 警示**。
2. 執行下列任一操作：
   - 選中您要變更狀態的警示旁邊的核取方塊。
   - 點選要變更狀態的警示ID連結。

     警示詳細資訊視窗開啟。
3. 點選**變更狀態**按鈕。
4. 在**變更狀態**面板中，選擇要設定的狀態。

   如果選擇*已關閉*狀態，則必須選擇一個解決方案。

如果將警示狀態變更為*已關閉*，且此警示包含未完成的常規程式或回應操作，則所有相關的常規程式和回應操作都將終止。

5. 按一下**儲存**按鈕。

所選警示的狀態已變更。

如果將警示新增至調查圖，您也可以透過圖表變更警示狀態。

您也可以使用常規程式來變更警示狀態。

手動建立警示

您可以從事件集中手動建立警示。您可以使用此功能來檢查尚未自動偵測到的假設事件。

如果手動建立警示，常規程式將不會自動啟動。您可以手動為此類警示啟動常規程式。

若要手動建立警示：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
2. 選取您要為其建立警示的事件。事件應屬於同一租用戶。
3. 按一下**建立警示**按鈕。

   此時將顯示一個窗口，其中顯示已建立的警示，如果已設定通知版本，您將收到相應的電子郵件通知。**嚴重等級**欄位值對應於所選事件中的最大嚴重程度。

手動建立的警示在**規則 → 警示監控警示**值為空白。

將警示連結到事件中

您可以將一個或多個警示連結到一個事件，原因如下：

- 多個警示可能被解釋為組織IT基礎設施中相同問題的指標。如果是這種情況，則可以將在事件中的警示作為單一問題進行調查。最多可以將200個警示連結到一個事件。
- 如果警示被定義為確認為真，則可以將單一警示連結到一個事件。

如果警示具有除*已關閉*以外的任何狀態，則可以將警示連結到事件。當連結到事件時，警示將失去其當前狀態並獲得*在事件中*的特殊狀態。如果連結目前連結到其他事件的警示，則警示將與目前事件取消連結，因為一個警示只能連結到一個事件。

警示只能連結到屬於同一租用戶的事件。

警示可以手動或自動連結到事件。

手動連結警示

若要將警示連結到現有事件或新事件：

1. 在主功能表中，轉至**監控→ 警示**。
2. 選中您要連結到事件的警示旁邊的核取方塊。
3. 如果您想將警示連結到現有事件：
   a. 點擊**連結到事件**按鈕。
   b. 選取警示要連結到的事件

   或者，按一下某個警示以顯示其詳情，然後按一下頂部工具列中的**連結到事件**按鈕。
4. 如果您想將警示連結到新事件：
   a. 點選**建立事件**按鈕。
   b. 填寫新事件的屬性：名稱、受讓人、優先順序和描述。

   或者，按一下某個警示以顯示其詳情，然後按一下頂部工具列中的**建立事件**按鈕。
5. 按一下**儲存**按鈕。

   選定的警示將連結到現有事件或新事件。

自動連結警示

如果您希望警示自動連結到事件，則必須設定分段規則。

取消警示與事件的連結

您可能需要取消警示與事件的連結，例如，如果警示分析和調查顯示警示未與在事件中的其他警示關聯。當您取消警示與事件的連結時，Kaspersky Next XDR Expert 會執行以下動作：

- 刷新與事件相關的所有資料，以反映警示不再屬於該事件。例如，您可以在事件中檢視變更。
- 將取消連結的警示的狀態重設為*新*。

若要取消警示與事件的連結：

1. 開啟警示詳情。
2. 點選頂部工具列中的**從事件中取消連結**按鈕。
   此時將開啟**取消警示連結**視窗。

3. 如果要變更受讓人，請選擇**將警示指派給** ，然後指定新的受讓人。
4. 如果要新增備注，請在**備注**部分中指定。您指定的備注將顯示在**歷程記錄**部分的**詳情**欄位中。

選定的警示已從事件中取消連結。

將事件連結到警示中

如果在調查期間，您發現與正在調查的警示相關的事件，您可以手動將此事件連結到警示。

> 您可以將事件連結到具有**已關閉**以外的任何狀態的警示。

若要將事件連結到警示：

1. 在主選單中，轉到**監控→警示**部分。
2. 在警示清單中，點擊具有您要連結事件的警示ID的連結。
   警示詳細資訊視窗開啟。
3. 轉到**詳細資訊**部分，然後點擊**在威脅搜尋中查詢**按鈕。
   搜尋威脅部分將開啟。預設情況下，事件表包含與選定警示相關的事件。

   > 事件表僅包含與您有存取權限的租用戶相關的事件。

4. 在視窗的上部，打開第一個下拉清單，然後選擇**儲存**。
5. 開啟第三個下拉清單，然後指定時間範圍。
   您可以選擇相對於目前日期和時間的預定義範圍，使用**範圍開始**和**範圍結束**欄位指定自訂範圍，或透過選擇日曆中的日期。
6. 點擊**執行查詢**按鈕。
7. 在更新的事件清單中，選擇要連結到警示的事件，然後按一下**連結到警報**。

選定的事件將連結到警報。

取消事件與警示的連結

您可能需要取消事件與警示的連結，例如，如果警示分析和調查顯示事件未連線到警報。

若要取消事件與警示的連結：

1. 在主選單中，轉到**監控→警示**部分。
2. 在警報清單中，按一下具有要取消事件連結的警報ID的連結。
   警示詳細資訊視窗開啟。
3. 在**詳細資訊**部分中，選擇要取消連結的事件，然後按一下**取消與警示的連結**按鈕。

選定的事件將與警示取消連結。

在調查圖表上使用警示

在調查圖表中，您可以對警示執行以下操作：

- 在圖表中新增警示。
- 隱藏圖表中的警示。
- 透過從警示節點的快顯表單中選擇相應項目來查看警示詳情。
- 變更警示狀態。
- 檢視與警示相關的事件。
- 檢視與警示相關的資產。
- 檢視與警示相關的可觀察物件。

在調查圖表中新增警示

您可以透過以下兩種方式之一將警示新增至調查圖中：

- 從點擊調查圖表中**新增警示**按鈕後開啟的警示總表中。您需要選取要在調查圖表中顯示的警示旁的核取方塊，然後點擊**在圖表上顯示**按鈕。
- 從相似警示表中。

若要從相似警示表向調查圖表新增警示：

1. 執行以下操作之一：
   - 如果調查圖中存在資產、可觀察物件或分段規則，請點選其節點，然後在快顯表單中點選**尋找類似警示**。
   - 如果調查圖表中存在事件，請點選其節點，然後在快顯表單中點選**檢視詳情**。在開啟的視窗中，按一下**在圖表上顯示**按鈕。

- 如果調查圖表中存在警示，請點選其節點，然後在快顯表單中點選**事件**。在事件表中，點擊要開啟其詳情的事件。如果事件詳情包含可觀察物件、資產或分段規則，請點擊對應欄位中的連結，然後在快顯表單中點選**尋找類似警示**。

- 在調查圖表中，按一下**威脅搜尋**按鈕，然後在事件總表中，按一下要開啟其詳情的事件。如果事件詳情包含可觀察物件、資產或分段規則，請點擊對應欄位中的連結，然後在快顯表單中點選**尋找類似警示**。

相似警示表隨即顯示。

2. 選取要在調查圖表中顯示的警示旁的核取方塊，然後按一下**在圖表上顯示**按鈕。

選定的警示隨即新增到調查圖表中。

隱藏調查圖表中的警示

您可以透過以下方式之一隱藏調查圖表中的警示：

- 按一下警示節點，然後在右鍵功能表中選取**隱藏**。
- 透過警示表。

若要透過警示表隱藏圖表中的警示：

1. 執行以下操作之一：

   - 在調查圖頂部的工具列中，按一下**新增警示**按鈕。
   - 如果圖表中顯示了可觀察物件、資產或事件節點，請按一下要為其新增警示的節點，然後在快顯表單中選擇**尋找類似警示**。

   警示表隨即顯示。

2. 選取要在調查圖表中隱藏的警示旁邊的核取方塊，然後按一下**在圖表上顯示**按鈕。

選定的警示及其連結將從調查圖中隱藏。相關節點仍保留在調查圖表中。

變更警示狀態

若要變更警示狀態：

1. 按一下警示節點，然後在快顯表單中選擇**變更狀態**。
2. 在開啟的**變更狀態**窗格中，選取狀態，然後按一下**儲存**。
   如果選擇*已關閉*狀態，則必須選擇一個解決方案。

所選警示的狀態已變更。

檢視與警示相關的事件

若要檢視與警示相關的事件，請執行下列其中一項操作：

- 按一下您要顯示事件的警示節點旁的數字。該數字顯示與警示相關的事件數量。
- 按一下要顯示事件的警示節點，然後在快顯表單中按一下**事件**。

如果要將表格中的事件新增至調查圖表中，請選取事件旁的核取方塊，然後按一下**在圖表上顯示**按鈕。

若要隱藏調查圖表中的事件，請選取事件旁邊的核取方塊，然後按一下**在圖表上隱藏**按鈕。

檢視與警示相關的資產

若要檢視與警示相關的資產，請按一下警示節點。

在快顯表單中，**裝置**和**使用者使用者**項目顯示與警示相關的裝置和使用者數量。

如果您要將裝置或使用者新增至調查圖表中，請按一下相應的功能表項目。

檢視與警示相關的可觀察物件

若要檢視與警示相關的可觀察物件，請按一下警示節點，然後在快顯表單中，按一下**事件**。

在開啟的功能表中，項目旁邊的數字顯示與警示相關的可觀察物件數量。

如果您要將可觀察物件（例如，**雜湊值**、**網域名稱**、**IP位址**）新增至調查圖表中，請按一下相應的功能表項目。

將IOA規則新增至排除清單

如果您不想為企業正常資產活動過程中產生的事件產生警示，您可以將IOA規則新增至清單。

若要將IOA規則新增至警示表的排除清單：

1. 在主功能表中，轉至**監控→警示**。
2. 按一下篩選器圖示。
3. 在**篩選器**頁籤上，指定並套用所需IOA規則的**偵測日期**篩選器條件。
4. 在警示表中，按一下警示的ID。
   將顯示警示詳情。
5. 在**摘要**部分，按一下IOA規則名稱。

6. 在IOA規則窗格中，按一下**新增到排除項目**。

   新增到排除項目窗格隨即彈出。

7. 在**新增到排除項目**窗格中，選擇要將IOA規則新增至排除清單的政策或設定檔。點擊"**下一頁**"。

8. 指定排除規則內容，然後按一下**新增**。

   IOA規則隨即新增到排除清單中。

若要檢視和編輯政策的IOA排除清單：

1. 在主功能表中，轉至**政策**。

2. 點選所需的政策。

3. 選取**應用程式設定**頁籤。延伸左側的**一般設定**選單，然後選擇**遙測設定**。

   在**EDR Expert（本機部署）遙測資料**頁籤中，**一般排除項**頁籤顯示IOA排除項。

   - 若要停用排除規則，請關閉其**狀態**切換開關。
   - 若要刪除排除規則，請選取排除規則旁的核取方塊，然後按一下**刪除**。
   - 若要檢視排除規則詳情，請按一下排除規則名稱。

管理聚合規則

本章節介紹有關彙總規則的一般資訊，並提供有關如何建立、編輯、複製、複製到其他租用戶和刪除彙總規則的說明。

若要編輯彙總規則，您必須具有以下其中一種XDR角色：主管理員、租用戶管理員或SOC管理員。

*彙總規則*可讓您將其他卡巴斯基解決方案的重複事件合併到Open Single Management Platform警示中。這些警示要麼與現有事件相關聯，要麼構成新的事件。

您可以在 **監控 → 資源和服務 → 彙總規則** 中建立和管理彙總規則。彙總規則以表格形式顯示。規則在彙總規則表格中的位置越高，其優先順序越高。若要變更彙總規則優先順序，必須透過按一下拖曳（⠿）圖示來拖放規則。

對於繼承的規則，您只能從父租用戶變更優先順序。在子租用戶中，繼承規則的優先順序一律高於在子租用戶中建立之規則的優先順序。此外，繼承規則也會維持其在父租用戶中的相同優先順序排序。

此外，該表格還包含卡巴斯基專家建立的預定義彙總規則。此規則將預設彙總間隔（30秒）內觸發相同關聯規則的事件合併在一起。

您無法刪除預先定義的彙總規則，但可以對其進行編輯。預設情況下，該規則已啟用。

依預設，會在所有租用戶上建立預定義規則，並且會停用其繼承功能。如果您在父租用戶上為規則啟用繼承，子租用戶上的對應規則將會被父租用戶設定覆寫。如果您停用繼承，父租用戶規則將會被刪除。不過，由於租用戶不能沒有預定義規則，因此系統會在子租用戶上自動建立新的本機預定義規則。

彙總規則根據指定的優先順序依順序處理。當符合在**觸發條件**區段中設定的條件時，彙總規則便會觸發，並繼續搜尋其他適用的彙總規則。僅當表格中的所有規則都處理完畢時，搜尋才會停止。

偵測技術的局限性

根據偵測技術的不同，警示彙總存在一些限制：

- 檔案中的YARA、沙盒和反惡意軟體偵測結果：
  - 您可以將這些技術偵測到的結果彙總到同一個檔案中。
  - 您無法新增IOA偵測結果或IOC或YARA掃描結果。
- IOA偵測結果：
  - 您可以將由一條或多條IOA規則觸發的警示偵測結果彙總為一個警示偵測結果。
  - 您無法新增所有其他技術的偵測結果。
- IOC掃描結果：
  - 您可以彙總IOC掃描結果（例如，以相同IOC規則、不同IOC規則、相同或不同主機進行的偵測）。
  - 您無法新增所有其他技術的偵測結果。
- YARA掃描結果：
  - 您可以彙總YARA掃描結果（例如，透過相同YARA規則、不同YARA規則、相同或不同主機進行的檢測）。
  - 您無法新增所有其他技術的偵測結果。

建立彙總規則

彙總規則可協助您將其他卡巴斯基解決方案的重複事件合併到Open Single Management Platform警示中。

若要編輯彙總規則，您必須具有以下其中一種XDR角色：主管理員、租用戶管理員或SOC管理員。

若要建立彙總規則：

1. 在主功能表中，轉至**監控→資源和服務→警示聚合**。
   彙總規則表格隨即開啟。
2. 點擊**建立**按鈕。
   建立彙總規則視窗隨即開啟。
3. 在**狀態**欄位中，啟用要建立的彙總規則。
   預設情況下，該規則已停用。
4. 在**租用戶所有者**欄位中，指定彙總規則所屬的租用戶。
5. 在**名稱**欄位中，指定彙總規則名稱。
   規則名稱必須是唯一的。

6. 在**警示中的最大事件數**欄位中，指定警示中合併的最大事件數。

   該值必須介於1和100之間。預設值是 100。

7. 在**彙總間隔**欄位中，以分鐘或秒為單位指定搜尋間隔。

   最大值是1500秒。預設值是 30。

8. 根據需要，請在**繼承自**欄位中變更繼承設定。

   依預設，階層中所有下層子租用戶都會繼承父租用戶的規則。您可以選取**僅目前租用戶**選項來停用繼承，或按一下**特定租用戶**，然後從下拉式清單中選取租用戶，以指定必須繼承規則的租用戶。

   > 您只能指定您具有以下 XDR 角色的租用戶：主管理員、租用戶管理員、SOC 管理員。
   > 只能從父租用戶編輯繼承設定、變更規則優先順序，以及複製或刪除繼承的規則。繼承規則的狀態可以從父租用戶和子租用戶變更。

   在子租用戶中，繼承規則的優先順序一律高於在該子租用戶中建立的規則優先順序。此外，繼承的規則會維持與其在父租用戶中相同的優先順序排列。複製繼承的規則時，會連同其範圍一起複製。將繼承的規則複製到另一個租用戶時，不會複製規則範圍。

9. 在**警示名稱**部分，指定定義用於建立新警示名稱的範本的jq運算式。此運算式也用於將事件合併到警示中。

   依預設，會指定以下運算式：`([.Rules[]?.Name // empty] | sort | join(","))`

   建立新警示時，名稱將根據範本中指定的欄位值產生。

   根據需要，您可以從另一個彙總規則複製**警示名稱**部分的jq運算式。為此，請按一下**從另一條規則複製**按鈕。

   警示名稱部分的jq運算式範例

   ```
   if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "Brute force
   admin" else "Brute force not admin" end
   ```

10. 在**觸發條件**部分，指定定義在事件中建立警示條件的jq運算式。

    如果需要，您可以從另一個彙總規則複製**觸發條件**部分的jq運算式。為此，請按一下**從另一條規則複製**按鈕。

    觸發條件部分的jq運算式範例

    ```
    .AggregationID | startswith("bruteforce_DestinationUserName")
    ```

11. 根據需要，請在**描述**欄位中，指定彙總規則的描述。

12. 點擊**建立**按鈕。

    彙總規則隨即建立。

預設情況下，彙總規則會以最低優先順序建立。若要變更彙總規則的優先順序，請在彙總規則表格中，透過點擊其名稱來拖放規則。規則在彙總規則表格中的位置越高，其優先順序越高。

編輯彙總規則

您可以編輯彙總規則的設定。

對於繼承的規則，您在子租用戶中只能變更規則狀態。如果您要編輯其他設定，必須從父租用戶進行編輯，然後變更將會傳播到子租用戶。

若要編輯彙總規則：

1. 在主功能表中，轉至**監控→資源和服務→彙總規則**。
2. 在開啟的彙總規則表格中，點擊要編輯的彙總規則名稱。
3. 在開啟的**編輯彙總規則**視窗中，編輯彙總規則的內容。有關可編輯規則內容的更多詳細資訊，請參閱建立彙總規則。
4. 點擊**套用**按鈕。
5. 如果要變更彙總規則的優先順序，請在彙總規則表格中，透過點擊其名稱來拖放規則。
   規則在彙總規則表格中的位置越高，其優先順序越高。

彙總規則的內容隨即修改並儲存。

將彙總規則複製到另一個租用戶

您可以將現有的彙總規則複製到另一個租用戶。

如果已建立OSMP 實例階層，您只能在單一實例內複製規則。

若要複製彙總規則：

1. 在主功能表中，轉至**監控→資源和服務→彙總規則**。
2. 在彙總規則表格中，選擇要複製的規則，然後按一下**複製至租用戶**。
3. 選擇一個或多個目標租用戶，然後按一下**複製**。
4. 如果目標租用戶包含同名的彙總規則，則會出現**覆寫或重新命名彙總規則？**視窗。
   - 若要刪除先前為目標租用戶建立的規則，並將其替換為要複製的規則，請按一下**覆蓋**。
   - 若要保留先前建立的規則，並複製指定的規則（在其標題後面附加（複製），請按一下**複製並重新命名**。

   如果您複製繼承的規則，而目標租用戶已經有同名規則，則此規則不會被覆蓋。您必須變更要複製的規則名稱。此外，繼承的規則在複製時會保留其狀態，但不包含範圍。

按一下關閉 (✕) 按鈕時，視窗關閉，且與目標租用戶中名稱相同的彙總規則不會被複制。但是，如果在步驟2中您也選擇了目標租用戶中不存在的彙總規則，則會複製這些規則。

彙總規則將複製到其他租用戶。

刪除彙總規則

您可以一次永久刪除一個或多個彙總規則。

如果彙總規則是繼承而來，您只能從其父租用戶刪除該規則。

您無法刪除預先定義的彙總規則。由於租用戶不能沒有預先定義規則，因此刪除該規則後，系統將自動建立新的本機預先定義規則。

若要刪除彙總規則：

1. 在主功能表中，轉至**監控→資源和服務→彙總規則**。
2. 在彙總規則表格中，選擇要刪除的一個或多個彙總規則，然後按一下**刪除**。
3. 在確認對話方塊，按一下**刪除**。

彙總規則隨即刪除。

處理事件

本部分包含有關事件、事件屬性、典型生命週期以及與警示的一般資訊。本部分還提供了有關如何建立事件、分析事件表、根據生命週期的當前狀態變更事件屬性以及合併事件的說明。

如果符合以下條件，則**事件**部分將顯示在主功能表中：

- 您擁有Kaspersky Next XDR Expert的產品授權金鑰。
- 您已連線到OSMP主控台中的根管理伺服器。
- 您具有以下XDR角色之一：主管理員、租用戶管理員、初級分析師、一級分析師、二級分析師、 SOC管理員、與NCIRCC互動、核准人、稽核員、與子事件互動。

關於事件

*事件*是警示的容器，通常表示組織IT基礎設施中存在確認為真的問題。一個事件可能包含一個或多個警示。透過使用事件，分析師可以將多個警示作為單一問題進行調查。

您可以手動建立事件，也可以啟用事件自動建立規則。建立事件後，您可以將警示連結到該事件。最多可以將200個警示連結到一個事件。

建立後，Kaspersky Next XDR Expert 會將事件新增至事件表，作為要由分析師處理的工作項目。

只能將事件指派給具有讀取和修改警示和事件存取權限的分析師。

您可以使用下列事件屬性將事件作為工作項目進行管理：

- **事件狀態**

  可能的值：*新建*、*進行中*、*暫停*或*已關閉*。

  事件狀態顯示事件在其生命週期中的目前狀態。您可以根據需要變更狀態，但有以下例外：

  - 狀態*新建*不能變更為*暫停*。
  - 狀態*已關閉*只能變更為*新建*。

- **事件嚴重等級**

  可能的數值：**低**、**中**、**高**或**緊急**。

  根據卡巴斯基的經驗，事件嚴重等級顯示此事件可能對電腦安全或企業LAN安全的影響。事件嚴重等級對應於連結警示的最高嚴重等級，不能手動變更。

- **事件優先順序**

  可能的數值：**低**、**中**、**高**或**緊急**。

  事件優先順序定義了分析師調查事件的順序。優先順序為**緊急**的事件是最緊急的事件，必須優先調查。您可以手動變更事件優先順序。

- **事件受讓人**

  指事件所有者，即負責事件調查和處理的分析師。如果狀態參數未設定為**已關閉** ，您可以隨時**變更事件受讓人**。

兩個或多個事件可能被解釋為組織IT基礎設施中同一問題的指標。如果是這種情況，您可以合併這些事件，將它們作為單一問題進行調查。

每個事件都有*事件詳細信息*，其中提供了與該事件相關的所有資訊。您可以使用這些資訊來調查事件或合併事件。

對於每個事件，您可以建立子事件。子事件可讓您調查和回應不同租用戶中的事件。您也可以建立另一個子事件的子事件。一個父事件最多可以包含200個子事件。

事件資料模型

事件的結構由包含值的欄位表示（參見下表）。某些欄位是物件或物件陣列，且具有自身的一組欄位（例如，`Assignee` 與 `Alerts` 欄位）。

事件

欄位	值類型	必要	描述
InternalID	字串	是	內部事件ID，格式為UUID。
ID	整數	是	短內部事件ID。
TenantID	字串	是	與事件關聯的租用戶的ID，採用UUID格式。
IncidentType	IncidentType 物件	是	事件類型
Name	字串	是	事件的名稱。
WorkflowName	字串	是	事件工作流程的名稱。
WorkflowUUID	字串	是	事件工作流程的唯一識別碼，採用UUID格式。
Description	字串	否	事件描述。
CreatedAt	字串	是	事件建立的日期和時間，採用RFC 3339格式。
UpdatedAt	字串	是	上次事件變更的日期和時間，採用RFC 3339格式。
StatusChangedAt	字串	否	事件狀態變更的日期和時間，採用RFC 3339格式。
Severity	字串	否	事件的嚴重等級。 可能的值： • critical • high • medium • low
Priority	字串	是	事件優先順序 可能的值： • critical • high • medium • low
Assignee	Assignee 物件	否	指派了事件的運算子。
FirstEventTime	字串	否	與事件相關的警示的第一個遙測事件的日期和時間，採用RFC 3339格式。
LastEventTime	字串	否	與事件相關的警示的最後一個遙測事件的日期和時間，採用RFC 3339格式。
State	字串	是	事件狀態 可能的值： • open • inProgress • hold • closed
StatusUUID	字串	是	事件狀態ID，格式為UUID。
StatusResolution	字串	否	事件狀態的解決方案。 可能的值： • truePositive • falsePositive • lowPriority • merged
DetectSources	字串陣列	否	偵測並產生事件的元件。
DetectionTechnologies	字串陣列	否	觸發的偵測技術。
Alerts	警示 物件陣列	否	事件中所包含的警示。
AdditionalData	物件	否	有關警示的附加資訊，採用JSON格式。此資訊可由使用者或常規程式填寫。

ExternalRef	字串	是	連結到外部系統中的實體（例如，指向Jira票證的連結）。
SignOfCreation	字串	是	建立事件的方法。
IsCII	布林值	是	指出受影響的資產（裝置或帳戶）是否為緊急資訊基礎設施物件的指標。
Attachments	UnkeyedAttachment 物件陣列	否	與事件相關的附件。

事件類型

欄位	值類型	必要	描述
ID	字串	是	事件類型ID，格式為UUID。
Name	字串	是	事件類型的名稱。
Description	字串	是	事件類型描述。

受讓人

欄位	值類型	必要	描述
ID	字串	是	事件指派到的運算子的使用者帳戶ID。
Name	字串	是	事件指派到的運算子的名稱。

無鍵附件

欄位	值類型	必要	描述
AttachmentID	字串	是	附件ID，格式為UUID。
Name	字串	是	附件名稱。
CreatedAt	字串	是	附件建立的日期和時間（UTC格式）。
UpdatedAt	字串	是	附件上次更改的日期和時間（UTC格式）。
CreatedBy	字串	是	指示受影響資產（裝置或帳戶）是受害者。
Size	整數	是	附件大小（以位元組為單位）。
State	字串	是	附件狀態，指示附件上傳是正在進行中、已完成還是因錯誤而中止。 可能的值： • completed • error • uploading
Description	字串	否	附件描述。
StatusCode	字串	否	向使用者顯示的狀態文字（例如，附件上傳失敗時顯示的錯誤訊息）。

建立事件

您可以手動建立事件，也可以啟用事件自動建立規則。本主題介紹如何手動建立事件。

要能夠建立事件，您必須具有讀取和修改警示和事件的存取權限。

如果手動建立事件，常規程式將不會自動啟動。您可以手動為此類事件啟動常規程式。

您可以使用事件表或警示表建立事件。

使用事件表建立事件

若要建立事件：

1. 在主功能表中，轉至**監控 → 事件**。點擊**建立事件**按鈕。
2. 在**一般設定**步驟中，指定以下設定：
   - 事件的名稱。
   - **租用戶**

     與事件關聯的租用戶。警示只能連結到屬於同一租用戶的事件。您以後不能變更事件的租用戶。
   - **受讓人**

     指事件所有者，即負責事件調查和處理的分析師。如果狀態參數未設定為**已關閉** ，您可以隨時**變更事件受讓人**。
   - **優先順序**

     可能的數值：**低**、**中**、**高**或**緊急**。

     事件優先順序定義了分析師調查事件的順序。優先順序為**緊急**的事件是最緊急的事件，必須優先調查。您可以手動變更事件優先順序。
   - **描述**

     在此欄位中，您可以留下事件的描述。例如，您可以描述問題或提供連結警示的調查結果。描述將會新增到事件詳情的**描述** 部分。

     該欄位是可選的。
3. 點選**確定**。

   事件已建立。

使用警示表建立事件

您可以透過選擇要連結到新事件的警示來建立事件。請參閱將警示連結到事件。

建立子事件

子事件可讓您監控調查進程和回應不同租用戶中的事件。您也可以建立另一個子事件的子事件。父事件最多可以包含200個子事件。

您必須具有以下XDR角色之一：主管理員、租用戶管理員、初級分析師、一級分析師、二級分析師、 SOC管理員、核准人、與子事件互動。

若要建立子事件：

1. 在主選單中，轉到**監控→事件**部分。
2. 在事件表中，按一下所需事件的ID。

   事件詳情視窗將開啟。
3. 在**子事件**部分中，點擊**建立**按鈕。

   建立子事件視窗隨即開啟。
4. 根據需要，請在**名稱**欄位中，變更子事件的名稱。

   預設情況下，子事件名稱包含[Child]標籤和父事件名稱。
5. 在**租用戶**下拉清單中，選擇要指派子事件的租用戶。
6. 在**分析師**下拉清單中，開始輸入分析師姓名，然後從清單中選擇該分析師。

   您也可以選擇**未分配**選項。
7. 根據需要，請在**優先順序**下拉清單中，變更事件的優先順序。

   預設情況下，子事件繼承父事件的優先順序。
8. 根據需要，請在**描述**欄位中指定子事件的描述。
9. 如果要複製父事件中的所有資，請選取**從父事件複製資訊**核取方塊。

   如果選取此核取方塊，則會複製父事件所有資訊，包括可觀察物件、資產和關聯警示。複製的警示將指派給子事件的租用戶。

   如果取消選取此核取方塊，則子事件將不包含父事件的資產、可觀察物件和關聯警示資訊。
10. 點擊**建立**按鈕。

子事件隨即建立並關聯到父事件。您可以在**事件詳情**視窗的**子事件**區段中找到子事件。

如果子事件被指派給一個租用戶，而該租用戶沒有父事件所屬的事件類型，則子事件將被指派預設事件類型和預設事件工作流程。根據需要，您可以變更事件類型。

檢視事件表

事件表顯示在**監控 → 事件**部分，並提供所有已建立事件的概覽。預設情況下，該表顯示與您有存取權限的所有租用戶相關的事件。如有必要，您可以設定事件表。

若要設定事件表，請執行下列操作之一：

- 套用租用戶篩選器：

  a. 按一下**租用戶篩選器**設定旁邊的連結。
  租用戶篩選器隨即開啟。

  b. 選取所需事件旁邊的核取方塊。

- 篩選警示表的資料：

  a. 點選過濾器（ ）圖示。

  b. 在**篩選器**頁籤，在喚起的功能表中指定並套用篩選條件。

- 如果要隱藏或顯示某一列，請按一下設定（ ）圖標，然後選擇必要的列。

事件表已設定並顯示您需要的資料。

事件表包含以下列：

- **建立日期**。新建立事件的日期和時間
- **威脅持續時間**。與事件連結的所有警示中，第一個事件與最後一個事件之間的時間間隔。
- **更新日期**。事件歷程記錄中最後一次變更的日期和時間。
- **事件 ID**。事件的唯一識別碼。
- **狀態**。事件的當前狀態。
- **分類時間**。接受事件的時間限制，以天、小時和分鐘為單位。
- **回應時間**。對在事件中進行初始回應的時間限制，以天、小時和分鐘為單位。
- **解決時間**。解決事件的時間限制，以天、小時和分鐘為單位。
- **狀態已變更**。事件狀態變更的日期和時間。
- **嚴重等級。**事件的嚴重等級。
- **優先順序**。事件的優先順序。
- **已關聯警示**在事件中包含的警示數。
- **名稱**。事件的名稱。

- **規則**。觸發建立事件的規則。
- **受影響的資產**。受事件影響的裝置和使用者。如果受事件影響或涉及事件的資產數量大於或等於三，則會顯示受影響裝置的數量。
- **租用戶**。偵測到事件的租用戶的名稱。
- **外部參考**。外部系統中的事件編號。
- **受指派者**.事件的當前受讓人。
- **有父事件**。顯示事件是否有父事件。如果值顯示為**是** ，則該事件為子事件。
- **子事件的狀態**。第一級子事件的結果狀態。可能的值：**已關閉**、**進行中**、**無子事件**。
- **建立方法**事件的建立方式—手動或自動。
- **可觀測項**。偵測產出物的數量，例如IP位址或檔案的MD5雜湊值。如果可觀察物件的數量大於或等於3，則顯示可觀察物件的數量。

如有必要，您可以將事件表中顯示的所有事件的資訊匯出到JSON檔案。

檢視事件詳細資料

事件詳情是介面中的一個頁面，其中包含與事件相關的所有資訊，包括事件內容。

若要檢視事件詳情：

1. 在主選單中，轉到**監控→事件**部分。
2. 在事件表中，按一下所需事件的ID。

   此時將顯示包含事件詳細資訊的視窗。

如有必要，您可以透過按一下事件名稱旁邊的重新整理 (🔄) 圖示來重新整理事件詳情中的資訊。

事件詳情上部的工具列可讓您執行以下操作：

- 編輯**名稱**、**描述**和**外部參考**欄位的值
- 在調查圖表中檢視事件
- 變更事件狀態
- 變更事件優先順序
- 將事件指派給分析師
- 選取常規程式。
- 將警示連結到事件中
- 將事件與其他事件合併

事件詳情包含以下部分：

- **摘要**

  概要部分包含以下事件內容：

  - **類型**。事件類型
  - **分析師**。事件的當前受讓人。
  - **建立方法**事件的建立方式–手動或自動。
  - **名稱**。事件建立時指定的名稱。您可以點擊頂部的**編輯**按鈕來變更事件名稱。
  - **租用戶**。偵測到事件的租用戶的名稱。
  - **資產**。受事件影響的使用者和裝置數量。
  - **已登記**。新建立事件的日期和時間
  - **更新日期**。事件歷程記錄中最後一次變更的日期和時間。
  - **第一個事件**。與警示相關的第一個事件的日期和時間。這是與該事件關聯的所有警示中，警示詳情部分中最早的事件。
  - **最近的事件。**與警示相關的最後一個事件的日期和時間。這是與該事件關聯的所有警示中，警示詳情部分中的最新事件。
  - **描述。**事件描述。您可以點擊頂部的**編輯**按鈕來指定描述。
  - **外部參考。**連結到外部系統中的實體。您可以點擊頂部的**編輯**按鈕指定外部參考。
  - **優先順序**。可能的數值：**低度**、**中度**、**高度**或**緊急**。事件優先順序定義了分析師調查事件的順序。優先順序為**緊急**的事件是最緊急的事件，必須優先調查。您可以按一下目前優先順序值來變更優先順序。
  - **嚴重等級**可能的數值：**低度**、**中度**、**高度**或**緊急**。根據卡巴斯基的經驗，事件嚴重等級顯示此事件可能對電腦安全或企業LAN安全的影響。
  - **分類時間** – 接受事件的時限，以天、小時和分鐘為單位。
  - **回應時間** – 對在事件中進行初始回應的時限，以天、小時和分鐘為單位。
  - **解決時間** – 解決事件的時限，以天、小時和分鐘為單位。

- **關聯規則**。觸發檢測連結警示的規則。透過點擊規則名稱旁邊的省略號圖標，可以開啟快顯表單。使用此功能表可以了解有關規則的更多詳細信息，查找由相同規則檢測到的警示或事件，或在**威脅搜尋**中搜尋觸發規則的事件，以查找警示的第一個事件和最後一個事件之間的時間段。**威脅搜尋**區域的標題會顯示您由其深入查看此區域的事件 ID 和名稱。

  點擊功能表中的**轉到威脅搜尋**時，**威脅搜尋**區域將於同一索引標籤中開啟。若要在新瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住 `Ctrl` 鍵，然後點擊功能表中的**轉到威脅搜尋**。

- **IOA規則**。觸發用於偵測威脅並建立警示的IOA規則。按一下IOA規則名稱即可開啟快顯表單。使用快顯表單，您可以執行以下操作：

  - 按一下**開啟內容**按鈕，即可檢視該IOA規則的詳細資訊。
  - 按一下**轉到威脅搜尋**按鈕，即可檢視相關事件。

    您將被重定向到**威脅搜尋**部分，該部分僅顯示此IOA規則追蹤的事件。事件的預設顯示時間間隔為24小時。此區段標題會顯示您深入檢視至此的來源事件 ID 和名稱。
  - 尋找類似事件。
  - 按一下**在 Kaspersky TIP 中尋找**按鈕，即可在Kaspersky TIP中檢視IOA規則的詳細資訊。
  - 複製IOA規則名稱。

- **MITRE 戰術**。在與該事件關聯的警示中偵測到的一種或多種策略。按一下MITRE策略名稱即可開啟右鍵功能表。使用快顯表單，您可以執行以下操作：

  - 按一下**在 Kaspersky TIP 中尋找**按鈕，即可在Kaspersky TIP中檢視MITRE策略的詳細資訊。
  - 按一下**在 MITRE ATTCK 中尋找**按鈕，即可在MITRE ATT&CK知識庫中檢視MITRE策略的詳細資訊。
  - 複製MITRE策略名稱。

- **MITRE 技術**。在與該事件關聯的警示中偵測到的一種或多種技術。按一下MITRE技術名稱即可開啟右鍵功能表。使用快顯表單，您可以執行以下操作：

  - 按一下**在 Kaspersky TIP 中尋找**按鈕，即可在Kaspersky TIP中檢視MITRE技術的詳細資訊。
  - 按一下**在 MITRE ATTCK 中尋找**按鈕，即可在MITRE ATT&CK知識庫中檢視MITRE技術的詳細資訊。
  - 複製MITRE技術名稱。

- **附加資料**。關於該事件的附加資訊。您只能使用常規程式編輯此欄位中的值。如果新增了值，則會顯示該欄位。

- **詳細資訊**

  在**詳請**部分中，您可以跟蹤與警示相關的遙測事件。

  若要檢視與該事件相關的事件，請按一下**在威脅搜尋中找尋**按鈕。開啟的表格顯示與該事件相關的警示事件。**威脅搜尋**區域的標題會顯示您由其深入查看此區域的事件 ID 和名稱。

事件表的工具列可讓您執行以下操作：

- **下載事件**。按一下此按鈕可將相關事件的資訊下載為TSV檔案。
- **與事件解除連結**。您可以在表中選擇一個或多個事件，然後按一下此按鈕取消所選事件與警示的連結。

您可以按一下**事件調查**或瀏覽器中的上一頁按鈕，返回事件詳細資訊。

- **類似事件**

在**類似事件**部分，您可以檢視與目前警示具有相同受影響產出物的事件清單。受影響的產出物包括與該事件關聯的警示的可觀察物件和受影響的裝置。此清單包含處於任何狀態的事件。

透過該清單，您可以評估目前事件和事件的相似度。相似度計算如下：

相似度=M/T*100

這裡，「M」表示目前警示和類似警示中符合的產出物數量，「T」表示目前警示中的產出物總數。

如果相似度為100%，則目前事件與類似事件相比沒有任何新內容。如果相似度為0%，則目前事件與類似事件完全不同。相似度為0%的事件不包含在清單中。

計算值將到四捨五入最接近的整數。如果相似度等於0%到1%之間的值，則應用程式不會將該值向下舍入為0%。在這種情況下，該值顯示為小於1%。

按一下事件ID可開啟事件詳細資料。

自訂類似事件清單

您可以使用以下選項自訂表格：

- 透過選擇事件已更新的週期來篩選事件。預設情況下，清單包含過去30天內更新的事件。
- 按一下**列設定**圖示 (⚙)，然後選擇要顯示的列及其顯示順序。
- 按一下**篩選器**圖示 (▽)，然後選擇並設定要套用的篩選器。如果選擇多個篩選器，它們將透過邏輯「AND」運算子同時套用。
- 按一下列標頭，然後選擇排序選項。您可以按升序或降序對事件進行排序。

- **警示**

在**警示**部分，您可以檢視與目前事件關聯的警示清單。

點擊警示ID，即可開啟警示詳情。您也可以使用工具列按鈕來取消警示與事件的關聯。

- **資產**

在**資產**部分，您可以進行以下操作：

- 檢視受警示影響或涉及的裝置和使用者。
- 執行回應操作。為此，請選取資產旁的複選框，然後在**選擇回應操作**下拉清單中，選擇所需的回應操作。

- 透過點擊**匯出到CSV**按鈕，將有關受影響資產的資訊匯出到CSV檔案。
- 使用遠端終端連線到資產。為此，請點擊**開啟遠端終端**按鈕。

資產表包含以下列：

- **資產類型**

  可能的值：裝置或使用者。
- **資產名稱**
- **資產ID**
- **授權狀態**

  此參數僅適用於裝置資產類型。裝置授權狀態由KICS for Networks定義。您可以透過對裝置套用相應的回應操作來變更授權狀態。
- **有跡象**

  可能的值：攻擊者或受害者。
- **管理伺服器**

  管理裝置的管理伺服器。
- **類別**

  包含該資產的資產類別。
- **已歸檔**

  資產的歸檔狀態。可能的值： 是或否。
- **計數**

  受事件影響或涉及事件的具有相同ID、類型和名稱的裝置和使用者數量。
- **管理群組**

  裝置所屬的管理群組。

透過點選使用者名稱或裝置名稱，您可以：

- 檢視使用者或裝置內容。

  若要檢視與裝置相關的警示或事件列表，請在裝置內容視窗中按一下**顯示相關**按鈕，然後根據要檢視的內容選擇**警示**或**事件**。
- 在剪貼簿中複製使用者名稱或裝置名稱。
- 在其他警示中搜尋使用者名稱或裝置ID。
- 在其他事件中搜尋使用者名稱或裝置ID。

- 在**威脅搜尋**中搜尋第一個事件和最後一個事件之間的使用者名稱或裝置ID。

  點擊使用者名稱或裝置名稱後，在功能表中選取**轉到威脅搜尋**，**威脅搜尋**區域將於同一頁籤中開啟。若要在新瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住 `Ctrl` 鍵，然後點擊功能表中的**轉到威脅搜尋**。

透過點選使用者ID或裝置ID，您可以：

- 檢視使用者或裝置內容。

  若要檢視與裝置相關的警示或事件列表，請在裝置內容視窗中按一下**顯示相關**按鈕，然後根據要檢視的內容選擇**警示**或**事件**。

- 在剪貼簿中複製使用者ID或裝置ID。
- 在其他警示中搜尋使用者ID或裝置ID。
- 在其他事件中搜尋使用者ID或裝置ID。
- 在**威脅搜尋**中搜尋事件第一個事件和最後一個事件之間的使用者ID或裝置ID。

  點擊使用者ID或裝置ID後，在功能表中選取**轉到威脅搜尋**，**威脅搜尋**區域將於同一頁籤中開啟。若要在新瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住 `Ctrl` 鍵，然後點擊功能表中的**轉到威脅搜尋**。

- **子事件**

  在**子事件**部分，您可以檢視目前事件的子事件清單。

- **檔案**

  檔案部分包含透過回應操作取得的檔案或手動新增至此事件的檔案。您可以上傳、下載、刪除與事件相關的檔案，或編輯檔案的描述。

  您可以上傳任何擴展名的檔案。允許使用重複的檔案名稱。您可以在組態檔案中指定可附加到事件的最大檔案數量以及最大檔案總大小。

  預設限制：

  - 每個事件的檔案數量不能超過100個。
  - 每個事件的檔案總大小不得超過25MB。

  若要上傳檔案，請點擊**上傳**按鈕並選擇一個或多個檔案。如果您嘗試上傳的檔案超出限制，則會開啟**上傳檔案**窗格，其中顯示一則警告訊息。在此窗格中，您可以從上傳佇列中移除檔案，直到警告訊息消失，然後點擊**上傳**按鈕上傳檔案。如果您忽略警告訊息點擊**上傳**按鈕，上傳將會失敗，檔案清單將包含無法上傳的檔案，檔案名稱旁邊會顯示警告圖示。

  點擊**上傳**按鈕後，窗格隨即關閉，上傳的檔案會顯示在事件詳細資料的檔案表格中，以及主選單的**檔案**區段中。上傳大檔案或多個檔案時，您必須重新整理表格，以便顯示新檔案。如果檔案正在上傳， **名稱或完整路徑**列會顯示載入指示器， **大小**欄位會顯示已上傳的檔案大小佔總檔案大小的比例。

  點擊檔案即可開啟**編輯檔案**窗格，其中顯示檔案詳情。在此窗格中，您可以編輯檔案描述。

  使用核取方塊選擇一個或多個檔案。選擇一個或多個檔案，然後點擊**下載**按鈕，以ZIP格式將其下載為存檔。此存檔受密碼*infected*保護。選擇一個或多個檔案，然後點擊**刪除**按鈕進行刪除。

上傳、刪除檔案以及編輯檔案描述需要**警示和事件**功能區中的**寫入**權限。下載檔案需要**警示和事件**功能區中的**讀取**權限。

- **可觀察物件**

  在**可觀察物件**區段中，您可以：

  - 檢視屬於與目前事件連結之警示的可觀察物件。
  - 點擊**匯出至 CSV**按鈕，將相關可觀察物件的資訊匯出至 CSV 檔案。
  - 依據**值**欄中的資料搜尋可觀察物件表格。

    若要執行此操作，請開始在搜尋欄位中輸入所需可觀察物件的資料。如果**值**欄中沒有相符的可觀察物件值，則會顯示空白表格。

  可觀察物件可能包括：

  - MD5 hash
  - URL
  - 網域名稱
  - SHA256
  - 使用者名稱
  - 主機名稱
  - IP位址

    以下私有IP位址未包含在與連結至目前事件的警示相關的可觀察物件中：
    從10.0.0.0到10.255.255.255，子網路遮罩為255.0.0.0或/8
    從172.16.0.0到172.31.255.255，子網路遮罩為255.240.0.0或/12
    從192.168.0.0到192.168.255.255，子網路遮罩為255.255.0.0或/16
    從100.64.0.0到100.127.255.255，子網路遮罩為255.192.0.0或/10

    若要在可觀察物件中包含私有IP位址，請在管理員主機上執行下列命令：

    ```
    k0s kubectl -n irp set env deploy/transformer -c transformer
    OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
    ```

    ```
    k0s kubectl -n irp set env deploy/incident -c incident
    OSMP_FILTER_PRIVATE_IPS_DISABLED=true
    ```

  透過點選**值**列中的連結，您可以：

  - 在**威脅搜尋**中搜尋可觀察物件值，搜尋期間為該事件的第一個事件與最後一個事件之間。

點擊**值**欄位中的連結後，在功能表中選取**轉到威脅搜尋**，**威脅搜尋**區域將於同一索引標籤中開啟。此區段標題會顯示您深入檢視至此的來源事件 ID 和名稱。如果您想在新的瀏覽器索引標籤中開啟**威脅搜尋**區域，請按住`Ctrl`金鑰，然後在功能表中點擊**轉到威脅搜尋**區域。

- 在其他警示中搜尋可觀察物件值。
- 在其他事件中搜尋可觀察物件值。
- 將可觀察物件值複製到剪貼簿。

此部分的工具列包含以下按鈕：

- **Kaspersky TIP 的請求狀態**。使用此按鈕可從卡巴斯基Kaspersky Threat Intelligence Portal（卡巴斯基TIP）取得所選可觀察物件的詳細資訊。取得後，**狀態更新**列中的資訊會更新。需要與Kaspersky Threat Intelligence Portal（進階存取權限）整合。
- **擴充來自 Kaspersky TIP 的資料**。使用此按鈕可從卡巴斯基TIP中取得所有列出的可觀察物件的詳細資訊。因此，**資料補足**列中的資訊會更新。使用**資料補足**列中的連結開啟有關可觀察物件的獲取的擴充詳細資訊。需要與Kaspersky Threat Intelligence Portal（進階存取權限）整合。
- **移動到隔離區**。使用此按鈕將檔案所在的裝置移至隔離區。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。
- **新增阻止規則**。使用此按鈕可新增阻止檔案運作的規則。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。
- **刪除阻止規則**。使用此按鈕可刪除封鎖檔案執行的規則。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。
- **終止處理程序**。使用此按鈕可終止與檔案關聯的進程。此按鈕僅適用於雜湊值（MD5或SHA256）可觀察物件。

- **歷程記錄**

在**事件日誌**部分，您可以追蹤作為工作項目對事件所做的更改：

- 變更事件狀態
- 更改事件受讓人
- 將警示連結到事件
- 取消警示與事件的連結
- 建立子事件
- 將事件與其他事件合併
- 將檔案上傳到事件
- 從事件中刪除檔案

在**回應歷史**部分，您可以查看手動和常規程式回應操作的日誌。資源表包含以下列：

- **時間**。事件發生的時間。
- **啟動者**。啟動回應操作的使用者的名稱。

- **事件**。事件敘述。
- **回應參數**。回應操作中指定的回應操作參數。
- **資產**。啟動回應操作的資產數量。您可以點選包含資產數量的連結來檢視資產詳情。
- **動作狀態**。回應操作的執行狀態。此列可以顯示以下值：
  - **等待核准**– 等待核准啟動的回應操作。
  - **已啟動**– 回應操作正在執行中。
  - **成功**– 回應操作已完成，沒有錯誤或警告。
  - **警告**– 回應操作已完成，但有警告。
  - **錯誤**– 回應操作已完成，但有錯誤。
  - **已停止**– 由於使用者中斷了執行，回應操作已完成。
  - **核准時間已過**– 由於啟動的核准時間已過，回應操作已完成。
  - **被拒絕**– 由於使用者拒絕了啟動，回應操作已完成。
- **常規程式**。啟動回應操作的常規程式的名稱。您可以單擊連結以查看常規程式詳細資訊。
- **回應動作**。已執行的回應操作的名稱。
- **資產類型** 啟動回應操作所針對的資產類型。可能的值：**裝置**或**使用者**。
- **資產租用戶**。租用戶，即啟動回應操作的資產所有者。

- **工作量日誌**

  在**工作量日誌**部分，您可以檢視分析師在與事件相關的工作上花費的工作量。

  在此部分，您可以管理自己的工作量。您無法修改或刪除其他分析師新增的工作量。

  點擊**資料**直欄中的連結，即可檢視和編輯您的工作量。

- **備註**

  在**備注**部分，您可以留下與事件相關的備注。例如，您可以輸入有關調查結果或變更事件內容（如警示受讓人或狀態）時的備注。

  若要儲存您的備注，請按**Enter** 。若要開始新行，請按**Shift+Enter** 。若要編輯或刪除您的備注，請使用右上角的按鈕。

  您只能在留下備註後的指定期間內編輯或刪除自己的備註。預設期間是 15 分鐘。

  如果您想變更此期間，請在管理員主機上執行以下命令：

  ```
  k0s kubectl -n irp set env deploy/comment -c comment
  OSMP_COMMENT_LOCK_AFTER_DURATION=Nx
  ```

  其中 `N` 是時間間隔，而 `x` 是測量單位：`h`（小時）或 `m`（分鐘）。

  其他用戶的備注無法修改或刪除。留下備注需要**警示和事件**功能區中的**寫入**權限。

將事件指派給分析師

作為工作項，必須將事件指派給SOC分析師或使用者群組以進行檢查與可能的調查。如果要將事件自動指派給所選群組內的分析師，則可以將事件指派給使用者群組。有關詳情，請參閱設定警示和事件的自動指派。

您可以隨時變更事件的受讓人。

只能將事件指派給具有讀取和修改警示和事件存取權限的分析師和使用者群組。

若要指派一個或多個事件：

1. 在主功能表中，轉至**監控 → 事件**。
2. 選取要指派的事件旁邊的核取方塊。

   您必須僅選擇在同一租用戶中偵測到的事件。否則，**指派給我**和**指派**按鈕將被停用。

   或者，您可以從事件詳情中將事件指派給分析師或使用者群組。若要開啟事件詳情，請點選包含事件ID的連結。
3. 執行以下操作之一：
   - 若要將事件指派給您，請點選**指派給我**按鈕。
   - 若要將事件指派給其他分析師或使用者群組：
     a. 點選**指派**按鈕。
     b. 在開啟的**指派**視窗中，選擇將事件指派給使用者或使用者群組。
     c. 開始輸入分析師或使用者群組的名稱，然後從清單中選擇受讓人。
     d. 點選**指派**按鈕。

   如果要取消指派事件，請選擇**未分配**。

事件已指派。

您也可以使用常規程式將事件指派給分析師。

變更事件狀態

作為工作項，事件具有一種狀態，顯示事件在其生命週期中的目前狀態。

只有當您具有讀取和修改警示和事件的存取權限時，您才可以變更您自己的事件或其他分析師的事件的狀態。

當您變更事件狀態時，事件和任何未指派的連結警示都會自動指派給您。

如果手動變更事件狀態，常規程式將不會自動啟動。您可以手動為此類事件啟動常規程式。

事件可以具有以下一種狀態：

- **新**

  當您建立事件或事件自動建立時，事件狀態為*新*。您可以將狀態變更到*執行中*或*已關閉*。當您將*新增*狀態變更為*已關閉*，且沒有受讓人，則該事件將自動指派給您。

- **調查中**

  此狀態表示分析師已開始處理該事件，或已透過變更*暫停*狀態恢復工作。您可以將*進行中*狀態變更為任何其他狀態。

- **暫停**

  此狀態表示分析師暫停了事件的工作。通常，在恢復工作時，您會將*暫停*狀態變更為*進行中*，但您也可以將*暫停*狀態變更為其他狀態。

- **已關閉**

  當預計事件不需要額外工作時，您可以關閉事件。您可以使用以下解決方案之一關閉事件：

  - 確認為真
  - 誤報。
  - 優先順序低。

  關閉事件時，連結的警示也會獲得*已關閉*狀態並繼承事件的解決方案。如果事件沒有受讓人，則已關閉的事件會自動指派給您。如果已關閉的事件有未指派的連結警示，則這些警示會自動指派給您。

  狀態*已關閉*只能變更為*新建*。如果您想要讓已關閉的事件恢復為活動狀態，請依照以下方式變更其狀態：*已關閉* → *新建* → *進行中*。

若要變更一個或多個事件的狀態：

1. 在主功能表中，轉至**監控 → 事件**。
2. 執行以下操作之一：
   - 選取您要安裝之更新旁邊的核取方塊。
   - 按一下要變更狀態的事件ID的連結。
     事件詳情視窗將開啟。
3. 點選**變更狀態**按鈕。
4. 在**變更狀態**面板中，選擇要設定的狀態。
   選擇*已關閉*狀態時，必須選擇一個解決方案。
   如果某個事件至少違反了一項SLA指標，則關閉該事件時會顯示**SLA違規原因**欄位。您需要在此欄位中指定SLA違規的原因。

   > 如果在事件工作流程中編輯**已關閉**狀態時選取了*僅允許具有特定權限的使用者關閉此事件*核取方塊，則您必須具有主管理員或核准人XDR角色才能關閉該事件。

   > 如果將事件狀態變更為*「已關閉」*，且此事件包含未完成的常規程式或回應操作，則所有相關的常規程式和回應操作都將終止。
5. 按一下**儲存**按鈕。

所選事件的狀態已變更。

您也可以使用常規程式來變更事件狀態。

變更事件優先順序

作為工作項，事件的優先順序定義了分析師必須調查事件的順序。您可以手動變更事件優先順序。

> 如果您擁有讀取及修改警示和事件的權限，便可變更自己或其他分析師之事件的優先順序。

事件可以有以下優先順序之一：

- **低度**
- **中度**（預設值）
- **高**
- **嚴重**

優先順序為**緊急**的事件是最緊急的事件，必須優先調查。**低**優先順序通常意味著事件被放在積壓工作中。您可以定義自己的標準來決定應為哪個事件設定哪個優先順序。

若要變更事件優先順序：

1. 在主功能表中，轉至**監控 → 事件**。
2. 執行以下操作之一：
   - 選取您要變更優先順序的事件旁邊的核取方塊。
   - 按一下事件ID以開啟要變更優先順序的事件詳情。
3. 按一下**變更優先順序**按鈕。
4. 在**變更優先順序**視窗中，選擇要設定的優先順序。
5. 按一下**儲存**按鈕。

   所選事件的優先順序已變更。

您也可以使用常規程式來變更事件優先順序。

對於處於**新增**狀態的事件（無論是剛建立，還是從任何其他狀態切換為此狀態）：

- 您可以編輯優先順序，但在此事件中新增或移除警報時，系統會自動重新評估優先順序。

  優先順序會設定為**事件嚴重性**值。
- 如果您手動變更沒有任何關聯警報的事件優先順序（該事件建立時沒有警報，或所有警報均已從事件中移除），則**事件嚴重性**會設定為優先順序值。
- 重新評估事件優先順序時，也會自動重新評估事件 SLA。

合併事件

兩個或多個事件可能被解釋為組織IT基礎設施中同一問題的指標。如果是這種情況，您可以合併這些事件以將它們作為單一問題進行調查。

合併事件時，您需要從中選擇一個目標事件。事件合併後，將在目標事件中調查問題。目標事件必須具有*已關閉*以外的狀態。其他事件將合併到目標事件中，合併後，獲得*已關閉*狀態和**合併的**解決方案。

連結到合併事件的所有警示都會自動連結到目標事件。由於一個事件的連結警示不能超過1000個，因此應用程式會計算連結到要合併的事件的警示。如果連結警示的總數超過1000，則無法合併選定的事件。選擇目標事件時，將顯示合併後的警示總數。

> 您無法合併子事件或包含子事件的事件。

若要合併事件表中的事件：

1. 在主選單中，轉到**監控→事件**部分。
2. 選取要合併到目標事件的事件旁邊的核取方塊。您將在精靈的第一步中選擇目標事件。
3. 點選**合併到事件**按鈕。

4. **合併事件**將會開啟。

5. 選擇目標事件。

6. 點選**合併**按鈕。

事件已合併。

若要使用事件詳情合併事件：

1. 在主選單中，轉到**監控→事件**部分。

2. 按一下事件ID以開啟事件詳情。此事件將合併到目標事件中。您將在精靈的第一步中選擇目標事件。

3. 點選**合併到事件**按鈕。
   合併事件將會開啟。

4. 選擇目標事件。

5. 點選**合併**按鈕。

事件已合併。

匯出事件到檔案

您可以將事件匯出為PDF或JSON檔案。

若要將事件匯出為PDF檔案：

1. 在主功能表中，請轉至**監控 → 事件**，以喚起事件表。

2. 按一下要匯出的事件ID。

3. 在事件詳情視窗中，按一下**匯出為PDF**按鈕。
   列印視窗隨即開啟。

4. 在**列印**視窗中，延伸**印表機**清單，然後選擇**另存為PDF**。

5. 按一下**儲存**按鈕，將事件儲存為PDF檔案。
   如果按**類型**或**名稱**欄位對事件表進行排序，匯出的PDF檔案也會使用此排序方式。

若要將所有事件匯出為JSON檔案：

1. 在主功能表中，請轉至**監控 → 事件**，以喚起事件表。

2. 點選事件表上方窗格中的**匯出**按鈕。

3. 指定檔案名稱並選擇要將事件匯出到的資料夾。

4. 點擊**儲存**將所有事件儲存為JSON檔案。

從XDR事件建立「受管理偵測和回應」事件

如果在OSMP中啟用了Managed Detection and Response整合，並且該事件的警示符合以下條件，則可以從XDR事件建立Managed Detection and Response事件：

- 偵測來源為端點。
- 所選事件必須至少有一個包含相關資產的警示。
- 偵測技術為下列任一技術：
  - IOA規則
  - IOC
  - YARA
  - SB (Sandbox)
  - AM（反惡意軟體引擎）。

有關如何在OSMP中啟用Managed Detection and Response整合的信息，請參閱以下文章：與卡巴斯基應用程式和解決方案整合。

若要將事件匯出至「受管理偵測和回應」：

1. 在主功能表中，轉至**監控 → 事件**。
2. 在事件表中，按一下所需事件的ID。此時將顯示包含事件詳細資訊的視窗。
3. 按一下工具列上的三點圖示，然後選擇**建立MDR事件**。
4. 在**建立MDR事件**窗格中，指定事件名稱和描述，然後按一下**建立**。

如果事件建立成功，則會顯示相應的訊息。現在，您可以在MDR網頁主控台中進行事件存取。事件連結位於XDR事件的「摘要」部分。

調查圖表

*調查圖表*是一種視覺化分析工具，可顯示以下物件之間的關係：

- 事件
- 警示
- 使用者
- 可觀察部件

- 資產（裝置）。
- 區隔規則

此圖表顯示事件的詳細資訊：對應的警示及其共同內容。

若要開啟調查圖表：

1. 在主選單中，轉到**監控→事件**部分。
2. 在事件表中，按一下所需事件的ID。
   此時將顯示包含事件詳細資訊的視窗。
3. 按一下**在圖表上檢視**按鈕。

需要**警示和事件**功能區域中的**寫入**權限才能檢視圖表。有關詳細資訊，請參閱以下主題：預定義的使用者角色。

您可以使用右下角的平移和縮放窗格來瀏覽複雜的圖表。

此外，您可以按一下復原圖示（）來復原調查圖表上的任何操作，並按一下取消復原圖示（）來取消復原先前已復原的操作。您可以復原或取消復原的最大操作數為10。

如果您在調查圖表中執行操作時關閉圖表，您的變更歷史記錄將會清除。這表示在您再次開啟調查圖表後，您無法復原並取消復原在關閉圖表之前執行的操作。

與其他使用者同時編輯調查圖表時，您可以檢視使用者所做的更改，但無法復原並取消復原他們的操作。

顯示模式

調查圖表有兩種顯示模式：自動模式（圖表節點沿著時間軸顯示）和手動模式。依預設會套用自動模式。

時間軸是螢幕下方的一個刻度，它以圖形方式直觀地展示了構成事件背景的物件、這些物件出現的時間以及它們出現的整個期間。

刻度的左端代表該期間的開始：在事件中包含所有警示中的最早事件或最早警示。刻度的右端代表該期間的結束：在事件中包含所有警示中的最新事件或最新警示。

在分析完事件中的所有警示後，系統會自動計算整個期間的持續時間。如果在調查圖表中新增或刪除新物件，或產生進程樹時，時間軸會自動重新排列。

與刻度上一個分度相對應的間隔（）取決於整個期間的持續時間。

計算間隔

如果整個期間是...	除法值為...
大於或等於1年	1年
大於或等於28天但小於1年	1個月

大於或等於1週但小於28天	7 天
大於或等於24小時但小於1週	24 小時
大於或等於1小時但小於24小時	1 小時
大於或等於10分鐘但小於1小時	5 分鐘
從100秒到10分鐘	1 分鐘
從1秒到1.6分鐘	10秒
少於1秒	100毫秒

在自動模式下，調查圖表上節點的位置取決於對應物件被偵測和定義的日期和時間，具體如下：

- 資產位於刻度的開頭。
- 警示根據其創建時間放置。
- 事件根據其時間戳記放置。
- 可觀察物件會根據其新增至調查圖表的方式放置：
  - 透過警示節點新增時，可觀察物件會根據警示建立時間放置。
  - 透過事件節點新增時，可觀察物件會根據事件時間戳記放置。

  可觀察物件的日期和時間與其關聯的警示或事件的日期和時間相同。

將滑鼠遊標懸停在節點上時，會顯示節點建立的日期和時間。

警示或事件在圖表上的位置對應刻度上的直欄元素（▌）。當您將滑鼠遊標停留在直欄元素上時，將顯示在事件中同時偵測到的警示和事件資訊。

自動模式有以下限制：

- 您無法移動圖表節點。
- 手動建立的連結不會顯示。
- 當一個物件有多個連結時（例如，一個可觀察物件連結到多個警示），圖表上僅顯示來自最早物件（創建時間最早的物件）的連結。
- 您無法手動新增與事件自動定義上下文無關的物件。

  您只能透過已顯示物件的快顯表單新增物件（與警示相關的事件和可觀察物件，或與事件相關的警示和可觀察物件）。將模式切換到手動後，在自動模式下新增的物件將放置在與其相關的節點附近。如果物件連結到多個節點，則必須將其放置在時間戳記最新的節點附近。

如有需要，您可以透過點擊圖示在調查圖表模式之間切換。在手動模式下，不會顯示時間線，您可以移動節點。

> 如果在手動顯示模式下新增一個沒有時間戳記的物件，則在將模式切換到自動模式後，該物件將不會顯示。

與圖表節點互動

您可以使用頂部的工具列新增警示和可觀察物件。

您可以點選並拖曳圖表節點以重新排列它們。

您可以按一下圖表節點以調出快顯功能表。

常見的快顯功能表項目：

- **檢視詳情**
  開啟所選節點的詳細資訊視窗。
- **複製**
  將節點值複製到剪貼簿。
- **隱藏**
  從圖表中刪除選定的節點
- **新增備註/編輯備註**
  喚起文本欄位以輸入備注。按一下**傳送**確認更改。按一下**取消**還原更改。

特定於事件的快顯功能表項目：

處理程序樹
僅適用於特定事件類型。為事件產生進程樹狀圖。事件的藍色指示表示您可以為此事件產生進程樹狀圖。
特定於警示的快顯功能表項目：

- **變更狀態**
  喚起**變更狀態**窗格，此窗格可讓您變更警示狀態。
- **事件**
  子功能表可讓您將事件新增為圖表節點。
- **可觀測項**
  子功能表可讓您將常用可觀察物件新增為圖表節點。
- **裝置**
  子功能表可讓您將常用裝置新增為圖表節點。
  透過使用此子功能表，您還可以檢視與裝置相關的警示或事件清單。為此，請在子功能表中，按一下**檢視詳情**以開啟**裝置詳情**視窗，然後按一下**顯示相關**按鈕並選擇**警示**或**事件**。
- **使用者**
  子功能表可讓您將使用者新增為圖表節點。

特定於可觀察物件的快顯功能表項目：

- **尋找類似事件**
  喚起**搜尋威脅**窗格以顯示類似事件。

- **尋找類似警示**

  喚起**警示**窗格以顯示類似警示。

- **Kaspersky TIP 的請求狀態**

  可讓您從Kaspersky Threat Intelligence Portal（Kaspersky TIP）獲取所選可觀察物件的詳細資訊。有關詳細資訊，請參閱以下主題：與Kaspersky Threat Intelligence Portal整合。

- **擴充來自 Kaspersky TIP 的資料**

  使用此按鈕可從Kaspersky TIP獲取所選可觀察物件的詳細資訊。有關詳細資訊，請參閱以下主題：與Kaspersky Threat Intelligence Portal整合。

特定於分段規則的快顯功能表項目：

- **在 KUMA 中編輯**

  在顯示規則詳細資訊的新瀏覽器頁籤中開啟KUMA主控台。

- **尋找類似警示**

  喚起**警示**窗格以顯示類似警示。

您也可以透過點選警示或事件來新增可觀察物件。為此，在開啟的快顯表單中，您需要選擇**可觀測項**，然後按一下可觀察物件。可觀察物件將會加入調查圖表中。如果需要，您可以從調查圖表中刪除可觀察物件。為此，您必須按一下可觀察物件，然後在開啟的快顯表單中按一下**隱藏**。

將圖表元素分組

調查圖表會自動將具有共用內容的警示分組。

若要取消警示分組：

1. 按一下與警示群組對應的圖表元素。

   將顯示一個列出警示的表格。

2. 選擇要在圖表上顯示的警示。

3. 點選表格工具列中的**在圖表上顯示**按鈕。

   警示將新增為圖表節點。

4. 如果要隱藏警示，請按一下**在圖表上隱藏**按鈕。

連結圖表元素

調查圖表會在適用時自動為新項目建立連結。可以手動新增連結。

若要手動新增連結：

1. 按一下**連結節點**按鈕。
   連結點出現在圖表節點周圍。
2. 點選並從一個節點的連結點拖曳到另一個節點的連結點。

手動建立的連結有顏色指示。

若要刪除手動建立的連結：

1. 將滑鼠遊標停留在手動建立的連結上。
   連結中間會出現一個十字圖示。
2. 按一下十字圖示可刪除連結。

威脅搜尋

您可以分析事件以搜尋尚未自動偵測到的威脅和弱點。為此，您需要按一下頂部工具列中的**搜尋威脅**按鈕，或喚起圖表節點的快顯表單，然後按一下**事件**或**尋找類似事件**。將開啟**搜尋威脅**面板。有關詳細資訊，請參閱以下部分：威脅搜尋。

匯出圖表

您可以將圖表儲存為SVG格式。為此，您需要按一下頂部工具列中的**匯出**按鈕。

檢視和編輯備注

您可以為任何圖表節點或連結留下備注。

若要新增或編輯備注：

1. 按一下圖表元素並選擇**新增備註**或**編輯備註**。
2. 按一下**儲存**以儲存變更。
   訊息 ( ) 圖示出現在圖表元素旁邊。您可以按一下訊息 ( ) 圖示以顯示備注。

若要顯示所有備注，

請按一下頂部工具列中的**備註**按鈕。右側會出現一個包含備注的窗格。您可以按一下窗格中的備注，以在圖表上突出顯示相應的訊息 ( ) 圖示。您可以使用窗格對整個圖表進行備注。

若要刪除備注：

在圖表上或具有備注的窗格中選擇一個備注。按一下省略號 (⋮) 圖示，然後選擇**刪除**。

進程樹狀圖

在Kaspersky Next XDR Expert中進行事件調查時，您可以使用進程樹狀圖來視覺化事件鏈。進程樹狀圖會顯示父程序和子程序，幫助您更詳細地分析事件，並追蹤事件的確切順序。

每個事件最多可以建構和保存五個進程樹狀圖。進程樹狀圖一旦建構完成，就會自動儲存。之後，您可以從**威脅搜尋**部分或特定事件詳情中存取已儲存的進程樹狀圖。

建構進程樹狀圖

您可以從事件或警示詳情、調查圖表或威脅搜尋部分建構進程樹狀圖。

若要從事件詳情建構進程樹狀圖：

1. 在主功能表中，轉至**監控→事件**。
2. 在事件表中，按一下所需事件的ID。
   此時將顯示**事件詳情**視窗。
3. 按一下**在圖表上檢視**按鈕。
4. 切換到**手動**顯示模式。
5. 點擊**威脅搜尋**按鈕。
6. 在**威脅搜尋**窗格中，指定所需事件的參數。
7. 點擊**執行查詢**按鈕。
8. 點選包含所需事件的行。
9. 點選**建構進程樹狀圖**按鈕。

進程樹狀圖已建構完成。

若要從調查圖表建構進程樹狀圖：

1. 在主功能表中，轉至**監控 →事件事件**。
2. 在事件表中，按一下所需事件的ID。
   此時將顯示**事件詳情**視窗。
3. 按一下**在圖表上檢視**按鈕。
4. 切換到**手動**顯示模式。
5. 右鍵點擊要為其建構進程樹狀圖的事件。
6. 按一下**在圖表上顯示**按鈕。

進程樹狀圖已建構完成。

若要從搜尋威脅中建構進程樹狀圖：

1. 在主功能表中，轉至**監控** → **搜尋威脅**。
2. 指定您的查詢，然後按一下**執行查詢**按鈕。
3. 在**事件**部分，按一下包含所需事件的行。
4. 按一下**在圖表上檢視**按鈕。

進程樹狀圖已建構完成。

刪除進程樹狀圖

若要刪除進程樹狀圖：

1. 點擊**檢視儲存的樹**按鈕。
2. 點選進程樹狀圖名稱左側的按鈕。
3. 點擊**刪除**按鈕。

進程樹狀圖隨即刪除且無法復原。

在進程樹狀圖上備注

您可以為進程樹狀圖中的特定節點或連結新增備注，並提供該樹狀圖的描述。所有備注都會顯示在**備註**部分。

若要新增備注：

1. 右鍵點選要新增備注的節點或連結。
2. 輸入您的備注。
3. 點擊**儲存**按鈕。

若要顯示所有備注，

請按一下頂部工具列中的**備註**按鈕。右側會出現一個包含備注的窗格。您可以點擊窗格中的備注，以在進程樹狀圖上突出顯示相應的訊息（ ）圖示。您可以使用此窗格為整個進程樹狀圖進行備注。

若要編輯或刪除備注：

1. 點選備注。
2. 點按省略號（ ⋮ ）圖示。
3. 選擇**編輯**或**刪除**。

區隔規則

*分段規則*可讓您依據建立規則時指定的條件自動將相關警報拆分為不同的事件。

使用分段規則可以依據相關警示建立不同的事件。例如，您可以將具有重要區別特徵的多個警示合併為一個單獨的事件。

警示只能連結到屬於同一租用戶的事件。

分段規則依據指定的優先順序觸發。規則在分段規則表格中的位置越高，其優先順序就越高。如果要變更分段規則優先順序，請透過點擊其名稱來拖放規則。

我們建議您將分段規則與彙總規則一起使用，以定義用於建立事件的更精確的規則。

若要建立分段規則，請執行以下操作：

1. 在主功能表中，轉至**監控→資源和服務→區隔規則**。

   分段規則表格隨即開啟。

2. 點擊「**建立**」按鈕。

   建立區隔規則視窗隨即出現。

3. 輸入分段規則設定。

   - **規則狀態**

     啟用或停用規則。預設情況下，該規則已停用。

   - **租用戶所有者**

     指定分段規則要隸屬的租用戶。

   - **名稱**

     規則的唯一名稱。

   - **事件中的警示**

     單一事件中的警示數量上限與下限。指定介於1到200之間的值。預設的最小值為1，最大值為200。最小數量必須小於或等於最大數量。如果警示數量未達最小值，則不會建立事件。最大數量必須大於或等於最小數量。如果警示數量超過最大值，則會建立另一個事件。

   - **搜尋間隔**

     用於選擇警示和事件的時間間隔。您可以指定以天或小時為單位的值。預設值是30天。

   - **繼承自**

     可選設定。繼承該規則的租用戶。預設情況下，所有子租用戶都會沿階層向下從父租用戶繼承規則。您可以選取**僅目前租用戶**選項來停用繼承，或按一下**特定租用戶**，然後從下拉式清單中選取租用戶，以指定必須繼承規則的租用戶。

     > 您只能指定您具有以下 XDR 角色的租用戶：主管理員、租用戶管理員、SOC 管理員。
     > 只能從父租用戶編輯繼承設定、變更規則優先順序，以及複製或刪除繼承的規則。繼承規則的狀態可以從父租用戶和子租用戶變更。

在子租用戶中，繼承規則的優先順序一律高於在該子租用戶中建立的規則優先順序。此外，繼承的規則會維持與其在父租用戶中相同的優先順序排列。

複製繼承的規則時，會連同其範圍一起複製。將繼承的規則複製到另一個租用戶時，不會複製規則範圍。

- **群組**

  一個jq運算式，定義了字串識別碼陣列，用於為事件指派警示。

  如果需要，您可以從另一個分段規則複製**群組**部分的jq運算式。為此，請按一下**從另一條規則複製**按鈕。

  範例： `if any(.Observables[]? | select(.Type | ascii_downcase == "username") | .Value; startswith("adm_")) then ["Brute force admin"] else ["Brute force not admin"] end`

- **事件名稱**

  用於定義依此分段規則建立之事件命名範本的jq運算式。預設會指定下列運算式：`"\(.Rules[]?.Name), \(.SourceCreatedAt)"`

  如果需要，您可以從另一個分段規則複製**事件名稱**部分的一下。為此，請按一下**從另一條規則複製**按鈕。

  範例：`if any(.Observables[]? | select(.Type | ascii_downcase == "username") | .Value; startswith("adm_")) then "Brute force admin" else "Brute force not admin" end`

- **觸發條件**

  定義在事件中包含警示的條件的jq運算式。

  如果需要，您可以從另一個分段規則複製**觸發條件**部分的jq運算式。為此，請按一下**從另一條規則複製**按鈕。

  範例：`any(.Rules[]?; .ID == "123")`

- **描述**

  可選設定。規則描述。

4. 點擊**建立**按鈕。

分段規則將會儲存並顯示在分段規則表中。如果需要，您可以透過點擊表格中的名稱來編輯規則設定。

您可以在jq運算式中使用`inSubnet`邏輯運算子，以測試左運算元（IP 位址）是否屬於右運算元（子網路）所表示的子網路。

範例：`any(.Observables[]? | select(.Type == "ip") | .Value // empty; inSubnet("11.11.11.1/11"))`

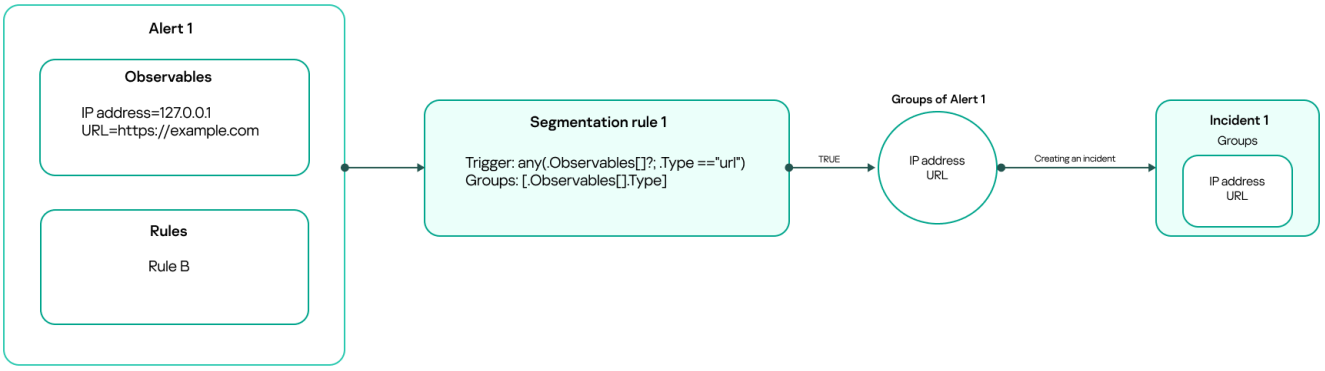
以下預先定義的分段規則可用：

- 連結至現有事件：相同的MD5檔案雜湊值
- 連結至現有事件：相同的主機資產
- 連結至現有事件：相同的IOA、IOC或Yara規則
- 建立事件：相同的MD5檔案雜湊值
- 建立事件：相同的主機資產
- 建立事件：相同的IOA、IOC或Yara規則

預先定義的規則會自動套用至租用戶。

依預設，會在所有租用戶上建立預先定義的規則，且這些規則的繼承會停用。如果您在父租用戶上為規則啟用繼承，子租用戶上的對應規則將會被父租用戶設定覆寫。如果您停用繼承，父租用戶規則將會被刪除。不過，由於租用戶無法在沒有預先定義的規則的情況下存在，因此系統會在子租用戶上自動建立新的本機預先定義規則。

建立警示時，所有活動的分段規則都會依據其優先順序進行檢查。觸發第一個規則後，將為警示形成一個字串識別碼陣列，並開始搜尋將與警示連結的事件。

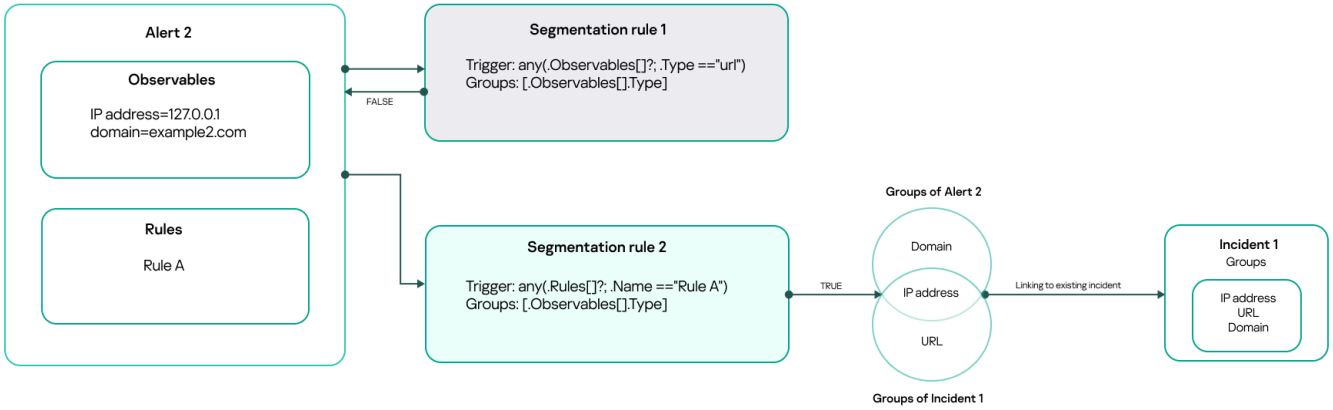


在觸發第一個分段規則後建立新事件

若您在**觸發條件區段**中指定的 jq 運算式傳回 `true`，則規則會被觸發。

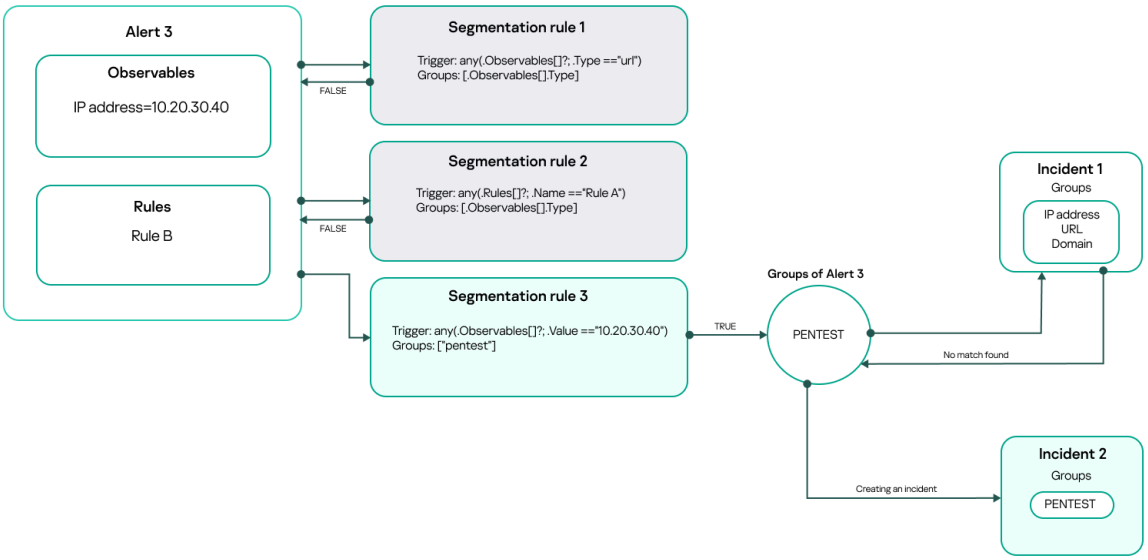
警示無法連結到手動建立的事件。

事件還具有一個字串識別碼陣列，其中包括已連結到此事件的警示陣列。如果觸發分段規則的警示在其陣列中至少有一個元素與事件陣列中的任意元素相符，則該警示連結到該事件。結果，此警示的陣列將新增至事件陣列。



偵測到相符元素後將警示連結到現有事件

如果有多個事件符合條件，則警示連結到最近更新的事件。如果陣列中沒有具有相符元素的事件，則建立一個新事件。



依據前兩個分段規則未找到相符元素後建立新事件

當事件是新事件時，其陣列為空。連結警示後，新事件將從警示中取得字串識別碼陣列。

分段規則。範例

從彙總規則中設定彙總規則。本主題中的範例部分。

下表說明如何將所有滲透測試警示合併到單一事件中。

分段規則

內容	值
觸發器	.AggregationID == "Pentest"
群組	["Pentest"]
事件名稱	"Pentest incident"

彙總和分段規則。範例

下表說明如何依據使用者名稱前綴合併兩個在事件中具有相同規則ID的警示。

彙總規則

內容	值	敘述
觸發器	any(.Rules[]?; .ID == "123")	搜尋規則ID為「123」的警示。
彙總規則ID	if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "rule123_DestinationUserName_adm" else "rule123_DestinationUserName_not_adm" end	搜尋具有「adm_」字首的使用者名稱。
警示名稱	if any(.OriginalEvents[]?.BaseEvents[]?.DestinationUserName // empty; startswith("adm_")) then "Rule123 admin" else "Rule123 not admin" end	依據使用者名稱前綴設定警示名稱。

內容	值
觸發器	.AggregationID | startswith("rule123_DestinationUserName")
群組	[.AggregationID]
事件名稱	.Name

將分段規則複製到另一個租用戶

您可以將現有的分段規則複製到另一個租用戶。

如果已建置OSMP 實例的階層，您只能在同一個實例內複製規則。

若要複製分段規則：

1. 在主功能表中，轉至**監控→資源和服務→區隔規則**。
   分段規則表格隨即開啟。
2. 選擇要複製的分段規則，然後按一下**複製到租用戶**。
3. 選擇一個或多個目標租用戶，然後按一下**複製**。
4. 如果目標租用戶包含同名的分段規則，則會出現**覆蓋或重新命名分段規則？**視窗。
   按一下**覆蓋**可刪除先前為目標租用戶建立的規則，並將其取代為要複製的規則。
   按一下**複製並重新命名**可保留先前建立的規則，並複製指定規則且在其標題後附加 (copy)。
   如果您複製繼承的規則，而目標租用戶已經有同名規則，則此規則不會被覆蓋。您必須變更要複製的規則名稱。此外，複製繼承的規則時會包含其狀態，但不包含範圍。

   按一下關閉 (✕) 按鈕時，視窗會關閉，且名稱與目標租用戶中的規則相同的分段規則不會複製。但是，如果在步驟2中您也選擇了目標租用戶中不存在的分段規則，則會複製這些規則。

分段規則將複製到其他租用戶。

管理服務等級協定（SLA）

Kaspersky Next XDR Expert可讓您設定服務等級協議（SLA）事項，這些事項定義了處理事件的時限。

您可以為事件工作流程和優先順序的組合定義SLA事項。

事件表和事件詳情會顯示SLA事項的剩餘時間。

您可以設定包含事件SLA到期**事件 SLA 即將到期**事件SLA已變更**事件 SLA 已變更電子郵件通知範本**。

當事件狀態復原時，SLA指標的計算將重新啟動

當事件被視為已回應時，該事件的SLA指標將停止計算。預設情況下，復原事件狀態會重新啟動SLA指標的計算。

若要防止在事件狀態復原時重新啟動SLA指標的計算：

1. 請確保管理員主機上已安裝kubectl公用程式。
2. 執行以下命令：

   ```
   kubectl -n irp set env deploy/incident
   OSMP_INCIDENT_SLA_DISABLE_RESTART_CALCULATION_ON_START_TRIGGER=true
   ```

3. 重新啟動事件服務。

建立服務等級協議（SLA）事項

建立SLA事項需要以下XDR角色之一：主管理員、租用戶管理員或SOC管理員。

若要建立SLA事項：

1. 在主功能表中，轉至**設定** → **租用戶**。

   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。

2. 按一下所需政策的名稱。

   這會開啟租用戶內容視窗。

3. 按一下**設定**頁籤，然後按一下**事件管理**。
4. 選擇**SLA**頁籤，然後按一下**建立**按鈕。
5. 在開啟的**建立 SLA**窗格中，配置下列設定：

   - **SLA 名稱**—事項的顯示名稱。
   - **優先順序**— 要套用該事項的事件優先順序。
   - **工作流程**— 若要套用該事項的事件工作流程。

     您只能將單一事項指派給**工作流程**和**優先順序**的組合。您不能選擇在其他具有相同優先順序的SLA中使用的事件工作流程。

   - **分類時間** — 接受事件的時限，以天、小時和分鐘為單位。當事件狀態從一種狀態變成另一種狀態時，該事件即被視為已被接受。

     若要定義此轉換，請選擇**來源狀態**和**目標狀態**的值。

   - **回應時間** — 對在事件中進行初始回應的時限，以天、小時和分鐘為單位。

選擇停止條件：

- 如果您希望在套用回應操作後將事件視為已回應，請選擇**首次回應動作時** 。之後，在**來源狀態**欄位中選擇一個或多個值。
- 如果您希望在事件狀態變更為其他狀態後將其視為已回應，請選擇**當狀態變更為**。之後，在**來源狀態**和**目標狀態**欄位中選擇一個或多個值。

- **解決時間** — 解決事件的時限，以天、小時和分鐘為單位。當事件狀態從一種狀態變成另一種狀態時，該事件即被視為已解決。

  若要定義此轉換，請選擇**來源狀態**和**目標狀態**的值。

6. 點擊**建立**按鈕。

   建立的SLA事項隨即顯示在表格中。

刪除服務等級協定（SLA）事項

刪除SLA事項需要以下XDR角色之一：主管理員、租用戶管理員、 SOC管理員。

若要刪除SLA事項：

1. 在主功能表中，轉至**設定 → 租用戶**。

   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。

2. 按一下所需政策的名稱。

   這會開啟租用戶內容視窗。

3. 按一下**設定**頁籤，然後按一下**事件管理**。

4. 選取**刪除**頁籤。

5. 選取您要刪除的SLA事項之旁邊的核取方塊。

6. 點擊**刪除**按鈕。

7. 在開啟的確認視窗中，按一下**刪除**。

刪除SLA事項後，將不再計算具有該事項**事件類型**和**優先順序**的事件的時限。

管理事件類型

Kaspersky Next XDR Expert可讓您使用事件類型來管理事件並自訂卡巴斯基事件處理流程。

事件類型是一組屬性，您可以為其設定不同的流程，例如，為事件類型指派工作流程、設定觸發器或設定常規程式演算法。

您可以建立事件類型，也可以使用可自訂的預先定義事件類型。

事件類型可以是活動或非活動狀態。如果事件類型處於活動，您可以在事件詳情視窗中選擇此類型。

標記為預設類型的事件類型將自動指派給所有新事件。您無法將預設事件類型切換為非活動狀態。

常規事件類型已設定為預設值。您可以編輯此設定。

一個租用戶中只能建立一個預設事件類型。

檢視事件類型表

若要檢視事件類型表：

1. 在主功能表中，轉至**設定** → **租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤上，按一下**事件管理**。
   類型頁籤以及事件類型表隨即顯示。
4. 如果要設定事件類型表，請執行下列任一操作：
   - 點擊篩選圖示 ( ) ，然後在開啟的功能表中指定並套用篩選條件。
   - 如果要隱藏或顯示某一直欄，請按一下設定圖示 ( ) ，然後選擇所需的直欄。

事件類型表包含以下資訊：

- **名稱**。自訂或預定義事件類型的名稱。
  此表包含下列預先定義的事件類型：
  - 一般

    預設情況下，此類型在**預設**直欄中具有**是**值。

  - 資訊收集
  - 入侵
  - 未經授權的存取
  - 惡意軟體攻擊
  - 網路釣魚
  - 可用性
  - 內部威脅
  - 資料外洩

    - 組態錯誤
    - 供應鏈攻擊
    - 網路應用程式攻擊
    - 弱點利用
- **作用中類型**。如果事件類型處於活動，您可以在事件詳情視窗中選擇此類型。
- **預設**。建立事件時，預設類型會自動指派給它。可能的值：
    - **True**
    - **False**
- **工作流程**。事件工作流程。
- **租用戶**。事件類型所屬租用戶的名稱。
- **建立類型**。事件類型的建立方式。可能的值：
    - **自訂**
    - **預定義**
- **ID**。自訂或預先定義事件類型的唯一識別碼。預設情況下，此列處於隱藏狀態。
- **描述**。事件類型描述。預設情況下，此列處於隱藏狀態。

根據需要，您可以建立新的事件類型，以及編輯和刪除預定義和自訂事件類型。

建立事件類型

若要建立事件類型：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤上，按一下**事件管理**，然後選擇**類型**頁籤。
4. 點擊**建立**按鈕。
   建立事件類型視窗隨即開啟。
5. 如果您希望新的事件類型為作用中，請啟用**作用中類型**切換開關。
6. 在**名稱**欄位中，輸入新事件類型的名稱。

7. 如果您希望所有新事件預設指派此類型，請選取**設定為預設值**核取方塊。

   一個租用戶中只能有一個預設事件類型。這意味著，如果租用戶已有預設事件類型，選取此核取方塊後，該類型將不再是預設類型。

8. 在**工作流程**欄位中，選擇事件工作流程。

9. 根據需要，在**描述**欄位中，輸入事件類型的描述或備注。

10. 點擊**建立**按鈕。

    新的事件類型將顯示在事件類型表中。

編輯事件類型

根據需要，您可以編輯事件類型。

若要編輯事件類型：

1. 在主功能表中，轉至**設定 → 租用戶**。

2. 按一下所需政策的名稱。

   租用戶內容視窗隨即開啟。

3. 在**設定**頁籤上，按一下**事件管理**。

   類型頁籤以及事件類型表隨即顯示。

4. 點擊您要編輯的事件類型名稱。

   編輯事件類型視窗隨即開啟。

5. 進行編輯，按一下**儲存**。有關可編輯的事件類型內容的更多詳細資訊，請參閱建立事件類型。

   事件類型內容隨即編輯並儲存。

刪除事件類型

如果要刪除常規程式中使用的事件類型，則必須從常規程式觸發器和/或演算法中刪除該事件類型，以避免出錯。

在下列情況下，您無法刪除事件類型：

- 事件類型在其建立所在的租用戶中被設定為預設值。

  嘗試刪除此事件類型時，系統會提示您設定新的預設事件類型。在開啟的視窗中，您必須從清單中選擇事件類型。

- 事件類型在子租用戶中被設定為預設值。

- 目前租用戶或子租用戶包含具有您要刪除的類型的事件。
  在刪除此類類型之前，您必須為該事件指派另一個類型。
- 已為事件類型定義了服務等級協議（SLA）規則。

若要刪除事件類型：

1. 在應用程式主視窗中，前往 **設定 → 租用戶**區段。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤上，按一下**事件管理**。
   類型頁籤以及事件類型表隨即顯示。
4. 執行以下操作之一：
   - 選取您要移除的事件類型，然後按一下**刪除**。
   - 按一下要刪除的事件類型名稱，然後在**編輯事件類型**視窗中，按一下**刪除**。
5. 在確認對話方塊，按一下**刪除**。

事件類型隨即刪除。

管理事件工作流程

Kaspersky Next XDR Expert可讓您設定靈活的事件工作流程。Kaspersky Next XDR Expert還能在視覺化編輯器中視覺化工作流程。

事件工作流程是指事件在其生命週期中所經歷的一系列狀態和轉換。*狀態*是 事件處理流程中的一個步驟。*轉換*幫助事件在不同狀態之間轉換。轉換是一種連結，允許您設定從一個事件狀態到另一個事件狀態的轉換，然後返回。如果需要，您可以使用轉換作為單向連結。

您可以建立事件工作流程，也可以使用可自訂的預定義工作流程。

您也可以將工作流程指派給事件類型。這將有助於您以最方便的方式管理事件生命週期。

檢視事件工作流程表

若要查看事件工作流程表：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。

3. 在**設定**頁籤上，按一下**事件管理** ，然後選擇**工作流程**頁籤。
   如果要隱藏或顯示某一直欄，請按一下設定圖示（ ⚙ ），然後選擇所需的直欄。

事件工作流程表隨即顯示。

事件工作流程表包含以下資訊：

- **名稱**。自訂或預定義事件工作流程的名稱。
- **關聯類型**。關聯的事件類型數量。
- **租用戶名稱**。事件工作流程所屬租用戶的名稱。
- **建立類型**。事件工作流程的建立方式。可能的值：
  - **自訂**。
  - **預定義**。
- **工作流程ID**。事件工作流程的唯一識別碼。預設情況下，此列處於隱藏狀態。
- **敘述**。事件工作流程描述。預設情況下，此列處於隱藏狀態。

預先定義的事件工作流程

Kaspersky Next XDR Expert允許您使用預先定義的事件工作流程來管理事件。在事件工作流程表中，此類工作流程被命名為**標準**。在**建立類型**直欄中，這些工作流程被標記為**預定義**。

根據需要，您可以編輯預先定義的工作流程進行自訂。

下表顯示了預定義工作流程的狀態，以及事件切換到這些狀態的原因。

州	原因
新增	• 新事件隨即建立（手動或自動）。 • 事件狀態已從以下狀態之一變更為**新增**：**進行中**、**暫停**或 **已關閉**。
進行中	使用者手動將事件狀態從**新增**或**暫停**變更為**進行中**。
暫停	使用者手動將事件狀態從**進行中**變更為**暫停**。
已關閉	• 使用者關閉了該事件。 • 使用者將此事件與另一起尚未關閉的類似事件關聯起來。

建立事件工作流程

事件工作流程可讓您管理事件生命週期。

若要建立事件工作流程：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。

3. 在**設定**索引標籤上，按一下**事件管理**，然後選取**工作流程**索引標籤。

4. 點擊**建立**按鈕。
   這會開啟**建立工作流程**視窗。

   > 預設情況下，每個事件工作流程都包含預先定義的**新增**和**已關閉**狀態。您無法刪除或編輯這些狀態。

5. 在**名稱**欄位中，輸入新工作流程的名稱。

6. 如有必要，在**描述**欄位中，輸入工作流程的描述或備注。

7. 若要新增狀態，在**工作流程**部分，按一下**新增狀態**。

8. 在開啟的視窗，指定以下設定：

   a. 在**狀態名稱**欄位中，輸入新狀態的名稱。

   b. 在**類別**欄位中，選擇下列狀態類別之一：

      - **新增**
      - **進行中**
      - **已解決**
      - **已關閉**

      類別決定狀態圖示的顏色。

   c. 在**入站轉換**欄位中，選擇一個或多個傳入狀態。
      如果要設定從所有狀態到傳入狀態的轉換，請選擇**允許所有狀態轉換至此狀態**選項。

   d. 在**出站轉換**欄位中，選擇一個或多個傳出狀態。
      如果要設定從傳出狀態到所有狀態的轉換，請選擇**允許此狀態轉換至所有狀態**選項

   e. 點擊**新增**。
      視覺化的工作流程會顯示在**建立工作流程**視窗中
      根據需要，請重複步驟7-8e來新增狀態。

9. 在**建立工作流程**視窗中，點擊**儲存**按鈕。

新的事件工作流程將顯示在表格中。

編輯事件工作流程與狀態

您可以編輯工作流程內容，以及工作流程的狀態和轉換。

若要編輯事件工作流程：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在 **設定** 索引標籤上，按一下 **事件管理**，然後選取 **工作流程** 索引標籤。
4. 點擊您要編輯的工作流程名稱。
   這會開啟 **編輯工作流程** 視窗。
5. 編輯工作流程內容。有關您可以編輯的工作流程內容的更多詳情，請參閱建立事件工作流程。

工作流程的內容隨即修改並儲存。

若要編輯事件工作流程的狀態：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在 **設定** 索引標籤上，按一下 **事件管理**，然後選取 **工作流程** 索引標籤。
4. 點擊您要編輯的工作流程名稱。
   這會開啟 **編輯工作流程** 視窗。
5. 點擊您要編輯的狀態名稱。
   編輯狀態視窗隨即開啟。
6. 編輯狀態和轉換設定。有關您可以編輯的狀態設定的更多詳情，請參閱建立事件工作流程。
   根據需要，您可以點擊**刪除**按鈕來刪除該狀態。

   > 您無法編輯以下預定義狀態的名稱和類別：**新增**和**已關閉**狀態。您也無法刪除這些預定義狀態。

   > 如果狀態已指派給事件，則無法刪除該狀態。

7. 點擊**儲存**按鈕。

工作流程狀態隨即修改並儲存。

刪除事件工作流程

如果存在屬於父租用戶或子租用戶的關聯事件類型，則無法刪除事件工作流程。在這種情況下，您需要為關聯的事件類型指派不同的工作流程，然後再嘗試刪除事件工作流程。

如果您想要刪除常規程式中使用的某個工作流程，請在刪除之前編輯常規程式的觸發器和/或演算法，以避免出錯。

若要刪除事件工作流程：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤上，按一下**事件管理** ，然後選擇**工作流程**頁籤。
4. 在工作流程清單中，選擇要刪除的工作流程，然後按一下**刪除**。
5. 在確認對話方塊，按一下**刪除**。

   事件工作流程隨即刪除。

管理事件工作量

Kaspersky Next XDR Expert可讓您追蹤與事件相關的工作量。這有助於計算分析師在事件分析和回應上花費的時間，評估分析師的工作量，並有效地分配人力資源。

分析師可以手動添加其在與事件相關的工作上花費的工作量詳情，包括花費的時間以及（根據需要）工作量類別。

您可以透過API檢視、新增、編輯或刪除工作量類別。為了管理工作量類別，您必須具有以下其中一種XDR角色：主管理員、租用戶管理員或SOC管理員。

為了管理事件工作量，您還必須擁有以下其中一個XDR角色：主要管理員、租用戶管理員、初級分析師、一級分析師、二级分析師、SOC管理員、核准人。

Kaspersky Next XDR Expert還允許您產生並匯出分析師或團隊的工作量報告，以便進一步分析。

新增事件工作量

您可以將事件相關工作所花費的工作量新增至事件詳情的**工作量記錄**部分。這有助於分析分析人員處理事件所花費的時間，規劃他們的工作量，並計算工資成本。

若要新增事件工作量：

1. 在主選單中，轉到**監控→事件**部分。
2. 在事件表中，按一下所需事件的ID。
   此時將顯示包含事件詳細資訊的視窗。
3. 轉至**工作量記錄**頁籤，然後按一下**新增**按鈕。
   新增工作量窗格隨即開啟。
4. 根據需要，請在**類別**下拉清單中，選擇工作量類別。
5. 在**小時**和**分鐘**欄位中，指定您在與事件相關的工作上花費的時間。

   分鐘欄位的最大值為59。
6. 點擊**新增**。

您在事件相關的工作上花費的工作量隨即新增。

編輯事件工作量

您可以編輯之前新增的工作量。

您無法編輯其他分析師新增的工作量。

若要編輯事件的工作量：

1. 在主選單中，轉到**監控→事件**部分。
2. 在事件表中，按一下所需事件的ID。
   此時將顯示包含事件詳細資訊的視窗。
3. 轉至**工作量記錄**頁籤。
4. 在**日期**直欄中，按一下要編輯的工作量的日期和時間的連結。
   編輯工作量窗格隨即開啟。
5. 修改工作量的內容，然後按一下**儲存**按鈕。

工作量的內容隨即修改並儲存。

刪除事件工作量

您可以刪除先前新增的工作量。

> 您無法刪除其他分析師新增的工作量。

若要刪除事件的工作量：

1. 在主選單中，轉到**監控→事件**部分。
2. 在事件表中，按一下所需事件的ID。
   此時將顯示包含事件詳細資訊的視窗。
3. 轉至**工作量記錄**頁籤。
4. 在工作量清單中，選取要刪除的工作量旁的核取方塊，然後點擊**刪除**按鈕。

   工作量隨即刪除。

產生和匯出事件報告

您可以產生並匯出有關分析師在處理事件上花費的工作量以及事件對SLA指標的遵守情況的報告。報告以CSV格式儲存。

若要產生事件報告，您必須具有：

- 事故所屬租用戶的存取權限。
- 下列 XDR 角色之一：主管理員、SOC 管理員、租用戶管理員、初級分析師、一級分析師、二級分析師、SOC 經理、與 NCIRCC 互動、核准者、稽核員。

若要產生並匯出報告：

1. 在主選單中，轉到**監控→事件**部分。
2. 在工具列中，按一下**匯出**按鈕，然後在下拉清單中選擇以下選項之一：
   - **工作量報告**，用於匯出分析師在處理事件時所花費的工作量報告。
   - **事件指標報告**，用於匯出有關事件是否符合SLA指標的報告。
3. 在開啟的右側窗格中，指定要在報告中顯示資料的期間。為此，請在**從**和**到**欄位中選擇日期和時間。
   預設情況下，在**從**欄位中，會選取當月的第一天，並將時間設為00:00。在**到**欄位中，選擇當天日期，並將時間設為23:59。

4. 根據需要，請根據您在步驟3中選擇的報告類型，指定其他設定：

   - 對於**工作量報告**：

     - 如果您希望報告包含需要您指定的使用者付出工作量的事件，請選擇分析師或使用者群組。
     - 如果您希望工作量報告包含這些詳情，請啟用**包括事件 ID 和工作量類別詳情**切換開關。
       預設情況下，切換開關是關閉的。

   - 對於**事件指標報告**：

     - 請選擇報告中要包含的事件的優先順序。可能的數值：**低度**、**中度**、**高度**或**緊急**。
     - 若要在報告中僅包含違反SLA的事件，請啟用**僅匯出違反 SLA 的事件**切換開關。
       如果事件中至少有一個過期的SLA事項，則該事件將包含在報告中。當至少一個時限（**分類時間**、**回應時間**或**解決時間**）小於0時，則SLA事項被視為過期。

5. 按一下**匯出**按鈕。

窗格隨即關閉，報告將產生並下載到您的電腦。

設定警示和事件的保存週期

Kaspersky Next XDR Expert可讓您根據需要縮短或延長警示和事件的保存期間。預設情況下，警示和事件的保存期間為360天。

子租用戶會複製父租用戶的警示和事件保存期間。根據需要，您可以編輯子租用戶的保存期間。

若要設定警示或事件的保存期間：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤上，按一下**警示與事件**。
4. 在**保留期**部分，在以下一個或兩個欄位中指定新的保存期間：

   - **警示保留期間（天）**
   - **事件保留期間（天）**

   最小值為 1。
5. 點擊**儲存**按鈕。

新的保存期間隨即設定。

無論設定的保存期間為何，如果已過期的警示關聯到未過期的事件，則該警示僅在關聯事件的保存期間到期後才會刪除。如果已過期的事件包含未過期的關聯警示，則該事件僅在關聯警示的保存期間到期後才會刪除。

如果已過期的父事件包含未過期的子事件，則父事件僅在最後一個子事件的保存期間到期後才會刪除。

設定警示和事件的自動指派

Kaspersky Next XDR Expert可讓您設定警示、事件和子事件自動指派給分析師。如果啟用自動分配，已手動或透過常規程式指派給使用者群組的警示或事件將自動指派給該群組中的分析師。被指派警示或事件的分析師必須符合以下條件：

- 具有**有空**工作狀態。
- 群組中的活動警示和事件數量最少。
- 使用者會話持續時間等於或長於設定的最小值。

如果多個分析師符合自動指派條件，應用程式會將警示或事件隨機指派給其中一位。

如果群組中沒有使用者被指派到該警示或事件，或沒有符合條件的使用者（例如，所有使用者都處於**忙碌**狀態），則該警示或事件將繼續指派給該群組。

自動指派功能僅在警示或事件指派給使用者群組時執行一次。如果應用程式在首次嘗試期間無法將警示或事件指派給用戶，則該警示或事件仍將指派給該群組。系統不會再嘗試指派該警示或事件。

若要設定自動指派功能，您必須擁有以下XDR角色之一：主管理員、 SOC管理員或租用戶管理員。

若要設定警示和事件的自動指派功能：

1. 在主功能表中，轉至**設定 → 租用戶**。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤上，按一下**警示與事件**。
4. 在**自動指派**部分，為以下一個或多個選項啟用自動指派功能：
   - **警示**
   - **事件**
   - **子事件**

5. 在**使用者活動的最短持續時間（分鐘）**欄位中，指定分析員使用者會話的最短持續時間。

   一旦達到此數值，該分析師將被列入符合警示及/或事件指派資格的使用者清單中。預設情況下，該值設為5。

6. 點擊**套用**按鈕。

自動指派功能隨即設定。

警示或事件自動指派給使用者後，指派資訊將顯示在警示或事件詳情的**歷史記錄**部分。自動指派警示或事件時，日誌會將**系統**記錄為指派者。

如果自動指派失敗，錯誤訊息會顯示在警示或事件詳情的**歷史記錄**部分。

檢視資產詳細資訊

「資產詳情」視窗包含與資產相關的所有資訊。

您可以使用下列可用方法之一檢視資產詳情：

- 從警示詳情
- 從事件詳情
- 從事件詳情（如果事件包含資產）：
- 從調查圖表

若要檢視資產詳情：

1. 在主功能表中，轉至**監控**部分，然後執行以下操作之一：

   - 若要從警示詳情檢視資產詳情，請按一下**警示**，然後在**ID**直欄中，按一下包含要檢視其詳情的資產的警示ID。在開啟的視窗中，請轉至**資產**頁籤。
   - 若要從事件詳情中檢視資產詳情，請按一下**事件**，然後在**ID**欄位中，按一下包含要檢視其詳情的資產的事件ID。在開啟的視窗中，請轉至**資產**頁籤。
   - 若要從事件詳情中檢視資產詳情，請按一下**威脅搜尋**，然後按一下包含要檢視其詳情的資產的事件。
   - 若要從調查圖表中檢視資產詳情，請按一下**事件**，然後在**ID**欄位中，按一下包含要檢視其詳情的資產的事件ID。在開啟的視窗中，按一下**在圖表上檢視**按鈕。按一下警示節點，然後在快顯表單中選擇**裝置**或**使用者**。

2. 執行以下操作之一：

   - 按一下所需資產的名稱，然後在下拉清單中，選擇**檢視內容**。
   - 在調查圖表中，按一下資產節點，然後在快顯表單中選擇**檢視詳情**。

資產詳情視窗隨即顯示。

在資產詳情視窗中，您可以在**一般**和**阻止規則**頁籤之間切換。

一般頁籤

一般頁籤包含以下部分：

- **資產內容**— 有關資產的訊息，例如資產名稱、ID和資產所屬的租用戶。

  如果KUMA中的目前產品授權包含AI模組，則會顯示**AI 評分**欄位，其中顯示了資產評分。此欄位顯示資產上的異常活動程度，並可能取值在0到1的範圍內，其中0是預期行為，1是基礎設施中資產的完全意外行為。如果包含內建代理程式的Kaspersky Endpoint Security已安裝在資產（裝置）上，則會顯示**隔離狀態**欄位。您可以點擊狀態旁的**設定**連結來檢視和變更裝置的網路隔離狀態。

- **類別**— 與資產關聯的類別資訊。

- **自訂欄位**— 您在KUMA主控台中建立的資產欄位。

- **已安裝的軟體**— 資產上已安裝的軟體資訊。

  您可以使用**搜尋**欄位快速找到所需的應用程式。開始輸入下列任一資訊後，該應用程式就會顯示出來：應用程式名稱、版本、供應商或安裝日期。

- **KSC：弱點**— 資產的弱點（如果提供）。此資訊適用於從卡巴斯基安全管理中心匯入的資產。

- **卡巴斯基應用程式**— 有關資產上已安裝的卡巴斯基應用程式的資訊。

- **裝置防護狀態**— 資產狀態；可能的值包括：*正常*、*緊急*、*警告*。此資訊適用於從卡巴斯基安全管理中心匯入的資產。

- **KICS for Networks：資產內容**— 有關資產的資訊。此資訊隨即從KICS for Networks匯入。

- **KICS for Networks：弱點**— 資產的弱點（如果提供）。此資訊適用於從KICS for Networks匯入的資產。

您可以按一下V形圖示（ > ）延伸各個部分。

在工具列中，您可以進行以下操作：

- 點選**編輯**按鈕，即可編輯資產詳情。

- 按一下**回應**按鈕，然後從下拉清單中選擇回應操作，即可執行回應操作。

- 透過點擊**連結至類別**按鈕，為資產分配類別。

- 點按**檢視於**按鈕，然後從下拉清單中選擇要移動的位置，轉至**回應歷史**部分，**搜尋威脅**部分，相關警示清單或相關事件清單。

  回應歷史部分，**搜尋威脅**部分中的警示或事件將根據您移動的資產詳情進行篩選。

- 使用遠端終端連線到資產。為此，請點擊**開啟遠端終端**按鈕。

- 透過點擊**匯出到 CSV**按鈕，將有關資產的資訊匯出到CSV檔案。

阻止規則頁籤

此頁籤包含套用於該裝置的阻止規則表。

表格顯示以下規則進度狀態之一：**已套用**、**正在套用**或**錯誤**。

要檢視阻止規則清單，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、SOC經理、一級分析師、二級分析師、初級分析師、核准人、稽核員。

此表格的直欄與您從資源和服務區段開啟的表格相同。

您可以檢視和編輯阻止規則的設定。為此，請點擊**名稱**直欄中帶有規則名稱的連結，打開阻止規則詳情。此時將開啟**編輯阻止規則**窗格，並且**詳細資訊**頁籤已選定。您可以編輯阻止規則的設定。

此外，您也可以點選**轉到威脅搜尋**按鈕，檢視觸發阻止規則時所取得的事件。在**變更記錄**頁籤中，您可以查看套用至阻止規則的所有變更。

若要開啟阻止規則詳情，您必須具備下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。
如果阻止規則屬於您沒有權限的父租用戶，您無法編輯該阻止規則。

透過遠端終端進行調查和回應

Kaspersky Next XDR Expert可讓您使用遠端終端連線到資產。連線成功後，您可以實時與作業系統shell互動，以調查警示和事件、執行診斷和回應威脅。

透過遠端終端，您可以使用資產上安裝的作業系統支援的命令來管理資產。

透過使用遠端終端，您可以同時連線到多個資產。在這種情況下，OSMP主控台中的每個資產都會開啟一個單獨的遠端終端視窗。

如果符合以下條件，您可以使用遠端終端連線到該資產：

- 您已在Kaspersky Next XDR Expert產品授權下啟動了該應用程式。
- 您擁有以下XDR角色之一：主管理員、一級分析師、二級分析師。
- 資產上已安裝Kaspersky Endpoint Security for Linux或Kaspersky Endpoint Security for Windows。

您無法使用遠端終端連線到您存取OSMP主控台的資產。

如果資產遭到入侵，透過遠端終端管理該資產可能會導致惡意代碼的意外執行。僅使用遠端終端連線到您信任的裝置。

管理遠端終端連線

您可以使用遠端終端即時調查資產上的威脅並做出回應。

您可以透過以下其中一種方式來存取遠端終端：

- 從事件詳情。
- 從警示詳情。
- 從資產詳情。
- 從資產表（ **偵測和響應**頁籤）中。

使用遠端終端連線到資產

若要連線到資產：

1. 在主功能表中，執行以下操作之一：
   - 若要從事件詳情存取遠端終端，請轉至**監控** ，然後按一下**事件**。在事件表中，按一下所需事件的ID，然後在開啟的視窗中，轉到**資產**頁籤。
   - 若要從警示詳情存取遠端終端，請轉至**監控**，然後按一下**警示**。在警示表中，按一下所需警示的ID，然後在開啟的視窗中，轉到**資產**頁籤。
   - 若要從資產詳情存取遠端終端，請轉至**資產管理**，然後按一下**資產（裝置）**。選擇**偵測和響應**頁籤，然後在資產表中，按一下所需資產的名稱。在快顯表單中，點擊**詳細資訊**。在開啟的「資產詳細資訊」面板中，點按省略號（ ⋮ ）圖示。
   - 若要從資產表存取遠端終端，請轉至**資產管理**，然後按一下**資產（裝置）**。選擇**偵測和響應**頁籤，然後在資產表中，選擇所需資產。
2. 按一下**開啟遠端終端**按鈕。
3. 如果要對資產執行回應操作，請執行下列步驟：
   a. 在開啟的**遠端終端**視窗中，執行以下其中一種操作：
      - 對於運行Windows的裝置：

        ```
        response.exe
        ```

      - 對於運行Linux的裝置：

        ```
        responser
        ```

b. 按一下**Enter**。

c. 按一下**複製密碼**連結複製密碼，然後將密碼貼上至遠端終端。

與資產建立遠端會話後，您可以調查威脅並根據需要執行回應操作。

遠端終端中執行的所有操作都會被記錄。

如果超過10分鐘沒有任何活動，則與資產的連線將被終止。

檢視遠端終端中的活動連線

使用遠端終端，您可以同時連線和操作多個資產。如果您沒有手動結束與某個資產的會話，或者會話沒有因不活動而過期，即使您訪問OSMP主控台的其他部分，該會話仍保持活動。

若要檢視活動的遠端終端會話，

在OSMP主控台的右上角，按一下**N connections**。

遠端終端視窗隨即開啟。

使用遠端終端斷開與資產的連線

若要斷開與資產的連線，

在**遠端終端**視窗中，按一下叉號（×）圖示來斷開與資產的連線。

或者，如果要斷開與多個資產的連線，請點選**斷開所有連線**按鈕。

資產隨即與遠端終端斷開連線。

透過遠端終端執行回應操作

透過遠端終端連線到資產後，您可以使用命令列介面調查威脅並做出回應。

若要執行指令，請使用下列語法：

```
<common> <parameter> <argument> [--option=value] [--flag]
```

請注意，`--flag`是布林值旗標。如果指定，則設定為`true`。您也可以將其明確設定為`true`或`false`。如果未指定，則設定為`false`。`--case-sensitive`旗標是此規則的例外，其行為在本頁下方有更詳細的描述。

常用命令列參數

設定	類型	描述
說明	字串	打開線上說明。
task-timeout	整數	工作執行時間限制（秒）。
storage-path	字串	用於儲存回應操作結果的檔案共用路徑。

回應操作參數

您可以根據要對資產執行的回應操作使用下列參數：

刪除檔案

要從裝置中刪除文件，請使用下列回應操作參數：

設定	參數	可能的值	類型	描述
`delete-file`	[filePath]	`md5`	字串	MD5檔案雜湊值。與檔案路徑一起使用。可以與SHA256雜湊值一起指定，也可以單獨指定。
		`sha256`	字串	SHA256檔案雜湊值。與檔案路徑一起使用。可以與MD5雜湊值一起指定，也可以單獨指定。
		`skip`	列舉陣列	跳過回應操作的條件。 可能的值： • `self-defence` • `sco` • `kl-signed` • `kl-by-trusted-app`
		`with-subfolders`	標誌	如果`filePath`指定了目錄，請執行遞迴搜尋。
		`case-sensitive`	標誌	指定路徑是否區分大小寫。 如果未指定`--case-sensitive`標誌，工作會使用作業系統的區分大小寫行為，並以區分大小寫的方式執行。若要以不區分大小寫的方式執行工作，請指定`--case-sensitive=false`。

範例

```
delete-file "C:/file path.txt" --md5=12345 --case-sensitive --skip=self-defence --skip=sco --skip=kl-signed --skip=kl-by-trusted-app
```

管理服務

此回應操作僅適用於 Windows 裝置。

若要管理裝置上的服務，請使用下列回應操作參數：

設定	參數	可能的值	類型	描述
change-service	[operationType] 可能的值： • start • stop • pause • resume • delete • change-startup-type	startup-type	enum	指定 change-startup-type 操作的啟動類型。其他操作會忽略此參數。 可能的值： • Boot • System • Automatic • Manual • Disabled
		service-name	字串	服務名稱。支援遮罩。
		md5	字串	MD5檔案雜湊值。可以與SHA256雜湊值一起指定，也可以單獨指定。
		sha256	字串	SHA256檔案雜湊值。可以與MD5雜湊值一起指定，也可以單獨指定。

範例

```
change-service change-startup-type --startup-type=auto --service-name=ServiceName --md5=12345
```

移動檔案到隔離區

為防止威脅傳播，您可以將受感染的檔案移至隔離區。為此，請使用以下回應操作參數：

設定	參數	可能的值	類型	描述
quarantine-file	[filePath]	skip	列舉陣列	跳過回應操作的條件。 可能的值： • self-defence • sco • kl-signed • kl-by-trusted-app
		legacy-file-id	標誌	指定後，將傳回舊版的64位元隔離ID而不是GUID。
		case-sensitive	標誌	指定路徑是否區分大小寫。 如果未指定 --case-sensitive 標誌，工作會使用作業系統的區分大小寫行為，並以區分大小寫的方式執行。若要以不區分大小寫的方式執行工作，請指定 --case-sensitive=false 。
		delete	標誌	隔離檔案後將其刪除。
		md5	字串	MD5檔案雜湊值。與檔案路徑一起使用。可以與SHA256雜湊值一起指定，也可以單獨指定。
		sha256	字串	SHA256檔案雜湊值。與檔案路徑一起使用。可以與MD5雜湊值一起指定，也可以單獨指定。

範例

```
quarantine-file C:/filePath --skip=self-defence --skip=sco --skip=kl-signed --skip=kl-by-trusted-app
```

從隔離區中刪除檔案

若要從裝置上的隔離目錄中刪除受感染的檔案，請使用以下回應操作參數：

設定	可能的值	類型	描述
delete-quarantined-file	file-id	字串	隔離檔案的ID。
	legacy-file-id	整數	舊版隔離ID。

範例

```
delete-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0
```

從隔離區中還原檔案

如果您有理由相信隔離區中的檔案是安全的，則可以將其還原到裝置上。為此，請使用以下回應操作參數：

設定	可能的值	類型	描述
restore-quarantined-file	file-id	字串	隔離檔案的ID。
	legacy-file-id	整數	舊版隔離ID。
	replace	標誌	替換現有檔案。
	remove	標誌	還原後將檔案從隔離區中移除。
	destination	字串	指定用於從備份中還原物件的目標路徑。如果未指定，則物件將還原到原始路徑。
	fallback-destination	字串	指定備用目標路徑。僅當還原到原始路徑失敗（例如路徑不存在或存取被拒絕）時才使用。

範例

```
restore-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0 --replace --fallback-destination="C:/path"
```

從隔離區中取得檔案

可從隔離區目錄取得位於裝置上的隔離檔案，以供進一步分析。若要從隔離區取得檔案，請使用下列回應動作參數：

設定	可能的值	類型	描述
get-quarantined-file	file-id	字串	隔離檔案的ID。
	legacy-file-id	整數	舊版隔離ID。
	stream-index	整數	要檢索的檔案流的索引。

回應操作完成後，所取得的檔案將顯示在OSMP主控台的**檔案**部分中。

範例

```
get-quarantined-file --file-id=453C4D2A-1B45-49C9-A954-1C086E4347F0 --stream-index=0
```

終止進程

若要終止裝置上的進程，請使用下列回應操作參數：

設定	可能的值	類型	描述
terminate-process	path	字串	進程可執行檔案的路徑。
	pid	整數	系統進程ID。
	unique-pid	整數	處理程序 ID。
	md5	字串	MD5檔案雜湊值。與檔案路徑一起使用。可以與SHA256雜湊值一起指定，也可以單獨指定。
	sha256	字串	SHA256檔案雜湊值。與檔案路徑一起使用。可以與MD5雜湊值一起指定，也可以單獨指定。
	case-sensitive	標誌	指定路徑是否區分大小寫。 如果未指定 `--case-sensitive` 標誌，工作會使用作業系統的區分大小寫行為，並以區分大小寫的方式執行。若要以不區分大小寫的方式執行工作，請指定 `--case-sensitive=false`。
	expand-env	標誌	延伸路徑中的環境變數。
	skip	列舉陣列	跳過回應操作的條件。 可能的值： • self-defence • sco • kl-signed • kl-by-trusted-app
	limit	整數	進程終止嘗試的最大次數。如果未指定，則嘗試次數不受限制。

範例

```
terminate-process --pid=1234 --limit=100
```

取得檔案

若要從裝置取得檔案，請使用下列回應操作參數：

設定	參數	可能的值	類型	描述
get-file	[filePath]	md5	字串	MD5檔案雜湊值。與檔案路徑一起使用。可以與SHA256雜湊值一起指定，也可以單獨指定。
		sha256	字串	SHA256檔案雜湊值。與檔案路徑一起使用。可以與MD5雜湊值一起指定，也可以單獨指定。
		max-size	整數	最大檔案大小，以位元組為單位。如果檔案超過此大小，則回應操作失敗。預設情況下，大小無限制。
		case-sensitive	標誌	指定路徑是否區分大小寫。 如果未指定 `--case-sensitive` 標誌，工作會使用作業系統的區分大小寫行為，並以區分大小寫的方式執行。若要以不區分大小寫的方式執行工作，請指定 `--case-sensitive=false`。

回應操作完成後，檔案將儲存到受密碼保護的ZIP封存檔案中。密碼被*感染*了。

範例

```
get-file C:/file --md5=1234567890 --max-size=1000 --case-sensitive
```

啟用網路隔離

若要啟用網路隔離，請使用下列回應操作參數：

設定	可能的值	類型	描述
`start-network-isolation`	`timeout`	整數	網路隔離持續時間。逾時後，隔離將自動停用。預設情況下，持續時間無限制。
	`expand-env`	標誌	延伸路徑中的環境變數。
	`no-notify-user`	標誌	停用網路隔離操作的使用者通知。
	`exclude`		網路排除規則。 此選項不能單獨使用。若要設定排除項，請指定一個或多個子選項： • `process` • `direction` • `remote-ip-v4` • `remote-ip-v6` • `local-port-from` • `local-port-to` • `remote-port-from` • `remote-port-to` • `protocol`
	`process`	字串	指定可選的接收或傳輸進程。該值必須是可執行檔的完整路徑。不支援遮罩。環境變數僅在Windows系統上支援。
	`direction`	enum	指定基於連線的協定（例如TCP）的連線方向或基於資料封包的協定（例如UDP）的資料包方向。如果未指定，則同時使用兩個方向。 可能的值： • `inbound` • `outbound` • `both`
	`remote-ip-v4`	字串	遠端IPv4位址，格式為xxx.xxx.xxx.xxx。支援子網前綴。如果未指定IPv4或IPv6，則符合任何IP位址。
	`remote-ip-v6`	字串	遠端IPv6位址，格式為xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。支援子網前綴。如果未指定IPv4或IPv6，則符合任何IP位址。
	`local-port-from`	整數	本機連接埠範圍的下限。如果未指定，則符合任何連接埠。如果連接埠不適用於封包寫的，則規則無效。
	`local-port-to`	整數	本地連接埠範圍的上限。如果未指定，則符合任何連接埠。如果連接埠不適用於封包寫的，則規則無效。
	`remote-port-from`	整數	遠端連接埠範圍的下限。如果未指定，則符合任何連接埠。如果連接埠不適用於封包寫的，則規則無效。
	`remote-port-to`	整數	遠端連接埠範圍的上限。如果未指定，則符合任何連接埠。如果連接埠不適用於封包寫的，則規則無效。
	`protocol`	整數	IANA協定識別碼（例如，TCP=6）。如果未指定，則符合任何協定。

範例

```
start-network-isolation --timeout=300 exclude --process="C:/process.exe" exclude --local-port-from=1 --local-port-to=10 --direction=inbound --no-notifyuser
```

停用網路隔離

若要停用裝置的網路隔離，請使用下列回應操作參數：

設定	可能的值	類型	描述
stop-network-isolation	no-notify-user	標誌	停用裝置的網路隔離。 預設情況下，當網路隔離被停用時，使用者會收到通知。 如果指定了 --no-notify-user 選項，則使用者不會收到通知。 --no-notify-user 選項僅適用於執行 Windows 的裝置。

範例

```
stop-network-isolation --no-notify-user
```

鑑識資訊

取得檔案清單

若要取得磁碟上儲存的檔案和資料夾清單，請使用下列回應操作參數。

設定	可能的值	類型	描述
get-forensic files	case-sensitive	標誌	指定路徑是否區分大小寫。 僅適用於運行Windows的裝置。 如果未指定 --case-sensitive 標誌，工作會使用作業系統的區分大小寫行為，並以區分大小寫的方式執行。若要以不區分大小寫的方式執行工作，請指定 --case-sensitive=false 。
	with-data-streams	標誌	指定是否在鑑識報告中包含NTFS交換資料流（Alternate Data Streams）。
	max-depth	整數	最大搜尋深度。0表示無限制搜尋深度。1表示僅搜尋指定目錄。
	max-files	整數	要找尋的最大檔案數或NTFS交換資料流（Alternate Data Streams）數。達到限制後搜尋停止。
	include-dir	字串陣列	要包含在掃描範圍內的目錄。目錄路徑可以包含環境變數（例如，%TMP%或%TEMP%）。如果未指定，則包含所有本機目錄。
	exclude-dir	字串陣列	要從掃描中排除的目錄。目錄路徑可以包含環境變數（例如，%TMP%或%TEMP%）。
	include-files	字串陣列	要包含在搜尋中的檔案名稱遮罩（例如，*.ps1）。除非另有說明，否則將包含所有檔案。
	exclude-files	字串陣列	要從搜尋中排除的檔案名稱遮罩（例如，*.ps1）。如果未指定，且已指定 exclude-dir，則會排除所有檔案。

範例

```
get-forensic files --max-depth=3 --max-files=1000 --include-dir="C:/include1" --include-dir=D:/include2
```

取得進程清單

若要取得裝置上正在執行的進程清單，請執行以下命令：

```
get-forensic processes
```

取得自動執行點清單

若要取得自動執行點清單，請執行以下命令：

```
get-forensic autoruns
```

取得進程記憶體傾印檔案

若要取得進程記憶體轉儲，請使用下列回應操作參數：

設定	可能的值	類型	描述
get-forensic process-dump	pid	整數	系統進程ID。
	unique-pid	整數	唯一進程ID。
	md5	字串	MD5檔案雜湊值。與檔案路徑一起使用。
	sha256	字串	SHA256檔案雜湊值。與檔案路徑一起使用。

範例

```
get-forensic process-dump --pid=123 --md5=abcdef123456
```

取得檔案轉儲

若要取得檔案轉儲，請使用下列回應操作參數：

設定	可能的值	類型	描述
`get-forensic files-dump`	`case-sensitive`	標誌	指定路徑是否區分大小寫。預設情況下，由檔案系統決定。 僅適用於運行Windows的裝置。 如果未指定 `--case-sensitive` 標誌，工作會使用作業系統的區分大小寫行為，並以區分大小寫的方式執行。若要以不區分大小寫的方式執行工作，請指定 `--case-sensitive=false` 。
	`path`	字串陣列	要轉儲的檔案的完整路徑。支援通用和元資料檔案（例如，$Mft、$Boot）。不支援遮罩。
	`with-data-streams`	標誌	指定是否在鑑識報告中包含NTFS交換資料流（Alternate Data Streams）。
	`sha256`	字串	SHA256檔案雜湊值。與檔案路徑一起使用。

範例

```
get-forensic files-dump --path="C:/path1"--path="D:/path2" --with-data-streams
```

取得登錄檔金鑰

> 僅適用於運行Windows的裝置。

若要取得登錄檔金鑰，請使用下列回應操作參數：

設定	可能的值	類型	描述
`get-forensic registry-dump`	`path`	字串陣列	要轉儲的登錄檔金鑰的完整路徑。不支援遮罩。

範例

```
get-forensic registry-dump --path="C:/path1" --path="D:/path2"
```

取得系統資訊

若要取得裝置的系統資訊，請執行以下命令：

```
get-forensic system-info
```

取得環境變數

僅適用於運行Windows的裝置。

若要取得環境變數，請執行下列命令：

```
get-forensic environment-variables
```

取得記憶體傾印檔案

若要取得記憶體轉儲，請使用下列回應操作參數：

設定	可能的值	類型	描述
get-forensic memory-dump	compress	旗標	指定轉儲是否使用具有快速壓縮級別的gzip進行壓縮。
	segment-size	整數	指定轉儲分段的大小（以位元組為單位）。轉儲將被分割成指定大小的分段。如果值為0或未指定，則不會分割轉儲。

範例

```
get-forensic memory-dump --compress --segment-size=1000
```

若要取得磁碟映像

若要取得磁碟映像，請使用下列回應操作參數：

設定	可能的值	類型	描述
get-forensic disk-dump	logical	字串	作業系統特定格式的邏輯磁碟機名稱（例如，Windows系統上的C:、D:、E:）。
	physical	字串	作業系統特定格式的實體磁碟機名稱（例如，Windows系統上的 \\.\PHYSICALDRIVE0）。
	compress	旗標	指定轉儲是否使用具有快速壓縮級別的gzip進行壓縮。
	segment-size	整數	指定轉儲分段的大小（以位元組為單位）。轉儲將被分割成指定大小的分段。如果值為0或未指定，則不會分割轉儲。

範例

```
get-forensic disk-dump --logical="C:" --segment-size=1000 --compress
```

威脅搜尋

威脅搜尋頁面包含可協助您分析事件以搜尋未自動偵測到的威脅和弱點的工具。若要從事件集中建立警示，請選擇事件，然後按一下**建立警示**按鈕。

您可以透過以下任一方式開啟**威脅搜尋**頁面：

- 在主功能表中，轉至**監控 → 威脅搜尋。**
- 在警示或事件詳細資訊中，喚起屬性的快顯功能表，然後選擇**在威脅搜尋中搜尋**。
- 在事件詳細資訊中，按一下**在圖表上檢視**按鈕。在開啟的調查圖表中，按一下**威脅搜尋**按鈕。

威脅搜尋頁面顯示事件。您可以透過以下方式篩選事件：

- 透過編輯SQL查詢
- 透過變更時間範圍
- 透過選擇事件所屬的租用戶

處理事件

威脅搜尋部分包含一些工具，可協助您透過分析事件來搜尋威脅和弱點。

事件資料模型

端點代理程式會將以下事件的資訊傳送到OSMP：

- Process
- File Create
- File Modify
- File Rename
- File Read
- File Delete
- File Attributes Modify
- File Creation Time Modify
- File Hardlink Created
- File Symlink Created

- Module
- Registry Create
- Registry Delete
- Registry Modify
- Registry Rename
- Registry Query
- Registry Save
- Connection
- Port Listen
- AMSI Scan
- Process Console Input
- Driver
- Process Interpreted File Run
- DNS
- Pipe Create
- Pipe Connect
- LDAP
- WMI Activity
- WMI Consumer Register
- Code Injection
- Process Access
- Threat Detect
- Threat Detect Processing Result
- Linux Event Log
- Windows Event Log
- Blocked Document
- Applock
- Process Terminated

- Device
- File System Mount
- File System Unmount
- Bits Job Create
- Bits Job Complete
- Bits Job Start
- Bits Job Stop
- Bits Job Add File
- Bits Job Error
- Service Create
- Service Modify
- Service Delete
- Scheduled Task Create
- Scheduled Task Modify
- Scheduled Task Delete
- File Owner Change
- File ACL Change
- Registry Owner Change
- Registry ACL Change
- Executable Memory Mapped
- Agent Start
- Agent Stop
- Agent Install
- Agent Uninstall
- Agent Action
- System Startup
- System Shutdown

- 連線關閉

  啟用 `Connection Close` 事件可能會顯著增加受保護裝置的資源使用量。

Process

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Process 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
ProcessUniqueid	int	進程唯一ID

欄位	類型	描述
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessCalltrace	string	進程堆疊追蹤
ProcessFileLnkName	string	用於執行進程的LNK檔名（不含路徑）
ProcessFileLnkPath	string	用於執行進程的LNK檔案路徑（不含檔名）
ProcessFileLnkFullname	string	用於執行進程的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	用於執行進程的LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限

欄位	類型	描述
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS

欄位	類型	描述
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）

欄位	類型	描述
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單

欄位	類型	描述
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Create

Windows操作系统支援此事件类型。

Registry Create 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegValueName	string	登錄檔項名稱
RegValueType	string	登錄檔項類型
RegValueData	string	登錄檔項中的資料
RegValueFileMd5 [保留將來使用]	string	RegValueData欄位中檔案的MD5雜湊值
RegValueFileFullname [保留將來使用]	string	RegValueData欄位中檔案的完整路徑
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型

欄位	類型	描述
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列

欄位	類型	描述
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值

欄位	類型	描述
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Create

此事件類型支援 Windows、Linux 和 macOS 作業系統。

File Create 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值

欄位	類型	描述
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	已執行檔案的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱

欄位	類型	描述
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID

欄位	類型	描述
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。適用於Linux和macOS
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間

欄位	類型	描述
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的目前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。

欄位	類型	描述
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Modify

此事件類型支援 Windows、Linux 和 macOS 作業系統。

File Modify 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值

欄位	類型	描述
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱

欄位	類型	描述
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID

欄位	類型	描述
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間

欄位	類型	描述
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位

欄位	類型	描述
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Rename

此事件類型支援 Windows、Linux 和 macOS 作業系統。

File Rename 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
FileOldName	string	先前的檔名
FileOldPath	string	先前的檔案路徑
FileOldFullname	string	先前的檔案完整路徑
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）

欄位	類型	描述
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本

欄位	類型	描述
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL

欄位	類型	描述
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑

欄位	類型	描述
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS

欄位	類型	描述
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Read

Windows和Linux作業系統均支援此事件類型（Linux僅支援整合eBPF的版本）。

File Read 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值

欄位	類型	描述
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱

欄位	類型	描述
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID

欄位	類型	描述
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間

欄位	類型	描述
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位

欄位	類型	描述
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Delete

此事件類型支援 Windows、Linux 和 macOS 作業系統。

File Delete 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值

欄位	類型	描述
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱

欄位	類型	描述
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID

欄位	類型	描述
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間

欄位	類型	描述
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位

欄位	類型	描述
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Attributes Modify

Windows和Linux操作系统支援此事件类型。

File Attributes Modify 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值

欄位	類型	描述
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱

欄位	類型	描述
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID

欄位	類型	描述
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間

欄位	類型	描述
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位

欄位	類型	描述
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Creation Time Modify

Windows操作系统支援此事件类型。

File Creation Time Modify 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileDelafterreboot	string	如果重新啟動後檔案將被刪除，則為True。用於刪除操作。僅適用於Windows
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）

欄位	類型	描述
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列

欄位	類型	描述
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值

欄位	類型	描述
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Hardlink Created

Windows操作系统支援此事件类型。

File Hardlink Created 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileTargetName	string	目標檔名
FileTargetPath	string	目標檔案路徑
FileTargetFullname	string	目標檔案的完整路徑
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間

欄位	類型	描述
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）

欄位	類型	描述
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑

欄位	類型	描述
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Symlink Created

Windows操作系统支援此事件类型。

File Symlink Created 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileTargetName	string	目標檔名
FileTargetPath	string	目標檔案路徑
FileTargetFullname	string	目標檔案的完整路徑
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間

欄位	類型	描述
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）

欄位	類型	描述
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑

欄位	類型	描述
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Module

Windows和Linux操作系统支援此事件类型。

Module 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileAttr	int	檔案系統屬性
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileType	string	檔案類型
FileAttrModificationtime	int	檔案屬性上次修改時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
FileHijackingpath	string	原始DLL的路徑
DotnetFileAssemblyName	string	完全限定程式集名稱。包含憑證雜湊值（用於篩選）
DotnetFileAssemblyFlags	int	.NET程式集標誌
DotnetFileModuleFlags	int	.NET程式集模組標誌
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS

欄位	類型	描述
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS

欄位	類型	描述
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名

欄位	類型	描述
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL

欄位	類型	描述
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑

欄位	類型	描述
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Create

Windows 作業系統支援此事件類型。

Registry Create 事件欄位

欄位	類型	描述
IoAId	字串陣列	攻擊指標的唯一識別碼
IoAName	字串陣列	攻擊指標的名稱
IoAVersion	整數陣列	攻擊指標版本
IoAAlert	字串陣列	觸發警示的屬性
IoAConfidence	字串陣列	攻擊指標偵測的信賴程度（高、中、低）
IoASeverity	字串陣列	攻擊指標的嚴重程度（高、中、低）
IoATactics	字串陣列	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	字串陣列	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	字串陣列	與目前攻擊指標相關的事件ID清單
IoAEventCount	整數陣列	與目前攻擊指標相關的事件數量
IoASB	字串陣列	根據攻擊指標邏輯將傳送至沙箱的檔案完整路徑
EventType	string	通知類型
EventId	string	唯一事件 ID
EventTimestamp	整數	用戶端的日期和時間（原始時區為 UTC）
EventReceivedtimestamp	整數	伺服器接收通知的日期和時間
EventSequenceid	整數	已傳送事件的序號
HostId	string	主機唯一識別碼
HostKscId	string	透過 KSC 管理的主機 ID
HostMdrId	string	MDR 解決方案中的受保護主機 ID
HostOsmpId	string	與受保護主機相關聯之 OSMP 型 XDR 解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列 (Windows)
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
主機名稱	string	產生事件的主機名稱

欄位	類型	描述
HostIp	string	主機的 IP 位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	整數	元件更新 KDB 的時間戳記
AgentSw2Timestamp	整數	元件更新 sw2 資料庫的時間戳記
AgentIndexTimestamp	整數	所有元件上次資料庫更新的時間戳記
RegKeyName	string	受此操作影響的登錄金鑰完整路徑和名稱
RegValueName	string	登錄值的名稱
RegValueType	string	登錄值的類型
RegValueData	string	登錄值中的資料
ProcessUniqueid	整數	處理程序唯一 ID
ProcessId	整數	處理程序 ID
ProcessCmdline	string	處理程序的命令列
ProcessCreationflags	string	處理程序建立旗標清單
ProcessDirectory	string	處理程序初始目錄
ProcessProperties	string	執行處理程序之帳戶的屬性清單
ProcessFileLnkName	string	已執行的 LNK 檔案名稱（不含路徑）
ProcessFileLnkPath	string	已執行的 LNK 檔案完整路徑（不含檔案名稱）
ProcessFileLnkFullname	string	已執行的 LNK 檔案完整路徑
ProcessFileLnkCmdline	string	已執行的 LNK 檔案命令列
ProcessFileLnkMd5	string	已執行的 LNK 檔案 MD5 雜湊值
ProcessFileLnkSha256	string	已執行的 LNK 檔案 SHA256 雜湊值
ProcessIntegritylevel	整數	程序完整性層級
ProcessFileName	string	程序可執行檔的名稱（不含路徑）
ProcessFilePath	string	程序可執行檔的完整路徑（不含檔案名稱）
ProcessFileFullname	string	程序可執行檔的完整路徑
ProcessFileSize	整數	程序可執行檔的大小（以位元組為單位）
ProcessFileCreationtime	整數	程序可執行檔的建立時間
ProcessFileModificationtime	整數	程序可執行檔上次修改的時間
ProcessFileMd5	string	程序可執行檔的 MD5 雜湊值
ProcessFileSha256	string	程序可執行檔的 SHA256 雜湊值
ProcessFileAttr	整數	程序可執行檔的檔案系統屬性清單
ProcessFileType	string	程序可執行檔的類型
ProcessFileUrl	string	下載程序可執行檔的來源 URL
ProcessFileEmailSrcAddress	string	以附件形式收到程序可執行檔的寄件者地址
ProcessFileZoneidentifier	整數	從與檔案相關聯的替代資料流 Zone.Identifier 取得的區域 ID
ProcessFileProductname	string	VERSIONINFO 資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO 資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO 資源中的原始檔案名稱
ProcessFileProductvendor	string	VERSIONINFO 資源中的公司名稱值
ProcessFileDescription	string	VERSIONINFO 資源中的描述
ProcessFileVersion	string	VERSIONINFO 資源中的檔案版本

欄位	類型	描述
ProcessFileSignResult	string	簽章驗證結果：通過為 true，否則為 false
ProcessFileSignTimestamp	整數	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案之憑證的主體名稱
ProcessLogonType	string	處理程序的登入工作階段類型
ProcessLogonSessionId	整數	處理程序存取權杖中的登入工作階段 ID
ProcessUserType	整數	執行處理程序之帳戶的屬性清單
ProcessUserName	string	執行處理程序的網域和使用者名稱
ParentProcessUniqueid	整數	父處理程序的唯一 ID
ParentProcessId	整數	父處理程序 ID
ParentProcessCmdline	string	父處理程序的命令列
ParentProcessCreationflags	string	父處理程序的建立旗標
ParentProcessFileLnkName	string	啟動父處理程序的 LNK 檔案名稱（不含路徑）
ParentProcessFileLnkPath	string	啟動父處理程序的 LNK 檔案完整路徑（不含檔案名稱）
ParentProcessFileLnkFullname	string	啟動父處理程序的 LNK 檔案完整路徑
ParentProcessFileLnkCmdline	string	啟動父處理程序的 LNK 檔案命令列
ParentProcessFileLnkMd5	string	啟動父處理程序的 LNK 檔案 MD5 雜湊值
ParentProcessFileLnkSha256	string	啟動父處理程序的 LNK 檔案 SHA256 雜湊值
ParentProcessIntegritylevel	整數	父處理程序的完整性層級
ParentProcessType	string	父處理程序的類型
ParentProcessFileName	string	父處理程序可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父處理程序可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父處理程序可執行檔的完整路徑
ParentProcessFileCreationtime	整數	父處理程序可執行檔的建立時間
ParentProcessFileModificationtime	整數	父處理程序可執行檔的上次修改時間
ParentProcessFileMd5	string	父處理程序可執行檔的 MD5 雜湊值
ParentProcessFileSha256	string	父處理程序可執行檔的 SHA256 雜湊值
ParentProcessFileAttr	整數	父處理程序可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父處理程序可執行檔的類型
ParentProcessFileUrl	string	父處理程序可執行檔的下載來源 URL
ParentProcessFileEmailSrcAddress	string	父處理程序可執行檔以附件形式接收時的寄件者地址
ParentProcessFileCapEffective	string	父處理程序可執行檔的有效權能
ParentProcessFileProductname	string	父處理程序可執行檔之 VERSIONINFO 資源中的產品名稱值
ParentProcessFileOriginalname	string	父處理程序可執行檔之 VERSIONINFO 資源中的原始檔名
ParentProcessFileProductvendor	string	父處理程序可執行檔之 VERSIONINFO 資源中的公司名稱值
ParentProcessFileDescription	string	父處理程序可執行檔之 VERSIONINFO 資源中的描述
ParentProcessFileSignResult	string	簽章驗證結果：通過為 true，否則為 false
ParentProcessFileSignTimestamp	整數	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案之憑證的主體名稱
ParentProcessLogonType	string	父處理程序的登入工作階段類型
ParentProcessLogonSessionId	整數	父處理程序存取權杖中的登入工作階段 ID
ParentProcessProperties	整數	執行父處理程序之帳戶的屬性清單

欄位	類型	描述
ParentProcessUserName	string	執行父處理程序的網域和使用者名稱
GrandParentProcessUniqueid	整數	祖父處理程序的唯一識別碼
GrandParentProcessId	整數	祖父處理程序 ID
GrandParentProcessCmdline	string	祖父處理程序的命令列
GrandParentProcessCreationflags	string	祖父處理程序建立旗標
GrandParentProcessFileLnkName	string	啟動祖父處理程序之 LNK 檔案的名稱（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父處理程序之 LNK 檔案的完整路徑（不含檔案名稱）
GrandParentProcessFileLnkFullname	string	啟動祖父處理程序之 LNK 檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父處理程序之 LNK 檔案的命令列
GrandParentProcessFileLnkMd5	string	啟動祖父處理程序之 LNK 檔案的 MD5 雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父處理程序之 LNK 檔案的 SHA256 雜湊值
GrandParentProcessIntegritylevel	整數	祖父處理程序的完整性層級
GrandParentProcessType	string	祖父處理程序的類型
GrandParentProcessFileName	string	祖父處理程序可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父處理程序可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父處理程序可執行檔的完整路徑
GrandParentProcessFileCreationtime	整數	祖父處理程序可執行檔的建立時間
GrandParentProcessFileModificationtime	整數	祖父處理程序可執行檔上次修改的時間
GrandParentProcessFileMd5	string	祖父處理程序可執行檔的 MD5 雜湊值
GrandParentProcessFileSha256	string	祖父處理程序可執行檔的 SHA256 雜湊值
GrandParentProcessFileAttr	整數	祖父處理程序可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父處理程序可執行檔的類型
GrandParentProcessFileUrl	string	祖父處理程序可執行檔的下載來源 URL
GrandParentProcessFileEmailSrcAddress	string	以附件形式接收祖父處理程序可執行檔時的寄件者地址
GrandParentProcessFileCapEffective	string	祖父處理程序可執行檔的有效權能
GrandParentProcessFileProductname	string	祖父處理程序可執行檔之 VERSIONINFO 資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父處理程序可執行檔之 VERSIONINFO 資源中的原始檔案名稱
GrandParentProcessFileProductvendor	string	祖父處理程序可執行檔之 VERSIONINFO 資源中的公司名稱值
GrandParentProcessFileDescription	string	祖父處理程序可執行檔之 VERSIONINFO 資源中的描述
GrandParentProcessFileSignResult	string	簽章驗證結果：通過為 true，否則為 false
GrandParentProcessFileSignTimestamp	整數	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案之憑證的主體名稱
GrandParentProcessLogonType	string	祖父處理程序的登入工作階段類型
GrandParentProcessLogonSessionId	整數	來自祖父處理程序存取權杖的登入工作階段 ID
GrandParentProcessProperties	整數	執行祖父處理程序之帳戶的屬性清單
GrandParentProcessUserName	string	執行祖父處理程序的網域和使用者名稱
CreatorProcessUniqueid	整數	目前處理程序之實際啟動處理程序的唯一 ID。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessId	整數	目前處理程序之實際啟動處理程序的 ID。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位

欄位	類型	描述
CreatorProcessCmdline	string	目前處理程序之實際啟動處理程序的命令列。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessCreationflags	string	目前處理程序之實際啟動處理程序的建立旗標。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessDirectory	string	目前處理程序之實際啟動處理程序的目前工作目錄。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileLnkName	string	啟動目前處理程序之實際啟動處理程序的 LNK 檔案名稱（不含路徑）。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileLnkPath	string	啟動目前處理程序之實際啟動處理程序的 LNK 檔案完整路徑（不含檔案名稱）。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileLnkFullname	string	啟動目前處理程序之實際啟動處理程序的 LNK 檔案完整路徑。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileLnkCmdline	string	啟動目前處理程序之實際啟動處理程序的 LNK 檔案命令列參數。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileLnkMd5	string	啟動目前處理程序之實際啟動處理程序的 LNK 檔案 MD5 雜湊值。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileLnkSha256	string	啟動目前處理程序之實際啟動處理程序的 LNK 檔案 SHA256 雜湊值。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessIntegritylevel	整數	目前處理程序之實際啟動處理程序的完整性層級。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileName	string	目前處理程序之實際啟動處理程序的可執行檔名稱。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFilePath	string	目前處理程序之實際啟動處理程序的可執行檔所在完整路徑（不含檔案名稱）。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileFullname	string	目前處理程序之實際啟動處理程序的可執行檔完整路徑。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileCreationtime	整數	目前處理程序之實際啟動處理程序的可執行檔建立時間。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileModificationtime	整數	目前處理程序之實際啟動處理程序的可執行檔修改時間。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileMd5	string	目前處理程序之實際啟動處理程序的可執行檔 MD5 雜湊值。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileSha256	string	目前處理程序之實際啟動處理程序的可執行檔 SHA256 雜湊值。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileAttr	整數	目前處理程序之實際啟動處理程序的檔案系統屬性清單。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileType	string	目前處理程序之實際啟動處理程序的類型。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位

欄位	類型	描述
CreatorProcessFileUrl	string	目前處理程序之實際啟動處理程序的下載來源 URL。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileEmailSrcAddress	string	作為附件接收之可執行檔的寄件者地址，該可執行檔是目前處理程序的實際啟動者。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileProductname	string	目前處理程序之實際啟動處理程序檔案的 VERSIONINFO 資源中所含的產品名稱值。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileOriginalname	string	目前處理程序之實際啟動處理程序檔案的 VERSIONINFO 資源中所含的原始檔案名稱。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileProductvendor	string	目前處理程序之實際啟動處理程序檔案的 VERSIONINFO 資源中所含的公司名稱值。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileDescription	string	目前處理程序之實際啟動處理程序的 VERSIONINFO 資源中所含的描述。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileSignResult	string	目前處理程序之實際啟動處理程序的可執行檔，其簽章驗證結果：通過為 true，否則為 false。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileSignTimestamp	整數	目前處理程序之實際啟動處理程序的檔案簽署日期和時間。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessFileSignSubjectname	string	用於簽署目前處理程序之實際啟動處理程序檔案的憑證主體名稱。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessLogonType	string	啟動目前處理程序之實際啟動處理程序的使用者登入工作階段類型。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessLogonSessionId	整數	目前處理程序之實際啟動處理程序的存取權杖中所取得的登入工作階段 ID。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessProperties	整數	啟動目前處理程序之實際啟動處理程序的使用者登入工作階段類型。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位
CreatorProcessUserName	string	啟動目前處理程序之實際啟動處理程序的使用者網域和使用者名稱。「ParentProcess」通常與「CreatorProcess」相同。此時，遙測資料中不會有 CreatorProcess* 欄位，因此必須查看 ParentProcess* 欄位

Registry Delete

Windows操作系统支援此事件类型。

Registry Delete 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegValueName	string	登錄檔項名稱
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱

欄位	類型	描述
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑

欄位	類型	描述
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Modify

Windows操作系统支援此事件类型。

Registry Modify 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegValueName	string	登錄檔項名稱
RegValueType	string	登錄檔項類型
RegValueData	string	登錄檔項中的資料
RegValueFileMd5 [保留將來使用]	string	RegValueData欄位中檔案的MD5雜湊值
RegValueFileFullname [保留將來使用]	string	RegValueData欄位中檔案的完整路徑
RegOldValueData	string	登錄檔項中的先前資料
RegOldValueMd5	string	RegValueData欄位中檔案的先前MD5雜湊值
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID

欄位	類型	描述
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false

欄位	類型	描述
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID

欄位	類型	描述
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	執行運行子進程的進程的網域名稱和使用者名稱。

Registry Rename

Windows操作系统支援此事件类型。

Registry Rename 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	
HostOsmpId	string	
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegValueName	string	登錄檔項名稱
RegValueType	string	登錄檔項類型
RegValueData	string	登錄檔項中的資料
RegOldKeyName	string	先前的登錄檔項名稱
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型

欄位	類型	描述
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌

欄位	類型	描述
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級

欄位	類型	描述
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Query

Windows操作系统支援此事件类型。

Registry Query 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegValueName	string	登錄檔項名稱
RegValueType	string	登錄檔項類型
RegValueData	string	登錄檔項中的資料
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID

欄位	類型	描述
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）

欄位	類型	描述
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型

欄位	類型	描述
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Save

Windows操作系统支援此事件类型。

Registry Save 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegValueName	string	登錄檔項名稱
RegValueType	string	登錄檔項類型
RegValueData	string	登錄檔項中的資料
FileFullname	string	檔案的完整路徑
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱

欄位	類型	描述
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列

欄位	類型	描述
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Connection

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Connection 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
NetSrcIp	string	來源IPv4/IPv6位址

欄位	類型	描述
NetSrcPort	int	來源連接埠號碼
NetDstIp	string	目標IPv4/IPv6位址
NetDstPort	int	目標連接埠號
NetUrlHostname	string	遠端主機名稱
NetUrlPort	int	遠端主機連接埠
NetUri	string	HTTP的目標URI
NetHttpMethod	string	HTTP方法
NetHttpUseragent	string	發起請求的用戶端程式識別碼
NetHttpReferrer	string	指向取得目標URI的資源的URI引用
NetProtocol	string	IP協定
NetDirection	string	網路連線方向（入站、出站）
NetHttpHeaderName	string	HTTP標頭名稱
NetHttpHeaderValue	string	HTTP標頭值
NetRaw	string	標記是否使用了原始套接字
NetTlsVersion	string	TLS 版本
NetTlsSni	string	TLS伺服器名稱指示
NetTlsSniEncrypted	string	TLS加密伺服器名稱指示
NetTlsCertificateMd5	string	TLS憑證的MD5雜湊值
NetTlsCertificateSha1	string	TLS憑證的SHA1雜湊值
NetTlsCertificateSubjectname	string	TLS主題備用名稱（SAN）
NetTlsCertificateIssuername	string	TLS憑證的簽發者名稱
NetTlsCertificateSerialnumber	string	TLS憑證的序號
NetTlsCertificateCheckresult	string	TLS憑證驗證結果
NetTlsCertificateValidfrom	int	TLS憑證生效日期
NetTlsCertificateValidto	int	TLS憑證失效日期
NetTlsCiphersuite	int	TLS支援的演算法
NetTlsJa3	string	TLS憑證的Ja3指紋
NetTlsJa3s	string	TLS憑證的Ja3s指紋
NetTlsJa3Md5	string	TLS憑證Ja3指紋的MD5雜湊值
NetTlsJa3sMd5	string	TLS憑證Ja3s指紋的MD5雜湊值
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列

欄位	類型	描述
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間

欄位	類型	描述
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID

欄位	類型	描述
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間

欄位	類型	描述
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位

欄位	類型	描述
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Port Listen

Windows和Linux操作系统支援此事件类型。

Port Listen 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
NetDstIp	string	來源IPv4/IPv6位址

欄位	類型	描述
NetDstPort	int	來源連接埠號碼
NetProtocol	int	IP協定
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱

欄位	類型	描述
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位

欄位	類型	描述
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型

欄位	類型	描述
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位

欄位	類型	描述
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型

欄位	類型	描述
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

AMSI Scan

Windows操作系统支援此事件类型。

AMSI Scan 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
AmsiContentType	string	傳送到AMSI掃描的物件類型。

欄位	類型	描述
AmsiContentData	string	偵測到的物件內容。
AmsiContentName	string	傳送到AMSI掃描的物件名稱。
AmsiContentMd5	string	傳送到AMSI掃描的物件的MD5雜湊值。
AmsiContentSha256	string	傳送到AMSI掃描的物件的SHA256雜湊值。
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型

欄位	類型	描述
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列

欄位	類型	描述
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Process Console Input

Windows和Linux操作系统支援此事件类型。

Process Console Input 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
InputText	string	互動式輸入文字

欄位	類型	描述
InputType	string	輸入物件類型
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱

欄位	類型	描述
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）

欄位	類型	描述
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS

欄位	類型	描述
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）

欄位	類型	描述
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID

欄位	類型	描述
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Driver

Windows操作系统支援此事件类型。

Driver 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間

欄位	類型	描述
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址

Process Interpreted File Run

Windows操作系统支援此事件类型。

Process Interpreted File Run 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	解釋器將執行的檔名（不含路徑）

欄位	類型	描述
FilePath	string	解釋器將執行的檔案路徑（不含檔名）
FileFullname	string	解釋器將執行的檔案的完整路徑
FileSize	int	解釋器將執行的檔案大小（以位元組為單位）
FileCreationtime	int	解釋器將執行的檔案建立時間
FileModificationtime	int	解釋器將執行的檔案上次修改時間
FileAttrModificationtime	int	解釋器將執行的檔案屬性上次修改時間
FileMd5	string	解釋器將執行的檔案的MD5雜湊值
FileSha256	string	解釋器將執行的檔案的SHA256 雜湊值
FileAttr	int	解釋器將執行的檔案的檔案系統屬性清單
FileType	string	解釋器將執行的檔案類型
FileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
FileProductname	string	VERSIONINFO資源中的應用程式名稱
FileProductvendor	string	VERSIONINFO資源中的企業名稱值
FileDescription	string	VERSIONINFO資源中的描述
FileOriginalname	string	VERSIONINFO資源中的原檔名
FileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	解釋器將執行的檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址，該地址將由解釋器執行
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級

欄位	類型	描述
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID

欄位	類型	描述
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱

欄位	類型	描述
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值

欄位	類型	描述
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位

欄位	類型	描述
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

DNS

Windows和Linux作業系統均支援此事件類型（Linux僅支援外部連線）。

DNS 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
DnsServerIp	string	正在查詢的DNS伺服器

欄位	類型	描述
DnsQueryOptions	string	執行的DNS查詢的選項
DnsQueryStatus	int	操作的錯誤代碼
DnsResourceName	string	正在查詢的URL
DnsResourceType	string	執行的DNS查詢類型
DnsAnswer	string	DNS查詢結果
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址

欄位	類型	描述
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位

欄位	類型	描述
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值

欄位	類型	描述
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID

欄位	類型	描述
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false

欄位	類型	描述
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Pipe Create

Windows操作系统支援此事件类型。

Pipe Create 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
PipeName	string	建立或建立連線的命名管道的名稱

欄位	類型	描述
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述

欄位	類型	描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述

欄位	類型	描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false

欄位	類型	描述
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間

欄位	類型	描述
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Pipe Connect

Windows操作系统支援此事件类型。

Pipe Connect 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
PipeName	string	建立或建立連線的命名管道的名稱

欄位	類型	描述
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述

欄位	類型	描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述

欄位	類型	描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false

欄位	類型	描述
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間

欄位	類型	描述
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

LDAP

Windows操作系统支援此事件类型。

LDAP 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
LdapSearchScope	string	要搜尋的目錄樹狀圖的區域或範圍

欄位	類型	描述
LdapSearchFilter	string	LDAP搜尋查詢用於符合目錄中條目的條件或標準
LdapSearchDn	string	搜尋操作將開始的目錄樹狀圖中的起點或基點
LdapSearchAttr	string	用於篩選或搜尋的特定屬性清單
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID

欄位	類型	描述
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌

欄位	類型	描述
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

WMI Activity

除Windows XP外，所有Windows作業系統均支援此事件類型。

WMI Activity 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
WmiRemote	string	遠端WMI操作標誌

欄位	類型	描述
WmiHostName	string	WMI活動的來源主機名稱
WmiUserName	string	執行WMI操作的使用者帳戶名稱
WmiNamespacename	string	查詢的WMI命名空間
WmiQuery	string	WMI查詢
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型

欄位	類型	描述
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌

欄位	類型	描述
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級

欄位	類型	描述
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

WMI Consumer Register

除Windows XP外，所有Windows作業系統均支援此事件類型。

WMI Consumer Register 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
WmiNamespacename	string	查詢的WMI命名空間

欄位	類型	描述
WmiFiltername	string	事件使用者使用的篩選器名稱
WmiConsumerName	string	已建立事件的使用者名稱
WmiConsumerText	string	事件使用者的MOF程式碼
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單

欄位	類型	描述
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。

欄位	類型	描述
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Code Injection

Windows和Linux操作系统支援此事件类型。

Code Injection 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
TargetProcessUniqueid	int	目標進程唯一ID

欄位	類型	描述
TargetProcessId	int	目標進程識別碼（PID）
TargetProcessCmdline	string	傳遞給目標進程的命令列參數
TargetProcessFileName	string	目標進程（執行代碼注入的進程）可執行檔名
TargetProcessFilePath	string	目標進程（執行代碼注入的進程）可執行檔的完整路徑（不含檔名）
TargetProcessFileFullname	string	目標進程（執行代碼注入的進程）的可執行檔的完整路徑
TargetProcessFileMd5	string	目標進程可執行檔的MD5雜湊值
TargetProcessFileSha256	string	目標進程可執行檔的SHA256雜湊值
TargetProcessIntegritylevel	int	目標進程的完整性等級
TargetProcessFileUrl	string	目標進程可執行檔的下載URL
TargetProcessFileEmailSrcAddress	string	作為附件接收目標進程可執行檔案的發件人地址
SyscallArgs	string	系統調用參數。僅適用於Linux
ProcessCalltrace	string	進程堆疊追蹤
ProcessModifiedcmdline	string	進程的命令列
InjectMethod	string	注入方法
InjectAddress	string	欄位包含有關注入後執行開始的地址的資訊
InjectImageFileName	string	僅適用於SET_WINDOWS_HOOK
InjectImageFileFullname	string	僅適用於SET_WINDOWS_HOOK
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）

欄位	類型	描述
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）

欄位	類型	描述
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID

欄位	類型	描述
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值

欄位	類型	描述
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型

欄位	類型	描述
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Process Access

Windows操作系统支援此事件类型。

Process Access 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
AccessOperationtype	string	對進程句柄執行的存取操作類型（由一個程序對另一個程序執行）。

欄位	類型	描述
AccessRights	string	對進程物件的所需存取權限
ProcessCalltrace	string	進程堆疊追蹤
TargetProcessFileName	string	目標進程（執行代碼注入的進程）可執行檔名
TargetProcessFilePath	string	目標進程（執行代碼注入的進程）可執行檔的完整路徑（不含檔名）
TargetProcessFileFullname	string	目標進程（執行代碼注入的進程）的可執行檔的完整路徑
TargetProcessFileMd5	string	目標進程可執行檔的MD5雜湊值
TargetProcessFileSha256	string	目標進程可執行檔的SHA256雜湊值
TargetProcessFileCreationtime	int	目標進程可執行檔建立時間
TargetProcessFileModificationtime	int	目標進程可執行檔上次修改時間
TargetProcessFileAttrModificationtime	int	目標進程可執行檔屬性上次修改時間
TargetProcessFileSize	int	目標進程可執行檔案大小（以位元組為單位）
TargetProcessUniqueid	int	目標進程唯一ID
TargetProcessId	int	目標進程識別碼（PID）
TargetProcessCmdline	string	傳遞給目標進程的命令列參數
TargetProcessFileUrl	string	目標進程可執行檔的下載URL
TargetProcessFileEmailSrcAddress	string	作為附件接收目標進程可執行檔案的發件人地址
HandleProcessSrcFileName	string	複製句柄的進程名稱
HandleProcessSrcFilePath	string	複製句柄的進程的完整路徑（不含檔名）
HandleProcessSrcFileFullname	string	複製句柄的進程的完整路徑
HandleProcessSrcFileMd5	string	複製句柄的進程的MD5雜湊值
HandleProcessSrcFileSha256	string	複製句柄的進程的SHA256雜湊值
HandleProcessSrcFileCreationtime	int	複製句柄的進程建立時間
HandleProcessSrcFileModificationtime	int	複製句柄的進程上次修改時間
HandleProcessSrcFileAttrModificationtime	int	複製句柄的進程屬性上次修改時間
HandleProcessSrcFileSize	int	複製句柄的進程可執行檔大小
HandleProcessSrcUniqueid	int	複製句柄的進程的唯一PID
HandleProcessSrcId	int	複製句柄的進程的進程識別碼（PID）
HandleProcessSrcIntegritylevel	int	複製句柄的進程的完整性級別
HandleProcessSrcCmdline	string	複製句柄的進程的命令列選項
HandleProcessSrcFileUrl	string	來源進程的下載URL
HandleProcessSrcFileEmailSrcAddress	string	作為附件接收來源進程可執行檔的發件人地址
HandleProcessDstFileName	string	句柄複製到的進程名稱
HandleProcessDstFilePath	string	句柄複製到的進程的完整路徑（不含檔名）
HandleProcessDstFileFullname	string	句柄複製到的進程的完整路徑
HandleProcessDstFileMd5	string	句柄複製到的進程的MD5雜湊值
HandleProcessDstFileSha256	string	句柄複製到的進程的SHA256雜湊值
HandleProcessDstFileCreationtime	int	句柄複製到的進程建立時間
HandleProcessDstFileModificationtime	int	句柄複製到的進程上次修改時間
HandleProcessDstFileAttrModificationtime	int	句柄複製到的進程屬性上次修改時間
HandleProcessDstFileSize	int	句柄複製到的進程可執行檔大小
HandleProcessDstUniqueid	int	句柄複製到的進程的唯一PID

欄位	類型	描述
HandleProcessDstId	int	句柄複製到的進程的進程識別碼（PID）
HandleProcessDstIntegritylevel	int	句柄複製到的進程的完整性等級
HandleProcessDstCmdline	string	句柄複製到的進程的命令列選項
HandleProcessDstFileUrl	string	來源進程的下載URL
HandleProcessDstFileEmailSrcAddress	string	作為附件接收來源進程可執行檔的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID

欄位	類型	描述
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱

欄位	類型	描述
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限

欄位	類型	描述
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值

欄位	類型	描述
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Threat Detect

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Threat Detect 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
ThreatObjectFullname	string	檔案的完整路徑

欄位	類型	描述
ThreatObjectMd5	string	檔案內容的MD5雜湊值
ThreatObjectSha256	string	檔案內容SHA256雜湊值
ThreatObjectType	string	偵測到的物件類型
ThreatVerdictname	string	威脅判定名稱
ThreatRecordid	int	偵測到威脅的記錄ID
ThreatDatabaseTimestamp	int	資料庫上次更新日期和時間
ThreatProcessingmode	int	偵測到物件的處理模式
ThreatSilent	string	True，靜默偵測
NetProtocol	int	IP協定
NetDstIp	string	本機（受攻擊）IPv4/IPv6位址
NetDstPort	int	本機（受攻擊）連接埠號
NetSrcIp	string	遠端（攻擊者）IPv4/IPv6位址
NetSrcPort	int	遠端（攻擊者）連接埠號
ThreatEmailAddress	string	作為附件接收偵測到的檔案的發件人地址
ThreatEmailDestination	string	偵測到的電子郵件的目標地址
ThreatEmailSubject	string	偵測到的電子郵件的主題
ThreatEmailMessageid	string	偵測到的電子郵件的訊息ID
ThreatEmailReceivedtimestamp	string	偵測到的電子郵件的接收時間
ThreatDownloaderFileFullname	string	下載偵測到的檔案的進程的可執行檔路徑
AmsiContentType	string	傳送到AMSI掃描的物件類型。
AmsiContentData	string	偵測到的物件內容。
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS

欄位	類型	描述
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID

欄位	類型	描述
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false

欄位	類型	描述
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID

欄位	類型	描述
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間

欄位	類型	描述
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Threat Detect Processing Result

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Threat Detect Processing Result 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
ThreatObjectFullname	string	檔案的完整路徑

欄位	類型	描述
ThreatObjectMd5	string	檔案內容的MD5雜湊值
ThreatObjectSha256	string	檔案內容SHA256雜湊值
ThreatObjectType	string	偵測到的物件類型
ThreatVerdictname	string	威脅判定名稱
ThreatRecordid	int	偵測到威脅的記錄ID
ThreatDatabaseTimestamp	int	資料庫上次更新日期和時間
ThreatProcessingmode	int	偵測到物件的處理模式
NetProtocol	int	IP協定
NetDstIp	string	本機（受攻擊）IPv4/IPv6位址
NetDstPort	int	本機（受攻擊）連接埠號
NetSrcIp	string	遠端（攻擊者）IPv4/IPv6位址
NetSrcPort	int	遠端（攻擊者）連接埠號
ThreatEmailAddress	string	作為附件接收偵測到的檔案的發件人地址
ThreatDownloaderFileFullname	string	下載偵測到的檔案的進程的可執行檔路徑
ThreatAction	string	對被精確偵測偵測到的物件所採取的操作類型
ThreatActionresult	string	ThreatAction欄位中指定操作的結果。
ThreatActionreason	string	如果操作成功，則該欄位包含0。如果操作失敗，此欄位包含失敗原因。
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）

欄位	類型	描述
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）

欄位	類型	描述
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID

欄位	類型	描述
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值

欄位	類型	描述
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型

欄位	類型	描述
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Linux Event Log

Linux操作系统支援此事件类型。

Linux Event Log 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
LinuxEventType	string	事件類型

欄位	類型	描述
LinuxEventMessage	string	來自日誌的訊息
LinuxOperationResult	string	操作結果 - 例如，成功或失敗
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱

欄位	類型	描述
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位

欄位	類型	描述
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型

欄位	類型	描述
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位

欄位	類型	描述
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型

欄位	類型	描述
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Windows Event Log

Windows操作系统支援此事件类型。

Windows Event Log 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
SystemLogEventXml	string	系統事件日誌中的XML
SystemLogEventId [包含篩選欄位，名稱為常數]	int	系統日誌中的事件ID
SystemLogChannelName [包含篩選欄位，名稱為常數]	string	系統日誌中的頻道名稱
SystemLogProviderName [包含篩選欄位，名稱為常數]	string	系統日誌中的提供者名稱
OmitQualifiers [包含篩選欄位，名稱為常數]		
WinBinary	string	正在處理的物件的檔案屬性
WinData	string	Windows事件日誌事件的主要資料

欄位	類型	描述
WinAccessGranted	string	Windows事件日誌事件的安全性參數
WinAccessList	string	正在處理的物件存取權限
WinAccessMask	string	正在處理的物件存取權限
WinAccessReason	string	將檔案移至該類別的原因
WinAccessRemoved	string	已從物件中移除的存取權限
WinAccountDomain	string	用於驗證登入會話所有者的域名
WinAccountExpires	string	Active Directory物件參數
WinAccountName	string	啟動受控進程所用的帳戶ID
WinAccountSessionIdentifier	string	網路政策伺服器事件中的身份驗證會話識別碼
WinAction	string	事件發生時的系統或安全措施
WinActionID	string	事件期間執行的操作的識別碼
WinActionName	string	事件期間執行的操作名稱
WinActiveProfile	string	活動組態或網路設定檔
WinAddedCAPs	string	新增的中央存取政策清單
WinAdditionalActionsID	string	與事件相關的其他操作的識別碼
WinAdditionalActionsString	string	與事件相關的其他操作的描述或字串
WinAdditionalDetails	string	查詢字串
WinAdditionalInfo	string	有關物件或物件的其他資訊
WinAdditionalInfo2	string	關於事件或物件的其他資訊（第二個欄位）
WinAdvancedOptions	string	進階組態選項
WinAlgorithmName	string	所用加密演算法的名稱
WinAllowedToDelegateTo	string	啟動受控進程所用的帳戶ID
WinAppCorrelationID	string	物件類型代碼
WinApplication	string	正在處理的物件名稱
WinAppName	string	軟體名稱
WinAppVersion	string	軟體元件的版本
WinAsIsCAPs	string	未修改的中央存取政策清單
WinAttributeLDAPDisplayName	string	正在處理的可執行檔的屬性
WinAttributes	string	物件或事件的屬性
WinAttributeSyntaxOID	string	正在處理的物件的檔案屬性
WinAttributeValue	string	正在處理的可執行檔的屬性
WinAuditPolicyChanges	string	Windows事件日誌事件的安全性參數
WinAuditSourceName	string	正在處理的物件名稱
WinAuditStatusCode	string	稽核事件狀態代碼
WinAuthenticationLevel	string	請求或連線的身份驗證等級
WinAuthenticationPackageName	string	正在處理的物件名稱
WinAuthenticationProvider	string	事件的身份驗證提供者
WinAuthenticationServer	string	執行身分驗證的伺服器
WinAuthenticationService	string	事件中使用的身份驗證服務
WinAuthenticationType	string	事件的身份驗證類型
WinBackupType	string	備份類型

欄位	類型	描述
WinBcdCCID	string	智慧卡裝置設定和內容
WinBMaxSlotIndex	string	智慧卡裝置設定和內容
WinBNumClockSupported	string	智慧卡裝置設定和內容
WinBNumDataRateSupported	string	智慧卡裝置設定和內容
WinBootMode	string	Windows事件日誌事件的使用者會話參數
WinBuildVersion	string	發送的統計資料版本
WinBVoltageSupport	string	智慧卡裝置設定和內容
WinCalledStationID	string	身分驗證中調用站識別碼
WinCallerProcessId	string	父進程系統ID（PID）
WinCallerProcessName	string	正在處理的物件名稱
WinCallingStationID	string	身分驗證中的調用站識別碼
WinCalloutKey	string	調用函式或規則的金鑰
WinCalloutName	string	調用函式或規則的名稱
WinCategoryId	string	Windows事件日誌事件中的操作參數
WinCategoryName	string	事件或威脅的類別
WinCertificateTemplate	string	事件中使用的憑證範本
WinCertIssuerName	string	憑證簽發者名稱
WinCertSerialNumber	string	憑證序號
WinCertThumbprint	string	掃描物件和雜湊演算法的數位憑證指紋
WinChangeType	string	更改類型
WinClassId	string	物件類型代碼
WinClassName	string	正在處理的物件名稱
WinClientAddress	string	本機IP位址
WinClientIPAddress	string	發起事件的用戶端IP位址
WinClientName	string	啟動受控進程所用的帳戶ID
WinClientProcessId	string	用戶端進程識別碼
WinClientProcessStartKey	string	建立工作的進程的唯一金鑰
WinCommandLine	string	已啟動進程的命令列
WinCompatibleIds	string	Windows事件日誌事件的附加參數
WinComputerAccountChange	string	Windows事件日誌事件中的操作參數
WinComputerName	string	發生事件的裝置名稱
WinConditions	string	與事件或篩選器相關的條件
WinConfigAccessPolicy	string	組態存取政策
WinConfiguredNames	string	已設定的資源或物件名稱
WinContextInfo	string	Windows事件日誌事件中記錄的工作參數
WinCountOfCredentialsReturned	string	傳回的憑據數量
WinCrashOnAuditFailValue	string	審計失敗時崩潰設定的值
WinCredType	string	憑據類型
WinCurrentEngineVersion	string	安全引擎的當前版本
WinCurrentSignatureVersion	string	當前簽名版本
WinCVEID	string	Windows事件日誌事件的附加參數

欄位	類型	描述
WinDCDNSName	string	網域控制器DNS名稱
WinDCOMorRPC	string	使用的DCOM或RPC協議
WinDeletedCAPs	string	已刪除的中央存取政策清單
WinDestAddress	string	網路事件的目標位址
WinDestinationDRA	string	Windows事件日誌事件的網路連線參數
WinDestPort	string	網路事件的目標連接埠
WinDetectionID	string	偵測到的威脅的識別碼
WinDetectionSource	string	威脅偵測來源
WinDetectionSourceIndex	string	偵測來源索引
WinDetectionTime	string	偵測到威脅的時間
WinDetectionType	string	威脅偵測類型
WinDetectionTypeIndex	string	偵測類型索引
WinDetectionUser	string	偵測到威脅的使用者
WinDeviceClaims	string	參與身分驗證的裝置
WinDeviceDescription	string	正在處理的物件的描述，如物件內容中所定義。
WinDeviceId	string	裝置ID
WinDirection	string	網路流量方向
WinDisabledPrivilegeList	string	已停用權限清單
WinDisableIntegrityChecks	string	標記以停用完整性檢查
WinDisplayName	string	啟動受控進程所用的帳戶ID
WinDisposition	string	處理事件或物件的結果
WinDnsHostName	string	使用者裝置名稱
WinDnsName	string	使用者裝置名稱
WinDomain	string	與事件或物件關聯的網域
WinDomainBehaviorVersion	string	Active Directory物件參數
WinDomainName	string	用於驗證登入會話所有者的域名
WinDomainPolicyChanged	string	Active Directory物件參數
WinDomainSid	string	使用者帳戶安全性識別碼（SID）
WinDSName	string	正在處理的物件名稱
WinDSType	string	軟體偵測到的物件類型
WinDummy	string	Windows事件日誌事件的附加參數
WinDuration	string	事件持續時間
WinDwDataRate	string	智慧卡裝置設定和內容
WinDwDefaultClock	string	智慧卡裝置設定和內容
WinDwFeatures	string	智慧卡裝置設定和內容
WinDwMaxDataRate	string	智慧卡裝置設定和內容
WinDwMaxIFSD	string	智慧卡裝置設定和內容
WinDwMaximumClock	string	智慧卡裝置設定和內容
WinDwMechanical	string	智慧卡裝置設定和內容
WinDwProtocols	string	智慧卡裝置設定和內容
WinDwSyncProtocols	string	智慧卡裝置設定和內容

欄位	類型	描述
WinEAPErrorCode	string	EAP錯誤代碼
WinEAPReasonCode	string	EAP原因代碼
WinEapRootCauseString	string	EAP錯誤根本原因描述
WinEAPType	string	EAP身分驗證類型
WinEffectiveState	string	物件或系統的當前狀態
WinElevatedToken	string	Windows事件日誌事件的安全性參數
WinEnabledPrivilegeList	string	已啟用權限清單
WinEndUSN	string	USN日誌中結束更改識別符號
WinEngineVersion	string	事件發生時的引擎版本
WinEntryType	string	軟體偵測到的物件類型
WinErrorCode	string	Windows事件日誌事件中的操作參數
WinErrorDescription	string	事件期間發生的錯誤描述
WinEventCount	string	事件重複次數
WinEventCountTotal	string	相關事件總數
WinEventId	string	事件識別器
WinEventIdx	string	序列中的事件索引
WinEventSourceId	string	物件類型代碼
WinExecutionID	string	產生事件的進程識別碼
WinExecutionName	string	產生事件的進程名稱
WinExecutionStatus	string	操作執行狀態
WinExecutionStatusIndex	string	執行狀態索引
WinExeFileName	string	正在處理的物件名稱
WinFailureId	string	故障標識符
WinFailurePoint	string	故障點
WinFailureReason	string	將檔案移至該類別的原因
WinFileName	string	正在處理的物件名稱
WinFilterId	string	篩選器識別碼
WinFilterKey	string	篩選器金鑰
WinFilterName	string	篩選器名稱
WinFilterRTID	string	Windows事件日誌事件的網路連線參數
WinFilterType	string	篩選器類型
WinFlags	string	Windows事件日誌事件中的操作參數
WinFlightSigning	string	飛行建造簽名標誌
WinForceLogoff	string	Active Directory物件參數
WinForestRoot	string	啟動受控進程所用的帳戶ID
WinForestRootSid	string	使用者帳戶安全性識別碼（SID）
WinFQDN	string	發起此事件的主機或電腦的完全限定網域名稱（FQDN）
WinFullyQualifiedSubjectMachineName	string	主題的完全限定電腦名稱
WinFullyQualifiedSubjectUserName	string	主題的完全限定使用者名稱
WinFWLink	string	描述該威脅的頁面連結
WinGPOList	string	正在處理的物件存取權限

欄位	類型	描述
WinGroupDomainName	string	群組網域名稱
WinGroupMembership	string	群組成員資格
WinGroupName	string	群組名稱
WinGroupPolicyApplied	string	已套用的群組政策
WinGroupSid	string	群組SID
WinGroupTypeChange	string	使用者群組資訊
WinHandleId	string	物件類型代碼
WinHangType	string	軟體偵測到的物件類型
WinHardwareIds	string	硬體識別碼
WinHomeDirectory	string	正在處理的物件路徑
WinHomePath	string	正在處理的物件路徑
WinHypervisorDebug	string	虛擬機器監控程式偵錯標誌
WinHypervisorLaunchType	string	虛擬機器管理程式啟動類型
WinHypervisorLoadOptions	string	虛擬機器管理程式載入選項
WinIdentity	string	使用者或裝置識別碼
WinImagePath	string	正在處理的物件路徑
WinImpersonationLevel	string	Windows事件日誌事件的安全性參數
WinInitiatorCookie	string	發起方操作cookie
WinInterfaceName	string	網路介面名稱
WinIntfGuid	string	網路介面GUID
WinIpAddress	string	本機IP位址
WinIpAddresses	string	與該物件關聯的IP位址
WinIpPort	string	正在處理的網路連線的來源連接埠號和目標連接埠號
WinKerberosPolicyChange	string	Windows事件日誌事件的安全性參數
WinKernelDebug	string	內核偵錯標誌
WinKeyFilePath	string	金鑰檔案路徑
WinKeyLength	string	Active Directory物件參數
WinKeyModName	string	金鑰模組名稱
WinKeyName	string	加密金鑰名稱
WinKeyType	string	加密金鑰類型
WinLayerId	string	篩選層識別碼
WinLayerKey	string	篩選層金鑰
WinLayerName	string	Windows事件日誌事件的網路連線參數
WinLayerRTID	string	Windows事件日誌事件的網路連線參數
WinLinkName	string	正在處理的物件名稱
WinLmPackageName	string	正在處理的物件名稱
WinLoadOptions	string	載入選項
WinLocalAddress	string	網路事件中的本機位址
WinLocalKeyModPort	string	本機金鑰模組連接埠
WinLocalMac	string	本機MAC位址
WinLocalMMPrincipalName	string	IPsec主模式身份驗證過程中使用的本機安全主體

欄位	類型	描述
WinLocationInformation	string	Windows事件日誌事件的使用者會話參數
WinLockoutDuration	string	Active Directory物件參數
WinLockoutObservationWindow	string	Active Directory物件參數
WinLockoutThreshold	string	Active Directory物件參數
WinLogDroppedPacketsEnabled	string	此標誌指示是否啟用丟棄的網路資料包的日誌記錄
WinLoggingResult	string	日誌記錄結果
WinLogonGuid	string	使用者群組資訊
WinLogonHours	string	Active Directory物件參數
WinLogonID	string	使用者帳戶安全性識別碼（SID）
WinLogonProcessName	string	從Windows事件日誌中取得的物件名稱
WinLogonType	string	登入會話類型
WinLogSuccessfulConnectionsEnabled	string	此標誌指示是否啟用了成功網路連線的日誌記錄
WinMachineAccountQuota	string	Active Directory物件參數
WinMachineInventory	string	電腦清查
WinMajorVersion	string	發送的統計資料版本
WinMandatoryLabel	string	進程的強制性安全標籤
WinMasterKeyId	string	資料加密主金鑰識別碼
WinMaxPasswordAge	string	Active Directory物件參數
WinMemberName	string	啟動受控進程所用的帳戶ID
WinMemberSid	string	使用者帳戶安全性識別碼（SID）
WinMessageNumber	string	Windows事件日誌事件的附加參數
WinMessageTotal	string	Windows事件日誌事件的附加參數
WinMinorVersion	string	發送的統計資料版本
WinMinPasswordAge	string	Active Directory物件參數
WinMinPasswordLength	string	Active Directory物件參數
WinMixedDomainMode	string	Active Directory物件參數
WinMMAuthMethod	string	IPSec主模式協商期間使用的身份驗證方法
WinMMFilterID	string	Windows指派給特定IPSec主模式篩選器的識別碼
WinMMImpersonationState	string	此欄位顯示IPSec主模式身分驗證過程中是否使用了模擬
WinModifiedCAPs	string	已修改的中央存取政策清單
WinModifiedObjectProperties	string	正在處理的物件的描述，如物件內容中所定義。
WinMulticastFlowsEnabled	string	多播流啟用標誌
WinNamingContext	string	Windows事件日誌事件的網路連線參數
WinNASIdentifier	string	網路存取伺服器（NAS）識別碼
WinNASIPv4Address	string	網路存取伺服器（NAS）IPv4位址
WinNASIPv6Address	string	網路存取伺服器（NAS）IPv6位址
WinNASPort	string	網路存取伺服器（NAS）連線的連接埠
WinNASPortType	string	網路存取伺服器（NAS）連接埠類型
WinNetbiosName	string	正在處理的物件名稱
WinNetworkPolicyName	string	已套用的網路政策名稱
WinNewMaxUsers	string	分散式檔案系統資源內容

欄位	類型	描述
WinNewObjectDN	string	物件可分辨名稱
WinNewProcessId	string	新進程ID
WinNewProcessName	string	新進程名稱
WinNewRemark	string	分散式檔案系統資源內容
WinNewSd	string	Windows事件日誌事件的安全性參數
WinNewShareFlags	string	分散式檔案系統資源內容
WinNewState	string	物件或系統的新狀態
WinNewTargetUserName	string	啟動受控進程所用的帳戶ID
WinNewTime	string	事件時間
WinNewUacValue	string	使用者帳戶控制元件的內容
WinNewValue	string	正在處理的物件的檔案屬性
WinNewValueType	string	軟體偵測到的物件類型
WinNotificationPackageName	string	正在處理的物件名稱
WinObjectClass	string	應用程式更新元件中應用程式程式類別的位元遮罩
WinObjectCollectionName	string	正在處理的物件名稱
WinObjectDN	string	物件可分辨名稱
WinObjectGUID	string	使用者群組資訊
WinObjectIdentifyingProperties	string	Windows事件日誌事件的附加參數
WinObjectName	string	從Windows事件日誌中取得的物件名稱
WinObjectProperties	string	Windows事件日誌事件中記錄的工作參數
WinObjectServer	string	Windows事件日誌事件中記錄的工作參數
WinObjectType	string	軟體偵測到的物件類型
WinObjectValueName	string	正在處理的物件名稱
WinOemInformation	string	正在處理的物件的描述，如物件內容中所定義。
WinOldMaxUsers	string	分散式檔案系統資源內容
WinOldObjectDN	string	物件可分辨名稱
WinOldRemark	string	分散式檔案系統資源內容
WinOldSd	string	Windows事件日誌事件的安全性參數
WinOldShareFlags	string	分散式檔案系統資源內容
WinOldTargetUserName	string	啟動受控進程所用的帳戶ID
WinOldUacValue	string	使用者帳戶控制元件的內容
WinOldValue	string	正在處理的物件的檔案屬性
WinOldValueType	string	軟體偵測到的物件類型
WinOpCorrelationID	string	物件類型代碼
WinOperation	string	操作執行類型
WinOperationId	string	Windows事件日誌事件中的操作參數
WinOperationMode	string	操作執行模式
WinOperationType	string	軟體偵測到的物件類型
WinOptions	string	Windows事件日誌事件中的操作參數
WinOriginID	string	物件來源識別碼
WinOriginName	string	物件來源名稱

欄位	類型	描述
WinPackage	string	與該事件相關的資料包名稱或識別碼
WinPackageFullName	string	正在處理的物件名稱
WinPackageName	string	正在處理的物件名稱
WinPackageRelativeAppId	string	物件類型代碼
WinPackageSid	string	與事件相關的資料包SID
WinParam1	string	查詢字串
WinParam2	string	查詢字串
WinParam3	string	查詢字串
WinParam4	string	查詢字串
WinParam5	string	查詢字串
WinParentProcessId	string	建立工作時啟動目前進程的父進程ID
WinParentProcessName	string	父進程名稱
WinPasswordHistoryLength	string	Active Directory物件參數
WinPasswordLastSet	string	Active Directory物件參數
WinPasswordProperties	string	正在處理的物件的描述，如物件內容中所定義。
WinPath	string	正在處理的物件路徑
WinPathFound	string	偵測到的檔案或物件的路徑
WinPayload	string	正在處理的物件的檔案屬性
WinPeerMac	string	對等裝置MAC位址
WinPostCleanStatus	string	威脅消除後狀態
WinPreAuthType	string	軟體偵測到的物件類型
WinPreExecutionStatus	string	操作執行前狀態
WinPreviousEngineVersion	string	安全引擎的先前版本
WinPreviousSignatureVersion	string	先前的簽名版本
WinPreviousTime	string	事件時間
WinPrimaryGroupId	string	使用者群組資訊
WinPrivilegeList	string	正在處理的物件存取權限
WinProcessCreationTime	string	進程建立時間
WinProcessId	string	進程系統ID（PID）
WinProcessName	string	正在處理的物件名稱
WinProductName	string	產生事件的安全性產品名稱
WinProductVersion	string	安全性產品版本
WinProfile	string	使用者或系統設定檔名/ID
WinProfileChanged	string	Windows事件日誌事件中的操作參數
WinProfilePath	string	正在處理的物件路徑
WinProfiles	string	已套用設定檔清單
WinProfileUsed	string	事件中使用的設定檔
WinProperties	string	正在處理的物件的描述，如物件內容中所定義。
WinPropertyName	string	物件的內容名稱
WinProtocol	string	Windows事件日誌事件的網路連線參數
WinProviderKey	string	篩選器或操作的提供者金鑰

欄位	類型	描述
WinProviderName	string	操作或事件的提供者名稱
WinProxyPolicyName	string	代理政策名稱
WinPuaCount	string	Windows事件日誌事件的附加參數
WinPuaPolicyId	string	物件類型代碼
WinQfeVersion	string	發送的統計資料版本
WinQuarantineSessionIdentifier	string	隔離區會話識別碼
WinQuarantineState	string	隔離中的物件狀態
WinReadOperation	string	讀取操作標誌
WinReason	string	事件或操作的原因
WinReasonCode	string	事件原因代碼
WinReasonForRejection	string	操作被拒的原因
WinReasonText	string	事件原因的文字描述
WinRecoveryKeyId	string	恢復金鑰識別碼
WinRecoveryReason	string	使用恢復金鑰的原因
WinRecoveryServer	string	資料恢復伺服器
WinRelativeTargetName	string	正在處理的物件名稱
WinRemediationUser	string	發起補救措施的使用者
WinRemoteAddress	string	連線或操作的遠端位址
WinRemoteAdminEnabled	string	遠端管理啟用標誌
WinRemoteEventLogging	string	遠端事件日誌記錄標誌
WinRemoteKeyModPort	string	遠端金鑰模組連接埠
WinRemoteMachineID	string	遠端電腦識別碼
WinRemoteMMPrincipalName	string	IPsec主模式身份驗證過程中使用的遠端安全主體
WinRemoteUserID	string	遠端使用者識別碼
WinReplicationEvent	string	複製事件標誌
WinReportId	string	物件類型代碼
WinRequestClientInfo	string	發送請求的用戶端資訊
WinRequestCSPProvider	string	事件發生時請求的CSP提供者
WinRequester	string	請求者
WinRequestId	string	請求ID
WinRequestOSVersion	string	請求用戶端的作業系統版本
WinResource	string	操作中涉及的資源或對象
WinResourceAttributes	string	正在處理的物件的檔案屬性
WinResourceManager	string	負責物件的資源管理器
WinResponderCookie	string	回應器操作cookie
WinRestrictedAdminMode	string	Windows事件日誌事件的安全性參數
WinRestrictedSidCount	string	操作受限的SID數量
WinReturnCode	string	操作結果的回傳碼
WinRole	string	主體在操作中的作用
WinRpcCallClientLocality	string	發起事件的RPC用戶端位置，指示呼叫是本機調用還是遠端調用。
WinRuleAttr	string	安全性規則或篩選屬性

欄位	類型	描述
WinRuleId	string	物件類型代碼
WinRuleName	string	正在處理的物件名稱
WinRunspaceId	string	PowerShell運行空間ID
WinSamAccountName	string	啟動受控進程所用的帳戶ID
WinScanID	string	掃描識別碼
WinScanParameters	string	掃描參數
WinScanParametersIndex	string	掃描參數索引
WinScanResources	string	掃描的資源
WinScanTimeHours	string	掃描耗費小時數
WinScanTimeMinutes	string	掃描耗費分鐘數
WinScanTimeSeconds	string	掃描耗費秒數
WinScanType	string	掃描類型
WinScanTypeIndex	string	掃描類型索引
WinSchema	string	物件或事件的結構
WinSchemaFriendlyName	string	結構的友善名稱
WinScriptBlockId	string	物件類型代碼
WinScriptBlockText	string	Windows事件日誌事件的使用者會話參數
WinScriptPath	string	正在處理的物件路徑
WinSecurityDescriptor	string	物件的安全性描述符
WinSecurityPackageName	string	正在處理的物件名稱
WinSerialNumber	string	憑證或安全性物件的序號
WinServerNames	string	參與操作的伺服器名稱清單
WinService	string	與該事件關聯的服務或服務元件的名稱
WinServiceAccount	string	啟動受控進程所用的帳戶ID
WinServiceFileName	string	正在處理的物件名稱
WinServiceName	string	從Windows事件日誌中取得的物件名稱
WinServicePrincipalNames	string	正在處理的物件名稱
WinServiceSid	string	使用者帳戶安全性識別碼（SID）
WinServiceStartType	string	Windows服務的啟動類型
WinServiceType	string	軟體偵測到的物件類型
WinServiceVersion	string	發送的統計資料版本
WinSessionId	string	登入會話的唯一ID
WinSessionName	string	Windows事件日誌事件的使用者會話參數
WinSettingType	string	軟體偵測到的物件類型
WinSettingValue	string	正在處理的物件的檔案屬性
WinSeverityID	string	威脅嚴重等級識別碼
WinSeverityName	string	威脅嚴重等級名稱
WinShareLocalPath	string	正在處理的物件路徑
WinShareName	string	啟動受控進程所用的帳戶ID
WinSID	string	與使用者或物件相關的安全性識別碼（SID）
WinSidFilteringEnabled	string	Windows事件日誌事件的安全性參數

欄位	類型	描述
WinSidHistory	string	使用者帳戶安全性識別碼（SID）
WinSidList	string	使用者帳戶安全性識別碼（SID）
WinSignatureType	string	威脅簽名類型
WinSignatureTypeIndex	string	簽名類型索引
WinSignatureVersion	string	事件發生時的簽名版本
WinSourceAddr	string	Windows事件日誌事件的網路連線參數
WinSourceAddress	string	本機IP位址
WinSourceDRA	string	Windows事件日誌事件的網路連線參數
WinSourceHandleId	string	來源物件的句柄ID
WinSourceID	string	事件或操作來源的識別碼
WinSourceName	string	事件或操作來源的名稱
WinSourcePort	string	正在處理的網路連線的來源連接埠號和目標連接埠號
WinSourceProcessId	string	來源進程ID
WinSourceSid	string	發起操作的主體SID
WinSourceUserName	string	來源用戶名
WinSpnName	string	用於身分驗證的SPN（服務主體名稱）
WinSSID	string	無線網路識別碼（SSID）
WinStagingReason	string	分階段稽核物件的原因
WinStartTime	string	事件時間
WinStartType	string	軟體偵測到的物件類型
WinStartUSN	string	Windows事件日誌事件的網路連線參數
WinState	string	事件發生時物件或系統的狀態
WinStatus	string	正在處理的物件的描述，如物件內容中所定義。
WinStatusCode	string	Windows事件日誌事件中的操作參數
WinStatusDescription	string	對事件或操作當前狀態的描述
WinStopTime	string	事件時間
WinSubcategoryGuid	string	使用者群組資訊
WinSubcategoryId	string	物件類型代碼
WinSubject	string	發起操作的主體相關資訊
WinSubjectAlternativeName	string	憑證SAN（主體備用名稱）欄位包含備用身份
WinSubjectDomainName	string	用於驗證登入會話所有者的域名
WinSubjectKeyIdentifier	string	憑證主體金鑰識別碼
WinSubjectLogonId	string	使用者帳戶安全性識別碼（SID）
WinSubjectMachineName	string	執行操作的電腦名稱
WinSubjectMachineSID	string	執行操作的系統的電腦SID
WinSubjectUserDomainName	string	用於驗證登入會話所有者的域名
WinSubjectUserName	string	啟動受控進程所用的帳戶ID
WinSubjectUserSid	string	使用者帳戶安全性識別碼（SID）
WinSubStatus	string	Windows事件日誌事件中的操作參數
WinTargetDomainName	string	用於驗證登入會話所有者的域名
WinTargetHandleId	string	目標物件的句柄ID

欄位	類型	描述
WinTargetInfo	string	正在處理的物件的描述，如物件內容中所定義。
WinTargetLinkedLogonId	string	使用者帳戶安全性識別碼（SID）
WinTargetLogonGuid	string	使用者群組資訊
WinTargetLogonId	string	使用者帳戶安全性識別碼（SID）
WinTargetName	string	目標物件或資源的名稱
WinTargetOutboundDomainName	string	用於驗證登入會話所有者的域名
WinTargetOutboundUserName	string	啟動受控進程所用的帳戶ID
WinTargetProcessId	string	進程系統ID（PID）
WinTargetProcessName	string	正在處理的物件名稱
WinTargetServer	string	事件的目標伺服器
WinTargetServerName	string	使用者裝置名稱
WinTargetSid	string	使用者帳戶安全性識別碼（SID）
WinTargetState	string	操作後目標物件的狀態
WinTargetUserDomain	string	目標使用者的網域
WinTargetUserName	string	啟動受控進程所用的帳戶ID
WinTargetUserSid	string	使用者帳戶安全性識別碼（SID）
WinTaskContent	string	與事件關聯的排程工作的原始內容
WinTaskContentActionsContext	string	作業系統工作排程器工作參數
WinTaskContentActionsExecCommand	string	進程的命令列參數
WinTaskContentPrincipalsPrincipalid	string	使用者帳戶安全性識別碼（SID）
WinTaskContentPrincipalsPrincipalLogonType	string	登入會話類型
WinTaskContentPrincipalsPrincipalRunLevel	string	作業系統工作排程器工作參數
WinTaskContentPrincipalsPrincipalUserId	string	使用者帳戶安全性識別碼（SID）
WinTaskContentRegistrationInfoAuthor	string	啟動受控進程所用的帳戶ID
WinTaskContentRegistrationInfoDate	string	事件日期
WinTaskContentSettingsAllowHardTerminate	string	作業系統工作排程器工作參數
WinTaskContentSettingsAllowStartOnDemand	string	作業系統工作排程器工作參數
WinTaskContentSettingsDisallowStartIfOnBatteries	string	作業系統工作排程器工作參數
WinTaskContentSettingsEnabled	string	作業系統工作排程器工作參數
WinTaskContentSettingsExecutionTimeLimit	string	事件時間
WinTaskContentSettingsHidden	string	作業系統工作排程器工作參數
WinTaskContentSettingsIdleSettingsRestartOnIdle	string	作業系統工作排程器工作參數
WinTaskContentSettingsIdleSettingsStopOnIdleEnd	string	作業系統工作排程器工作參數
WinTaskContentSettingsMultipleInstancesPolicy	string	作業系統工作排程器工作參數
WinTaskContentSettingsPriority	string	作業系統工作排程器工作參數
WinTaskContentSettingsRunOnlyIfIdle	string	作業系統工作排程器工作參數
WinTaskContentSettingsRunOnlyIfNetworkAvailable	string	作業系統工作排程器工作參數
WinTaskContentSettingsStartWhenAvailable	string	作業系統工作排程器工作參數
WinTaskContentSettingsStopIfGoingOnBatteries	string	作業系統工作排程器工作參數
WinTaskContentSettingsWakeToRun	string	作業系統工作排程器工作參數
WinTaskContentTriggers	string	Windows事件日誌事件中記錄的工作參數

欄位	類型	描述
WinTaskContentversion	string	工作的原始內容版本
WinTaskContentNew	string	排程工作的更新內容
WinTaskContentNewActionsContext	string	作業系統工作排程器工作參數
WinTaskContentNewActionsExecCommand	string	進程的命令列參數
WinTaskContentNewPrincipalsPrincipalid	string	使用者帳戶安全性識別碼（SID）
WinTaskContentNewPrincipalsPrincipalLogonType	string	登入會話類型
WinTaskContentNewPrincipalsPrincipalRunLevel	string	作業系統工作排程器工作參數
WinTaskContentNewPrincipalsPrincipalUserId	string	使用者帳戶安全性識別碼（SID）
WinTaskContentNewRegistrationInfoAuthor	string	啟動受控進程所用的帳戶ID
WinTaskContentNewRegistrationInfoDate	string	事件日期
WinTaskContentNewSettingsAllowHardTerminate	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsAllowStartOnDemand	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsDisallowStartIfOnBatteries	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsEnabled	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsExecutionTimeLimit	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsHidden	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsIdleSettingsRestartOnIdle	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsIdleSettingsStopOnIdleEnd	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsMultipleInstancesPolicy	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsPriority	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsRunOnlyIfIdle	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsRunOnlyIfNetworkAvailable	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsStartWhenAvailable	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsStopIfGoingOnBatteries	string	作業系統工作排程器工作參數
WinTaskContentNewSettingsWakeToRun	string	作業系統工作排程器工作參數
WinTaskContentNewTriggers	string	Windows事件日誌事件中記錄的工作參數
WinTaskContentNewversion	string	更新內容中的工作版本
WinTaskName	string	正在處理的物件名稱
WinTdoAttributes	string	正在處理的物件的檔案屬性
WinTdoDirection	string	Windows事件日誌事件的網路連線參數
WinTdoType	string	軟體偵測到的物件類型
WinTemplateContent	string	憑證範本的內容
WinTemplateDSObjectFQDN	string	Active Directory中範本物件的FQDN
WinTemplateInternalName	string	憑證範本的內部名稱
WinTemplateOID	string	憑證範本的OID（物件識別碼）
WinTemplateSchemaVersion	string	憑證範本的結構版本
WinTemplateVersion	string	憑證範本的版本
WinTerminationTime	string	事件時間
WinTestSigning	string	此標誌指示系統是否啟用測試簽名模式
WinThreatID	string	威脅識別碼
WinThreatName	string	威脅名稱

欄位	類型	描述
WinTicketEncryptionType	string	軟體偵測到的物件類型
WinTicketOptions	string	Active Directory物件參數
WinTokenElevationType	string	安全性權杖提升類型
WinTopLevelName	string	正在處理的物件名稱
WinTransactionId	string	物件類型代碼
WinTransitionsToOn	string	物件或元件過渡到"開啟"狀態
WinTransmittedServices	string	Windows事件日誌事件中的操作參數
WinTreeDelete	string	Windows事件日誌事件的附加參數
WinType	string	事件或物件的類型
WinTypeID	string	事件或威脅類型的識別碼
WinTypeName	string	事件或威脅類型的名稱
WinUnused	string	保留或未使用欄位
WinUnused2	string	事件未使用的其他預留欄位
WinUnused3	string	事件未使用的其他預留欄位
WinUnused4	string	事件未使用的其他預留欄位
WinUnused5	string	事件未使用的其他預留欄位
WinUnused6	string	事件未使用的其他預留欄位
WinUpdateType	string	產品或簽名更新的類型
WinUpdateTypeIndex	string	更新類型索引
WinUser	string	與事件關聯的使用者
WinUserAccountControl	string	使用者帳戶控制元件的內容
WinUserClaims	string	新登入會話的使用者聲明清單
WinUserData	string	Windows事件日誌事件的使用者會話參數
WinUserName	string	使用者
WinUserParameters	string	啟動受控進程所用的帳戶ID
WinUserPrincipalName	string	啟動受控進程所用的帳戶ID
WinUserSid	string	與事件關聯的使用者SID
WinUserUPN	string	使用者的使用者主體名稱（UPN）
WinUserWorkstations	string	使用者裝置名稱
WinVendorIds	string	Windows事件日誌事件的使用者會話參數
WinVirtualAccount	string	啟動受控進程所用的帳戶ID
WinVsmLaunchType	string	虛擬安全模式（VSM）的啟動類型
WinWakeFromState	string	系統從何種電源狀態喚醒（睡眠、休眠等）
WinWakeRequesterTypeAc	string	使用交流電源運作時喚醒請求器類型
WinWakeRequesterTypeDc	string	使用直流電源運作時喚醒請求器類型
WinWeight	string	與事件物件關聯的權重或優先等級
WinWorkstation	string	使用者裝置名稱
WinWorkstationName	string	使用者裝置名稱
WinProcessingErrorDataDataItemName	string	導致處理錯誤的資料項名稱
WinProcessingErrorDataErrorCode	string	事件處理過程中發生的錯誤代碼
WinProcessingErrorDataEventPayload	string	導致錯誤的原始事件有效負載

欄位	類型	描述
WinSystemChannel	string	記錄事件的Windows事件日誌頻道
WinSystemComputer	string	產生事件的電腦名稱
WinSystemEventID	string	用於定義系統中發生的事件類型的事件識別碼
WinSystemEventIDQualifiers	string	提供有關事件擴充資訊的其他事件限定符
WinSystemEventRecordID	string	日誌中的唯一記錄識別碼
WinSystemExecutionProcessID	string	與執行事件關聯的進程識別碼（PID）
WinSystemExecutionThreadID	string	觸發事件的執行緒識別碼（TID）
WinSystemKeywords	string	用於分類和篩選事件的事件關鍵字
WinSystemLevel	string	事件等級表示其嚴重等級或重要性
WinSystemOpcode	string	事件操作代碼，用於描述與事件關聯的操作類型。
WinSystemProviderEventSourceName	string	產生事件的來源名稱
WinSystemProviderGuid	string	事件提供者的全局唯一識別碼
WinSystemProviderName	string	事件提供者的內部名稱
WinSystemSecurityUserID	string	與事件關聯的使用者識別碼
WinSystemTask	string	與事件關聯的工作識別碼
WinSystemTimeCreatedSystemTime	string	事件建立時的時間戳記
WinSystemVersion	string	事件結構版本
WinAutoBackupBackupPath	string	儲存自動備份的檔案或資料夾路徑
WinAutoBackupChannel	string	用於自動備份的通道或來源
WinEventProcessingFailureErrorCode	string	事件處理期間遇到的錯誤代碼
WinEventProcessingFailureEventID	string	導致處理失敗的事件ID
WinEventProcessingFailurePublisherID	string	嘗試記錄失敗事件的應用程式或服務的識別碼
WinEventXMLAddress	string	與事件相關的地址
WinEventXMLParam1	string	附加事件資訊欄位
WinEventXMLParam2	string	附加事件資訊欄位
WinEventXMLParam3	string	附加事件資訊欄位
WinEventXMLSessionID	string	與事件關聯的使用者會話ID
WinEventXMLSource	string	事件來源
WinEventXMLTargetSession	string	與事件相關的目標會話
WinEventXMLUser	string	與事件關聯的使用者
WinFileIsFull	string	日誌已滿且無法再接受新條目的指示器。
WinLogFileClearedSubjectDomainName	string	清除事件日誌的使用者的網域
WinLogFileClearedSubjectLogonId	string	清除事件日誌的使用者的登入ID
WinLogFileClearedSubjectUserName	string	清除事件日誌的使用者名稱
WinLogFileClearedSubjectUserSid	string	清除事件日誌的使用者SID
WinOperationClientFailureClientMachine	string	發生操作故障的用戶端電腦名稱
WinOperationClientFailureClientProcessId	string	導致操作失敗的用戶端進程ID
WinOperationClientFailureComponent	string	發生操作故障的系統組件
WinOperationClientFailureId	string	操作失敗的唯一識別碼
WinOperationClientFailureOperation	string	失敗的操作的名稱或描述
WinOperationClientFailurePossibleCause	string	操作失敗的可能原因

欄位	類型	描述
WinOperationClientFailureResultCode	string	指示成功或失敗原因的操作結果代碼
WinOperationClientFailureUser	string	發起失敗操作的使用者
WinOperationStartedOperationalCode	string	已啟動操作的代碼
WinOperationStartedOperationalHostProcess	string	發起操作的主機進程
WinOperationStartedOperationalProcessID	string	與已啟動操作關聯的進程ID
WinOperationStartedOperationalProviderName	string	提供者或事件來源的名稱
WinOperationStartedOperationalProviderPath	string	提供者或事件來源的路徑
WinServiceShutdown	string	已停止的Windows服務

Blocked Document

Windows和Linux操作系统支援此事件类型。

Blocked Document 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）

欄位	類型	描述
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL

欄位	類型	描述
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS

欄位	類型	描述
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列

欄位	類型	描述
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID

欄位	類型	描述
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述

欄位	類型	描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Applock

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Applock 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
ProcessUniqueid	int	進程唯一ID

欄位	類型	描述
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessCalltrace	string	進程堆疊追蹤
ProcessFileLnkName	string	用於執行進程的LNK檔名（不含路徑）
ProcessFileLnkPath	string	用於執行進程的LNK檔案路徑（不含檔名）
ProcessFileLnkFullname	string	用於執行進程的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	用於執行進程的LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限

欄位	類型	描述
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS

欄位	類型	描述
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）

欄位	類型	描述
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單

欄位	類型	描述
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Process Terminated

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Process Terminated 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
ProcessUniqueid	int	進程唯一ID

欄位	類型	描述
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessCalltrace	string	進程堆疊追蹤
ProcessFileLnkName	string	用於執行進程的LNK檔名（不含路徑）
ProcessFileLnkPath	string	用於執行進程的LNK檔案路徑（不含檔名）
ProcessFileLnkFullname	string	用於執行進程的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	用於執行進程的LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限

欄位	類型	描述
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS

欄位	類型	描述
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）

欄位	類型	描述
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單

欄位	類型	描述
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
ProcessTerminationtime	int	進程完成時間

Device

Windows操作系统支援此事件类型。

Device 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventVersion	string	事件架構版本
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
DeviceId	string	裝置ID
DeviceName	string	裝置名稱
DevicePath	string	裝置路徑
DeviceOperationtype	string	裝置操作類型（例如1 - 連線）
DeviceType	string	裝置類型
DeviceSystemflag	string	標記裝置是否為系統裝置

File System Mount

Windows和Linux操作系统支援此事件类型。

File System Mount 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
VolumeName	string	磁碟卷名稱
VolumePath	string	磁碟卷掛載點
DeviceClass	string	官方規範的裝置類型的GUID
DeviceId	string	裝置ID
DeviceBustype	string	連線裝置使用的匯流排類型
DeviceType	string	裝置類型
DeviceHotpluggable	string	該裝置是否支援熱插拔（是/否）

欄位	類型	描述
DeviceSerialnumber	string	製造商裝置ID
VolumeFilesystemtype	string	磁碟卷的檔案系統類型
DeviceSpaceTotal	uint	磁碟總容量（單位：MB）
DeviceSpaceUsed	uint	磁碟已用空間（單位：MB）
DeviceSpaceFree	uint	磁碟可用空間（單位：MB）

File System Unmount

Windows和Linux操作系统支援此事件类型。

File System Unmount 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
VolumeName	string	磁碟卷名稱
VolumePath	string	磁碟卷掛載點
DeviceClass	string	官方規範的裝置類型的GUID
DeviceId	string	裝置ID
DeviceBustype	string	連線裝置使用的匯流排類型
DeviceType	string	裝置類型
DeviceHotpluggable	string	該裝置是否支援熱插拔（是/否）

欄位	類型	描述
DeviceSerialnumber	string	製造商裝置ID
VolumeFilesystemtype	string	磁碟卷的檔案系統類型
DeviceSpaceTotal	uint	磁碟總容量（單位：MB）
DeviceSpaceUsed	uint	磁碟已用空間（單位：MB）
DeviceSpaceFree	uint	磁碟可用空間（單位：MB）

Bits Job Create

Windows操作系统支援此事件类型。

Bits Job Create 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
BitsjobId	string	作業識別碼（GUID）

欄位	類型	描述
BitsjobName	string	作業名稱
BitsjobOwnerUserName	string	作業所有者的使用者名稱
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	已執行檔案的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名

欄位	類型	描述
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值

欄位	類型	描述
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名

欄位	類型	描述
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Bits Job Complete

Windows操作系统支援此事件类型。

Bits Job Complete 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
BitsjobId	string	作業識別碼（GUID）
BitsjobName	string	作業名稱
BitsjobOwnerUserName	string	作業所有者的使用者名稱
BitsjobUserName	string	執行操作的使用者名稱
BitsjobFilestotal	int	作業中的檔案總數
BitsjobBytestransferred	int	作業中傳輸的位元組總數
BitsjobPeerBytestransferred	int	透過P2P傳輸的位元組數

Bits Job Start

Windows操作系统支援此事件类型。

Bits Job Start 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
BitsjobId	string	作業識別碼（GUID）
BitsjobName	string	作業名稱
BitsjobTransferid	string	作業中檔案傳輸的唯一識別碼（GUID）
BitsjobRemotename	string	資料來源URL
BitsjobDatasourceCreationtime	int	資料來源建立時間
BitsjobDatasourceSize	int	資料來源大小
BitsjobBytestotal	int	作業中的檔案總數

欄位	類型	描述
BitsjobBytestransferred	int	作業中傳輸的位元組總數
BitsjobPeerHostname	int	p2p資料來源的主機名
BitsjobPeerBytestransferred	int	透過P2P傳輸的位元組數

Bits Job Stop

Windows操作系统支援此事件类型。

Bits Job Stop 事件欄位

欄位	類型	描述
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
BitsjobId	string	作業識別碼（GUID）
BitsjobName	string	作業名稱
BitsjobTransferid	string	作業中檔案傳輸的唯一識別碼（GUID）
BitsjobRemotename	string	資料來源URL
BitsjobDatasourceCreationtime	int	資料來源建立時間
BitsjobDatasourceSize	int	資料來源大小
BitsjobBytestotal	int	作業中的檔案總數
BitsjobBytestransferred	int	作業中傳輸的位元組總數

欄位	類型	描述
BitsjobResultStatuscode	int	透過BITS進行資料傳輸操作的結果
BitsjobResultAdditionalinfo	int	關於透過BITS進行資料傳輸結果的其他資訊
BitsjobPeerHostname	string	p2p資料來源的主機名
BitsjobPeerContextinfo	int	P2P資料來源的識別訊息
BitsjobPeerProtocolflags	int	用於確定電腦是否向對等節點提供內容以及是否可以從對等節點下載內容的組態標誌
BitsjobPeerBytestransferred	int	透過P2P傳輸的位元組數
BitsjobProxy	string	用於傳輸資料的代理伺服器
BitsjobBandwidthLimit	int	BITS作業可用於下載或上傳資料的最大速度
BitsjobBandwidthIgnoreonlan	int	此參數決定當來源位址或目標位址位於本機網路時是否忽略速度限制。

Bits Job Add File

Windows操作系统支援此事件类型。

Bits Job Add File 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
Bitsjobld	string	作業識別碼（GUID）

欄位	類型	描述
BitsjobName	string	作業名稱
BitsjobOwnerUserName	string	作業所有者的使用者名稱
BitsjobUserName	string	執行操作的使用者名稱
BitsjobFilestotal	int	作業中的檔案總數
BitsjobRemotename	string	資料來源URL
BitsjobLocalname	string	用於保存作業資料的檔案的本機路徑
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限

欄位	類型	描述
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型

欄位	類型	描述
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型

欄位	類型	描述
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Bits Job Error

Windows操作系统支援此事件类型。

Bits Job Error 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
BitsjobErrorid	int	錯誤識別碼
BitsjobId	string	作業識別碼（GUID）
BitsjobName	string	作業名稱
BitsjobTransferid	string	作業中檔案傳輸的唯一識別碼（GUID）
BitsjobRemotename	string	資料來源URL
BitsjobDatasourceCreationtime	int	資料來源建立時間
BitsjobDatasourceSize	int	資料來源大小

欄位	類型	描述
BitsjobBytestotal	int	作業中的位元組總數
BitsjobBytestransferred	int	作業中傳輸的位元組總數
BitsjobResultStatuscode	int	透過BITS進行資料傳輸操作的結果
BitsjobResultAdditionalinfo	int	關於透過BITS進行資料傳輸結果的其他資訊
BitsjobPeerHostname	string	p2p資料來源的主機名
BitsjobPeerContextinfo	int	P2P資料來源的識別訊息
BitsjobPeerProtocolflags	int	用於確定電腦是否向對等節點提供內容以及是否可以從對等節點下載內容的組態標誌。
BitsjobPeerBytestransferred	int	透過P2P傳輸的位元組數
BitsjobProxy	string	用於傳輸資料的代理伺服器
BitsjobBandwidthLimit	int	BITS作業可用於下載或上傳資料的最大速度
BitsjobBandwidthIgnoreonlan	uint	此參數決定當來源位址或目標位址位於本機網路時是否忽略速度限制。
BitsjobOwnerUserName	string	作業所有者的使用者名稱

Service Create

Windows和Linux操作系统支援此事件类型。

Service Create 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值

欄位	類型	描述
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileAttr	int	檔案系統屬性
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ServiceTitle	string	服務名稱，服務的唯一識別碼
ServiceType	string	服務類型
ServiceStarttype	string	服務啟動類型
ServiceCmdline	string	啟動服務的命令列
ServiceLoadordergroup	string	此服務的載入順序群組名稱
ServiceTagid	uint	ServiceLoadOrderGroup中此服務的唯一標籤值
ServiceDependencies	string	必須在此服務之前開始的載入順序群組名稱或服務名稱
ServiceStartname	string	用於啟動服務的帳戶名稱
ServiceDisplayname	string	顯示的服務名稱
ServiceDeletedelayed	uint	延遲刪除標誌。1 - 服務停止後刪除；0 - 服務立即刪除。對於「服務建立」事件，此欄位為可選欄位。
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessIntegritylevel	int	進程完整性等級
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ParentProcessUniqueid	int	父進程唯一ID

欄位	類型	描述
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessUserName	string	執行父進程的網域和使用者名稱
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessProperties	string	執行父進程的帳戶屬性清單
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單

Service Modify

Windows和Linux操作系统支援此事件类型。

Service Modify 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間

欄位	類型	描述
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileAttr	int	檔案系統屬性
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ServiceTitle	string	服務名稱，服務的唯一識別碼
ServiceType	string	服務類型
ServiceStarttype	string	服務啟動類型
ServiceCmdline	string	啟動服務的命令列
ServiceLoadordergroup	string	此服務的載入順序群組名稱
ServiceTagid	uint	ServiceLoadOrderGroup中此服務的唯一標籤值
ServiceDependencies	string	必須在此服務之前開始的載入順序群組名稱或服務名稱
ServiceStartname	string	用於啟動服務的帳戶名稱
ServiceDisplayname	string	顯示的服務名稱
ServiceOldType	string	修改前的服務類型
ServiceOldStarttype	string	修改前的服務啟動類型
ServiceOldCmdline	string	修改前的服務可執行檔路徑
ServiceOldLoadordergroup	string	修改前此服務的載入順序群組名稱
ServiceOldTagid	uint	修改前ServiceLoadOrderGroup中此服務的唯一標籤值
ServiceOldDependencies	string	必須在此服務之前啟動的載入順序群組名稱或服務名稱（服務修改前）
ServiceOldStartname	string	服務修改前用於啟動服務的帳戶名稱
ServiceOldDisplayname	string	服務修改前顯示的服務名稱
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessIntegritylevel	int	進程完整性等級
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值

欄位	類型	描述
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessUserName	string	執行父進程的網域和使用者名稱
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessProperties	string	執行父進程的帳戶屬性清單
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單

Service Delete

Windows和Linux操作系统支援此事件类型。

Service Delete 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
FileName	string	檔案名稱（不含路徑）
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值

欄位	類型	描述
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileType	string	檔案類型
FileAttr	int	檔案系統屬性
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ServiceTitle	string	服務名稱，服務的唯一識別碼
ServiceType	string	服務類型
ServiceStarttype	string	服務啟動類型
ServiceCmdline	string	啟動服務的命令列
ServiceLoadordergroup	string	此服務的載入順序群組名稱
ServiceTagid	uint	ServiceLoadOrderGroup中此服務的唯一標籤值
ServiceDependencies	string	必須在此服務之前開始的載入順序群組名稱或服務名稱
ServiceStartname	string	用於啟動服務的帳戶名稱
ServiceDisplayname	string	顯示的服務名稱
ServiceDeletedelayed	uint	延遲刪除標誌。1 - 服務停止後刪除；0 - 服務立即刪除。對於「服務建立」事件，此欄位為可選欄位。
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessIntegritylevel	int	進程完整性等級
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ParentProcessUniqueid	int	父進程唯一ID

欄位	類型	描述
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessUserName	string	執行父進程的網域和使用者名稱
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessProperties	string	執行父進程的帳戶屬性清單
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單

Scheduled Task Create

Windows和Linux操作系统支援此事件类型。

Scheduled Task Create 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
TaskName	string	工作名稱，服務的唯一識別碼

欄位	類型	描述
TaskAuthorName	string	工作作者的使用者名稱
TaskUserName	string	用於啟動服務的使用者名稱
TaskUserId	int	用於啟動服務的使用者識別碼。僅適用於Linux/Mac OS
TaskUserSid	string	啟動該服務的使用者SID。僅適用於Windows
TaskRunlevel	string	工作運行的權限等級
TaskCreationtime	int	工作的建立日期和時間
TaskCmdline	string	工作中執行的操作
TaskEnabled	string	標記工作是否已啟用
TaskHidden	string	標記工作是否隱藏
TaskLocation	string	作業系統中工作物件的路徑
TaskSchedule	string	工作運行排程
TaskSource	string	工作來源
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間

欄位	類型	描述
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級

欄位	類型	描述
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌

欄位	類型	描述
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱

欄位	類型	描述
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱

欄位	類型	描述
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Scheduled Task Modify

此事件類型支援 Windows（Windows Vista、Windows Server 2008 及更新版本）和 Linux 作業系統。

Scheduled Task Modify 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
TaskName	string	工作名稱，服務的唯一識別碼

欄位	類型	描述
TaskAuthorName	string	工作作者的使用者名稱
TaskUserName	string	用於啟動服務的使用者名稱
TaskUserSid	string	啟動該服務的使用者SID。僅適用於Windows
TaskRunlevel	string	工作運行的權限等級
TaskCreationtime	int	工作的建立日期和時間
TaskCmdline	string	工作中執行的操作
TaskEnabled	string	標記工作是否已啟用
TaskHidden	string	標記工作是否隱藏
TaskLocation	string	作業系統中工作物件的路徑
TaskSchedule	string	工作運行排程
TaskSource	string	工作來源
TaskOldUserName	string	啟動服務的先前使用者名稱
TaskOldUserSid	string	執行工作的先前使用者SID
TaskOldEnabled	string	標記工作是否已啟用的先前值
TaskOldHidden	string	標記工作是否隱藏的先前值
TaskOldRunlevel	string	執行工作權限的先前等級
TaskOldCmdline	string	先前在工作中執行的操作
TaskOldSchedule	string	先前的工作執行排程
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值

欄位	類型	描述
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位

欄位	類型	描述
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Scheduled Task Delete

Windows和Linux操作系统支援此事件类型。

Scheduled Task Delete 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
TaskName	string	工作名稱，服務的唯一識別碼

欄位	類型	描述
TaskAuthorName	string	工作作者的使用者名稱
TaskUserName	string	用於啟動服務的使用者名稱
TaskUserId	int	用於啟動服務的使用者識別碼。僅適用於Linux/Mac OS
TaskUserSid	string	啟動該服務的使用者SID。僅適用於Windows
TaskRunlevel	string	工作運行的權限等級
TaskCreationtime	int	工作的建立日期和時間
TaskCmdline	string	工作中執行的操作
TaskEnabled	string	標記工作是否已啟用
TaskHidden	string	標記工作是否隱藏
TaskLocation	string	作業系統中工作物件的路徑
TaskSchedule	string	工作運行排程
TaskSource	string	工作來源
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間

欄位	類型	描述
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列

欄位	類型	描述
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間

欄位	類型	描述
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱

欄位	類型	描述
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File Owner Change

此事件類型支援 Windows 和 Linux 作業系統，但不包括 Windows XP x64、Windows Server 2003 x64，以及核心版本早於 4.19.* 的 Linux。

File Owner Change 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記

欄位	類型	描述
FileOldOwnerUserName	string	先前檔案所有者的網域使用者名稱
FileOldOwnerGroupName	string	先前檔案所有者的網域群組名稱
FileName	string	檔案名稱（不含路徑）
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑

欄位	類型	描述
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false

欄位	類型	描述
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址

欄位	類型	描述
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間

欄位	類型	描述
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS

欄位	類型	描述
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

File ACL Change

此事件類型支援 Windows 和 Linux 作業系統，但不包括 Windows XP x64、Windows Server 2003 x64，以及核心版本早於 4.19.* 的 Linux。

File ACL Change 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記

欄位	類型	描述
FileDacl	string	檔案的DACL中定義的存取控制條目清單
FileOldDacl	string	先前在檔案的DACL中定義的存取控制條目清單
FileModifiedDacl	string	檔案的DACL中的修改條目清單
FileSacl	string	檔案的SACL中定義的存取控制條目清單
FileOldSacl	string	檔案的SACL中定義的存取控制條目的先前清單
FileModifiedSacl	string	檔案的SACL中的修改條目清單
FileName	string	檔案名稱（不含路徑）
FilePath	string	檔案的完整路徑（不含檔名）
FileFullname	string	檔案的完整路徑
FileMd5	string	檔案內容的MD5雜湊值
FileSha256	string	檔案內容SHA256雜湊值
FileSize	int	檔案大小（以位元組為單位）
FileCreationtime	int	檔案創建時間
FileModificationtime	int	檔案上次修改時間
FileOwnerUserId	int	檔案所有者用戶ID適用於Linux和macOS
FileOwnerUserName	string	檔案所有者用戶名。適用於Linux和macOS
FileOwnerGroupName	string	檔案所有者群組名稱。適用於Linux和macOS
FileOwnerGroupId	int	檔案所有者群組ID。適用於Linux和macOS
FileType	string	檔案類型
FileCapPermitted	string	檔案的允許權限
FileCapInheritable	string	檔案的可繼承權限
FileCapEffective	string	檔案的有效權限
FileOpenflags	string	指定的開啟標誌（例如O_RDWR | O_APPEND），用於建立/修改/讀取操作。
FileAttrModificationtime	int	檔案屬性上次修改時間
FileAttr	int	檔案系統屬性
FileZoneidentifier	int	從檔案備用流Zone.Identifier中取得的區域ID
FileProductname	string	檔案的VERSIONINFO資源中的產品名稱值
FileProductvendor	string	檔案的VERSIONINFO資源中的企業名稱值
FileDescription	string	檔案的VERSIONINFO資源中的描述
FileOriginalname	string	檔案的VERSIONINFO資源中的原始文件名
FileSignSubjectname	string	關於簽署檔案的組織訊息
FileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
FileSignTimestamp	int	檔案簽署的日期和時間
FileUrl	string	檔案的下載URL
FileEmailSrcAddress	string	作為附件接收檔案的發件人地址
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數

欄位	類型	描述
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名

欄位	類型	描述
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值

欄位	類型	描述
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。

欄位	類型	描述
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型

欄位	類型	描述
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry Owner Change

此事件類型支援 Windows 作業系統，但不包括 Windows XP x64 和 Windows Server 2003 x64。

Registry Owner Change 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱
RegOwnerUserName	string	金鑰登錄檔所有者的網域使用者名稱

欄位	類型	描述
RegOldOwnerUserName	string	先前金鑰登錄檔所有者的網域使用者名稱
RegOwnerGroupName	string	金鑰登錄檔所有者的網域群組名稱
RegOldOwnerGroupName	string	先前金鑰登錄檔所有者的網域群組名稱
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本

欄位	類型	描述
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID

欄位	類型	描述
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID

欄位	類型	描述
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID

欄位	類型	描述
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Registry ACL Change

此事件類型支援 Windows 作業系統，但不包括 Windows XP x64 和 Windows Server 2003 x64。

Registry ACL Change 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
RegKeyName	string	受操作影響的登錄檔項的完整路徑和名稱

欄位	類型	描述
RegDacl	string	登錄檔項的DACL中定義的存取控制條目清單
RegOldDacl	string	登錄檔項的DACL中定義的存取控制條目的先前清單
RegModifiedDacl	string	登錄檔項的DACL中的修改條目清單
RegSacl	string	SACL登錄檔項中的存取控制條目清單
RegOldSacl	string	登錄檔項的SACL中定義的存取控制條目的先前清單
RegModifiedSacl	string	登錄檔項的SACL中的修改條目清單
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限

欄位	類型	描述
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型

欄位	類型	描述
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型

欄位	類型	描述
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型

欄位	類型	描述
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Executable Memory Mapped

Linux操作系统支援此事件类型。

Executable Memory Mapped 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
SyscallArgs	string	系統調用參數。僅適用於Linux

欄位	類型	描述
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	LNK檔案的命令列
ProcessFileLnkMd5	string	執行的LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	已執行進程的檔名（不含路徑）
ProcessFilePath	string	已執行檔案的進程完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	已執行進程的檔案大小（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	當前進程可執行檔的上次修改時間
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	已執行檔案的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	啟動進程的可執行檔案的檔案系統屬性清單
ProcessFileType	string	已執行進程的檔案類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔案的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限

欄位	類型	描述
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	簽發憑證的實體（個人或組織）名稱
ProcessLogonType	string	執行進程的使用者的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	string	啟動進程的使用者的帳戶類型。可能的值：Unknown、Admin、NotAdmin
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	啟動進程的使用者登入的遠端主機的完全限定網域名稱（FQDN）
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）

欄位	類型	描述
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	string	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS

欄位	類型	描述
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	string	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）

欄位	類型	描述
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	string	執行下載器進程的帳戶內容清單

欄位	類型	描述
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

Agent Start

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Agent Start 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
InitiatorId	string	事件發起方識別碼
InitiatorName	string	事件發起方名稱
InitiatorType	string	事件發起方類型
AgentInstanceid	string	唯一代理程式執行的識別碼
ProcessId	int	進程ID
ProcessUniqueid	int	進程唯一ID

Agent Stop

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Agent Stop 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
InitiatorId	string	事件發起方識別碼
InitiatorName	string	事件發起方名稱
InitiatorType	string	事件發起方類型
AgentInstanceid	string	唯一代理程式執行的識別碼
ProcessId	int	代理程式進程ID
ProcessUniqueid	int	代理程式進程唯一識別碼

欄位	類型	描述
AgentStopreason	string	代理程式終止的原因
AgentExitcode	int	代理程式退出代碼

Agent Install

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Agent Install 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
InitiatorId	string	事件發起方識別碼
InitiatorName	string	事件發起方名稱
InitiatorType	string	事件發起方類型

Agent Uninstall

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Agent Uninstall 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
InitiatorId	string	事件發起方識別碼
InitiatorName	string	事件發起方名稱
InitiatorType	string	事件發起方類型

Agent Action

此事件類型支援 Windows、Linux 和 macOS 作業系統。

Agent Action 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
InitiatorId	string	事件發起方識別碼

欄位	類型	描述
InitiatorName	string	事件發起方名稱
InitiatorType	string	事件發起方類型
AgentInstanceid	string	唯一代理程式執行的識別碼
ProcessId	int	代理程式進程ID
ProcessUniqueid	int	代理程式進程唯一識別碼
AgentActionType	string	代理程式中執行的操作類型：0 → SelfProtectionDisabled,1 → SelfProtectionEnabled,2 → SelfProtectionTriggered,3 → PasswordProtectionOn,4 → PasswordProtectionOff,5 → CheckedPermission,Otherwise → Unknown
AgentActionDescription	string	對所執行操作的描述
AgentResultcode	int	執行操作的結果代码

System Startup

此事件類型支援 Windows、Linux 和 macOS 作業系統。

System Startup 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記

System Shutdown

此事件類型支援 Windows、Linux 和 macOS 作業系統。

System Shutdown 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows、Linux、 macOS）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	事件產生的主機名
HostIp	string	主機的IP位址
AgentVersion	string	電腦上安裝的產品版本
AgentKdbTimestamp	int	元件更新KDB的時間戳記
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記

Connection Close

啟用 `Connection Close` 事件可能會顯著增加受保護裝置的資源使用。

Windows和Linux操作系统支援此事件类型。

Connection Close 事件欄位

欄位	類型	描述
IoAId	string array	攻擊指標唯一ID
IoAName	string array	攻擊指標的名稱
IoAVersion	integer array	攻擊版本指標
IoAAlert	string array	提高警覺性的屬性
IoAConfidence	string array	攻擊指標偵測置信度等級（高、中、低）
IoASeverity	string array	攻擊指標嚴重程度等級（高、中、低）
IoATactics	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix政策
IoATechniques	string array	目前攻擊指標所對映的MITRE ATT&CK® Matrix技術
IoAEventIds	string array	與目前攻擊指標相關的事件ID清單
IoAEventCount	integer array	與目前攻擊指標相關的事件計數
IoASB	string array	根據攻擊邏輯指標，發送到沙盒的檔案的完整路徑
EventType	string	通知類型
EventId	string	唯一事件ID
EventTimestamp	int	用戶端上的日期和時間（原為UTC時間）
EventReceivedtimestamp	int	伺服器收到通知的日期和時間
EventSequenceid	int	已發送事件的序號
HostId	string	主機唯一ID
HostKscId	string	透過KSC管理的主機ID
HostMdrId	string	MDR解決方案中的受保護主機ID
HostOsmpId	string	與受保護主機關聯的基於OSMP的XDR解決方案伺服器的識別碼清單
HostOsFamily	string	作業系統系列（Windows和Linux）
HostOsName	string	作業系統名稱
HostOsVersion	string	作業系統版本
HostName	string	主機名稱產生的事件
HostIp	string	主機的IP位址
AgentVersion	string	安裝在電腦上的產品
AgentKdbTimestamp	int	元件更新KDB的時間戳記

欄位	類型	描述
AgentSw2Timestamp	int	元件更新sw2基礎版的時間戳記
AgentIndexTimestamp	int	所有元件上次基礎版更新的時間戳記
NetSrcIp	string	來源IPv4/IPv6位址
NetSrcPort	int	來源連接埠號碼
NetDstIp	string	目標IPv4/IPv6位址
NetDstPort	int	目標連接埠號
NetProtocol	string	IP協定
NetDirection	string	網路連線方向（入站、出站）
NetCreationtime	int	連線的建立時間
NetBytessent	int	連線期間傳送的位元組數
NetBytesreceived	int	連線期間接收的位元組數
NetDuration	int	連線持續時間（秒）
ProcessUniqueid	int	進程唯一ID
ProcessId	int	進程ID
ProcessCmdline	string	進程的命令列
ProcessCreationflags	string	進程建立標誌列表
ProcessDirectory	string	進程初始目錄
ProcessEnvironment	string	環境變數
ProcessProperties	string	執行進程的帳戶的屬性列表
ProcessFileLnkName	string	執行的LNK檔名（不含路徑）
ProcessFileLnkPath	string	執行的可執行檔的完整路徑（不含檔名）
ProcessFileLnkFullname	string	執行的LNK檔案的完整路徑
ProcessFileLnkCmdline	string	可執行LNK檔案命令列
ProcessFileLnkMd5	string	已執行LNK檔案的MD5雜湊值
ProcessFileLnkSha256	string	執行的LNK檔案的SHA256雜湊值
ProcessIntegritylevel	int	進程完整性等級
ProcessType	string	進程類型
ProcessUserRealid	int	真實使用者ID。適用於Linux和macOS
ProcessGroupRealid	int	真實使用者群組ID。適用於Linux和macOS
ProcessUserRealname	string	真實用戶名。適用於Linux和macOS
ProcessGroupRealname	string	真實群組名稱。適用於Linux和macOS
ProcessUserEffectiveid	int	有效使用者ID。適用於Linux和macOS
ProcessGroupEffectiveid	int	有效使用者群組ID。適用於Linux和macOS
ProcessUserEffectivename	string	對映的有效使用者名稱。適用於Linux和macOS
ProcessGroupEffectivename	string	對應的有效群組名稱。適用於Linux和macOS
ProcessFileName	string	進程可執行檔名（不含路徑）
ProcessFilePath	string	進程可執行檔的完整路徑（不含檔名）
ProcessFileFullname	string	進程可執行檔案的完整路徑
ProcessFileSize	int	進程可執行檔（以位元組為單位）
ProcessFileCreationtime	int	進程可執行檔的建立時間
ProcessFileModificationtime	int	進程可執行檔上次修改時間

欄位	類型	描述
ProcessFileAttrModificationtime	int	進程可執行檔案內容的上次修改時間
ProcessFileMd5	string	進程可執行檔的MD5雜湊值
ProcessFileSha256	string	進程可執行檔的SHA256雜湊值
ProcessFileAttr	int	進程可執行檔的檔案系統屬性清單
ProcessFileType	string	進程可執行檔案的類型
ProcessFileUrl	string	進程可執行檔案的下載URL
ProcessFileEmailSrcAddress	string	作為附件接收進程可執行檔的發件人地址
ProcessFileOwnerUserId	int	檔案所有者使用者ID
ProcessFileOwnerGroupId	int	檔案所有者群組ID
ProcessFileOwnerUserName	string	檔案所有者使用者名稱
ProcessFileOwnerGroupName	string	檔案所有者群組名稱
ProcessFileCapPermitted	string	進程可執行檔的允許權限
ProcessFileCapInheritable	string	進程可執行檔的可繼承權限
ProcessFileCapEffective	string	進程可執行檔的有效權限
ProcessFileZoneidentifier	int	從與檔案連線的替代資料流Zone.Identifier取得的區域ID
ProcessFileProductname	string	VERSIONINFO資源中的應用程式名稱
ProcessFileProductversion	string	VERSIONINFO資源中的應用程式版本
ProcessFileOriginalname	string	VERSIONINFO資源中的原檔名
ProcessFileProductvendor	string	VERSIONINFO資源中的企業名稱值
ProcessFileDescription	string	VERSIONINFO資源中的描述
ProcessFileVersion	string	VERSIONINFO資源中的檔案版本
ProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ProcessFileSignTimestamp	int	檔案簽署的日期和時間
ProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ProcessLogonType	string	進程的登入會話類型
ProcessLogonSessionId	int	進程存取權杖中的登入會話ID
ProcessUserType	int	執行進程的帳戶內容清單
ProcessUserName	string	執行進程的網域名稱和使用者名稱
ProcessLogonUserId	int	登入使用者ID。適用於Linux和macOS
ProcessLogonHostName	string	登入遠端主機/IP。適用於Linux和macOS
ParentProcessUniqueid	int	父進程唯一ID
ParentProcessId	int	父進程ID
ParentProcessCmdline	string	父進程的命令列
ParentProcessCreationflags	string	父進程的建立標誌
ParentProcessDirectory	string	父進程的目前工作目錄。適用於Linux和macOS
ParentProcessFileLnkName	string	啟動父進程的LNK檔名（不含路徑）
ParentProcessFileLnkPath	string	啟動父進程的LNK檔案的完整路徑（不含檔名）
ParentProcessFileLnkFullname	string	啟動父進程的LNK檔案的完整路徑
ParentProcessFileLnkCmdline	string	啟動父進程的LNK檔案命令列
ParentProcessFileLnkMd5	string	啟動父進程的LNK檔案的MD5雜湊值
ParentProcessFileLnkSha256	string	啟動父進程的LNK檔案的SHA256雜湊值

欄位	類型	描述
ParentProcessIntegritylevel	int	父進程的完整性等級
ParentProcessType	string	父進程的類型
ParentProcessUserRealid	int	啟動父進程的使用者的真實使用者ID。適用於Linux和macOS
ParentProcessGroupRealid	int	啟動父進程的使用者的真實使用者群組ID。適用於Linux和macOS
ParentProcessUserRealname	string	啟動父進程的使用者的真實使用者名稱。適用於Linux和macOS
ParentProcessGroupRealname	string	啟動父進程的使用者的真實群組名稱。適用於Linux和macOS
ParentProcessUserEffectiveid	int	啟動父進程的使用者的有效使用者ID。Auditd引用欄位
ParentProcessGroupEffectiveid	int	啟動父進程的使用者的有效群組ID。Auditd引用欄位
ParentProcessUserEffectivename	string	啟動父進程的使用者的有效使用者名稱。Auditd引用欄位
ParentProcessGroupEffectivename	string	啟動父進程的使用者的有效群組名稱。Auditd引用欄位
ParentProcessFileName	string	父進程可執行檔的名稱（不含路徑）
ParentProcessFilePath	string	父進程可執行檔的完整路徑（不含檔名）
ParentProcessFileFullname	string	父進程可執行檔的完整路徑
ParentProcessFileCreationtime	int	父進程可執行檔的建立時間
ParentProcessFileModificationtime	int	父進程可執行檔的上次修改時間
ParentProcessFileAttrModificationtime	int	父進程可執行檔屬性的上次修改時間
ParentProcessFileMd5	string	父進程可執行檔的MD5雜湊值
ParentProcessFileSha256	string	父進程可執行檔的SHA256雜湊值
ParentProcessFileAttr	int	父進程可執行檔的檔案系統屬性清單
ParentProcessFileType	string	父進程可執行檔的類型
ParentProcessFileUrl	string	父進程可執行檔的下載URL
ParentProcessFileEmailSrcAddress	string	作為附件接收父進程可執行檔的發件人地址
ParentProcessFileOwnerUserId	int	父進程可執行檔所有者的使用者ID
ParentProcessFileOwnerGroupId	int	父進程可執行檔所有者的群組ID
ParentProcessFileOwnerUserName	string	父進程可執行檔所有者的使用者名稱
ParentProcessFileOwnerGroupName	string	父進程可執行檔所有者的群組名稱
ParentProcessFileCapEffective	string	父進程可執行檔的有效權限
ParentProcessFileProductname	string	父進程可執行檔的VERSIONINFO資源中的產品名稱值
ParentProcessFileOriginalname	string	父進程可執行檔的VERSIONINFO資源中的原檔名
ParentProcessFileProductvendor	string	父進程可執行檔的VERSIONINFO資源中的企業名稱值
ParentProcessFileDescription	string	父進程可執行檔的VERSIONINFO資源中的描述
ParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
ParentProcessFileSignTimestamp	int	檔案簽署的日期和時間
ParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
ParentProcessLogonType	string	父進程的登入會話類型
ParentProcessLogonSessionId	int	父進程存取權杖中的登入會話ID
ParentProcessProperties	int	執行父進程的帳戶屬性清單
ParentProcessUserName	string	執行父進程的網域和使用者名稱
GrandParentProcessUniqueid	int	祖父進程唯一ID
GrandParentProcessId	int	祖父進程ID
GrandParentProcessCmdline	string	祖父進程的命令列

欄位	類型	描述
GrandParentProcessCreationflags	string	祖父進程的建立標誌
GrandParentProcessDirectory	string	祖父進程的當前工作目錄。Linux或macOS特定欄位
GrandParentProcessFileLnkName	string	啟動祖父進程的LNK檔名（不含路徑）
GrandParentProcessFileLnkPath	string	啟動祖父進程的LNK檔案的完整路徑（不含檔名）。
GrandParentProcessFileLnkFullname	string	啟動祖父進程的LNK檔案的完整路徑
GrandParentProcessFileLnkCmdline	string	啟動祖父進程的LNK檔案命令列
GrandParentProcessFileLnkMd5	string	啟動祖父進程的LNK檔案的MD5雜湊值
GrandParentProcessFileLnkSha256	string	啟動祖父進程的LNK檔案的SHA256雜湊值
GrandParentProcessIntegritylevel	int	祖父進程的完整性等級
GrandParentProcessType	string	祖父進程的類型
GrandParentProcessUserRealid	int	啟動祖父進程的使用者的真實使用者ID。適用於Linux和macOS
GrandParentProcessGroupRealid	int	啟動祖父進程的使用者的真實使用者群組ID。適用於Linux和macOS
GrandParentProcessUserRealname	string	啟動祖父進程的使用者的真實使用者名稱。適用於Linux和macOS
GrandParentProcessGroupRealname	string	啟動祖父進程的使用者的真實群組名稱。適用於Linux和macOS
GrandParentProcessUserEffectiveid	int	啟動祖父進程的使用者的有效使用者ID。Auditd引用欄位
GrandParentProcessGroupEffectiveid	int	啟動祖父進程的使用者的有效群組ID。Auditd引用欄位
GrandParentProcessUserEffectivename	string	啟動祖父進程的使用者的有效使用者名稱。Auditd引用欄位
GrandParentProcessGroupEffectivename	string	啟動祖父進程的使用者的有效群組名稱。Auditd引用欄位
GrandParentProcessFileName	string	祖父進程可執行檔的名稱（不含路徑）
GrandParentProcessFilePath	string	祖父進程可執行檔的完整路徑（不含檔名）
GrandParentProcessFileFullname	string	祖父進程可執行檔的完整路徑
GrandParentProcessFileCreationtime	int	祖父進程可執行檔的建立時間
GrandParentProcessFileModificationtime	int	祖父進程可執行檔的上次修改時間
GrandParentProcessFileAttrModificationtime	int	祖父進程可執行檔屬性的上次修改時間
GrandParentProcessFileMd5	string	祖父進程可執行檔的MD5雜湊值
GrandParentProcessFileSha256	string	祖父進程可執行檔的SHA256雜湊值
GrandParentProcessFileAttr	int	祖父進程可執行檔的檔案系統屬性清單
GrandParentProcessFileType	string	祖父進程可執行檔的類型
GrandParentProcessFileUrl	string	祖父進程可執行檔的下載URL
GrandParentProcessFileEmailSrcAddress	string	作為附件接收祖父進程可執行檔案的發件人地址
GrandParentProcessFileOwnerUserId	int	祖父進程可執行檔的所有者的使用者ID
GrandParentProcessFileOwnerGroupId	int	祖父進程可執行檔的所有者的群組ID
GrandParentProcessFileOwnerUserName	string	祖父進程可執行檔的所有者的使用者名稱
GrandParentProcessFileOwnerGroupName	string	祖父進程可執行檔的所有者的群組名稱
GrandParentProcessFileCapEffective	string	祖父進程可執行檔的有效權限
GrandParentProcessFileProductname	string	祖父進程可執行檔的VERSIONINFO資源中的產品名稱值
GrandParentProcessFileOriginalname	string	祖父進程可執行檔的VERSIONINFO資源中的原檔名
GrandParentProcessFileProductvendor	string	祖父進程可執行檔的VERSIONINFO資源中的企業名稱值
GrandParentProcessFileDescription	string	祖父進程可執行檔的VERSIONINFO資源中的描述
GrandParentProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
GrandParentProcessFileSignTimestamp	int	檔案簽署的日期和時間

欄位	類型	描述
GrandParentProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
GrandParentProcessLogonType	string	祖父進程的登入會話類型
GrandParentProcessLogonSessionId	int	祖父進程存取權杖中的登入會話ID
GrandParentProcessProperties	int	執行祖父進程的帳戶內容清單
GrandParentProcessUserName	string	執行祖父進程的網域名稱和使用者名稱
DownloaderProcessUniqueid	int	下載器唯一ID
DownloaderProcessId	int	下載器進程ID
DownloaderProcessCmdline	string	下載器進程的命令列
DownloaderProcessCreationflags	string	下載器進程的建立標誌
DownloaderProcessDirectory	string	下載器進程的當前工作目錄。Linux或macOS特定欄位
DownloaderProcessFileLnkName	string	啟動下載器進程的LNK檔名（不含路徑）
DownloaderProcessFileLnkPath	string	啟動下載器進程的LNK檔案的完整路徑（不含檔名）
DownloaderProcessFileLnkFullname	string	啟動下載器進程的LNK檔案的完整路徑
DownloaderProcessFileLnkCmdline	string	啟動下載器進程的LNK檔案命令列
DownloaderProcessFileLnkMd5	string	啟動下載器進程的LNK檔案的MD5雜湊值
DownloaderProcessFileLnkSha256	string	啟動下載器進程的LNK檔案的SHA256雜湊值
DownloaderProcessIntegritylevel	int	下載器進程的完整性等級
DownloaderProcessType	string	下載器進程類型
DownloaderProcessUserRealid	int	下載器進程發起者的實際使用者ID。適用於Linux和macOS
DownloaderProcessGroupRealid	int	下載器進程發起者的實際使用者群組ID。適用於Linux和macOS
DownloaderProcessUserRealname	string	下載器進程發起者的實際使用者名稱。適用於Linux和macOS
DownloaderProcessGroupRealname	string	下載器進程發起者的實際群組名稱。適用於Linux和macOS
DownloaderProcessUserEffectiveid	int	下載器進程發起者的有效使用者ID。Auditd引用欄位
DownloaderProcessGroupEffectiveid	int	下載器進程發起者的有效群組ID。Auditd引用欄位
DownloaderProcessUserEffectivename	string	下載器進程發起者的有效使用者名稱。Auditd引用欄位
DownloaderProcessGroupEffectivename	string	下載器進程發起者的有效群組名稱。Auditd引用欄位
DownloaderProcessFileName	string	下載器進程可執行檔的名稱（不含路徑）
DownloaderProcessFilePath	string	下載器進程可執行檔的完整路徑（不含檔名）
DownloaderProcessFileFullname	string	下載器進程可執行檔的完整路徑
DownloaderProcessFileCreationtime	int	下載器進程可執行檔的建立時間
DownloaderProcessFileModificationtime	int	下載器進程可執行檔的上次修改時間
DownloaderProcessFileAttrModificationtime	int	下載器進程可執行檔屬性的上次修改時間
DownloaderProcessFileMd5	string	下載器進程可執行檔的MD5雜湊值
DownloaderProcessFileSha256	string	下載器進程可執行檔的SHA256雜湊值
DownloaderProcessFileAttr	int	下載器進程可執行檔的檔案系統屬性清單
DownloaderProcessFileType	string	下載器進程可執行檔的類型
DownloaderProcessFileUrl	string	下載器進程可執行檔的下載URL
DownloaderProcessFileEmailSrcAddress	string	附件中收到下載器可執行檔案的發件人地址
DownloaderProcessFileOwnerUserId	int	下載器進程可執行檔的所有者的使用者ID
DownloaderProcessFileOwnerGroupId	int	下載器進程可執行檔的所有者的群組ID
DownloaderProcessFileOwnerUserName	string	下載器進程可執行檔的所有者的使用者名稱

欄位	類型	描述
DownloaderProcessFileOwnerGroupName	string	下載器進程可執行檔的所有者的群組名稱
DownloaderProcessFileCapEffective	string	下載器進程可執行檔的有效權限
DownloaderProcessFileProductname	string	下載器進程可執行檔的VERSIONINFO資源中的產品名稱值
DownloaderProcessFileOriginalname	string	下載器進程可執行檔的VERSIONINFO資源中的原檔名
DownloaderProcessFileProductvendor	string	下載器進程可執行檔的VERSIONINFO資源中的企業名稱值
DownloaderProcessFileDescription	string	下載器進程可執行檔的VERSIONINFO資源中的描述
DownloaderProcessFileSignResult	string	簽名驗證結果：通過 - true，不通過 - false
DownloaderProcessFileSignTimestamp	int	檔案簽署的日期和時間
DownloaderProcessFileSignSubjectname	string	用於簽署檔案的憑證的主體名稱
DownloaderProcessLogonType	string	下載器程式進程的登入會話類型
DownloaderProcessLogonSessionId	int	下載器過程存取權杖的登入會話ID
DownloaderProcessProperties	int	執行下載器進程的帳戶內容清單
DownloaderProcessUserName	string	執行下載器進程的網域名稱和使用者名稱
CreatorProcessUniqueid	int	當前進程的實際發起進程的唯一ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessId	int	當前進程的實際發起進程的ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCmdline	string	當前進程的實際發起進程的命令列。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessCreationflags	string	當前進程的實際發起進程的建立標誌。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessDirectory	string	當前進程的實際發起進程的目前工作目錄。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkName	string	當前進程的實際發起進程的LNK檔名（不包含路徑）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkPath	string	當前進程的實際發起進程的LNK檔案的完整路徑（不包含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkFullname	string	當前進程的實際發起進程的LNK檔案的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkCmdline	string	當前進程的實際發起進程的LNK檔案的命令列參數。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkMd5	string	當前進程的實際發起進程的LNK檔案的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileLnkSha256	string	當前進程的實際發起進程的LNK檔案的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessIntegritylevel	int	當前進程的實際發起進程的完整性等級。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessType	string	當前進程的實際發起進程的類型。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealid	int	當前進程的實際發起者的真實使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessGroupRealid	int	當前進程的實際發起者（即啟動該進程的使用者）的真實群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupRealname	string	當前進程的實際發起者（即啟動該進程的使用者）的真實群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效使用者ID。適用於Linux和macOS。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectiveid	int	當前進程的實際發起者（即啟動該進程的使用者）的有效群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserEffectivename	string	當前進程的實際發起者的有效用戶名。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessGroupEffectivename	string	當前進程的實際發起者的有效群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileName	string	當前進程的實際發起進程的可執行檔名。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFilePath	string	當前進程的實際啟動進程的可執行檔的完整路徑（不含檔案名稱）。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileFullname	string	當前進程的實際啟動進程的可執行檔的完整路徑。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCreationtime	int	當前進程的實際發起進程的可執行檔的建立時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileModificationtime	int	當前進程的實際發起進程的可執行檔的修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttrModificationtime	int	當前進程的實際發起進程的可執行檔的屬性修改時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileMd5	string	當前進程的實際發起進程的可執行檔的MD5雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSha256	string	當前進程的實際發起進程的可執行檔的SHA256雜湊值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileAttr	int	當前進程的實際發起進程的檔案系統屬性清單。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileType	string	當前進程的實際發起進程的類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileUrl	string	當前進程的實際發起進程的下載URL。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileEmailSrcAddress	string	作為附件發送可執行檔的發送者位址，即目前進程的實際發起者。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserId	int	當前進程的實際發起進程檔案的擁有者使用者ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

欄位	類型	描述
CreatorProcessFileOwnerGroupId	int	當前進程的實際發起進程檔案的擁有者群組ID。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerUserName	string	當前進程的實際發起進程檔案的所有者使用者名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOwnerGroupName	string	當前進程的實際發起者進程文件的所有者群組名稱。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileCapEffective	string	當前進程的實際發起進程的有效效能。適用於Linux和macOS。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的產品名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileOriginalname	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的原始檔案名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileProductvendor	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的公司名稱值。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileDescription	string	當前進程的實際發起進程檔案的VERSIONINFO資源中的描述。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignResult	string	當前進程的實際發起進程的可執行檔的簽名驗證結果：通過-true，否則-false。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignTimestamp	int	檔案（當前流程的實際發起者）簽署的日期和時間。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessFileSignSubjectname	string	用於簽署當前進程的實際發起進程檔案的憑證的主題名稱。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonType	string	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessLogonSessionId	int	當前進程的實際發起進程的存取權杖中的登入會話ID。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessProperties	int	當前進程的實際發起者的登入會話類型。通常，“ParentProcess”與“CreatorProcess”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段
CreatorProcessUserName	string	當前進程的實際發起者的網域名稱和使用者名稱。通常情況下，“父進程”與“創建者進程”相同。此時，遙測資料中將缺少CreatorProcess*字段，需要查看ParentProcess*字段

事件的細粒度存取

在KUMA中，擁有不同權限的使用者可以對事件進行細粒度的存取控制。事件的存取權限在儲存空間層級進行控制。

您可以在**空間權限**部分為使用者指派空間。升級到最新版本後，「所有空間」空間集將指派給所有現有使用者，即所有空間的存取均不受限制。事件包含租用戶ID和容器ID，因此使用者需要擁有對應租用戶和容器的權限才能存取該事件。

顯示儲存體時，請考量以下特性：

- 如果儲存體未列在**活動服務**部分，則該儲存體及其空間不會顯示在空間集清單中。
- 若儲存服務是透過 `systemctl stop kuma-<storage ID>` 命令停止，該儲存體及其空間將不會顯示於空間集的空間清單中。
- 若儲存體啟動後透過 `uninstall` 命令刪除，該儲存體及其空間仍會保留於空間集的空間清單中。

在事件清單中，您可以向表中新增**SpaceID**欄位，該欄位將顯示空間名稱。稽核事件的空間顯示為「KUMA稽核」。「KUMA預設」是每個儲存體中的預設空間，如果儲存體未設定空間或事件不符合現有空間的條件，則所有事件都會進入該空間。

將事件清單匯出到TSV檔案時，空間ID和名稱會顯示出來。

若要區分存取權限：

1. 設定空間集。

   您可以建立、編輯或刪除空間集。這些操作會導致稽核事件。

2. 設定空間集的存取權限。您可以授予或撤銷所選使用者的存取權限。

建立空間集

若要建立空間集：

1. 在 KUMA 網頁主控台中，前往**設定 → 存取 → 空間存取權**區段。
2. 在開啟的視窗中，按一下**新增**按鈕。
3. 在**建立空間集合**視窗中，設定下列項目：

   a. 在**名稱**欄位中，指定空間集名稱。最多可以使用128個Unicode字元。

   b. 在**空間**下拉清單中，選取空間名稱旁的核取方塊，即可選擇要包含在集合中的空間。若要從集合中刪除空格，請清除核取方塊。

   c. 如果您希望預設空間集對所有未指派任何空間集的使用者可用，請選取**設為預設值**核取方塊。

   這使得建立的集合成為預設集合。在空間集清單中，它被標記為預設集：在**預設**直欄中，其值為**是**。

   只能有一個預設集。如果在其他集合的設定中選取**設為預設值**核取方塊並儲存設定，則預設集將重新指派。

4. 點擊**建立**。

空間集隨即建立並顯示在空間清單。建立空間集後，KUMA 會產生稽核事件。

然後，您需要授予使用者對已建立空間集的存取權限。

編輯空間集

若要編輯空間集：

1. 在 KUMA 網頁主控台中，前往**設定 → 存取 → 空間存取權**區段。
2. 在開啟的視窗中，點擊一個空間集。

3. 在**編輯空間集合**視窗中，設定以下項目：

   a. 在**名稱**欄位中，指定空間集名稱。最多可以使用128個Unicode字元。

   b. 在**空間**下拉清單中，選取空間名稱旁的核取方塊，即可選擇要包含在集合中的空間。若要從集合中刪除空格，請清除核取方塊。

   c. 如果您希望預設空間集對所有未指派任何空間集的使用者可用，請選取**設為預設值**核取方塊。

   這樣，儲存變更時，該集合將成為預設集。在空間集清單中，它被標記為預設集：在**預設**直欄中，其值為**是**。

   只能有一個預設集。如果在其他集合的設定中選取**設為預設值**核取方塊並儲存設定，則預設集將重新指派。

4. 按一下**儲存**。

空間集隨即儲存並顯示在空間清單中。

現在所有可以存取原始空間集的使用者都可以存取編輯後的空間集。您可以使用**存取控制**按鈕來控制對已編輯空間集的存取，並授予或撤銷存取權限。

刪除空間集

若要刪除空間集：

1. 在 KUMA 網頁主控台中，前往**設定 → 存取 → 空間存取權**區段。

2. 在**空間存取權**視窗中，選取相關空間集旁的核取方塊。

   如果要刪除所有空間集，請選取清單左上角的**全選**核取方塊，然後按一下**刪除**。

   > 您無法刪除預設空間集和「所有空間」空間集。

3. 點擊**刪除**。

空間集隨即刪除並從空間清單中移除。刪除空間集後，KUMA 會產生稽核事件。

如果使用者只能存取已刪除的空間集，無法存取任何其他空間集，該使用者會自動取得預設空間集的存取權限。

授予對空間集的存取權限

若要授予對空間集的存取權限

1. 在 KUMA 網頁主控台中，前往**設定 → 存取 → 空間存取權**區段。

2. 請在清單中選取空間集旁的核取方塊，然後按一下工具列上的**存取控制**按鈕。

3. 這將開啟**使用者**視窗；在該視窗中，按一下**新增使用者** 。

4. 在**新增使用者**視窗的清單中，選擇要授予空間集存取權限的用戶，然後按一下**新增**。

   如果要授予所有使用者對所選空間集的存取權限，請選取左上角的核取方塊，然後選擇下列選項之一： **在頁面中全選**或**全選** ，然後按一下**新增**。

這將打開一個確認視窗。

5. 若要授予所列使用者存取權限，請在確認視窗中按一下**確認**。

使用者現在擁有對空間集的存取權限。

撤銷對空間集的存取權限

撤銷空間集存取權限

1. 在 KUMA 網頁主控台中，前往**設定** → **空間存取權**區段。
2. 請在清單中選取空間集旁的核取方塊，然後按一下工具列上的**存取控制**按鈕。
3. 這將開啟**使用者**視窗；在該視窗中，選取使用者的核取方塊以選擇使用者，然後按一下**刪除**。

   若要撤銷所有使用者對所選空間集的存取權限，請選取左上角的核取方塊，然後選擇下列選項之一： **在頁面中全選**或**全選**，然後按一下**刪除**。

   這將打開一個確認視窗。
4. 若要撤銷所列使用者的存取權限，請在確認視窗中按一下**確認**。

這些使用者將不再擁有對該空間集的存取權限。

如果使用者沒有對任何其他空間集的存取權限，則該使用者將自動獲得對預設空間集的存取權限。

使用案例

遷移到具有差異化事件存取權限的KUMA最新版

目標：更新產品。

操作：管理員將KUMA更新到4.0版本。

結果：使用者的事件存取權限不變；所有使用者都可以存取那些允許使用者檢視事件清單的租用戶中的事件。在新增使用者、租用戶或空間時，所有使用者都可以查看租用戶的事件，這取決於他們是否被允許檢視事件清單，沒有其他限制。

限制所有使用者對空間的存取權限

目標：某些使用者必須無法存取安裝中的某些空間。現有使用者和新使用者都不得存取此類空間。

操作：管理員建立一個新的空間集，其中包含所有使用者都必須擁有存取權限的空間。每個空間被指定為元組：clusterID、tenantID、spaceID。這樣，就可以從有限數量的空間中建構一個空間集。建立集合後，管理員會將該集合設定為預設集合。

結果：對於所有未明確指定此空間集的使用者（包括新使用者），事件存取權限將根據預設空間集受到額外限制。也就是說，此類使用者可以存取其有權檢視事件清單的租用戶中的事件，以及預設空間集中包含的空間中的事件。

允許部分使用者檢視所有事件

目標：KUMA有一個預設空間集，其中僅明確指定了有限數量的空間。此外，KUMA中的某些使用者必須擁有對所有事件的無限制存取權限。您希望允許這些使用者檢視未在預設空間集中指定的空間中的事件。

操作：管理員前往**空間存取權**區段，選取「所有空間」空間集。此空間集可讓使用者不受限制地存取所有空間，管理員並將其存取權限授予選取的使用者。

結果：已明確取得「所有空間」空間集存取權限的使用者，現在可以不受限制地存取空間中的事件。他們對事件的存取權限僅取決於其根據指派的角色所擁有的檢視事件清單的權限。新增空間或租用戶後，這些使用者將可以存取位於這些新空間和租用戶中的活動，前提是他們擁有檢視相應租用戶活動清單的權限。未明確取得「所有空間」空間集存取權限的使用者，其事件存取權限將根據預設空間集受到限制。

允許部分使用者檢視有限空間集中的事件

目標：KUMA有一個預設空間集，其中僅明確指定了有限數量的空間。部分使用者需要查看不同的空間集，但並非所有可用空間。

操作：管理員建立一個包含相關空間的空間集，並授予選取使用者對該空間集的存取權限。

結果：使用者對事件的存取權限將根據可用空間集進行限制。未被明確授予存取權限的用戶，其對事件的存取權限將根據預設空間集進行限制。

為使用者補充明確指定的空間集

目標：使用者u1、u2、u3和u4已明確授予空間集「set1」的存取權限，該空間集包含Windows和Linux事件所在的空間。除了Windows和Linux事件外，使用者u1和u2還需要檢視傳送到各自空間的Cisco和VMware事件。

操作：管理員建立一個空間集「set2」，其中包含Cisco和VMware事件所在的空間。除了set1之外，管理員還將set2指派給u1和u2。

結果：使用者u1和u2現在可以存取所有可用集合中的事件，即來自set1和set2的事件：Windows、Linux、Cisco和VMware。使用者u3和u4對事件的存取權限保持不變。

編輯空間集

目標：部分使用者擁有對某個空間集的存取權限（存取權限已明確授予或該空間集為預設空間集）。對於所有這些用戶，您需要新增對某個不在該空間集中的特定空間的存取權限，或撤銷對某個已在該空間集中的空間的存取權限。

操作：管理員透過新增或刪除相關空間來編輯現有的空間集。

結果：所有擁有該空間集存取權限的使用者現在都可以根據更新後的空間集檢視事件。

刪除空間集

目標：此空間集不再相關，需要從KUMA中刪除。

操作：管理員刪除現有的空間集。「所有空間」空間集不能刪除。預設空間集不能刪除。

結果：已刪除的空間集已從KUMA中移除。所有已明確授予此空間集存取許可權的使用者現在都可以根據仍然可用的空間集存取事件。如果使用者沒有任何已明確授予存取權限的空間集，則該使用者對事件的存取權限將由預設空間集控制。

檢視事件表

事件表為您提供了KUMA Core從資料來源接收的所有事件的概覽。此表顯示依據執行的SQL查詢篩選的事件清單。

若要檢視事件表，請執行以下操作：

1. 在主功能表中，轉至**監控 → 威脅搜尋**。
2. 如有需要，請篩選租用戶。預設情況下，租用戶篩選器處於停用狀態，事件表顯示與您具有**讀取**存取權限的所有租用戶相關的事件。若要套用租用戶篩選器：
   a. 按一下**租用戶篩選器**設定旁邊的連結。
      租用戶篩選器隨即開啟。
   b. 選取所需事件旁邊的核取方塊。
      事件表僅顯示與選定的租用戶相關的事件。

隨即顯示事件表。有關表列的詳細資訊，請參閱標準化事件資料模型。

搜尋和篩選事件

執行事件搜尋時，對於手動執行的查詢，系統會產生稽核事件。

對於由儀表板、報告或資料收集和分析規則發起的查詢，系統不會產生稽核事件。用於接收事件的REST API請求也不會產生稽核事件。

使用GROUP BY選項時，展開分組會觸發稽核事件的創建，因為此時會執行額外的查詢。

選擇**在後台執行**選項後，會產生兩個稽核事件：事件讀取嘗試和搜尋查詢已取消。

若要搜尋和篩選事件，請在搜尋欄位中修改SQL查詢，然後按一下**執行查詢**按鈕。您可以手動輸入SQL查詢，也可以使用查詢建構器產生它。

SQL查詢支援資料彙總和分組。

您可以在用於檢視統計資料的視窗、事件表和事件詳細資訊區域為已產生的SQL查詢新增篩選條件。

若要在統計資料視窗中變更篩選設定

1. 請依照下列步驟開啟事件表。
2. 使用以下方法之一開啟**威脅統計資訊**詳細資訊區域：
   - 按一下事件表右上角的**⋯**按鈕，然後選擇**威脅統計資訊**。
   - 在事件表中，按一下任意值，然後在開啟的快顯功能表中選擇**威脅統計資訊**。

   威脅統計資訊詳細資訊區域出現在Web介面視窗的右側。
3. 開啟相關參數的下拉清單，將滑鼠遊標停留在必要的值上。

4. 透過執行下列操作之一來變更篩選器設定：

   - 若要僅包含具有選取值的事件，請按一下 ＋ 按鈕。
   - 若要排除所有具有選取值的事件，請按一下 － 按鈕。

若要變更事件表中的篩選設定

1. 請依照下列步驟開啟事件表。
2. 按一下事件表中的事件參數值。
3. 在開啟的功能表中，選擇以下選項之一：

   - 若要僅顯示具有選定值的事件，請選擇**按此值篩選**。
   - 若要從表格中排除具有選定值的所有事件，請選擇**從篩選器中排除**。

若要在事件詳細資訊區域中變更篩選器設定

1. 請依照下列步驟開啟事件表。
2. 按一下相關事件以喚起事件詳細資訊窗格。
3. 透過執行下列操作之一來變更篩選器設定：

   - 若要僅包含具有選取值的事件，請按一下 ＋ 按鈕。
   - 若要排除所有具有選取值的事件，請按一下 － 按鈕。

因此，篩選器設定和事件表就會更新，新的搜尋查詢會顯示在螢幕上方。

> 切換到使用建構器時，在搜尋欄位中手動輸入的查詢參數不會傳輸到建構器，因此您需要重新建立查詢。在建構器中建立的查詢不會覆蓋在搜尋字串中輸入的查詢，直到您點選建構器視窗中的**套用**按鈕。

點選 按鈕儲存目前篩選器。

手動建立SQL查詢

您可以使用搜尋字串手動建立任何複雜度的SQL查詢來篩選事件。

執行SQL查詢會影響顯示的表格列。

如果SQL查詢包含*值，則查詢中指定的列（如果不存在）將會新增至表中。從後續查詢中刪除顯示的列不會隱藏對應的列。

如果SQL查詢不包含*值，則表格僅顯示符合標準化事件資料模式的指定欄位的列。即使沒有資料，也會顯示列。

若要手動產生SQL查詢：

1. 請依照下列步驟開啟事件表。
2. 在輸入欄位中輸入您的SQL查詢。

   在SQL查詢欄位中輸入函式名稱時，會顯示可用函式清單。選取函式會在右側顯示使用範例。例如，`concatWithSeparator` 函式會隨附下列範例：

   ```
   concatWithSeparator('a', '1', '2', '3')
   ```

3. 點擊**執行查詢**按鈕。

   查詢最多可能需要數分鐘才能完成。

   您也可以在後台執行查詢。若要這麼做，請按一下**執行查詢**按鈕旁的箭頭圖示，然後選取**在背景執行**。在這種情況下，會發生以下情況：

   - 查詢會排入佇列以在背景執行，並在**偵測與回應**區段中建立用於執行此查詢的工作。
   - 後台查詢以低優先等級並行執行。
   - 包含超過10,000個事件的查詢無法排入後台執行佇列。

   表格將根據產生的SQL查詢顯示搜尋結果。您可以在**偵測和回應**部分檢視後台執行查詢的結果。

   如有必要，您可以透過點擊**執行查詢**按鈕旁的箭頭圖示並選擇**取消查詢**來取消後台查詢的執行。查詢取消時，會自動產生稽核事件。

   如有需要，您可以依期間篩選表格中的事件。

若要在SQL查詢欄位中顯示不可列印字元，請按下下列任一組合鍵：

- **Ctrl+*/Command+***
- **Ctrl+Shift+8/Command+Shift+8**

如果您在XDR元件中啟用不可列印字元的顯示，則其他元件（例如KUMA）不會自動顯示不可列印字元，直到您重新載入元件的瀏覽器頁籤。

支援的函式和運算子

SELECT

應傳回的事件欄位。

對於**SELECT**欄位，程式支援以下函式和運算子：

彙總函式：**count**, **avg**, **max**, **min**, **sum**。

算術運算子：**+, -, *, /, <, >, =, !=, >=, <=**。

您可以組合使用這些函式和運算子。

如果在查詢中使用彙總函式，則無法自訂事件表顯示，按升序或降序對事件進行排序或接收統計資料。

從

資料來源。

WHERE

篩選事件的條件。

- **AND, OR, NOT, =, !=, >, >=, <, <=**
- **IN**
- **BETWEEN**
- **LIKE**
- **ILIKE**
- **inSubnet**
- **符合**（查詢中使用正規表示式的 re2 語法；特殊字元必須以「\」逸出）

分組方式

用於對傳回資料進行分組的事件欄位或別名。

如果您在查詢中使用資料分組，則無法自訂事件表顯示，按升序或降序對事件進行排序，接收統計資料或執行回顧性掃描。

排序方式

用於對傳回資料進行排序的欄位。

可能的值：

- **DESC**—降序。
- **ASC**—升序。

OFFSET

在列印查詢結果輸出之前跳過指定的行數。

LIMIT

表格中可顯示的列數。

預設值是 250。

切換至查詢建構器時，手動輸入搜尋字串的查詢參數不會轉移至建構器，因此您需要重新建立查詢。此外，在建構器中建立的查詢不會覆寫輸入到搜尋字串中的查詢，直到您點選建構器視窗中的套用按鈕。

別名不能包含空格。

查詢範例：

- **SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有具有**基本**和**稽核**類型的事件都按**時間戳**列降序排列。表中可以顯示的字串數為250。

- **SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250**

  事件表中所有**BytesIn**欄位包含接收流量值在1,000到2,000位元組範圍內的事件都按**时间戳**升序排列。表中可以顯示的字串數為250。

- **SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有**訊息**欄位包含與定義的%ssh:%小寫範本對應的資料的事件均依**時間戳記**列降序排序。表中可以顯示的字串數為250。

- **SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有位於00.0.0.0/00子網路中的主機的事件均依**時間戳**列降序排序。表中可以顯示的字串數為250。

- **SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250**

  在事件表中，所有**訊息**欄位包含與ssh.*範本對應的文本的事件均依**時間戳**列降序排列。表中可以顯示的字串數為250。

- **SELECT max(BytesOut) / 1024 FROM `events`**

  指定時間段內的最大出站流量（KB）。

- **SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250**

  事件數量和連接埠號碼。事件依連接埠號碼分組，並依**連接埠**列升序排列。表中可以顯示的字串數為250。

  事件表中的**ID**列名為Count，**SourcePort**欄位名為Port。

- **SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250**

  如果要在查詢中使用特殊字元，您需要透過在字元前面放置一個反斜槓（\）字元來轉義此字元。

  在事件表中，所有**訊息**欄位包含與ssh: 'connection'範本對應的文本的事件均依**時間戳記**列降序排列。表中可以顯示的字串數為250。

使用建構器產生SQL查詢

您可以使用查詢建構器產生用於篩選事件的SQL查詢。

執行SQL查詢會影響顯示的表格列。

如果SQL查詢包含*值，則查詢中指定的列（如果不存在）將會新增至表中。從後續查詢中刪除顯示的列不會隱藏對應的列。

如果SQL查詢不包含*值，則表格僅顯示符合標準化事件資料模式的指定欄位的列。即使沒有資料，也會顯示列。

若要使用建構器產生SQL查詢：

1. 請依照下列步驟開啟事件表。
2. 點選 按鈕開啟查詢建構器。

   透過在以下參數區塊中提供資料來產生搜尋查詢：

   - **SELECT**

     應傳回的事件欄位。預設選擇*值，這表示必須傳回所有可用的事件欄位。若要調整顯示的欄位，請在下拉清單中選擇所需的欄位。請注意，選擇*會增加請求執行的持續時間，但無需在請求中指定欄位。

     選擇事件欄位時，您可以使用下拉清單右側的欄位為顯示的資料列指定別名，並且可以使用最右邊的下拉清單選擇要對資料執行的操作：**count**, **max**, **min**, **avg**, **sum**。

   - **從**

     資料來源。選擇**事件**值。

   - **WHERE**

     篩選事件的條件。

     若要新增篩選條件和群組，請點選**新增篩選條件**和**新增篩選群組**按鈕。預設情況下，條件群組中的**AND**運算子值處於選取狀態。點選運算子值即可變更。可用值： **AND** 、 **OR** 、 **NOT** 。

     若要變更篩選條件和篩選條件群組的結構，請使用 圖示拖放運算式。

     若要新增篩選條件：

     a. 在左側的下拉清單中，選擇要用於篩選的事件欄位。

     b. 從中間的下拉清單中選擇必要的運算子。可用的運算子取決於所選事件欄位的值類型。

     c. 輸入篩選條件的值。根據所選欄位的類型，您可能需要手動輸入值，從下拉清單中選擇值或在日曆上選擇值。

     若要刪除篩選條件，請點選**X**按鈕。若要刪除篩選群組，請按一下**刪除群組**按鈕。

   - **分組方式**

     用於對傳回資料進行分組的事件欄位或別名。

     如果您在查詢中使用資料分組，則無法自訂事件表顯示，按升序或降序對事件進行排序，接收統計資料或執行回顧性掃描。

- **排序方式**

  用於對傳回資料進行排序的欄位。在右側的下拉式清單中，您可以選擇所需的排序順序：**DESC**—降冪，**ASC**—升冪。

- **限制**

  表格中可顯示的列數。

  預設值是250。

  如果您按使用者定義的時間段篩選事件，且搜尋結果中的字串數量超出了定義值，則可以點擊**顯示後續記錄**按鈕以在表中顯示更多字串。依標準時段篩選事件時，不會顯示此按鈕。

3. 點選**套用**。

   目前的SQL查詢將被覆蓋。產生的SQL查詢將顯示在搜尋欄位中。

   若要重設建構器設定，請點選**預設查詢**按鈕。

   若要關閉建構器而不覆蓋現有查詢，請點選 按鈕。

4. 按一下**執行查詢**按鈕以顯示表格中的資料。

   查詢最多可能需要數分鐘才能完成。

   您也可以在後台執行查詢。若要這麼做，請按一下**執行查詢**按鈕旁的箭頭圖示，然後選取**在背景執行**。在這種情況下，會發生以下情況：

   - 查詢會排入佇列以在背景執行，並在**偵測與回應**區段中建立用於執行此查詢的工作。
   - 後台查詢以低優先等級並行執行。
   - 包含超過10,000個事件的查詢無法排入後台執行佇列。

   表格將根據產生的SQL查詢顯示搜尋結果。您可以在**偵測和回應**部分檢視後台執行查詢的結果。

   如有必要，您可以透過點擊**執行查詢**按鈕旁的箭頭圖示並選擇**取消查詢**來取消後台查詢的執行。查詢取消時，會自動產生稽核事件。

切換到網頁介面的另一個部分時，建構器中產生的查詢不會保留。如果從另一個部分返回事件部分，則建構器將顯示預設查詢。

使用 KUMA SQL 函數產生 SQL 查詢

KUMA 的 SQL 函數可在搜尋查詢中使用資產和帳戶的屬性，以篩選事件、產生報告和小工具（圖表類型：**表格**）。您可以使用下列函數集，透過字典、表格、資產和帳戶中的資料擴充事件：

- enrich 函數集。可使用資產或帳戶的欄位、**字典**類型字典中的值，或**表格**類型字典中的值擴充查詢結果。`enrich` 函數集包含下列函數：
  - `enrich_assets`；
  - `enrich_accounts`；

- `enrich_table`；
- `enrich_dictionary`。

- lookup 函數集。可將資產和帳戶的條件新增至搜尋查詢。`lookup` 函數集包含下列函數：
  - `lookup_assets`；
  - `lookup_accounts`；
  - `lookup_assets_category`。

每個查詢最多可包含 10,000 個事件。

在 SQL 查詢中使用「enrich」函數集

`enrich` 函數集（請參閱下表）用於 SQL 查詢的 `SELECT` 子句，以擴充結果。

使用此函數集時，無法依擴充欄位將事件分組。

透過這些函數擴充的小工具和報告最多只能屬於一個租用戶。

SQL 查詢中指定的資產欄位值區分大小寫。

「enrich」函數集的描述

功能	事件欄位	資產欄位	描述
enrich_assets	DeviceAssetID DestinationAssetID SourceAssetID	name os osBuild ipAddress macAddress fqdn source software cii ramSize kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart kscStatusMask kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus lastVisible aistatus aiscore	根據傳遞給函數的指定 ID，以資產欄位擴充查詢結果。 範例 `enrich_assets(DeviceAssetID, name)`
enrich_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name uac	根據傳遞至函式的指定 ID，以帳戶欄位擴充查詢結果。 範例 `enrich_account(SourceAccountID, name)` 此功能僅適用於已啟用 LDAP 擴充的租用戶。

功能	事件欄位	資產欄位	描述
enrich_table	任何	–	根據 ClickHouse 叢集回應中的事件欄位，使用**資料表**類型字典中的值擴充查詢結果。 範例 enrich_table('Main/some-table', [DeviceProduct], 'value') 資料表只能有一個欄位作為金鑰，但記錄金鑰可以是複合金鑰。 範例 enrich_table('Main/Dictionary', [BytesOut|BytesIn], 'value2') enrich_table 函式只會傳回資料表中的一個欄位。若需要呼叫更多欄位，請再次呼叫函式並指定相關欄位。
enrich_dictionary	任何	–	根據 ClickHouse 叢集回應中的事件欄位，使用「**字典**」類型字典中的值擴充查詢結果。 例子 1 enrich_dictionary('Main/some-dict', [SourceAddress] 例子 2 enrich_dictionary('Main/some-dict', [SourceAddress, DeviceAddress]) 您可以在「**資源**」→「**字典**」區段中檢視字典的路徑。

手動建立 SQL 查詢時，您可以指定 enrich 函式。

使用 enrich 函式的查詢範例

取得 events 資料表的所有事件及其 Name 和 Message 欄位，並加入 macAddress 和 osBuild 資產欄位，以使用資產資料擴充結果。資料表中可顯示的資料列數為 250。

```
SELECT Name,
Message,
   enrich_assets(DeviceAssetID, macAddress),
   enrich_assets(DeviceAssetID, osBuild)
FROM `events`
WHERE DeviceAssetID != ''
LIMIT 250
```

events 資料表中的所有事件，包含事件欄位 SourceUserName 和 SourceAddress，以及用於以帳戶資料擴充結果的 mobile 欄位值。資料表中可顯示的資料列數為 10。

```
SELECT SourceUserName,
SourceAddress,
   enrich_accounts(SourceAccountID, mobile) as mobile
FROM `events`
WHERE SourceAccountID != ''
LIMIT 10
```

events 資料表中的所有事件，其中 DeviceProduct 事件欄位的值來自 **Main/[OOTB] Linux.Auditd 記錄類型**。依 **時間戳記** 降冪排序。資料表中可顯示的資料列數為 1000。

```
SELECT DeviceProduct,
   enrich_table('Main/[OOTB] Linux&period; Auditd record types', [DeviceProduct], 'Description') as HTTP
FROM `events` WHERE Type!=4
LIMIT 1000
```

`events` 資料表中所有 `DeviceAction` 事件欄位值來自 **Main/[OOTB] KEDR** 字典的事件。資料表中可顯示的資料列數為 250。

```
SELECT DeviceAction,
   enrich_dictionary('Main/[OOTB] KEDR&period; AccountType', [BytesOut]) as accountType
FROM `events` WHERE Type!=4
LIMIT 255
```

在 SQL 查詢中使用「lookup」函數集

`lookup` 函數集（請參閱下表）用於 SQL 查詢的 `WHERE` 子句，以便在搜尋查詢中新增資產和帳戶的條件。

在包含 `lookup` 函數的查詢中，KUMA 會自動將查詢內 `lookup` 函數所使用的 `*ID` 欄位新增至 `SELECT` 子句。例如，在包含 `lookup_assets(DeviceAssetID, osBuild, '=', '19045.000000')` 函數的查詢中，`DeviceAssetID` 欄位會新增至 `SELECT` 子句。

在包含 `lookup` 函數的查詢中，我們建議在 `SELECT` 子句中指定要傳回的欄位清單。我們不建議在 `SELECT` 子句中使用 `*`。這會傳回所有可用欄位，可能會大幅延長查詢的處理時間。

「lookup」函數集的描述

函數類型	事件欄位	資產欄位	運算子	描述
lookup_assets	DeviceAssetID SourceAssetID DestinationAssetID	name os osBuild source cii ramSize kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus aistatus aiscore	=	允許您為欄位值與查詢中指定 增查詢結果條件。 對於數值，您必須指定包含所 例如： lookup_assets(DeviceAss '=', '19045.000000') lookup_assets(DeviceAss '=', '3241234234')
		kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart lastVisible ramSize aiscore	< > <= >=	允許您為欄位值符合以下條件 件： • 小於查詢中指定的值 • 大於查詢中指定的值 • 小於或等於查詢中指定的 • 大於或等於查詢中指定的 對於數值，您必須指定包含所 例如： lookup_assets(DeviceAss '>', '50') 日期值可以使用以下格式指定 • 秒數： lookup_assets(Device lastVisible, '>', '1 • 毫秒數： lookup_assets(Device lastVisible, '<', '1725971837834') • 天數： lookup_assets(Device lastVisible, '<', 'n
		name os osBuild fqdn software	like	可讓您針對欄位值符合查詢中 算式的資產，為查詢結果新增 如需 LIKE 操作員的詳細資訊 言運算式 參考資料。 lookup_assets(Destinati name, 'like','test.compa
		ipAddress macAddress fqdn software kscStatusMask	in	可讓您將值與查詢中指定值相 增至結果中。 例如： lookup_assets(DeviceAss 'in', ['test_fqdn1.compa 'test_fqdn2.company.ru'
		ipAddress	insubnet	可讓您新增條件，以搜尋 IP 位 路中的資產。IP 位址以 CIDR 例如： lookup_assets(DeviceAss ipAddress, 'insubnet',

函數類型	事件欄位	資產欄位	運算子	描述
		ipAddress	inrange	可讓您新增條件，以搜尋 IP 位內的資產。 查詢中指定的第一個 IP 位址是第二個則是結束 IP 位址。 例如： `lookup_assets(DeviceAss ipAddress, 'inrange', [ '192.168.1.184'])` 此查詢會篩選出 IP 位址介於 1 192.168.1.184 範圍內的資產。

函數類型	事件欄位	資產欄位	運算子	描述
lookup_accounts	SourceAccountID DestinationAccountID	name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn title division department manager location company street_address physical_delivery_office_name uac	=	可讓您為查詢結果新增條件，查詢中指定值相符的帳戶。 對於數值，您必須指定包含所 例如： lookup_accounts(SourceA employee_id, '=', '1545
		name guid domain cn dn employee_id email mail_nickname mobile sid sam_name telephone_number principal_name sn type title division department manager location company street_address physical_delivery_office_name	like	可讓您為查詢結果新增條件，符合查詢中所指定「like」運算 如需 LIKE 操作員的詳細資訊 言運算式參考資料。 lookup_accounts(Destina name, 'like', '_ccount1

函數類型	事件欄位	資產欄位	運算子	描述
lookup_assets_category	DeviceAssetID SourceAssetID DestinationAssetID	–	–	尋找所有具有位於指定資料夾事件。 例如： `lookup_assets_category(['Main/Business Impact']` 其中 `Main` 是租用戶的名稱，`Impact` 是資料夾的名稱。

使用 lookup 函式的 SQL 查詢範例

您可以在手動建立 SQL 查詢時指定 `lookup` 函式。使用 `lookup` 函式的查詢範例

- 「events」資料表中包含 `TenantID` 和 `DeviceProduct` 事件欄位以及 `fqdn` 資產欄位的所有事件，其中資產欄位的值包含 win10 子字串。資料表中可顯示的資料列數為 250。

```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets(DeviceAssetID, fqdn, 'match', 'win10')
LIMIT 250
```

- 「events」資料表中包含 `TenantID` 和 `DeviceProduct` 事件欄位的所有事件，以及 `the EmployeeID` 欄位值為 `15452.` 的所有事件。資料表中可顯示的資料列數為 10。

```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE SourceAccountID != ''
AND lookup_accounts(SourceAccountID, employee_id, '=', '15452')
LIMIT 10
```

- 「events」資料表中包含 `TenantID` 和 `DeviceProduct` 事件欄位的所有事件，以及資產所在的資料夾。資料表中可顯示的資料列數為 100。

```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets_category(DeviceAssetID, ['Main/Business Impact'])
LIMIT 100
```

檢視事件詳情

若要開啟事件詳情窗格，請在**威脅搜尋**部分的事件表中或警示詳情頁面中選擇事件。

事件詳細資訊窗格顯示在網頁介面視窗的右側，其中包含事件參數及其值的清單。在此區域中，您可以：

- 按一下參數值旁的＋或－，將選取的欄位包含在搜尋中，或將其從搜尋中排除。
- 透過點選**FileHash**和**DeviceCustomString**值，尋找相似事件並新增或刪除防護規則。
- 與Kaspersky CyberTrace和Kaspersky Threat Intelligence Portal整合時，您可以透過點選**FileHash**和**DeviceCustomString**值新增至CyberTrace的內部TI並顯示來自威脅查詢的資訊。
- 透過點選**服務**值檢視註冊事件的服務的設定。
- 透過點擊**DeviceAssetID**值並選擇**資產詳細資訊**，檢視與裝置相關的警示或事件清單。在開啟的**裝置詳情**視窗中，按一下**顯示相關**按鈕，然後根據要檢視的內容選擇**警示**或**事件**。
- 檢視事件建立時觸發的IOA規則清單；按一下規則名稱即可檢視這些IOA規則的詳細資訊。

  開啟的IOA 規則窗格會顯示詳細資訊。

  在開啟的IOA規則詳細資料中，您可以執行以下操作：

  - 查看IOA規則名稱、ID、嚴重等級和置信度等級。
  - 將IOA規則新增至排除項。

- 按一下**在 Kaspersky TIP 中尋找**按鈕以查看搜尋資訊；
- 按一下**檢視於**按鈕，查看觸發IOA規則時所建立的警示和事件。
- 按一下**在威脅搜尋中尋找**按鈕以查看相關事件。

  事件的預設顯示時間間隔為24小時。

  您也可以在Kaspersky TIP中查看IOA規則的詳細資訊。為此，請在IOA規則詳細資料視窗中，按一下**在 Kaspersky TIP 中尋找**按鈕。

- 按一下 圖示並將切換開關移至所需位置，即可啟用或停用 `*Label` 欄位的精簡顯示模式。預設情況下，切換開關位於**完整視圖**位置。為 `DeviceCustom*` 和 `Flex*` 欄位選取**精簡檢視畫面**模式時，對應 `*Label` 欄位的值會顯示為欄位名稱，而 `*Label` 欄位本身則會從事件欄位清單中隱藏。如果缺少 `*Label` 欄位值，則會顯示原始欄位名稱。重新整理頁面並離開**威脅搜尋**區段後，仍會保留所選的顯示模式。

在**事件詳細資訊**窗格中，以下設定的值中顯示的是所描述物件的名稱，而不是其ID。如果您從**事件詳細資訊**窗格更改篩選器設定，則會將物件的ID（而不是其名稱）新增到SQL查詢中：

- TenantID
- SeriviceID
- DeviceAssetID
- SourceAssetID
- DestinationAssetID
- SourceAccountID
- DestinationAccountID

儲存和選取事件篩選器組態

您可以儲存目前的篩選器組態，包括基於時間的篩選器、查詢建構器和事件表設定，以供將來使用。已儲存的篩選器組態可供您和其他具有相應存取權限的使用者使用。

若要儲存篩選器、查詢和時間段的目前設定

1. 請依照下列步驟開啟事件表。
2. 點選搜尋查詢旁的 圖示，然後選擇**儲存目前篩選器**。
3. 在開啟的**新篩選器**視窗中，在**名稱**欄位中輸入篩選器組態的名稱。名稱必須包含128個或更少的Unicode字元。
4. 在**租用戶**下拉清單中，選擇要為其儲存所建立篩選器的租用戶。
5. 按一下**儲存**按鈕。

   篩選器組態現已儲存。

若要選擇先前儲存的篩選器組態

1. 請依照下列步驟開啟事件表。
2. 點選搜尋查詢旁的 圖示，然後選擇所需的篩選器。

若要儲存篩選器、查詢和事件表設定的目前設定

1. 請依照下列步驟開啟事件表。
2. 點選事件表上方窗格中的齒輪圖示。
3. 點選**儲存目前預設**。
4. 在開啟的**新增預設**視窗中，在**名稱**欄位中輸入預設的名稱。名稱必須包含128個或更少的Unicode字元。
5. 在**租用戶**下拉清單中，選擇要為其儲存建立的預設的租用戶。
6. 按一下**儲存**按鈕。
   預設組態現已儲存。

若要選擇先前儲存的預設

1. 請依照下列步驟開啟事件表。
2. 點選事件表上方窗格中的齒輪圖示。選取**預設**頁籤。
3. 選擇所需的預設。

若要刪除所有使用者先前儲存的篩選器組態

1. 請依照下列步驟開啟事件表。
2. 點選搜尋查詢旁的 圖示。
3. 點選要刪除的組態旁的 圖示。
4. 點擊**"確定"**。

依期間篩選事件

您可以指定顯示事件的時間段。

若要依期間篩選事件：

1. 請依照下列步驟開啟事件表。
2. 開啟視窗上部的第二個下拉清單。
3. 指定時間範圍。您可以選擇相對於目前日期和時間的預定義範圍，也可以透過使用**範圍開始**和**範圍結束**欄位或在日曆中選擇日期來指定自訂範圍。
4. 點選**套用**。

匯出事件

您可以將事件資訊匯出到TSV檔案。將匯出到TSV檔案的事件分類取決於篩選器設定。資訊從事件表中顯示的直欄中匯出。即使由於SQL查詢的特殊功能，匯出檔案中的列未顯示在**威脅搜尋**部分的事件表中，它們也會填入可用資料。

若要匯出事件資訊：

1. 請依照下列步驟開啟事件表。
2. 點選事件表右上角的**•••**按鈕，然後選擇**匯出TSV**。

   新的匯出 TSV 檔案工作會建立在 KUMA 的 **工作管理器**區段中。
3. 在KUMA部分，找到您在**工作管理器**部分中建立的工作。
4. 按一下工作類型名稱，然後從下拉清單中選擇**上傳**。

   TSV檔案將使用您的瀏覽器設定下載。預設情況下，檔案名稱為event-export-<date>_<time>.tsv。

此檔案根據您的網頁瀏覽器設定儲存。

查看稽核事件和設定通知

稽核是一個監控、註冊和分析使用者操作和系統操作的進程，旨在確保更改的安全性和可追溯性。

Kaspersky Next XDR Expert會自動從解決方案元件中收集稽核事件，無需額外設定。在解決方案部署期間，Kaspersky Next XDR Expert會在根租用戶中建立一個預先定義的收集器**[OOTB]Kaspersky OSMP**。此收集器關聯了一個預先定義的連接器**[OOTB] Kaspersky OSMP**和關聯的預先定義規範化器**[OOTB] Kaspersky OSMP稽核**。收集器將稽核事件傳送至**KUMA稽核**儲存空間。此儲存空間會自動建立。

僅當您在單節點部署、多節點部署期間，或在解決方案介面中，於`license`參數中為SIEM元件指定有效的產品授權金鑰時，Kaspersky Next XDR Expert才會收集稽核事件。

如有必要，您可以在建立儲存資源集時配置稽核事件的儲存設定。

有關稽核事件的參數和操作類型的詳細資料，請參閱文章：稽核事件。

如何查看稽核事件並將其匯出到文件

稽核事件可在以下位置取得：**監控 →威脅搜尋**。

如果您希望事件表僅顯示稽核事件，請執行下列操作之一：

- 在事件表中，在**EventType**欄位中，設定`Audit`值。
- 透過稽核事件區分空間存取權限。

  為此，轉至**設定→KUMA→開啟KUMA設定→空間存取**，然後設定KUMA稽核空間的存取權限。只有被授予存取權限的使用者才能在**威脅搜尋**部分查看稽核事件。

在事件表中篩選稽核事件後，您可以將事件匯出到文件。

如何設定稽核事件的電子郵件通知

當發生特定事件時（例如，使用者嘗試登入OSMP主控台超過五次均失敗），系統會觸發預定義關聯規則並產生警示。

如果您希望接收警示的電子郵件通知，則必須建立通知範本。在**建立電子郵件範本**窗格中，指定下列參數：

- 在**事件類型**下拉清單中，選擇**建立新警示**通知範本類型。
- 在**關聯規則**下拉清單中，選擇預定義關聯規則。

稽核事件

稽核事件顯示在**威脅搜尋**部分，可能包括下表所列的操作類型。

操作類型	動作名稱	參數和描述
元件操作	`Service start`	

	Service stop	reason 服務中斷原因（如有）。
使用警示的操作	Alert assigning	• alert_id 執行操作的警示ID。 • group_name 被指派警示的群組名稱。 • group_id 被指派警示的群組ID。
	Changing alert status	• alert_id 執行操作的警示ID。 • alert_status 警示的先前狀態。 • new_alert_status 警示的新狀態：
	Alert auto assigning	• alert_id 執行操作的警示ID。 • account_name 被指派警示的使用者姓名。 • account_id 被指派警示的使用者ID。
使用事件的操作	Creating incident	incident_id 執行操作的事件ID。
	Incident assigning	• incident_id 執行操作的事件ID。 • group_name 被指派事件的群組名稱。 • group_id 被指派事件的群組ID。
	Changing incident status	• incident_id 執行操作的事件ID。 • incident_status 事件的先前狀態。 • new_incident_status 事件的新狀態。
	Merge incidents	incident_id 合併後的目標事件ID。
	Incident auto assigning	• incident_id 執行操作的事件ID。 • account_name 被指派事件的使用者名稱。 • account_id 被指派事件的使用者ID。
使用分段規則的操作	Creating segmentation rule	rule_name 分段規則的名稱。
	Changing segmentation rule	
	Enabling segmentation rule	
	Disabling segmentation rule	
	Deleting segmentation rule	
使用分段規則的操作	Creating aggregation rule	rule_name 彙總規則的名稱。
	Changing aggregation rule	
	Enabling aggregation rule	
	Disabling aggregation rule	
	Deleting aggregation rule	

電子郵件通知	Creating e-mail templates	subject 執行操作的電子郵件通知範本的主題。
	Enabling e-mail templates	
	Disabling e-mail template	
	Changing e-mail templates	
	Deleting e-mail templates	
設定	Enabling auto send to SB by IOA trigger	tenant_name 執行操作的租用戶名稱。
	Disabling auto send to SB by IOA trigger	
	Turning on the Assign "Untrusted" status to alerts toggle switch	
	Turning off the Assign "Untrusted" status to alerts toggle switch	
	Enabling the use of KSN	
	Disabling the use of KSN	
	Enabling the use of KPSN	
	Disabling the use of KPSN	
	Enabling the use of MDR	
	Disabling the use of MDR	
	Configuring the connection of OSMP to a local reputation database of KPSN	
	Enabling auto send to SB	
	Disabling auto send to SB	
	Enabling manual send to SB	
	Disabling manual send to SB	
	Selecting a database update source	
	Updating database manually	version_of_updated_databases 病毒資料庫的版本。
	Auto updating database	
	Changing passwords for archives	
	Enabling the required password change	
	Disabling the required password change	
	Enabling user password change	period 密碼必須更改的天數。
租戶管理	Creating tenant	tenant_name 租用戶的名稱。
	Changing tenant	
	Bind Administration Server	
	Changing integration KATA/KEDR	integration_parameters 整合設定。
	Changing integration TIP	
	Changing custom integration	

	Changing integration	
儲存庫	Uploading file to storage	• file_name 檔案名稱。 • alert_id 執行操作的事件ID。 • incident_id 執行操作的事件ID。
	Downloading file from storage	
	Deleting file from storage	
	Auto deleting file from storage	
設定	Configuring an IOC scan schedule	
阻止規則	Uploading prevention rules from file	• file_name 檔案名稱。 • count 匯入檔案後建立的阻止規則數量。
	Creating a prevention rule	file_name 檔案名稱。
	Modifying a prevention rule	
	Enabling the use of a prevention rule	
	Disabling the use of a prevention rule	
	Removing a prevention rule	
指令劇本	Creating a playbook	playbook_name 常規程式的名稱。
	Removing a playbook	
	Changing the operation mode	
YARA	Uploading a YARA file	file_name 檔案名稱。
	Downloading a YARA rule	rule_name YARA規則名稱。
	Changing YARA rule	
	Enabling the automatic use of YARA rules	
	Disabling the automatic use of YARA rules	
	Deleting a YARA rule	
IOC	Uploading an IOC file	file_name 檔案名稱。
	Downloading an IOC rule	rule_name IOC規則的名稱。
	Changing IOC rule	
	Enabling the automatic use of IOC rules	
	Disabling the automatic use of IOC rules	
	Deleting an IOC rule	
使用TLS憑證的操作	Generating a TLS certificate for the Endpoint Agent component	
	Uploading a TLS certificate for the Endpoint Agent component	
	Deleting a TLS certificate for the Endpoint Agent component	
	Downloading the TLS certificate of the server	

沙盒設定	OS set of virtual machines changed	sb_name 沙盒名稱。
	Creating a request for connection to the server with the Sandbox component	
	Enabling a connection with the Sandbox component	
	Disabling a connection with the Sandbox component	
	Deleting a connection with the Sandbox component	
	Renaming the Sandbox server	• new_sb_name 新沙盒名稱。 • sb_ip 沙盒IP位址。
沙盒規則	Creating a file scanning rule in custom images	virtual_machine_name 虛擬機器的名稱。
	Enabling a file scanning rule in custom images	
	Disabling a file scanning rule in custom images	
	Deleting a file scanning rule in custom images	
	Editing a file scanning rule in custom images	• virtual_machine_name 虛擬機器的名稱。 • new_virtual_machine_name 如果虛擬機器名稱已更改，則顯示虛擬機器的新名稱。
	Export a file scanning rule in custom images	file_name 檔案名稱。
	Import a file scanning rule in custom images	file_name 檔案名稱。
分散式解決方案	Assigning the PCN OSMP role	tenant_name 租用戶的名稱。
	Assigning the SCN OSMP role	
	Creating a request for connection of the SCN OSMP to the PCN OSMP	
	Accepting a request for connection of the SCN OSMP to the PCN OSMP	
	Rejecting a request for connection of the SCN OSMP to the PCN OSMP	
	Confirming the assign PCN role to CN	
	Disconnecting an SCN from PCN	
使用帳戶的操作	Creating a user account	• account_name 使用者名稱。 • account_id 使用者ID。 • account_authorization 執行操作的帳戶的上次登入日期和時間。 • password_verification 執行操作的帳戶的密碼驗證狀態。 • account_expiration_date 執行操作的帳戶的到期日。此值一律為 01.01.2222。 • account_status 執行操作的帳戶狀態。 • account_type 執行操作的帳戶類型。
	Changing access rights of user account	
	Change the password	
	Enabling account	
	Disabling account	
	Deleting an account	

使用者身分驗證和授權	登入成功	`administrator_rights` 指示使用者是否具有管理員權限。
	登入被拒絕，因為使用者未註冊	
	登入被拒絕，因為使用者被阻止了	
	登入被拒絕，因為密碼不正確	
	登入被拒絕，因為超過了密碼嘗試限制	
	登入被拒絕，因為密碼已過期	
	登出	

回溯掃瞄

您可以使用追溯掃描來最佳化關聯規則資源或分析歷史資料。

您也可以選擇根據追溯掃描建立警示。

若要使用追溯掃描：

1. 在主功能表中，前往**監控 → 威脅搜尋**。
2. 按一下事件表右上角的**•••**按鈕，然後選擇**追溯掃描**。
   追溯掃描窗格將開啟。
3. 在**關聯器**下拉清單中，選擇要為選定的事件提供關聯器。
4. 在**關聯規則**下拉清單中，選擇處理事件時必須使用的關聯規則。
5. 若要在事件處理期間執行回應，請開啟**執行回應**切換開關。
6. 若要在事件處理期間產生警示，請開啟**建立警示**切換開關。
7. 按一下**建立工作**按鈕。
   追溯掃描工作會建立在 KUMA 的**工作管理器**區段中。

獲取事件表統計資訊

您可以取得事件表中目前顯示的事件分類的統計資料。事件分類取決於篩選器設定。

若要獲取統計資料，請執行以下操作：

1. 請依照下列步驟開啟事件表。
2. 執行以下操作之一：
   - 在事件表的右上角，從**•••**下拉清單中選擇**統計資料**。
   - 在事件表中，按一下任意值，然後從開啟的快顯功能表中選擇**統計資料**。

統計資料詳情區域將顯示目前事件分類的參數清單。每個參數附近的數字表示選擇中包含該參數的事件數。如果延伸某個參數，則會顯示五個最常出現的值。在**搜尋欄位**中輸入參數名稱以篩選顯示的資料。

統計資料視窗可讓您修改事件篩選器。

> 當使用具有資料分組和彙總的SQL查詢來篩選事件時，統計資料不可用。

威脅回應

若要執行回應操作，檢視您從常規程式執行的擴充結果並手動啟動常規程式，您必須轉至**警示**或**事件**部分。

如果符合以下條件，主功能表中將顯示**警示**和**事件**部分：

- 您擁有Kaspersky Next XDR Expert的產品授權金鑰。
- 您已連線到OSMP主控台中的根管理伺服器。
- 您擁有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師、 SOC管理員、與NCIRCC互動、核准人和稽核員。

執行回應操作後，您可以檢視回應歷史記錄。

回應操作

可以透過以下方式之一啟動回應操作：

- 手動，如本部分所述。

  針對未安裝 內建代理的 Kaspersky Endpoint Security 的裝置，您無法執行以下回應操作：管理服務、刪除檔案、YARA 掃描、IOC 掃描、從隔離區取得檔案，以及取得檔案以進行進一步分析部分中所述的回應操作。

  從警示或事件詳情或資產表進行回應時，您無法選擇歸檔的裝置。

- 在常規程式中。

  在這種情況下，在建立或編輯常規程式時，您可以將回應操作設定為自動運行，或在常規程式啟動前請求使用者手動核准。預設情況下，手動核准回應操作是停用的。

  如果在執行回應操作期間裝置被歸檔，則常規程式結果將顯示**錯誤**訊息。如果針對包含已歸檔裝置的警示觸發常規程式，常規程式結果會顯示警告訊息，以及裝置已歸檔的說明。

終止進程

終止處理程序 回應操作可讓您遠端終止裝置上的進程。您可以對可觀察物件或資產執行終止處理程序回應操作。

您可以透過以下方式之一執行終止處理程序回應操作：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從遙測事件

  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。

- 從調查圖表

  如果已建置調查圖，則該選項可用。

- 從資產表
- 從**回應歷史**部分。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要執行終止處理程序回應操作，您必須具備下列XDR角色之一：主管理員、一級分析師、二級分析師、租用戶管理員。

由於受管理裝置和管理伺服器之間的同步間隔，可能需要最多15分鐘才能啟動回應操作。

從警示或事件詳細資訊回應

若要從警示或事件詳情終止進程：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。
2. 在開啟的視窗中，請轉至**資產**頁籤。

   您也可以轉至**可觀測項**頁籤，選擇一個或多個要終止進程的可觀察物件。這些可觀察物件可以包括MD5或SHA256雜湊值。

3. 在資產清單中，選擇所需的一個或多個裝置。
4. 在**選取回應動作**下拉清單中，點擊**終止處理程序**。
5. 在開啟的右側窗格中，執行以下操作：
   a. 在**完整路徑**欄位中，指定進程檔案的完整路徑。
   b. 在**資產**下拉清單，選取要終止其進程的裝置。

      如果在步驟2中選擇了**資產**頁籤，則預設情況下，您選取的核取方塊對應的裝置名稱會顯示在**資產**欄位中。您可以更改它們或在**所有資產**下拉清單中選擇**範圍**選項，以終止屬於警示或事件租用戶（及其子租用戶）的所有裝置上的進程。

只有可執行此回應操作的資產可供選取。
裝置顯示如下：屬於警示或事件的裝置會置於下拉清單開頭，接著依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

c. 如有必要，請在相應的欄位中配置以下設定：

- 指定進程檔案的SHA256或MD5雜湊值。
  如果在步驟2中選擇了**可觀測項**頁籤，則預設會指定您選擇的雜湊值。您可以變更這些雜湊值。
- 為回應操作編寫描述或註釋。

6. 按一下**終止**按鈕。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊回應

若要從裝置詳情中終止進程：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。
4. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從遙測事件回應

若要從警示或事件詳情中開啟遙測事件時終止該事件的進程：

1. 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的警示ID。
2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：
   - 按一下所需事件的名稱並選擇裝置。
   - 按一下**在威脅搜尋中尋找**按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。

您也可以轉至**可觀測項**頁籤，選擇一個或多個要終止進程的可觀察物件。這些可觀察物件可以包括MD5或SHA256雜湊值。

3. 在**選取回應動作**下拉清單中，點擊**終止處理程序**。

4. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

若要從威脅搜尋部分開啟遙測事件時對其進行回應：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
事件表隨即開啟。

2. 點擊要開啟其詳情的事件名稱。

3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從開啟的下拉清單中選擇**終止處理程序**。

4. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從調查圖表回應

> 如果已建置調查圖，則該選項可用。

若要從調查圖終止進程：

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。

2. 在開啟的**事件詳情**視窗中，按一下**在圖表上檢視**按鈕。
調查圖表視窗將開啟。

3. 按一下所需裝置的名稱，然後在下拉清單中，選擇**檢視詳情**。

4. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從資產表進行回應

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）**。
這將開啟資產表。

2. 選取要執行回應操作的裝置旁的核取方塊。
您可以選擇多個裝置。

已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，點擊**終止處理程序**。
4. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從回應歷史部分回應

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。
包含所有警示和事件的回應歷史記錄的表格將開啟。
2. 在**回應**下拉清單中，選擇**終止處理程序**。
3. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

流程終止。如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作的結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則，將顯示錯誤訊息以及錯誤原因的相關資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

將裝置移動至管理群組

作為回應操作，您可以將裝置移至Open Single Management Platform的另一個管理群組。當警示或事件分析顯示裝置的防護等級較低時，可能需要執行此操作。將裝置移至另一個管理群組時，群組政策和工作將會套用至該裝置。

裝置移動到的管理群組必須與裝置屬於同一租用戶。

您可以透過以下方式之一將裝置移至另一個管理群組：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從調查圖表

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要將裝置移至另一個管理群組，您必須具有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

由於受管理裝置和管理伺服器之間的同步間隔，可能需要最多15分鐘才能啟動回應操作。

將裝置從警示或事件詳細資訊移至另一個管理群組

若要將裝置從警示或事件詳細資訊移至另一個管理群組：

1. 執行以下其中一項操作：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移動的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移動的裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 選取要移至另一個管理群組的裝置旁的核取方塊。

   如果裝置由相同管理伺服器管理，則可以選擇多個裝置：主管理伺服器、從屬管理伺服器或虛擬伺服器。

4. 在**選取回應動作**下拉清單中，選擇**移至群組** 。
   螢幕右側開啟的**移至群組**視窗顯示管理選定裝置的管理伺服器的管理群組。
5. 選擇要將裝置移至的管理群組，然後按一下**移動**按鈕。

選取的裝置會移至選取的管理群組。螢幕上會顯示對應的訊息。

將裝置從裝置詳細資訊移至其他管理群組

若要將裝置從裝置詳細資訊移至其他管理群組：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移動的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移動的裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。
4. 在**選取回應動作**下拉清單中，選擇**移至群組** 。
   螢幕右側開啟的**移至群組**視窗顯示管理選定裝置的管理伺服器的管理群組。
5. 選擇要將裝置移至的管理群組，然後按一下**移動**按鈕。

選取的裝置會移至選取的管理群組。螢幕上會顯示對應的訊息。

將裝置從調查圖表移至其他管理群組

如果調查圖表已建立，則此選項可用。

若要將裝置從調查圖表移至其他管理群組：

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移動的裝置的事件ID。
2. 按一下**在圖表上檢視**按鈕。
3. 在開啟的調查圖中，按一下裝置名稱以開啟裝置詳細資訊。
4. 在**選取回應動作**下拉清單中，選擇**移至群組** 。
   螢幕右側開啟的**移至群組**視窗顯示管理選定裝置的管理伺服器的管理群組。
5. 選擇要將裝置移至的管理群組，然後按一下**移動**按鈕。

選取的裝置會移至選取的管理群組。螢幕上會顯示對應的訊息。

更新資料庫

為了快速偵測威脅並使用戶端裝置的防護等級保持最新，您必須定期更新裝置上的資料庫和應用程式模組。

您可以透過以下方式之一更新裝置上的資料庫：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從調查圖表

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要更新裝置上的資料庫，您必須具備下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

由於受管理裝置和管理伺服器之間的同步間隔，可能需要最多15分鐘才能啟動回應操作。

從警示或事件詳細資訊更新資料庫

若要從警示或事件詳細資訊更新裝置上的資料庫：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要更新資料庫的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要更新資料庫的裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 選取要更新資料庫的裝置旁的核取方塊。
   如有必要，您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**更新資料庫**。

   如果操作成功完成，螢幕上將顯示對應的訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊更新資料庫

若要從裝置詳細資訊更新裝置上的資料庫：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要更新資料庫的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要更新資料庫的裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。

4. 在**選取回應動作**下拉清單中，選擇**更新資料庫**。

如果操作成功完成，螢幕上將顯示對應的訊息。否則，將顯示錯誤訊息。

從調查圖表更新資料庫

如果調查圖表已建立，則此選項可用。

若要從調查圖表更新裝置上的資料庫：

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要更新資料庫的裝置的事件ID。

2. 按一下**在圖表上檢視**按鈕。

3. 在開啟的調查圖中，按一下裝置名稱以開啟裝置詳細資訊。

4. 在**選取回應動作**下拉清單中，選擇**更新資料庫**。

如果操作成功完成，螢幕上將顯示對應的訊息。否則，將顯示錯誤訊息。

變更裝置的授權狀態

當對警示或事件的分析顯示裝置的防護級別較低或裝置對您的基礎架構造成損害時，您可以變更裝置的授權狀態。

此回應操作在安裝了KICS for Networks的裝置上執行。

您可以透過以下其中一種方式變更裝置的授權狀態：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從遙測事件
- 從調查圖表

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要變更裝置的授權狀態，您必須具備以下一種XDR角色：主管理員、租用戶管理員、一級分析師、二級分析師。

從警示事件詳細資訊中變更裝置的授權狀態

若要從警示或事件詳細資訊中變更裝置的授權狀態：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要變更授權狀態的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要變更授權狀態的裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 選取要變更授權狀態的裝置旁的核取方塊。
   如有必要，您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**變更授權狀態**。
5. 在螢幕右側開啟的視窗中，選擇裝置的新狀態（*授權*或*未授權*），然後按一下**變更**按鈕。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊變更裝置的授權狀態

若要從裝置詳細資訊變更裝置的授權狀態：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要變更授權狀態的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要變更授權狀態的裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。
4. 在**選取回應動作**下拉清單中，選擇**變更授權狀態**。
5. 在螢幕右側開啟的視窗中，選擇裝置的新狀態（*授權*或*未授權*），然後按一下**變更**按鈕。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從遙測事件變更裝置的授權狀態

若要從遙測事件變更裝置的授權狀態：

1. 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要變更授權狀態的裝置的警示ID。
2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：
   - 按一下所需事件的名稱並選擇裝置。
   - 按一下**在威脅搜尋中找尋**按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。
3. 在**選取回應動作**下拉清單中，選擇**變更授權狀態**。
4. 在螢幕右側開啟的視窗中，選擇裝置的新狀態（*授權* 或 *未授權*），然後按一下**變更**按鈕。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

從調查圖表變更裝置的授權狀態

> 如果調查圖表已建立，則此選項可用。

若要從調查圖表變更裝置的授權狀態：

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要變更授權狀態的裝置的事件ID。
2. 在開啟的視窗中，按一下**在圖表上檢視**按鈕。
   調查圖表將開啟。
3. 按一下裝置名稱以開啟裝置詳細資訊。
4. 在**選取回應動作**下拉清單中，選擇**變更授權狀態**。
5. 在螢幕右側開啟的視窗中，選擇裝置的新狀態（*授權* 或 *未授權*），然後按一下**變更**按鈕。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

裝置選定的授權狀態顯示在警示或事件卡的**資產**頁籤 → **授權狀態**列中。

將檔案移至隔離區

為防止威脅傳播，您可以透過以下方式之一將受感染的檔案移至隔離區：

- 從警示或事件詳細資訊
- 從裝置詳細資訊

- 從遙測事件

  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。

- 從調查圖表
- 從資產表
- 從**回應歷史**部分。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要將檔案移至隔離區，您必須具備下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

由於受管理裝置和管理伺服器之間的同步間隔，可能需要最多15分鐘才能啟動回應操作。

從警示或事件詳細資訊回應

若要從警示或事件詳細資訊將檔案移至隔離區：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。

   您也可以轉至**可觀測項**頁籤，選取要移至隔離區的檔案旁的核取方塊，然後點選**移至隔離區**按鈕。

3. 選取要移至隔離區的檔案所在裝置旁的核取方塊。
   如有必要，您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**移動到隔離區**。
5. 在開啟的右側窗格中，執行以下操作：
   a. 在**完整路徑**欄位中，指定要移至隔離區的檔案的完整路徑。
   b. 在**資產**欄位中，選擇要將檔案移至隔離區的檔案所在的裝置。

      如果在步驟2中選擇了**資產**頁籤，則預設情況下，您選取的核取方塊對應的裝置名稱會顯示在**資產**欄位中。您可以變更這些名稱，並指定與警示或事件無關但屬於警示或事件租用戶（及其子租用戶）的裝置。

      只有可執行此回應操作的資產可供選取。
      裝置顯示如下：屬於警示或事件的裝置會置於下拉清單開頭，接著依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

c. 如有必要，請在相應的欄位中配置以下設定：

- 指定檔案的SHA256或MD5雜湊值。

  > 如果在步驟2中選擇了**可觀測項**頁籤，則會自動指定雜湊值。您可以變更該值。

- 為回應操作編寫描述或註釋。

6. 按一下**移動**按鈕。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

從裝置詳細資訊回應

若要從裝置詳細資料中將檔案移至隔離區：

1. 執行以下操作之一：

- 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的警示ID。
- 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的事件ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。

4. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

從遙測事件回應

若要從警示或事件詳情中開啟遙測事件時將檔案從遙測事件中移至隔離區：

1. 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的警示ID。

2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：

- 按一下所需事件的名稱並選擇裝置。
- 按一下**在威脅搜尋中找尋**按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。

> 您也可以轉至**可觀測項**頁籤，選取要移至隔離區的檔案旁的核取方塊，然後點選**移至隔離區**按鈕。

3. 在**選取回應動作**下拉清單中，選擇**移動到隔離區**。

4. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

若要從威脅搜尋部分開啟遙測事件時對其進行回應：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**

事件表隨即開啟。

2. 點擊要開啟其詳情的事件名稱。

3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從開啟的下拉清單中選擇**移動到隔離區**。

4. 執行與*從警示或事件詳情進行回應*第5-6步中所述的相同操作。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

從調查圖表回應

如果調查圖表已建立，則此選項可用。

若要從調查圖表中將檔案移至隔離區：

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要移至隔離區的檔案所在裝置的事件ID。

2. 在開啟的視窗中，按一下**在圖表上檢視**按鈕。

調查圖表將開啟。

3. 按一下裝置名稱以開啟裝置詳細資訊。

4. 在**選取回應動作**下拉清單中，選擇**移動到隔離區**。

5. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

從資產表進行回應

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）**。

這將開啟資產表。

2. 選取要執行回應操作的裝置旁的核取方塊。

   您可以選擇多個裝置。

   > 已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇**移動到隔離區**。

4. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

   如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

從回應歷史部分回應

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。

   包含所有警示和事件的回應歷史記錄的表格將開啟。

2. 在**回應**下拉清單中，選擇**移動到隔離區**。

3. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

   如果操作成功完成，螢幕上將顯示相應訊息。檔案將從其所在裝置的目錄中刪除，並移至同一裝置上的隔離目錄。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作的結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

從隔離區還原檔案

如果您有理由相信已移至隔離區的檔案是安全的，則可以透過以下方式之一將檔案還原到裝置上：

- 從主功能表的**隔離**部分
- 從**移動到隔離區**回應操作的結果。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從隔離部分進行回應

若要從隔離部分進行回應：

1. 在主功能表中，轉至**儲存區 → 隔離**。
2. 執行以下操作之一：
   - 選擇要從隔離區還原的檔案。
     您可以選擇多個檔案。
   - 按一下要從隔離區還原的檔案名稱。

   檔案詳情隨即開啟。
3. 按一下**還原**按鈕，然後確認操作。
   您可以根據需要在確認操作之前在**描述**欄位中寫下備注。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將還原到您先前將其移至隔離區的裝置上，並位於原始路徑（即您在將檔案移至隔離區應用情境的步驟5中指定的路徑）。否則，將顯示錯誤訊息。

從**移動到隔離區**回應操作的結果進行回應

若要從移動到隔離區回應操作的結果進行回應：

1. 您可以透過以下方式之一開啟**移動到隔離區**回應操作的結果：
   - 在主功能表中，轉至**監控 → 回應歷史**。
   - 在主功能表中，轉至**監控**，然後選擇**警示**或**事件**部分。在**ID**直欄中，按一下包含您已執行**移動到隔離區**回應操作的資產或可觀察物件的警示或事件的ID。在開啟的警示或事件詳情中，轉至**歷史記錄**頁籤。
2. 對於**移動到隔離區**回應操作的結果，請在**動作狀態**直欄中，點按**成功**連結。
3. 在開啟的詳情視窗中，按一下**還原**按鈕，然後確認操作。
4. 您可以根據需要在確認操作之前在**描述**欄位中寫下備注。

如果操作成功完成，螢幕上將顯示相應訊息。檔案將還原到您先前將其移至隔離區的裝置上，並位於原始路徑（即您在將檔案移至隔離區應用情境的步驟5中指定的路徑）。否則，將顯示錯誤訊息。

檢視回應操作結果

如果包含內建代理的Kaspersky Endpoint Security已安裝在您的裝置上，則回應操作的結果將顯示在**回應歷史**區段。

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

從隔離區取得檔案

若要執行回應操作，您必須具備：

- 下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。
- 包含內建代理程式的Kaspersky Endpoint Security已安裝在您的裝置上。

可以從隔離目錄中取得裝置上的已隔離檔案，以便進行進一步分析。取得的檔案將顯示在OSMP主控台的**檔案**部分。

您可以透過以下其中一種方式執行回應操作：

- 從主功能表的**隔離**部分
- 從**移動到隔離區**回應操作的結果。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從隔離部分進行回應

若要從隔離部分進行回應：

1. 在主功能表中，轉至**儲存區 → 隔離**。
2. 執行以下操作之一：
   - 選擇要從隔離區取得的檔案。
   - 按一下要從隔離區取得的檔案名稱。

   檔案詳情隨即開啟。

3. 點擊**獲取檔案**按鈕，然後確認操作。

> 如果您希望在取得檔案後檢查其是否有威脅，可以點擊**獲取並掃描**按鈕。

如果操作成功完成，螢幕上將顯示相應的訊息，並從裝置中取得已隔離的檔案。否則，將顯示錯誤訊息。

從移動到隔離區回應操作的結果進行回應

若要從移動到隔離區回應操作的結果進行回應：

1. 您可以透過以下方式之一開啟**移動到隔離區**回應操作的結果：

   - 在主功能表中，轉至**監控** → **回應歷史**。
   - 在主功能表中，轉至**監控**，然後選擇**警示**或**事件**部分。在**ID**欄中，按一下警示或事件的 ID；該警示或事件包含您曾對其執行**移動到隔離區**回應操作的資產或可觀測物件。在開啟的警示或事件詳情中，轉至**歷史記錄**頁籤。

2. 對於**移動到隔離區**回應操作的結果，請在**動作狀態**直欄中，點按**成功**連結。
3. 在開啟的詳情視窗中，按一下**獲取檔案**按鈕，然後確認操作。

> 如果您希望在取得檔案後檢查其是否有威脅，可以點擊**獲取並掃描**按鈕。

檢視回應操作結果

回應操作的結果將顯示：

- 在主功能表的**檔案**部分
- 在主功能表中的**回應歷史**部分

  點按**動作狀態**直欄中的連結後，檔案詳情將開啟，並選擇**結果**頁籤，根據需要，您可以在其中檢視和下載受密碼保護的ZIP存檔到您的電腦。密碼被*感染了*。

  如果回應操作失敗，則會顯示**錯誤**訊息以及有關錯誤原因的資訊。

  若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

從隔離區刪除檔案

> 若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

您可以透過以下方式之一從裝置上的隔離目錄中刪除受感染的檔案：

- 从OSMP主控台功能表的**隔離**部分
- 從**移動到隔離區**回應操作的結果。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從隔離部分進行回應

若要從隔離部分進行回應：

1. 在主功能表中，轉至**儲存區 → 隔離**。
2. 執行以下操作之一：
   - 選擇要從隔離區刪除的檔案。
     您可以選擇多個檔案。
   - 按一下要從隔離區刪除的檔案名稱。
     檔案詳情隨即開啟。
3. 點選**刪除** 按鈕，然後確認操作。

如果操作成功完成，螢幕上將顯示相應訊息。該檔案隨即從其所在裝置的隔離目錄中永久刪除。否則，將顯示錯誤訊息。

從**移動到隔離區**回應操作的結果進行回應

若要從移動到隔離區回應操作的結果進行回應：

1. 您可以透過以下方式之一開啟**移動到隔離區**回應操作的結果：
   - 在主功能表中，轉至**監控 → 回應歷史**。
   - 在主功能表中，轉至**監控**，然後選擇**警示**或**事件**部分。在**ID**直欄中，按一下包含您已執行**移動到隔離區**回應操作的資產或可觀察物件的警示或事件的ID。在開啟的警示或事件詳情中，轉至**歷史記錄**頁籤。
2. 對於**移動到隔離區**回應操作的結果，請在**動作狀態**直欄中，點按**成功**連結。
3. 在開啟的詳細資料視窗中，按一下**刪除**按鈕，然後確認操作。

如果操作成功完成，螢幕上將顯示相應訊息。該檔案隨即從其所在裝置的隔離目錄中永久刪除。否則，將顯示錯誤訊息。

檢視回應操作結果

如果包含內建代理的Kaspersky Endpoint Security已安裝在您的裝置上，則回應操作的結果將顯示在**回應歷史**區段。

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

檢視KASAP使用者的資訊並變更學習群組

設定KASAP與KUMA整合後，當您檢視與警示或事件關聯的使用者資料時，OSMP主控台中提供來自KASAP的以下資訊：

- 使用者所屬的學習群組。
- 使用者完成的學習課程。
- 所計劃的學習課程及其當前進度。

您可以檢視KASAP使用者的資料。為此，您必須透過以下方式之一開啟使用者詳細資訊：

- 從警示或事件詳細資訊
- 從遙測事件中（如果從警示詳情中開啟它）。
- 從調查圖表中。

> 如果已建立調查圖表，則此選項可用。

若要開啟使用者詳細資訊：

1. 在主功能表中，轉至**監控**，然後選擇**警示**或**事件**部分。
   如果要從遙測事件中開啟使用者詳細資訊，請選擇**警示**部分。
   如果您要從調查圖表中開啟使用者詳細資訊，請選擇**事件**部分。
2. 按一下所需警示或事件的ID。
3. 在開啟的視窗中，執行以下操作之一：
   - 如果您要從遙測事件中開啟使用者詳細資訊，請轉至**詳細資訊**頁籤，然後按一下所需事件的名稱並選擇使用者；或按一下**在威脅搜尋中找尋**按鈕，轉至**威脅搜尋**部分，然後選取所需的使用者。
   - 如果您要從警示或事件詳細資訊中開啟使用者詳細資訊，請轉至**資產**頁籤，然後按一下所需使用者的名稱。
   - 如果您要從調查圖表中開啟使用者詳細資訊，請按一下**在圖表上檢視**按鈕。在開啟的視窗中，按一下所需子使用者的名稱。

帳戶詳細資訊視窗將在螢幕右側開啟。

4. 選擇**網路安全課程**頁籤。

   此視窗顯示有關KASAP使用者的資訊。

您可以透過以下方式之一更改KASAP使用者的學習群組：

- 從警示或事件詳細資訊中
- 從遙測事件中（如果從警示詳情中開啟它）。
- 從調查圖表中

> 如果調查圖表已建立，則此選項可用。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。在這種情況下，如果您將使用者移至未開始學習的群組，則該使用者將無法開始學習。

> 若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要變更KASAP使用者學習群組：

1. 在主功能表中，轉至**監控**，然後選擇**警示**或**事件**部分。

   如果您想從遙測事件中變更KASAP使用者學習群組，請選擇**警示**部分。

   如果您想從調查圖表中變更KASAP使用者學習群組，請選擇**事件事件**

2. 按一下所需警示或事件的ID。

3. 在開啟的視窗中，執行以下操作之一：

   - 如果您想透過遙測事件進行回應，請轉至**詳細資訊**選項卡，然後按一下所需事件的名稱，然後選擇使用者；或按一下**在威脅搜尋中找尋**按鈕，轉至**威脅搜尋**部分，然後選取所需的使用者。
   - 如果您想透過使用者詳細資訊回應，請轉至**資產**頁籤，然後按一下使用者的名稱。
   - 如果您想透過調查圖表進行回應，請按一下**在圖表上檢視**按鈕。在開啟的視窗中，按一下使用者的名稱。

   帳戶詳細資訊視窗將在螢幕右側開啟。

4. 在**指派 KASAP 群組**下拉清單中，選擇要將使用者指派到的KASAP學習群組。

> 重新計算KASAP使用者培訓計畫可能需要長達30分鐘。在此期間不建議更改KASAP學習組。

使用者將移至所選的KASAP群組。KASAP公司管理員將收到學習群組變更通知，並重新計算所選學習群組的學習計畫。

有關學習群組以及如何開始使用的詳細資訊，請參閱KASAP 說明文件。

啟用和停用網路隔離

您可以透過以下方式之一啟用和停用裝置上的網路隔離：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從調查圖表
- 從資產表
- 從事件詳細資訊
  此選項僅在啟用網路隔離時可用。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

對於已安裝包含內建代理的 Kaspersky Endpoint Security的裝置，網路隔離狀態會顯示在裝置詳細資訊中。

裝置可能具有以下狀態之一：*已隔離*、*正在隔離*、*套用隔離時發生錯誤*、*未隔離*。

此外，當您從警示或事件詳細資訊中的**資產**頁籤，或從**資產管理 → 資產（裝置）中開啟資產表時，網路隔離狀態會顯示在資產表中。**您可以篩選資產表中**隔離狀態**直欄的值，以顯示具有所需網路隔離狀態的裝置。

從警示或事件詳細資訊執行回應操作

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 選取所需裝置旁邊的核取方塊。
   如有必要，您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**網路隔離**，然後在快顯表單中，選擇要執行的回應操作：
   - **啟用**
     如果您為已啟用網路隔離的裝置選擇此回應操作，則參數將被新值覆蓋。

在啟用網路隔離之前，請確保已從卡巴斯基安全管理中心匯入資產：在 **工作 → 偵測和響應** 中，**KSC資產匯入**工作顯示為已完成狀態。

- **停用**

  選擇此回應操作後，在確認對話方塊中，按一下**停用** 。

  您可以為啟用了網路隔離的裝置選擇此回應操作。

5. 如果在步驟4中選擇了**啟用**，則在開啟的右側窗格中，您可以配置下列設定：

   a. 在**資產**下拉清單中，指定要隔離的裝置。

   預設情況下，會顯示您先前選取的核取方塊對應的裝置。根據需要，您可以變更裝置。您無法選擇具有以下狀態的裝置：**已隔離**、 **正在隔離**或**套用隔離時發生錯誤**。

   只有可對其執行回應操作的裝置可供選擇。
   裝置顯示如下：屬於警示或事件的裝置會置於下拉清單開頭，接著依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

   b. 請指定裝置隔離的時間段和組件。

   c. 在**描述**欄位中，編寫對回應操作的描述或備注。

   d. 如果您要將裝置新增至網路隔離規則的例外清單中，請按一下**新增排除項目**按鈕，然後在**網路流量方向**下拉清單中選擇下列其中一個值：

   - **入站**，然後在對應的欄位中指定要從網路流量封鎖中排除的裝置的IP位址和本機連接埠範圍。
   - **出站**，然後在對應的欄位中指定要從網路流量封鎖中排除的裝置的IP位址和遠端連接埠範圍。
   - **入站/出站**，然後指定要從網路隔離中排除的裝置的IP位址。

6. 按一下**啟用**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊執行回應操作

若要從裝置詳細資訊進行回應：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中，選擇**檢視內容**。

4. 執行與*執行裝置詳情中的回應操作*第4-6步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從調查圖表執行回應操作

> 如果調查圖表已建立，則此選項可用。

若要從調查圖表進行回應

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。

2. 在開啟的視窗中，按一下**在圖表上檢視**按鈕。
調查圖表將開啟。

3. 按一下裝置名稱以開啟裝置詳細資訊。

4. 執行與*執行裝置詳情中的回應操作*第4-6步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從資產表執行回應操作

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）。**
這將開啟資產表。

2. 選取要執行回應操作的裝置旁的核取方塊。
您可以選擇多個裝置。

> 已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇下列選項之一：

- **啟用網路隔離**，然後在開啟的右側窗格中，配置回應操作設定。
- **停用網路隔離**，然後在確認對話方塊中，按一下**停用**。

從事件詳情啟用網路隔離

若要從事件詳情啟用網路隔離：

1. 在主功能表中，轉至**監控 → 威脅搜尋**。
   事件表隨即開啟。
2. 點擊要開啟其詳情的事件名稱。
3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從開啟的下拉清單中選擇**啟用網路隔離**。
4. 在開啟的右側窗格中，配置回應操作設定。

如果您尚未在裝置上安裝具有內建代理的 Kaspersky Endpoint Security 應用程式，而且執行回應操作時發生錯誤，請確認 Kaspersky Next XDR Expert 中的裝置名稱與 8.0 之前版本的 Kaspersky Anti Targeted Attack Platform 中的裝置名稱相符。

執行「新增阻止規則」和「刪除阻止規則」回應操作

阻止規則可讓您阻止您認為不安全的檔案或進程在裝置上執行。Kaspersky Next XDR Expert使用MD5和SHA256雜湊值演算法，根據檔案的雜湊值識別檔案。

您可以透過以下方式之一設定**新增阻止規則**和**刪除阻止規則**回應操作，以新增和刪除裝置或檔案雜湊值的阻止規則：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從調查圖表
- 從資產表
- 從**回應歷史**部分。
- 從事件詳細資訊
  此選項適用於**新增阻止規則**回應操作。您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。
- 從檔案詳情

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

從警示或事件詳細資訊執行回應操作

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**警示 ID** 列中，按一下包含所需裝置的警示 ID。
   - 在主選單中，轉到**監控→事件**部分。在**事件 ID** 列中，按一下包含所需裝置的事件 ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 選取所需裝置旁邊的核取方塊。
   如有必要，您可以選擇多個裝置。

4. 在**選取回應動作**下拉清單中，選擇**管理阻止規則**，然後在快顯表單中，選擇要執行的回應操作：

   - **新增阻止規則**
   - **刪除阻止規則**

5. 在開啟的視窗中，設定您在步驟4中選擇的回應操作的必要參數：

   - **若要新增阻止規則**

     在開啟的右側窗格中，配置以下設定：

     1. 在**MD5 或 SHA256**欄位中，指定要封鎖的檔案的雜湊值。
        如果要指定多個雜湊值，請點選**新增雜湊值**按鈕。

     2. 如果必要，配置以下設定：

        - 更改回應操作的範圍。

          預設情況下，在設定的**範圍**群組中，會選取**特定資產**選項，而**資產**下拉清單則包含您先前選取其核取方塊的裝置名稱。

          您可以變更要新增阻止規則的裝置，或在設定群組的**所有資產**中選擇**範圍**選項，為屬於警示或事件租用戶及其子租用戶的所有裝置新增阻止規則。

          > 只有您可以對其執行回應操作的資產才可供選擇。
          > 裝置顯示如下：屬於警示或事件的裝置會置於下拉清單開頭，然後依字母順序顯示屬於警示或事件租用戶及子租用戶的裝置。

        - 啟用**通知使用者關於封鎖檔案執行的事宜**切換開關。
        - 在**描述**欄位中，編寫對回應操作的描述或備注。

     3. 按一下**新增**按鈕。

     視窗即會關閉。

- **若要刪除阻止規則**

  在開啟的右側窗格中，配置以下設定：

  1. 選取您要刪除的內容。

     預設情況下，在**規則**群組設定中，選擇了**具體規則**選項。若要透過檔案雜湊值刪除阻止規則，請在**MD5 或 SHA256**欄位中指定要刪除的檔案雜湊值。如果要指定多個雜湊值，請點選**新增雜湊值**按鈕。

     如果要刪除所有阻止規則，請選擇**全部規則**選項。

  2. 如果必要，配置以下設定：

     - 更改回應操作的範圍。

       預設情況下，在設定的**範圍**群組中，會選取**特定資產**選項，而**資產**下拉清單則包含您先前選取其核取方塊的裝置名稱。

       您可以變更要刪除阻止規則的裝置，或在設定**所有資產**群組中選擇**範圍**選項，以刪除屬於警示或事件租用戶及其子租用戶的所有裝置的阻止規則。

       > 只有可執行此回應操作的資產可供選取。
       > 裝置顯示如下：屬於警示或事件的裝置會置於下拉清單開頭，接著依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

     - 在**描述**欄位中，編寫對回應操作的描述或備注。

  3. 接著，點擊**刪除**按鈕。

     視窗即會關閉。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊執行回應操作

若要從裝置詳細資訊進行回應：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**警示 ID** 列中，按一下包含所需裝置的警示 ID。
   - 在主選單中，轉到**監控→事件**部分。在**事件 ID** 列中，按一下包含所需裝置的事件 ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中，選擇**檢視內容**。

4. 執行與*從裝置詳細資訊執行回應操作*中步驟4-5相同的操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從調查圖表執行回應操作

如果調查圖表已建立，則此選項可用。

若要從調查圖表進行回應

1. 在主選單中，轉到**監控→事件**部分。在**事件 ID** 列中，按一下包含所需裝置的事件 ID。
2. 在開啟的視窗中，按一下**在圖表上檢視**按鈕。
   調查圖表將開啟。
3. 按一下裝置名稱以開啟裝置詳細資訊。
4. 執行與*從裝置詳細資訊執行回應操作*中步驟4-5相同的操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從資產表執行回應操作

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）。**
   這將開啟資產表。
2. 選取要執行回應操作的裝置旁的核取方塊。
   您可以選擇多個裝置。

   已存檔的裝置無法選擇。

3. 在**響應**下拉式清單中，選取**管理阻止規則**，然後在右鍵功能表中選取要執行的回應操作。
4. 在開啟的右側窗格中，請依照*從警示或事件詳情執行回應操作*中的步驟5所述配置回應操作設定。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從回應歷史部分執行回應操作

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。
   包含所有警示和事件的回應歷史記錄的表格將開啟。

2. 在**回應**下拉清單中，選擇**新增阻止規則**或**刪除阻止規則**。

3. 在開啟的右側窗格中，請依照*從警示或事件詳情執行回應操作*中的步驟5所述配置回應操作設定。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從事件詳情執行回應動作

此選項適用於**新增阻止規則**回應操作。

若要從事件詳情執行回應操作：

1. 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。

2. 在打開的視窗中，轉到 **詳細資訊**頁籤，然後選擇所需的檔案。

3. 按一下**新增阻止規則**按鈕，然後選擇要為其新增阻止規則的裝置。

您也可以前往**可觀察項目**頁籤，然後選取要封鎖之檔案雜湊旁的核取方塊。在**選取回應操作**下拉式清單中，按一下**管理阻止規則**，然後選取**新增阻止規則**或**刪除阻止規則**。

4. 執行與*從裝置詳情執行回應操作*第5步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

在開啟的事件詳情視窗中，在主機名稱欄位中，按一下裝置名稱，然後從開啟的下拉式清單中選取新增阻止規則。

執行與從裝置詳情執行回應操作第5步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息和**檢視資產**按鈕。您可以點擊該按鈕，然後在開啟的視窗中前往**阻止規則**頁籤，以檢視裝置上阻止規則的狀態。

否則，將顯示錯誤訊息以及錯誤原因的相關資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

如果您的裝置尚未安裝具有內建代理的 Kaspersky Endpoint Security 應用程式，且執行回應操作時發生錯誤，請確定 Kaspersky Next XDR Expert 中的裝置名稱與 8.0 之前版本的 Kaspersky Anti Targeted Attack Platform 中的裝置名稱相符。

執行程式

您可以透過以下其中一種方式執行回應操作：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從調查圖表
- 從資產表
- 從**回應歷史**部分。
- 從事件詳細資訊

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

從警示或事件詳情執行回應操作

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 選取所需裝置旁邊的核取方塊。
   如有必要，您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**執行** ，然後在快顯表單中，按一下**程式**。

5. 在開啟的右側窗格中，執行以下操作：

   a. 在**完整路徑**欄位，指定要執行的可執行檔的完整路徑。

   b. 如果必要，配置以下設定：

   - 更改回應操作的範圍。

     預設情況下，在**範圍**下拉清單中選取了**特定資產**選項，並且**資產**下拉清單包含您先前選取的核取方塊對應的裝置名稱。這意味著，該可執行檔將在這些裝置上執行。

     您可以更改裝置或在**所有資產**欄位中選擇**範圍**選項，以便在屬於警示或事件租用戶（及其子租用戶）的所有裝置上執行可執行檔案。

     僅可選擇您能夠對其執行回應操作的資產。
     裝置的顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單開頭，然後依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

   - 在**命令列參數**欄位中，指定執行可執行檔的其他選項，例如：`/all argument`。
   - 在**工作目錄**欄位中，指定工作目錄。
   - 在**描述**欄位中，編寫對回應操作的描述或備注。

6. 按一下**執行**按鈕。

窗格隨即關閉。視窗即會關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從裝置詳情執行回應操作

若要從裝置詳細資訊進行回應：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中，選擇**檢視內容**。

4. 執行與*從裝置詳情執行回應操作*第4-6步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從調查圖表執行回應操作

如果調查圖表已建立，則此選項可用。

若要從調查圖表進行回應

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。
2. 在開啟的視窗中，按一下**在圖表上檢視**按鈕。
   調查圖表將開啟。
3. 按一下裝置名稱以開啟裝置詳細資訊。
4. 執行與*從裝置詳詳情執行回應操作*第4-6步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

如果您的裝置尚未安裝具有內建代理的 Kaspersky Endpoint Security 應用程式，且執行回應操作時發生錯誤，請確定 Kaspersky Next XDR Expert 中的裝置名稱與 8.0 之前版本的 Kaspersky Anti Targeted Attack Platform 中的裝置名稱相符。

從資產表執行回應操作

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）**。
   這將開啟資產表。
2. 選取要執行回應操作的裝置旁的核取方塊。
   您可以選擇多個裝置。

   已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇**程式**。
4. 在開啟的右側窗格中，依照*從裝置詳情執行回應操作*第4-6步中所述配置回應操作設定。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從回應歷史部分執行回應操作

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。
   包含所有警示和事件的回應歷史記錄的表格將開啟。
2. 在**回應**下拉清單中，選擇**程式**。
3. 在開啟的右側窗格中，依照*從裝置詳情執行回應操作*第4-6步中所述配置回應操作設定。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從事件詳情執行回應動作

若要從事件詳情執行回應操作：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
   事件表隨即開啟。
2. 點擊要開啟其詳情的事件名稱。
3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從開啟的下拉清單中選擇**程式**。
4. 在開啟的右側窗格中，依照*從裝置詳情執行回應操作*第4-6步中所述配置回應操作設定。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作的結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則，將顯示錯誤訊息以及錯誤原因的相關資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

管理服務

您可以遠端啟動、停止、暫停、恢復或刪除裝置上的服務。

若要執行**管理服務**回應操作，您必須具備：

- 下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。
- 包含內建代理程式的Kaspersky Endpoint Security已安裝在您的裝置上。

您可以透過以下其中一種方式指定回應操作：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從遙測事件
  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。
- 從調查圖表中

  如果調查圖表已建立，則此選項可用。
- 從資產表
- 從**回應歷史**部分。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從警示或事件詳細資訊回應

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。

   您也可以轉至**可觀察物件**頁籤，選取要執行回應操作的警示旁邊的核取方塊，然後點擊**管理服務**按鈕。
3. 選取要執行回應操作的裝置旁的核取方塊。
   您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**管理服務**。
5. 在開啟的右側窗格中，在對應的欄位中配置以下設定：
   a. 要管理該服務的裝置。

依預設，在設定的**範圍**群組中，會選取**特定資產**選項，而**資產**下拉清單會包含您在步驟 3 中選取其核取方塊的裝置名稱。

您可以更改裝置或在設定的**所有資產**群組中選擇**範圍**選項，以便管理屬於警示或事件租用戶（及其子租用戶）的所有裝置上的服務。

僅可選擇您能夠對其執行回應操作的資產。
裝置的顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單開頭，然後依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

b. 服務名稱。

c. 若要對服務執行的操作：**修改啟動類型**、**開始**、**停止**、**暫停**、**繼續**或**刪除**。

如果選擇**修改啟動類型**操作，則必須在**新的啟動類型**欄位中選擇值。

強烈不建議停止、暫停、刪除會影響主機運作的服務，或變更這類服務的啟動類型。
不建議管理的服務清單

- AVP*
- BFE
- CertPropSvc
- CoreMessagingRegistrar
- CryptSvc
- DcomLaunch
- Dhcp
- DispBrokerDesktopSvc
- EventLog
- EventSystem
- LanmanServer
- LanmanWorkstation
- LSM
- mpssvc
- Netlogon
- Netman
- PlugPlay
- PolicyAgent

- Power
- ProfSvc
- RasMan
- RpcEptMapper
- RpcSs
- SamSs
- SCardSvr
- SecurityHealthService
- SessionEnv
- Spooler
- SstpSvc
- TermService
- UmRdpService
- UserManager
- UsoSvc
- VaultSvc
- W32Time
- WebClient
- Winmgmt
- WlanSvc
- wscsvc

d. 如果必要，配置以下設定：

- 指定檔案的SHA256或MD5雜湊值。
  如果在步驟2中選擇了**可觀測項**頁籤，則會自動指定雜湊值。您可以變更該值。
- 為回應操作編寫描述或註釋。

6. 按一下**啟動**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊回應

若要從裝置詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。
   裝置詳情窗格隨即開啟。
4. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從遙測事件回應

若要從警示或事件詳情開啟遙測事件時回應該事件：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含所需裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。
2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：
   - 按一下所需事件的名稱並選擇裝置。
   - 按一下**在威脅搜尋中找尋**按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。
3. 執行與*從警示或事件詳情進行回應*第4-6步中所述的相同操作。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

若要從威脅搜尋部分開啟遙測事件時對其進行回應：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
   事件表隨即開啟。
2. 點擊要開啟其詳情的事件名稱。

3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從下拉清單中選擇**管理服務**。

4. 在開啟的右側窗格中，依照*從警報或事件詳情回應*第5步中所述配置回應操作設定，然後啟動回應操作。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從調查圖表回應

若要從調查圖表進行回應

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，點選包含所需裝置的事件ID。

2. 按一下**在圖表上檢視**按鈕。

3. 在開啟的調查圖表中，按一下裝置名稱，然後在下拉清單中選擇**檢視內容**。

4. 在開啟的裝置詳情窗格中，執行與*從警示或事件詳情回應*步驟4-6中所述相同的操作。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從資產表進行回應

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）。**
這將開啟資產表。

2. 選取要執行回應操作的裝置旁的核取方塊。
您可以選擇多個裝置。

> 已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇**管理服務**。

4. 在開啟的右側窗格中，依照*從警示或事件詳情中回應*步驟5-6所述配置回應操作設定。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從回應歷史部分回應

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。
包含所有警示和事件的回應歷史記錄的表格將開啟。

2. 在**回應**下拉清單中，選擇**管理服務**。

3. 在開啟的右側窗格中，依照*從警示或事件詳情回應*第5步中所述配置回應操作設定，然後啟動回應操作。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

透過Kaspersky NGFW阻止IP位址

您可以透過將IP位址新增到黑名單中，透過Kaspersky NGFW防止網路裝置上的潛在威脅傳播和惡意活動。

如果Open Single Management Platform分發套件包含Kaspersky NGFW網頁外掛程式，則回應操作可用。
若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

您可以透過以下其中一種方式執行回應操作：

- 從警示或事件詳細資訊
- 從遙測事件
  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從警示或事件詳細資訊回應

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。
2. 在開啟的視窗中，請轉至**可觀測項**頁籤。

3. 選取您要封鎖其 IP 位址的裝置旁的核取方塊。

4. 在**選取回應動作**下拉清單中，選擇**將 IP 新增至網路裝置上的封鎖清單**回應操作。

視窗即會關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從遙測事件回應

若要從警示或事件詳情開啟遙測事件時回應該事件：

1. 執行以下操作之一：

- 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
- 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。

2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：

- 按一下所需事件的名稱。

3. 按一下**在威脅搜尋中尋找**按鈕以轉至**威脅搜尋**部分，然後按一下所需事件的名稱。

4. 在開啟的事件詳情視窗中，按一下您要封鎖之裝置的 IP 位址連結，然後從下拉式清單中選取**將 IP 新增至網路裝置上的封鎖清單**。

視窗即會關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

若要從威脅搜尋部分開啟遙測事件時回應該事件：

1. 在主功能表中，轉至**監控 → 威脅搜尋**。
事件表隨即開啟。

2. 按一下您要開啟其詳情的事件名稱。

3. 在開啟的事件詳情視窗中，按一下您要封鎖之裝置的 IP 位址連結，然後從下拉式清單中選取**將 IP 新增至網路裝置上的封鎖清單**。

視窗即會關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

取得文件以進行進一步分析

本章節包含旨在收集安全漏洞證據以進行進一步調查的回應操作。您可以取得：

- 檔案
- 登錄機碼
- NTFS 中繼檔
- 鑑證資料

- 磁碟映像檔
- 記憶體傾印
- 處理程序記憶體傾印

若要執行回應操作，您必須具備：

- 下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。
- 包含內建代理程式的Kaspersky Endpoint Security已安裝在您的裝置上。

您可以透過以下其中一種方式指定回應操作：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從遙測事件
  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。
- 從調查圖表中

  > 如果調查圖表已建立，則此選項可用。

- 從資產表
- 從**回應歷史**部分。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從警示或事件詳細資訊回應

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 選取要執行回應操作的裝置旁的核取方塊。
   如果要執行**登錄機碼**或**鑑證資料**回應操作，您可以選擇多個裝置。
4. 在**選取回應動作**下拉清單中，選擇**取得**。
5. 在開啟的快顯表單中，選擇所需的回應操作。

從裝置詳細資訊回應

若要從裝置詳細資訊進行回應：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。
2. 在開啟的視窗中，請轉至**資產**頁籤。
3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。
   裝置詳情視窗隨即開啟。
4. 在**選取回應動作**下拉清單中，選擇**取得**。
5. 在開啟的快顯表單中，選擇所需的回應操作。

從遙測事件回應

若要從警示或事件詳情開啟遙測事件時執行針對該事件的回應操作：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。
2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：
   - 按一下所需事件的名稱並選擇裝置。
   - 按一下**在威脅搜尋中找尋**按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。
3. 在**選取回應動作**下拉清單中，選擇**取得**。
4. 在開啟的快顯表單中，選擇所需的回應操作。

若要從威脅搜尋部分開啟遙測事件時對其進行回應：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
   事件表隨即開啟。
2. 點擊要開啟其詳情的事件名稱。
3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從開啟的下拉清單中選擇所需的回應操作。

從調查圖表回應

若要從調查圖表進行回應

1. 在主選單中，轉到**監控→事件**部分。在"ID"直欄中，按一下包含要執行回應操作的裝置的事件ID。
2. 在開啟的視窗中，按一下**在圖表上檢視**按鈕。
   調查圖表將開啟。
3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。
   裝置詳情視窗隨即開啟。
4. 在**選取回應動作**下拉清單中，選擇**取得**。
5. 在開啟的快顯表單中，選擇所需的回應操作。

從資產表進行回應

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）**。
   這將開啟資產表。
2. 選取要執行回應操作的裝置旁的核取方塊。
   若要執行鑑證資料或登錄機碼回應操作，您可以選擇多個裝置。

   > 已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇所需的回應操作。

從回應歷史部分回應

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。
   包含所有警示和事件的回應歷史記錄的表格將開啟。
2. 在**回應**下拉清單中，選擇所需的回應操作。

取得檔案

若要取得檔案：

1. 選取檔案回應動作。
   獲取檔案窗格隨即開啟。
2. 在**完整路徑**欄位中，指定要取得的檔案路徑。
3. 如果必要，配置以下設定：
   - 在**資產**下拉清單中，更改要取得檔案的裝置。
   - 預設情況下，此欄位包含您先前選取的核取方塊對應的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

     只有您可以對其執行回應操作的資產可供選擇。
     裝置的顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單開頭，然後依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。
   - 在**MD5 或 SHA256**欄位中，指定要取得的檔案的雜湊值。
   - 如果您不想掃描檔案，請停用**掃描檔案**選項。
     預設情況下已啟用該選項。這意味著取得檔案後，系統會對其進行威脅檢查。

     在常規程式中啟動回應操作時，如果要掃描取得的檔案，則必須手動新增此選項。
   - 在**描述**欄位中，編寫對回應操作的描述或備注。
4. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，檔案將儲存為ZIP封存檔案。密碼被*感染了*。

檢視回應操作結果

您可以透過以下方式之一檢視和下載該封存檔案：

- 從主功能表的回應歷史部分，或從警示或事件詳情中的歷史記錄頁籤
- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。

如果您沒有在步驟2中停用**掃描檔案**選項，檔案掃描結果也會顯示。按一下**動作狀態**欄中的連結後，檔案詳情會隨即開啟並選取**結果頁籤**，您可在其中檢視掃描結果，並視需要將檔案下載至您的電腦。

取得登錄檔金鑰

若要取得登錄檔金鑰

1. 選取登錄機碼回應操作。

   取得登錄機碼窗格隨即開啟。

2. 在**登錄機碼的相對路徑**欄位中，以下列格式之一指定要取得的登錄檔金鑰的路徑：

   - 根金鑰的相對路徑，例如：

     \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

   - 根金鑰完整名稱的相對路徑，例如：

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

   - 根金鑰的縮寫（而非完整名稱）的相對路徑，例如：

     HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator

3. 如果必要，配置以下設定：

   - 在**資產**下拉清單中，變更要從中取得登錄檔金鑰的裝置。

     預設情況下，此欄位包含您先前選取核取方塊的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

     > 只有您可以對其執行回應操作的資產可供選擇。
     > 裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單的開頭，然後依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

4. 在**描述**欄位中，編寫對回應操作的描述或備注。

5. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，系統會產生 REG 檔案。該檔案包含您指定路徑下的登錄檔金鑰及其值的清單。

檢視回應操作結果

您可以透過以下方式之一檢視和下載該檔案：

- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。
- 從主功能表的回應歷史部分，或警示或事件詳情中的歷史記錄頁籤

  點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。若回應操作成功完成，則將顯示**成功**訊息和產生的檔案。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

  若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

取得NTFS元檔案

取得 NTFS 中繼檔工作僅檢索檔案的預設資料流。不支援備用（命名）資料流。

若要取得NTFS元檔案：

1. 選取NTFS 中繼檔回應動作。
   取得 NTFS 中繼檔窗格隨即開啟。
2. 在**中繼檔**欄位中，請選取您要取得之元檔案旁的核取方塊。
   - $MFT
   - $LogFile
   - $Boot
   - $Secure
   - $Extend/$UsnJrnl
3. 在**磁區**欄位中，指定要從中取得元檔案的磁碟名稱。
   預設情況下，指定了*%SystemDrive%*值。
4. 如果必要，配置以下設定：
   - 在**資產**下拉清單中，變更要從中取得元檔案的裝置。
     預設情況下，此欄位包含您先前選取的核取方塊對應的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

     僅可選擇您能夠對其執行回應操作的資產。
     裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單的開頭，然後依字母順序顯示屬於警示或事件租用戶及子租用戶的裝置。
   - 在**描述**欄位中，您可以為回應操作編寫描述或備注。
5. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，NTFS元檔案將儲存到ZIP封存檔案中。

檢視回應操作結果

您可以透過以下方式之一檢視和下載該封存檔案：

- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。
- 從主功能表的回應歷史部分，或警示或事件詳情中的歷史記錄頁籤

  點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息和取得的檔案。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

  若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

取得鑑識資訊

若要取得鑑識資訊：

1. 選取鑑證資料回應動作。

   取得鑑證資料窗格隨即開啟。

2. 在**資訊類型**部分中，選取要收集之資料類型旁的核取方塊：

   - **處理程序清單**。用於查看裝置上正在執行的進程清單。
   - **自動執行點清單**。用於查看自動執行點清單。

     該清單包括有關新增到啟動資料夾或在登錄檔的「執行」登錄檔金鑰中註冊的應用程式的資訊，以及在指定裝置啟動和使用者登入裝置上的作業系統時自動執行的應用程式。

     支援的自動執行點清單

     支援下列類型的自動執行點：

     - 登入
     - Shell
     - Office
     - 瀏覽器
     - Scheduler
     - 服務
     - 驅動程式
     - 加密
     - 偵錯器
     - COM
     - SessionManager

- 網路
- LSA
- 應用程式
- WMI
- GroupPolicy
- DriverLog
- BootLog
- Process
- OsUpdate
- 印表機
- 未指定
- OsLoader
- EfiLoader

- **檔案清單**。用於查看磁碟上儲存的檔案和資料夾清單。

> 清單中最多可顯示20,000個檔案。

3. 如果您選取了**檔案清單**核取方塊，請執行下列操作：

   a. 透過選擇下列設定群組之一來指定檔案搜尋範圍：

   - **所有本機磁碟**。該清單將包含儲存在本機磁碟所有資料夾中的檔案。
   - **資料夾**，然後在**初始資料夾**欄位中，指定檔案搜尋的起始資料夾路徑。
     清單將包含儲存在指定資料夾及其子資料夾中的檔案。

   b. 根據需要，請指定下列資料夾內檔案的搜尋條件：

   - 要包含在檔案清單中的檔案遮罩。
   - **備用資料流**選項用於在檔案清單中記錄有關備用資料流的資訊。
     切換開關預設為開啟。
   - 應用程式搜尋檔案時資料夾的最大巢狀層級。
   - 在**排除項目**欄位中，指定要禁止搜尋檔案資訊的資料夾路徑。

4. 如果必要，配置以下設定：

- 在**資產**下拉清單中，您可以變更要從中取得鑑識資訊的裝置。

預設情況下，此欄位包含您先前選取核取方塊的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

僅可選擇您能夠對其執行回應操作的資產。
裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單的開頭，然後依字母順序顯示屬於警示或事件租用戶及子租用戶的裝置。

- 在**描述**欄位中，編寫對回應操作的描述或備注。

5. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，所選資料將儲存到受密碼保護的ZIP封存檔案中。密碼被*感染了*。

檢視回應操作結果

您可以透過以下方式之一檢視和下載該封存檔案：

- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。
- 從主功能表的回應歷史部分，或從警示或事件詳情中的歷史記錄頁籤

  點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息和取得的檔案。否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

  若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

若要取得磁碟映像

若要取得磁碟映像：

1. 選擇磁碟映像檔回應動作。

   取得磁碟映像檔窗格將會開啟。

2. 在**共用網路資源的路徑**欄位中，以UNC格式指定共用網路資源的路徑。
3. 在**使用者名稱**欄位中，選擇用於存取共用網路資源的帳戶使用者名稱。

   您必須在租用戶設定中預先設定存取共用網路資源的憑證。

4. 在**磁碟類型**設定群組中，請選擇以下選項之一：

   - **邏輯**，然後在**磁區**欄位中，指定驅動器名稱，不帶冒號和斜杠，例如E或C。

     預設值是%SystemDrive%。

- **實體**，然後在**實體磁碟**欄位中，以下列格式指定磁碟路徑：
  - 對於安裝了Kaspersky Endpoint Security for Windows的裝置：\\.\PHYSICALDRIVE0、\\.\PHYSICALDRIVE1、\\.\PHYSICALDRIVE2
  - 對於安裝了Kaspersky Endpoint Security for Linux的裝置：/dev/sda

5. 如果要將磁碟映像檔案分成幾個部分，請開啟**將檔案分割為多個部分**選項，然後以GB為單位指定已儲存檔案的一個部分的最小大小。

6. 如果必要，配置以下設定：

   - 在**資產**下拉清單中，更改要從中取得磁碟映像的裝置。

     預設情況下，此欄位包含您先前選取的核取方塊對應的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

     僅可選擇您能夠對其執行回應操作的資產。
     裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單的開頭，然後依字母順序顯示屬於警示或事件租用戶及子租用戶的裝置。

   - 在**描述**欄位中，編寫對回應操作的描述或備注。

7. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，磁碟映像會儲存至 EWF 檔案。

這些檔案無法被覆蓋：如果目標資料夾中已存在同名檔案，則EWF檔案的名稱將包含一個後綴，例如Filename-1。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作的結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息以及位於共用網路資源中的記憶體磁碟映像檔的路徑。您可以複製該路徑。

否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

您無法直接從回應操作結果跳到共用網路資源。

取得記憶體傾印檔案

若要取得記憶體傾印檔案：

1. 選取已選取的記憶體傾印回應操作。

   取得記憶體傾印窗格隨即開啟。

2. 在**共用網路資源的路徑**欄位中，以UNC格式指定共用網路資源的路徑。

3. 在**使用者名稱**欄位中，選擇用於存取共用網路資源的帳戶使用者名稱。

   > 您必須在租用戶設定中預先設定存取共用網路資源的憑證。

4. 如果必要，配置以下設定：

   - 在**資產**下拉清單中，選擇要從中取得記憶體轉儲的裝置。

     預設情況下，此欄位包含您先前選取的核取方塊對應的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

     > 僅可選擇您能夠對其執行回應操作的資產。
     > 裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單的開頭，然後依字母順序顯示屬於警示或事件租用戶及子租用戶的裝置。

   - 在**描述**欄位中，編寫對回應操作的描述或備注。

5. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，磁碟映像將儲存為RAW檔案。

> 這些檔案無法被覆蓋：如果目標資料夾中已存在同名檔案，則RAW檔案的名稱將包含一個後綴，例如Filename-1。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作的結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，螢幕上會顯示**成功**訊息以及位於共用網路資源中的記憶體傾印檔案路徑。您可以複製該路徑。

否則， 將顯示**錯誤**訊息以及有關錯誤原因的資訊。

若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

您無法直接從回應操作結果跳到共用網路資源。

取得進程記憶體傾印檔案

若要取得進程記憶體傾印檔案：

1. 選取處理程序記憶體傾印回應動作。
   取得處理程序記憶體傾印窗格將會開啟。
2. 在**處理程序 ID**欄位中，指定要取得記憶體傾印檔案的進程ID。
3. 如果必要，配置以下設定：
   - 在**資產**下拉清單中，更改要取得程序記憶體轉儲的裝置。
     預設情況下，此欄位包含您先前選取的核取方塊對應的裝置名稱。您可以選擇與警示或事件無關，但屬於警示或事件租用戶（及其子租用戶）的裝置。

     僅可選擇您能夠對其執行回應操作的資產。
     裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單開頭，然後屬於警示或事件的租用戶及其子租用戶的裝置會依字母順序顯示。
   - 在**MD5 或 SHA256**欄位中，指定要取得其進程記憶體傾印檔案的檔案的雜湊值。
   - 在**描述**欄位中，編寫對回應操作的描述或備注。
4. 按一下**取得**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

回應操作完成後，進程的記憶體傾印檔案將儲存到ZIP封存檔案中。

檢視回應操作結果

您可以透過以下方式之一檢視和下載該封存檔案：

- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。
- 從主功能表的回應歷史部分，或警示或事件詳情中的歷史記錄頁籤
  點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息以及包含掃描結果的受密碼保護的ZIP封存檔案。您可以將該封存檔案下載到您的電腦。密碼如下：infected。
  否則，將顯示錯誤訊息以及錯誤原因的相關資訊。
  若要檢視啟動ID和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

掃描裝置來偵測威脅

為了防止威脅在受感染的裝置上傳播，您可以透過執行以下回應操作之一來掃描裝置來偵測威脅：

- 惡意軟體掃描
- YARA 掃描
- IOC 掃描

> 若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

您可以透過以下其中一種方式指定回應操作：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從遙測事件
  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。
- 從調查圖表中

  > 如果調查圖表已建立，則此選項可用。

- 從資產表
- 從**回應歷史**部分。
- 從YARA規則或IOC規則清單

  > 此選項適用於YARA 掃描和IOC 掃描回應操作。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從警示或事件詳情執行掃描

若要從警示或事件詳情掃描裝置：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要掃描裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要掃描裝置的事件ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 選取要掃描的裝置旁的核取方塊。
   如有必要，您可以選擇多個裝置。

4. 在**選取回應動作**下拉清單中，選擇**掃描**。

5. 在開啟的快顯表單中，選擇所需的回應操作。

從裝置詳情執行掃描

若要從裝置詳情掃描裝置：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下包含要掃描裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要掃描裝置的事件ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中選擇**檢視內容**。

4. 在**選取回應動作**下拉清單中，選擇**掃描**。

5. 在開啟的快顯表單中，選擇所需的回應操作。

從調查圖表中執行掃描

若要從調查圖表掃描裝置：

1. 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下包含要掃描裝置的事件ID。

2. 按一下**在圖表上檢視**按鈕。

3. 在開啟的調查圖中，按一下裝置名稱以開啟裝置詳細資訊。

4. 在**選取回應動作**下拉清單中，選擇**掃描**。

5. 在開啟的快顯表單中，選擇所需的回應操作。

從遙測事件執行掃描

若要從警示或事件詳情中開啟裝置時從遙測事件中掃描裝置：

1. 執行以下操作之一：
   - 在主選單中，轉到**監控→警示**部分。在**ID**列中，按一下所需警示ID的連結。
   - 在主選單中，轉到**監控→事件**部分。在**ID**列中，按一下所需事件ID的連結。
2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：
   - 按一下所需事件的名稱並選擇裝置。
   - 按一下「在威脅搜尋中找尋」按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。
3. 在**選取回應動作**下拉清單中，選擇**掃描**。
4. 在開啟的快顯表單中，選擇所需的回應操作。

若要從威脅搜尋部分開啟裝置時從遙測事件中掃描裝置：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
   事件表隨即開啟。
2. 點擊要開啟其詳情的事件名稱。
3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從開啟的下拉清單中選擇所需的回應操作。

從資產表執行掃描

若要從資產表執行掃描：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）。**
   這將開啟資產表。
2. 選取要執行回應操作的裝置旁的核取方塊。
   您可以選擇多個裝置。

   > 已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇所需的回應操作。

從回應歷史部分執行掃描

若要從回應歷史部分執行掃描：

1. 在主功能表中，轉至**監控→ 回應歷史**。
   包含所有警示和事件的回應歷史記錄的表格將開啟。
2. 在**回應**下拉清單中，選擇所需的回應操作。

從YARA規則或IOC規則清單中執行掃描

若要從YARA規則或IOC規則清單中掃描裝置：

1. 在主功能表中，轉至**規則和服務**，然後選擇下列選項之一： **YARA 規則**或**IOC 規則**。
   規則清單隨即顯示。
2. 選取要掃描的一個或多個裝置旁的核取方塊。
3. 在工具列上，按一下按鈕：
   - 若在步驟1中選擇了**YARA 規則**，則**執行 YARA 掃描**。
   - 若在步驟1中選擇了**IOC 規則**，則**執行 IOC 掃描**。
4. 在開啟的右側窗格中，配置掃描設定。

執行惡意軟體掃描

由於受管理裝置和管理伺服器之間的同步間隔，可能需要最多15分鐘才能啟動回應操作。

如有需要，您可以按一下**在 KUMA 中編輯**按鈕，以在 KUMA 主控台中編輯裝置的參數。

如果您選擇了惡意軟體掃描回應操作，請在**執行惡意軟體掃描**窗格中執行以下操作：

1. 選擇惡意軟體掃描類型：
   - **完整掃描**
     您可以切換**掃描網路磁碟機**按鈕，將網路裝置納入掃描範圍。預設情況下已停用該選項。

     完整掃描可能會降低裝置速度，因為會增加作業系統的負載。
     對於安裝了 Kaspersky Endpoint Security for Linux 12.4 版本的裝置，不支援完整掃描。
   - **關鍵區域掃描**
     如果您選擇此類型，則會掃描核心記憶體、正在執行的進程和磁碟啟動磁區。

- **自訂掃描**

  在**指定路徑**欄位中，指定要掃描的檔案路徑。如果要設定多個路徑，請點選**新增路徑**按鈕，然後指定路徑。

2. 按一下**掃描**按鈕。

所選類型的惡意軟體掃描將啟動。

如果惡意軟體掃描成功完成，螢幕上將顯示對應的訊息，並且警示或事件將顯示在警示表或事件表中，且操作狀態為**成功** 。否則，將顯示錯誤訊息，並且警示或事件將顯示**錯誤**操作狀態。

惡意軟體掃描作業完成後，您可以檢視結果。

YARA 掃描

YARA掃描是透過使用透過OSMP主控台手動下載的YARA檔案，在裝置上搜尋惡意的活動簽名。

若要執行YARA掃描，您必須具備：

- 包含內建代理程式的Kaspersky Endpoint Security已安裝在您的裝置上。
- YARA規則清單中至少包含一條規則

若要執行YARA掃描：

1. 選取YARA 掃描回應動作。

   執行 YARA 掃描窗格將會開啟。

2. 在**規則**下拉清單中，選擇一個或多個YARA規則。

   您可以輸入規則名稱或規則名稱中的字元序列。

   > 最多可指定200條規則。

3. 在**掃描範圍**視窗中，執行以下操作：

   a. 選擇此選項並指定其必填參數：

   - **RAM**，用於掃描在執行回應操作時正在執行的進程。

     預設選取此選項，並且在**掃描**欄位，**所有處理程序**選項也已選取。

     若要掃描特定進程，請在**掃描**設定群組中，選擇**特定處理程序**選項，然後輸入要掃描的一個或多個進程的名稱。否則，將掃描所有進程。

     > 應用程式不會掃描低優先順序的進程。

   - **自動執行點**掃描從**鑑證資料**回應操作中取得的自動執行點。

然後指定掃描類型：

- **快速掃描**。掃描所有自動運行點，但不包含COM物件。
- **完整掃描**。掃描所有自動運行點及其相關檔案。

支援的自動執行點清單

支援下列類型的自動執行點：

- 登入
- Shell
- Office
- 瀏覽器
- Scheduler
- 服務
- 驅動程式
- 加密
- 偵錯器
- COM
- SessionManager
- 網路
- LSA
- 應用程式
- WMI
- GroupPolicy
- DriverLog
- BootLog
- Process
- OsUpdate
- 印表機
- 未指定

- OsLoader
- EfiLoader

- **所有本機磁碟**，用於掃描本機磁碟上所有資料夾中儲存的檔案。

  > 掃描所有本機磁碟可能會導致裝置負載過高。

- **指定目錄**，用於掃描指定資料夾及其所有巢狀資料夾中的檔案。

  您必須在對應的欄位中指定目錄的完整路徑，並在末端附加遮罩*以包含子目錄，例如 `C:\Users\Administrator\Desktop\*`。

b. 根據需要，請在對應的欄位中，為所選選項指定以下參數：

- **最大掃描持續時間（小時）**

  預設值是 23。指定時間過後，即使某些規則未套用於掃描裝置，掃描也會停止。回應操作結果包含掃描停止時最新的資料。

- **排除項目**

  指定要從掃描中排除的進程的簡稱或檔案遮罩。如果裝置上運行著多個同名進程，應用程式會將所有此類進程從掃描中排除。

4. 如果必要，配置以下設定：

- 指定租用戶。

  如果您從YARA規則清單中執行回應操作，並選擇了屬於不同租用戶的規則，則**租用戶**欄位為空。您必須手動指定要對其裝置執行YARA掃描的租用戶。

- 更改回應操作的範圍。

  預設情況下，在設定的**範圍**群組中，會選取**特定資產**選項，而**資產**下拉清單則包含您先前選取其核取方塊的裝置名稱。YARA掃描將在這些裝置上執行。

  您可以更改要掃描的裝置，或在設定的**範圍**群組中選擇**所有資產**選項，以掃描屬於警示或事件租用戶（及其子租用戶）的所有裝置。

  > 僅可選擇您能夠對其執行回應操作的資產。
  > 裝置顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單的開頭，然後依字母順序顯示屬於警示或事件租用戶及子租用戶的裝置。

- 在**描述**欄位中，編寫對回應操作的描述或備注。

5. 按一下**執行**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

在**資產**直欄中，您必須按一下已啟動YARA掃描的資產數量對應的連結。在開啟的視窗中，選取**結果**頁籤，您可以查看每個YARA規則的掃描狀態。如果掃描偵測到威脅，則會建立相應的警示。您可以從回應操作結果跳到警示。

如果回應操作失敗，則會顯示**錯誤**訊息以及有關錯誤原因的資訊。

IOC 掃描

IOC掃描使用透過OSMP主控台手動下載的IOC檔案（入侵指標檔案）來搜尋裝置上是否有定向攻擊的跡像以及已感染和可能已感染的物件。

若要執行IOC掃描，您必須具備：

- 包含內建代理程式的Kaspersky Endpoint Security已安裝在您的裝置上。
- IOC規則清單中至少包含一條規則

若要執行IOC掃描：

1. 選擇IOC 掃描回應操作。

   執行 IOC 掃描窗格隨即開啟。

2. 在**規則**欄位中，選擇一個或多個IOC規則。

3. 如果必要，配置以下設定：

   - 指定租用戶。

     如果您從IOC規則清單中執行回應操作，並選擇了屬於不同租用戶的規則，則**租用戶**欄位為空。您必須手動指定要對其裝置執行IOC掃描的租用戶。

   - 更改回應操作的範圍。

     預設情況下，在設定的**範圍**群組中，會選取**特定資產**選項，而**資產**下拉清單則包含您先前選取其核取方塊的裝置名稱。這意味著將對這些裝置執行IOC掃描。

     您可以更改要掃描的裝置，或在設定的**範圍**群組中選擇**所有資產**選項，以掃描屬於警示或事件租用戶（及其子租用戶）的所有裝置。

     僅可選擇您能夠對其執行回應操作的資產。
     裝置的顯示方式如下：屬於警示或事件的裝置會置於**資產**下拉清單開頭，然後依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

- 在**最大掃描持續時間（小時）**欄位中，指定最大掃描持續時間。

  預設值是 23。指定時間過後，即使某些規則未套用於掃描裝置，掃描也會停止。回應操作結果包含掃描停止時最新的資料。

- 在**描述**欄位中，編寫對回應操作的描述或備注。

4. 按一下**執行**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

在**資產**直欄中，您必須按一下顯示已啟動IOC 掃描的資產數量的連結。在開啟的視窗中，選取**結果**頁籤，您可以檢視每個IOC規則的掃描狀態。如果掃描偵測到威脅，則會建立相應的警示。您可以從回應操作結果跳到警示。

如果回應操作失敗，則會顯示錯誤訊息及錯誤原因的相關資訊。

掃描從裝置取得的文件

從裝置或隔離目錄中取得檔案後，您可以掃描該檔案是否有威脅。

若要執行回應操作，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

您可以透過以下其中一種方式執行檔案掃描：

- 執行檔案回應操作時。

  掃描檔案選項預設為啟用。詳情請參閱取得檔案一文。

- 在主功能表的**儲存區 → 隔離**區段中，按一下**獲取並掃描**按鈕。

  如果包含內建代理的Kaspersky Endpoint Security已安裝在您的裝置上，則可以使用此選項。

- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。

  該選項適用於由於**檔案**或檔案回應操作而放置到獲取檔案部分的檔案，以及您手動上傳的檔案。

- 從以下回應操作的結果：
  - 檔案
  - 獲取檔案
  - 移動到隔離區

從檔案部分或頁籤執行掃描

若要從檔案部分或頁籤執行掃描：

1. 在主功能表中，執行以下操作之一：
   - 轉至**儲存區 → 檔案**。
   - 轉至**監控**，然後選擇**警示**或**事件**部分。在**ID**直欄中，按一下包含因取得檔案和從隔離區取得檔案回應操作而取得的檔案的警示或事件的ID。在開啟的警示或事件詳情中，轉至**檔案**頁籤。
2. 在開啟的視窗中，執行以下其中一項操作：
   - 選取所需檔案旁的核取方塊，然後在工具列中，按一下**掃描**按鈕。
   - 按一下檔案名稱，然後在開啟的檔案詳情窗格中，按一下**掃描**按鈕。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從其他回應操作的結果執行掃描

若要從其他回應操作的結果執行掃描：

1. 在主功能表中，執行以下操作之一：
   - 轉至**監控 → 回應歷史**。
   - 轉至**監控**，然後選擇**警示**或**事件**部分。在**ID**直欄中，點按您執行取得檔案、從隔離區取得檔案或將檔案移動到隔離區回應操作的警示或事件的ID。在開啟的警示或事件視窗中，轉到**歷史記錄**頁籤，然後選擇**回應歷史**頁籤以顯示事件清單。
2. 在**動作狀態**直欄中，點按要檢視所需回應操作結果的事件的**成功**狀態連結。
3. 在開啟的右側窗格中，按一下包含檔案名稱的連結。
   檔案詳情窗格隨即開啟。
4. 在工具列上，按一下**掃描**按鈕。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視檔案掃描結果

您可以透過以下方式之一檢視該檔案掃描結果：

- 從主功能表的**檔案**部分，或警示或事件詳情中的**檔案**頁籤。
- 從主功能表的**回應歷史**部分，或警示或事件詳情中的**歷史記錄**頁籤

  點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息以及包含掃描結果的受密碼保護的ZIP封存檔案。您可以將該封存檔案下載到您的電腦。密碼如下：infected。

  否則，將顯示錯誤訊息以及錯誤原因的相關資訊。

  若要檢視**啟動 ID**和包含回應操作結果的JSON，請轉至**偵錯資料**頁籤。

刪除檔案

若要執行**刪除檔案**回應操作，您必須具備：

- 下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。
- 包含內建代理程式的Kaspersky Endpoint Security已安裝在您的裝置上。

您可以透過以下其中一種方式指定回應操作：

- 從警示或事件詳細資訊
- 從裝置詳細資訊
- 從遙測事件

  您可以從警示或事件詳情中開啟事件詳情，也可以從**威脅搜尋**部分開啟事件詳情。
- 從調查圖表中

  > 如果調查圖表已建立，則此選項可用。

- 從資產表
- 從**回應歷史**部分。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

從警示或事件詳細資訊回應

若要從警示或事件詳細資訊進行回應：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的事件 ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

   > 您也可以轉至**可觀察物件**頁籤，選取要刪除檔案旁的核取方塊，然後按一下**刪除檔案**按鈕。

3. 選中要刪除檔案所在的裝置旁邊的核取方塊。
   您可以選擇多個裝置。

4. 在**選取回應動作**下拉清單中，選擇**刪除檔案**。

5. 在開啟的右側窗格中，執行以下操作：

   - 在**完整路徑**欄位中，指定要取得的檔案完整路徑。
   - 在**資產**下拉清單中，選擇檔案所在的裝置。
     如果在步驟2中選擇了**資產**頁籤，則預設情況下，您選取的核取方塊對應的裝置名稱會顯示在**資產**欄位中。
     您可以更改裝置，或在設定的**所有資產**群組中選擇**範圍**選項，以對屬於警示或事件租用戶（及其子租用戶）的所有裝置執行回應操作。

     > 僅可選擇您能夠對其執行回應操作的資產。
     > 裝置顯示如下：屬於警示或事件的裝置會列於**資產**下拉清單的開頭，接著依字母順序顯示屬於警示或事件租用戶及其子租用戶的裝置。

   - 如有必要，請在相應的欄位中配置以下設定：
     - 指定檔案的SHA256或MD5雜湊值。

       > 如果在步驟2中選擇了**可觀察物件**頁籤，則會自動指定雜湊值。您可以變更該值。

     - 為回應操作編寫描述或註釋。

6. 點擊**刪除**按鈕。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從裝置詳細資訊回應

若要從裝置詳細資訊進行回應：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的事件 ID。

2. 在開啟的視窗中，請轉至**資產**頁籤。

3. 按一下所需裝置的名稱，然後在下拉清單中，選擇**檢視內容**。

4. 執行*與從警示或裝置詳情進行回應*第4-6步中所述的相同操作。

   窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從遙測事件回應

若要從警示或事件詳情開啟遙測事件時回應該事件：

1. 執行以下操作之一：

   - 在主選單中，轉到**監控→警示**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的警示ID。
   - 在主選單中，轉到**監控→事件**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的事件 ID。

2. 在開啟的視窗中，轉至**詳細資訊**頁籤，然後執行下列其中一項操作：

   - 按一下所需事件的名稱並選擇裝置。
   - 按一下**在威脅搜尋中找尋**按鈕，以轉至**威脅搜尋**部分並選擇所需的裝置。

3. 執行*與從警示或裝置詳情進行回應*第4-6步中所述的相同操作。

   窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

若要從威脅搜尋部分開啟遙測事件時對其進行回應：

1. 在主功能表中，轉至**監控 → 威脅搜尋。**
   事件表隨即開啟。

2. 點擊要開啟其詳情的事件名稱。

3. 在開啟的事件詳情視窗中，按一下裝置名稱，然後從下拉清單中選擇**刪除檔案**。

4. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從調查圖表回應

若要從調查圖表掃描裝置：

1. 在主選單中，轉到**監控→事件**部分。在**ID**直欄中，按一下包含要刪除檔案的裝置的事件 ID。

2. 按一下**在圖表上檢視**按鈕。

3. 在開啟的調查圖中，按一下裝置名稱以開啟裝置詳細資訊。

4. 在**選取回應動作**下拉清單中，選擇**刪除檔案**。

5. 執行與*從警示或裝置詳情進行回應*第5-6步中所述的相同操作。

如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從資產表進行回應

若要從資產表中進行回應：

1. 在主功能表中，轉至**資產管理 → 資產（裝置）**。
這將開啟資產表。

2. 選取要執行回應操作的裝置旁的核取方塊。
您可以選擇多個裝置。

> 已存檔的裝置無法選擇。

3. 在**選取回應動作**下拉清單中，選擇**刪除檔案**。

4. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

從回應歷史部分回應

若要從回應歷史部分執行回應操作：

1. 在主功能表中，轉至**監控→ 回應歷史**。
   包含所有警示和事件的回應歷史記錄的表格將開啟。
2. 在**回應**下拉清單中，選取**刪除檔案**。
3. 在開啟的右側窗格中，依照*從警示或事件詳情進行回應*步驟5-6所述設定回應操作設定。

窗格隨即關閉。如果回應操作成功完成，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

檢視回應操作結果

您可以透過以下方式之一檢視回應操作的結果：

- 從主功能表中的回應歷史區段
- 從警示或事件詳細資料中的歷史記錄頁籤

點按**動作狀態**直欄中的連結後，視窗將開啟並選中**結果**頁籤。如果回應操作成功完成，則會顯示**成功**訊息。否則，將顯示錯誤訊息以及錯誤原因的相關資訊。

若要檢視啟動 ID和包含回應操作結果的 JSON，請移至**偵錯資料**頁籤。

如果檔案已被其他程序阻止，則結果將顯示為**成功**狀態，但檔案只有在裝置重新啟動後才會被刪除。建議重新啟動裝置後檢查檔案是否已成功刪除。

透過Active Directory進行回應

您可以將Kaspersky Next XDR Expert與您組織中使用的Active Directory服務整合。在設定Active Directory和KUMA之間的整合後，Active Directory被視為與Kaspersky Next XDR Expert整合。

設定Kaspersky Next XDR Expert和Active Directory之間的整合的過程包括設定與LDAP的連線。您必須為每個租用戶單獨設定與LDAP的連線。

因此，如果發生警示或事件，您將能夠針對該租用戶的關聯使用者執行回應操作。

您可以透過下列方式之一透過Active Directory執行回應操作：

- 從警示或事件詳細資訊中
- 從遙測事件中（如果從警示詳情中開啟它）。

- 從調查圖表中

  如果調查圖表已建立，則此選項可用。

您也可以設定在建立或編輯常規程式時自動執行的回應操作。

若要透過Active Directory執行回應操作，您必須具備下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要透過Active Directory執行回應操作：

1. 在主功能表中，轉至**監控**，然後選擇**警示**或**事件**部分。

   如果要從遙測事件回應，請選擇**警示**部分。

   如果要從調查圖表回應，請選擇**事件**部分。

2. 按一下所需警示或事件的ID。

3. 在開啟的視窗中，執行以下操作之一：

   - 如果要透過警示或事件詳細資訊進行回應，請轉至**資產**頁籤，然後按一下使用者的名稱。
   - 如果要透過遙測事件進行回應，轉至**詳細資訊**頁籤，然後按一下所需事件的名稱，然後選擇使用者；或按一下**在威脅搜尋中找尋**按鈕，轉至**威脅搜尋**部分，然後選取所需的使用者。
   - 如果您想透過調查圖表進行回應，請按一下**在圖表上檢視**按鈕。在開啟的視窗中，按一下使用者的名稱。

   帳戶詳細資訊視窗將在螢幕右側開啟。

4. 在**透過 Active Directory 回應**下拉清單中，選擇要執行的操作：

   - **鎖定帳戶**

     如果使用者帳戶因相關警示或事件而被鎖定，則螢幕上會顯示對應的訊息。否則，會顯示錯誤訊息。

   - **重設密碼**

     如果使用者帳戶密碼因相關警示或事件而重置，則螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

   - **將使用者新增至安全群組**

     在開啟的視窗中，在必填欄位**安全群組 DN**中，指定要新增使用者的安全群組的完整路徑。CN = Team, OU = Groups, OU = ExchangeObjects, DC = example, DC = com.按一下**新增**按鈕。一次運作只能指定一個群組。

     如果使用者因相關警示或事件而被加入到安全群組，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

   - **將使用者從安全群組中刪除**

     在開啟的視窗中，在必填欄位**安全群組 DN**中，指定要從中刪除使用者的安全群組的完整路徑。例如，CN = Team、OU = Groups、OU = ExchangeObjects、DC = example、DC = com。點擊**刪除**按鈕。一次運作只能指定一個群組。

     如果使用者因相關警示或事件而被從安全群組中刪除，螢幕上會顯示對應的訊息。否則，將顯示錯誤訊息。

使用協力廠商指令碼進行回應

本章節包含您可以透過在遠端用戶端裝置上啟動協力廠商指令碼，經由外部系統執行的回應操作。

為此，您必須：

- 設定Kaspersky Next XDR Expert與指令碼啟動服務之間的整合。
- 建立一個常規程式，用於啟動回應指令碼。
- 下載指令碼，然後按照本章節提供的說明使用它。

透過UserGate進行回應

UserGate包含統一威脅管理解決方案的功能，並為您的本機網路提供以下防護：

- 防火牆
- 入侵和攻擊防護
- 防毒流量病毒掃描
- 應用程式控制

支援UserGate UTM API 7版本。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過UserGate回應警示和事件。您可以透過點擊此連結來檢視fix_tablespace.sql指令碼：

下載指令碼

存取UserGate的登入名稱和密碼儲存在ug.py指令碼中。您可以在此指令碼中變更*端點*、*登入名稱*和*密碼*值。

執行指令碼需要Python 3.12及更高版本。

若要透過UserGate執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

您可以建立將透過UserGate執行以下回應操作的常規程式：

- 封鎖IP位址、URL和網域名稱。

  UserGate將在常規程式啟動後封鎖IP位址、URL和網域名稱。

- 登出使用者。

  所有登入UserGate的使用者都將在常規程式啟動後登出。

若要啟動透過UserGate回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過UserGate回應的常規程式。
3. 按一下**啟動**按鈕。
   所選常規程式將啟動透過UserGate進行回應的指令碼。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過Ideco NGFW進行回應

Ideco NGFW是一種解決方案，可充當企業和私人網路中網路流量的篩選器。如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務的整合，它允許您封鎖Kaspersky Next XDR Expert偵測到的IP位址和URL。

支援Ideco NGFW 16.0或更高版本。

存取Ideco NGFW的登入名稱和密碼儲存在指令碼中，以便與Ideco NGFW整合。您可以點擊以下連結下載指令碼：

下載指令碼

若要使用指令碼：

1. 以下列其中一種方式安裝指令碼：
   - 例如，透過pip：
     ```
     pip install -r requirements.txt
     ```
   - 例如，從WHL檔案：
     ```
     pip install ./dist/kaspersky_xdr_ideco_integration-<version>-py3-none-any.whl
     ```
   - 離線安裝。
     如果您無法存取網際網路，則必須離線安裝指令碼。在這種情況下，請執行以下操作：
     a. 透過執行以下命令在可存取網路的電腦上下載依賴項：
        ```
        pip download -r requirements.txt
        ```
     b. 將下載的依賴項移至您將執行指令碼的裝置上。
     c. 使用下列命令安裝依賴項：
        ```
        pip install --no-index --find-links <folder_path_to_downloaded_dependencies> -r requirements.txt
        ```
2. 以下列其中一種方式設定指令碼：
   - 例如，透過ENV檔案：

```
cp .env.sample .env
nano .env
```

- 在指令碼（ideco.py）的主體中，編輯下列字串中的參數：

```
BASE_URL: str = getenv("BASE_URL", "https://your-ip:your-port")
LOGIN: str = getenv("LOGIN", "your-login")
PASSWORD: str = getenv("PASSWORD", "your-password")
IP_DENY_LIMIT: int = int(getenv("IP_DENY_LIMIT", 1000))
```

3. 為Kaspersky Next XDR Expert檢測到的IP地址和惡意URL新增封鎖規則。

若要新增將封鎖IP位址的防火牆規則：

1. **使用add_firewall_rule命令執行指令碼**。

   此命令具有以下邏輯：

   1. 檢查Ideco NGFW物件清單中是否存在IP位址。
      如果存在，則不會新增目前IP位址。
      如果不存在，則會新增目前IP位址。

   2. 檢查名稱為 XDR 的 IP 位址清單是否存在。
      如果該清單存在，則重複使用該清單，並將IP位址新增至其中。
      如果該清單不存在，則建立一個新清單，並將IP位址新增至其中。

   3. 檢查名稱為 XDR 的防火牆規則是否存在。
      如果防火牆規則存在，則重複使用該規則，並將步驟2中的IP位址清單新增至其中。
      如果防火牆規則不存在，則建立新的防火牆規則，並將步驟2中的IP位址清單新增至其中。

2. 請指定要封鎖的IP位址。

   > 預設情況下，IP位址的最大數量為1000。您可以編輯此值，如步驟2*設定指令碼*中所述。

   您必須新增一個有效的IPv4位址，以逗號分隔且不帶空格，例如：

   ```
   python ideco.py add_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
   ```

   所選IPv4地址的拒絕規則隨即新增。

若要新增將封鎖惡意URL的篩選規則：

1. **使用add_content_filter_file命令執行指令碼**。

   此命令具有以下邏輯：

   1. 檢查名稱為 XDR 的類別是否存在。
      如果存在，則將URL新增至此類別。
      如果不存在，則建立一個新類別，然後將URL新增至其中。

   2. 檢查名稱為 XDR 的內容篩選規則是否存在。

如果內容篩選規則存在，則將步驟1中的類別新增至其中。

如果不存在，則建立新的內容篩選規則，然後將步驟1中的類別新增至其中。

2. 指定要封鎖的URL。

URL必須以逗號分隔，並以http://或https://前綴表示，例如：

```
python ideco.py add_content_filter_rule --url "https://url_1.com, http://url_2.com.uk,
http://qwerty.nl, http://zxc.xc"
```

指定URL的拒絕規則隨即新增。

透過Ideco UTM進行回應

Ideco UTM是一種為您的企業網路提供以下保護措施的解決方案：

- 防火牆 — 篩選網路流量，以保護網路免受未經授權的存取。
- 入侵和攻擊防護 — 識別和封鎖可疑操作，以確保系統完整性。
- 防毒流量病毒掃描 — 防禦惡意軟體和惡意的活動。
- 應用程式控制 — 封鎖或限制執行未經授權的應用程式。
- 網頁篩選 — 限制使用者造訪您認為不需要的網站以提升協助工具體驗。

現支援Ideco UTM 15.7.35。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過Ideco UTM回應警示和事件。啟動常規程式後，Ideco UTM將根據您建立常規程式時指定的操作，封鎖IP位址、IP位址範圍或URL。

若要解除已封鎖IP位址、IP位址範圍或URL的封鎖，您需要建立並啟動另一個常規程式。

您可以透過點擊此連結來下載指令碼：

下載指令碼

存取Ideco UTM的登入名稱和密碼儲存在env.sample組態檔中。您需要將此檔案中的資訊複製到您建立的新ENV檔案中，然後在新檔案中指定必要的參數。

執行指令碼需要Python 3.10。

若要透過Ideco UTM執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要啟動透過Ideco UTM回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過Ideco UTM回應的常規程式。
3. 按一下**啟動**按鈕。
   所選常規程式將啟動透過Ideco UTM進行回應的指令碼。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過Redmine進行回應

Redmine是一個用於管理專案和追蹤問題的網頁應用程式。如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，則它允許您使用指令碼自動執行處理Redmine專案中的問題。

點擊該連結下載指令碼：

下載指令碼

若要使用指令碼：

1. 以下列其中一種方式安裝指令碼：
   - 例如，透過pip：
     ```
     pip install -r requirements.txt
     ```
   - 例如，從WHL檔案：
     ```
     pip install ./dist/kaspersky_xdr_redmine_integration-1.0-py3-none-any.whl
     ```
   - 離線安裝。
     如果您無法存取網際網路，則必須離線安裝指令碼。在這種情況下，請執行以下操作：
     a. 在可存取網際網路的電腦上使用以下命令下載相依性：
        ```
        pip download -r requirements.txt
        ```
     b. 將下載的依賴項移至您將執行指令碼的裝置上。
     c. 使用以下命令安裝依賴項：
        ```
        pip install --no-index --find-links <folder_path_to_downloaded_dependencies> -r
        requirements.txt
        ```
2. 以下列其中一種方式設定指令碼：
   - 例如，透過ENV檔案：
     ```
     cp .env.sample .env
     nano .env
     ```
   - 在指令碼（redmine.py）的主體中，編輯以下字串中的參數：

```
REDMINE_URL: str = getenv("REDMINE_URL", "http://<ip_or_hostname>")
REDMINE_PORT: str = getenv("REDMINE_PORT", "8080")
REDMINE_API_KEY: str = str(getenv("REDMINE_API_KEY", "<redmine_api_key>"))
```

您可以使用該指令碼處理Redmine中的問題。

- 如果您要建立新問題，請執行以下命令：

  ```
  python redmine.py create_issue "project-identifier" "Issue subject" --description
  "Issue description text" --priority_id <id: int>
  ```

  結果：

  ```
  {"issue_id": 57}
  ```

- 如果您想要更新問題，請執行以下命令：

  ```
  python redmine.py update_issue <issue_id: int> --subject "Subject text to be updated"
  --description "Description text to be updated" --priority_id <id: int>
  ```

  結果：

  ```
  {"status": "issue_updated"}
  ```

- 如果您想要取得問題，請執行以下命令：

  ```
  python redmine.py get_issue <issue id: int>
  ```

  結果：

  ```
  {
  "subject": "86",
  "description": "18",
  "project_name": "Test project",
  "author_name": "Redmine Admin",
  "status_name": "backlog",
  "priority_name": "high",
  "start_date": "24.07.2023",
  "due_date": null,
  "created_on": "24.07.2023 10:56:15",
  "updated_on": "24.07.2023 17:18:38"
  }
  ```

透過Check Point NGFW進行回應

Check Point NGFW是一種解決方案，可充當企業網路中網路流量的篩選器。與Check Point NGFW整合可讓您封鎖Kaspersky Next XDR Expert偵測到的IP位址和URL。

Check Point NGFW包含統一威脅管理解決方案的功能，並為您的本機網路提供以下防護措施：

- 防火牆 — 篩選網路流量，以保護網路免受未經授權的存取。
- 入侵和攻擊防護 — 識別和封鎖可疑操作，以確保系統完整性。
- 防毒流量病毒掃描 — 防禦惡意軟體和惡意的活動。

- 應用程式控制 — 封鎖或限制執行未經授權的應用程式。
- 網頁篩選 — 限制使用者造訪您認為不需要的網站以提升協助工具體驗。

現支援Check Point NGFW R81.20或更高版本。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過Check Point NGFW回應警示和事件。若要解除已封鎖的IP位址或URL的封鎖，您需要建立並啟動另一個常規程式。

執行指令碼需要Python 3.12及更高版本。

若要透過Check Point NGFW執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

您可以點擊以下連結下載回應指令碼：

下載指令碼

用於存取 Check Point NGFW 的登入帳戶與密碼儲存於 `.envSample` 檔案中。

若要使用指令碼：

1. 以下列其中一種方式安裝指令碼：
   - 例如，透過pip：
     ```
     pip install -r requirements.txt
     ```
   - 離線安裝。
     如果您無法存取網際網路，則必須離線安裝指令碼。在這種情況下，請執行以下操作：
     a. 透過執行以下命令在可存取網路的電腦上下載依賴項：
        ```
        pip download -r requirements.txt
        ```
     b. 將下載的依賴項移至您將執行指令碼的裝置上。
     c. 使用下列命令安裝依賴項：
        ```
        pip install --no-index --find-links <folder_path_to_downloaded_dependencies> -r
        requirements.txt
        ```
2. 以下列其中一種方式設定指令碼：
   - 例如，透過ENV檔案：
     ```
     cp .env.sample .env
     nano .env
     ```
   - 在指令碼（main.py）的主體中，編輯以下字串中的參數：
     ```
     BASE_IP: str = getenv("BASE_IP", "your-ip")
     ```

```
BASE_PORT: str = getenv("BASE_PORT", "your-port")
LOGIN: str = getenv("LOGIN", "your-login")
PASSWORD: str = getenv("PASSWORD", "your-password")
```

3. 為Kaspersky Next XDR Expert檢測到的IP地址和惡意URL新增封鎖規則。

若要新增將封鎖IP位址的防火牆規則：

1. **使用add_firewall_rule命令執行指令碼**。

   此命令具有以下邏輯：

   1. 檢查Check Point NGFW物件清單中是否存在IP位址。
      如果存在，則不會新增目前IP位址。
      如果不存在，則會新增目前IP位址。

   2. 檢查名稱為 XDR 的 IP 位址清單是否存在。
      如果該清單存在，則重複使用該清單，並將IP位址新增至其中。
      如果該清單不存在，則建立一個新清單，並將IP位址新增至其中。

   3. 檢查名稱為 XDR 的防火牆規則是否存在。
      如果防火牆規則存在，則重複使用該規則，並將步驟2中的IP位址清單新增至其中。
      如果防火牆規則不存在，則建立新的防火牆規則，並將步驟2中的IP位址清單新增至其中。

2. 請指定要封鎖的IP位址。

   > 預設情況下，IP位址的最大數量為1000。您可以編輯此值，如上一步第2步*設定指令碼*中所述。

   您必須新增一個有效的IPv4位址，以逗號分隔且不帶空格，例如：

   ```
   python main.py add_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
   ```

   所選IPv4地址的拒絕規則隨即新增。

若要刪除封鎖IP位址的防火牆規則：

1. **使用delete_firewall_rule命令執行指令碼**。

   此命令具有以下邏輯：

   1. 檢查Check Point NGFW物件清單中是否存在IP位址。
      如果存在，則不會新增目前IP位址。
      如果不存在，則會新增目前IP位址。

   2. 檢查名稱為 XDR 的 IP 位址清單是否存在。
      如果該清單存在，則重複使用該清單，並將IP位址新增至其中。
      如果該清單不存在，則建立一個新清單，並將IP位址新增至其中。

   3. 檢查名稱為 XDR 的防火牆規則是否存在。
      如果防火牆規則存在，則重複使用該規則，並將步驟2中的IP位址清單新增至其中。

如果防火牆規則不存在，則建立新的防火牆規則，並將步驟2中的IP位址清單新增至其中。

2. 請指定要封鎖的IP位址。

> 預設情況下，IP位址的最大數量為1000。您可以編輯此值，如上一步第2步*設定指令碼*中所述。

您必須新增一個有效的IPv4位址，以逗號分隔且不帶空格，例如：

```
python main.py delete_firewall_rule --ip_address "12.12.12.12, 13.13.13.13"
```

所選IPv4地址的封鎖規則隨即刪除。

若要新增將封鎖惡意URL的篩選規則：

1. **使用add_content_filter_file命令執行指令碼**。

此命令具有以下邏輯：

1. 檢查名稱為 XDR 的類別是否存在。
   如果存在，則將URL新增至此類別。
   如果不存在，則建立一個新類別，然後將URL新增至其中。

2. 檢查名稱為 XDR 的內容篩選規則是否存在。
   如果內容篩選規則存在，則將步驟1中的類別新增至其中。
   如果不存在，則建立新的內容篩選規則，然後將步驟1中的類別新增至其中。

2. 指定要封鎖的URL。

URL必須以逗號分隔，並以http://或https://前綴表示，例如：

```
python main.py add_content_filter_rule --url "https://url_1.com, http://url_2.com.uk,
http://qwerty.nl, http://zxc.xc"
```

指定URL的拒絕規則隨即新增。

若要刪除封鎖惡意URL的篩選規則：

1. **使用delete_content_filter_file命令執行指令碼**。

此命令具有以下邏輯：

1. 檢查名稱為 XDR 的類別是否存在。
   如果存在，則將URL新增至此類別。
   如果不存在，則建立一個新類別，然後將URL新增至其中。

2. 檢查名稱為 XDR 的內容篩選規則是否存在。
   如果內容篩選規則存在，則將步驟1中的類別新增至其中。
   如果不存在，則建立新的內容篩選規則，然後將步驟1中的類別新增至其中。

2. 指定要封鎖的URL。

URL必須以逗號分隔，並以http://或https://前綴表示，例如：

```
python main.py delete_content_filter_rule --url "https://url_1.com,
http://url_2.com.uk, http://qwerty.nl, http://zxc.xc"
```

指定URL的封鎖規則隨即刪除。

若要啟動透過Check Point NGFW回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過Check Point NGFW回應的常規程式。
3. 按一下**啟動**按鈕。
   所選常規程式將啟動透過Check Point NGFW進行回應的指令碼。
   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳情的**歷程記錄**頁籤上找到。

透過Sophos防火牆進行回應

Sophos防火牆是一種為您的企業網路提供以下保護措施的解決方案：

- 防火牆 — 篩選網路流量，以保護網路免受未經授權的存取。
- 入侵和攻擊防護 — 識別和封鎖可疑操作，以確保系統完整性。
- 防毒流量病毒掃描 — 防禦惡意軟體和惡意的活動。
- 應用程式控制 — 封鎖或限制執行未經授權的應用程式。
- 網頁篩選 — 限制使用者造訪您認為不需要的網站以提升協助工具體驗。

現支援Sophos防火牆19.5。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過Sophos防火牆回應警示和事件。啟動常規程式後，Sophos防火牆將根據您在建立常規程式時指定的操作，封鎖IP位址、IP位址範圍或URL。

若要解除已封鎖IP位址、IP位址範圍或URL的封鎖，您需要建立並啟動另一個常規程式。

您可以透過點擊此連結來下載指令碼：

下載指令碼

存取Sophos防火牆的登入名稱和密碼儲存在env.sample組態檔中。您需要將此檔案中的資訊複製到您建立的新ENV檔案中，然後在新檔案中指定必要的參數。

執行指令碼需要Python 3.10。

若要透過Sophos防火牆執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要啟動透過Sophos防火牆回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過Sophos防火牆回應的常規程式。
3. 按一下**啟動**按鈕。

   所選常規程式將啟動透過Sophos防火牆進行回應的指令碼。

   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過Continent 4進行回應

Continent 4是一種為您的企業網路提供以下保護措施的解決方案：

- 防火牆 — 篩選網路流量，以保護網路免受未經授權的存取。
- 入侵和攻擊防護 — 識別和封鎖可疑操作，以確保系統完整性。
- VPN閘道 — 建立安全隧道，用於在您組織的網路之間傳輸資料。
- 存取控制 — 根據安全規則和政策管理使用者對內部和外部網路資源的存取。
- 資料加密 — 使用加密演算法保護傳輸的資料。

現支援Continent 4.1.7。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過Continent 4回應警示和事件。

您可以建立將透過Continent 4執行以下回應操作的常規程式：

- 封鎖IP位址和URL。

  Continent 4將封鎖IP位址和URL。若要解除已封鎖的IP位址或URL的封鎖，您需要建立並啟動另一個常規程式。

- 封鎖入侵指標（以下簡稱IoC）。

  Continent 4將封鎖您在常規程式觸發器中指定的可觀察物件。

您可以透過點擊此連結來下載指令碼：

下載指令碼

存取Continent 4的登入名稱和密碼儲存在env.sample組態檔中。您需要將此檔案中的資訊複製到您建立的新ENV檔案中，然後在新檔案中指定必要的參數。

執行指令碼需要Python 3.10。

若要透過Continent 4執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要啟動透過Continent 4回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過Continent 4回應的常規程式。
3. 按一下**啟動**按鈕。

   所選常規程式將啟動透過Continent 4進行回應的指令碼。

   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過SKDPU NT進行回應

SKDPU NT是一種特權帳戶管理解決方案。

現支援SKDPU NT 7.0.4版本。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過SKDPU NT回應警示和事件。

您可以建立將透過SKDPU NT執行以下回應操作的常規程式：

- 終止使用者會話。當偵測到可疑活動或違反安全規則時，常規程式將終止使用者的所有會話。
- 封鎖使用者帳戶。常規程式將封鎖使用者帳戶並限制使用者對系統的存取。
- 撤銷使用者權限。使用者將被從特權使用者群組中移除，並且使用者的權限將被撤銷。

您可以透過點擊此連結來下載指令碼：

下載指令碼

存取SKDPU NT的登入名稱和密碼儲存在env.sample組態檔中。您需要將此檔案中的資訊複製到您建立的新ENV檔案中，然後在新檔案中指定必要的參數。

執行指令碼需要Python 3.10。

若要透過SKDPU NT執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要啟動透過SKDPU NT回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過SKDPU NT回應的常規程式。
3. 按一下**啟動**按鈕。

   所選常規程式將啟動透過SKDPU NT進行回應的指令碼。

   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過FortiGate進行回應

FortiGate是一種為您的企業網路提供以下保護措施的解決方案：

- 防火牆 — 篩選網路流量並防止未經授權的存取；
- 入侵和攻擊防護 — 識別並封鎖可疑操作；
- 網頁篩選 — 限制使用者存取您認為不適宜的網站；
- 惡意軟體防護 — 防止惡意軟體感染；
- 電子郵件篩選——封鎖垃圾郵件和可疑郵件。

現支援FortiGate 7.6.0版本。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過FortiGate回應警示和事件。執行常規程式後，FortiGate將根據您建立常規程式時指定的操作，封鎖IP位址、URL或網域名稱。

若要解除已封鎖的IP位址、URL或域名的封鎖，您需要建立並執行另一個常規程式。

您可以點擊以下連結下載指令碼：

下載指令碼

存取FortiGate的登入名稱、密碼和API金鑰儲存在env.sample組態檔中。您需要將此檔案中的資訊複製到您建立的新ENV檔案中，然後在新檔案中指定必要的參數。

執行指令碼需要Python 3.10。

若要透過FortiGate執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師或二級分析師。

若要啟動透過FortiGate回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過FortiGate回應的常規程式。
3. 按一下**啟動**按鈕。

   所選常規程式將啟動透過FortiGate進行回應的指令碼。

   如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過Palo Alto NGFW回應

Palo Alto NGFW是一種為您的企業網路提供以下保護措施的解決方案：

- 防火牆 — 篩選網路流量，以保護網路免受未經授權的存取。
- 入侵和攻擊防護 — 識別和封鎖可疑操作，以確保系統完整性。
- 惡意軟體防護——防止惡意軟體感染；
- 網頁篩選 - 限制使用者存取您認為不需要的網站。

支援PAN-OS（執行Palo Alto NGFW的作業系統）11.1.6-h7版本。

如果您之前設定了Kaspersky Next XDR Expert與指令碼啟動服務之間的整合，並建立了啟動指令碼進行回應的常規程式，則您可以透過Palo Alto NGFW回應警示和事件。若要檢視常規程式範例，請點擊此連結。

常規程式啟動後，Palo Alto NGFW將根據您在建立常規程式時指定的操作封鎖IP位址或URL。若要解除已封鎖的IP位址或URL的封鎖，您需要建立並啟動另一個常規程式。

您可以透過點擊此連結來下載指令碼：

下載指令碼

您需要依照README檔案中的說明設定指令碼：

a. 在config.ini中重新命名config.ini.example檔案。

b. 在檔案中，指定部署了Palo Alto NGFW的裝置的位址，以及您先前在Palo Alto NGFW介面中產生的API金鑰，或者，您也可以在指令碼所在的目錄中執行以下命令來取得：

```
python main.py --get-api-key
```

根據需要，您也可以變更要新增IP位址或URL的預設群組和政策。

若要透過Palo Alto NGFW執行回應操作，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要啟動透過Palo Alto NGFW回應的指令碼：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分中，點選所需警示或事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您建立的用於透過Palo Alto NGFW回應的常規程式。
3. 按一下**啟動**按鈕。

   所選常規程式將啟動透過Palo Alto NGFW進行回應的指令碼。

   如果操作成功完成，螢幕上將顯示對應的訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在警示或事件詳細資訊的**歷史記錄**頁籤上找到。

透過 Jira 進行回應

Kaspersky Next XDR Expert 可讓您將 Kaspersky XDR 事件與 Atlassian Jira 問題同步。

透過 Jira 整合進行回應可讓您：

- 根據 XDR 事件建立包含完整背景資訊的 Jira 問題。
- 在事件資料變更時更新現有 Jira 問題。
- 擷取 Jira 問題以用於診斷目的。
- 將證據檔案附加到 Jira 問題。
- 在不進行 API 呼叫的情況下，以試執行模式測試整合。
- 在 Jira 問題中新增註解。

如果您先前已設定 Kaspersky Next XDR Expert 與指令碼啟動服務之間的整合，並建立了會啟動回應指令碼的常規程式，則可以透過 Jira 進行回應。

執行指令碼需要 Python 3.12。

支援 Jira Software Cloud 或 Jira 資料中心 8.4 或更新版本。

您可以點擊以下連結下載回應指令碼：

下載指令碼

若要使用指令碼：

1. 以下列其中一種方式安裝指令碼：
   - 例如，透過pip：

     ```
     pip install -r requirements.txt
     ```

   - 例如，透過 uv：

     ```
     uv sync
     ```

2. 根據您的 Jira 部署，執行以下其中一項操作：
   - 對於 Jira Cloud，請產生 API 權杖。
   - 對於 Jira 資料中心，請在您的 Jira 資料中心實例中產生個人存取權杖 (PAT)。
3. 執行以下命令，從 `.env.sample` 檔案建立 `.env` 檔案：

   ```
   cp .env.sample .env
   ```

4. 編輯 `.env` 檔案並指定您的 Jira 憑證，例如：

   ```
   JIRA_BASE_URL="https://your-company.atlassian.net"
   JIRA_USER_EMAIL="bot@your-company.com"
   JIRA_API_TOKEN="your-api-token-here"
   JIRA_PROJECT_KEY="SEC"
   JIRA_ISSUE_TYPE="Incident"
   JIRA_ATTACHMENT_MAX_MB=10
   JIRA_INSECURE=false
   JIRA_AUTH_TYPE="basic"
   ```

   設定 `JIRA_INSECURE=true` 會停用 SSL 憑證驗證。建議僅在使用自我簽署憑證的測試環境中啟用此選項。不建議在生產環境中啟用此選項。

   `JIRA_AUTH_TYPE` 的值取決於您的 Jira 部署：Jira Cloud 使用 `basic`，Jira Data Center / Server 使用 `bearer`。

指令碼已設定並安裝。

使用 Jira 議題

設定指令碼後，您可以使用它來執行下列操作：

- 建立議題。

  為此，執行以下命令：

  ```
  uv run python -m src.jira --create \
    --incident-id 12345 \
    --name "Suspicious Lateral Movement Detected" \
    --severity high \
    --description "Detected unusual network activity" \
    --deep-link "https://xdr-console/incidents/12345" \
    --asset "host01|10.0.0.5|Windows" \
    --asset "host02|10.0.0.6|Linux" \
    --observable "md5:abcd1234" \
    --observable "url:https://malicious.com" \
    --mitre-technique "T1021" \
    --mitre-technique "T1003"
  ```

  如果命令成功執行，輸出會類似以下內容：

  ```
  {
    "status": "created",
    "issue_key": "SEC-123",
    "issue_id": "10001",
    "self": "https://company.atlassian.net/rest/api/2/issue/10001"
  }
  ```

- 更新問題。

  為此，執行以下命令：

  ```
  uv run python -m src.jira --update \
    --issue-key SEC-123 \
    --incident-id 12345 \
    --severity critical \
    --observable "ip:192.168.1.100" \
    --hash "new-hash-value" \
    --previous-hash "old-hash-value"
  ```

  如果命令成功執行，輸出會類似以下內容：

  ```
  {
    "status": "updated",
    "issue_key": "SEC-123"
  }
  ```

- 擷取 Jira 問題以用於診斷目的。

  為此，執行以下命令：

  ```
  uv run python -m src.jira --get --issue-key SEC-123
  ```

  如果命令成功執行，輸出會類似以下內容：

  ```
  {
    "status": "success",
    "issue_key": "SEC-123",
    "fields": {
      "summary": "[XDR] Suspicious Activity - host01",
      "status": "Open",
      "priority": "High",
      "created": "2025-11-28T10:00:00.000+0000",
      "updated": "2025-11-28T10:30:00.000+0000",
      "labels": ["XDR_12345", "TECHNIQUE_T1021"]
    }
  }
  ```

- 在模擬執行模式下測試整合。

  為此，執行以下命令：

  ```
  uv run python -m src.jira --create \
    --incident-id 12345 \
    --name "Test Incident" \
    --severity high \
    --dry-run
  ```

- 將檔案附加到問題。

  為此，執行以下命令：

  ```
  uv run python -m src.jira --create \
    --incident-id 12345 \
    --name "Malware Detected" \
    --severity critical \
    --attachment "/path/to/evidence.json" \
    --attachment "/path/to/screenshot.png"
  ```

- 為問題新增註解。

  為此，執行以下命令：

  ```
  uv run python -m src.jira --comment \
    --issue-key SEC-123 \
    --comment-text "Investigation in progress, escalating to L2"
  ```

  如果命令成功執行，輸出會類似以下內容：

  ```
  {"status":"commented","issue_key":"SEC-123"}
  ```

使用常規程式進行回應

若要使用常規程式對 Jira 問題執行操作：

1. 在主功能表中，轉至**監控**部分，然後在**事件**部分中，點選所需事件的ID。
2. 點擊**選取常規程式**按鈕，然後在開啟的視窗中，選擇您為透過 Jira 進行回應而建立的常規程式。
3. 按一下**啟動**按鈕。
   所選常規程式將啟動透過 Jira 進行回應的指令碼。
   如果操作成功完成，螢幕上將顯示對應的訊息。否則，將顯示錯誤訊息。

常規程式啟動的結果可以在事件詳細資訊的**歷史記錄**頁籤上找到。

從警示或事件詳細資訊中檢視回應歷史記錄

執行回應操作後，您可以透過以下其中一種方式檢視回應歷程記錄：

- 從警示或事件詳細資訊。
- 從回應歷程記錄部分。
- 從常規程式詳細資訊。
- 從隔離部分。
  選取所需檔案旁的核取方塊，然後按一下**在回應歷程記錄中檢視檔案**按鈕，即可轉至**回應歷史**部分。您可以檢視將檔案移至**隔離**的回應操作。

若要從警示或事件詳細資訊檢視回應操作歷程記錄：

1. 在主功能表中，轉至**監控**部分。
2. 開啟**警示**或**事件**部分，然後按一下執行回應操作的警示ID或事件ID。
3. 在開啟的視窗中，轉到**歷史記錄**頁籤，然後選擇**回應歷史**頁籤。
   將顯示事件表並包含以下直欄：
   - **時間**。事件發生的時間。
   - **啟動者**。啟動回應操作的使用者的名稱。
   - **事件**。事件敘述。
   - **回應參數**。回應操作中指定的回應操作參數。
   - **資產**。啟動回應操作的資產數量。您可以點選包含資產數量的連結來檢視資產詳情。

- **動作狀態**。回應操作的執行狀態。此列可以顯示以下值：
  - **等待核准**– 等待核准啟動的回應操作。
  - **已啟動**– 回應操作正在執行中。
  - **成功**– 回應操作已完成，沒有錯誤或警告。
  - **警告**– 回應操作已完成，但有警告。
  - **錯誤**– 回應操作已完成，但有錯誤。
  - **已停止**– 由於使用者中斷了執行，回應操作已完成。
  - **核准時間已過**– 由於啟動的核准時間已過，回應操作已完成。
  - **被拒絕**– 由於使用者拒絕了啟動，回應操作已完成。
- **常規程式**。啟動回應操作的常規程式的名稱。您可以單擊連結以查看常規程式詳細資訊。
- **回應動作**。已執行的回應操作的名稱。
- **資產類型** 啟動回應操作所針對的資產類型。可能的值：**裝置**或**使用者**。
- **資產租用戶**。租用戶，即啟動回應操作的資產所有者。

4. 如有必要，請點擊設定圖示 (⚙)，然後選擇要在表中顯示的直欄。
5. 如有必要，請點擊篩選器圖示 (▽)，然後在開啟的視窗中指定並套用篩選條件：
   - 按一下**新增篩選器**按鈕來新增篩選器。
   - 透過在下列欄位中選擇必要的值來編輯篩選器：
     - **內容**
     - **條件**
     - **值**
   - 刪除篩選器。
   - 按一下全部**全部重設**按鈕刪除所有篩選器。

檢視惡意軟體掃描結果

惡意軟體掃描完成後，您可以透過以下方式之一檢視其結果：

- 從警示或事件詳細資訊
- 從回應歷史記錄
- 從常規程式詳細資訊

若要檢視惡意軟體掃描的結果：

1. 在主功能表中，轉至**監控**部分，然後執行以下操作之一：

   - 如果您想檢視警示或事件詳細資訊的結果，請轉到**警示**或**事件**部分，然後按一下執行惡意軟體掃描的警示或事件的ID。在開啟的視窗中，轉到**歷史記錄**頁籤，然後選擇**回應歷史**頁籤以顯示事件清單。
   - 如果您想檢視回應歷史記錄的結果，請轉至**回應歷史**部分。
   - 如果您想從常規程式表中檢視惡意軟體掃描的結果，請轉至**指令劇本**部分，然後執行以下操作之一：
     - 選擇執行了惡意軟體掃描的常規程式。在工具列中，按一下**檢視歷史記錄**按鈕，然後選擇**檢視回應歷史記錄**。
     - 點選執行了惡意軟體掃描的常規程式的名稱。在開啟的視窗中，按一下**檢視歷史記錄**按鈕，然後選擇**檢視回應歷史記錄**。

2. 在**動作狀態**列中，按一下您要查看其惡意軟體掃描結果的事件的狀態。

   在開啟的視窗中，將顯示一個偵測表。在**管理伺服器**欄位中，您可以選擇顯示偵測表的管理伺服器。

   資源表包含以下列：

   - **裝置**。裝置名稱或ID
   - **路徑**。檔案路徑
   - **雜湊**。SHA-256雜湊值
   - **偵測名稱**。裝置上發生的偵測的名稱。
   - **動作狀態**。威脅處理結果。
   - **使用者**。與偵測關聯的使用者的帳戶。

處理回應操作取得的檔案

要檢視**檔案**部分，您必須擁有以下XDR角色之一：主管理員、租用戶管理員、 SOC管理員、 SOC經理、一級分析師、二級分析師、初級分析師、核准人、稽核員。

檔案部分顯示您手動下載的檔案以及執行下列回應操作後所取得的檔案：檔案、鑑證資料、登錄機碼、NTFS 中繼檔、處理程序記憶體傾印、從隔離區獲取檔案。

我們建議您啟用檔案自動輪換功能，以便從**檔案**儲存庫中刪除最舊的檔案，然後您可以上傳新檔案。偵測到威脅的檔案不會被刪除。這些檔案與因偵測到威脅建立的警示相關聯。
您不會收到刪除最舊檔案的通知。

檢視檔案表

若要開啟檔案表，請在主功能表中前往 **儲存區** → **檔案**。此表顯示儲存在您擁有存取權限的租用戶中的檔案。

在工具列的右上角，您可以按如下方式對錶中的資料進行分組、篩選和搜尋：

- 點擊設定圖示 ()，然後選擇要在表格中顯示的欄位。
- 點擊篩選圖示 ( )，然後在開啟的功能表中指定並套用篩選條件。
- 點擊搜尋圖示 ()，在顯示的 **搜尋** 欄位中，輸入您要尋找的內容，然後按 **ENTER 鍵**。

資源表包含以下列：

- **名稱或完整路徑**。如果您手動下載了檔案，則會在該直欄中顯示檔案名稱。如果檔案是透過回應操作獲得的，則會顯示檔案的完整路徑。
- **大小**。檔案大小。
- **MD5**。檔案的MD5雜湊值（如有）。
- **SHA256**。檔案的SHA256雜湊值（如有）。
- **上傳日期**。檔案加入到**檔案**儲存庫的日期。
- **更新日期**。檔案在**檔案**儲存庫中更新的日期。
- **租用戶**。檔案所屬的租用戶。

  在OSMP 實例階層中，如果租用戶是在子實例上建立的，則**租用戶**欄位中的值會與子實例圖示（）一起顯示。
- **來源**。將檔案新增到**檔案**儲存庫的使用者名稱或回應操作後取得檔案的裝置名稱。
- **正在新增方法**。將檔案新增到**檔案**儲存庫的方法。

  如果檔案是由使用者上傳的，則該直欄會顯示**由使用者上傳**值。如果檔案是透過回應操作取得的，則會顯示回應操作名稱。
- **掃描狀態**。上次對檔案執行掃描的結果。以下值會顯示在此直欄：
  - **未掃描**
  - **正在掃描**
  - **未偵測**

- **偵測日期**
- **錯誤**

- **說明**。此列包含您在設定回應操作參數或手動上傳檔案時在**說明**欄位中輸入的資訊（如有）。

> 您可以透過點擊直欄標頭並從下拉清單中選擇所需的方法或狀態來篩選**正在新增方法**和**掃描狀態**直欄中的資料。

在檔案表中執行操作

在工具列的左上角，您可以執行以下操作：

- 點按**重新整理**按鈕來更新表中的資料。
- 按一下**檔案**按鈕，將檔案從您的電腦上傳到**上傳**儲存庫。

  這會開啟右側的側邊欄。在**租用戶**欄位中，指定您想要擁有該檔案的租用戶。然後點按**上傳檔案**連結，並選取您電腦上的檔案。根據需要，您還可以在**描述**欄位中新增備注或描述，若要掃描檔案來搜尋威脅，請開啟**上傳後掃描檔案**切換開關。

  點擊**上傳**按鈕後，窗格將關閉，上傳的檔案將顯示在表中。上傳大檔案或多個檔案時，您必須重新整理表格，以便顯示新檔案。如果檔案正在上傳， **名稱或完整路徑**列會顯示載入指示器， **大小**欄位會顯示已上傳的檔案大小佔總檔案大小的比例。
- 將檔案儲存到您的電腦。為此，請選取表格中一個或多個檔案旁的複選框，然後按一下**下載**按鈕。
- 使用以下技術掃描所選檔案是否有威脅：YARA、沙盒和反惡意軟體引擎。為此，請選取表格中一個或多個檔案旁的核取方塊，然後按一下**掃描**按鈕。
- 刪除檔案。為此，請選取表格中一個或多個檔案旁邊的核取方塊，然後按一下**刪除**按鈕。
- 轉到與這些檔案相關的警示清單。為此，請選取表格中一個或多個檔案旁邊的核取方塊，然後按一下**尋找警示**按鈕。因威脅偵測而建立的警示以及執行回應操作的詳情的警示（如果回應操作導致檔案被放入**檔案**儲存庫）隨即顯示。

> 如果執行以下回應操作，則**掃描**選項不可用，且不會計算透過這些操作獲得的檔案雜湊值：鑑證資料、登錄機碼、NTFS 中繼檔、處理程序記憶體傾印。

檢視檔案詳情

您可以按一下表中**名稱或完整路徑**的連結來開啟檔案詳情。

在開啟的右側窗格中，會顯示檔案元資料（例如，檔案名稱或路徑、大小、雜湊值）、掃描狀態和掃描結果：

- 如果傳送了存檔進行掃描，檔案詳情將顯示存檔中偵測到威脅的檔案的資訊，以及此類檔案的雜湊值和每種技術的狀態：反惡意軟體、沙盒、YARA。
- 如果檔案未掃描，則會顯示相應的資訊。
- 如果檔案沒有可用的掃描，則檔案詳情僅顯示元資料。

如果檔案是手動上傳並進行了威脅掃描，則在檔案詳情中，您也可以透過點擊掃描狀態**掃描狀態下載報告**連結來檢視掃描報告。

在檔案詳情中，您可以進行以下操作：

- 透過點擊工具列中的相應按鈕執行以下操作：掃描、下載、刪除檔案、查詢連結的警示、編輯檔案描述、移動到回應歷程記錄。

  手動上傳的檔案無法使用**在回應歷史中顯示**選項。對於因回應操作而取得的文件，按一下**在回應歷史中顯示**後，您將進入**回應歷史**部分，其中事件表將按檔案進行篩選。

- 點擊包含MD5或SHA256哈希值的連結，然後在下拉清單中選擇要執行的操作：
  - 針對偵測到威脅的檔案**建立阻止規則**。選擇該選項後，將開啟**新增阻止規則**窗格，您可以在其中使用阻止規則表。
  - **在 Kaspersky TIP 上尋找**，以在Kaspersky Threat Intelligence Portal中檢查檔案雜湊。
  - **檢視沙盒報告**。該選項適用於手動上傳到**檔案**儲存庫並使用沙盒技術掃描的檔案。
  - **尋找關聯警示**。關聯的警示是由於威脅偵測而建立的警示，以及您執行回應操作的詳情的警報（如果回應操作導致檔案被放入**檔案**儲存庫）。
  - **尋找關聯事件**，將其移至**威脅搜尋**部分，其中的事件表會依檔案雜湊值進行篩選。

在OSMP 實例階層中，在子實例上執行回應操作後下載及取得的檔案，會顯示在父實例的檔案表中，並在**租用戶**欄位中顯示以下圖示：(⛓)。

使用阻止規則表

阻止規則可讓您阻止您認為不安全的檔案或進程在裝置上執行。Kaspersky Next XDR Expert使用MD5和SHA256雜湊值演算法，根據檔案的雜湊值識別檔案。

您可以透過以下方式管理阻止規則：

- 如本文所述，從阻止規則表中手動建立、匯入、編輯和刪除阻止規則
- 透過執行相應的回應操作來建立和刪除阻止規則
- 設定回應操作，以便在建立或編輯常規程式時自動執行

> 若要開啟阻止規則表，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、SOC經理、一級分析師、二級分析師、初級分析師、核准人、稽核員。
> 若要建立或匯入阻止規則，您必須具有以下XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

若要開啟阻止規則表，在主選單中，依序選擇**監控→資源和服務→阻止規則**。

資源表包含以下列：

- **名稱**。對於手動建立的阻止規則，此直欄顯示您在**建立阻止規則**窗格中指定的名稱。對於匯入的阻止規則，此直欄顯示檔案雜湊值。
- **雜湊**。要阻止的檔案的MD5或SHA256雜湊值。
- **租用戶所有者**。阻止規則所屬的租用戶。

  在分散式解決方案模式下，如果租用戶是在從屬節點上建立的，則**租用戶**欄位中的值會與從屬節點圖示（ ）一起顯示。
- **資產**。套用此阻止規則的裝置。此直欄顯示裝置數量或**租用戶的所有資產**的總值。
- **建立日期**。阻止規則的建立或匯入日期和時間。
- **建立者**。建立或匯入此阻止規則的使用者。
- **更新日期**。阻止規則設定的最後編輯日期和時間。
- **更新者**。最後編輯此阻止規則設定的使用者。
- **規則狀態**。如果阻止規則已啟用，則此直欄顯示此規則的**已啟用**值。否則，系統將顯示**停用**值。
- **檔案封鎖通知**。如果在建立或編輯阻止規則時停用了檔案封鎖通知，則該欄位顯示**否**值。否則，系統將顯示**是**值。

在表格中，您可以進行以下操作：

- 建立或匯入阻止規則。
- 若要刪除阻止規則，請選取所需規則名稱旁的核取方塊，然後按一下工具列中的**刪除**按鈕。您也可以一次刪除所有規則。
- 若要啟用或停用阻止規則，請選取所需規則名稱旁的核取方塊，按一下**變更狀態**按鈕，然後選取**啟用**或**停用**。您也可以一次啟用和停用所有規則。
- 透過點擊表格中的規則名稱來檢視和編輯阻止規則詳情。

此時將開啟**編輯阻止規則**窗格，並且**詳細資訊**頁籤已選定。您可以編輯阻止規則的設定。這些設定與您從規則表中建立阻止規則時的設定相同。此外，您也可以點選**轉到威脅搜尋**按鈕，檢視觸發阻止規則時所取得的事件。

在**變更記錄**頁籤中，您可以檢視套用至阻止規則的所有變更：從阻止規則表中手動檢視，透過執行回應操作，或透過啟動常規程式。

若要一次將操作套用至所有規則：

1. 選取**名稱** 欄旁的核取方塊。
2. 在下拉式清單中按一下其中一個項目：
   - 如果您想要對表格中的所有規則執行操作，請選取**全選**。
   - 如果您想要對目前頁面上的所有規則執行操作，請選取**全部選取目前頁面**。
3. 如有必要，您可以取消選取規則名稱旁的核取方塊，將一或多個規則從範圍中排除。
4. 在工具列中，根據您要執行的操作，按一下所需的按鈕：**刪除** 或**變更狀態**（啟用或停用規則）。

此操作將套用至您選取的所有規則。

建立阻止規則。

若要建立阻止規則：

1. 在主功能表中，轉至**監控→資源和服務→阻止規則**。
   阻止規則表隨即顯示。
2. 在工具列中，按一下**新增**按鈕。
3. 在開啟的**建立阻止規則**窗格中，配置下列設定：
   a. 在**租用戶所有者**欄位中，指定阻止規則所屬的租用戶。

   > 儲存阻止規則設定後，您將無法編輯**租用戶所有者**欄位中的值。如果要變更租用戶，則必須刪除阻止規則，建立一個新規則，並在**租用戶所有者**欄位中指定所需的值。

   b. 在**MD5 或 SHA256**欄位中，指定要封鎖的檔案的雜湊值。
   如果要指定多個雜湊值，請點選**新增雜湊值**按鈕。

   > 應用程式檢查雜湊值是否存在於要阻止的檔案雜湊清單中的租用戶中。建立新的阻止規則時，您無法指定此類雜湊值。

   c. 如果必要，配置以下設定：
   - 改變阻止規則的範圍。
     預設情況下，在**套用規則至**設定群組中，**所有資產**選項已選取。這意味著該阻止規則將套用至所有裝置。您可以選擇**特定資產**選項，然後在顯示的**資產**欄位中指定要套用該阻止規則的一個或多個裝置。

如果您設定了要套用該阻止規則的裝置，之後某個裝置被刪除，則該裝置也會從阻止規則中刪除，並且相應的資訊將顯示在阻止規則詳情的**變更記錄**頁籤中。

- 在**規則名稱**欄位中，指定阻止規則的名稱。如果名稱未指定，該欄位將顯示為空。
- 在**通知使用者關於封鎖檔案執行的事宜**欄位中，如果您不想收到檔案被封鎖時的通知，請停用切換開關。

  預設情況下已啟用該選項。
- 在**狀態**欄位中，如果您不想套用該阻止規則，請停用切換開關。

  如果要建立狀態為**已停用**的阻止規則，必須先配置其他設定。否則，您將無法儲存該規則。

d. 點擊**建立**按鈕。

窗格關閉後，阻止規則將顯示在規則清單中。

匯入阻止規則

若要匯入阻止規則：

1. 在主功能表中，轉至**監控→資源和服務→阻止規則**。

   阻止規則表隨即顯示。
2. 在工具列上，點擊「**匯入**」按鈕。

   從檔案匯入的阻止規則將套用至屬於租用戶（包括子租戶）的所有資產。
3. 在開啟的**匯入阻止規則**窗格中，配置必要的設定：

   a. 從您的電腦中選擇一個CSV檔案。

   您只能新增一個包含雜湊值的CSV檔案。雜湊值的數量等於要建立的阻止規則的數量。最大檔案大小不得超過15MB

   b. 在下拉式清單中，選取要套用阻止規則的租用戶。

   預設情況下，系統會選取您擁有存取權限的租用戶。根據需要，您可以變更規則。

   如果您擁有多個租用戶的存取權限，則該值為空，您必須指定所需的租用戶。

   c. 點擊**匯入**按鈕。

窗格關閉後，匯入的阻止規則將顯示在規則表中。

使用IOC規則表

Kaspersky Next XDR Expert掃描裝置以查找入侵指標（IOC）。多個IOC可以組合成一個IOC檔案中的結構化描述。匯入IOC規則時，Kaspersky Next XDR Expert會從IOC檔案中擷取結構化描述，並根據該描述建立規則。觸發IOC規則後，將產生IOC警示。

檢視IOC規則表

要檢視IOC規則清單，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、SOC經理、一級分析師、二級分析師、初級分析師、核准人、稽核員。

若要開啟IOC規則表，在主選單中，轉至**監控→資源和服務→IOC 規則**。該表顯示儲存在您擁有存取權限的租用戶中的IOC規則。

您可以對表格中的資料進行分組、篩選和搜尋，如下所示：

- 點擊設定圖示 ( )，然後選擇要在表中顯示的列。
- 點擊篩選圖示 ( )，然後在開啟的功能表中指定並套用篩選條件。
- 點擊搜尋圖示 ( )，在顯示的 **搜尋** 欄位中，輸入您要尋找的內容，然後按 **ENTER**。

資源表包含以下列：

- **名稱**。IOC規則名稱。
- **建立日期**。IOC規則的建立日期和時間。
- **建立者**。建立IOC規則的使用者。
- **更新日期**。IOC規則的更新日期。
- **更新者**。最後編輯此IOC規則設定的使用者。
- **重要性**IOC規則的重要性等級：**低**、**中**或**高**。
- **租用戶所有者**。IOC規則所屬的租用戶。
  在分散式解決方案模式下，如果租用戶是在子實例上建立的，則**租用戶**欄位中的值會與子實例圖示 ( ) 一起顯示。
- **排定的掃描**。排程掃描的狀態：**已啟用**或**已停用**。您可以將切換開關撥到**已啟用**或**已停用**位置來變更狀態。

在IOC規則表中執行操作

在工具列的左上角，您可以執行以下操作：

- 點按**重新整理**按鈕來更新表中的資料。
- 按一下**匯入**按鈕，匯入。
  為此，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、一級分析師、二級分析師。
- 將IOC規則儲存到您的電腦。為此，請選取表格中一個或多個規則旁邊的核取方塊，然後按一下**匯出**按鈕。

- 刪除IOC規則。為此，請選取表格中一個或多個規則旁邊的核取方塊，然後按一下**刪除**按鈕。您也可以一次刪除所有規則。

- 執行IOC掃描回應操作。為此，請選取表格中一個或多個規則旁的核取方塊，然後按一下**執行 IOC 掃描**按鈕。您也可以一次對所有規則執行回應操作。

  若要執行掃描，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。

- 啟用或停用所選IOC規則的排程掃描。為此，請選取表格中一個或多個規則旁的核取方塊，按一下**排定的掃描**按鈕，然後在下拉清單中，選擇**啟用**或**停用**選項之一。您也可以一次啟用和停用所有規則的掃描。

  必須設定排程掃描。

若要一次將操作套用至所有規則：

1. 選取**名稱** 欄旁的核取方塊。
2. 在下拉式清單中按一下其中一個項目：
   - 如果您想要對表格中的所有規則執行操作，請選取**全選**。
   - 如果您想要對目前頁面上的所有規則執行操作，請選取**全部選取目前頁面**。
3. 如有必要，您可以取消選取規則名稱旁的核取方塊，將一或多個規則從範圍中排除。
4. 在工具列中，根據您要執行的操作，按一下所需的按鈕：**刪除**、啟用或停用**排定的掃描**。

   此操作將套用至您選取的所有規則。

在 OSMP 實例階層中，如果您在子實例中一次啟用、停用或刪除所有規則，且選取範圍包含父實例的某些規則，則操作不會套用至這些規則。
如果您按一下 **全選 → 排定的掃描**或 **全選 → 刪除**，操作只會套用至子實例的規則。
如果您按一下 **全部選取目前頁面**，則 **排定的掃描**和 **刪除**按鈕會停用。

查看IOC規則詳情

您可以按一下表中**名稱**的連結來開啟IOC規則詳情。

在開啟的右側窗格中，IOC規則的資訊顯示在相應的欄位中：規則名稱、規則所屬的租用戶、規則的重要性、排程掃描狀態（啟用或停用）以及觸發規則的條件。

在詳情窗格中，您可以執行以下操作：

- 按一下**匯出**按鈕，將IOC規則儲存到您的電腦。
- 按一下**執行 IOC 掃描**按鈕，執行IOC掃描回應操作。
- 按一下**尋找警示**按鈕，轉至與IOC規則相關的警示清單。

  此時將顯示觸發了IOC規則的警示。如果沒有此類警示，則會顯示所有IOC警示。

使用YARA規則表

YARA規則是針對組織IT基礎設施的定向攻擊和入侵的特徵碼描述。Kaspersky Next XDR Expert根據這些規則掃描物件。

檢視YARA規則表

要檢視YARA規則表，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、SOC經理、一級分析師、二級分析師、初級分析師、核准人、稽核員。

若要開啟YARA規則表，在主選單中，轉至**監控→資源和服務→YARA 規則**。

此表顯示儲存在您擁有存取權限的租用戶中的YARA規則。

您可以對表格中的資料進行分組、篩選和搜尋，如下所示：

- 點擊設定圖示 ( )，然後選擇要在表中顯示的列。
- 點擊篩選圖示 ( )，然後在開啟的功能表中指定並套用篩選條件。
- 點擊搜尋圖示 ( )，在顯示的 **搜尋** 欄位中，輸入您要尋找的內容，然後按 **ENTER**。

資源表包含以下列：

- **名稱**。YARA規則名稱。
- **建立日期**。YARA規則的建立日期和時間。
- **建立者**。建立YARA規則的使用者。
- **更新日期**。YARA規則的更新日期。
- **更新者**。最後編輯此YARA規則設定的使用者
- **重要性**YARA規則的重要性等級：**低**、**中**或**高**。
- **租用戶所有者**。YARA規則所屬的租用戶。
  在分散式解決方案模式下，如果租用戶是在子實例上建立的，則**租用戶**欄位中的值將顯示子實例圖示 ( )。
- **檔案掃描中**。YARA掃描的狀態：**已啟用**或**已停用**。您可以將切換開關撥到**已啟用**或**已停用**位置來變更狀態。
- **說明**。YARA規則的描述或註解。

在YARA規則表中執行操作

在工具列的左上角，您可以執行以下操作：

- 點按**重新整理**按鈕來更新表中的資料。
- 按一下**匯入**按鈕，匯入。

  若要匯入YARA規則，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、一級分析師、二級分析師。
- 將YARA規則儲存到您的電腦。為此，請選取表格中一個或多個規則旁邊的核取方塊，然後按一下**匯出**按鈕。
- 刪除YARA規則。為此，請選取表格中一個或多個規則旁邊的核取方塊，然後按一下**刪除**按鈕。您也可以一次刪除所有規則。
- 執行YARA掃描回應操作。為此，請選取表格中一個或多個規則旁的核取方塊，然後按一下**執行 YARA 掃描**按鈕。您也可以一次對所有規則執行回應操作。

  若要執行掃描，您必須擁有下列XDR角色之一：主管理員、租用戶管理員、一級分析師、二級分析師。
- 啟用或停用所選YARA規則的排程掃描。為此，請選取表格中一個或多個規則旁的核取方塊，按一下**檔案掃描中**按鈕，然後在下拉清單中，選擇**啟用**或**停用**選項之一。您也可以一次啟用和停用所有規則的掃描。

若要一次將操作套用至所有規則：

1. 選取**名稱** 欄旁的核取方塊。
2. 在下拉式清單中按一下其中一個項目：
   - 如果您想要對表格中的所有規則執行操作，請選取**全選**。
   - 如果您想要對目前頁面上的所有規則執行操作，請選取**全部選取目前頁面**。
3. 如有必要，您可以取消選取規則名稱旁的核取方塊，將一或多個規則從範圍中排除。
4. 在工具列中，根據您要執行的操作，按一下所需的按鈕：**刪除**、啟用或停用**檔案掃描中**。

   此操作將套用至您選取的所有規則。

如果您想要一次啟用或停用所有規則，且所選項目包含屬於子租用戶的規則：

- 按一下**全選**時，只有屬於根租用戶的規則才會變更其狀態。
- 按一下**全部選取目前頁面**時，**檔案掃描中**按鈕會呈灰色。

在OSMP 實例階層中，一次將操作套用至所有規則時，涉及特定考量事項。

按一下這裡檢視

一次啟用或停用所有規則

在父實例中

- 如果您按一下**全選**，且所選項目包含屬於父實例或子實例之子租用戶的規則，則該操作將不會套用至這些規則。

  對於這兩個實例，只有屬於根租用戶的規則會被啟用或停用。

- 如果您按一下**全部選取目前頁面**，且所選項目包含屬於父實例或子實例之子租用戶的規則，則**檔案掃描中**按鈕會呈灰色。

在子實例中

- 如果您按一下**全選**，且所選項目包含屬於子租用戶的規則或父實例的任何規則，則該操作將僅套用至屬於根租用戶的子實例規則。

- 如果您按一下**全部選取目前頁面**，且所選項目包含屬於子租用戶的規則或父實例的任何規則，則**檔案掃描中**按鈕會呈灰色。

一次刪除所有規則

在父實例中，

您可以刪除屬於父實例和子實例之任何租用戶的任何規則。

在子實例中：

- 如果您按一下**全選**，且所選項目包含父實例規則，則這些規則將不會被刪除。

- 如果您按一下**全部選取目前頁面**，且所選項目包含父實例規則，則**刪除**按鈕會呈灰色。

查看YARA規則詳情

您可以按一下表格中**名稱**欄內的連結，開啟YARA規則詳情。

在開啟的右側窗格中，YARA規則的資訊會顯示在相應的欄位中：規則名稱、規則所屬的租用戶、規則的重要性、掃描狀態（啟用或停用）、規則描述以及觸發規則的條件。

在詳情窗格中，您可以執行以下操作：

- 按一下**匯出**按鈕，將YARA規則儲存到您的電腦。

- 按一下**執行 YARA 掃描**按鈕，執行YARA掃描回應操作。

- 按一下**尋找警示**按鈕，轉至與YARA規則相關的警示清單。

  此時將顯示觸發了YARA規則的警示。如果沒有此類警示，則會顯示所有YARA警示。

常規程式

Kaspersky Next XDR Expert 使用常規程式自動化工作流程，並縮短處理警示和事件所需的時間。

*常規程式*根據指定的*演算法*回應警示或事件。常規程式會啟動一個演算法，該演算法包含一系列有助於分析和處理警示或事件的回應操作。您可以手動啟動常規程式，也可以設定所需常規程式的自動啟動。

常規程式的自動啟動是根據您在*建立常規程式*時配置的觸發器執行的。觸發器定義警示或事件必須滿足的條件才能自動啟動此常規程式。

一個常規程式範圍僅限於警示或事件。

常規程式無法為子事件自動啟動。對於子事件，您只能手動啟動常規程式。在啟動之前，您需要選擇必須為其啟動常規程式的資產和可觀察物件。請注意，只能為屬於警示或事件租用戶的物件啟動常規程式。

請注意，常規程式只能屬於一個租用戶，並且會被父租用戶的所有子租用戶自動繼承，包括在常規程式建立後新增的子租用戶。您可以在建立或編輯常規程式時停用子租用戶繼承常規程式。

在 Kaspersky Next XDR Expert 中，有兩種類型的常規程式：

- 預定義常規程式

  預定義常規程式由卡巴斯基專家建立。這些常規程式的名稱具有[KL]前綴，無法編輯或刪除。

  預設情況下，預定義常規程式在**培訓**運作模式下運作。有關更多資訊，請參閱預定義常規程式部分。

- 自訂常規程式

  您可以自行建立和設定常規程式。建立自訂常規程式時，需要指定常規程式範圍（警示或事件）、自動啟動常規程式的觸發器以及回應威脅的演算法。有關建立常規程式的詳細資訊，請參閱建立常規程式。

您可以使用XDR REST API為特定租用戶匯入和匯出常規程式。

運作模式

您可以設定自動和手動啟動常規程式。啟動常規程式的方式取決於所選的運作模式。

運作模式包括以下類型：

- **自動**。此運作模式下的常規程式在偵測到對應的警示或事件時會自動啟動。
- **培訓**。當偵測到對應的警示或事件時，此運作模式下的常規程式會請求使用者核准啟動。
- **手動**。此運作模式下的常規程式只能手動啟動。

使用者角色

您可以透過為使用者指派使用者角色來授予使用者管理常規程式的權限。

下表顯示了管理常規程式和執行使用者操作的存取權限。

使用者角色	使用者角色權限				
	讀取	寫入	刪除	執行	回應確認
一般管理員	✓	✓	✓	✓	✓
SOC管理員	✓	✓	✓	—	—
初級分析師	✓	—	—	—	—
第 1 層分析師	✓	—	—	✓	—
第 2 層分析師	✓	✓	✓	✓	—
SOC管理員	✓	—	—	—	—
核准人	✓	—	—	—	✓
稽核員	✓	—	—	—	—
租用戶管理員	✓	✓	✓	✓	✓

檢視常規程式表

常規程式表顯示在**監控→指令劇本**部分。預設情況下，該表顯示與您有存取權限的所有租用戶相關的常規程式。

> 常規程式表顯示所有現有常規程式，**已刪除**狀態的常規程式除外。

若要設定常規程式表，請執行下列其中一項操作：

- 套用租用戶篩選器：
  a. 按一下**租用戶篩選器**設定旁的連結。
  b. 租用戶篩選器隨即開啟。
  c. 選取所需事件旁邊的核取方塊。
- 篩選常規程式表的資料：
  a. 按一下篩選器（ ）圖示。
  b. 在**篩選器**頁籤，在喚起的功能表中指定並套用篩選條件。
- 如果要隱藏或顯示某一欄，請按一下設定（ ）圖示，然後選取所需的欄。

常規程式表隨即設定並顯示您需要的資料。

常規程式表包含以下資訊：

- **名稱**。自訂或預定義常規程式的名稱。

  > 預定義常規程式的名稱以[KL]前綴標記，無法編輯或刪除。

- **狀態**。常規程式狀態。可能的值：

  - **作用中**。常規程式隨即建立並可供使用（所有必要的網頁外掛程式即會安裝）。
  - **草稿**。常規程式隨即建立並儲存為草稿。常規程式無法啟動，但可以在常規程式所屬的租用戶中檢視、編輯、自訂和刪除。
  - **已刪除**。常規程式已刪除。預設情況下，處於此狀態的常規程式不會顯示在表中。如果要檢視它們，請按一下**狀態**列，然後在下拉清單中，選擇**已刪除**。

    > 只有活動且不可用的常規程式在刪除後才具有**已刪除**狀態。處於**草稿**狀態的常規程式將永久刪除，不會顯示在常規程式表中。

  - **不可用**。常規程式演算法使用不可用的網頁外掛程式或包含產品授權不允許的回應操作。

- **操作模式**。定義啟動常規程式方式的常規程式運作模式。有關運作模式的更多詳細資訊，請參閱常規程式部分。
- **標籤**。指派給常規程式的標籤。您可以使用已指派的標籤篩選常規程式。
- **操作**。在常規程式中啟動的操作。
- **啟動**。常規程式啟動的總次數。
- **修改日期**。上次編輯常規程式的日期和時間。
- **建立時間**。建立常規程式的日期和時間。
- **父租用戶**。常規程式所屬租用戶的名稱。
- **描述。**常規程式的描述或備注。預設情況下，此列處於隱藏狀態。
- **範圍**。常規程式的範圍。可能的值：**警示**或**事件**。
- **建立者**。建立常規程式的使用者名稱預設情況下，此列處於隱藏狀態。
- **更新者**。更新常規程式的使用者名稱預設情況下，此列處於隱藏狀態。

建立常規程式

您可以建立一個常規程式來自動化威脅分析和威脅回應。

若要建立常規程式，您必須具有以下角色之一：主管理員、 SOC管理員、一級分析師、二級分析師、租用戶管理員。

Kaspersky Next XDR Expert還可讓您基於現有常規程式建立滿足您需要的新常規程式。有關更多詳細資訊，請參閱自訂常規程式。

若要建立新常規程式：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 點擊**建立**按鈕。

   建立常規程式視窗打開，左側是視覺化編輯器工作區，右側是**常規程式設定**窗格。視覺化編輯器可讓您建立和視覺化常規程式執行流程，以及常規程式建立過程中涉及的各個步驟之間的關係。

   根據您在視覺化編輯器中執行的操作，系統會產生常規程式演算法的DSL架構。您在視覺化編輯器工作區中所做的變更會顯示在程式碼中，反之亦然。如有必要，您可以點擊工具列中的**顯示程式碼**按鈕來開啟程式碼編輯器。

3. 在**常規程式設定**窗格中，指定以下設定：

   - 在**租用戶和繼承**欄位中，選擇要為其啟動常規程式的父租用戶和子租用戶。

     所選父租用戶的所有子租用戶將自動繼承此常規程式。若要停用常規程式繼承，請清除所需子租用戶旁邊的核取方塊。將針對此租用戶及其子租用戶（如果有）停用常規程式繼承。
     如果您選取子租用戶，系統會自動選取其子租用戶。

   - 在**名稱**欄位中，輸入常規程式名稱。

     請注意，常規程式名稱在租用戶內必須是唯一的，且長度不能超過255個字元。

   - 在**範圍**清單中，選取以下選項之一：
     - **警示**。常規程式將僅在出現警示時啟動。預設情況下已選取此選項。
     - **事件**。常規程式將僅在出現事件時啟動。
   - 在**操作模式**清單中，選取以下選項之一：
     - **自動**。此運作模式下的常規程式在偵測到對應的警示或事件時會自動啟動。
     - **培訓**。當偵測到對應的警示或事件時，此運作模式下的常規程式會請求使用者核准啟動。
     - **手動**。此運作模式下的常規程式只能手動啟動。

- 如有必要，在**標籤**欄位中，指定最多30個標籤。您可以使用已指派的標籤過濾常規程式。

  請注意，標籤的最大長度為50個字元。

- 如有必要，在**描述**欄位中，輸入常規程式描述或備注。

- 在**同時啟動多個常規程式實例時**下拉清單中，選擇當兩個或多個常規程式實例同時啟動時要執行的操作：

  - **將新的常規程式實例新增至佇列**。新的常規程式實例將在目前實例完成後啟動。預設情況下已選定此操作。

  - **終止目前執行並啟動新實例**。目前常規程式實例的執行將被終止。之後，將啟動一個新的常規程式實例。

  - **請勿啟動新的常規程式實例**。不會啟動新的常規程式實例。目前常規程式實例的執行將繼續。

  > 只有在選擇**同時啟動多個常規程式實例時**運作模式時才會顯示**自動**清單。

- 預設情況下，僅針對與觸發器相符的新警示或事件啟動常規程式。

  如果您要針對與觸發器相符的現有警示或事件啟動新常規程式，請選取**針對所有符合的警示或事件啟動常規程式。請注意，系統可能會過載**核取方塊。

- 如有必要，在**其他設定**部分中，指定以下常規程式參數：

  - **常規程式逾時**—常規程式的最長執行時間。預設情況下，該值為24小時。最大值為48小時。

    如果您要建立政策以進一步套用於回應操作，請啟用**對回應動作使用逾時政策**切換開關，然後新增政策。

    > 停用切換開關後，已新增的政策將被刪除。

  - **輸入**— 用於在執行前修改常規程式傳入資料的jq運算式。

  - **輸出**— 用於執行後修改常規程式輸出資料的jq運算式。

  - **變更方法**— 如何更改輸出資料。選取**合併**或**覆蓋**選項，選擇是合併目前資料和新資料，還是用新資料覆蓋目前資料。

  其他附加設定是預先定義的，無法更改：

  - **常規程式版本**— 常規程式的版本。可能需要更準確地識別遙測中的常規程式。

  - **DSL 版本**— DSL架構版本。

  - **動作版本**— 回應操作架構版本，其中包含回應函式輸入參數的說明。

4. 在視覺化編輯器工作區中，設定常規程式的觸發器和演算法。點擊**觸發條件**步驟，然後在開啟的觸發器設定窗格中，指定自動啟動常規程式的條件。

> 如果選取**手動**運作模式，則觸發器設定不可用。

若要描述觸發條件，請使用jq運算式。有關 jq 運算式的更多資訊，請參閱 jq 手冊。

根據您在建立或編輯常規程式時在**範圍**清單中選取的選項，使用警示資料模式或事件資料模式。

例如，若要以緊急程度篩選警示或事件，請指定以下運算式：

```
.Severity == "critical"
```

您也可以指定複雜的表運算式來篩選警示或事件。

例如，若要按規則名稱篩選緊急警示或事件，請指定以下運算式：

```
(.Severity == "critical") and (.Rules[] |.Name | contains("Rule_1"))
```

其中 `Rules[] |.Name` 定義觸發規則的名稱。

已設定jq運算式的驗證。如果在設定常規程式觸發器時指定了不正確的運算式，則錯誤將以紅色標記。如果要檢視詳細資訊，請將滑鼠遊標停留在錯誤上。

5. 如果要檢視與常規程式觸發器相符的警示或事件，請在**觸發比對**部分中按一下**尋找**按鈕。預設情況下，顯示最近修改的10個警示和事件。如果要變更值，請開啟下拉清單，然後選擇所需的值。

   亦可請求完整的警示或事件清單。為此，請在**觸發條件**部分中輸入 `true` ，然後按一下**尋找**按鈕。

   將顯示完整的警示或事件清單。

6. 指定常規程式演算法步驟。

   您可以從另一個常規程式中複製演算法。若要執行此操作，請在工具列中按一下**複製演算法**按鈕，然後在開啟的視窗中，從中要複製演算法的常規程式，然後按一下**確定**。

   已設定jq運算式和JSON語法的驗證。如果在設定常規程式演算法時指定了錯誤的運算式，則錯誤將以紅色標記。如果要檢視詳細資訊，請將滑鼠遊標停留在錯誤上。

   若要新增演算法步驟，請執行以下操作：

   a. 將滑鼠遊標停留在要與新步驟建立關係的步驟上。

      如果您是第一次新增步驟，則只能將滑鼠遊標停留在**觸發條件**步驟上。

   b. 按一下並按住顯示的白點符號 (○)，然後開始繪製箭頭。

   c. 釋放滑鼠遊標，然後在開啟的功能表中選取該步驟。

      所選步驟將顯示在視覺化編輯器中。

   d. 按一下該步驟即可配置其設定。有關更多詳細資訊，請參閱在視覺化編輯器中設定常規程式執行步驟。

   或者，您可以右鍵按一下視覺化編輯器工作區的任何部分以喚起功能表，然後選擇要新增的步驟。在這種情況下，新增步驟後，您必須透過在所需步驟之間繪製箭頭來建立關係。如果沒有建立任何關係，您只能將常規程式儲存為草稿。

   如果沒有新增演算法步驟，您只能將常規程式儲存為草稿。

7. 以下列方式之一儲存常規程式：

- 透過點選**發佈**按鈕。儲存的常規程式即可使用，並顯示在常規程式表中，狀態為**作用中**
- 透過點選**建立為草稿**按鈕。這可讓您透過只指定其名稱和它所屬的租用戶來建立常規程式。常規程式會顯示在常規程式清單中，狀態為**草稿**。您可以打開它並繼續編輯。

  當您將常規程式儲存為草稿時，系統會進行檢查；錯誤會醒目顯示，但不予理會。
  只有在執行步驟與觸發條件之間未建立連結、未設定必要參數或指定了無效參數時，才能將常規程式儲存為草稿。

新的常規程式將建立並顯示在常規程式清單中。

在視覺化編輯器中設定常規程式執行步驟

建立或編輯常規程式時，新增常規程式執行步驟後，必須配置其設定。為此，請按一下包含該步驟的區塊，然後在右側窗格中，使用jq運算式指定所需的參數。

在視覺化編輯器中，您可以新增和設定以下類型的常規程式執行步驟：

- **動作**
  - 在**動作類型**清單中，選擇回應操作的類型。其他設定因所選類型而異。

    回應操作的類型一般可分**為幾組**

    KATA/KEDR 回應操作：

    - **新增阻止規則**

      指定要套用操作的資產，以及要封鎖的檔案的SHA256或MD5雜湊值。
    - **刪除阻止規則**

      指定套用了阻止規則的資產，以及要刪除的檔案雜湊值。
    - **重設阻止規則**

      指定要重設阻止規則的資產。
    - **執行程式**

      指定資源和可執行檔參數：在**完整路徑**欄位中的完整檔案路徑，以及要在**命令列參數**欄位中啟動檔案的參數。在**工作目錄**檔案中，您可以指定要儲存命令或檔案執行結果的目錄路徑。
    - **啟用網路隔離**

      指定要啟用隔離的資產以及隔離期間。若要從網路隔離規則新增例外，請點選**新增排除項目**按鈕，然後指定所需的參數：
    - **停用網路隔離**

      指定已套用網路隔離的資產。

Active Directory回應操作：

- **鎖定帳戶**

  指定要封鎖其帳戶的使用者。

- **重設密碼**

  指定要重設密碼的使用者。

- **將使用者新增至安全群組**

  指定要新增使用者的使用者及其所屬群組。

- **將使用者從安全群組中刪除**

  指定要從中刪除使用者的使用者及其所屬群組。

Kaspersky NGFW回應操作：

- **將 IP 新增至網路裝置上的封鎖清單**

  請指定要封鎖的IP位址。

KES for Windows回應操作：

- **執行惡意軟體掃描**

  指定資產和掃描類型：

  - **緊急區域掃描**。
  - **自訂掃描**。然後，指定要掃描的檔案路徑。
  - **完整掃描**。如有需要，請啟用**掃描網路磁碟機**切換開關，將網路裝置納入掃描範圍。

  如果您希望僅在惡意軟體掃描完成後啟動下一個回應操作，請啟用**等待回應動作完成**切換開關。

- **更新資料庫**

  指定要更新資料庫的裝置。如果您希望僅在資料庫更新後啟動下一個回應操作，請啟用**等待回應動作完成**切換開關。

- **終止處理程序**

  指定要終止進程的裝置。然後，選擇一個參數，並使用所需資訊指定jq運算式：進程檔案的**雜湊值和路徑**、檔案的**完整路徑**或**PID**（進程ID）。

  > 當內建代理程式的Kaspersky Endpoint Security以EDR Expert模式運作時，不支援透過系統PID終止進程。

- **移動到隔離區**

  指定要移動的檔案所在的裝置。然後，選擇一個參數，並指定包含所需資訊的jq運算式：要隔離的檔案的**完整路徑**，或檔案的**雜湊值和路徑**。

KASAP回應操作：

- **指派 KASAP 群組**

  指定要移至KASAP學習群組的使用者，然後指定群組ID。

卡巴斯基安全管理中心回應操作：

- **移至群組**

  指定要將裝置移至的群組及其路徑。

KICS for Networks回應操作：

- **變更授權狀態**

  指定裝置及其狀態：*已授權*或*未授權*。

自訂協力廠商回應操作：

- **執行自訂指令碼**

  在對應的欄位中，指定要執行的命令、要套用於該命令的具有命令列參數的jq運算式以及工作目錄的路徑。如果指令碼需要從標準輸入取得其他數據，請在**標準輸入**欄位中指定這些資料。

Kaspersky Threat Intelligence Portal回應操作：

- **擴充資料**

  選擇要擴充物件的數量：所有物件或來自來源的前100個物件。指定一個jq運算式，其中包含要擴充的可觀察物件陣列。您可以擴充以下類型的可觀察物件：MD5、SHA256、URL、網域或 IP 位址。

使用常規程式編輯警示或事件：

- **指派給使用者或群組**

  選擇要將警示或事件指派給的使用者或使用者群組。

- **變更外部參考內容**

  指定一個具有警示或事件外部參考屬性的jq運算式，然後選擇是覆蓋目前輸出資料還是合併目前資料和新資料。

- **變更其他資料**

  選擇是覆蓋目前輸出資料，還是合併目前資料和新資料。

- **變更狀態**

  選擇警示或事件的狀態：**新建**、**執行中**或**已關閉**。如果常規程式範圍是事件，則還需要選擇事件類型。

- **變更類型**

  選擇事件的類型：

  只有在**建立事件編輯**常規程式時，在**範圍**下拉清單中選擇事件時，此操作類型才可用。

- **變更描述**

  指定一個包含事件描述的jq運算式，然後選擇覆蓋目前輸出資料，或合併新資料和目前資料。

  只有在**建立事件編輯**常規程式時，在**範圍**下拉清單中選擇事件時，此操作類型才可用。

- **變更優先順序**

  請選擇事件的優先順序：**緊急**、**高**、**中**或**低**。

  只有在**建立事件編輯**常規程式時，在**範圍**下拉清單中選擇事件時，此操作類型才可用。

- **新增備註**

  為警示或事件指定具有備注的jq運算式。

- 如有需要，請在**其他設定**區段中按一下 V 形箭頭圖示 (>)，然後**指定其他設定**
  - 按一下**終止**或**繼續**按鈕，以選擇發生錯誤時要終止還是繼續執行常規程式。
  - 設定回應操作逾時。您可以選擇**政策**選項，然後指定所需的逾時政策；或選擇**自訂**選項，然後以小時為單位指定逾時時間。
  - 啟用**輸出資料**切換開關，修改常規程式的輸出資料。在**輸出**欄位中，指定用於取代回應操作傳回資料的jq運算式，然後選擇**合併**或**覆蓋**替換方法。
  - 透過啟用**手動核准**切換開關，手動核准回應函式呼叫，然後以分鐘為單位指定核准逾時時間。預設值是60分鐘。

    若要啟用電子郵件通知，請選取**透過電子郵件通知**核取方塊，然後指定傳送電子郵件通知前的延遲時間。最小值為5分鐘，最大值為30分鐘。此外，請確保SMTP伺服器連線已設定，並在使用者內容中指定了電子郵件地址。

- 迴圈

  選擇此類型的步驟後， **迴圈**和**結束迴圈**區塊將會新增至視覺化編輯器。
  - 按一下**迴圈**區塊，指定jq運算式以形成傳入資料陣列，然後選擇**並行**或**順序**模式來處理元素。
  - 如有需要，請在**其他設定**區段中按一下 V 形箭頭圖示 (>)，然後**指定其他設定**
    - 按一下**終止**或**繼續**按鈕，以選擇發生錯誤時要終止還是繼續執行常規程式。
    - 在**批次大小上限**欄位中，指定常規程式可以作為輸入的元素數量。
    - 設定規則，將常規程式執行的結果彙總到傳入陣列的元素上。啟用**彙總結果**切換開關後，在**表達式**欄位中指定jq運算式，以便將輸出資料用作後續執行步驟的輸入資料。
    - 透過在**輸出**欄位中指定jq運算式來修改輸出資料。
    - 點選**合併**或**覆蓋**按鈕，選擇是覆寫目前輸出資料，還是合併新資料和目前資料。

- 並行

  選擇此步驟類型後，**並行** 並將**並行結束**區塊隨即新增到可視化編輯器中。
  - 點擊**並行** 區塊，指定一個jq運算式來產生傳入資料陣列，然後輸入分支名稱。

    您可以透過點擊**新增分支**來新增分支。
  - 如有需要，請在**其他設定**區段中按一下 V 形箭頭圖示 (>)，然後**指定其他設定**
    - 按一下**終止**或**繼續**按鈕，以選擇發生錯誤時要終止還是繼續執行常規程式。
    - 設定規則，將常規程式執行的結果彙總到傳入陣列的元素上。啟用**彙總結果**切換開關後，在**運算式**欄位中，指定jq運算式，以便將輸出資料用於後續執行步驟。
    - 透過在**輸出**欄位中指定jq運算式來修改輸出資料。
    - 點選**合併**或**覆蓋**按鈕，選擇是覆寫目前輸出資料，還是合併新資料和目前資料。

- 決定

  選擇此步驟類型後，**決定**和**決策結束**區塊隨即新增到可視化編輯器中。點擊**決定**區塊，指定一個具有條件的jq運算式，以及條件名稱。

根據需要，請點選**新增條件**按鈕來新增條件。

- **更新資料**
  在**輸出**欄位中指定jq運算式，然後選擇是覆蓋目前輸出資料，還是合併新資料和目前資料。

您可以使用常規程式執行步驟執行以下操作：

- 按一下執行步驟區塊進行編輯，然後在開啟的內容視窗中，變更所需的參數。

  對於需要輸入jq運算式的參數，當您開始輸入時，語法會被高亮顯示，並且會顯示建議。

- 透過點擊並拖動執行步驟區塊，在視覺化編輯器工作區域中移動。
- 點選執行步驟區塊，然後按**退格鍵**或**刪除鍵**進行刪除。

在工具列中，您可以進行以下操作：

- 按一下**設定**按鈕，開啟**常規程式設定**窗格。
- 點選**顯示程式碼**按鈕，開啟包含DSL架構的程式碼編輯器。
  您可以點擊（⌃）圖示來延伸程式碼窗格，然後按一下（×）圖示來關閉窗格。
- 按一下**複製演算法**按鈕，即可從另一個常規程式複製演算法。
- 按一下檢視回應歷程記錄**檢視回應歷史記錄回應歷程記錄**。
- 按一下在測試模式下啟動**以測試模式啟動模擬啟動常規程式**，而無需實際執行回應操作。
- 按一下**撤銷**按鈕，即可在視覺化編輯器中撤銷任何操作。
- 按一下**重做**按鈕，即可復原先前未執行的操作。
- 按一下**排列**按鈕，即可自動對齊元素。

編輯常規程式

若要編輯常規程式，您必須具有以下角色之一：主管理員、 SOC管理員、一級分析師、二級分析師、租用戶管理員。

對於預先定義的常規程式，您只能更改常規程式模式和啟動規則。您也可以檢視與預定義常規程式相符的警示或事件。

只有當您具有更改常規程式所屬租用戶的權限時，才可以編輯常規程式。

若要編輯政策，請執行以下操作：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 點擊您要編輯的常規程式名稱。
3. 在開啟的視窗中，編輯常規程式內容。有關可編輯的常規程式內容的更多詳細資訊，請參閱建立常規程式。
4. 如果您將運作模式變更為**自動**，請在**同時啟動多個常規程式實例時**下拉清單中選擇以下操作之一：
   - **將新的常規程式實例新增至佇列**。新的常規程式實例將在目前實例完成後啟動。預設情況下已選定此操作。
   - **終止目前執行並啟動新實例**。目前常規程式實例的執行將被終止。之後，將啟動一個新的常規程式實例。
   - **請勿啟動新的常規程式實例**。不會啟動新的常規程式實例。目前常規程式實例的執行將繼續。
5. 如果您將操作模式變更為**手動**，請在**對已啟動常規程式實例執行的動作**下拉清單中，選擇要套用於啟動常規程式實例的操作：
   - **終止正在進行或等待核准的實例**。
   - **僅終止正在等待核准的實例**。
   - **執行所有正在進行或等待核准的實例**。
6. 點選**儲存**按鈕儲存變更。
   如果您想在儲存之前為常規程式新增備注，也可以按一下**儲存並新增註解**按鈕。

常規程式的內容被修改並保存。

自訂常規程式

您可以根據需要自訂任何常規程式。

若要自訂常規程式：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 從清單中選擇常規程式，然後按一下**重複並編輯**按鈕，即可開啟常規程式進行編輯。
3. 在開啟的視窗中，根據您的需求設定常規程式的內容。
   有關可編輯的常規程式內容的更多詳細資訊，請參閱建立常規程式。
   若要自訂常規程式演算法參數，請參閱常規程式演算法。

   > 自訂常規程式的名稱必須是唯一的。

4. 點擊**儲存**按鈕。

自訂的常規程式隨即修改並儲存。

檢視常規程式內容

常規程式可讓您自動化工作流程並減少處理警示和事件所需的時間。

若要檢視常規程式，您必須具有以下角色之一：主管理員、 SOC管理員、一級分析師、二級分析師、 SOC管理員、核准人、稽核員、租用戶管理員。

若要檢視常規程式的內容：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 在常規程式清單中，按一下要檢視的常規程式名稱。

   開啟的視窗包含有關常規程式的資訊。

在右側的**常規程式設定**窗格中，顯示以下一般資訊：

- **租用戶和繼承**。常規程式所屬租用戶的名稱。
- **名稱**。常規程式的名稱。
- **範圍**。常規程式的範圍。可能的值：**警示**或**事件**。
- **操作模式**。常規程式運作模式。可能的值：**自動**、**培訓**、**手動**。

  如果將常規程式運作模式設為**自動**，則會顯示**同時啟動多個常規程式實例時**檔案。可能的值：**請勿啟動新的常規程式實例**、**終止目前執行並啟動新實例**、**將新的常規程式實例新增至佇列**。
- **標籤**。指派給常規程式的標籤。
- **描述**。常規程式的描述。
- **其他設定**。建立常規程式時指定的可選設定。

左側的視覺化編輯器工作區中顯示了常規程式觸發器和演算法（常規程式執行步驟）。

如果您擁有以下角色之一，則可以編輯常規程式的內容：主管理員、SOC管理員、一級分析師、二級分析師、租用戶管理員。

您可以透過點選工具列中的**檢視回應歷史記錄**按鈕來檢視常規程式的回應歷史記錄。常規程式中啟動的所有常規程式或回應操作的清單將開啟。您可以透過點選**終止**按鈕來終止任何已啟動的常規程式或回應操作。

如有需要，您可以對表格中的資料進行分組和篩選，如下所示：

- 點選設定圖示 (⚙)，然後選擇要在表格中顯示的欄位。
- 點選篩選圖示 (⧩)，然後在開啟的功能表中指定並套用篩選條件。

> 當您對**狀態**列套用篩選條件時，該表會顯示狀態包含所選值的手動啟動的回應，以及包含狀態包含所選值的回應動作的常規程式。這意味著只會顯示符合篩選條件的常規程式的回應操作。

顯示篩選後的常規程式表格。

資源表包含以下列：

- **動作**。回應操作名稱。
- **回應參數**。常規程式演算法中指定的回應操作參數。
- **開始**。啟動常規程式或回應操作的日期和時間。
- **結束**。常規程式或回應操作完成的日期和時間。
- **警示或事件 ID** 。包含指向警示或事件詳細資訊的連結的ID。
- **啟動者**啟動常規程式或回應操作的使用者的名稱。
- **核准者**。核准啟動常規程式或回應操作的使用者的名稱。
  預設情況下，此列處於隱藏狀態。若要顯示此列，請按一下設定圖示（⚙），然後選擇**核准者**列。
- **核准時間**。使用者確認或拒絕啟動常規程式或回應操作的日期和時間。
  預設情況下，此列處於隱藏狀態。若要顯示此列，請按一下設定圖示（⚙），然後選擇**核准時間**列。
- **狀態**。常規程式的執行狀態。此列可以顯示以下值：
  - **等待核准**—常規程式正在等待啟動核准。
  - **進行中**—常規程式正在執行中。
  - **成功**— 常規程式已完成，沒有錯誤或警告。
  - **警告**—常規程式已完成，但有警告。
  - **錯誤**—常規程式已完成，但有錯誤。
  - **已停止**—常規程式已完成，因為使用者中斷了執行。
  - **核准時間已過**—常規程式已完成，因為啟動的核准時間已過。
  - **被拒絕**—常規程式已完成，因為使用者拒絕了啟動。

您可以點選**狀態**值開啟包含常規程式啟動結果的視窗。技術支援可以使用啟動ID下載執行錯誤時分析所需的資料。預設情況下，資料會儲存 72 小時。
如果狀態為 **進行中**，您可以將滑鼠游標停留在狀態旁的圖示上，以檢視啟動ID。

- **資產**。啟動常規程式或回應操作的資產數量。您可以點選包含資產數量的連結來檢視資產詳情。如果常規程式或回應操作不涉及資產，則該欄位為空。

您也可以從**回應歷史**部分或從警示或事件詳細資訊檢視回應歷史記錄。

終止常規程式

您可以強制終止已啟動的常規程式。在這種情況下，未完成的回應操作將被終止。常規程式終止後，已完成的回應操作不會被取消。

若要終止常規程式，您必須具有以下角色之一：主管理員、一級分析師、二級分析師、租用戶管理員。

若要終止常規程式：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 在開啟的視窗中，執行以下其中一項操作：
   - 選擇所需的常規程式，然後在工具列中按一下**檢視歷史記錄**按鈕。
   - 按一下所需常規程式的名稱，然後在開啟的視窗中按一下**檢視歷史記錄**按鈕。
3. 選擇**檢視回應歷史記錄**。
   包含已啟動的常規程式實例清單的窗格將開啟。
4. 選擇要終止的一個或多個實例，然後按一下**終止**按鈕並確認選擇。

常規程式將終止。

刪除常規程式

預定義常規程式無法被刪除。

若要刪除自訂常規程式，您必須具有以下角色之一：主管理員、SOC管理員、一級分析師、二級分析師、租用戶管理員。

若要刪除自訂常規程式：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 從清單中選擇常規程式，然後按一下**刪除**按鈕。

3. 在確認對話方塊，按一下**刪除**。

> 如果有啟動的常規程式實例，則無法刪除常規程式。在這種情況下，請終止所有啟動的實例，然後再刪除常規程式。

如果您刪除了處於**作用中**或**不可用**狀態的常規程式，則該常規程式將以**已刪除**狀態顯示在已刪除中，並且僅可檢視和複製。

> **已刪除**狀態的常規程式將永久刪除。

管理常規程式版本

Kaspersky Next XDR Expert會儲存常規程式的版本記錄。建立常規程式或儲存現有常規程式的變更時，會自動建立新版本。您只能在常規程式發布後管理其版本。版本管理不適用於常規程式草稿。

新發布的常規程式會被指派版本 `1`。每次儲存變更時，版本號碼都會加一。最新儲存的版本在版本清單中標記為 `Current`。

如果您是從Kaspersky Next XDR Expert 2.0版本升級，首次編輯現有常規程式後，系統會自動為其指派版本號。現有常規程式的先前版本也會被儲存，以便與最新版本進行比較。

比較常規程式版本

Kaspersky Next XDR Expert允許您比較常規程式的不同版本，以便追蹤變更並簡化版本管理。

> 為此，您必須擁有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、一級分析師、二級分析師、SOC經理、批准人、稽核員。

要比較常規程式版本：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 在常規程式清單中，選擇要比較版本的常規程式。
3. 按一下**檢視歷史記錄**按鈕，然後選擇**檢視版本歷史記錄**。

   常規程式版本歷史記錄視窗隨即開啟。
4. 在常規程式版本清單中，選擇兩個版本進行比較，然後按一下**比較**按鈕。

   顯示常規程式版本差異的視窗隨即顯示。請注意，您無法在此視窗中編輯常規程式。

   如有必要，在開啟的視窗中，您可以選擇不同的常規程式版本進行比較。

常規程式版本隨即比較。

還原常規程式版本

您可以隨時恢復到常規程式的先前版本。

為此，您必須具有以下XDR角色之一：主管理員、租用戶管理員、SOC管理員、一級分析師、二級分析師。

若要恢復常規程式版本：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 在常規程式清單中，選擇要恢復先前版本的常規程式。
   或者，您可以點擊常規程式名稱。
3. 按一下**檢視歷史記錄**按鈕，然後選擇**檢視版本歷史記錄**。
   常規程式版本歷史記錄視窗隨即開啟。
4. 在常規程式版本清單中，找到要恢復的版本。
   如果要查看所選常規程式版本的詳細資訊，請按一下版本名稱。
5. 在**動作**直欄中，按一下**還原**按鈕。
6. 在開啟的確認對話方塊中，按一下**還原**。
   如有必要，您可以新增備注。如果您不新增註釋，系統會自動新增一條，指示恢復常規程式的版本。

先前版本的常規程式隨即恢復。

以測試模式啟動常規程式

您可以以測試模式啟動常規程式來進行偵錯或驗證結果。在測試執行期間，常規程式會處理選定的警示和事件，但不會對資產執行任何操作。

任何狀態的常規程式都可以以測試模式啟動。

若要在測試操作模式中啟動常規程式，您必須具有下列其中一種角色：主管理員、初級分析師、一級分析師、二級分析師、租用戶管理員。

若要在測試模式下啟動常規程式：

1. 在主功能表中，轉至**監控→常規程式**。
2. 執行以下操作之一：
   - 點擊您要編輯的常規程式名稱。在開啟的**常規程式詳情**視窗中，按一下**以測試模式啟動**按鈕。
   - 從清單中選擇常規程式，然後按一下**以測試模式啟動**按鈕。
     根據常規程式的範圍，將喚起**選取事件**或**選取警示**窗格。

3. 在喚起的窗格中選擇事件或警示。

   如果常規程式需要選擇可觀察物件和資產，請啟用**在啟動常規程式之前選取目標物件**選項。

4. 按一下**啟動**。

   如果啟用了**在啟動常規程式之前選取目標物件**選項，則會喚起**目標物件**。從**可觀測項**和**資產**頁籤中選擇要為其啟動常規程式的物件，然後按一下**套用並啟動**按鈕。

5. **以測試模式啟動的常規程式**彈出視窗隨即出現。測試運行結束後，**常規程式以測試模式完成**彈出視窗隨即顯示。點擊此彈出視窗中的**檢視結果**連結，即可顯示包含結果的窗格。如果測試運行成功，**常規程式成功**窗格隨即喚出。如果測試運行失敗，**常規程式錯誤**窗格隨即喚出。

   測試運行結果儲存在常規程式的**回應歷史**部分。測試運行結果不會顯示在一般回應歷史部分中。

啟動常規程式和回應操作

啟動常規程式

您可以根據需要設定啟動常規程式的方式。您可以在常規程式建立期間選擇以下運作模式之一：

- **自動**。如果您要自動啟動常規程式和回應操作，請選擇此運作模式。

  此模式下的常規程式有助於自動化威脅回應，並減少分析警示和事件所需的時間。

- **培訓**。如果要檢查常規程式是否設定正確，請選擇此運作模式。

  當偵測到相應的警示或事件時，此模式的常規程式不會自動啟動。相反，常規程式會請求使用者核准啟動。

- **手動**。如果您只想手動啟動常規程式，請選擇此運作模式。

  此模式下的常規程式沒有觸發器，因此您可以根據所選的常規程式範圍針對任何警示或事件啟動此類常規程式。有關更多詳細資訊，請參閱手動啟動常規程式。

您也可以變更現有常規程式的運作模式。有關更多詳細資訊，請參閱編輯常規程式。

啟動回應操作

回應操作可以手動啟動、在常規程式中自動啟動，也可以設定在常規程式中啟動之前請求使用者核准。預設情況下，回應操作的手動核准是停用的。

有關如何設定在常規程式中啟動的回應操作的手動核准的更多詳細資訊，請參閱設定手動核准回應操作。

手動啟動常規程式

Kaspersky Next XDR Expert可讓您手動啟動與您想要回應的警示或事件相符的任何常規程式。

若要手動啟動常規程式，您必須具有以下角色之一：主管理員、一級分析師、二級分析師、租用戶管理員。

如果您在建立和啟動常規程式時指定了可觀察物件和資產，您也可以啟動這些物件的常規程式。

啟動警示的常規程式

若要手動啟動警示的常規程式：

1. 在主選單中，轉到**監控→警示**部分。
2. 在警示表中，按一下要為其啟動常規程式的警示ID的連結。
3. 在開啟的**警示詳細資訊**視窗中，按一下**選取常規程式**按鈕。
   選取常規程式視窗將開啟。
4. 在與警示相符的常規程式清單中，選擇要啟動的常規程式，然後按一下**啟動**按鈕。
   如果所選的常規程式已針對此警示執行，請在出現的**監控**視窗中執行下列其中一項：
   - 如果您想等到目前常規程式實例完成，請按一下**等待並啟動**按鈕。
     新的常規程式實例將在目前實例完成後啟動。
   - 如果您想立即啟動新的常規程式實例，請按一下**終止並啟動新的**按鈕。
     目前的常規程式實例將被終止，新的常規程式實例將啟動。
   - 如果您想取消新的常規程式啟動，請按一下**關閉**按鈕（✕）。

   如果選定的常規程式已經具有**等待核准**狀態，則手動啟動後，常規程式狀態將變更為**已啟動**。

常規程式已針對選定警示啟動。常規程式完成後，您將收到通知。

為事件啟動常規程式

若要為事件手動啟動常規程式：

1. 在主選單中，轉至**監控→事件**，然後選擇**XDR 事件**頁籤。
2. 在事件表中，按一下要為其啟動常規程式的事件ID的連結。
3. 在開啟的**事件詳情**視窗中，按一下**選取常規程式**按鈕。
   選取常規程式視窗將開啟。
4. 在與事件相符的常規程式清單中，選擇要啟動的常規程式，然後按一下**啟動**按鈕。
   如果選定的常規程式已針對此事件運行，則在出現的**監控**視窗中，執行下列其中一項操作：
   - 如果您想等到目前常規程式實例完成，請按一下**等待並啟動**按鈕。
     新的常規程式實例將在目前實例完成後啟動。

- 如果您想立即啟動新的常規程式實例，請按一下**終止並啟動新的**按鈕。
  目前的常規程式實例將被終止，新的常規程式實例將啟動。
- 如果您想取消新的常規程式啟動，請按一下**關閉**按鈕（ × ）。

如果選定的常規程式已經具有**等待核准**狀態，則手動啟動後，常規程式狀態將變更為**已啟動**。

常規程式針對選定的事件啟動。常規程式完成後，您將收到通知。

為使用者指定的物件啟動常規程式

您可以指定常規程式必須執行的可觀察物件和資產。您必須使用下列設定建立常規程式：

- 在**範圍**清單中，選擇**警示**或**事件**。
- 在**操作模式**清單中，選擇**手動**。
- 在視覺化編輯器的工作區中，在視覺化編輯器中設定常規程式執行步驟時，使用 jq 運算式指定您要為其啟動常規程式的物件（可觀察物件或資產）。這些物件將成為常規程式啟動時的輸入內容。

如果您未在常規程式演算法中指定物件，而只是在啟動常規程式之前選擇它們，則這些物件將被忽略。

建立常規程式後，您可以針對所選物件啟動它。

若要終止常規程式，您必須具有以下XDR角色之一：主管理員、一級分析師、二級分析師、租用戶管理員。

若要為選定物件啟動常規程式：

1. 在主功能表中，轉至**監控**部分，然後在**警示**或**事件**部分，按一下要從中啟動常規程式的警示或事件的ID。
2. 在開啟的事件詳情視窗中，按一下**選取常規程式**按鈕。
   選取常規程式視窗將開啟。
3. 選取**啟動常規程式前選擇目標物件**選項，然後按一下**啟動**按鈕。
4. 在開啟的**目標對象**視窗中，從**可觀察物件**和**資產**標籤中選擇要為其啟動常規程式的物件，然後按一下**套用並啟動**按鈕。
   常規程式針對選定的物件啟動。

   您可以在警示或事件詳情中的**歷史記錄**頁籤中檢視常規程式的結果，透過點擊檢視歷程記錄按鈕，從**常規程式詳情**或檢視歷史記錄中，以及從回應歷程記錄部分檢視常規程式的結果。

例如，您可以編寫一個在executeCustomScript回應操作期間呼叫的指令碼。建立常規程式時，在視覺化編輯器工作區域中，您可以新增具有常規程式輸入資料的**執行自訂指令碼**執行步驟。然後，您必須為在啟動常規程式時選擇的IP類型的可觀察物件執行指令碼。指令碼使用您選擇的IP位址作為參數：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
```

```
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "executeCustomScript",
                    "params": {
                        "commandLine": "./script.py",
                        "commandLineParameters": "${ \"-ip \" + ([.input.observables[] | select(.type == \"ip\")]
| map(.value) | join(\",\")) }",
                        "workingDirectory": "/folder/with/script"
                    }
                },
                "onError": "stop"
            }
        },
      {
        "action": {
          "function": {
            "type": "updateBases",
            "params": {
              "wait": false
            },
            "assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
          }
        }
      }
    ]
}
```

常規程式將以多個物件作為輸入，其中以逗號分隔的IP位址清單必須作為指令碼的輸入：

```
{
    "input": {
        "observables": [
            {
                "type": "ip",
                "value": "127.0.0.1"
            },
            {
                "type": "ip",
                "value": "127.0.0.2"
            },
            {
                "type": "md5",
                "value": "29f975b01f762f1a6d2fe1b33b8e3e6e"
            }
        ],
        "assets":[
      {
         "AttackerOrVictim": "unknown",
         "ID": "c13a6983-0c40-4986-ab30-e85e49f98114",
         "InternalID": "6d831b04-00c2-44f4-b9e3-f7a720643fb7",
         "KSCServer": "E5DE6B73D962B18E849DC0BF5A2BA72D",
         "Name": "VIM-W10-64-01",
         "Type": "host"
      }
   ]
}
```

jq運算式對常規程式操作資料執行計算後，會將下列資訊作為命令列參數傳遞：

```
-ip 127.0.0.1,127.0.0.2
```

對於需要輸入資料的常規程式，如果您在建立常規程式時和啟動常規程式時指定了不同類型的物件，或者如果您沒有選擇**啟動常規程式前選擇目標物件**選項，則常規程式將以以下結果之一結束：

- 由於常規程式未收到輸入資料，因此會發生錯誤。
- 由於常規程式中包含基於輸入資料的條件或循環，因此不會執行此操作。
- 結果將取決於執行該操作的應用程式、服務或指令碼的回應。

以訓練操作模式啟動常規程式

培訓操作模式可讓您檢查常規程式是否設定正確。如果您打算將常規程式操作模式變更為**自動**，這將很有幫助。

培訓操作模式下的所有常規程式都需要使用者核准才能啟動。

要在**培訓**操作模式中啟動常規程式，您必須具有下列其中一種角色：主管理員、一級分析師、二級分析師、租用戶管理員。

在**培訓**操作模式下，常規程式由警示或事件觸發，但需要手動核准才能啟動。您可以透過以下其中一種方式在**培訓**操作模式下測試啟動常規程式：

- 建立與常規程式觸發器相符的警示或事件。
- 編輯與常規程式觸發器相符的警示或事件。警示或事件必須處於**已關閉**以外的狀態。

  僅當觸發器設定為回應手動變更時，編輯警示或事件才會觸發常規程式。預設情況下，對警示或事件的手動變更將被略過。為使常規程式回應手動變更，觸發器必須使用`event.manual`函式。如需詳細資訊，請參閱常規程式觸發器。

完成上述操作之一後，常規程式將請求使用者核准啟動。有關如何核准常規程式的更多信息，請參閱核准常規程式或回應操作。

啟動常規程式的手動核准時間限制為60分鐘。

設定回應操作的手動核准

Kaspersky Next XDR Expert可讓您設定在自訂常規程式中啟動的回應操作的手動核准。預設情況下，回應操作的手動核准是停用的。

在設定手動核准之前，請確保已設定租用戶的電子郵件通知並已指定核准人的電子郵件地址。

我們建議您設定以下回應操作的手動核准：將裝置移至另一個管理群組、將檔案移至隔離區、啟用和停用網路隔離、透過Active Directory回應帳戶以及資料擴充。

若要設定回應操作的手動核准：

1. 在主功能表中，轉至**監控→指令劇本**。
2. 透過執行下列操作之一開啟常規程式：
   - 點擊您要編輯的常規程式名稱。在開啟的**常規程式詳情**視窗中，按一下**編輯**按鈕。
   - 從清單中選擇常規程式，然後按一下**編輯**按鈕。
     如果您選擇了多個項目，**編輯**按鈕將被停用。

   編輯常規程式視窗將開啟。
3. 在**演算法**部分中，為要啟用手動核准的回應操作指定下列參數之一：
   - 若要啟用具有預設核准時間的回應操作的手動核准，請指定下列參數：

     ```
     "manualApprove": true
     ```

     預設情況下，核准時間為5分鐘。
   - 若要啟用具有可調整核准時間的回應操作的手動核准，請指定以下參數：

     ```
     "manualApprove": {"timeout": "period"}
     ```

     其中「`period`」為可調整的核准時間。
     您能以小時（h）及/或分鐘（m）為單位設定最大執行時間。

     ```
     "manualApprove": {"timeout": "20h"}
     "manualApprove": {"timeout": "2h30m"}
     ```
   - 若要啟用手動核准回應操作並將通知傳送至核准人的電子郵件地址，請指定下列參數：

     ```
     "emailNotifications": {
      "enabled":true
     }
     ```

- 若要啟用手動核准回應操作並在一定時間後將通知傳送至核准人的電子郵件位址，請指定以下參數：

```
"manualApprove": {
  "emailNotifications": {
    "enabled": true,
    "delay": "period"
  }
```

其中「`period`」是可調整的傳送時間。

您可以分鐘（m）為單位設定傳送時間，例如：

```
"delay": "20m"
```

4. 按一下**儲存**按鈕。

已設定手動核准回應操作。包含核准回應操作請求的電子郵件通知將傳送至使用者帳戶內容中指定的電子郵件地址。

您可以在核准請求**核准請求檢視核准回應操作的請求**。

核准常規程式或回應操作

培訓運作模式下的所有常規程式都需要使用者核准。您也可以設定手動核准常規程式內啟動的回應操作。

若要核准或拒絕常規程式啟動，您必須具有以下角色之一：主管理員、一級分析師、二級分析師、租用戶管理員。

若要核准或拒絕回應操作啟動，您必須具有以下角色之一：主管理員、核准人、租用戶管理員。

如果有任何常規程式或回應正在等待使用者核准，OSMP 控制台上方會顯示通知。此外，如果回應操作啟動需要使用者核准，則會在常規程式指定的時間段內向電子郵件地址發送電子郵件通知。

檢視常規程式和回應操作清單

若要檢視等待核准的常用程式和回應操作，請執行以下其中一項操作：

- 按一下 OSMP 控制台上方的**檢視核准請求**連結。
- 依照發送到您電子郵件地址的通知中的連結操作。

將開啟**核准請求**窗格，其中包含包含完整核准請求清單的表格。

核准請求表格包含以下欄：

- **時間**。常規程式或回應操作請求使用者核准的日期和時間。
- **核准到期日**。使用者必須核准或拒絕常規程式或回應操作的日期和時間。如果使用者在此時間之前未核准常規程式或回應操作，則啟動將被取消。
- **常規程式**。請求用戶核准的自訂或預定義常規程式的名稱。
- **回應動作**。在常規程式中啟動的操作。
- **資產**。啟動常規程式或回應操作的資產數量。您可以透過點選包含資產數量的連結來檢視請求使用者批准的資產清單。
- **回應參數**。在回應操作或常規程式演算法中指定的回應操作參數。
- **警示或事件 ID** 。包含指向警示或事件詳細資訊的連結的ID。

核准和拒絕常規程式

若要核准或拒絕常規程式：

1. 在 OSMP 主控台頂端的通知中，按一下 **檢視核准請求**連結。

   只有當存在等待使用者核准的常規程式時，才會顯示具有**檢視核准請求**連結的通知。

2. 在開啟的**核准請求**窗格中，選擇一個或多個常規程式，然後執行下列其中一項操作：

   - 若要核准啟動常規程式，請按一下**批准**按鈕。
     之後，常規程式將會啟動。**回應歷史**部分中的操作狀態將變更為**進行中** 。
   - 若要拒絕啟動常規程式，請按一下**拒絕**按鈕。
     之後，常規程式的啟動將會取消。**回應歷史**部分中的操作狀態變更為**被拒絕**。

3. 按一下**關閉**按鈕（ ✕ ）以關閉**核准請求**窗格。

核准或拒絕常規程式後，您可以在**回應歷史**部分檢視其狀態。

批准和拒絕回應操作

若要批准或拒絕回應操作：

1. 在 OSMP 主控台頂端的通知中，按一下 **檢視核准請求**連結。

   只有當有回應操作等待使用者核准時，才會顯示具有**檢視核准請求**連結的通知。

核准請求窗格將開啟。

2. 在開啟的**核准請求**窗格中，在**資產**列中，按一下具有資產數量的連結。

   包含完整資產清單的**待核准資產**窗格將開啟。

3. 檢查需要手動核准的資產列表，然後執行以下其中一項操作：

   - 要核准啟動資產的回應操作，請選擇您需要的一個或多個資產，然後按一下**批准**按鈕。之後，將啟動所選資產的回應操作。
   - 若要拒絕啟動資產的回應操作，請選擇所需的一個或多個資產，然後按一下**拒絕**按鈕。之後，將取消啟動所選資產的回應操作。

4. 按一下**關閉**按鈕（ ✕ ）以關閉**待核准資產**窗格。

5. 按一下**關閉**按鈕（ ✕ ）以關閉**核准請求**窗格。

核准或拒絕回應操作後，您可以在**回應歷史**區段中檢視其狀態。

從常規程式擴充

設定Kaspersky Next XDR Expert與Kaspersky TIP之間的整合後，您可以從Kaspersky TIP或Kaspersky OpenTIP取得與警示或事件相關的可觀察物件的信譽資訊，然後擴充取得的資料。

您只能取得以下類型的可觀察物件的資訊：網域、URL、IP、MD5、SHA256。

您可以設定資料擴充自動執行。為此，在建立或編輯常規程式時，必須在視覺化編輯器工作區域中新增在視覺化編輯器中設定常規程式執行步驟，並指定以下內容：

1. 如有必要，限制 Kaspersky TIP 或 Kaspersky OpenTIP 傳回的資料。

   您可以指定以下其中一個值。

   - 所有記錄
   - Top100

     預設設定此值。

2. 常規程式從 Kaspersky TIP 或 Kaspersky OpenTIP 請求資料的可觀察物件。

   使用與Kaspersky Threat Intelligence Portal整合中指定的服務來執行資料擴充。

在常規程式演算法中，您可以使用 Kaspersky TIP 傳回欄位中顯示的輸出擴充參數。

您可以透過以下其中一種方式檢視與警示或事件相關的所有可觀察物件的擴充結果：

- 從警示或事件詳細資訊
- 從回應歷史記錄
- 從常規程式

若要檢視擴充結果：

1. 在主功能表中，轉至**監控**部分，然後執行以下操作之一：
   - 如果要檢視警示或事件詳細資料的結果，請轉至**警示**或**事件** 部分，然後按一下執行了擴充的警示 ID 或事件 ID。在開啟的視窗中，轉到**歷程記錄**頁籤，然後選擇**回應歷程記錄**頁籤。
   - 如果要檢視回應歷程記錄的結果，請轉至**回應歷史**部分。
   - 如果要檢視常規程式表中的結果，請轉至**指令劇本**部分，然後執行以下操作之一：
     - 選擇執行了擴充的常規程式。在工具列中，按一下**檢視歷史記錄**按鈕，然後選擇**檢視回應歷史記錄**。
     - 點擊執行了擴充的常規程式的名稱。在開啟的視窗中，按一下**檢視歷史記錄**按鈕，然後選擇**檢視回應歷史記錄**。
2. 在**動作狀態**直欄中，按一下要檢視擴充結果的常規程式的狀態。

您也可以從 Kaspersky TIP 取得資訊，然後在**警示**或事件詳情中的可觀察物件頁籤上手動擴充資料。

檢視回應歷史記錄

回應歷史部分可讓您檢視所有偵測到的警示和事件的詳細回應歷史記錄。請注意，如果刪除了警示或事件，則不會顯示此警示或事件的回應歷史記錄。

若要檢視回應歷程記錄，您必須具備下列角色之一：主管理員、一級分析師、二級分析師、 SOC管理員、初級分析師、核准人、稽核員和租用戶管理員。

若要檢視回應歷史記錄，在主功能表中，轉至**監控→回應歷史**。包含所有警示和事件的回應歷史記錄的表格將開啟。

預設情況下，表格會根據啟動常規程式或回應操作的時間排序。常規程式中的回應操作根據它們在常規程式演算法中的順序排序。

表格上部的工具列可讓您以下列方式分組並篩選表格中的資料：

- 點擊設定圖示 ( )，然後選擇要在表中顯示的列。
- 點擊篩選圖示 ( ), 然後在喚起的功能表中指定並套用篩選條件。

  當您對**動作狀態**列套用篩選條件時，表格會顯示狀態包含所選值的手動啟動的回應，以及包含狀態包含所選值的回應操作的常規程式。這意味著只會顯示符合篩選條件的常規程式的回應操作。

表格搜尋適用於除**動作狀態**和**常規程式狀態**以外的所有欄位。若要篩選這些列中的資料，請按一下列標題並從下拉清單中選擇所需的狀態。

資源表包含以下列：

- **動作**。回應操作或常規程式名稱。
- **回應參數**。在回應操作或常規程式演算法中指定的回應操作參數。
- **開始**。啟動常規程式或回應操作的日期和時間。
- **結束**。常規程式或回應操作完成的日期和時間。
- **警示或事件 ID** 。包含指向警示或事件詳細資訊的連結的ID。
- **啟動者**。啟動常規程式或回應操作的使用者的名稱。
- **動作狀態**。回應操作的執行狀態。此列可以顯示以下值：
  - **等待核准**— 等待核准啟動的回應操作。
  - **進行中**— 回應操作正在執行中。
  - **成功**— 回應操作已完成，沒有錯誤或警告。
  - **警告**— 回應操作已完成，但有警告。
  - **錯誤**— 回應操作已完成，但有錯誤。
  - **已停止**— 由於使用者中斷了執行，回應操作已完成。
  - **核准時間已過**— 由於啟動的核准時間已過，回應操作已完成。
  - **被拒絕**— 由於使用者拒絕了啟動，回應操作已完成。

  > 已啟用網路隔離的裝置，可能會在隔離程序完成前收到**成功**狀態。

- **常規程式狀態**。常規程式的執行狀態。此列可以顯示以下值：
  - **等待核准**—常規程式正在等待啟動核准。
  - **進行中**—常規程式正在執行中。
  - **成功**— 常規程式已完成，沒有錯誤或警告。
  - **警告**—常規程式已完成，但有警告。
  - **錯誤**—常規程式已完成，但有錯誤。
  - **已停止**—常規程式已完成，因為使用者中斷了執行。
  - **核准時間已過**—常規程式已完成，因為啟動的核准時間已過。
  - **被拒絕**—常規程式已完成，因為使用者拒絕了啟動。

您可以按一下**常規程式狀態**值或**動作狀態**值以開啟窗口，其中包含常規程式或回應操作啟動的結果。在出現執行錯誤時，技術支援可以使用**偵錯資料**頁籤上顯示的啟動ID來下載分析所需的資料。預設情況下，資料會儲存 72 小時。
如果狀態為 **進行中**，您可以將滑鼠游標停留在狀態旁的圖示上，以檢視啟動ID。

- **資產**。啟動常規程式或回應操作的資產數量。您可以點選包含資產數量的連結來檢視資產詳情。如果常規程式或回應操作不涉及資產，則該欄位為空。
- **租用戶**。常規程式所屬租用戶的名稱。
- **批准者**。核准或拒絕常規程式或回應操作啟動的使用者的姓名。
  預設情況下，此列處於隱藏狀態。若要顯示此列，請按一下設定圖示（ ），然後選擇**批准者**列。
- **核准時間**。核准或拒絕常規程式或回應操作啟動的日期和時間。預設情況下，此列不顯示。
  預設情況下，此列處於隱藏狀態。若要顯示此列，請點選設定圖示（ ），然後選擇**核准時間**列。

預定義常規程式

Kaspersky Next XDR Expert提供由卡巴斯基專家建立的即用型預定義常規程式。預定義常規程式基於KUMA關聯規則運作。有關分發套件中包含的KUMA關聯規則的更多資訊，請參閱關聯規則。

您可以在常規程式部分找到預定義**指令劇本**。此類常規程式標有**預先定義**標籤，名稱具有[KL]前綴。

請注意，除了**操作模式**和**對已啟動常規程式實例執行的動作**欄位外，您無法編輯預定義常規程式的參數。如果要編輯預訂常規程式的其他參數，則需要複製該常規程式，然後將其用作範本來建立自訂常規程式。如需詳細資訊，請參閱自訂常規程式。

在使用預定義常規程式之前，您必須在KUMA中執行以下操作：

- 配置事件擴充的規則設置，並選擇**事件**類型作為**來源類型**設定。指定目標欄位中VictimUserID和AttackerUserID 的值。
- 在KUMA中設定擴充功能以取得Windows事件日誌。

預定義常規程式無法被刪除。

預定義常規程式屬於父租用戶，並由所有子租用戶繼承。

[KL] P001「辦公室應用程式建立可執行檔」

此常規程式包含透過KASAP回應操作，且只能用作範本。若要啟動此常規程式，請按一下**重複並編輯**按鈕。在開啟的視窗中，在**指派 KASAP 群組**操作中，指定KASAP群組ID。

使用此常規程式之前，必須在KUMA中設定擴充功能以取得Windows事件日誌。

預設情況下，該常規程式會針對警示中的所有使用者啟動回應操作。若要該常規程式僅針對受害者帳戶啟動回應操作，可以執行下列操作：

1. 在KUMA中，配置擴充規則設定。對於**事件**類型設定為**來源類型**的事件擴充，請在**目標欄位**中指定**VictimUserID**值。
2. 在**指派 KASAP 群組**操作中，在**資產**欄位中指定 `and .IsVictim`，如下所示：

   ```
   [ alert.Assets[] | select(.Type == \"user\" and .IsVictim) | .ID]
   ```

[KL] P001「透過辦公應用程式建立可執行檔案」預定義的常規程式允許您防止攻擊者使用辦公應用程式，例如，當使用者開啟受影響的檔案時執行網路釣魚攻擊，然後文件會建立並執行可執行檔案。

觸發該常規程式的警示是根據*辦公應用程式建立可執行檔*關聯規則建立的。此規則有助於偵測代表辦公應用程式建立的具有可疑副檔名的檔案，例如指令碼和可執行檔。

常規程式觸發器包含下列運算式：

```
[.OriginalEvents[] | .ExternalID == "R350"] | any
```

執行期間，此常規程式將啟動下列回應動作：

1. 透過Active Directory回應，然後重設攻擊者和受害者帳戶的密碼。

   如果在執行回應操作期間發生錯誤，常規程式將終止。

2. 透過KASAP回應，然後為該帳戶指派資訊安全課程。

   如果在執行回應操作期間發生錯誤，常規程式將繼續執行。

常規程式演算法包含以下回應操作序列：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "resetLDAPPassword",
```

```
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}"
                },
                "onError": "stop"
            }
        },
        {
            "action": {
                "function": {
                    "type": "assignKasapGroup",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\") | .ID]}",
                    "params": {
                        "groupId": "SET KASAP GROUP ID"
                    }
                },
                "onError": "continue"
            }
        }
    ]
}
```

[KL] P002「Windows事件日誌已清除」

預設情況下，該常規程式在**手動**運作模式下運作。我們不建議將此常規程式切換到**自動**或**培訓**運作模式。

在使用常規程式之前，您必須在KUMA中執行以下操作：

- 設定事件擴充的擴充規則設定，其中「來源種類」設定已選取「事件」類型。指定**目標欄位**中的**AttackerUserID**值。
- 在KUMA中設定擴充功能以取得Windows事件日誌。

[KL] P002「Windows事件日誌已清除」預定義的常規程式允許您防止攻擊者清除Windows事件日誌，因為該日誌包含足夠的遙測，用於調查攻擊者的惡意活動。

觸發此常規程式的事件包含依據*Windows事件日誌已清除*關聯規則建立的一個或多個警示。此規則有助於偵測何時使用wevutil公用程式、使用者介面或PowerShell命令清除或刪除Windows日誌。若要啟用建立事件，您必須設定分段規則。

常規程式觸發器包含下列運算式：

```
[.Alerts[] | .OriginalEvents[] | .ExternalID  == "R050"] | any
```

執行期間，此常規程式會啟動透過Active Directory回應操作，然後封鎖攻擊者的帳戶。

如果在執行回應操作期間發生錯誤，常規程式將終止。

如果在事件中的一個或多個警示是由其他關聯規則產生的，則此常規程式不適用於這些警示。

常規程式演算法包含以下回應操作序列：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "blockLDAPAccount",
                    "assets": "${[ incident.Alerts[] | select(.OriginalEvents[] | .ExternalID == \"R050\") |
.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
                },
                "onError": "stop"
            }
        }
    ]
}
```

[KL] P003「來自wmiprvse.exe的可疑子程序」

在使用常規程式之前，您必須在KUMA中執行以下操作：

- 設定事件擴充的擴充規則設定，其中「來源種類」設定已選取「事件」類型。指定**目標欄位**中的**AttackerUserID**值。
- 在KUMA中設定擴充功能以取得Windows事件日誌。

[KL] P003「來自wmiprvse.exe的可疑子程序」預定義常規程式允許您檢測偏離規範且必須被視為可疑的父進程和子進程對。

觸發常規程式的警示是依據*wmiprvse.exe的R297_Suspicious子進程*關聯規則建立的。此規則有助於偵測以wmiprvse.exe名義啟動的可疑進程。

常規程式觸發器包含下列運算式：

```
[.OriginalEvents[] | .ExternalID  == "R297"] | any
```

執行期間，此常規程式將啟動下列回應動作：

1. 透過Active Directory回應，然後封鎖攻擊者的帳戶。
2. 在警示中註冊的裝置上終止該進程。
3. 執行惡意軟體掃描，然後對偵測到警示的裝置執行完整掃描。

> 為避免系統過載，預設不會掃描網路磁碟機。若要掃描網路磁碟機，則必須先複製此常規程式，然後在**執行惡意軟體掃描**操作中啟用**掃描網路磁碟機**切換開關，或在程式碼編輯器中將`allowScanNetworkDrives`參數設為`true`。

常規程式演算法包含以下回應操作序列：

```
{
    "dslSpecVersion": "1.1.0",
    "version": "1",
```

```
    "actionSpecVersion": "1",
    "executionFlow": [
        {
            "action": {
                "function": {
                    "type": "blockLDAPAccount",
                    "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
                },
                "onError": "stop"
            }
        },
        {
            "loop": {
                "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and
.DestinationProcessName != \"\")][] | .DestinationProcessName] }",
                "onError": "stop",
                "steps": [
                    {
                        "action": {
                            "function": {
                                "type": "killProcess",
                                "params": {
                                    "path": "${ .[0] }"
                                },
                                "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
                            }
                        }
                    }
                ]
            }
        },
        {
            "action": {
                "function": {
                    "type": "avScan",
                    "params": {
                        "scope": {
                            "area": "full",
                            "allowScanNetworkDrives": false
                        },
                        "wait": false
                    },
                    "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}"
                },
                "onError": "stop"
            }
        }
    ]
}
```

如果在執行任何回應操作期間發生錯誤，常規程式將終止。

[KL] P004「沙盒中等偵測」

[KL] P004「沙盒中等偵測」預先定義常規程式建立一條規則，以阻止在分析期間由沙盒元件分配的警示**中**嚴重等級的檔案的執行。

常規程式觸發器包含下列運算式：

```
"event.new and .Severity == \"medium\" and any(.DetectionTechnologies[] == \"SB\"; .)"
```

常規程式使用的 ResponseFunction：`addFilePreventionRules`。

在執行過程中，此常規程式使用新增阻止規則回應操作。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "addFilePreventionRules",
          "assets":[
            "selector": "execution-tenant"
          },
          "params": {
            "files": "${[alert.ScannedFiles[] | select(any(.DetectionTechnologies[] == \"SB\"; .)) | .Hashes |
map(.Value)] | flatten}",
            "notify": true
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

[KL] P005「沙盒高等偵測」

[KL] P005「沙盒高等偵測」預先定義常規程式建立一條規則，以阻止在分析期間由沙盒元件指派的警示**高**嚴重等級的檔案的執行。

常規程式觸發器包含下列運算式：

```
"event.new and .Severity == \"high\" and any(.DetectionTechnologies[] == \"SB\"; .)"
```

常規程式使用的 ResponseFunction：`addFilePreventionRules`。

在執行過程中，此常規程式使用新增阻止規則回應操作。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "addFilePreventionRules",
          "assets":[
            "selector": "execution-tenant"
          },
          "params": {
            "files": "${[alert.ScannedFiles[] | select(any(.DetectionTechnologies[] == \"SB\"; .)) | .Hashes |
map(.Value)] | flatten}",
            "notify": true
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

[KL]「檢查外部IP位址的常規程式」

[KL] 檢查外部IP位址的常規程式的預定義常規程式在偵測到外部IP位址的連線時觸發，並啟動TIP擴充進程。如果擴充結果顯示威脅評分高於80，則會要求「主機」類型資產的取證資料（進程清單），並啟用網路隔離。

有關常規程式的附加資訊：

- 要使常規程式正常運行，必須設定Kaspersky TIP整合；
- 要執行帳戶鎖定操作，需要與Active Directory整合；
- 如果擴充結果顯示威脅分數低於80，則終止執行常規程式；
- 如果在執行過程中任何步驟發生錯誤，將停止執行常規程式；
- 「啟用網路隔離」操作需要在常規程式執行期間進行手動批准。

常規程式觸發器包含下列運算式：

```
"event.new and ([ .Alerts[] | .Observables[] | select(.Value | test("^(10\\.|172\\.(1[6-9]|2[0-9]|3[01])\\.|192\\.168\\.|127\\.)") | not) | .Value ] | length > 0)"
```

常規程式使用的 ResponseFunction：`iocsEnrichment, getForensics, netIsolateOn`。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "iocsEnrichment",
          "params": {
            "fullEnrichment": true,
            "observables": "${[ incident.Alerts[] | .Observables[] | {\"type\": .Type, \"value\": .Value } | select(.type==\"ip\" and (.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.)\") | not)) ] | unique_by(.value)}"
          }
        },
        "onError": "stop",
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        },
        "output": {
          "filter": "${.}",
          "action": "overwrite"
        }
      }
    },
    {
      "decision": {
        "conditions": [
          {
            "condition": "${\"${([.details.observableData[] | select(.status == \\\"ok\\\" and .ipObservableData.ipGeneralInfo.threatScore > 80)] | length > 0)}\"}",
            "name": "Condition 1",
            "steps": [
              {
                "decision": {
                  "conditions": [
                    {
```

```
                    "condition": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type == \"host\")) |
length > 0}",
                    "name": "alert has host(s)",
                    "steps": [
                      {
                        "action": {
                          "function": {
                            "type": "getForensics",
                            "assets": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type ==
\"host\")) | map(.ID)}",
                            "params": {
                              "processes": {
                                "collect": true
                              },
                              "autoruns": {
                                "collect": false
                              }
                            }
                          },
                          "onError": "stop",
                          "timeout": {
                            "scheduleToCloseTimeout": "24h"
                          }
                        }
                      },
                      {
                        "action": {
                          "function": {
                            "type": "netIsolateOn",
                            "assets": "${incident.Alerts | map(.Assets) | flatten | map(select(.Type ==
\"host\")) | map(.ID)}",
                            "params": {
                              "exclusions": [],
                              "exclusionsConflictBehavior": "replace",
                              "isolationTimeoutSec": 28800
                            }
                          },
                          "onError": "stop",
                          "timeout": {
                            "scheduleToCloseTimeout": "24h"
                          },
                          "manualApprove": {
                            "timeout": "60m",
                            "emailNotifications": {
                              "enabled": true,
                              "delay": "10m"
                            }
                          }
                        }
                      }
                    ]
                  }
                ]
              }
            }
          ]
        }
      ]
    }
  ]
}
```


[KL]「檢測到受感染文件時隔離裝置的常規程式」

[KL] 用於隔離偵測到受感染檔案的裝置的常規程式的預設常規程式會在偵測到受感染檔案後隔離裝置。

該常規程式中不包含觸發器。必須手動啟動常規程式，並且需要使用者選擇上下文。若要執行此常規程式，您必須勾選**在啟動常規程式之前選取目標物件**核取方塊，並選擇要執行常規程式的事件、資產和可觀察物件。

對於每個所選雜湊值類型的可觀察對象，將執行下列操作：

1. 從選定的資產中擷取檔案。
2. 傳送檢索到的檔案進行掃描。
    - 如果在掃描過程中發生錯誤，則終止執行常規程式；
    - 如果掃描完成且未偵測到威脅，則終止執行常規程式；
    - 如果掃描完成並偵測到威脅：
        - 所有選定的裝置都將啟用網路隔離；
        - 租用戶內的所有裝置將新增基於雜湊值的阻止規則。

有關常規程式的附加資訊：

- 如果在新增阻止規則或啟用網路隔離的步驟中發生錯誤，常規程式將停止執行；在所有其他情況下，常規程式將繼續執行。
- 「啟用網路隔離」和「新增阻止規則」作業需要在常規程式執行期間手動核准。

常規程式使用的 ResponseFunction：`getFile`、`serverScan`、`addCommentToIncident`、`addFilePreventionRules`、`netIsolateOn`。

常規程式演算法包含以下回應操作序列：


```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "decision": {
        "conditions": [
          {
            "condition": "${((.input.assets // []) | length) > 0 and ([.input.observables[] | select(.type ==
\"md5\" or .type == \"sha256\" and .value != null and .value != \"\")] | length) > 0}",
            "name": "has input data",
            "steps": [
              {
                "loop": {
                  "input": "${[(.input.observables | map(select(.type == \"md5\" or .type == \"sha256\") |
select(.value != null and .value != \"\") | .value))[] as $hash | [incident.Alerts[] | .Observables[]? |
select((.Type == \"md5\" or .Type == \"sha256\") and .Value == $hash and .Details != \"\")][0] | {\"path\":
.Details,\"hash\":.Value}]}",
                  "steps": [
                    {
                      "decision": {
                        "conditions": [
                          {
                            "condition": "${.[0].path? | length > 0}",
                            "name": "hash with path",
                            "steps": [
                              {
                                "updateData": {
                                  "action": "merge",
                                  "filter": "${.[0]}"
                                }
                              },
                              {
                                "action": {
                                  "function": {
                                    "type": "getFile",
                                    "asset": "${([incident.Alerts[] | .Assets[]? | select(.Type == \"host\")]
[0].ID // (.assets[0] // \"\"))}",
```

```
                                    "params": {
                                      "path": "${.path}"
                                    }
                                  },
                                  "onError": "continue",
                                  "timeout": {
                                    "scheduleToCloseTimeout": "24h"
                                  },
                                  "output": {
                                    "action": "merge",
                                    "filter": "${{\"fileID\": (.details[0].details.file.id // null),
\"scanResult\": null}}"
                                  }
                                }
                              },
                              {
                                "decision": {
                                  "conditions": [
                                    {
                                      "condition": "${.fileID != null and .fileID != \"\"}",
                                      "name": "fileID exists",
                                      "steps": [
                                        {
                                          "action": {
                                            "function": {
                                              "type": "serverScan",
                                              "params": {
                                                "file": {
                                                  "id": "${.fileID}"
                                                }
                                              }
                                            },
                                            "onError": "continue",
                                            "timeout": {
                                              "scheduleToCloseTimeout": "24h"
                                            },
                                            "output": {
                                              "action": "merge",
                                              "filter": "${{\"scanResult\": .}}"
                                            }
                                          }
                                        },
                                        {
                                          "decision": {
                                            "conditions": [
                                              {
                                                "condition": "${.scanResult != null and (.scanResult.resultCode ==
\"error\" or .scanResult.resultCode == null)}",
                                                "name": "scan error",
                                                "steps": [
                                                  {
                                                    "action": {
                                                      "function": {
                                                        "type": "addCommentToIncident",
                                                        "params": {
                                                          "text": "${\"[DEBUG scan ERROR] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \" | errorCode: \" +
(.scanResult.result.errorCode // \"null\") + \" | internalCode: \" + (.scanResult.result.internalCode // \"null\")
+ \"\\noriginalError: \" + (.scanResult.result.originalError // \"null\")}"
                                                        }
                                                      },
                                                      "onError": "continue",
                                                      "timeout": {
                                                        "scheduleToCloseTimeout": "24h"
                                                      }
                                                    }
                                                  }
                                                ]
                                              },
                                              {
                                                "condition": "${.scanResult != null and .scanResult.resultCode ==
\"success\"}",
                                                "name": "scan success",
                                                "steps": [
                                                  {
                                                    "action": {
                                                      "function": {
                                                        "type": "addCommentToIncident",
                                                        "params": {
                                                          "text": "${\"[DEBUG scan] fileID: \" + (.fileID //
\"null\") + \" | resultCode: \" + (.scanResult.resultCode // \"null\") + \"\\nresult: \" + ({\"fileID\": .fileID,
\"resultCode\": .scanResult.resultCode, \"technologies\": .scanResult.details.scanResult.technologies} |
```

```
tostring)}"
                                                    }
                                                  },
                                                  "onError": "continue",
                                                  "timeout": {
                                                    "scheduleToCloseTimeout": "24h"
                                                  }
                                                }
                                              },
                                              {
                                                "decision": {
                                                  "conditions": [
                                                    {
                                                      "condition":
"${[.scanResult.details.scanResult.technologies[] | .result] | contains([\"Infected\"])}",
                                                      "name": "infected",
                                                      "steps": [
                                                        {
                                                            "action": {
                                                                "function": {
                                                                  "type": "addFilePreventionRules",
                                                                  "assets":[
                                                                    "selector": "execution-tenant"
                                                                  },
                                                                  "params": {
                                                                    "files": "${[.hash]}"
                                                                  }
                                                                },
                                                                "onError": "stop",
                                                                "timeout": {
                                                                  "scheduleToCloseTimeout": "24h"
                                                                },
                                                                "manualApprove": true
                                                            }
                                                        },
                                                        {
                                                          "updateData": {
                                                            "action": "overwrite",
                                                            "filter": "${{\"isInfected\": true}}"
                                                          }
                                                        }
                                                      ]
                                                    }
                                                  ]
                                                }
                                              }
                                            ]
                                          }
                                        ]
                                      }
                                    ]
                                  }
                                ]
                              }
                            ]
                          }
                        ]
                      }
                    ]
                  }
                ],
                "onError": "continue",
                "batchSize": 1,
                "aggregate": "${.}",
                "output": {
                  "filter": "${{\"scanResult\": .}}"
                }
              }
            },
            {
              "decision": {
                "conditions": [
                  {
                    "condition": "${.scanResult | map(.isInfected) | any}",
                    "name": "isInfected",
                    "steps": [
                      {
                        "action": {
                          "function": {
                            "type": "netIsolateOn",
                            "assets": "${.input.assets | map(select(.Type == \"host\") | .ID)}",
```

```
                        "params": {
                          "exclusions": [],
                          "exclusionsConflictBehavior": "replace",
                          "isolationTimeoutSec": 28800
                        }
                      },
                      "onError": "stop",
                      "timeout": {
                        "scheduleToCloseTimeout": "24h"
                      }
                    }
                  }
                ]
              }
            ]
          }
        ]
      }
    }
  ]
}
```

[KL][EDR]「刪除從警示傳送至主機的惡意檔案」

預先定義的**[KL][EDR] 從警示中刪除已傳輸至主機的惡意檔案**常規程式，旨在自動回應針對惡意檔案的偵測，這類檔案用於將其他惡意軟體傳送至裝置。當偵測到與技術 T1105（傳入工具傳輸）相關的活動時，常規程式會從裝置中刪除此類檔案，以防止其遭到進一步使用。

常規程式的範圍為警示。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any(.S.KL_EventType == "File Modify" and (.FileFullname // "") != "" and ([.SA.KL_IoAAlert,
.SA.KL_IoATechniques] | transpose | any(.[0] and .[1] == "t1105"))))] | any)"
```

常規程式 `deleteFile` 使用的 ResponseFunction。

在執行階段，常規程式會使用**刪除檔案**回應。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select(.S.KL_EventType == \"File Modify\" and (.FileFullname //
\"\") != \"\" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0] and .[1] == \"t1105\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].FileFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
```

```
              "scheduleToCloseTimeout": "24h"
            }
          }
        }
      ],
      "onError": "continue",
      "batchSize": 1
    }
  }
 ]
}
```

[KL][EDR]「刪除從事件傳送至主機的惡意檔案」

預先定義的常規程式 **[KL][EDR] 刪除從事件傳輸至主機的惡意檔案**，旨在自動回應對用於將其他惡意軟體傳送至裝置之惡意檔案的偵測。常規程式會處理與事件相關聯的警示，並在偵測到與技術 T1105（輸入工具傳輸）相關的活動時，從裝置刪除此類檔案，以防止其遭到進一步使用。

常規程式的範圍為事件。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .OriginalEvents // [] | select(any(.S.KL_EventType ==
"File Modify" and (.FileFullname // "") != "" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0]
and .[1] == "t1105")))) ] | any)"
```

常規程式 `deleteFile` 使用的 ResponseFunction。

在執行階段，常規程式會使用**刪除檔案**回應。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select(.S.KL_EventType == \"File Modify\" and
(.FileFullname // \"\") != \"\" and ([.SA.KL_IoAAlert, .SA.KL_IoATechniques] | transpose | any(.[0] and .[1] ==
\"t1105\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].FileFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
```

```
  ]
}
```

[KL][EDR]「當從警示中偵測到探索活動時隔離主機」

[KL][EDR] 從警報中偵測到探索活動時隔離主機預先定義常規程式旨在自動回應涉及收集裝置及其環境相關資訊的活動。如果偵測到此類活動，常規程式會為裝置啟用網路隔離，以防止攻擊者在調查期間進一步活動。

常規程式的範圍為警示。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.Rules // [] |
select(any(.Name == "Discovery_activity_on_the_host"))] | any)"
```

常規程式 `netIsolateOn` 所使用的 ResponseFunction。

在執行階段，常規程式會使用 **啟用網路隔離**回應。此回應會為裝置啟用網路隔離 8 小時。必須取得使用者確認，才能啟用網路隔離。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ alert.Assets[] | select(.Type == \"host\") | .ID] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]「當從事件中偵測到探索活動時隔離主機」

[KL][EDR] 從事件中偵測到探索活動時隔離主機預定義常規程式旨在自動回應涉及收集裝置及其環境相關資訊的活動。常規程式會處理與事件關聯的警示；如果偵測到此類活動，則會啟用裝置的網路隔離，以防止攻擊者在調查期間繼續活動。

常規程式的範圍為事件。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .Rules // [] | select(any(.Name ==
"Discovery_activity_on_the_host")) ] | any)"
```

常規程式 `netIsolateOn` 所使用的 ResponseFunction。

在執行階段，常規程式會使用 **啟用網路隔離**回應。此回應會為裝置啟用網路隔離 8 小時。必須取得使用者確認，才能啟用網路隔離。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | select(.Rules | any(.Name == \"Discovery_activity_on_the_host\")) |
.Assets[] | select(.Type == \"host\") | .ID] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]「當偵測到資料外洩活動時隔離主機」

[KL][EDR] 偵測到資料外洩活動時隔離主機預先定義常規程式旨在自動回應從裝置進行未經授權的資料傳輸，以及嘗試連線至攻擊者的命令與控制 (C2) 基礎架構。此常規程式會處理與事件相關聯的警示。如果偵測到這類活動，便會對該裝置啟用網路隔離，以防止進一步的資料傳輸及惡意活動。

常規程式的範圍為事件。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert,
.SA.KL_IoAName] | transpose | map(select(.[0]) | .[1]) | any(. as $v | ["not_standard_directory_archive",
"compress_data_for_exfiltration_via_archive"] | index($v)) and any(. as $v | ["lolc2_connection_activity_network",
"lolc2_connection_activity_dns", "network_connection_to_cloud_storage_win"] | index($v)))) ] | any)"
```

常規程式 `netIsolateOn` 所使用的 ResponseFunction。

在執行階段，常規程式會使用 **啟用網路隔離**回應。此回應會為裝置啟用網路隔離 8 小時。必須取得使用者確認，才能啟用網路隔離。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | map(select(.[0]) | .[1]) | any(. as $v | [\"not_standard_directory_archive\",
\"compress_data_for_exfiltration_via_archive\"] | index($v)) and any(. as $v |
[\"lolc2_connection_activity_network\", \"lolc2_connection_activity_dns\",
\"network_connection_to_cloud_storage_win\"] | index($v))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR] 從警示偵測到反向 Shell 活動時隔離主機

[KL][EDR] 從警報偵測到反向 Shell 活動時隔離主機預先定義的常規程式，旨在自動回應裝置上的反向 Shell 使用跡象。偵測到此類活動時，常規程式會對裝置啟用網路隔離，以防止攻擊者遠端控制該裝置。

常規程式的範圍為警示。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and
(["invoke_golang_reverse_shell", "invoke_lua_reverse_shell", "invoke_netcat_reverse_or_bind_shell",
"invoke_perl_reverse_shell", "invoke_php_reverse_shell", "invoke_reverse_shell_via_curl"] | index($ioaname))))) ]
| any)"
```

常規程式 `netIsolateOn` 所使用的 ResponseFunction。

在執行階段，常規程式會使用 **啟用網路隔離**回應。此回應會為裝置啟用網路隔離 8 小時。必須取得使用者確認，才能啟用網路隔離。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ alert.OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1]
```

```
as $ioaname | .[0] and ([\"invoke_golang_reverse_shell\", \"invoke_lua_reverse_shell\",
\"invoke_netcat_reverse_or_bind_shell\", \"invoke_perl_reverse_shell\", \"invoke_php_reverse_shell\",
\"invoke_reverse_shell_via_curl\"] | index($ioaname)))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
    }
  ]
}
```

[KL][EDR]「當從事件中偵測到反向 Shell 活動時隔離主機」

[KL][EDR] 在事件中偵測到反向 Shell 活動時隔離主機預先定義的常規程式，旨在自動回應裝置上使用反向 Shell 的跡象。常規程式會處理與事件相關聯的警示；如果偵測到此類活動，常規程式會對裝置啟用網路隔離，以防止攻擊者從遠端控制裝置。

常規程式的範圍為事件。

常規程式觸發器包含下列運算式：

"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . == "incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and (["invoke_golang_reverse_shell", "invoke_lua_reverse_shell", "invoke_netcat_reverse_or_bind_shell", "invoke_perl_reverse_shell", "invoke_php_reverse_shell", "invoke_reverse_shell_via_curl"] | index($ioaname)))))] | any)"

常規程式 `netIsolateOn` 所使用的 ResponseFunction。

在執行階段，常規程式會使用 **啟用網路隔離**回應。此回應會為裝置啟用網路隔離 8 小時。必須取得使用者確認，才能啟用網路隔離。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "netIsolateOn",
          "assets": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | any(.[1] as $ioaname | .[0] and ([\"invoke_golang_reverse_shell\", \"invoke_lua_reverse_shell\",
\"invoke_netcat_reverse_or_bind_shell\", \"invoke_perl_reverse_shell\", \"invoke_php_reverse_shell\",
\"invoke_reverse_shell_via_curl\"] | index($ioaname)))) | .AffectedAssets.assets[] | .OsmpID ] }",
          "params": {
            "exclusions": [],
            "exclusionsConflictBehavior": "replace",
            "isolationTimeoutSec": 28800
          }
        },
        "manualApprove": true,
        "timeout": {
          "scheduleToCloseTimeout": "24h"
        }
      }
```

```
    }
  ]
}
```

[KL][EDR]「緩解警示中由電子郵件附件引起的惡意活動」

[KL][EDR] 從警示緩解電子郵件附件的惡意活動預先定義的常規程式旨在自動回應與透過電子郵件接收的檔案相關之惡意活動。如果在裝置上偵測到此類活動，常規程式會終止與惡意檔案相關聯的進程，並從裝置中刪除該檔案。

常規程式的範圍為警示。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([ .OriginalEvents //
[] | select(any(. as $event | $event.SA.KL_IoAName | index("mail_utility_threatdetect") as $idx | if $idx != null
then $event.SA.KL_IoAAlert[$idx] else false end)) ] | any)"
```

常規程式使用的 ResponseFunction：`killProcess`、`deleteFile`。

執行期間，常規程式會使用下列回應：

- 終止進程

  > 如果無法終止進程，常規程式會繼續執行。

- 刪除檔案

警示中的事件可能涉及不同的裝置和惡意檔案。常規程式會針對每個符合條件的事件分別觸發回應。如果警示中沒有符合條件的事件，常規程式會停止執行。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select((.FileName == \"OUTLOOK.exe\" or .ParentFileName ==
\"OUTLOOK.exe\") and .ThreatObjectType == \"file\" and (.ThreatObjectFullname | test(\"\\\\w\\\\:\\\\\\\\\"))) ]
}",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
```

```
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
}
```

[KL][EDR]「緩解事件中由電子郵件附件引起的惡意活動」

[KL][EDR] 緩解事件中電子郵件附件的惡意活動預先定義常規程式旨在自動回應與透過電子郵件接收的檔案相關的惡意活動。常規程式會處理與事件相關的警示；如果偵測到裝置上有惡意活動，便會終止與惡意檔案相關的處理程序，並從裝置中刪除該檔案。

常規程式的範圍為事件。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([ .Alerts[]? | .OriginalEvents // [] | select(any(. as $event |
$event.SA.KL_IoAName | index("mail_utility_threatdetect") as $idx | if $idx != null then
$event.SA.KL_IoAAlert[$idx] else false end)) ] | any)"
```

常規程式使用的 ResponseFunction：`killProcess`、`deleteFile`。

執行期間，常規程式會使用下列回應：

- 終止進程

  > 如果無法終止進程，常規程式會繼續執行。

- 刪除檔案

警示中的事件可能涉及不同的裝置和惡意檔案。常規程式會針對每個符合條件的事件分別觸發回應。如果警示中沒有符合條件的事件，常規程式會停止執行。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select((.FileName == \"OUTLOOK.exe\" or
```

```
.ParentFileName == \"OUTLOOK.exe\") and .ThreatObjectType == \"file\" and (.ThreatObjectFullname |
test(\"\\\\w\\\\:\\\\\\\\\"))) ] }",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ThreatObjectFullname }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue",
        "batchSize": 1
      }
    }
  ]
  }
```

[KL][EDR]「緩解警示中的記憶體傾印活動」

[KL][EDR] 從警示緩解記憶體傾印活動預先定義的常規程式旨在自動回應記憶體傾印的建立活動，這些傾印可能會用於取得認證資料及其他敏感資訊。如果在裝置上偵測到此類活動，常規程式會終止建立記憶體傾印的進程，並刪除該進程建立的檔案。

常規程式的範圍為警示。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "alertChangedOriginalEvents"))) and ([.OriginalEvents //
[] | select(any([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and
(["createdump_lolbin_execution_process", "credentials_dumping_tools_epp",
"credentials_dumping_tools_file_artifacts_creation"] | index($ioaname))))) ] | any)"
```

常規程式使用的 ResponseFunction：`killProcess`、`deleteFile`。

執行期間，常規程式會使用下列回應：

- 終止進程

  如果無法終止進程，常規程式會繼續執行。

- 刪除檔案

警示中的事件可能涉及不同的裝置和惡意檔案。常規程式會針對每個符合條件的事件分別觸發回應。如果警示中沒有符合條件的事件，常規程式會停止執行。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ alert.OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] | transpose | any( .[1]
as $ioaname | .[0] and ([\"createdump_lolbin_execution_process\", \"credentials_dumping_tools_epp\",
\"credentials_dumping_tools_file_artifacts_creation\"] | index($ioaname)))) ] }",
        "batchSize": 1,
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue"
      }
    }
  ]
}
```

[KL][EDR]「緩解事件中的記憶體傾印活動」

[KL][EDR] 緩解事件中的記憶體傾印活動預先定義常規程式旨在自動回應可用於取得憑證及其他敏感資訊的記憶體傾印建立活動。常規程式會處理與事件相關聯的警示，如果在裝置上偵測到此類活動，則會終止建立記憶體傾印的進程，並刪除該進程建立的檔案。

常規程式的範圍為事件。

常規程式觸發器包含下列運算式：

```
"(event.new or (event.updateOperations // [] | any(. == "incidentLinkedWithAlertsBySystem" or . ==
"incidentLinkedWithAlertsByUser"))) and ([.Alerts[]? | .OriginalEvents // [] | select(any([.SA.KL_IoAAlert,
.SA.KL_IoAName] | transpose | any(.[1] as $ioaname | .[0] and (["createdump_lolbin_execution_process",
```

```
"credentials_dumping_tools_epp", "credentials_dumping_tools_file_artifacts_creation"] | index($ioaname))))) ] |
any)"
```

常規程式使用的 ResponseFunction：`killProcess`、`deleteFile`。

執行期間，常規程式會使用下列回應：

- 終止進程

  > 如果無法終止進程，常規程式會繼續執行。

- 刪除檔案

警示中的事件可能涉及不同的裝置和惡意檔案。常規程式會針對每個符合條件的事件分別觸發回應。如果警示中沒有符合條件的事件，常規程式會停止執行。

常規程式演算法包含以下回應操作序列：

```
{
  "version": "1",
  "dslSpecVersion": "1.1.0",
  "actionsSpecVersion": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "loop": {
        "input": "${ [ incident.Alerts[] | .OriginalEvents[] | select([.SA.KL_IoAAlert, .SA.KL_IoAName] |
transpose | any(.[1] as $ioaname | .[0] and ([\"createdump_lolbin_execution_process\",
\"credentials_dumping_tools_epp\", \"credentials_dumping_tools_file_artifacts_creation\"] | index($ioaname)))) ]
}",
        "batchSize": 1,
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          },
          {
            "action": {
              "function": {
                "type": "deleteFile",
                "assets": "${ [ .[0].AffectedAssets.assets[] | .OsmpID ] }",
                "params": {
                  "path": "${ .[0].ProcessFileFullName }"
                }
              },
              "onError": "continue",
              "timeout": {
                "scheduleToCloseTimeout": "24h"
              }
            }
          }
        ],
        "onError": "continue"
      }
    }
  ]
}
```

常規程式觸發器

常規程式觸發器是一個篩選器，允許選取必須啟動之常規程式的警示或事件。篩選器（觸發器）會個別套用於每個物件（警示或事件），並採用單一值：`true` 或 `false`。觸發器由jq語言的運算式組成，用於處理JSON格式的結構化資料。有關 jq 運算式的更多資訊，請參閱 jq 手冊。

在Kaspersky Next XDR Expert中，使用了gojq。它是用go語言編寫的jq的實現，它與jq有以下區別：

- 數學函式的實作方式更加便捷。
- 錯誤訊息會清楚地指出應該在哪裡修復您的查詢。
- 整數運算更加準確。
- gojq改進了jq中運作不正確的功能。

有關gojq和jq之間差異的更多資訊，請參閱GitHub。

如何編寫觸發器

在**建立觸發條件編輯常規程式**時，您可以在視覺化編輯器的觸發器區塊中編寫觸發器。

根據您在建立或編輯常規程式時在**範圍**清單中選取的選項，使用警示資料模式或事件資料模式。

常規程式觸發器中的參數名稱必須與資料模型中的參數名稱相同。請注意，jq運算式中的元素區分大小寫。

為避免系統過載，不建議在觸發器中指定`OriginalEvents, Observables, Extra,`和`Alerts`資料。

當您開始編寫觸發器時，可能會顯示以下建議：

- 函式名稱。
- 特定值。
- 根據資料模型指定為物件識別碼的欄位。

當您開始輸入時，系統會篩選出適當的值，並將其顯示在建議清單中。為方便起見，部分建議包含搜尋字串。例如，若要指定事件類型ID或事件狀態ID，您可以依名稱搜尋對應的記錄，然後在觸發器中將指定ID。

請注意，標準狀態（*新增*和*已關閉*）在不同的工作流程中具有相同的 ID。這表示系統會針對所有具有指定狀態 ID 的事件觸發常規程式。若要限制常規程式執行的事件範圍，您必須在觸發器中指定事件狀態ID和事件類型。

jq語言也提供jq運算式的語法高亮顯示和驗證。如果觸發器包含無效運算式，則無法儲存常規程式。

編寫觸發器時，需要使用基本語法規則。

若要引用結構內容，必須使用點號"."並指定屬性，例如：

- .MITRETactics[]—檢視與警示中所有觸發的IOA規則關聯的MITRE策略陣列。
- .MITRETactics[0]—檢視MITRE策略陣列中的第一個元素。

若要引用子內容，可使用管道（|）或不帶管道的相同組合，例如：

- .Assignee.Name—該運算式會輸出警示所指派使用者的名稱。
- .MITRETactics[0].ID 或 .MITRETactics[0] | .ID—該運算式會輸出第一個MITRE策略的ID。

要取得值，您必須使用下列操作員：==、>、<、>=、<=、!=，例如：

- .Assignee.Name == "user"—如果警示已指派給該使用者，該運算式會傳回true。
- (.Severity == "high") and (.DetectSource == "KES")—如果警示嚴重等級為高，且資料來源為 Kaspersky Endpoint Security，該運算式會傳回true。
- [.DetectionTechnologies[] | . == "IOC"] | any —如果觸發 IOC 偵測技術，該運算式會傳回true。
- .DetectionTechnologies | length > 1—如果觸發多個偵測技術，該運算式會傳回 true。

若要列舉物件陣列中的值，可以使用 any 方法，例如：

- [.Assets[] | .Name == "W21H2-X64-3160"] | any—該運算式會篩選符合以下條件的警示：Assets 陣列的任一元素在 Name 欄位中具有 W21H2-X64-3160 值。
- [.Observables[] | .Value == "127.0.0.1"] | any—該運算式會篩選符合以下條件的警示：Observables 陣列的任一元素在 Value 欄位中具有 127.0.0.1 值。
- [.Assets[].ID]—輸出 ID 陣列。
- [.Assets[] | select(.AttackerOrVictim=="attacker") | .ID]—顯示依 AttackerOrVictim 欄位篩選之資產的 ID 陣列。

若想重複使用計算結果，請使用 $ 指定變數。例如，運算式 event.manual != true as $not_manual | [.DetectionTechnologies[] | . == "IOC"] | any and $not_manual 會定義並使用 $not_manual 變數，其中包含一個旗標，用於指示變更是否為手動。

若要處理日期，您可以使用下列函式：

- now—取得目前的 Unix 時間（以秒為單位），例如 now == 1690541520.537496。
- todate—將目前 Unix 時間轉換為日期字串，例如 now | todate == "2023-07-28T10:47:36Z".
- fromdate—將日期轉換為秒數，例如：
  - .CreatedAt | split(".")[0] + "Z"—此命令會移除毫秒，並將字串轉換為 2023-07-15T07:49:51Z 格式。
  - (.CreatedAt | split(".")[0] + "Z") | fromdate == 1689407391—秒數轉換完成。

Jq使用迭代器——一種介面，提供對集合元素（例如陣列）的存取，並允許您瀏覽它們。迭代器始終是計算的結果。差別在於迭代器包含的元素數量。在 Kaspersky Next XDR Expert 中，迭代器只能包含一個元素。其他所有情況均視為錯誤。

要編寫正確的觸發器，必須將迭代器括在方括號中（`[ ... ]`）。例如，`.DetectionTechnologies[] == "IOC"` 觸發器會導致錯誤，因為它會傳回包含兩個元素的迭代器。正確的觸發器必須採用以下形式：`[ .DetectionTechnologies == "IOC" ] | any`，其中，您必須先使用 `[]` 將比較結果包裝成陣列，然後使用 `any` 方法進行處理；若陣列中至少有一個元素為 `true`，該方法會傳回 `true`。否則會傳回 `false`。

觸發器執行時

當發生以下任一觸發事件時，將開始搜尋適當的常規程式：

- 新警示/事件隨即建立；
- 任何活動警示/事件的欄位隨即變更；
- 建立或修改常規程式時，使用者選取了 **針對所有符合的警示或事件啟動常規程式。請注意，系統可能會過載**。

現支援以下類型的警示變更事件：

- 指派或移除分析師。
- 變更警示狀態。
- 變更基本事件。
- 將警示關聯到事件或從事件中取消關聯。
- 變更 `ExternalReference` 欄位中的值。

現支援以下類型的事件變更事件：

- 指派或移除分析師。
- 變更事件狀態。
- 變更基本事件。
- 將警示關聯到事件或從事件中取消關聯。
- 變更事件名稱。
- 編輯事件描述
- 變更事件優先順序
- 變更 `ExternalReference` 欄位中的值。
- 合併事件。

警示/事件結構不包含任何關於警示/事件變更的資料。這些資料透過附加資訊傳輸。若要在常規程式觸發器中引用這些變更，請使用不含引數的事件函式。

預設會略過對警示或事件詳細資訊的手動變更。若想讓常規程式因手動變更而啟動，必須在觸發器中使用 `event.manual` 函式，例如：

- `event.manual and ([ event.updateOperations[] | . == "alertReopened" ] | any)`—只有在手動重新開啟警示時，觸發器才會運作。
- `[ event.updateOperations[] | . == "alertLinkedWithIncidentBySystem" ] | any`—只有在警示自動連結至事件時，觸發器才會運作。
- `event.manual != null and (([ event.updateOperations[] | . == "alertChangedToNew" ] | any) | not)`—如果警示狀態變更為 *新增* 以外的任何狀態，無論是手動還是自動，觸發器都會運作。
- `event == null and .Status == "inIncident"`—觸發器適用於所有狀態為 *在事件中* 的警示，但只有在變更的是常規程式而非警示時才會運作。

如有必要，您可以在 Jq playground 服務中測試 jq 運算式範例、套用篩選器，然後檢視結果。

常規程式演算法

Kaspersky Next XDR Expert允許您使用常規程式手動或自動回應警示和事件。回應警示或事件可能不包含單一操作，而包含一整套步驟和參數。這些步驟取決於指定的條件、警示或事件資料以及先前回應操作的結果。

常規程式演算法可讓您以JSON格式指定回應操作的順序、必要條件以及對目標物件的必要影響。常規程式演算法步驟依序執行。您可以在建立或編輯常規程式時指定常規程式演算法。

啟動後，常規程式會取得所有警示或事件資料，並將它們放置在全域資料中。常規程式使用以下資料：

- 全域資料

  全域資料在常規程式的任何步驟中均可讀取。全域資料包含有關啟動常規程式的警示或事件的資訊。

  > 您無法透過使用常規程式或變更警示或事件資料來編輯全域資料。全域資料在常規程式實例的整個生命週期中保持不變。

- 作業資料

  作業資料會在常規程式的各步驟之間傳輸。您可以使用 jq 運算式來管理作業資料，這些運算式是在 `input` 與 `output` 參數中指定。

- 本機資料

  本地資料僅限於特定步驟中使用。您可透過 `input`（本地資料產生）參數與 `output`（從本地資料產生作業資料）參數來管理本地資料。

如何編寫演算法

常規程式演算法以JSON格式編寫，包含兩個主要部分：

- 常規程式的一般資訊：
  - 名稱（ `name` ）
  - 描述（ `description` ）
  - 範圍（ `inputType` ）
  - 常規程式輸入資料的轉換（ `input` ）
  - 常規程式輸出資料的轉換（ `output` ）
  - 常規程式執行逾時（ `playbookRunTimeout` ）
  - 可在特定步驟套用的逾時政策（ `timeouts` ）
  - 常規程式版本（ `version` ）
  - DSL 結構描述版本（ `dslSpecVersion` ）
  - 回應動作結構描述版本（ `actionsSpecVersion` ）
- 常規程式執行步驟（ `executionFlow` ）。

編寫演算法時需要以下參數：

- `dslSpecVersion`。必填值：1.1.0。
- `actionsSpecVersion`
- `version`
- `executionFlow`（至少一個執行步驟）

> 每個執行步驟都有自己的必填欄位。

如果您嘗試在未填寫必填欄位的情況下儲存常規程式，則會發生錯誤。

常規程式演算法不區分大小寫。若要使用警示的資產資料，需將`Assets`參數首字母大寫。例如：`alert.Assets[]`。但是，若要在針對目標物件手動啟動常規程式時，於輸入資料中使用資產資料，切勿將`assets`參數首字母大寫。例如：`.input.assets[]`。

依據在建立或編輯常規程式時選取的範圍，您可以在以 jq 語言編寫的運算式中使用警示資料模型或事件資料模型。為此，請使用`alert`或`incident`值編寫運算式（切勿在值的開頭使用點號「`.`」）。例如：

```
"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
```

您可以在任何執行步驟中在jq運算式中使用警示或事件資料。警示或事件資料僅在讀取模式下可用。此資料在常規程式運行期間不會更改。如果在啟動常規程式後警示或事件資料發生變化，則不會影響常規程式執行。

在演算法中使用常規程式資料時，也可以使用jq運算式。有關 jq 運算式的更多資訊，請參閱 jq手冊。

若於 jq 運算式中使用引號，需以反斜線對這些符號進行跳脫。例如：`"${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"`。

未用於跳脫引號的反斜線也必須用其他反斜線進行跳脫處理。例如：`${\"add_firewall_rule --ip_address=\" + ([.input.observables[] | select(.type == \"ip\") | select(.value | test(\"^(10\\\\.|172\\\\.(1[6-9]|2[0-9]|3[01])\\\\.|192\\\\.168\\\\.|127\\\\.).*\") | not) | .value] | join(\",\"))}`。

若想為特定物件（可觀測項或資產）啟動常規程式，請於演算法中使用`.input`參數。這些物件將成為常規程式啟動時的輸入內容。例如：

```
"assets": "${ [.input.assets[] | select(.Type == \"host\") | .ID] }"
```

有關詳細資訊，請參閱為使用者指定的物件啟動常規程式。

如何呼叫提示

在編寫演算法時，如需有關可用欄位的提示，請使用引號 (`""`)。隨後會顯示可用欄位清單。

若要在警示或事件資料上顯示提示，

請在 jq 運算式中編寫 `alert` 或 `incident`，並在末尾加上點號`"."`。

如果上述運算式沒有錯誤，則會顯示正確的提示。否則，可用欄位清單可能不正確。

如何呼叫提示

您可以在編寫常規程式演算法時呼叫建議功能。提示包含搜尋字串，可協助您快速指定欄位值。若要檢視建議，請使用引號 (`""`)。隨後會顯示建議清單。

建議也允許您依名稱搜尋。但是，當您選擇所需的值時，名稱將在演算法中自動變更為ID。如需詳細資訊，請參閱使用常規程式編輯事件和使用常規程式編輯警示。

如果您選擇然後刪除引號之間指定的參數名稱，則即使您在引號之間指定了新參數，也不會出現該參數的建議。

若要傳回參數的建議模式，請執行下列其中一項操作：

- 刪除引號，然後新增一個左雙引號。將自動添加右雙引號，並會出現建議。
- 在引號之間鍵入任意字符，然後按**退格鍵** 。這將使您返回建議模式。

如果逐個字元刪除參數名稱，即使完全刪除參數名稱，也不會退出建議模式。

常規程式演算法範例

```
{
  "actionsSpecVersion": "1",
  "dslSpecVersion": "1.1.0",
  "version": "1",
  "playbookRunTimeout": "24h",
  "executionFlow": [
    {
      "action": {
        "function": {
          "type": "blockLDAPAccount"
          "assets": "${[ alert.Assets[] | select(.Type == \"user\" and .IsAttacker) | .ID]}"
        },
        "onError": "stop"
      }
    },
    {
      "loop": {
        "batchSize": 1,
        "input": "${ [alert.OriginalEvents[] | [select(.DestinationProcessName != null and .DestinationProcessName
!= \"\")][] | .DestinationProcessName] }",
        "mode": "parallel",
        "onError": "stop",
        "steps": [
          {
            "action": {
              "function": {
                "type": "killProcess",
                "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
                "params": {
                  "path": "${ .[0] }"
                }
              }
            }
          }
        ]
      }
    },
    {
      "action": {
        "function": {
          "type": "avScan",
          "assets": "${[ alert.Assets[] | select(.Type == \"host\") | .ID]}",
          "params": {
            "scope": {
              "allowScanNetworkDrives": false,
              "area": "full"
            },
            "wait": false
          }
        },
        "onError": "stop"
      }
    }
  ]
}
```

常規程式參數

參數ID	描述
`name`	常規程式的名稱。由系統在建立或更新常規程式時指定。若該值已於演算法中設定，將由系統替換。
`description`	常規程式的描述。由系統在建立或更新常規程式時指定。若該值已於演算法中設定，將由系統替換。
`version`	常規程式版本。最小值為1。 這是必要參數。
`dslSpecVersion`	DSL結構描述版本。最小值為1。 這是必要參數。
`actionSpecVersion`	回應動作結構描述版本。最小值為1。 這是必要參數。
`playbookRunTimeout`	常規程式的最大執行時間，包含在佇列中等待的時間。最大值為48小時（ `48h` ）。您能以小時 (h) 及/或分鐘 (m) 為單位設定最大執行時間。 該值預設為 `24h` 。
`inputType`	傳入物件類型。可能的值： `alert` 或 `incident` 。傳入物件類型由系統在建立或更新常規程式時指定。若該值已於演算法中設定，將由系統替換。
`input`	可用於在執行常規程式之前轉換或篩選傳入資料的jq運算式。
`output`	可用於在執行之前修改常規程式輸出的jq運算式。
`timeouts`	逾時定義。
`executionFlow`	常規程式執行的步驟。 這是必要參數。

執行步驟參數

執行步驟元素陣列描述了常規程式的邏輯。執行步驟按照常規程式中所述的順序執行。執行步驟有以下幾種類型：

- 操作
- 迴圈
- 並行
- 決定
- UpdateData

操作參數

`Action` 參數會呼叫回應函式。

參數ID	描述
`function`	定義回應操作的物件。有關更多資訊，請參閱ResponseFunction參數。

filterProduct	此參數可讓您篩選執行回應操作的元件。請求時，元件外掛程式將依允許和限制的元件進行篩選。 例如，參數可如下指定： `"filterProduct": { "allowed": ["PRODUCT_NAME"] }`
output	此參數可讓您編輯回應操作傳回的值，方法是使用jq運算式並將其放入常規程式資料（本機或作業）中。
timeout	此參數可讓您設定呼叫回應函式的逾時時間。您可以指定常規程式中設定的逾時政策名稱，也可以手動設定逾時值。 若未指定值，則將套用預設值。
manualApprove	此參數可讓您設定手動批准回應操作。可能的值： • 布爾值： • true – 已使用預設參數啟用手動批准。 • false – 手動批准已停用。 • 物件 ManualApprove。
onError	此參數定義在執行回應操作期間發生錯誤時的行為。可能的值： • stop – 定義在執行回應操作期間發生錯誤時，常規程式執行會終止。 • continue – 定義即使其中一項回應操作以錯誤狀態完成，常規程式執行仍會繼續。此種情況下，常規程式將啟動演算法中指定的下一項回應動作。 該值預設為 stop。 請注意，若系統發生錯誤，無論 onError 參數的指定值為何，常規程式執行皆會以錯誤狀態完成。

逾時政策

執行步驟的逾時政策。系統會自動決定預設逾時政策。

您可以使用預設政策名稱重新設定預設逾時政策。在這種情況下，新政策將自動套用於所有執行步驟。

參數ID	描述
name	逾時政策名稱。
scheduleToCloseTimeout	最大執行時間，包括在佇列中等待和重試。此參數以Go 字串格式 指定。 若未指定值或值為 0，則使用 playbookRunTimeout 欄位中的值。

輸出

output 參數會在步驟結束時產生作業資料，然後將其傳輸到下一個步驟。若想在下一個步驟中使用常規程式目前步驟的結果，請指定 output 參數。

為避免系統過載，建議限制放置在常規程式資料（本機或作業）的資料。

參數ID	描述
action	此參數定義常規程式資料（本機或作業）是否將被覆蓋或合併。可能的值： • merge – 新資料會與目前資料合併。 • overwrite – 目前資料會被新資料覆寫。
filter	此參數定義用於處理輸出資料的jq運算式。

手動核准

參數ID	描述
`timeout`	手動核准的逾時時間（以分鐘為單位）。最小值為 10 分鐘（ `10m` ），最大值為 180 分鐘（ `180m` ）。該值預設為 60 分鐘（ `60m` ）。
`emailNotifications`	此參數可讓您設定電子郵件通知的傳送。

郵件通知設定

參數ID	描述
`enabled`	用於啟用電子郵件通知的標誌。
`delay`	此參數定義發送電子郵件通知之前的延遲。該值以分鐘為單位。 最小值為 5 分鐘 (`5m`)，最大值為 30 分鐘 (`30m`)。 該值預設為 10 分鐘 (`10m`)。

循環

在指定 Loop 參數前，請確保常規程式演算法中也指定了 aggregate 參數。

Loop 參數用於按元素拆分傳入資料陣列，並對各元素執行多種動作。

參數ID	描述
`input`	用於組成陣列或引用陣列的jq運算式。
`aggregate`	此參數可讓您使用jq運算式設定彙總規則。
`output`	設定如何將輸出資料套用於目前常規程式資料。可能的值： • 字串常數：`merge` 或 `overwrite`。 • 物件 `Output`。
`mode`	循環操作模式。可能的值： • `parallel` — 定義所有元素皆以平行方式進行處理。執行緒數量由解譯器控制。 • `sequence` — 定義所有元素皆以循序方式進行處理。 該值預設為 `parallel`。
`batchSize`	此參數可讓您指定在一個循環或一個並行執行緒中處理的陣列元素數量。如果外掛程式函式限制了輸入元素的數量，則可以使用此參數。 例如，若外掛程式函式在一次循環中最多只能處理 10 個元素，您可指定如下參數值：`batchSize=10`。 該值預設為 `1`。
`onError`	此參數定義其中一個分支發生錯誤時的行為。可能的值： • `stop` — 定義發生錯誤時終止所有分支。其餘分支將繼續執行。 • 若 `mode=sequence`，當某一分支發生錯誤後，所有後續分支都會停止。 • 若 `mode=parallel`，當某一分支發生錯誤後，所有分支都會繼續獨立執行。 • `continue` — 定義發生錯誤時僅停止發生錯誤的分支。其餘分支將繼續執行。 該值預設為 `stop`。
`steps`	執行步驟陣列。

並行

在指定 Parallel 參數前，請確保常規程式演算法中也指定了 aggregate 參數。

`Parallel` 參數用於同時對資料執行多項操作。與 Loop 不同，`Parallel` 會將相同的輸入資料傳送至不同的執行分支。

參數ID	描述
`input`	用於組成陣列的jq運算式。
`aggregate`	此參數可讓您使用jq運算式設定彙總規則。
`output`	設定如何將輸出資料套用於目前常規程式資料。可能的值： • 字串常數：`merge` 或 `overwrite`。 • 物件 `Output`。
`onError`	此參數定義其中一個分支發生錯誤時的行為。可能的值： • `stop` — 定義發生錯誤時終止所有分支。其餘分支將繼續執行。 • `continue` — 定義發生錯誤時僅停止發生錯誤的分支。其餘分支將繼續執行。 該值預設為 `stop`。
`branches`	執行分支。

分支

參數ID	描述
`name`	`Parallel` 內唯一的分支名稱。
`steps`	執行步驟陣列。

決定

`Decision` 執行步驟可讓您根據條件執行一個步驟或一組步驟。請注意，僅會執行第一個通過驗證的條件。

參數ID	描述
`conditions`	條件陣列。

條件

參數ID	描述
`condition`	包含執行條件的jq運算式。
`steps`	目前分支的執行步驟。

UpdateData

UpdateData 參數可以描述為具有狀態變更邏輯的 jq 指令碼，也可以描述為 `Output` 物件。

回應函式參數

參數ID	描述
`action`	回應操作名稱。
`params`	此參數可讓您描述要啟動的回應操作的參數。您可以將參數指定為jq運算式或物件。下表描述了回應操作的參數。
`assets`	該參數允許使用 jq 運算式或字串陣列來指定要啟動回應動作的資產清單。`assets` 參數是包含資產之回應操作的必要參數，不適用於不包含資產的回應操作。

回應操作參數

回應操作名稱	設定
`updateBases`	更新資料庫回應操作。可能的參數： • `wait`。可能的值： • `true` • `false` 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`avScan`	執行惡意軟體掃描回應操作。可能的參數： • `wait`。可能的值： • `true` • `false` • `scope`。可能的值： • `full`—對偵測到警示的裝置執行完整掃描。 • `critical`—對核心記憶體、執行中的處理程序與磁碟開機磁區執行掃描。 • `selective`—對指定檔案執行掃描。若要指定檔案的路徑，請使用 `path` 參數。 • `allowScanNetworkDrives`。可能的值： • `true` • `false` 該值預設為 `false`。 只有當您要執行完整掃描時，此參數才可用。 請注意，掃描網路磁碟機可能會使系統過載。 • `path`—jq 運算式或包含欲掃描檔案路徑的字串。您也可以指定多個檔案路徑。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`moveHostsToAdministrationGroup`	移至群組回應操作。可能的參數： • `group`—Open Single Management Platform 管理群組路徑。如需範例，請參閱 `HQ/OrgUnit1`。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`quarantineFile`	移至隔離回應操作。可能的參數： • `path`—欲隔離檔案的路徑。 • `md5`—檔案的 MD5 雜湊值。 • `sha256`—檔案的 SHA256 雜湊值。 您可以透過以下其中一種方式指定回應操作參數： • 指定要隔離的檔案的完整路徑。在這種情況下，您不需要指定MD5雜湊值或SHA256雜湊值。 • 指定檔案路徑和檔案雜湊值（MD5或SHA256）。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`restoreQuarantinedFile`	從隔離區回應動作中還原檔案。可能的參數： • `path`—欲還原檔案的路徑。 • `md5`—檔案的 MD5 雜湊值。 • `sha256`—檔案的 SHA256 雜湊值。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`killProcess`	終止進程回應操作。可能的參數： • `pid`—處理程序 ID。 • `path`—欲隔離檔案的路徑。 • `md5`—檔案的 MD5 雜湊值。 • `sha256`—檔案的 SHA256 雜湊值。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。

changeAuthorizationStatus	更改授權狀態回應操作。可能的參數： • authorized。可能的值： • true • false 若要啟動此回應操作，需指定回應函式的 asset 參數。
netIsolateOn	啟用網路隔離回應操作。可能的參數： • isolationTimeoutSec—網路隔離期間。可以小時或天為單位指定此參數。最小值為1小時，最大值為9999小時。 網路隔離期間以秒為單位指定。 • exclusions—排除規則。可以指定一或多條排除規則。 • remoteIPV4Address—來自指定 IPv4 位址的網路流量將被排除於封鎖範圍外。例如，192.168.2.15。 • remoteIPV6Address—來自指定 IPv6 位址的網路流量將被排除於封鎖範圍外。例如，2001:0db8:0000:0000:0000:ff00:0042。 • remotePortRange—遠端連接埠範圍。 • localPortRange—本機連接埠範圍。 如果未指定 remotePortRange 和 localPortRange，排除規則會套用至所有連接埠。 • exclusionsConflictBehavior—定義不同排除規則之間發生衝突時的行為。可能的參數： • replace • skip • fail
netIsolateOff	停用網路隔離回應操作。 若要啟動此回應操作，需指定回應函式的 asset 參數。
executeCommand	執行可執行檔回應操作。可能的參數： • commandLine—要執行的命令或可執行檔的完整路徑。 • workingDirectory—工作目錄的路徑。 • commandLineParameters—要套用於命令的命令列參數。 若要啟動此回應操作，需指定回應函式的 asset 參數。
addFilePreventionRules	新增防護規則回應操作。可能的參數： • md5—MD5 雜湊值陣列。 • sha256—SHA256 雜湊值陣列。 若要啟動此回應操作，需指定回應函式的 asset 參數。
deleteFilePreventionRules	刪除防護規則回應操作。可能的參數： • md5—MD5 雜湊值陣列。 • sha256—SHA256 雜湊值陣列。 若要啟動此回應操作，需指定回應函式的 asset 參數。
resetFilePreventionRules	刪除所有防護規則。 若要啟動此回應操作，需指定回應函式的 asset 參數。
assignKasapGroup	指派KASAP群組回應操作。可能的參數： groupId—KASAP 群組識別碼。 若要啟動此回應操作，需指定回應函式的 asset 參數。
addToLDAPGroup	將使用者新增至安全群組回應操作。可能的參數： groupDN—LDAP 群組的區分名稱 (DN)。 若要啟動此回應操作，需指定回應函式的 asset 參數。
removeFromLDAPGroup	從安全組回應操作中刪除使用者。可能的參數： groupDN—LDAP 群組的區分名稱 (DN)。 若要啟動此回應操作，需指定回應函式的 asset 參數。

`blockLDAPAccount`	鎖定帳戶回應操作。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`resetLDAPPassword`	重設密碼回應操作。 若要啟動此回應操作，需指定回應函式的 `asset` 參數。
`executeCustomScript`	執行自訂指令碼。可能的參數： • `commandLine`—待執行命令。 • `commandLineParameters`—要套用於命令的命令列參數。 • `stdIn`—標準輸入資料流。若指令碼需從標準輸入取得額外資料，請使用此參數。 • `workingDirectory`—工作目錄的路徑。
`iocsEnrichment`	資料擴充。可能的參數： • `observables`—包含要擴充的可觀測項陣列的 jq 運算式。 • `fullEnrichment`—定義要請求的記錄數。可能的值： • `true`—從來源請求所有記錄。 • `false`—從來源請求前 100 筆記錄。

使用常規程式編輯事件

Kaspersky Next XDR Expert允許您手動或使用常規程式編輯事件。建立常規程式時，您可以設定常規程式演算法來編輯事件內容。

為了使用常規程式編輯事件，您必須具有以下角色之一：主管理員、 SOC管理員、一級分析師、二級分析師、租用戶管理員。

您無法編輯狀態為**已關閉**的事件。

您可以使用常規程式編輯下列事件內容：

- 受讓人
- 事件工作流程狀態
- 事件類型
- 註解
- 描述
- 優先順序
- 外部參考屬性
- 其他資料內容

以下是一些範例運算式，您可以在常規程式中使用這些運算式來編輯事件內容。您可以在視覺化編輯器的**顯示程式碼**部分指定這些運算式。

- **向使用者指派事件**

```
{
  "action": {
    "function": {
       "type": "assignIncident",
      "params": {
     "assignee": {
        "id": "user_ID"
       }
        }
        }
    }
       }
```

在常規程式演算法中編輯受讓人時，系統會顯示建議。為了方便起見，建議中包含一個搜尋字串，您可以依名稱進行搜尋。如果您想指定事件受讓人，可以依照使用者名稱搜尋對應的記錄，系統會在演算法中指定該ID。

- **向使用者群組指派事件**

```
{
    "action": {
      "function": {
         "type": "assignIncident",
          "params": {
            "group": {
               "id": "GROUP_ID"
                                }
                        }
                }
            }
        }
```

在常規程式演算法中編輯受讓人時，系統會顯示建議。為了方便起見，建議中包含一個搜尋字串，您可以依名稱進行搜尋。如果您想要指定事件受讓人，可以依照使用者群組名稱搜尋對應的記錄，系統會在演算法中指定該ID。

- **取消事件指派給使用者**

```
{
  "action": {
    "function": {
       "type": "assignIncident",
      "params": {
     "assignee": {
        "id": "nobody"
       }
        }
        }
    }
       }
```

- **取消事件指派給使用者群組**

```
{
    "action": {
      "function": {
```

```
          "type": "assignIncident",
           "params": {
             "group": {
                "id": "nobody"
                              }
                          }
                    }
                }
           }
```

- **變更事件工作流程狀態**

  若要將事件工作流程狀態變更為**開啟**：

```
{
    "action": {
      "function": {
         "type": "setIncidentStatus",
         "params": {
           "typeId": "af9dd279-fc30-4596-963b-942f79920375",
           "statusId": "4db36105-5223-4078-b72c-e9e9983b0987"
                          }
                    }
                }
           }
```

  若要將事件工作流程狀態變更為**關閉**：

```
{
  "action": {
    "function": {
       "type": "setIncidentStatus",
       "params": {
        "statusId": "INCIDENT_STATUS_ID",
                  "statusResolution": "truePositive"
         }
         }
    }
       }
```

  您亦可為 `statusResolution` 參數指定如下值：`falsePositive` 和 `lowPriority`。

  若要將事件工作流程狀態變更為自訂狀態：

```
{
  "action": {
    "function": {
       "type": "setIncidentStatus",
       "params": {
                  "typeId": "22222222-2222-2222-2222-222222222222",
                  "statusId": "11111111-1111-1111-1111-111111111111"
         }
         }
    }
       }
```

  在常規程式演算法中編輯事件工作流程狀態時，系統會顯示建議。為了方便起見，建議中包含一個搜尋字串，您可以依名稱進行搜尋。若要指定事件工作流程狀態，可以按名稱搜尋對應的記錄，系統會在演算法中指定該ID。

- **更改事件類型**

```
{
  "action": {
    "function": {
       "type": "setIncidentType",
       "params": {
        "id": "INCIDENT_TYPE_UUID"
         }
         }
    }
       }
```

在常規程式演算法中編輯事件類型時，系統會顯示建議。為了方便起見，建議中包含一個搜尋字串，您可以依名稱進行搜尋。若要指定事件類型，可以按名稱搜尋對應的記錄，系統會在演算法中指定該ID。

- **為事件新增備注**

```
{
  "action": {
    "function": {
       "type": "addCommentToIncident",
       "params": {
     "text": "${ \"ID 為 [[: \\(incident.ID)\" }"          ]] 的事件的新備註
         }
         }
    }
       }
```

- **編輯事件描述**

```
{
   "action": {
     "function": {
        "type": "setIncidentDescription",
        "params": {
              "description": "${ incident.ID | tostring | \"ID 為 [[: \" + . }",]] 的事件有新評論
              "mode": "replace"
                       }
                  }
              }
         }
```

若要附加至現有描述，請為 mode 參數指定 append 值。

- **變更事件優先順序**

```
{
  "action": {
    "function": {
       "type": "setIncidentPriority",
       "params": {
        "priority": "critical"
         }
         }
    }
       }
```

您也可以為 priority 參數指定以下值：high、medium、low。

- **編輯外部參考屬性**

```
{
    "action": {
      "function": {
         "type": "setIncidentExternalRef",
         "params": {
               "externalRef": "${ \"新值 extReference\" }",
               "mode": "replace"
                        }
                    }
                }
          }
```

若要附加至 ExternalReference 屬性，請為 `mode` 參數指定 `append` 值。

- **編輯附加資料屬性**

```
{
  "action": {
    "function": {
       "type": "addIncidentAdditionalData",
       "params": {
     "data": "${ {\"customKey\": \"customValue\"} }",
               "mode": "replace"
         }
         }
    }
       }
```

若要附加至附加資料屬性，請為 `mode` 參數指定 `append` 值。

使用常規程式編輯警示

Kaspersky Next XDR Expert可讓您手動或使用常規程式編輯警示。建立常規程式時，您可以設定常規程式演算法來編輯警示內容。

若要使用常規程式編輯警示，您必須具有以下XDR角色之一：主管理員、 SOC管理員、一級分析師、二級分析師或租用戶管理員。

您無法編輯狀態為**已關閉**的警示。

您可以使用常規程式編輯下列警示內容：

- 受讓人
- 警示狀態
- 註解
- 外部參考屬性
- 其他資料內容

以下是一些範例運算式，您可以在視覺化常規程式編輯器的**顯示程式碼**部分輸入這些運算式來變更警示內容。

- **向使用者指派警示**

```
{
       "action": {
           "function": {
               "type": "assignAlert",
                   "params": {
                      "assignee": {
                         "id": "user_ID"
                       }
                   }
               }
           }
       }
```

在常規程式演算法中編輯受讓人時，系統會顯示建議。為了方便起見，建議中包含一個搜尋字串，您可以依名稱進行搜尋。如果您想要指定警示受讓人，可以依照使用者名稱搜尋對應的記錄，系統會在演算法中指定ID。

- **向使用者群組指派警示**

```
{
    "action": {
      "function": {
         "type": "assignAlert",
          "params": {
            "group": {
               "id": "GROUP_ID"
                                }
                        }
                    }
                }
          }
```

在常規程式演算法中編輯受讓人時，系統會顯示建議。為了方便起見，建議中包含一個搜尋字串，您可以透過使用者群組名稱進行搜尋。如果您想要指定警示受讓人，可以依照使用者名稱搜尋對應的記錄，系統會在演算法中指定ID。

- **從使用者中取消指派警示**

```
{
            "action": {
                "function": {
                    "type": "assignAlert",
                    "params": {
                        "assignee": {
                            "id": "nobody"
                        }
                    }
                }
            }
        }
```

- **從使用者群組中取消指派警示**

```
{
    "action": {
      "function": {
         "type": "assignAlert",
          "params": {
```

```
            "group": {
               "id": "nobody"
                                }
                           }
                      }
                 }
            }
```

- **更改警示狀態**

  若要將警示狀態變更為**調查中**：

```
{
            "action": {
                "function": {
                    "type": "setAlertStatus",
                        "params": {
                            "status": "inProgress"
                     }
                }
            }
        }
```

  若要將警示狀態變更為**已關閉**：

```
{
            "action": {
                "function": {
                    "type": "setAlertStatus",
                        "params": {
                            "status": "closed",
                            "statusResolution": "truePositive"
                     }
                }
            }
        }
```

  您也可以為 statusResolution 參數指定如下值：`falsePositive` 與 `lowPriority`。

  在常規程式演算法中編輯警示狀態時，可能會顯示以下建議選項：`new`、`inProgress`、`closed`。

- **向警示新增備注**

```
{
            "action": {
                "function": {
                    "type": "addCommentToAlert",
                    "params": {
                        "text": "${ \"New comment for alert with ID: \" + alert.InternalID }"
                    }
                }
            }
        }
```

- **編輯外部參考屬性**

```
{
      "action": {
          "function": {
                "type": "setAlertExternalRef",
                   "params": {
                     "externalRef": "${ \"Appended externalRef for alert with ID: \" + alert.InternalID }",
                       "mode": "append"
```

```
                    }
                }
            }
        }
```

若要以常規程式中的值替換警示中 ExternalReference 屬性的目前值，請為 `mode` 參數指定 `replace` 值。

- **編輯附加資料屬性**

```
{
      "action": {
           "function": {
              "type": "addAlertAdditionalData",
                "params": {
                   "data": "${ {\"customKey_1 (alert.InternalID)\": (\"customValue_1 (\" + alert.InternalID +
\")\" )} }",
                   "mode": "append"
                   }
                }
            }
        }
```

若要以常規程式中的值替換警示中 AdditionalData 屬性的目前值，請為 `mode` 參數指定 `replace` 值。

管理沙盒shahe

沙盒是一種安全元件，它利用具有作業系統映像的虛擬機器（VM）來分析物件（例如檔案、程式或指令碼）的行為，以發現潛在的惡意活動和針對企業IT基礎設施的定向攻擊跡象。

要讓沙盒處理物件，需要對其進行設定，然後在沙盒中安裝虛擬機器。

初始社會設定

在安裝虛擬機器之前，您需要設定沙盒：

- 設定資料庫更新。
- 確保在安裝沙盒期間正確設定了網際網路存取。請根據需要調整設定。

您也可以選擇變更管理員密碼並設定身分驗證政策。

為沙盒設定資料庫更新

在產品授權有效期限內，沙盒會每小時自動取得一次更新套件。

若要配置沙盒資料庫更新：

1. 在沙盒網頁介面中，請轉至**資料庫更新**。
2. 在**更新來源**設定群組中，選擇要從中接收更新的來源：
   - **卡巴斯基更新伺服器**
     沙盒透過HTTP連線到卡巴斯基更新伺服器並下載最新的資料庫。
   - **卡巴斯基更新伺服器（安全連線）**
     沙盒透過HTTPS連線到卡巴斯基更新伺服器，以下載最新的資料庫。建議使用HTTPS進行安全性更新。
   - **自訂伺服器**
     沙盒連線到您的FTP或HTTP伺服器，或連線到您電腦上的程式資料庫資料夾，以下載最新的資料庫。
3. 如果您選取了**自訂伺服器**：
   - 如果您要將 FTP 或 HTTP 伺服器指定為更新來源，請在此設定下方的欄位中，指定應用程式資料庫更新套件目錄的完整路徑，以下載最新的資料庫。
   - 如果您要將託管沙盒元件的 Kaspersky Next XDR Expert 伺服器指定為更新來源，請在此設定下方的欄位中，指定以下更新來源位址，以下載最新的資料庫：

     ```
     http://updater.<smp_domain>:8083/retranslation
     ```

4. 決定下載更新時是否使用代理伺服器：

   - 若要啟用代理伺服器，請開啟**代理伺服器**設定群組名稱旁的切換開關，然後指定連線到代理伺服器的設定：

     - 代理伺服器位址和連接埠號。

     - 輸入使用者名稱和密碼。

   - 若要停用代理伺服器，請關閉**代理伺服器**設定群組名稱旁的切換開關。

5. 按一下**套用**以儲存設定。

沙盒網路介面

設定沙盒網路介面包括設定DNS伺服器、設定管理網路介面、管理已處理物件的網際網路存取以及新增靜態網路路由。

配置DNS設定

若要設定DNS：

1. 在沙盒網頁介面中，請轉至**網路介面**。

2. 在**主機名稱**欄位中，指定要安裝沙盒的伺服器名稱。伺服器名稱必須採用FQDN格式。

3. 按一下**DNS伺服器**右側的**新增**按鈕。

4. 在出現的空白欄位中，以IPv4格式指定主要DNS伺服器的IP位址。

5. 按一下指定的IP位址右側的✓按鈕。

DNS伺服器隨即新增。

若要新增更多DNS伺服器，請重複步驟2至5。

若要刪除先前新增的DNS伺服器，請按一下指定的DNS伺服器IP位址右側的🗑。請注意，您只能刪除其他DNS伺服器，而無法刪除主要DNS伺服器。如果您新增了兩個或兩個以上的DNS伺服器，您可以刪除其中任何一個。剩餘的DNS伺服器將成為主要伺服器。

設定管理網路介面

管理網路介面旨在透過SSH協定提供對沙盒伺服器的存取。沙盒也透過此介面接收物件。

管理網路介面是在沙盒安裝期間初始設定的。沙盒安裝完成後，您可以按照以下說明從沙盒網頁介面變更管理網路介面設定。

若要設定管理網路介面：

1. 在沙盒網頁介面中，請轉至**網路介面**。
2. 在**介面**下拉清單中的**管理介面**設定群組中，選擇要用作管理介面的網路介面。
3. 配置管理介面參數：
   - **IP** ：如果未指派IP位址，則要指派給此網路介面的IP位址。
   - **遮罩**：您要使用此網路介面的網路的遮罩。
4. 點選**套用**。

管理網路介面隨即設定。

設定已處理物件的網際網路存取

沙盒處理的物件可能會嘗試透過設定為存取網際網路的網路介面在網際網路上執行操作。在這種情況下，沙盒可以分析這些物件在網路上的行為。如果阻止網路存取，沙盒會分析物件的行為，但不包括它們在網路上的操作。

安全風險及注意事項

如果貴組織的安全政策阻止本地網路電腦存取網際網路，而用於存取網際網路的沙盒網路介面是開放的，則可能會出現以下情況：

1. 駭客將惡意的應用程式添加到隨機檔案中，然後從本地網路電腦將其傳送到沙盒進行掃描。
2. 掃描過程中，檔案會傳送到本地網路以外。

如果阻止對已處理物件的網際網路存取，則這種風險已消除。然而，這也意味著警示品質降低，因為處理後的物件無法得到正確的分析。

若要設定用於處理物件存取網際網路的網路介面：

1. 在沙盒網頁介面中，請轉至**網路介面**。
2. 在**介面**清單中的**網際網路介面**設定群組中，選擇要用於處理物件的網際網路存取的網路介面。
3. 設定介面參數：
   - **IP** ：如果未指派IP位址，則要指派給此網路介面的IP位址。
   - **遮罩**：您要使用此網路介面的網路的遮罩。
   - **預設閘道**：您希望使用此網路介面的網路的閘道位址。
4. 點選**套用**。

用於透過網際網路存取處理物件的網路介面隨即設定。

新增靜態網路路由

若要新增靜態網路路由：

1. 在沙盒網頁介面中，請轉至**網路介面**。
2. 在**靜態路由**設定群組中，按一下**新增**按鈕。
   靜態網路路由清單中出現了一組空白欄位。
3. 設定路由參數：
   - **IP**：要為其設定靜態網路路由的伺服器的IP位址。
   - **遮罩**：子網路遮罩。
   - **閘道**：閘道的IP位址。
4. 從**介面**清單中，選擇要為其新增靜態網路路由的網路介面。
5. 點選指定路由右側的✓按鈕。
6. 點選**套用**。

靜態網路路由隨即新增。

新增靜態網路路由後，您可以透過按下🗑刪除按鈕或按下✎修改按鈕它來進一步管理它。修改時，您需要指定與建立新路由時相同的參數，如上所述。

變更沙盒管理員帳戶密碼

若要變更沙盒管理員帳戶密碼：

1. 在沙盒網頁介面中，轉至**管理** → **更改密碼**。
2. 在**目前密碼**欄位中，輸入您用於登入沙盒的密碼。
3. 在**新密碼**和**確認密碼**欄位中，輸入新密碼。
4. 點選**更改密碼**。

沙盒身分驗證政策

您可以在沙盒中為 Kaspersky Next XDR Expert 使用者設定身分驗證政策。

終止不活躍的會話

如果使用者沒有進行任何操作（會話處於空閒狀態），我們建議終止該會話。這樣可以降低使用者實際完成應用程式操作但未結束會話時，未經授權存取沙盒的風險。

關於身分驗證嘗試失敗的通知

頻繁嘗試登入網頁介面失敗可能表示網路犯罪分子正試圖透過暴力破解密碼來存取沙盒。為防止此類未經授權的存取，我們建議啟用關於身份身分驗證嘗試次數超過限制的通知。

終止不活躍的沙盒會話

如果使用者沒有進行任何操作（會話處於空閒狀態），我們建議終止該會話。這樣可以降低使用者實際完成應用程式操作但未結束會話時，未經授權存取沙盒的風險。

若要啟用和設定終止非活動會話的功能：

1. 在沙盒網頁介面中，請轉至**身份驗證政策**。
2. 在**終止不活動會話**部分，指定如果使用者未執行任何操作，則希望在多長時間後終止使用者會話。在**終止不活動會話時間**欄位中輸入以分鐘為單位的時間。
3. 點選**套用**。

沙箱會在指定時間後終止不活躍的使用者會話。

關於沙盒身分驗證嘗試失敗的通知

頻繁嘗試登入網頁介面失敗可能表示網路犯罪分子正試圖透過暴力破解密碼來存取沙盒。為防止此類未經授權的存取，我們建議啟用關於身份身分驗證嘗試次數超過限制的通知。

若要啟用並設定有關身分驗證失敗嘗試的通知：

1. 在沙盒網頁介面中，請轉至**身份驗證政策**。
2. 在**統計身份身分驗證嘗試次數**部分中，將**計數嘗試**切換開關設定為**啟用**。
3. 在**計數期間**欄位中，輸入要統計失敗身分驗證嘗試次數的期間。時間以分鐘為單位指定。如果使用者嘗試登入網頁介面或管理主控台，並且連續失敗超過兩次，則會發生以下情況：
   - 將使用者失敗的驗證嘗試記錄寫入使用者活動日誌。
   - 如果已建立用於傳送失敗身分驗證嘗試次數過多通知的規則，則會傳送電子郵件至通知規則中指定的電郵地址。該郵件包含有關失敗使用者身分驗證嘗試的資訊訊息。

在**計數期間**欄位中，您可以指定`0`，在此情況下，無論失敗的身分驗證嘗試之間間隔多久，都會計入所有失敗的身分驗證嘗試。

4. 點選**套用**。

設定將偵測到的物件傳送到KPSN拒絕清單

該應用程式允許具有一級分析師和二級分析師角色的用戶啟用或停用將沙盒掃描到的惡意的檔案雜湊值自動發送到KPSN拒絕清單。此參數的組態因租用戶而異。它只能在OSMP安裝程式的根租用戶中變更：在子租用戶中，此選項無法變更。

在啟用將偵測到的物件自動傳送至KPSN拒絕清單之前，請確保已啟用KPSN使用，並且與KPSN本機信譽評比資料庫的連線已設定。

若要啟用將偵測到的物件自動傳送至KPSN拒絕清單的功能：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 按一下**根租用戶**，然後轉至**設定→KPSN本機信譽資料庫**子區段。
3. 開啟**將物件狀態設為「不受信任」**切換按鈕。
4. 按一下**儲存**按鈕。

準備虛擬機器

沙盒使用虛擬機器在各種作業系統上運行物件，以便分析物件的行為並偵測其惡意的活動。

您可以安裝兩種類型的虛擬機器：

- *預配置*或*預設定*。這些是基於分發套件中的作業系統映像（ISO檔案）的虛擬機器。您無法修改這些映像或其中安裝的應用程式。

  > 預設作業系統和應用程式可能需要啟動。啟動需要使用您的產品授權。

- *自訂*。這些是基於您選擇的作業系統的虛擬機器。你可以在這些作業系統上安裝任何應用程式。

您可以同時使用自訂作業系統映像和預設作業系統映像。

安裝虛擬機器包括以下步驟：

1. *可選*。將映像上傳到儲存體。建立範本時，您可以跳過此步驟，直接從電腦上傳映像。
2. 透過匯入預先配置範本或建立自訂虛擬機器範本來建立範本。
3. *對於自訂範本*。設定作業系統和軟體。

4. 建立虛擬機器。
5. 安裝虛擬機器。

將映像上傳到儲存體

若要將映像上傳到儲存體：

1. 在沙盒網頁介面中，轉至**範本與儲存體 → 儲存體**。
2. 點擊**上傳**。
3. 選擇要上傳到儲存體的ISO檔案，然後按一下**開啟**。

匯入範本

如果要安裝預先配置的虛擬機，第一步是匯入範本。

如果您之前已經建立並匯出了自訂虛擬機器範本，也可以匯入該範本。

若要匯入虛擬機器範本：

1. 在沙盒網頁介面中，轉至**範本與儲存體 → 範本**。
2. 從**新增**下拉清單中，選擇**匯入範本**。
3. 選擇要匯入的檔案，然後按一下**開啟**。

建立自訂虛擬機器範本

若要建立自訂虛擬機器範本：

1. 在沙盒網頁介面中，轉至**範本與儲存體 → 範本**。
2. 從**新增**下拉清單中，選擇**建立範本**。
   範本建立視窗隨即開啟。

3. 在**準備映像**步驟中：

   a. 指定映像**名稱**和可選**描述**。

   b. 若要為範本指定作業系統，請執行下列操作之一：

   - 從**作業系統映像**下拉清單中選擇一個映像。
   - 上傳作業系統映像：點選**上傳**，選擇一個ISO檔案，然後點選**開啟**。

   c. 點選**繼續**。

4. 在**自訂範本**步驟中：

   a. 在**掛載ISO**下拉清單中，選擇要安裝到作業系統中的應用程式的映像。
   若要將映像顯示在清單中，請執行下列其中一項操作：

   - 將映像上傳到儲存體。
   - 上傳應用程式映像檔案：按一下**上傳**，選擇ISO檔案，然後按一下**開啟**。

   b. 應用程式安裝完成後，解除安裝已安裝的映像：在**掛載ISO**下拉清單中，按一下映像旁邊的⏏圖示。

   c. 設定作業系統和已安裝的軟體。

設定作業系統和軟體

準備作業系統以供使用

安裝Windows 7、8.1或10作業系統時，必須符合以下需求：

- 停用螢幕保護程式。
- 選擇「始終開啟」電源計劃。
- 停用自動更新。
- 停用Windows防火牆。

如果您使用的是Windows 7，則需要支援SHA-2雜湊演算法。為確保支援此雜湊演算法，請安裝適用於64位元系統的Windows 7安全性更新（KB3033929）。對於32位元的Windows7作業系統，也必須安裝更新KB3033929。

> 請勿安裝更新KB4474419。此更新可能會導致虛擬機器在部署期間崩潰。

若要使用Windows 7，必須在作業系統設定中啟用TLS 1.1和TLS 1.2。為此，在Windows 7中，請依序點選**控制窗格 → 網際網路選項 → 進階**部分，選取**使用 TLS 1.1**和**使用 TLS 1.2**核取方塊。

使用 Windows 8.1 或 10 時，您必須停用快速啟動並啟用自動登入。

作業系統在地化

您可以在安裝系統時選擇在地化語言，或者使用英語在地化安裝系統，並在該系統中額外安裝在地化軟體套件。您可以選擇以下語言之一：俄語、繁體中文（台灣）、簡體中文、阿拉伯語、西班牙語（墨西哥）。如果選擇其他在地化語言，物件掃描品質會降低。

Windows XP作業系統僅支援俄語和繁體中文（台灣）。

設定作業系統

安裝作業系統時：

- 請確保已設定預設命令shell。
- 啟動作業系統和其他產品授權軟體。

您可以使用已安裝的作業系統執行以下操作：

- 給電腦指定一個靜態名稱。
- 建立使用者帳戶。

  在這種情況下，您需要設定自動登入。

- 安裝軟體。
  軟體安裝限制：
  - 一次只能將一個映像聯繫到一個範本。範本儲存後，您可以斷開一個映像並掛載另一個映像。
  - 不支援2016年之後的Microsoft Office版本。
  - 強烈建議不要安裝以下類型的軟體：
    - 將自身程式碼注入到另一個正在執行的進程中的軟體
    - 防護驅動器
    - 包括Windows Defender在內的防毒應用程式
  - 對於依賴高度專業化軟體運行的檔案，無法保證能夠偵測到惡意的活動。

Kaspersky Next XDR Expert不會就作業系統上安裝的軟體問題發出通知。

建立虛擬機器

若要建立具有自訂作業系統映像的虛擬機器，需要存取網際網路。

若要建立虛擬機器：

1. *對於自訂範本*。請確保用於建立虛擬機器的範本已關閉：
   a. 在沙盒網頁介面中，轉至**範本與儲存體 → 範本**。
   b. 選取範本。
   c. 如果範本已啟用，請從**關閉**下拉清單中選擇其中一個選項：
      - 如果您想在儲存應用程式運行結果的同時關閉系統，請使用**關機命令**。
      - 如果想在不儲存結果的情況下關閉系統，**請關機**。
2. 在沙盒網頁介面中，轉至**虛擬機器**。
3. 點擊**建立虛擬機器**。
4. 在**範本**下拉清單中，選擇一個範本。
5. *對於自訂作業系統*：指定虛擬機器**名稱**和可選的**描述**。
6. 按一下**儲存**按鈕。
7. *對於預先配置的作業系統*：分發套件中的某些作業系統需要接受最終使用者產品授權協定的條款。閱讀最終使用者產品授權協定的文字，然後按一下**接受**。
8. *對於自訂作業系統*：如果您要建立虛擬機器的伺服器未設定網際網路存取，則會在*範本*視窗中顯示**無網際網路存取**錯誤訊息。若要完成虛擬機器建立過程，您必須下載偵錯符號。

安裝虛擬機器

若要安裝預先配置作業系統的虛擬機器：

1. 在沙盒網頁介面中，轉至**虛擬機器 → 預先配置**。
2. 在**未安裝的虛擬機器**部分，按一下**安裝就緒的虛擬機器**。

若要安裝包含自訂作業系統的虛擬機器：

1. 在沙盒網頁介面中，轉至**虛擬機器 → 自訂**。
2. 在清單中找到虛擬機器，然後在**操作**直欄中，按一下**安裝**。
3. 安裝虛擬機器後，在**操作**直欄中，按一下**啟用**。

下載偵錯符號

如果安裝了自訂映像的虛擬機器的伺服器未設定網際網路訪問，則必須下載Microsoft偵錯符號才能正確完成虛擬機器的安裝。

為了正確下載偵錯符號，用於虛擬機器範本的作業系統必須安裝Windows偵錯工具，且聯繫到網路的主機名稱（hostname）必須僅包含拉丁字母、數字和特殊字元。

若要下載偵錯符號：

1. 在沙盒網頁介面中，轉至**範本與儲存體 → 範本**。
2. 選取範本。
3. 在顯示**無網際網路存取**錯誤訊息的視窗中，點選**下載清查檔案**。

   只有當虛擬機器狀態變成**失敗**時，才能**下載清查檔案**。
4. 解壓縮下載的存檔。
5. 使用Windows PowerShell執行sbsymtool.ps1。
   此指令碼會下載一個包含偵錯符號的存檔。
6. 在沙盒網頁介面中，轉至**範本與儲存體 → 範本**。
7. 選擇已下載偵錯符號的範本。
8. 在**操作**下拉清單中，選擇**上傳符號**。
9. 在開啟的視窗中，選擇包含偵錯符號的存檔，然後按一下**開啟**。

偵錯符號隨即下載。

設定OSMP以使用偵測技術

Kaspersky Next XDR Expert使用不同的偵測技術（例如反惡意軟體引擎或沙盒）來偵測威脅。您需要設定OSMP才能使用這些偵測技術。

反惡意軟體引擎

對於反惡意軟體引擎，請執行以下操作：

- 設定取得防病毒資料庫的更新。
- 建立受密碼保護的封存檔案的密碼清單。

沙盒

安裝和設定沙盒，並在其中安裝虛擬機器後，您需要執行以下操作：

- 設定取得防病毒資料庫的更新。
- 選擇要掃描物件的作業系統。
- 若要使用自訂作業系統，請建立自訂沙盒規則。
- 設定從端點代理程式傳送檔案。

YARA

對於YARA掃描，請執行以下操作：

匯入YARA規則

IOC

對於IOC掃描，請執行以下操作：

- 設定排定的IOC掃描
- 匯入IOC規則

更新沙盒和反惡意軟體引擎的防病毒資料庫

掃描物件時，沙盒和反惡意軟體引擎需要最新的防病毒資料庫，因此應定期更新防病毒資料庫。作為更新來源，您可以使用卡巴斯基伺服器或您自己的來源，該來源可以是HTTP伺服器、FTP伺服器或資料夾。

Kaspersky Next XDR Expert每30分鐘自動從指定來源尋找新的更新套件。您也可以隨時手動更新防病毒資料庫。

若要設定沙盒和反惡意軟體引擎的更新，您必須具有以下XDR 角色之一：主管理員、SOC 管理員、租用戶管理員、稽核員。
具有稽核員角色的使用者只能檢視目前的更新來源。具有其他角色的使用者可以檢視和更改更新來源。

若要設定沙盒和反惡意軟體引擎的更新：

1. 在主功能表中，轉至**設定 → 租用戶**。
   租用戶篩選器隨即開啟。該清單僅包含您至少擁有**讀取**存取權限的租用戶。
2. 按一下**根**租用戶（無法在其他租用戶中變更更新設定）。
   這會開啟租用戶內容視窗。
3. 選取**設定**頁籤。
4. 在**正在掃描**部分，選擇**更新資料庫**頁籤。
5. 在**更新來源**下拉清單中，選擇下列更新來源之一：
   - **卡巴斯基更新伺服器（安全連線）**
     Kaspersky Next XDR Expert透過HTTPS連線到卡巴斯基更新伺服器並下載最新的資料庫。建議使用HTTPS下載資料庫更新。
   - **卡巴斯基更新伺服器**
     Kaspersky Next XDR Expert透過HTTP連線到卡巴斯基更新伺服器並下載最新的資料庫。
   - **自訂伺服器**
     Kaspersky Next XDR Expert會連線到您的更新來源以下載最新的資料庫。在**URL 或資料夾路徑**中指定更新來源的路徑。它可以是HTTP或FTP伺服器的URL，也可以是包含更新套件的資料夾的完整路徑。
6. 如果要立即更新防毒資料庫，請按一下**更新**。
7. 點擊**儲存**按鈕。

沙盒和反惡意軟體引擎的更新隨即設定。Kaspersky Next XDR Expert在**更新日期**欄位中顯示有關最新的更新資訊。

您可以隨時點擊**更新**按鈕手動更新防毒資料庫。

建立受密碼保護的封存檔案的密碼清單

預設情況下，Kaspersky Next XDR Expert無法掃描受密碼保護的封存檔案中的物件。此類封存檔案必須先解除壓縮。您可以建立一個組織內常用封存檔案的密碼清單。Kaspersky Next XDR Expert在掃描封存檔案時會嘗試清單中的密碼。如果其中一個密碼匹配，Kaspersky Next XDR Expert將解除壓縮封存檔案並掃描其中的物件。

若要使用受密碼保護的壓縮檔案的密碼清單，您必須具有以下XDR 角色之一：主管理員、租用戶管理員、一級分析師、二級分析師、稽核員。
具有稽核員角色的使用者只能檢視密碼清單。具有其他角色的使用者可以查看和編輯該清單。

若要建立用於解除壓縮受密碼保護的封存檔案的密碼清單：

1. 在主功能表中，轉至**設定 → 租用戶**。
   租用戶篩選器隨即開啟。該清單僅包含您至少擁有**讀取**存取權限的租用戶。
2. 按一下**根**租用戶（其他租用戶中的密碼清單無法變更）。
   這會開啟租用戶內容視窗。
3. 選取**設定**頁籤。
4. 在**正在掃描**區段，選擇**存檔**頁籤。
5. 在**封存檔案的密碼**欄位中，新增用於解壓縮受密碼保護的歸檔檔案的密碼，每個密碼佔一行。
6. 如果您想限制對密碼清單的訪問，請啟用**需要密碼才能存取密碼清單**切換開關，然後在**設定存取密碼**窗格中指定密碼。您可以將此密碼共用給需要存取受密碼保護的封存檔案密碼清單的OSMP使用者。
   按一下**儲存**以儲存存取密碼。
   如有必要，您可以稍後透過點擊**存檔**頁籤上的**變更密碼**來變更此密碼。
7. 按一下**儲存**或**儲存並關閉**，以儲存受密碼保護的壓縮檔案密碼清單。

選擇用於掃描沙盒中物件的作業系統

沙盒元件在多個作業系統中執行物件，並分析這些物件的行為，以檢測惡意活動和定向攻擊和侵入企業IT基礎設施的指標。

您可以選擇用於掃描物件的作業系統。它可以是預定義集之一、自訂集或它們的組合。

若要選擇作業系統集：

1. 在主功能表中，轉至**設定 → 租用戶**。
   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。
2. 按一下所需政策的名稱。
   這會開啟租用戶內容視窗。

3. 選取**設定**頁籤。
4. 在**Sandbox 伺服器**區段，點選**待檢查的作業系統**。
5. 在開啟的**編輯作業系統集**窗格中，在**作業系統集**下，選擇預先定義的作業系統集之一或**自訂**。
   如果要將預設作業系統與自訂作業系統結合使用，請選擇**自訂**。
6. 如果選擇了**自訂**，則**集內容**下會顯示可用作業系統的列表。
   此清單始終包含預設的作業系統。如果在沙盒中沒有執行預設作業系統的虛擬機器，則該作業系統的狀態為**未知**。
   如果沙盒伺服器上執行某個作業系統，則該自訂作業系統也會包含在清單中。
   選取要包含在集合中的作業系統旁的核取方塊。
7. 點擊**儲存**按鈕。

用於掃描物件的作業系統集隨即準備就緒。

對於自訂作業系統集，您還需要建立自訂規則。

建立自訂沙盒規則

如果您已選擇自訂作業系統來掃描物件，則還需要建立自訂規則來定義應掃描哪種類型的物件以及在哪個作業系統上進行掃描。

您無需建立規則將要掃描的物件傳送到預設的作業系統，Kaspersky Next XDR Expert會自動將物件傳送到那裡。

> 自訂沙盒規則僅適用於在沙盒網頁介面中建立的自訂虛擬機器。

若要新增自訂沙盒規則：

1. 在主選單中，轉至**監控→資源和服務→沙盒規則**。
2. 點擊**新增**。
   規則建立視窗隨即開啟。
3. 配置下列設定：
   - 若要在規則建立後立即啟用規則，請開啟**規則狀態**切換開關。
   - 選擇租用戶所有者。
   - 選擇要掃描檔案的虛擬機器。
     您只能從執行您選擇的自訂作業系統的虛擬機器中進行選擇。
   - 在**匹配標準**下，選擇您要使用**遮罩**、**檔案類別**或**兩者**作為符合條件。
   - 如果您選擇**遮罩**或**兩者**作為符合條件：
     - 請指定一個**遮罩**，用於指定要根據規則傳送到沙盒的檔案名稱。

您可以指定多個值，每個值佔一行。

你可以使用*和?萬用字元。不支援其他萬用字元。

- 指定一個可選的**遮罩排除**，用於排除即使檔案名稱與先前指定的遮罩相符的檔案，這些檔案也必須從掃描中排除。

  您可以指定多個值，每個值佔一行。

  你可以使用*和?萬用字元。不支援其他萬用字元。

> 如果在**遮罩排除**設定的**自訂**清單中僅選擇了標記為**自訂集**的虛擬機，則可以使用**Sandbox 伺服器**欄位。如果同時選擇了自訂虛擬機和預先設定的虛擬機，則會忽略**遮罩排除**欄位。

- 如果您選擇**檔案類別**或**兩者**作為符合條件：

  在**檔案類別**下拉清單中，選擇要依照規則傳送到沙盒的檔案類別。

- 若要限制傳送至沙盒的檔案大小，請按一下**新增檔案大小** ，然後指定檔案的**最小**和**最大**大小。這樣就可以設定多個大小範圍。

4. 點擊**儲存**按鈕。

此規則出現在自訂沙盒規則清單中。

掃描封存檔案的具體內容

封存檔案掃描方式如下：

1. Kaspersky Next XDR Expert解除壓縮該封存檔案。
2. 如果存檔中的一些檔案符合規則，Kaspersky Next XDR Expert會傳送它們進行掃描。

包含MSI副檔名的檔案與封存檔案處理方式類似。

設定將檔案從端點代理程式傳送到沙盒

端點代理程式可以透過多種方式將檔案傳送至沙盒進行掃描：

- 端點代理程式**自動**偵測物件並將其提交至沙盒進行掃描。
- 端點代理用戶**手動**提交檔案進行掃描。
- 端點代理程式傳送一個觸發了**IOA規則**的檔案。當裝置上觸發IOA規則，且此IOA規則包含將偵測到的物件傳送到沙盒的條件時，Kaspersky Next XDR Expert會自動啟動**獲取檔案**回應，並啟用**掃描檔案**選項。

> 自動向沙盒傳送檔案可能會顯著增加OSMP的負載。

若要設定向沙盒傳送待掃描檔案：

1. 請確保沙盒已與OSMP整合。
2. 在主功能表中，轉至**設定** → **租用戶**。
   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。
3. 按一下所需政策的名稱。
   這會開啟租用戶內容視窗。
4. 選取**設定**頁籤。
5. 在**正在掃描**區段，選擇**沙盒**頁籤。
6. 配置以下設定：
   - 若要啟用端點代理程式偵測到的檔案**自動**傳送功能：
     在**將檔案從裝置傳送至 Sandbox 進行分析**下，開啟**自動傳送檔案**切換開關。
     預設情況下已停用該選項。
   - 若要啟用使用者**手動**傳送檔案功能：
     在**將檔案從裝置傳送至 Sandbox 進行分析**下，開啟**手動傳送檔案**切換開關。
     預設情況下，啟用該功能。
   - 若要啟用觸發**IOA規則**時傳送檔案功能：
     在**自動將檔案傳送至 Sandbox**下，開啟**傳送檔案**切換開關。
     預設情況下已停用該選項。
7. 按一下**儲存並關閉**。

向沙盒傳送檔案隨即設定。根據掃描結果，Kaspersky Next XDR Expert可能會建立警示。

關於入侵指標、IOC檔案和IOC規則

Kaspersky Next XDR Expert可以掃描裝置以查找入侵指標。入侵指標（IOC）是數位物件，例如檔案雜湊值或IP位址，它們可能表示存在網路攻擊。您可以在卡巴斯基IT百科全書和Securelist上瞭解有關IOC的更多資訊。

IOC檔案

多個IOC可以組合成一個*IOC檔案*中的結構化描述。此類檔案有標準的*OpenIOC格式*。

下面是一個簡單IOC檔案的範例。

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="unique
ID in the UUID format" last-modified="date of the last modification of the rule in the YYYY-MM-DDThh:mm:ss format"
xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>Rule name</short_description>
```

```
  <authored_by>Rule name</authored_by>
  <authored_date>file creation date in the YYYY-MM-DDThh:mm:ss format</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="Unique ID in the UUID format">
      <IndicatorItem id="Unique ID in the UUID format" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">MD5 hash of the file</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```

您可以使用文字編輯器建立自己的IOC檔案，並將其儲存為.ioc副檔名。根據您的端點代理應用程式，您可以使用檔案中列出的OpenIOC術語：

Kaspersky Endpoint Security for Windows的OpenIOC術語

Kaspersky Endpoint Security for Linux的OpenIOC術語

Kaspersky Endpoint Security for Mac沒有OpenIOC術語清單，因為Kaspersky Next XDR Expert不會向Kaspersky Endpoint Security for Mac傳送IOC掃描工作。

IOC 規則

匯入IOC規則時，Kaspersky Next XDR Expert會從IOC檔案中擷取結構化描述，並根據該描述建立規則。

IOC規則可在OSMP主控台介面 →**監控**→**資源和服務**→**IOC 規則**的IOC規則清單中找到。

匯入IOC規則

Kaspersky Next XDR Expert從包含IOC規則的檔案中匯入IOC規則。一個檔案只能包含一條IOC規則，因此IOC規則清單也是建立這些規則的IOC檔案清單。

IOC規則清單可在OSMP主控台介面→**監控**→**資源和服務**→**IOC 規則**中找到。

若要匯入IOC規則：

1. 在主選單中，轉至**監控**→**資源和服務**→**IOC 規則**。
   IOC規則清單隨即開啟。
2. 點擊**匯入**。
3. 在開啟的**匯入 IOC 規則**窗格中，配置下列設定：
   - 在**租用戶**下拉清單中，選擇租用戶。
   - 在**重要性**下拉清單中，選擇規則的重要性。Kaspersky Next XDR Expert會將此值指派給因觸發IOC規則而建立的警示。

- 如果您希望Kaspersky Next XDR Expert定期掃描裝置以尋找規則中描述的入侵指標，請開啟**排定的掃描**切換開關（必須設定排程掃描）。

  您也可以稍後透過開啟IOC規則清單的**排定的掃描**直欄中的切換開關來啟用排程掃描。

4. 上傳包含 IOC 規則的檔案。

5. 點擊**匯入**。

匯入的規則出現在IOC規則清單中。

匯入YARA規則

Kaspersky Next XDR Expert使用YARA規則掃描傳送到OSMP的檔案並掃描裝置。

Kaspersky Next XDR Expert從包含YARA規則的容器中匯入YARA規則。一個檔案可以包含多個YARA規則。Kaspersky Next XDR Expert解析文件，擷取規則並將其新增至規則清單。無法保證能成功匯入包含超過 65,535 個規則的檔案。

YARA規則清單可在OSMP主控台介面→**監控**→**資源和服務**→**YARA 規則**中找到。

若要匯入YARA規則：

1. 在主選單中，轉至**監控→資源和服務→YARA 規則**。

   YARA規則清單隨即開啟。

2. 點擊**匯入**。

3. 在開啟的**匯入 YARA 規則**窗格中，配置下列設定：

   - 在**租用戶**下拉清單中，選擇租用戶。

   - 任何YARA規則的重要性預設為**高度**，您無法變更。Kaspersky Next XDR Expert會將此值指派給因觸發YARA規則而建立的警示。

   - 如果您希望Kaspersky Next XDR Expert使用所有匯入的規則來掃描傳送到OSMP的檔案，請開啟**檔案掃描中**切換開關。

     您也可以稍後透過開啟YARA規則清單的**檔案掃描中**直欄中的切換開關，將任何規則新增至檔案掃描規則集。

     > 此功能僅適用於根租用戶。

   - 指定密碼短語（可選）

4. 上傳包含YARA規則的檔案。

   檔案上傳後，Kaspersky Next XDR Expert會從檔案中擷取規則，並顯示有關擷取規則的資訊。

5. 點擊**匯入**。

導入的規則會出現在YARA規則清單中。

Kaspersky Next XDR Expert API

Kaspersky Next XDR Expert允許您使用REST API和OpenAPI。

使用REST API

透過使用 API，您可以從第三方解決方案存取 Kaspersky Next XDR Expert。REST API在HTTP上運行，由一組請求/回應方法組成。

REST API說明Swagger：XDR

REST API說明Swagger：KUMA

在Swagger頁面上，使用**選擇定義**下拉清單以在KUMA和XDR（OSMP）API集之間切換。

REST API請求必須傳送至以下位址：

https://<api_host>.<smp_domain>/xdr/api/v1/<request>

https://<api_host>.<smp_domain>/xdr/api/v3/kuma/<request>（用於KUMA特定API）

其中，<smp_domain>參數是在Kaspersky Next XDR Expert部署期間的組態檔中指定的服務網域。

範例：

https://api.example.com/xdr/api/v1/

https://api.example.com/xdr/api/v3/kuma/（用於KUMA特定API）

由於REST API請求必須經過授權，因此您需要建立一個權杖。

使用OpenAPI

OpenAPI可讓您使用指令碼自動化和自訂管理伺服器的管理。OpenAPI還可用於開發自訂用戶端應用程式，透過使用基於JSON的同步請求和回應，透過HTTP與Kaspersky Next XDR Expert進行互動。

OpenAPI請求必須傳送到以下地址：

https://api.<smp_domain>:13299

其中，<smp_domain>參數是在Kaspersky Next XDR Expert部署期間的組態檔中指定的服務網域。

範例：

https://api.example.com:13299

建立權杖

若要產生使用者API權杖：

1. 在主功能表中，轉至**設定 → API權杖**。
2. 按一下**新增令牌**按鈕。
3. 在**新增權杖**窗格中，設定權杖選項：
   a. 按一下**到期日**並使用行事曆指定到期日期。如果要停用權杖的自動到期，請選取**無到期日**核取方塊。
   最長到期日期間為365天。

   > 我們建議您為可以存取POST方法的權杖啟用自動到期。

   b. 選取您要允許存取之API 方法旁的核取方塊。
   除了 API 方法之外，您也可以選取建立權杖的用途：
   - POST:DynamicClientRegistration，用於動態註冊 OAuth 用戶端。
   - POST:KSCOpenAPI，用於使用 API 權杖進行OpenAPI驗證。
4. 點選**產生**按鈕。
5. 按一下**複製並關閉**。

> 之後您將無法複製權杖。

權杖已建立並複製到剪貼簿。以任何方便的方式儲存權杖。

授權API請求

每個API請求都必須包含基於權杖的授權。使用權杖發出API請求的使用者必須擁有執行此類請求的權限。

每個請求都必須包含以下標頭：

```
Authorization: Bearer <token>
```

可能發生的錯誤

HTTP代碼	描述	message 欄位值
400	無效標頭	無效授權標頭
403	權杖不存在或所有者使用者被停用	存取被拒絕

使用Open Single Management Platform

Open Single Management Platform（以下簡稱OSMP）是一個開放式技術平台，可讓您將卡巴斯基應用程式和協力廠商應用程式整合到單一安全系統中，並提供跨應用程式場景。Kaspersky Next XDR Expert基於OSMP運作。OSMP 網頁介面（以下簡稱 OSMP 控制台）用於管理 Kaspersky Next XDR Expert。

OSMP 控制台可讓您執行下列操作：

- 管理組織的安全系統狀態。
- 檢視您組織網路的安全資訊。
- 設定威脅的偵測、搜尋和回應。
- 管理為您網路中的裝置所建立的政策。
- 管理安裝在您網路裝置上的應用程式工作。
- 管理使用者和角色。
- 設定資料到Kaspersky Next XDR Expert的遷移。
- 將卡巴斯基應用程式安裝到您網路上的裝置並管理已安裝的應用程式。
- 可讓您輪詢網路來發現用戶端裝置，以及手動或自動將裝置分發到管理群組。
- 管理Kaspersky Next XDR Expert與其他應用程式的整合。

OSMP主控台是一個多國語言網頁介面。您可以在任意時刻變更介面語言，而不重新開啟應用程式。

OSMP主控台中的預設身分驗證方法是輸入使用者名稱、密碼以及用於雙因素驗證的附加一次性安全代碼。從Kaspersky Next XDR Expert 2.0開始，雙因素驗證會自動啟用，並且預設停用登入時設定雙因素驗證的選項。

您可以透過Kerberos協定設定網域身分驗證。網域身份驗證可讓您在OSMP主控台中啟用安全身份驗證，而無需在企業網路上重新輸入密碼（單一登入）。

設定管理伺服器

此區段說明設定過程與管理伺服器的內容。

配置管理伺服器連線位址

管理伺服器連連線址是用於以下用途的網路位址：

- 作為建立網路代理安裝套件時的預設位址

  安裝網路代理後，受管理裝置透過此位址連線到管理伺服器。

- 作為 KSN 代理伺服器位址
  受管理裝置透過此位址連線到 KSN 代理伺服器。

設定管理伺服器連線位址：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**一般**區段。
3. 在開啟的視窗中，在**管理伺服器連線位址** 欄位中，指定新的管理伺服器連線位址。
   連線位址的最大長度為 255 個字元。
   您可以將管理伺服器連線位址指定為 NetBIOS 名稱、FQDN 或管理伺服器的 IP 位址。
4. 點擊**儲存**按鈕。

指定的位址用作管理伺服器位址和 KSN 代理伺服器位址。

設定 OSMP 主控台與管理伺服器的連線

您可以透過管理伺服器屬性或使用管理伺服器政策設定來配置OSMP主控台與管理伺服器的連線。

要透過管理伺服器內容設定連線連接埠：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤，選取**連線連接埠**區段。
3. 如有必要，請指定**網頁主控台的 SSL 連接埠**設定或指定其他管理伺服器連線連接埠。

所選伺服器的主要連線設定已指定。

若要透過管理伺服器政策設定設定連線連接埠：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 點擊管理伺服器政策的名稱，然後前往**應用程式設定**標籤。
3. 如有必要，請指定**網頁主控台的 SSL 連接埠**設定或指定其他管理伺服器連線連接埠。

> 如果您停用**開啟網頁主控台的連接埠**選項，且此政策設定將套用至裝置，您將無法使用OSMP主控台連線到管理伺服器。在這種情況下，連線將被終止。如果您有一個未套用此策略的管理伺服器，您可以透過OSMP主控台重新連線至此管理伺服器。

所選伺服器的主要連線設定已指定。

設定網際網路存取設定

Kaspersky Next XDR Exper元件的正常運作需要網際網路連線，並且可用於卡巴斯基和協力廠商的特定整合。例如，您必須設定管理伺服器的網際網路存取，才能使用卡巴斯基安全網路，以及下載 Kaspersky Next XDR Expert 和受管理的卡巴斯基應用程式所需的病毒資料庫更新。

某些卡巴斯基應用程式的整合設定包含啟用或停用代理伺服器使用的選項。例如，當您設定與Kaspersky Threat Intelligence Portal的整合時，可以使用這樣的選項。

若要指定網際網路存取設定：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選取**設定網際網路存取**區段。

3. 如果您要在連線到網際網路時使用代理伺服器，請啟用**使用代理伺服器**選項。如果啟用此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

   - **位址**

     Kaspersky Next XDR Expert 連線至網際網路時所使用的代理伺服器位址。

   - **連接埠號**

     Kaspersky Next XDR Expert 代理連線將透過其建立的連接埠號碼。

   - **略過本機位址的代理伺服器**

     將不會使用代理伺服器連線本機網路的裝置。

   - **代理伺服器身分驗證**

     如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

     如果選取**使用代理伺服器**核取方塊，則可使用該輸入欄位。

   - **使用者名稱**

     用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

   - **密碼**

     其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

     若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

Open Single Management Platform工作憑證

本章節包含有關Open Single Management Platform憑證的資訊，並描述如何簽發和替換OSMP主控台的憑證，以及如何在伺服器與OSMP主控台交互時更新管理伺服器憑證。

關於Open Single Management Platform憑證

Open Single Management Platform使用以下類型的憑證來啟用應用程式元件之間的安全互動：

- 管理伺服器憑證
- OSMP主控台伺服器憑證
- OSMP主控台憑證

預設情況下，Open Single Management Platform 使用自我簽署憑證（即由 Open Single Management Platform 自行發行的憑證）。如有需要，您可以依據組織的安全標準，將自我簽署憑證取代為使用者憑證。在管理伺服器驗證自訂憑證是否滿足所有適用要求之後，該憑證將承擔與自我簽署憑證相同的功能範圍。唯一的區別是自訂憑證在到期後不會自動重新發行。您可以透過klsetsrvcert公用程式或透過OSMP主控台中的「管理伺服器屬性」區段將憑證替換為自訂憑證，具體視憑證類型而定。使用klsetsrvcert公用程式時，您需要使用以下值之一指定憑證類型：

- C—適用於連接埠 13000 和 13291 的常見憑證。
- CR—適用於連接埠 13000 和 13291 的預留憑證。

任何管理伺服器憑證的最長有效期不得超過 397 天。

管理伺服器憑證

管理伺服器憑證需要用於以下目的：

- 連線到OSMP主控台時對管理伺服器進行驗證
- 受管理裝置上管理伺服器和網路代理之間的安全交互
- 主管理伺服器連線到從屬管理伺服器時的身分驗證。

管理伺服器憑證是在安裝管理伺服器元件時自動產生的，並儲存在 /var/opt/kaspersky/klnagent_srv/1093/cert/ 資料夾中。您在建立回應檔案以安裝OSMP主控台時指定管理伺服器憑證。該憑證稱為通用憑證 ("C")。

管理伺服器憑證 397 天有效。Open Single Management Platform 會在通用憑證到期前 90 天自動建立通用預留 ("CR") 憑證。公用預留憑證隨後會用來無縫替換管理伺服器憑證。當公用憑證即將到期時，公用預留憑證會用來維持與安裝在受管理裝置上網路代理實例的連線。為此，通用預留憑證會在舊的通用憑證到期前 24 小時自動變為新的通用憑證。

> 任何管理伺服器憑證的最長有效期不得超過 397 天。

如有必要，您可以為管理伺服器分配協力廠商憑證。例如，為了更好的整合您企業的現有 PKI 或為了憑證欄位的自訂設定，這可能是必要的。當取代憑證時，所有先前透過SSL連線到管理伺服器的網路代理將遺失它們的連線，並將返回「*管理伺服器身分驗證錯誤*」。要消除該錯誤，您將必須在憑證取代後還原連線。

如果遺失了管理伺服器憑證，要想還原憑證，就只能重新安裝管理伺服器元件，然後還原資料。

您也可以與其他管理伺服器設定獨立的備份管理伺服器憑證，以在將管理伺服器從一部裝置移至另一部裝置時不會遺失資料。

行動憑證

在行動裝置上對管理伺服器進行驗證需要行動憑證（「M」）。您可以在管理伺服器內容中指定行動憑證。

此外還有行動預留（「MR」）憑證：該憑證會用來無縫替換行動憑證。Open Single Management Platform會在通用憑證到期前90天自動產生此憑證。當行動憑證即將到期時，將使用行動備用憑證來維護與安裝在受管理行動裝置上的網路代理實例的連線。為此，行動備用憑證會在舊的行動憑證到期前 24 小時自動變為新的行動憑證。

如果連線情境要求在行動裝置上使用用戶端憑證（涉及雙向 SSL 驗證的連線），則您可以透過用於自動產生的使用者憑證（「MCA」）的憑證機構來產生那些憑證。此外，在管理伺服器內容中，您可以指定由其他憑證機構發行的自訂用戶端憑證，而與組織的網域公用金鑰基礎架構 (PKI) 整合，可讓您透過網域憑證機構發佈用戶端憑證。

網頁伺服器憑證

Web 伺服器是卡巴斯基安全管理中心管理伺服器的一個元件，使用特殊類型的憑證。發布網路代理安裝套件（隨後將其下載到受管理裝置）需要此憑證。基於此用途，網頁伺服器可以使用各種憑證。

網頁伺服器按優先級順序使用以下憑證之一：

1. 您透過OSMP主控台手動指定的自訂網頁伺服器憑證
2. 通用管理伺服器憑證 ("C")

OSMP主控台憑證

OSMP主控台伺服器有自己的憑證。當您開啟網站時，瀏覽器會驗證您的連線是否可信。網頁主控台憑證允許您對網頁主控台進行身分驗證，並被用於加密瀏覽器和網頁主控台之間的流量。

當您開啟網頁主控台時，瀏覽器會通知您與OSMP主控台的連線不是私有，並且OSMP主控台憑證無效。出現此警告是因為OSMP主控台憑證為自簽名並由Open Single Management Platform自動產生。要刪除此警告，您可以執行以下操作之一：

- 用自訂憑證替代網頁主控台憑證（建議選項）。建立一個在您的基礎架構中受信任且滿足自訂憑證的要求的憑證。
- 將網頁主控台憑證新增到受信任的瀏覽器憑證清單中。我們建議您僅在無法建立自訂憑證時使用此選項。

Open Single Management Platform中使用的自訂憑證的要求

下表顯示了為Open Single Management Platform的不同元件指定的自訂憑證的要求。

憑證類型	要求	註解
一般憑證，一般備用憑證（「C」、「CR」）	最小金鑰長度：2048。 基本限制： • 路徑長度限制：無 金鑰使用情況： • 電子簽名 • 憑證籤名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證、用戶端身分驗證。 憑證必須包含有效的使用者備用名稱（SAN），其中包含管理伺服器環回位址： • IPv4位址：127.0.0.1 • IPv6位址：0:0:0:0:0:0:0:1	延伸金鑰使用參數為選填。 路徑長度限制值可以有別於「無」，但不能小於「1」。
移動憑證、移動備用憑證（「M」、「MR」）	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：無 金鑰使用情況： • 電子簽名 • 憑證籤名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證。	延伸金鑰使用參數為選填。 如果一般憑證的「路徑長度限制」值不小於「1」，則「路徑長度限制值」可能與「無」不同。
自動產生之使用者憑證（「MCA」）的憑證 CA	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：無 金鑰使用情況： • 電子簽名 • 憑證籤名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證、用戶端身分驗證。	延伸金鑰使用參數為選填。 如果一般憑證的「路徑長度限制」值不小於「1」，則「路徑長度限制值」可能與「無」不同。
網頁伺服器憑證	延伸金鑰使用：伺服器身分驗證。 從中指定憑證的 PKCS # 12/PEM 容器會包括整個公開金鑰鏈。 出現憑證的主體別名 (SAN)；也就是說，`subjectAltName` 欄位值有效。 該憑證符合瀏覽器對伺服器憑證施加的有效要求，以及 CA/瀏覽器論壇 的目前基準要求。	—
OSMP主控台憑證	從中指定憑證的 PEM 容器會包括整個公開金鑰鏈。 出現憑證的主體別名 (SAN)；也就是說，`subjectAltName` 欄位值有效。 該憑證符合瀏覽器對伺服器憑證的有效要求，以及 CA/瀏覽器論壇 的目前基準要求。	OSMP 主控台不支援加密憑證。
Kaspersky Next XDR Expert公共服務的中級憑證	卡巴斯基的PEM容器，其中包含完整的憑證鏈（或單一憑證）以及一個未加密的私鑰。 中級憑證必須由貴組織的私鑰基礎設施（PKI）核發。自訂中級憑證的有效期限必須至少為399天。	—

為OSMP主控台重新簽發憑證

大多數瀏覽器都對憑證的有效期施加了限制。為了符合此限制，OSMP主控台憑證的有效期會限制為397天。您可以透過手動發佈新的自主簽發憑證來取代從憑證機構 (CA) 收到的現有憑證。或者，您可以重新簽發過期的OSMP主控台憑證。

不支援自動為OSMP主控台重新簽法憑證。您必須手動重新發佈過期的憑證。

當您開啟OSMP主控台時，瀏覽器會通知您與OSMP主控台的連線不是私有，並且OSMP主控台憑證無效。出現此警告是因為OSMP主控台憑證為自簽名並由Open Single Management Platform自動產生。要刪除或防止此警告，您可以執行以下操作之一：

- 重新發行憑證時指定自訂憑證（建議選項）。建立一個在您的基礎架構中受信任且滿足自訂憑證的要求的憑證。
- 重新簽發憑證後，將OSMP主控台憑證新增到受信任的瀏覽器憑證清單中。我們建議您僅在無法建立自訂憑證時使用此選項。

若要重新簽發過期的OSMP主控台憑證：

透過執行下列操作之一重新安裝OSMP主控台：

- 如果要使用相同的OSMP主控台安裝文件，請刪除OSMP主控台，然後安裝相同的OSMP主控台版本。
- 如果想要使用升級版的安裝檔案，請執行升級命令。

重新簽發OSMP主控台憑證的有效期為397天。

取代OSMP主控台的憑證

預設下，當您安裝OSMP主控台伺服器（也叫OSMP主控台）時，應用程式的瀏覽器憑證被自動產生。您可以使用自訂憑證取代自動產生的憑證。

要用自訂憑證OSMP主控台的憑證：

1. 開啟在安裝程式OSMP主控台時所建立的回應檔案。
   如果需要的話，您可以建立新的回應檔案。
2. 在檔案中，指定以下路徑：
   - 使用 `certPath` 參數存取 OSMP 主控台自訂憑證檔案
   - 使用 `keyPath` 參數存取與 OSMP 主控台自訂憑證關聯的私密金鑰。

   您必須指定這兩條路徑。否則，Web 瀏覽器會不斷通知您您的連線不是私密的。

3. 透過指定新的回應檔案重新安裝OSMP主控台。執行以下操作之一：

   - 如果要使用相同的OSMP主控台安裝文件，請刪除OSMP主控台，然後安裝相同的OSMP主控台版本。
   - 如果想要使用升級版的安裝檔案，請執行升級命令。

OSMP主控台使用指定的憑證。

將 PFX 憑證轉換為 PEM 格式

要在OSMP主控台中使用PFX憑證，您必須先使用任何便捷的 OpenSSL跨平台公用程式將其轉換為PEM格式。

要在 Linux 作業系統中將 PFX 憑證轉換為 PEM 格式：

1. 在 OpenSSL 跨平台公用程式中，執行以下命令：

   ```
   openssl pkcs12 -in <檔案名稱.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <檔案名稱.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 確保在儲存 .pfx 檔案的目錄中產生憑證檔案和私密金鑰。

3. OSMP主控台不支援受密碼保護的憑證。因此，在基於 OpenSSL 的跨平台公用程式中執行以下命令以從 .pem 文件中刪除複雜密碼：

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

   > 不要對輸入和輸出 .pem 檔案使用相同的名稱。

   結果，新的 .pem 檔案未加密。您無需輸入複雜密碼即可使用它。

.crt和.pem格式的檔案已準備就緒，您可以在OSMP主控台安裝程式中指定它們。

情境：指定自訂管理伺服器憑證

例如，您可以分配自訂管理伺服器憑證以便更好地與企業的現有公鑰基礎結構 (PKI) 進行整合，或自訂配置憑證欄位。在安裝管理伺服器後立即更換憑證是有用的。

> 任何管理伺服器憑證的最長有效期不得超過 397 天。

先決條件

新憑證必須以 PKCS#12 格式（例如，透過組織的 PKI）建立，並且必須由受信任的憑證頒發機構 (CA) 頒發。此外，新憑證必須包含整個信任鏈和私密金鑰，該私密金鑰必須儲存在副檔名為 pfx 或 p12 的檔案中。對於新憑證，必須滿足以下列出的要求。

憑證類型：一般憑證，一般備用憑證（「C」、「CR」）

要求：

- 最小金鑰長度：2048。
- 基本限制：
  - CA：真
  - 路徑長度限制：無
    路徑長度限制值可以有別於「無」，但不能小於「1」。
- 金鑰使用情況：
  - 電子簽名
  - 憑證簽名
  - 金鑰加密
  - CRL 簽署
- 延伸金鑰使用 (EKU)：伺服器身分驗證和用戶端身分驗證。EKU 可選，但如果您的憑證包含它，則必須在 EKU 中指定伺服器和用戶端身分驗證資料。
- 憑證必須包含有效的主題備用名稱（SAN）。
- `subjectAltName` 欄位必須包含管理伺服器環回位址：
  - IPv4位址：127.0.0.1
  - IPv6位址：0:0:0:0:0:0:0:1

公共 CA 頒發的憑證沒有憑證簽名權限。要使用此類憑證，請確保您在網路中的發佈點或連線閘道上安裝了網路代理版本 13 或更高版本。否則，您將無法在沒有簽名權限的情況下使用憑證。

階段

指定管理伺服器憑證分階段進行：

1. **替換管理伺服器憑證**

   為此使用指令行 klsetsrvcert utility。

2. **指定新憑證和還原網路代理與管理伺服器的連線**

   當憑證被取代時，所有先前透過 SSL 連線到管理伺服器的網路代理會遺失它們的連線，並返回「管理伺服器身分驗證錯誤」。要指定新憑證和還原連線，使用 klmover 公用程式。

結果

當您結束情境時，管理伺服器憑證被取代，且伺服器得到受管理裝置上的網路代理的身分驗證。

使用 klsetsrvcert 公用程式替換管理伺服器憑證

若要替換管理伺服器憑證：

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke ksc --action klsetsrvcert \
  --param ksc_server_certificate="<新憑證路徑>" \
  --param ksc_server_cert_pass="<密碼>"
```

其中：

- < 新憑證路徑 > 為包含 PKCS #12 格式憑證和私密金鑰之容器的路徑（副檔名為 .P12 或 .PFX 的檔案）。
- < 密碼 > 是用來保護 PKCS #12 容器的密碼。憑證和私密金鑰儲存在容器中，因此需要密碼才能使用容器解密檔案。

  若密碼包含雙引號，請使用反斜線對雙引號進行跳脫 (\")。

預設情況下，未指定憑證驗證參數，使用沒有簽署權限的自訂憑證。您可以替換連接埠13000的公用憑證。

您無需下載 klsetsrvcert 公用程式。它包含在Kubernetes叢集中，不能直接運作。您只能透過使用管理員主機上的KDT來執行klsetsrvcert公用程式。

使用 klmover 公用程式將網路代理連線到管理伺服器

使用命令列 klsetsrvcert 公用程式替換管理伺服器憑證後，您需要在網路代理和管理伺服器之間建立 SSL 連線，因為連線已斷開。

要指定新管理伺服器憑證並還原連線：

在命令列下，執行以下公用程式：

```
klmover [-address <伺服器位址>] [-pn <埠號>] [-ps <SSL 埠號>] [-nossl] [-cert <憑證檔案路徑>]
```

當網路代理安裝在用戶端裝置上時，此公用程式會自動複製到網路代理安裝資料夾。

下表列出了 klmover 公用程式參數的說明。

設定	參數值
`-address <伺服器位址>`	用於連線的管理伺服器的位址。 您可以指定 IP 位址或 DNS 名稱。
`-pn <埠號>`	用來建立與管理伺服器非加密連線的埠號。 預設埠號為 14000。
`-ps <SSL 埠號>`	使用 SSL 與管理伺服器建立加密連線時使用的 SSL 埠號。 預設埠號為 13000。 連接埠 13000 用於根管理伺服器；此埠號無法變更。
`-nossl`	使用非加密方式連線管理伺服器。 如果未使用該鍵值，網路代理將透過使用加密的 SSL 協定連線至管理伺服器。
`-cert <憑證檔案路徑>`	存取管理伺服器時使用指定的憑證檔案作為身分驗證。

管理伺服器階層

一些用戶端公司，例如MSP，可能執行多台管理伺服器。可能不方便管理幾個不同的管理伺服器，因此可以應用階層結構。每個管理伺服器可以在階層結構的不同巢狀層級上擁有多個次要管理伺服器。根管理伺服器只能作為主要伺服器運行。

在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。

兩個管理伺服器的"主要/從屬"組態提供了以下選項：

- 一個從屬管理伺服器從主管理伺服器繼承政策、工作、使用者角色和安裝套件，從而防止重複設定。
- 主管理伺服器上的裝置分類可以包含從屬管理伺服器的裝置。
- 主管理伺服器的報告和事件分類可以包含從屬管理伺服器的資料（包括詳細資訊）。
- 主管理伺服器可作為從屬管理伺服器的更新來源。

主管理伺服器僅會從上列選項範圍內的非虛擬從屬管理伺服器收到資料。此限制之所以不適用於虛擬管理伺服器，是因為虛擬管理伺服器與其主管理伺服器共用一個資料庫。

建立管理伺服器階層：新增次要管理伺服器

在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。根管理伺服器只能作為主要伺服器運行。

您可以新增管理伺服器作為次要管理伺服器，進而建立"主要 / 次要"層級。

要新增一個可透過OSMP主控台連線的從屬管理伺服器：

1. 確保未來主管理伺服器的連接埠 13000 可用於從從屬管理伺服器接收連線。
2. 前往未來主管理伺服器的屬性：
   a. 在主選單中，選擇任意部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。
   b. 在開啟的導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後點擊設定圖示 (⚙)。
   或者，您可以按一下管理伺服器名稱，然後在主選單中顯示該名稱後，在主選單中按一下它以開啟伺服器屬性視窗。
3. 在開啟的屬性視窗中，點擊**管理伺服器**頁籤。
4. 選取您要向其新增管理伺服器的管理群組名稱旁邊的核取方塊。
5. 在功能表行中，點擊**連線從屬管理伺服器**。
   新增從屬管理伺服器精靈啟動。使用 **NEXT** 按鈕進行精靈。
6. 填充以下欄位：
   - **從屬管理伺服器顯示名稱**

     從屬管理伺服器將顯示在層級的名稱。如果需要，您可以輸入 IP 位址作為名稱，也可以使用例如「群組 1 的從屬伺服器」之類的名稱。
   - **從屬管理伺服器位址（可選）**

     指定從屬管理伺服器的 IP 位址或網域名稱。
     如果啟用了**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**選項，則需要此參數。
   - **管理伺服器 SSL 連接埠號**

     指定主管理伺服器上的 SSL 埠號。預設埠號為 13000。
     連接埠 13000 用於根管理伺服器；此連接埠號碼無法變更。
   - **管理伺服器 API 連接埠**

     網頁主控台用於透過 OpenAPI 接收來自從屬管理伺服器之連線的連接埠號碼。預設埠號為 13299。

     在構建層級結構時，網頁主控台會連線至未來的從屬伺服器、請求憑據、擷取公開憑證，並執行初始設定。

     管理伺服器的層級結構構建完成後，將不再使用連接埠 13299。管理伺服器將透過連接埠 13000 進行互動。
   - **將主管理伺服器連線到 DMZ 中的從屬管理伺服器**

     如果從屬管理伺服器位於非武裝區 (DMZ)，選取該選項。
     如果選擇此選項，主管理伺服器將啟動與從屬管理伺服器的連線。否則，從屬管理伺服器將啟動與主管理伺服器的連線。
7. 指定未來從屬伺服器的憑證。
   精靈已完成。

8. 傳送未來主要管理伺服器的憑證檔案到未來次要管理伺服器所在辦公室的系統管理員。（您可以，例如，寫入檔案到外部裝置，例如快閃記憶體磁碟機，或者透過郵件傳送它）

   憑證檔案位於未來的主管理伺服器上，位於 /var/opt/kaspersky/klnagent_srv/1093/cert/。

9. 提示未來從屬管理伺服器的責任系統管理員做以下事情：

   a. 按一下管理伺服器名稱。

   b. 在開啟的內容頁面中，前往**一般**頁籤的**管理伺服器階層**區段。

   c. 選擇**此管理伺服器是階層中的從屬伺服器**選項。

   > 根管理伺服器只能作為主要伺服器運行。

   d. 在**主管理伺服器位址**欄位，輸入未來主要管理伺服器的網路名稱。

   e. 透過按一下**瀏覽**選取先前儲存的帶有未來主管理伺服器憑證的檔案。

   f. 如有需要，請選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**核取方塊。

   g. 若未來主管理伺服器的連線會透過代理伺服器執行，請選取**使用代理伺服器**核取方塊並指定連線設定。

   h. 點擊**儲存**按鈕。

「主要/從屬」層級被建立。主管理伺服器開始使用連接埠 13000 從從屬管理伺服器接收連線。主管理伺服器的工作和政策被接收和套用。從屬管理伺服器顯示在主管理伺服器上，在新增其的管理群組中。

檢視次要管理伺服器清單

要檢視從屬（包括虛擬）管理伺服器清單：

1. 在主功能表中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外）。

2. 在頁面頂部，點擊**顯示階層**按鈕。

在開啟的導覽窗格中，從屬（包括虛擬）管理伺服器的清單將顯示。您可透過點及其名稱前往這些管理伺服器的任何一個。

如果您從**IP 範圍**和**已刪除物件**部分開啟了導覽窗格，則無法前往虛擬管理伺服器。
管理群組也會顯示。如果您從下列部分開啟導覽窗格，則可以管理這些群組：**資產（裝置）**、**政策**、**工作**和**發佈點**。否則，這些群組將成為灰色。

如果您已連接到OSMP主控台中的主要管理伺服器，但無法連接由從屬管理伺服器管理的虛擬管理伺服器，您可以使用以下其中一種方法：

- **修改現有的OSMP主控台安裝，將從屬伺服器新增到受信任的管理伺服器列表中**。然後，您將能夠在OSMP主控台中連線到虛擬管理伺服器。

  1. 在安裝了OSMP主控台的裝置上，以具有管理員權限的帳戶運行對應於您裝置上安裝的Linux發行版的OSMP主控台安裝檔案。

     安裝精靈將啟動。使用**下一步**按鈕進行精靈。

  2. 選取**升級**選項。

  3. 在**修改類型**步驟，選擇**編輯連線設定**選項。

  4. 在**受信任的管理伺服器**步驟，新增所需的從屬管理伺服器。

  5. 在最後的步驟，按一下**修改**以套用新設定。

  6. 在應用程式重新設定成功完成後，按一下**完成**按鈕。

- 使用OSMP主控台直接連線到建立虛擬伺服器的從屬管理伺服器。然後，您將能夠在OSMP主控台中切換到虛擬管理伺服器。

管理虛擬管理伺服器

本章節說明用來管理虛擬管理伺服器的以下操作：

- 建立虛擬管理伺服器
- 啓用和停用虛擬管理伺服器
- 為虛擬管理伺服器指派管理員
- 變更用戶端裝置的管理伺服器
- 刪除虛擬管理伺服器

建立虛擬管理伺服器

您可以建立虛擬管理伺服器並新增它們到管理群組。

當您建立虛擬管理伺服器時，它會繼承主管理伺服器的使用者清單和所有使用者權限。如果使用者有權存取主伺服器，則該使用者也有權存取虛擬伺服器。建立後，您可以分別設定對伺服器的存取權限。

要建立和新增虛擬管理伺服器：

1. 在主選單中，按一下管理伺服器名稱。

2. 在開啟的頁面中，前往**管理伺服器**頁籤。

3. 選取您要新增虛擬管理伺服器到的管理群組。
   虛擬管理伺服器將管理所選群組（包括子群組）中的裝置。

4. 在功能表行中，點擊**新虛擬管理伺服器**。

5. 在開啟的頁面上，定義新虛擬管理伺服器的內容：

   - **虛擬管理伺服器名稱**。

   - **管理伺服器連線位址**

     您可指定管理伺服器的名稱或 IP 位址。

6. 從使用者清單中，選擇虛擬管理伺服器管理員。如果您想，您可以編輯現有帳戶之一，然後分配其管理員角色，或建立一個新使用者帳戶。

   如有必要，您可以使用 kladduser 公用程式建立一個將充當虛擬管理伺服器的新帳戶。為此，請使用以下指令：

   `kladduser -n <使用者名稱> -p <密碼> -vs <虛擬伺服器名稱>`

   其中 虛擬伺服器名稱 是虛擬管理伺服器的名稱。

7. 點擊**儲存**按鈕。

新虛擬管理伺服器會建立並新增至管理群組，同時顯示在**管理伺服器**頁籤上。

如果您已連接到OSMP主控台中的主要管理伺服器，但無法連接由從屬管理伺服器管理的虛擬管理伺服器，您可以使用以下其中一種方法：

- **修改現有的OSMP主控台安裝，將從屬伺服器新增到受信任的管理伺服器列表中**。然後，您將能夠在OSMP主控台中連線到虛擬管理伺服器。

  1. 在安裝了OSMP主控台的裝置上，以具有管理員權限的帳戶運行對應於您裝置上安裝的Linux發行版的OSMP主控台安裝檔案。

     安裝精靈將啟動。使用**下一步**按鈕進行精靈。

  2. 選取**升級**選項。

  3. 在**修改類型**步驟，選擇**編輯連線設定**選項。

  4. 在**受信任的管理伺服器**步驟，新增所需的從屬管理伺服器。

  5. 在最後的步驟，按一下**修改**以套用新設定。

  6. 在應用程式重新設定成功完成後，按一下**完成**按鈕。

- 使用OSMP主控台直接連線到建立虛擬伺服器的從屬管理伺服器。然後，您將能夠在OSMP主控台中切換到虛擬管理伺服器。

啓用和停用虛擬管理伺服器

當您建立新的虛擬管理伺服器時，預設情況下會啟用它。您可以隨時停用或再次啟用它。停用或啟用虛擬管理伺服器等同於關閉或開啓實體管理伺服器。

要啓用或停用虛擬管理伺服器：

1. 在主選單中，按一下管理伺服器名稱。
2. 在開啟的頁面中，前往**管理伺服器**頁籤。
3. 選擇要啟用或停用的虛擬管理伺服器。
4. 在功能表行上，點擊**啟用/停用虛擬管理伺服器**按鈕。

虛擬管理伺服器狀態被變更為啟用或停用，具體取決於其先前的狀態。更新後的狀態顯示在管理伺服器名稱旁邊。

為虛擬管理伺服器指派管理員

當您的組織使用虛擬管理伺服器時，您可能希望為每個虛擬管理伺服器指派一個專用管理員。例如，當您建立虛擬管理伺服器來管理組織的獨立辦公室或部門時，或者如果您是 MSP 供應商並透過虛擬管理伺服器管理您的租用戶，這可能很有用。

當您建立虛擬管理伺服器時，它會繼承主管理伺服器的使用者清單和所有使用者權限。如果使用者有權存取主伺服器，則該使用者也有權存取虛擬伺服器。建立後，您可以分別設定對伺服器的存取權限。如果您只想為虛擬管理伺服器指派管理員，請確保該管理員沒有主管理伺服器的存取權限。

您可以授予管理員對虛擬管理伺服器的存取權限，來為虛擬管理伺服器指派管理員。您可以透過以下方式之一授予所需的存取權限：

- 手動設定管理員的存取權限
- 為管理員指派一個或多個使用者角色

若要登入OSMP主控台，虛擬管理伺服器的管理員需指定虛擬管理伺服器名稱、使用者名稱和密碼。OSMP主控台會對管理員進行身分驗證，然後開啟管理員具有存取權限的虛擬管理伺服器。管理員不能在管理伺服器之間切換。

先決條件

在開始之前，請確保滿足以下條件：

- 已建立虛擬管理伺服器。
- 在主管理伺服器上，您已為虛擬管理伺服器指派的管理員建立一個帳戶。
- 您在**一般功能**：**修改物件 ACL**功能區域中有**一般功能** 權限。

手動設定存取權限

為虛擬管理伺服器指派管理員：

1. 切換到所需的虛擬管理伺服器：

   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，點擊所需虛擬管理伺服器的名稱。

   > 您無法從**IP 範圍**和**已刪除物件**部分切換到虛擬管理伺服器。

   在主選單中，管理伺服器將變更為您選擇的伺服器。

2. 在主選單中點選管理伺服器的名稱，移至其屬性。
   或者，在導覽窗格中，將滑鼠遊標停留在所需虛擬管理伺服器的名稱上，然後按一下設定圖示 (⚙)。
   管理伺服器內容視窗將開啟。

3. 在**存取權限**頁簽上，點擊**新增**按鈕。
   主管理伺服器和當前虛擬管理伺服器的統一使用者清單開啟。

4. 從使用者清單中，選擇要指派給虛擬管理伺服器的管理員帳戶，然後按一下**確定**按鈕。
   應用程式將選取的使用者新增到**存取權限**頁籤上的使用者清單。

5. 選取新增帳戶旁邊的核取方塊，然後點擊**存取權限**按鈕。

6. 設定管理員對虛擬管理伺服器的權限。
   要成功進行身分驗證，管理員至少必須具有以下權限：

   - **讀取 → 一般功能**功能區域中的**基本功能**權限。
   - **讀取 → 一般功能**功能區域中的**虛擬管理伺服器**權限。

   應用程式將修改後的使用者權限儲存到管理員帳戶中。

若要為多個虛擬管理伺服器指派管理員：

1. 在主選單中，按一下主管理伺服器名稱。

2. 在開啟的頁面上，轉至**存取權限**頁籤，然後按一下**指派**。
   在開啟的**新增使用者或群組**視窗中，選取要指派為管理員的使用者旁的核取方塊。

3. 您可以切換到**群組**頁籤來選擇使用者群組。

4. 按一下**下一步**。

5. 選取要為其指派管理員的伺服器，然後按一下**下一步**。

6. 如有必要，請選取要為使用者設定的管理員角色。

   如果要為使用者設定目前管理伺服器的自訂角色，請前往所需管理伺服器的內容，按一下**設定角色**，然後選取自訂角色。

7. 按一下**完成**以套用變更。

具有所選角色的管理員現在已指派給多個虛擬管理伺服器。

若要撤銷管理員存取權限：

1. 切換到所需的管理伺服器。
2. 在主選單中，按一下管理伺服器名稱。
3. 在開啟的頁面上，轉至**存取權限**頁籤。
4. 選取要撤銷其存取權限的使用者旁的核取方塊。
5. 按一下**撤銷**並確認您的操作。

所選使用者的存取權限被撤銷。

指派使用者角色來設定存取權限

或者，您可以透過使用者角色，將存取權限授予虛擬管理伺服器管理員。例如，如果您想在同一個虛擬管理伺服器上指派多個管理員，這可能很有用。如果是這種情況，您可以為管理員帳戶指派相同的一個或多個使用者角色，而不是為多個管理員設定相同的使用者權限。

要指派使用者角色來為虛擬管理伺服器指派管理員：

1. 在主管理伺服器上，建立一個新的使用者角色，然後指定管理員必須在虛擬管理伺服器上擁有的所有必需存取權限。您可以建立多個角色，例如，如果您想要單獨存取不同的功能區域。
2. 切換到所需的虛擬管理伺服器：

   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，點擊所需虛擬管理伺服器的名稱。

   > 您無法從**IP 範圍**和**已刪除物件**部分切換到虛擬管理伺服器。

   在主選單中，管理伺服器將變更為您選擇的伺服器。

3. 將新角色或多個角色指派給管理員帳戶。

應用程式將角色指派給管理員帳戶。

在物件層級設定存取權限

除了指派功能區域層級的存取權限，您還可以在虛擬管理伺服器上設定對特定物件的存取，例如，特定的管理群組或工作。為此，請切換到虛擬管理伺服器，然後在物件的屬性中設定存取權限。

變更用戶端裝置的管理伺服器

您可以使用"*變更管理伺服器*"工作來變更用戶端裝置連線的管理伺服器。工作完成後，所選用戶端裝置將被置於您指定的管理伺服器的管理之下。

您無法對透過連線閘道連線到管理伺服器的用戶端裝置使用*變更管理伺服器*工作。對於這樣的裝置，您必須重新設定網路代理或重新安裝網路代理並指定連線閘道。

要變更用戶端裝置連線的管理伺服器：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在精靈的**新工作設定**步驟中，指定以下設定：

   a. 在**應用程式**下拉清單中，選擇**Open Single Management Platform**。

   b. 在**工作類型**欄位中，選擇**變更管理伺服器**。

   c. 在**工作名稱**視窗中，指定您正在建立的工作的名稱。

   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

   d. 選取要對其分配工作的裝置：

   - **指派工作給管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

     例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

     如果工作被指派給管理群組，則工作內容視窗中不會顯示**安全**頁籤，因為群組工作受其所套用的群組的安全設定的約束。

   - **手動指定裝置位址或是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。

     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **指派工作給裝置分類**

     該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

     例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

4. 在精靈的**工作範圍**步驟，指定管理群組、具有特定位址的裝置或裝置選擇。

5. 在精靈的該步驟，確認您同意變更用戶端裝置的管理伺服器的條款。

6. 在精靈的該步驟，選擇您想要用來管理所選裝置的管理伺服器：

- **變更到另一個主管理伺服器**

  若要將用戶端裝置移至另一台主管理伺服器，請指定下列管理伺服器連線設定：

  1. 在**管理伺服器位址**欄位中，指定新的主管理伺服器的位址。

  2. 在**連接埠號**欄位中，指定連線到管理伺服器的連接埠號碼。
     預設埠號為 14000。

  3. 在**SSL 連接埠**欄位中，指定主管理伺服器上的 SSL 連接埠號。
     預設埠號為 13000。

  4. 如有必要，請啟用**使用代理伺服器**選項。
     如果停用此選項，則使用直接連線將裝置連線到管理伺服器。
     如果啟用此選項，請指定代理伺服器參數：

     - **代理伺服器位址**

     - **代理伺服器連接埠**

     如果您的代理伺服器需要身分驗證，請在**使用者名稱** 和 **密碼**欄位中指定與代理伺服器建立連線的帳戶的憑據。我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

  5. 如果有必要，請上傳新的管理伺服器憑證。

- **變更到該主伺服器上的另一個虛擬伺服器**

  選擇此選項可以將用戶端裝置移至目前主管理伺服器上的虛擬管理伺服器。為此，在**虛擬管理伺服器名稱**下拉清單中，選擇必要的虛擬管理伺服器。

7. 在精靈的**選取要執行此工作的帳戶**步驟中，指定帳戶設定：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。
  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

8. 如果要變更預設工作設定，請在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項。
   如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時變更預設設定。

9. 點擊**完成**按鈕。
   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 如果要變更預設工作設定，請在工作屬性視窗中根據需要指定一般工作設定。

12. 點擊**儲存**按鈕。
    工作被建立和配置。

13. 執行建立的工作。

在工作完成後，為其建立工作的用戶端裝置將被工作設定中指定的管理伺服器管理。

刪除虛擬管理伺服器

當您刪除虛擬管理伺服器時，在管理伺服器上建立的所有物件（包括政策和工作）也將被刪除。由虛擬管理伺服器管理的管理群組中的受管理裝置將被從管理群組中移除。要返回Kaspersky Next XDR Expert管理的裝置，請執行網路輪詢，然後將找到的裝置從未分配的裝置群組移動到管理群組。

要刪除虛擬管理伺服器：

1. 切換到要刪除的虛擬管理伺服器所屬的主實體管理伺服器：

   a. 在主選單中，選擇任意部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，點擊主實體管理伺服器的名稱。
      在主選單中，管理伺服器將變更為您選擇的伺服器。

2. 透過以下方式之一移動到主實體管理伺服器的屬性：

   - 在導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後按一下設定圖示 (⚙)。
   - 在主選單中，按一下管理伺服器名稱。

3. 在開啟的屬性頁面中，前往**管理伺服器**頁籤。

4. 選擇要刪除的虛擬管理伺服器。

5. 在功能表行中，點擊 **刪除**按鈕。

虛擬管理伺服器將被刪除。

配置管理伺服器連線事件記錄

操作期間的連線歷程和到管理伺服器的連線嘗試可以被儲存到檔案。檔案中的資訊允許您跟蹤不僅您的網路基礎架構中的連線，還有對伺服器的非授權存取嘗試。

要記錄連線管理伺服器事件：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤，選取**連線連接埠**區段。

3. 啟用**記錄管理伺服器連線事件**設定。

   所有連入管理伺服器的後續事件、身分驗證結果和 SSL 錯誤將被儲存到檔案 /var/opt/kaspersky/klnagent_srv/logs/SC.syslog。

設定事件儲存區中的最大事件數量

在管理伺服器內容視窗的**事件儲存區**區域中，您可以透過限制事件記錄數和儲存期限來編輯管理伺服器資料庫的事件儲存設定。當您指定事件最大數時，應用程式計算用於指定數目的儲存空間的大概大小。您可以使用該大概計算來評估您在磁碟上是否具有足夠空間以避免資料庫溢出。管理伺服器資料庫的預設容量是 400,000 個事件。最大建議的資料庫容量是 45,000,000 個事件。

應用程式每 10 分鐘檢查一次資料庫。如果事件數達到指定的最大值加 10,000，應用程式將刪除最舊的事件，以便僅保留指定的最大事件數。

若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入作業係統記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。預設情況下，事件佇列的上限為 20,000 個事件。您可以透過編輯 KLEVP_MAX_POSTPONED_CNT 標誌的值來自訂佇列上限。

要限制儲存在管理伺服器事件儲存區中的事件的數量：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤，選取**事件儲存區**區段。指定儲存在資料庫中的最大事件數量。

3. 點擊**儲存**按鈕。

此外，您可以執行以下操作：

- 變更任何工作的設定，以儲存與工作進度相關的事件，或者只儲存工作執行結果。
- 減少或停用安裝在受管理裝置上的管理伺服器、網路代理和卡巴斯基應用程式的事件的儲存期限。

為此，您將降低資料庫中的事件數量，提高與資料庫中事件表分析相關之情境的執行速度，並降低緊急事件被大數量事件覆寫的風險。

變更 DBMS 憑證

有時，您可能需要變更 DBMS 憑證，例如，基於安全目的而執行的憑證變更。

更改管理伺服器資料庫憑據

若要在 Linux 環境中變更管理伺服器和 IAM 資料庫憑據：

1. 停止管理伺服器。根據卡巴斯基安全管理中心 Linux 的部署類型，使用 Root 帳戶執行下列其中一個命令：

   - 對於卡巴斯基安全管理中心 Linux 容錯移轉叢集：
     在作用中節點上，執行下列命令：

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

   - 對於異地分散式卡巴斯基安全管理中心 Linux 容錯移轉叢集：
     在兩個節點上，執行下列命令：

     ```
     crm node standby
     ```

   - 對於非叢集管理伺服器部署：
     執行以下指令：

     ```
     systemctl stop kladminserver_srv.service
     systemctl stop kliam_srv.service
     ```

2. 使用 DBMS 超級使用者權限連線至管理伺服器資料庫，並執行下列命令：

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   其中 `<old_kscdbadmin>` 是管理伺服器先前用來連線至其資料庫的 DBMS 帳戶，而 `<new_kscdbadmin>` 是新的 DBMS 帳戶。

3. 使用 DBMS 超級使用者權限連線至 IAM 資料庫，並執行下列命令：

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   其中 `<old_iamdbadmin>` 是管理伺服器先前用來連線至其資料庫的 DBMS 帳戶，而 `<new_iamdbadmin>` 是新的 DBMS 帳戶。

4. 查找 IAM 設定檔：/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. 在 `dbms_iam` 區段中，在使用者和密碼欄位中指定新帳戶憑證。確保該帳戶存在於 DBMS 中，並已指定為 IAM 資料庫擁有者。

6. 執行管理伺服器。根據卡巴斯基安全管理中心 Linux 的部署類型，使用 Root 帳戶執行下列其中一個命令：

   - 對於卡巴斯基安全管理中心 Linux 容錯移轉叢集：
     在作用中節點上，執行下列命令：

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - 對於異地分散式卡巴斯基安全管理中心 Linux 容錯移轉叢集：
     在兩個節點上，執行下列命令：

     ```
     crm node online
     ```

   - 對於非叢集管理伺服器部署：
     執行以下指令：

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. 執行klsrvconfig公用程式：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

8. 指定一個新的帳戶名稱。您應該指定 DBMS 中存在之帳戶的憑證。

9. 輸入新密碼。

10. 指定新密碼進行確認。

11. 等待管理伺服器恢復運作，並等待作用中節點上出現 syslog 項目，指出管理伺服器已準備好執行 GUI 操作。

    管理伺服器資料庫憑據已變更。

管理伺服器資料的備份與還原

資料備份可讓您以特定狀態儲存管理伺服器資料，並在需要時恢復資料，例如，如果管理伺服器資料已損壞。

備份管理伺服器資料之前，請檢查管理群組中是否新增了虛擬管理伺服器。如果新增了虛擬管理伺服器，請確保在備份之前為該虛擬管理伺服器分配了管理員。備份後，您將無法授予管理員對虛擬管理伺服器的存取權限。請注意，如果管理員帳戶憑據丟失，您將無法向虛擬管理員伺服器分配新管理員。

您只能透過執行*管理伺服器備份*工作來建立管理伺服器資料的備份副本。部署Kaspersky Next XDR Expert時，系統會自動建立此工作。

在主管理伺服器上，無法建立和刪除*備份管理伺服器資料*工作。

備份副本會儲存在 `/var/spool/ksc/backup` 目錄中。在部署 Kaspersky Next XDR Expert 時，備份目錄將自動建立於安裝了管理伺服器的工作節點上。在主管理伺服器上，您無法變更備份目錄路徑。

以下資料儲存在管理伺服器的備份副本中：

- 管理伺服器資料庫（政策、工作、應用程式設定、管理伺服器上儲存的事件）。
- 管理群組和用戶端裝置結構的組態詳情
- 用於遠端安裝的應用程式分發套件的儲存
- 管理伺服器憑證

只用使用KDT公用程式才能進行管理伺服器資料還原。

您可以建立KUMA Core的備份副本，並在需要時從備份中還原。您也可以使用協力廠商工具備份其他Kaspersky Next XDR Expert元件，但前提是必須使用安裝在Kubernetes叢集之外的獨立伺服器上的DBMS。您不得使用協力廠商工具建立管理伺服器資料庫備份。

配置管理伺服器備份工作

部署*Kaspersky Next XDR Expert*時會自動建立管理伺服器備份工作，且無法刪除。您只能透過執行*管理伺服器備份*工作，建立管理伺服器資料的備份副本。

若要設定管理伺服器資料備份工作：

1. 在主功能表中，前往**工作**，然後選擇**管理伺服器備份**工作。
2. 按一下**管理伺服器備份**工作。
   工作內容視窗隨即開啟。
3. 如有必要，請根據您的需求指定一般工作設定。
4. 在**應用程式設定**部分，您可以根據需要設定備份防護密碼和備份副本數量。
   我們建議限制備份管理伺服器資料的數量，以避免分配給儲存備份的磁碟空間溢出。
5. 點擊**儲存**以套用變更。

*管理伺服器資料備份*工作已配置。

使用KDT公用程式恢復管理伺服器資料

*備份管理伺服器資料*工作可讓您複製管理伺服器資料以進行備份。若要恢復管理伺服器資料，必須使用KDT公用程式。

若要還原管理伺服器資料：

1. 在KDT公用程式所在的管理員主機上，執行以下命令：

   `./kdt invoke ksc --action listBackup`

   顯示位於 `/var/spool/ksc/backup` 目錄中的備份清單。

2. 執行以下命令：

   ```
   ./kdt invoke ksc --action restoreBackup \
     --param ksc_file_backup="<檔案名稱>" \
     --param ksc_backup_password="<密碼>"
   ```

   其中：

   - `ksc_file_backup` 是所需備份壓縮檔案的路徑及壓縮檔案名稱。
   - `ksc_backup_password` 是備份以密碼儲存時的壓縮檔案密碼。如果未使用密碼，請將 `ksc_backup_password` 變數設定為 `""`。

     若密碼包含雙引號，請使用反斜線對雙引號進行跳脫 (`\"`)。

管理伺服器資料從選定的備份存檔中還原。

刪除管理伺服器階層

如果不再想擁有管理伺服器階層，您可以從該階層將其斷開連線。

要刪除管理伺服器階層：

1. 在主選單中，按一下管理伺服器名稱。
2. 在開啟的頁面中，前往**管理伺服器**標籤。
3. 在您要刪除次要管理伺服器的管理群組，選取次要管理伺服器。
4. 在功能表中，點擊**刪除**。
5. 在開啟的視窗中，點擊**確定**以確認您要刪除該次要管理伺服器。

先前的主要和次要管理伺服器現在彼此獨立。層級不再存在。

存取公用 DNS 伺服器

如果無法使用系統DNS存取卡巴斯基伺服器，Open Single Management Platform可以依以下順序使用這些公用DNS伺服器：

1. Google Public DNS™ (8.8.8.8)
2. Cloudflare® DNS (1.1.1.1)
3. 阿里雲 DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

對這些 DNS 伺服器的請求可能包含網域位址和管理伺服器的公用 IP 位址，因為應用程式建立了到 DNS 伺服器的 TCP/UDP 連線。如果Open Single Management Platform使用公用DNS伺服器，則資料處理受相關服務的隱私權政策約束。

要透過使用 klscflag 公用程式配置公共 DNS 的使用：

1. 在KDT公用程式所在的管理員主機上，執行以下命令以停用公共DNS的使用：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1'
```

2. 要啟用公共 DNS 的使用，請執行以下指令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0'
```

設定介面

您可根據使用的功能顯示和隱藏區段與介面元素設定OSMP主控台介面。

若要根據目前使用的功能集設定OSMP主控台介面：

1. 在主功能表中，轉至**設定 → 介面選項**。

2. 啟用或停用所需的選項：

   - **顯示資料加密與防護**
   - **顯示 MDR 功能**
   - **顯示 EDR 警示**

3. 按一下**儲存**按鈕。

   啟用所需選項後，主控台會在主功能表中顯示對應區域。例如，如果您啟用**顯示 EDR 警示** ，則**監控 → 警示**區域會出現在主功能表中。

使用 TLS 的加密通信

要修復您組織企業網路中的弱點，您可以使用 TLS 協定啟用流量加密。您可以在管理伺服器上啟用 TLS 加密協定和受支援的密碼套裝。Open Single Management Platform支援TLS協定版本1.0、1.1、1.2 和 1.3。您可以選取所需的加密協定和加密套裝。

Open Single Management Platform使用自簽名憑證。您也可以使用您自己的憑證。我們建議使用由受信任的憑證授權機構簽發的憑證。

要在管理伺服器上設定允許的加密協議和加密套裝：

1. 在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <值> -t d'
```

使用 SrvUseStrictSslSettings 旗標在管理伺服器上設定允許的加密協議和加密套件。

指定 SrvUseStrictSslSettings 旗標的<value>參數：

- 4 — 僅啟用 TLS 1.2 和 TLS 1.3 協定。此外，還啟用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密碼套裝（需要這些密碼套裝才能向後相容卡巴斯基安全管理中心 11）。這是預設值。

  TLS 1.2 協定支援的密碼套裝：

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - AES256-GCM-SHA384（具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密碼套裝）
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 協定支援的密碼套裝：

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

- 5 — 僅啟用 TLS 1.2 和 TLS 1.3 協定。對於 TLS 1.2 和 TLS 1.3 協定，下面列出的特定密碼套裝受支援。

  TLS 1.2 協定支援的密碼套裝：

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 協定支援的密碼套裝：

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

我們不建議使用 0、1、2 或 3 作為 SrvUseStrictSslSettings 標誌的參數值。這些參數值對應於不安全的 TLS 協定版本（TLS 1.0 和 TLS 1.1 協定）和不安全的密碼套裝，僅用於向後相容早期的卡巴斯基安全管理中心版本。

2. 重新啟動以下Open Single Management Platform服務：

   - 管理伺服器
   - 網頁伺服器
   - 啟動代理

啟用了使用 TLS 協定的流量加密。

您可以使用 KLTR_TLS12_ENABLED 和 KLTR_TLS13_ENABLED 標誌分別啟用對 TLS 1.2 和 TLS 1.3 協定的支援。這些標誌預設啟用。

要啟用或停用對TLS 1.2和TLS 1.3協定的支援：

在KDT公用程式所在的管理員主機上，執行以下命令之一：

- 使用此指令啟用或停用對TLS 1.2協定的支援：

  ```
  ./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
  ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <值> -t d'
  ```

- 使用此指令啟用或停用對TLS 1.3協定的支援：

  ```
  ./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv
  ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <值> -t d'
  ```

指定旗標的 <值> 參數：

- `1` — 啟用對 TLS 協定的支援。
- `0` — 停用對 TLS 協定的支援。

發現網路裝置

該部分描述網路裝置的搜尋和發現。

Open Single Management Platform可讓您依照指定規則找尋裝置。您可以儲存搜尋結果到文字檔案。

搜尋和發現功能允許您尋找以下裝置：

- Open Single Management Platform 管理伺服器及其從屬管理伺服器之管理群組中的受管理裝置。
- 由管理伺服器及其從屬管理伺服器管理的未配置裝置。

情境：發現網路裝置

您必須在安裝安全應用程式之前執行裝置發現。當所有網路裝置被發現時，您可以接收它們的資訊並透過政策管理。一般網路輪詢用於發現是否有新裝置以及先前發現的裝置是否仍在網路中。

網路裝置發現分步驟進行：

1. **初始裝置發現**

   手動執行裝置搜尋。

2. **配置未來輪詢**

   確保 IP 範圍輪詢被啟用且輪詢排程滿足您組織的需要。當設定輪詢排程時，使用建議的網路輪詢頻率。

   如果您的網路包含 IPv6 裝置，也可以啟用 Zeroconf 輪詢。

   如果網域中包含聯網裝置，建議使用網域控制器輪詢。

   使用Windows的發佈點來輪詢Windows網路。

   > 您只能使用發佈點執行IP範圍輪詢和Zeroconf輪詢。

3. **設定規則以新增發現的裝置到管理群組（可選）**

   新裝置經由網路輪詢偵測後，會出現在網路上。這些裝置會自動歸入**未指派的裝置**群組。如有需要，您可以設定自動移動這些裝置到**受管理裝置**群組。您也可以建立保留規則。

   如果您略過該規則設定步驟，所有先發現的裝置都移到**未指派的裝置**群組並留在該處。如果您想，您可以手動移動這些裝置到**受管理裝置**群組。如果您移動這些裝置到**受管理裝置**群組，您可以分析每部裝置的資訊，並決定您是否要移動它到管理群組以及移動到哪個群組。

結果

完成情境可以導致如下：

- 卡巴斯基安全管理中心管理伺服器發現網路中的裝置並提供您它們的資訊。
- 未來輪詢被設定並根據指定的排程工作。

新發現的裝置會依照指定的規則進行分配。如果未設定任何規則，裝置會留在**未指派的裝置**群組中。

Windows 網路輪詢

關於 Windows 網路輪詢

Kaspersky Next XDR Expert 管理伺服器不支援 Windows 網路輪詢。使用基於 Windows 的發佈點來輪詢 Windows 網路。

在快速輪詢過程中，發佈點只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。在完整輪詢中，以下資訊被從每個用戶端裝置請求：

- 作業系統名稱
- IP 位址
- DNS 名稱
- NetBIOS 名稱

快速輪詢和完整輪詢都需要以下：

- 連接埠 UDP 137/138、TCP 139、UDP 445、TCP 445 必須在網路中可用。
- SMB 協定已啟用。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在管理伺服器上啟用。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在用戶端裝置上啟用。
  - 至少一台裝置上，如果網路裝置數量不超過 32。
  - 對每 32 台網路裝置至少一台裝置上。

完整輪詢僅在快速輪詢至少執行了一次時可以執行。

IP 範圍輪詢

Kaspersky Next XDR Expert 允許僅使用發佈點來輪詢 IP 範圍。發佈點會嘗試利用標準 DNS 請求，對指定範圍中的每個 IPv4 位址執行反向名稱解析來得出 DNS 名稱。若該操作成功，發佈點會向接收到的名稱傳送 `ICMP ECHO REQUEST`（與 `ping` 命令相同）。若裝置回應，其相關資訊將被新增至 Kaspersky Next XDR Expert 資料庫。若要排除具有 IP 位址但不是電腦的網路裝置，例如網路印表機或路由器，反向名稱解析是必要的。

該輪詢方法依賴正確配置的本機 DNS 服務。它必須具有反向查詢網域。如果該網域未被配置，IP 子網路輪詢將沒有結果。

最初，發佈點從指派為發佈點的裝置的網路設定中獲取用於輪詢的IP範圍。如果裝置位址是192.168.0.1且子網路遮罩是255.255.255.0，網路192.168.0.0/24自動包含在輪詢位址清單中。發佈點會輪詢192.168.0.1到192.168.0.254之間的所有位址。

如果僅啟用IP範圍輪詢，發佈點將僅發現具有IPv4位址的裝置。如果您的網路包含IPv6裝置，請開啟裝置的Zeroconf輪詢。

對於 Microsoft Active Directory 或 Samba 網域控制器內所有以 Linux 為基礎的主機，請在 `/etc/samba/smb.conf` 檔案中指定 `netbios name` 和 `workgroup` 參數。否則，輪詢結果可能包含重複的主機。

使用發佈點進行網域控制器輪詢

若要使用發佈點設定網域控制器輪詢：

1. 開啟發佈點屬性。
2. 轉至**IP 範圍輪詢**部分，然後選擇**啟用範圍輪詢**選項。

   IP 範圍視窗將開啟。
3. 指定新的IP位址範圍名稱。
4. 按一下**新增** ，然後使用位址和子網路遮罩或使用起始IP位址和結束IP位址指定IP範圍。或者，透過點擊**瀏覽**按鈕新增現有子網路。
5. 如果需要，點擊**設定輪詢排程**按鈕以指定輪詢排程選項。

   輪詢僅根據指定的排程開始。無法手動啟動輪詢。

   輪詢排程選項：

   - **每 N 天**

     輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

     預設下，輪詢每天執行一次，從目前系統日期和時間開始。
   - **每 N 分鐘**

     輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。
   - **按每週中的指定日**

     輪詢定期執行，在指定星期的指定時間。
   - **每月於選定的週間日**

     輪詢定期執行，在指定月日的指定時間。
   - **執行錯過的工作**

     如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

     如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

     如果停用該選項，管理伺服器等待下一次排程輪詢。

     預設情況下已停用該選項。
6. 如果啟用**使用 Zeroconf 來輪詢 IPv6 網路**選項，發佈點將使用零組態網路（也稱為*Zeroconf*）自動輪詢IPv6網路。

   在這種情況下，指定的 IP 範圍將被忽略，因為發佈點會輪詢整個網路。如果發佈點執行 Linux，則**使用 Zeroconf 來輪詢 IPv6 網路**選項可用。要使用 Zeroconf IPv6 輪詢，您必須在發佈點上安裝 avahi-browse 公用程式。

輪詢完成後，如果您設定並啟用了**裝置移動規則受管理裝置**受管理裝置群組中。如果未啟用移動規則，新發現的裝置被自動包含在**未指派的裝置**群組。

網域控制器輪詢

Open Single Management Platform支援輪詢下列網域控制器類型：

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

對於 Samba 網域控制器， Samba 4 用作 Active Directory 網域控制器。

當您輪詢網域控制器時，管理伺服器或發佈點會檢索有關網域中包含的裝置的網域結構、使用者帳戶、安全群組和 DNS 名稱的資訊。

如果所有聯網裝置都是網域的成員，我們建議使用網域控制器輪詢。如果某些聯網裝置未包含在網域中，則網域控制器輪詢無法發現這些裝置。

先決條件

在輪詢網域控制器之前，請確保啟用以下協定：

- 簡單身分驗證和安全層 (SASL)
- 輕量級目錄訪問協定 (LDAP)

確保網域控制器裝置上的以下連接埠可用：

- 389 用於 SASL
- 636 用於 TLS

對於 Microsoft Active Directory、Samba、FreeIPA 或 ALD Pro 網域控制器內的所有 Linux 型主機，需要在 `/etc/samba/smb.conf` 檔案中指定 `netbios name` 和 `workgroup` 參數。否則，輪詢結果可能包含重複的主機。

如果 Microsoft Active Directory 網域包含多個網域控制器，則不支援在網域輪詢期間選取特定控制器。將與偵測到的第一個網域控制器建立連線。為確保與 Microsoft Active Directory 網域進行正確的身分驗證，憑證的「主體別名 (SAN)」欄位必須包含此網域中包含的所有網域控制器位址，以及 Microsoft Active Directory 網域的 NetBIOS 名稱。

使用管理伺服器進行網域控制器輪詢

要使用管理伺服器輪詢網域控制器：

1. 在主功能表中，轉至**發現和佈署 → 發現 → 網域控制器**。
2. 點擊**配置輪詢設定**。
   網域控制器輪詢設定視窗將開啟。
3. 在**輪詢**欄位中，將切換按鈕切換到**已啟用**位置。
4. 在**輪詢指定網域**中，按一下**新增**，然後指定網域控制器的位址和使用者憑據，然後按一下**確定**。
5. 在**網域控制器輪詢設定**視窗中，執行下列操作：
   - 選擇要輪詢的網域控制器的類型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。
   - 如有必要，設定輪詢排程。預設間隔是一小時。下次輪詢接收的資料完全取代舊資料。
     有以下輪詢排程選項可用：
     - **每 N 天**

       輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。
       預設下，輪詢每天執行一次，從目前系統日期和時間開始。
     - **每 N 分鐘**

       輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。
     - **按每週中的指定日**

       輪詢定期執行，在指定星期的指定時間。
     - **每月於選定的週間日**

       輪詢定期執行，在指定月日的指定時間。
     - **執行錯過的工作**

       如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。
       如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。
       如果停用該選項，管理伺服器等待下一次排程輪詢。
       預設情況下已停用該選項。

   如果您變更網域安全群組中的使用者帳戶，這些變更將在您輪詢網域控制器一小時後顯示在Open Single Management Platform中。
6. 如有必要，請變更要指派給已發現使用者帳戶的租用戶。為此，請從**租用戶**下拉清單中選擇所需的租用戶。
   預設情況下，指定管理伺服器的租用戶。您可以選取多個租用戶。

7. 點擊**儲存**以套用變更。

8. 如果您要立即執行輪詢，請點擊**開始輪詢**按鈕。

使用發佈點進行網域控制器輪詢

您還可以使用發佈點輪詢網域控制器。基於 Windows 或 Linux 的受管理裝置可以充當發佈點。

對於 Linux 發佈點，支援輪詢所有類型的網域控制器。
對於 Windows 發佈點，僅支援輪詢 Microsoft Active Directory 網域控制器。
不支援使用 Mac 發佈點進行輪詢。

要使用發佈點配置網域控制器輪詢：

1. 開啟發佈點內容。

2. 選擇**網域控制器輪詢**部分。

3. 在**輪詢**欄位中，將切換按鈕切換到**已啟用**位置。

4. 如果使用 Linux 發佈點，請選擇要輪詢的網域控制器的類型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。

   當使用發佈點和管理伺服器設定輪詢時，無需指定相同的網域控制器類型。

5. 選擇要輪詢的網域控制器。

   如果您使用 Linux 發佈點，請在**輪詢指定網域**部分中點擊**新增**，然後指定網域控制器的位址和使用者憑據。

   如果您使用 Windows 發佈點，則可以選擇以下選項之一：

   - **輪詢目前網域**
   - **輪詢整個網域樹系**
   - **輪詢指定網域**

6. 如果需要，點擊**設定輪詢排程**按鈕以指定輪詢排程選項。

   輪詢僅根據指定的排程開始。無法手動啟動輪詢。

輪詢完成後，網域結構將顯示在**網域控制器**部分中。

如果您設定和啟用了裝置移動規則，新發現的裝置會自動包含在**受管理裝置**群組中。如果未啟用移動規則，新發現的裝置被自動包含在**未指派的裝置**群組。

已發現的使用者帳戶可用於透過Kerberos協定在OSMP主控台中進行網域身分驗證。

身分驗證與網域控制器連線

初次與網域控制器連線時，管理伺服器會識別連線通訊協定。未來所有與該網域控制器的連線，都會使用此通訊協定。

初次與網域控制器連線的程序如下：

1. 管理伺服器嘗試透過 TLS 連線到網域控制器。

   預設並不會要求執行憑證驗證。將 KLNAG_LDAP_TLS_REQCERT 標旗標誌設為 1，即可強制執行憑證驗證。

   預設會使用依作業系統而定的憑證授權單位 (CA) 路徑來存取憑證鏈。使用 KLNAG_LDAP_SSL_CACERT 旗標，即可指定自訂路徑。

2. 如果 TLS 連線失敗，管理伺服器會嘗試透過 SASL (DIGEST-MD5) 連線到網域控制器。

3. 如果 SASL (DIGEST-MD5) 連線失敗，管理伺服器會改用以未加密 TCP 連線進行的簡單身分驗證，連線到網域控制器。

您可以使用KDT命令設定旗標。例如，您可以強制執行憑證驗證。為此，在KDT公用程式所在的管理員主機上執行以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
KLNAG_LDAP_TLS_REQCERT -t d -v 1'
```

配置 Samba 網域控制器

Open Single Management Platform支援僅在Samba 4上執行的Linux網域控制器。

Samba網域控制器支援與Microsoft Active Directory網域控制器相同的架構延伸。您可以使用 Samba 4 架構延伸啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容。這是一個可選操作。

我們建議啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容。這將確保Open Single Management Platform和Samba網域控制器之間的正確交互。

要啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容：

1. 執行以下指令以使用 RFC2307 架構延伸：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 網域控制器中啟用架構更新。若要這麼做，請將以下行新增至 `/etc/samba/smb.conf` 檔案：

   ```
   dsdb:schema update allowed = true
   ```

   如果架構更新完成時出現錯誤，則需要對充當架構主機的網域控制器執行完整還原。

針對 Samba 網域控制器內所有以 Linux 為基礎的主機，請在 `/etc/samba/smb.conf` 檔案中指定 `netbios name` 和 `workgroup` 參數。否則，輪詢結果可能包含重複的主機。

在用戶端裝置上使用 VDI 動態模式

虛擬基礎架構可以使用動態虛擬機佈署企業網路。Kaspersky Next XDR Expert 可偵測動態虛擬機，並將其資訊新增至管理伺服器資料庫。使用者使用完動態虛擬機後，這些虛擬機將從虛擬架構中移除。動態虛擬機記錄將儲存在管理伺服器資料庫中。此外，不存在的虛擬機器可以在OSMP主控台中顯示。

為防止儲存不存在的虛擬機資訊，Kaspersky Next XDR Expert 支援虛擬桌面基礎架構 (VDI) 的動態模式。管理員可在要安裝於臨時虛擬機的網路代理安裝套件內容中啟用 VDI 動態模式支援。

當動態虛擬機被停用，網路代理通知管理伺服器該虛擬機已被停用。虛擬機被成功停用，它將從連線到管理伺服器的裝置清單中被移除。如果虛擬機被停用錯誤，網路代理沒有傳送停用虛擬機的通知到管理伺服器，使用備份方案。使用這個方案，和管理伺服器嘗試同步三次未成功後，虛擬機將從連線管理伺服器的裝置清單中移除。

在網路代理安裝套件的內容中啟用 VDI 動態模式

要啟用 VDI 動態模式，請執行以下操作：

1. 在主功能表中，轉至**軟體管理→安裝套件**。
2. 在網路代理安裝套件的右鍵，選取"**內容**"。

   內容視窗隨即開啟。
3. 在**內容**視窗中，選取**進階**區域。
4. 在**進階**區段上選取**為 VDI 啟用動態模式**選項。

   要安裝網路代理的裝置將成為 VDI 的一部分。

將啟用 VDI 的裝置移至管理群組

要將啟用 VDI 的裝置移至管理群組，請執行以下操作：

1. 轉至**資產管理 → 移動規則**。
2. 點擊**新增**。
3. 在**規則條件**頁簽上，選擇**虛擬機**頁簽。
4. 將**這是一台虛擬機**規則設定為**是** ，將**虛擬桌面基礎架構的一部分**設定為**是。**
5. 點擊**儲存**。

管理用戶端裝置

卡巴斯基Next XDR Expert允許您管理用戶端裝置：

- 檢視受管理裝置的設定和狀態，包括叢集和伺服器陣列。
- 配置發佈點。
- 管理工作。

您可以使用管理群組將用戶端裝置合併到一個集合中，並將其作為一個單元進行管理。一台客戶端裝置只能包含在一個管理群組中。**規則條件**可以根據規則條件自動將裝置指派至群組：

- 建立裝置移動規則。
- 複製裝置移動規則。
- 裝置移動規則的條件。

您可以使用裝置分類來根據條件過濾裝置。您也可以標記裝置以建立分類、尋找裝置以及在管理群組之間發佈裝置。

受管理裝置設定

要檢視受管理裝置設定：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。

   受管理裝置清單隨即顯示。

2. 在受管理裝置清單中，按一下有所需裝置名稱的連結。

所選裝置的內容視窗隨即顯示。

以下分頁顯示在屬性視窗的上部，代表主設定群組：

- **一般**

  此頁籤包含以下部分：

  - **一般**區域顯示有關用戶端裝置的一般資訊。資訊基於上一次用戶端裝置與管理伺服器之間的同步接收的資料來提供：

    - **名稱**

      在該欄位中，您可以檢視和修改管理群組中的用戶端裝置名稱。

    - **描述**

      在該欄位中，您可以輸入用戶端裝置的附加敘述。

- **裝置狀態**

  根據管理員針對裝置病毒防護狀態定義之條件，以及網路上裝置的活動所指派的用戶端裝置狀態。

- **裝置所有者**

  裝置擁有者的名稱。作為裝置擁有者，您可以點擊**管理裝置所有者**連接來分配或刪除使用者。

- **完整的群組名稱**

  包括了用戶端裝置的管理群組。

- **上次病毒資料庫更新**

  裝置上病毒資料庫或應用程式最後更新日期。

- **連線至管理伺服器**

  裝置上的網路代理上一次連線到管理伺服器的日期和時間。

- **上一次可見**

  裝置在網路中最後可見的日期和時間。

- **網路代理版本**

  安裝的網路代理的版本。

- **建立日期**

  Open Single Management Platform內裝置的創建日期。

- **強制同步**

  雖然 Open Single Management Platform 會自動同步受管理裝置的狀態、設定、工作和政策，但在某些情況下，管理員需要確切知道目前是否已對指定裝置執行同步。

  如果按一下**強制同步**按鈕，應用程式會將所選裝置與管理伺服器同步。

- **不斷開與管理伺服器的連線**

  如果啟用此選項，受管理裝置和管理伺服器之間將保持持續連線。如果您使用的不是推送伺服器，您可能想要使用此選項，它提供了這樣的連線。

  如果停用此選項且不在使用推送伺服器，則受管理裝置將僅在同步資料或傳輸資訊時連線至管理伺服器。

  不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

  預設情況下，受管理裝置上停用此選項。預設情況下，此選項在安裝了管理伺服器的裝置上處於啟用狀態，即使您嘗試停用它也會保持啟用狀態。

- **連線**

  本節包含一個表格，其中含有有關目前登入裝置的使用者的資訊。該表格在對應的欄中顯示以下資料：

  - 使用者名稱。
  - SAM 帳戶名稱

- 使用者主體名稱
- 電子郵件地址。

若要正確顯示有關網域使用者工作階段的資訊，必須使用網域控制器輪詢。

- **網路**區段會顯示有關用戶端裝置網路屬性的以下資訊：
  - **IP 位址**

    裝置 IP 位址。
  - **Windows 網域**

    包含裝置的工作組。
  - **DNS 名稱**

    用戶端裝置的 DNS 網域名稱。
  - **NetBIOS 名稱**

    用戶端裝置的名稱。
  - **IPv6 位址**

    用戶端裝置的 IPv6 位址。
- **系統**區段會顯示安裝在用戶端裝置上應用程式的相關資訊。
  - **作業系統**
  - **CPU 架構**
  - **裝置名稱**
  - **虛擬機類型**

    虛擬機製造商。
  - **作為 VDI 一部分的動態虛擬機**

    此行顯示用戶端裝置是否是作為 VDI 一部分的動態虛擬機。
  - **作業系統組建版本**
- **防護**區域將提供有關用戶端裝置上病毒防護的目前狀態的一下資訊：
  - **可見**

    用戶端裝置的可見性狀態。
  - **裝置狀態**

    根據管理員針對裝置病毒防護狀態定義之條件，以及網路上裝置的活動所指派的用戶端裝置狀態。

- **狀態描述**

  用戶端裝置防護狀態和與管理伺服器的連線。

- **防護狀態**

  該欄位顯示目前的用戶端裝置即時防護狀態。

  當裝置狀態變更時，新狀態僅在用戶端裝置與管理伺服器同步之後顯示在裝置屬性視窗。

- **上一次完整掃描**

  用戶端裝置上執行的最後一次惡意軟體掃描的日期和時間。

- **偵測到的病毒**

  自安裝安全應用程式（第一次掃描）或自上次重設威脅計數器以來，在用戶端裝置上偵測到的威脅總數。

- **解毒失敗的物件**

  用戶端裝置上的未處理檔案數量。

  該欄位行動裝置上的未處理檔案數量。

- **磁碟加密狀態**

  裝置本機磁碟機上的目前檔案加密狀態。有關狀態的說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

  檔案只能在安裝了 Kaspersky Endpoint Security for Windows 的受管理裝置上進行加密。

- **檢視資料加密錯誤**

  有關裝置上資料加密錯誤的資訊。加密由卡巴斯基應用程式的加密資料功能執行。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。

- **應用程式定義的裝置狀態**區段會提供相關資訊，說明由裝置上安裝的受管理應用程式所定義的裝置狀態。此裝置狀態可能與 Kaspersky Next XDR Expert 定義的狀態不同。

- **應用程式**

  此分頁列出了用戶端裝置上安裝的所有 Kaspersky 應用程式。此分頁包含**開始**和**停止**按鈕，可用來啟動和停止所選的 Kaspersky 應用程式（網路代理除外）。如果受管理裝置上的連接埠15000 UDP可用於接收來自管理伺服器的推播通知，則可以使用這些按鈕。如果受管理裝置無法用於推播通知，但啟用了與管理伺服器的連續連線模式（啟用了**不斷開與管理伺服器的連線**部分中的**一般**選項），則**開始**和**停止**按鈕也可用。否則，當您嘗試啟動或停止應用程式時，會顯示錯誤訊息。您也可以按一下應用程式名稱以檢視有關該應用程式的一般資訊、裝置上發生的事件清單以及應用程式設定。

- **啟用政策和政策設定檔**

  此標籤會列出分派給受管理裝置的政策和政策設定檔。

- **工作**

  在**工作**標籤上，您可以管理用戶端工作：檢視現有工作清單、建立新工作、移除、啟動和停止工作、修改工作設定以及檢視執行結果。該工作清單會根據用戶端最近一次與管理伺服器同步的連線期間所收到的資料提供。管理伺服器向用戶端裝置請求工作狀態詳情。如果受管理裝置上的連接埠15000 UDP可用於接收來自管理伺服器的推播通知，則會顯示工作狀態並啟用用於管理工作的按鈕。如果推送伺服器無法與受管理裝置建立連線，但啟用了與管理伺服器的持續連線模式（啟用了**一般**部分中的**不斷開與管理伺服器的連線**選項），則也可以使用工作操作。

如果未建立連線，則不顯示狀態，按鈕被停用。

- **事件**

  事件標籤將顯示選定用戶端裝置在管理伺服器上所記錄事件的資訊。

  您可以匯出、複製和刪除裝置事件。

- **安全問題**

  在**安全問題**頁籤中，您可為用戶端裝置檢視、編輯和建立安全問題。安全問題可以透過安裝在用戶端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。例如，如果使用者定期將惡意軟體從其卸除式磁碟機移至裝置，則管理員可以建立安全問題。管理員可以在安全問題文字中提供情況的簡要說明和建議的操作（例如對於一個使用者的紀律性操作），還可以新增連結到使用者。

  對其採用了所有必要操作的安全問題稱為*已處理安全問題*。存在的未處理安全問題可被選為將裝置的狀態變更為*緊急*或*警告*的條件。

  此部分包含已為裝置建立的安全問題的清單。安全問題按照幾個等級和類型分類。安全問題的類型是由建立安全問題的 Kaspersky 應用程式定義。選中**已處理**列中的核取方塊即可突出顯示清單上的已處理安全問題。

- **標籤**

  在**標籤**分頁，您可以編輯用來尋找用戶端裝置的關鍵字清單，並可以檢視現有標籤清單、從清單中配置標籤、設定自動標記規則、新增標籤和重新命名舊標籤以及移除標籤。

- **進階**

  此分頁包含以下區段：

  - **應用程式登錄資料**。在此區域，您可以檢視用戶端裝置上安裝的應用程式及其更新的登錄檔，您還可以設定應用程式登錄資料的顯示方式。

    如果用戶端裝置上安裝的網路代理將所需資訊傳送到管理伺服器，則將提供有關已安裝應用程式的資訊。您可以在網路代理或其政策的內容視窗中的**儲存區**區域，設定將資訊傳送到管理伺服器。

    按一下應用程式名稱會開啟一個視窗，其中包含應用程式詳細資訊以及為該應用程式安裝的更新軟體套件的清單。

  - **可執行檔**。此區域會顯示在用戶端裝置上發現的可執行檔案。

  - **發佈點**。該區域提供裝置與之互動的發佈點清單。

    - **匯出至檔案**

      按一下**匯出至檔案**按鈕儲存裝置與之互動的發佈點清查檔案。預設下，應用程式匯出裝置清單到 CSV 檔案。

    - **內容**

      按一下**屬性**按鈕檢視和配置裝置與之互動的發佈點。

  - **硬體登錄資料**。在此區域，您可以檢視安裝在用戶端裝置上的硬體資訊。

    如果網路代理安裝在執行 Windows 的裝置上，它會向管理伺服器傳送有關裝置硬體的下列資訊：

    - RAM
    - 大容量儲存裝置
    - 主機板

- CPU
- 網卡
- 監視器
- 顯示卡
- 音效卡

如果網路代理安裝在執行 Linux 或 macOS 的裝置上，它會向管理伺服器傳送有關裝置硬體的下列資訊（如果該資訊由作業係統提供）：

- RAM 總容量
- 大容量儲存裝置總容量
- 主機板
- CPU
- 網卡

- **可用更新**。該區域顯示在該裝置上發現的未安裝的軟體更新清單。
- **軟體弱點**。此區域會顯示安裝在用戶端裝置上的協力廠商應用程式的弱點資訊。

  若要將弱點儲存到檔案中，請選擇要儲存之弱點旁邊的核取方塊，然後點擊「確定」，接著點擊**匯出到CSV**按鈕或**匯出到 TXT**按鈕。

  區段會包含以下設定：

  - **僅顯示可以被修復的弱點**

    如果啟用此選項，該區域會顯示可透過使用修補程式修復的弱點。

    如果停用此選項，該區域會同時顯示可透過使用修補程式修復的弱點，以及未發佈修補程式的弱點。

    預設情況下已啟用該選項。

  - **弱點內容**

    選取清單中的軟體弱點並按一下名稱，以在個別視窗中檢視所選軟體弱點的屬性。在視窗中，您可以進行以下操作：

    - 忽略此受管理裝置上的軟體弱點（在OSMP主控台中）。
    - 檢視對弱點的建議修復清單。
    - 手動指定軟體更新以修復弱點（在OSMP主控台中）。
    - 檢視弱點實例。
    - 檢視要修復弱點的現有工作清單，並建立新工作來修復弱點。

- **遠端診斷**。在本節中，您可以執行用戶端裝置的遠端診斷。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，**事件**頁簽可能會顯示所選用戶端裝置的不完整事件清單。當 DBMS 儲存大量事件時，就會發生這種情況。您可以執行下列任一操作來增加顯示的事件數目：

- 刪除不必要的事件。
- 減少不必要事件的儲存週期。

若要查看裝置的管理伺服器上記錄的事件的完整清單，請使用報告。

檢查用戶端裝置與管理伺服器之間的連線。klnagchk 公用程式

您可以透過使用 klnagchk 公用程式手動檢查連線和取得用戶端裝置與管理伺服器之間的連線設定資訊。klnagchk 公用程式位於網路代理的安裝資料夾。

使用指令提示字元時，klnagchk 公用程式可以執行以下操作（依據當時使用的指令）：

- 顯示或記錄用以連線裝置上網路代理到管理伺服器的設定值。
- 將網路代理統計資料（自上次啟動以來）和公用程式執行結果記錄在事件記錄檔案中或者顯示在螢幕上。
- 嘗試建立網路代理和管理伺服器之間的連線。

  如果連線嘗試失敗，公用程式將傳送 ICMP 封包檢查管理伺服器的裝置狀態。

要使用 klnagchk 公用程式檢查用戶端裝置和管理伺服器之間的連線，請執行以下操作：

在安裝了網路代理的裝置上，使用本機管理員帳戶從命令列啟動 klnagchk 公用程式。

公用程式的命令列語法：

```
klnagchk [-logfile <檔案名稱>] [-sp] [-savecert <憑證檔案路徑>] [-restart][-sendhb]
```

參數敘述：

- `-logfile <檔案名稱>`—將網路代理和管理伺服器之間的連線設定值以及公用程式執行結果記錄到記錄檔案中。

  預設情況下，資訊將被儲存在標準輸出流中 (stdout)。如果未使用此參數，設定、執行結果和錯誤訊息將顯示在螢幕上。

- `-sp`—顯示用於在代理伺服器上驗證使用者身分的密碼。

  如果是透過代理伺服器與管理伺服器建立連線，則需使用此金鑰。

- `-savecert <檔案名稱>`—將用於存取管理伺服器的憑證儲存到指定檔案中。
- `-restart`—公用程式執行完成後啟動網路代理。
- `-sendhb`—啟動網路代理與管理伺服器的同步。

啟動後，klnagchk 公用程式將存取網路代理的設定檔並顯示連線參數。這些參數是在網路代理安裝期間和網路代理政策設定中指定的：

- `Current device`—用戶端裝置的 Windows 網路名稱。
- `Network Agent version`—安裝在裝置上的網路代理版本完整編號（含修補程式）。
- `Server address`—管理伺服器的位址。
- `Use SSL`—指示連線到管理伺服器時是否使用安全連線的參數。
  可能的值：
  - 0 — 不使用安全連線。
  - 1— 使用安全連線。
- `Compress traffic`—指示用戶端裝置和管理伺服器之間的流量是否壓縮的參數。
- `Server SSL ports`— 使用安全連線時與管理伺服器通訊的有效連接埠數。
- `Server ports`— 使用普通連線時與管理伺服器通訊的有效連接埠號碼。
- `Use proxy server`—指示是否使用代理伺服器的參數。
  可能的值：
  - 0 — 不使用代理伺服器。
  - 1— 使用代理伺服器。
- `Address`—代理伺服器的位址和連接埠，以冒號分隔。僅當使用代理伺服器時才會顯示此參數。
- `User name`—用於存取代理伺服器的使用者名稱。僅當使用代理伺服器時才會顯示此參數。
- `Password`—用於存取代理伺服器的密碼。僅當使用代理伺服器時才會顯示此參數。若要顯示代理伺服器密碼，您需要在命令中使用`sp`金鑰。
- `Certificate`—指示用戶端裝置是否具有管理伺服器憑證的參數。例如，如果網路代理從未成功連線到管理伺服器，則憑證可能不存在。
  可能的值：
  - `not installed`—用戶端裝置沒有管理伺服器憑證。
  - `present`— 用戶端裝置具有管理伺服器憑證。
- `Open UDP port`—指示網路代理是否使用 UDP 連接埠從管理伺服器接收同步請求的參數。
  可能的值：
  - 0 — UDP 連接埠已關閉，無法接收來自管理伺服器的同步請求。
  - 1— UDP 連接埠已開啟，用來接收來自管理伺服器的同步請求。
- `UDP ports`—網路代理可使用的 UDP 連接埠號碼。

- `Location name`—裝置的網路位置。
- `State of network location`—指示用戶端裝置是否可以從一個管理伺服器連線設定檔切換到另一個設定檔的參數。

  可能的值：

  - `Enabled`—可以為用戶端裝置切換管理伺服器連線設定檔。
  - `Disabled`—無法為用戶端裝置切換管理伺服器連線設定檔。
- `Profile to use`—管理伺服器的連線設定檔。
- `Condition`—用戶端裝置所連線網路的 IP 位址和子網路遮罩。
- `Ping period, minutes`—標準同步間隔。
- `Conn timeout, s`—連線逾時。
- `RW timeout, s`—讀寫作業的連線逾時。
- `Host ID`—網路中的裝置識別碼。`Device ID`在特定管理伺服器管理的用戶端裝置中是唯一的。
- `Locations of connection gateways`—用於透過連線閘道將用戶端裝置連線到管理伺服器的參數。
- `Location of distribution points`—用於透過發佈點將用戶端裝置連線到管理伺服器的參數。
- `Connection with server`—指示連線閘道是否與管理伺服器保持持續連線的參數。此參數僅在用戶端裝置充當連線閘道時顯示。

  可能的值：

  - `active`—連線閘道與管理伺服器保持持續連線。
  - `inactive`—連線閘道未與管理伺服器保持持續連線。
- `Connection with server through connection gateway`—指示是否已透過連線閘道正確建立與管理伺服器的連線的參數。此參數僅在用戶端裝置充當連線閘道時顯示。

  可能的值：

  - `active`—已透過連線閘道正確建立與管理伺服器的連線。
  - `inactive`—未透過連線閘道正確建立與管理伺服器的連線。

此外，klnagchk 公用程式輸出可以包含以下行之一：

- `Administration Server is installed on this device`—klnagchk 公用程式在管理伺服器裝置上執行。
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`—klnagchk 公用程式在安裝網路代理的裝置上，以連線閘道模式執行。配置的連線閘道正在等待來自管理伺服器的連線，但管理伺服器未在受管理裝置中列出該裝置。您需要確保管理伺服器啟動到連線閘道的連線。
- `This device is a connection gateway`—klnagchk 公用程式在充當連線閘道的裝置上執行。
- `Acts as a distribution point`—klnagchk 公用程式在充當發佈點的裝置上執行。

klnagchk 公用程式檢查網路代理服務的狀態。如果該服務未執行，則公用程式將停止。如果服務正在執行，則公用程式會顯示以下連線統計資料：

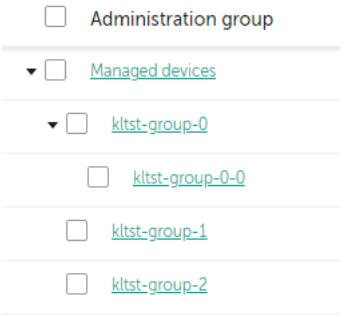
- `Ping count`—嘗試將用戶端裝置連線至管理伺服器的次數。
- `Succ. pings`—成功嘗試將用戶端裝置連線至管理伺服器的次數。
- `Sync count`—嘗試將用戶端裝置設定與管理伺服器設定同步的次數。
- `Succ. syncs`—成功嘗試將用戶端裝置設定與管理伺服器同步的次數。
- `Last ping`—上次連線的日期和時間。

分析管理伺服器與網路代理之間的連線時，您需要使用 `Ping count` 和 `Succ. pings` 參數。只有當管理伺服器設定發生變更（例如，新增工作或修改政策設定）時，用戶端裝置設定才會與管理伺服器設定同步。否則，`Ping count` 和 `Succ. pings` 參數的值會維持不變。

有關如何對網路代理程式連線到管理伺服器的問題進行故障排除的更多資訊，請參閱Open Single Management Platform常見問題解答。

建立管理群組

Kaspersky Next XDR Expert 安裝完成後，管理群組階層中只包含一個名為 **受管理裝置** 的管理群組。當建立管理群組階層架構時，您可以將裝置和虛擬機器新增到**受管理裝置**群組中，也可以新增嵌套群組（參閱下圖）。



檢視管理群組階層架構

要建立管理群組，請執行以下操作：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 在管理群組結構中，選取要加入新管理群組的管理群組。
3. 點擊**新增**。
4. 在開啟的**新管理群組名稱**視窗中，輸入群組名稱，然後點擊**新增**按鈕。

管理群組階層中將顯示帶有指定名稱的新管理群組。

要建立管理群組的架構：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 點擊**匯入**。

新管理群組架構精靈啟動。遵照精靈的說明。

裝置移動規則

建議您，將裝置設定為透過*裝置移動規則*自動指派到管理群組。裝置移動規則由三個主要部分組成：名稱、執行條件（裝置內容邏輯表達）和目的管理群組。如果裝置內容滿足規則執行條件，則規則移動裝置到目的管理群組。

所有裝置移動規則都有優先順序。管理伺服器檢查裝置內容以檢視它們是否滿足每條規則的執行條件（昇冪優先順序）。如果裝置內容滿足某條規則的執行條件，裝置被移動到目的群組，至此規則處理在該裝置上完成。如果裝置內容滿足多個規則的條件，裝置被移動到具有高優先順序的規則的目的群組。

裝置移動規則可以被間接建立。例如，在安裝套件或遠端安裝工作的內容中，您可以指定安裝網路代理後裝置必須被移動到的管理群組。此外，Kaspersky Next XDR Expert 管理員也可以在 **資產管理 → 移動規則**區段中明確建立裝置移動規則。

預設下，裝置移動規則用於裝置到管理群組的一次性初始分配。規則僅移動未配置的裝置群組的裝置一次。一旦裝置被該規則移動，該規則不會再次移動該裝置，即便您把裝置手動放回未配置裝置群組。這是應用移動規則的建議方法。

您可以移動已經被分配的裝置到一些管理群組。要這麼做，請在規則的內容中，不要勾選**僅移動不屬於任何管理群組的裝置**核取方塊。

應用移動規則到已經分配到一些管理群組中的裝置會顯著增加管理伺服器負載。

僅移動不屬於任何管理群組的裝置"核取方塊在自動建立的移動規則的屬性中被鎖定。當您新增*遠端安裝應用程式*工作或建立獨立安裝套件時，會建立此類規則。

您可以建立重複影響單一裝置的移動規則。

我們強烈建議您避免從一個群組重複移動單一裝置到另一個群組（例如，為了套用特別政策到該裝置，執行特別群組工作，或者透過特別發佈點更新裝置）。

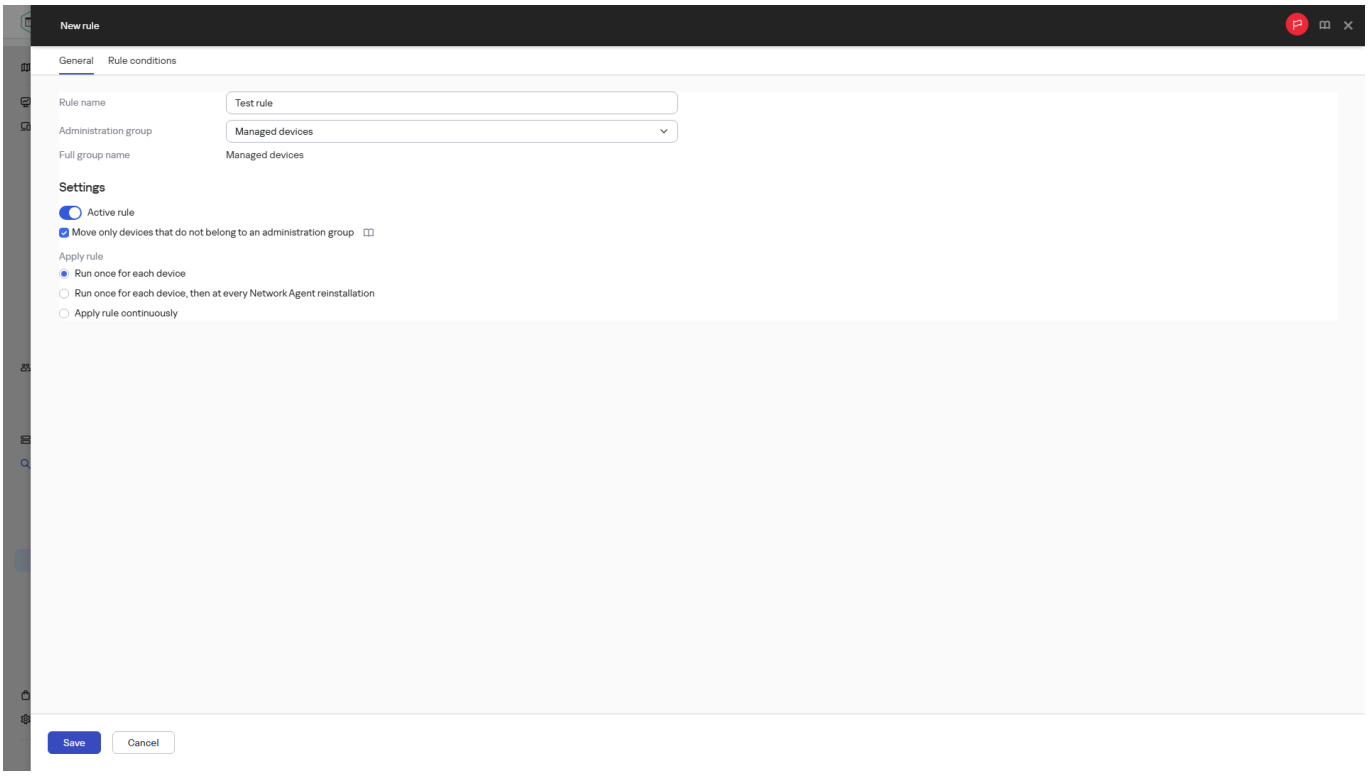
不支援此類應用情境，因為它們顯著增加了管理伺服器負載和網路流量。這些應用情境也與 Kaspersky Next XDR Expert 的運作原則衝突（尤其是在存取權限、事件和報告方面）。必須找到其他解決方案，例如，透過使用政策設定檔、裝置分類的工作、根據標準應用情境分配網路代理。

建立裝置移動規則

您可以設定裝置移動規則，即自動分配裝置到管理群組的規則。

要建立移動規則：

1. 在主功能表中，轉至 **資產管理** → **移動規則**。
2. 點擊**新增**。**新規則** 視窗隨即開啟。



建立新的移動規則

3. 在開啟的視窗中，在**一般**頁籤指定以下資訊：

- **規則名稱**

  輸入新規則名稱。

  如果您正複製規則，新規則與來源規則名稱相同，但是索引格式（ ）被新增到名稱，例如：（1）。

- **管理群組**

  選取要自動移動裝置的管理群組。

- **啟動的規則**

  如果啟用該選項，規則被啟用並在被儲存後開始工作。

  如果停用該選項，規則被建立，但不被啟用。直到您啟用該選項它才工作。

- **優先順序**

  您可以指定移動規則的優先順序。最高優先等級為1。**優先順序**值越大，規則的優先順序及其在清單中的位置就越低。

  如果未指派優先等級，則規則將被指派最低優先等級。

  複製規則時，規則副本將被指派原始規則的優先等級。然後，原始規則的優先等級將提升1。

- **僅移動不屬於任何管理群組的裝置**

  如果啟用該選項，僅未配置的裝置將被移動到所選群組。

如果停用該選項，已經屬於其他管理群組的裝置以及未配置的裝置將被移動到所選群組。

- **套用規則**

  您可以選取以下選項之一：

  - **對每台裝置執行一次**
    規則對比對標準的每台裝置套用一次。

  - **對每台裝置執行一次，然後在每次網路代理重新安裝時執行**
    規則對比對標準的每台裝置套用一次，然後僅在網路代理被重新安裝到這些裝置時。

  - **持續套用規則**
    規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

4. 在**規則條件**頁簽上，指定至少一個標準，裝置將根據該標準被移至管理群組。

5. 點擊**儲存**。

移動規則被建立。它顯示在移動規則清單。

位置在清單中越高，規則的優先順序越高。

若要修改移動規則的優先等級：

1. 在主功能表中，轉至 **資產管理 → 移動規則**。

2. 在移動規則清單中，選取要變更優先等級的移動規則旁的核取方塊。

3. 執行以下操作之一：

   - 按一下**變更優先順序**按鈕，然後在開啟的視窗中指定新的優先等級。

   - 點選**向上移動**或**向下移動**按鈕，即可在清單中上下移動規則。

4. 點擊**儲存**按鈕。

> 如果選擇**持續套用規則**選項，無論優先順序設定為何都會套用移動規則。此類規則係根據管理伺服器自動設定的時間表來套用。

如果裝置內容滿足多個規則的條件，裝置被移動到具有高優先順序的規則的目的群組。

複製裝置移動規則

您可以複製移動規則，例如，如果您要對不同目標管理群組擁有幾個相同規則。

要複製現有移動規則：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **資產管理 → 移動規則**。
   - 在主功能表中，轉至 **發現和佈署 → 佈署和指派 → 移動規則**。

   移動規則清單被顯示。

2. 選取您要複製的規則旁邊的核取方塊。
3. 點擊**複製**。
4. 在開啟的視窗中，變更在**一般**頁籤的以下資訊，若您緊要複製規則而不改變其設定，請不要進行任何變更：

   - **規則名稱**

     輸入新規則名稱。
     如果您正複製規則，新規則與來源規則名稱相同，但是索引格式（ ）被新增到名稱，例如：（1）。

   - **管理群組**

     選取要自動移動裝置的管理群組。

   - **啟動的規則**

     如果啟用該選項，規則被啟用並在被儲存後開始工作。
     如果停用該選項，規則被建立，但不被啟用。直到您啟用該選項它才工作。

   - **優先順序**

     您可以指定移動規則的優先順序。最高優先等級為1。**優先順序**值越大，規則的優先順序及其在清單中的位置就越低。

     如果未指派優先等級，則規則將被指派最低優先等級。

     複製規則時，規則副本將被指派原始規則的優先等級。然後，原始規則的優先等級將提升1。

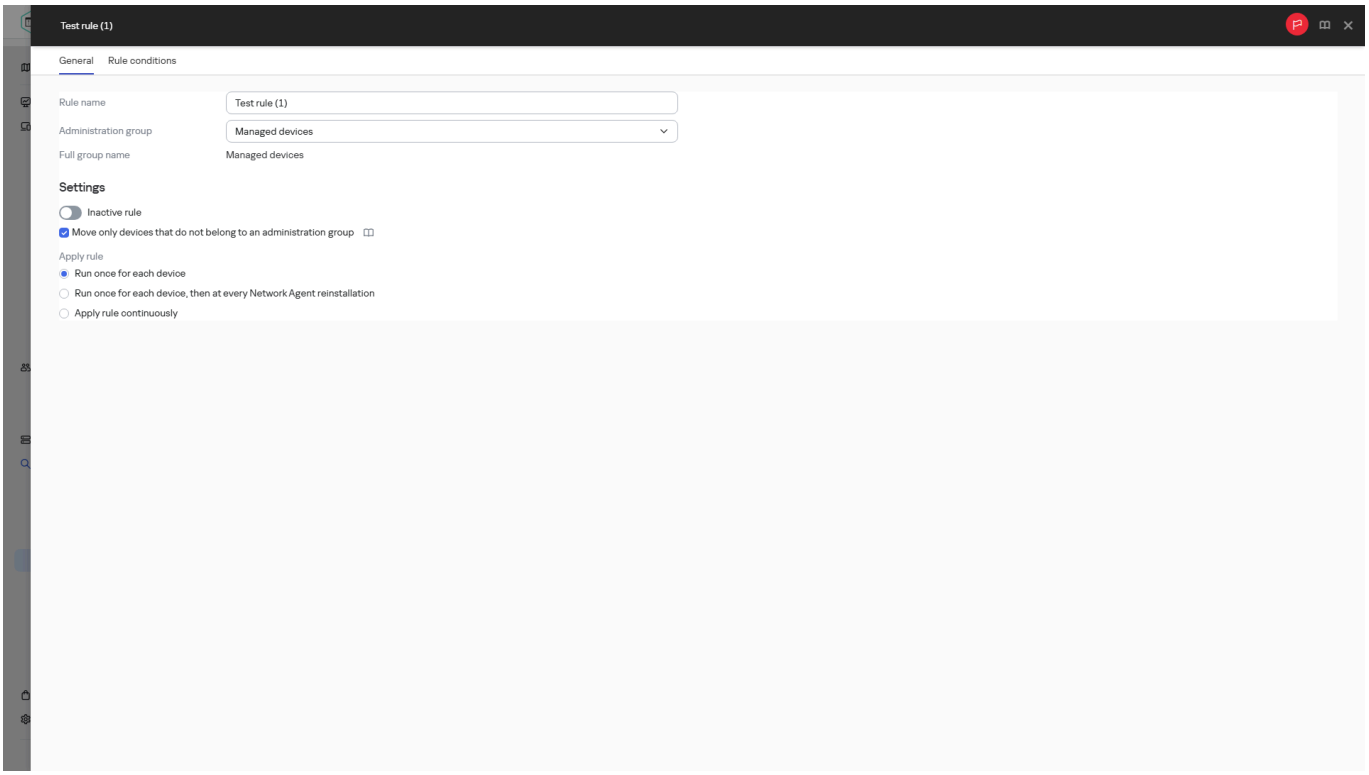
   - **僅移動不屬於任何管理群組的裝置**

     如果啟用該選項，僅未配置的裝置將被移動到所選群組。
     如果停用該選項，已經屬於其他管理群組的裝置以及未配置的裝置將被移動到所選群組。

   - **套用規則**

     您可以選取以下選項之一：

     - **對每台裝置執行一次**
       規則對比對標準的每台裝置套用一次。
     - **對每台裝置執行一次，然後在每次網路代理重新安裝時執行**
       規則對比對標準的每台裝置套用一次，然後僅在網路代理被重新安裝到這些裝置時。
     - **持續套用規則**
       規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。



裝置移動規則的屬性

5. 在**規則條件**標籤上，為要自動移動的裝置指定至少一個條件。

6. 點擊**儲存**。

新移動規則被建立。它顯示在移動規則清單。

裝置移動規則的條件

當您建立或複製將用戶端裝置移動到管理群組的規則時，在**規則條件**頁籤上，設定移動裝置的條件。如要確定要移動哪些裝置，您可以使用以下標準：

- 分配給用戶端裝置的標籤。
- 網路參數。例如，您可以移動具有指定範圍內 IP 位址的裝置。
- 裝置所有者、其角色及安全性群組成員資格。
- 安裝在用戶端裝置上的受管應用程式，例如網路代理或管理伺服器。
- 虛擬機，即用戶端裝置。
- 網域控制站組織單位。
- 雲端區段。

下面，您可以找到有關如何在裝置移動規則中指定此資訊的描述。

如果您在規則中指定了多個條件，則 AND 邏輯運算子起作用並且所有條件同時套用。如果您不選擇任何選項或將某些欄位留空，則此類條件不套用。

標籤標籤

在此標籤上，您可以基於先前新增到受管理裝置的裝置標籤設定裝置移動規則。為此，請選擇所需的標籤。此外，您可以啟用以下選項：

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，則具有指定標籤的所有裝置都將被從裝置移動規則中排除。如果停用此選項，則裝置移動規則套用到具有所有選定標籤的裝置。

  預設情況下已停用該選項。

- **如果有至少一個指定的標籤符合則套用**

  如果啟用此選項，則裝置移動規則將套用到具有至少一個選定標籤的用戶端裝置。如果停用此選項，則裝置移動規則套用到具有所有選定標籤的裝置。

  預設情況下已停用該選項。

網路標籤

在此頁簽上，您可以指定裝置移動規則要考慮的裝置的網路資料：

- **Windows 網路中的裝置名稱**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **Windows 網域**

  裝置移動規則會套用於指定 Windows 網域中包含的所有裝置。

- **裝置的 DNS 名稱**

  您要移動的用戶端裝置的 DNS 網域名稱。如果您的網路包含 DNS 伺服器，請填寫此欄位。

  > 如果為您用於Open Single Management Platform的資料庫設定了區分大小寫的排序規則，請在指定裝置DNS名稱時保持大小寫。否則，裝置移動規則將不起作用。

- **DNS 網域**

  裝置移動規則套用於指定主 DNS 後綴中包括的所有裝置。如果您的網路包含 DNS 伺服器，請填寫此欄位。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。

  預設情況下已停用該選項。

- **用於連線管理伺服器的 IP 位址**

  如果啟用此選項，您可以設定用戶端裝置連線到管理伺服器的 IP 地址。為此，請指定包括所有必要 IP 位址的 IP 範圍。

  預設情況下已停用該選項。

- **裝置在網域群組的子群組中**

  如果啟用此選項，您可以選取網域群組的子群組。相關裝置必須位於選取的子群組中。

  預設情況下已停用該選項。

- **裝置在 IP 範圍中**

  如果啟用此選項，您可以選擇先前在**IP 範圍**部分新增的IP範圍。相關裝置必須包含在所選的 IP 範圍內。
  預設情況下已停用該選項。

- **連線設定檔已變更**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅套用於連線設定檔已變更的用戶端裝置。
  - **否**。裝置移動規則僅套用於連線設定檔未變更的用戶端裝置。
  - **未選取值**。該條件不適用。

- **由不同管理伺服器管理**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅套用於由其他管理伺服器管理的用戶端裝置。這些伺服器與您配置裝置移動規則的伺服器不同。
  - **否**。裝置移動規則僅套用於由目前管理伺服器管理的用戶端裝置。
  - **未選取值**。該條件不適用。

裝置所有者頁籤

在此頁籤上，您可以根據裝置所有者、安全群組成員資格和角色設定裝置移動規則：

- **裝置所有者**

  從內部安全群組中選擇裝置所有者的使用者名稱。在本節中了解有關使用者和使用者角色的更多資訊。

  > 最多只能有一名使用者註冊為裝置所有者。

- **裝置所有者列入 Active Directory 安全群組**

  選擇裝置所有者所屬的外部 Active Directory 安全群組。

  > 使用者可以是 Active Directory 安全群組的一部分，也可以是此 Active Directory 安全群組中包含的群組的一部分。

- **裝置所有者角色**

  選擇裝置所有者的指派角色。在本文中了解有關使用者角色的更多資訊。

- **裝置所有者在內部安全群組中之成員資格**

  選擇裝置所有者所屬的內部安全群組。

應用程式標籤

在此頁籤上，您可以根據用戶端裝置上安裝的受管應用程式和作業系統設定裝置移動規則：

- **網路代理已安裝**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅適用於安裝了網路代理的用戶端裝置。
  - **否**。裝置移動規則僅適用於未安裝網路代理的用戶端裝置。
  - **未選取值**。該條件不適用。

- **應用程式**

  指定應在用戶端裝置上安裝哪些受管應用程式，以便裝置移動規則套用於這些裝置。例如，您可以選擇**卡巴斯基安全管理中心 16.3 網路代理**或**卡巴斯基安全管理中心 16.3 管理伺服器**。

  如果您不選擇任何受管應用程式，則該條件不適用。

- **作業系統版本**

  您可以根據作業系統版本剔除用戶端裝置。為此，請指定應安裝在用戶端裝置上的作業系統。因此，裝置移動規則將套用到具有所選作業系統的用戶端裝置。

  如果您不啟用此選項，則條件不適用。預設情況下已停用該選項。

- **作業系統架構**

  您可以透過作業系統位元大小來剔除用戶端裝置。在**作業系統架構**欄位，您可以選擇以下一個值：

  - **未知**
  - **x86**
  - **AMD64**
  - **IA64**

  要檢查用戶端裝置的作業系統位元大小：

  1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
  2. 按一下右側的設定圖示 (⚙)。
  3. 選擇**作業系統架構**選項，然後點擊**儲存**按鈕。

     之後，將顯示每個受管理裝置的作業系統位元大小。

- **作業系統套件管理程序**

  您可以透過作業系統套件管理器來剔除用戶端裝置。在**作業系統套件管理程序**欄位，您可以選擇以下一個值：

  - rpm - 適用於運行Red Hat Enterprise Linux、CentOS、Fedora、SUSE、Oracle Linux作業系統的裝置
  - apt (dpkg) - 適用於運行Debian、 Ubuntu、Kali作業系統的裝置
  - pkg - 適用於運行FreeBSD、OpenBSD作業系統的裝置

  若要檢查用戶端裝置的作業系統套件管理器：

  1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
  2. 點擊右側的**列設定**按鈕（ ）。
  3. 選擇**作業系統套件管理程序**選項，然後按一下**儲存**按鈕。

     每個受管理裝置都會顯示作業系統套件管理器。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（格式為*X.Y*），這將決定將移動規則套用至裝置的方式。預設情況下，不指定版本值。

- **使用者憑證**

  您可以選取以下值之一：

  - **已安裝**。裝置移動規則僅套用到具有行動憑證的行動裝置。
  - **未安裝**.裝置移動規則僅套用到沒有行動憑證的行動裝置。
  - **未選取值**。該條件不適用。

- **作業系統組建版本**

  該設定僅套用到 Windows 作業系統。

  您可以指定所選作業系統是否必須具有相等、更早或更晚的發行版本號。您也可以設定對所有版本號的裝置移動規則，除了指定的版本號。

- **作業系統發佈號**

  該設定僅套用到 Windows 作業系統。

  您可以指定所選作業系統是否必須具有相等、更早或更晚的發行版本號。您也可以設定對所有版本號的裝置移動規則，除了指定的版本號。

虛擬機頁簽

在此頁籤上，您可以根據用戶端是否是虛擬機或虛擬桌面基礎設施 (VDI) 的一部分來設定裝置移動規則：

- **這是一台虛擬機**

  在該下拉清單中，您可以選取以下一個值：

  - **N/A**。該條件不適用。
  - **否**。移動不是虛擬機的裝置。
  - **是**。移動是虛擬機的裝置。

- **虛擬機類型**
- **虛擬桌面基礎架構的一部分**

  在該下拉清單中，您可以選取以下一個值：

  - **N/A**。該條件不適用。
  - **否**。移動不屬於 VDI 的裝置。
  - **是**。移動屬於 VDI 的裝置。

網域控制器頁簽

在此頁籤上，您可以指定必須移動網域組織單元中包含的裝置。您還可以從指定網域組織單元的所有下級組織單元移動裝置：

- **裝置包括在以下組織單元中**

  如果啟用此選項，則裝置移動規則將套用於該選項下清單中指定網域控制器組織單元中的裝置。
  預設情況下已停用該選項。

- **包括子組織單元**

  如果啟用此選項，選取範圍將包括指定網域控制器組織單元的所有子組織單元中的裝置。
  預設情況下已停用該選項。

- **將裝置從子單元移動到對應子群組**
- **建立對應於新偵測到裝置的容器的子群組**
- **刪除網域中不存在的子群組**
- **裝置包括在以下網域安全群組中**

  如果啟用此選項，裝置移動規則將套用於該選項下清單中指定安全群組中的裝置。
  預設情況下已停用該選項。

雲端區段頁簽

在此索引標籤上，您可以指定必須移動雲端區段中包含的裝置。您還可以從指定網域組織單元的所有下級組織單元移動裝置：

- **裝置在雲端區段中**

  如果選擇此選項，則裝置移動規則將套用於屬於雲端區段的用戶端裝置。您可以在選項下的清單中選擇所需的雲端區段，甚至選擇子網路。

  預設情況下已停用該選項。

- **包含子物件**

  如果啟用此選項，選取範圍將包括指定雲端區段之所有子組織單元中的裝置。

  預設情況下已停用該選項。

- **從嵌套物件移動裝置到對應子群組**
- **建立對應於新偵測到裝置的容器的子群組**
- **刪除在雲端區段中未找到比對的子群組**
- **使用 API 發現的裝置**

  在該下拉清單中，您可以選取以下一個值：

  - 未選取值。該條件不適用。
  - **否**。移動未使用 API 發現的裝置。
  - **AWS**。移動使用 AWS API 發現的裝置。
  - **Azure**。移動使用 Azure API 發現的裝置。
  - **Google Cloud**。移動使用 Google Cloud API 發現的裝置。

  之後，根據選取的值，您可以填寫以下欄位：

  - **雲端裝置子網路**。
  - **雲端裝置可用區域**。
  - **雲端裝置放置群組**。

將裝置手動新增至管理群組

您可用下列方式將裝置自動移至管理群組：建立裝置移動規則、手動將裝置從某一管理群組移至另一個，或將裝置新增至選取的管理群組。下節說明如何手動將裝置新增至管理群組。

新增一或多個裝置至選取的管理群組：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
2. 選擇您要向其新增裝置的管理群組：
   - 對於根群組：
     在這種情況下，您可以繼續執行下一步。
   - 對於子群組：
     a. 點擊頁面頂部的**顯示階層**按鈕。
     按鈕名稱將變更為**隱藏階層**。
     b. 在開啟的視窗中，按一下子群組的名稱。

   所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。
3. 點擊**新增裝置**按鈕。
   行動裝置精靈啟動。
4. 列出您希望新增裝置的管理群組。

   > 您只可新增建立裝置時或裝置發現後已將資訊新增至管理伺服器資料庫的裝置。

   選取您希望將裝置新增至清單的方式：
   - 點擊**新增裝置**按鈕，接著以下列其中一種方式指定裝置：
     - 從管理伺服器偵測到的裝置清單中選取該裝置。
     - 指定裝置 IP 位址或 IP 範圍。

       > IP位址範圍不得超過1,048,576個位址。

     - 指定裝置 DNS 名稱。

       > 裝置名稱欄位不得包含空格、退格鍵，以及以下禁用字元：: , \ / * ‘ “ ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
   - 點擊**從檔案匯入裝置**按鈕以從 .txt 檔案匯入裝置清單。各裝置位址或名稱均需在獨立的資料行中指定。

     > 檔案不得包含空格、退格鍵，以及以下停用字元：: , \ / * ‘ “ ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

5. 檢視要新增至管理群組的裝置清單。您可新增或移除裝置來編輯清單。

6. 確認清單正確後，請點擊**下一步**按鈕。

精靈會處理裝置清單並顯示結果。系統會將已成功處理的裝置新增至管理群組，並顯示在管理伺服器產生的名稱下的裝置清單中。

將裝置或者叢集手動移動至管理群組

您可將裝置從一個管理群組移至另一個，或從未配置的裝置群組移至另一個管理群組。

您還可以將叢集或伺服器陣列從一個管理群組移動到另一個管理群組。當您將叢集或伺服器陣列移動到另一個群組時，其所有節點都會隨之移動，因為叢集及其任何節點始終屬於同一管理群組。當您在**裝置**頁簽上選擇單個叢集節點時，**移至群組**按鈕將變得不可用。

要把一台或多台裝置或者叢集移動至一個選定的管理群組中，請執行以下操作：

1. 從您要移動裝置的位置開啟管理群組。若要執行此操作，請採取下列其中一種做法：

   - 若要開啟管理群組，請在主功能表中前往**資產管理→資產（裝置）**，然後選擇所需的管理群組。

     - 對於根群組，您可以繼續下一步。

     - 對於子群組，請按一下頁面頂部的**顯示階層**按鈕，然後在開啟的視窗中選擇所需的管理群組。

   - 若要開啟**未指派的裝置**群組，請在主功能表中，轉至**資產管理→未指派的裝置**。

2. 如果管理群組包含叢集或伺服器陣列，則**資產（裝置）**部分將分為兩個頁簽：**裝置**頁簽以及**叢集和伺服器陣列**頁簽。開啟要移動的物件的頁簽。

3. 選取您要移至不同群組之裝置或者叢集旁的核取方塊。

4. 點擊**移至群組**按鈕。

5. 在管理群組階層中，選取您要將選取的裝置或者叢集移至管理群組旁的核取方塊。

6. 點擊**移動**按鈕。

選取的裝置或者叢集會移至選取的管理群組。

關於叢集和伺服器陣列

Kaspersky Next XDR Expert 支援叢集技術。如果網路代理向管理伺服器傳送資訊確認組成伺服器陣列的用戶端裝置上已安裝該應用程式，則該用戶端裝置就成為一個叢集節點。

如果管理群組包含叢集或伺服器陣列，則**資產（裝置）**頁面將顯示兩個頁簽：一個用於單個裝置，另一個用於叢集和伺服器陣列。受管理裝置被偵測為叢集節點後，叢集將作為單獨物件被新增到**叢集和伺服器陣列**頁簽中。

叢集或伺服器陣列節點與其他受管理裝置一起列在**裝置**頁簽上。您可以將節點作為單個裝置檢視屬性並執行其他操作，但不能刪除叢集節點或將其從叢集中單獨移動到另一個管理群組。您只能刪除或移動整個叢集。

您可以對叢集或伺服器陣列執行以下操作：

- 檢視屬性
- 將叢集或伺服器陣列移至另一個管理群組

  當您將叢集或伺服器陣列移動到另一個群組時，其所有節點都會隨之移動，因為叢集及其任何節點始終屬於同一管理群組。

- 刪除

  僅當組織網路中不再存在叢集或伺服器陣列時，刪除該叢集或伺服器陣列才合理。如果叢集在您的網路上仍然可見，並且網路代理程式和卡巴斯基安全應用程式仍然安裝在叢集節點上，Open Single Management Platform會自動將已刪除的叢集及其節點返回到受管理裝置清單。

叢集或伺服器陣列的屬性

檢視叢集或伺服器陣列的設定：

1. 在主功能表中，轉至**資產管理 → 資產（裝置） → 叢集和伺服器陣列**。

   叢集和伺服器陣列的清單將得以顯示。

2. 點擊所需叢集或伺服器陣列的名稱。

所選叢集或伺服器陣列的屬性視窗將得以顯示。

一般

一般區域顯示有關叢集或伺服器陣列的一般資訊。資訊基於上一次叢集節點與管理伺服器之間的同步接收的資料來提供：

- **名稱**
- **描述**
- **Windows 網域**

  Windows 網域或工作群組，包含叢集或伺服器陣列。

- **NetBIOS 名稱**

  叢集或伺服器陣列的 Windows 網路名稱。

- **DNS 名稱**

  叢集或伺服器陣列的 DNS 網域名稱。

工作

在**工作**標籤中，您可以管理被分配給叢集或者伺服器陣列的工作：檢視現有工作清單；建立新工作；移除、啟動和停止工作；修改工作設定；以及檢視執行結果。列出的工作與安裝在叢集節點上的卡巴斯基安全應用程式相關。Open Single Management Platform從叢集節點接收工作清單和工作狀態詳細資訊。如果未建立連線，則不顯示狀態。

節點

此頁簽顯示叢集或伺服器陣列中包含的節點清單。您可以點擊節點名稱來檢視裝置屬性視窗。

Kaspersky 應用程式

屬性視窗還可包含其他頁簽，其中包含與叢集節點上安裝的卡巴斯基安全應用程式相關的資訊和設定。

發佈點和連線閘道器的調整

Kaspersky Next XDR Expert 中的管理群組結構執行以下功能：

- 設定政策範圍
  套用相關設定到裝置有另一種方式，透過使用*政策設定檔*。
- 設定群組工作範圍
  還有一個不基於管理群組層級定義群組工作範圍的方法：使用裝置分類的工作和特定裝置的工作。
- 設定裝置、虛擬管理伺服器和次要管理伺服器的存取權限
- 分配發佈點

當建立管理群組結構時，您必須考慮到組織網路的拓撲以便最優分配發佈點。發佈點的最優分發允許您在企業網路中儲存流量。

根據組織圖表和網路拓撲，以下標準配置可以被套用到管理群組結構：

- 單一辦公室
- 多個小遠端分辦公室

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

發佈點的標準配置：單一辦公室

在標準「單一辦公室」配置中，所有裝置都在組織網路上，因此它們能看見彼此。組織網路可能包含幾部分（網路或網段），由窄通道連線。

有以下構建管理群組結構的方法：

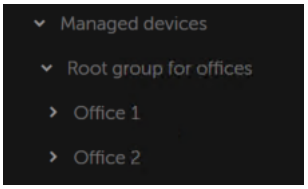
- 構建管理群組結構涉及到網路拓撲。管理群組結構可能不精確反映網路拓撲。網路各部分之間以及特定管理群組相互比對。您可以使用發佈點自動分配或手動分配它們。

- 不考慮網路拓撲而構建管理群組結構。在此情況下，您必須停用發佈點自動分配，然後為網路中每個部分的根管理群組（例如**受管理裝置**群組）分配一或多個裝置作為發佈點。所有發佈點將處於相同等級，並將掌控組織網路中所有裝置的相同範圍。此種情況下，每個網路代理將連線到具有最小路由的發佈點。發佈點的路由可以使用 tracert 公用程式偵錯。

發佈點的標準配置：多個小遠端辦公室

該標準配置用於一定數量的小型遠端辦公室，您可透過網際網路與總部通訊。每個遠端辦公室都位於 NAT 之外，就是說，從一個遠端辦公室到另一個遠端辦公室的連線是不可能的，因為辦公室是彼此隔離的。

配置必須在管理群組中體現：必須為每個遠端辦公室建立各自的管理群組（下圖中的群組**辦公室 1** 和**辦公室 2**）。



遠端辦公室包含在管理群組結構

您必須指定一或多個發佈點給一間辦公室的每個對應管理群組。發佈點必須是遠端辦公室中具有足夠剩餘磁碟空間的裝置。佈署在**辦公室 1** 群組的裝置，例如，將存取分配到**辦公室 1** 管理群組的發佈點。

如果一些使用者在辦公室之間移動他們的攜帶式電腦，您必須在遠端辦公室選取兩個或更多裝置（除了現有的發佈點）並分配它們作為等級管理群組的發佈點（上圖中**辦公室根群組**）。

例如：攜帶式電腦佈署在**辦公室 1** 管理群組，然後被移動到對應於**辦公室 2** 管理群組的辦公室。在移動攜帶式電腦後，網路代理試圖存取分配到**辦公室 1** 群組的發佈點，但是那些發佈點不可用。然後，網路代理開始嘗試存取分配到**辦公室根群組**的發佈點。因為遠端辦公室是彼此隔離的，嘗試存取分配到**辦公室根群組**管理群組的發佈點僅在網路代理嘗試存取**辦公室 2** 群組中的發佈點時才會成功。就是說，攜帶式電腦將保持在原始辦公室對應的管理群組，但是將使用它當時所在辦公室的發佈點。

計算發佈點的數量和配置

網路包含越多的用戶端裝置，就需要越多的發佈點。我們建議您停用發佈點的自動分配。當發佈點的自動分配被啟用時，如果用戶端裝置數量很大，管理伺服器就分配發佈點並定義其配置。

使用單獨分配的發佈點

如果您計畫使用特定裝置作為發佈點（就是，單獨分配的伺服器），您可以不使用發佈點的自動分配。此種情況下，確保您要分配為發佈點的裝置具有足夠的剩餘磁碟空間磁區，不定期關閉，且停用了睡眠模式。

包含一個網段的網路中，依網路裝置數量而定的專用發佈點數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 300	0（不分配發佈點）
大於 300	可接受：(N/10,000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

包含多個網段的網路中，依網路裝置數量而定的專用發佈點數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 10	0（不分配發佈點）
10–100	1
大於 100	可接受：(N/10000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

使用標準用戶端裝置（工作站）作為發佈點

如果您計畫使用標準用戶端裝置（就是，工作站）作為發佈點，我們建議您按照所示分配發佈點（參見下表），以便避免通信管道和管理伺服器超載。

網路中基於網路裝置數量作為發佈點工作的包含單一網段的工作站的數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 300	0（不分配發佈點）
大於 300	(N/300 + 1)，N 是網路裝置數量；至少有三台發佈點

網路中基於網路裝置數量作為發佈點工作的包含多個網段的工作站的數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 10	0（不分配發佈點）
10–30	1
31–300	2
大於 300	(N/300 + 1)，N 是網路裝置數量；至少有三台發佈點

如果裝置被關閉（或由於某些原因不可用），其範圍內的受管理裝置可以存取管理伺服器以更新。

自動分配發佈點

我們建議您自動指派發佈點。在此情況下，Kaspersky Next XDR Expert 將自行選擇必須指派為發佈點的裝置。

運行Microsoft Windows on Arm的裝置不能充當發佈點。

要自動分配發佈點：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 選取**自動指派發佈點**選項。

   如果自動指派裝置作為發佈點被啟用，您無法手動配置發佈點，也不能編輯發佈點清單。

4. 點擊**儲存**按鈕。

管理伺服器便自動指派和配置發佈點。

手動分配發佈點

Kaspersky Next XDR Expert 可讓您手動指派裝置作為發佈點。

我們建議您自動指派發佈點。在此情況下，Kaspersky Next XDR Expert 將自行選擇必須指派為發佈點的裝置。然後，如果您由於一些原因必須不自動指派發佈點（例如，如果您要使用單獨指派的伺服器），您可以在計算發佈點的數量和組態後手動指派。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

運行Microsoft Windows on Arm的裝置不能充當發佈點。

要手動指派裝置作為發佈點：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 選取**手動指派發佈點**選項。
4. 點選**指派**按鈕。
5. 選擇您要製作發佈點的裝置。
   選取裝置時，請牢記發佈點的操作功能以及裝置作為發佈點的需求。
6. 選擇您要包含在所選發佈點範圍的管理群組。
7. 點擊**確定**。
   您新增的發佈點將顯示在**發佈點**區域的發佈點清單。
8. 在清單中點擊新增的發佈點以開啟其內容視窗。

9. 在內容視窗中配置發佈點：

- **一般**區域中包含用於設定發佈點與用戶端裝置進行互動的設定。

  - **SSL 連接埠**

    用戶端裝置與發佈點之間，使用 SSL 進行安全連線的 SSL 埠號。

    預設埠號為 13000。

  - **已啟用**

    如果啟用此選項，程式會使用 IP 多點傳送，在群組中的各用戶端裝置上自動發佈安裝套件。

    IP 多點傳送會減少從安裝套件安裝應用程式至一組用戶端裝置的時間，但當您安裝應用程式至單一用戶端裝置時安裝時間會增加。

  - **IP 多點傳送位址**

    用於多點傳送的 IP 位址。您可以定義範圍是 224.0.0.0 – 239.255.255.255 的 IP 位址

    預設情況下，Kaspersky Next XDR Expert 會在指定範圍內自動指派唯一的 IP 多點傳送位址。

  - **IP 多點傳輸連接埠號**

    IP 多點傳輸的埠號。

    預設情況下，埠號指定為 15001。如果執行管理伺服器的裝置指定為發佈點，連接埠 13001 預設用於 SSL 連線。

  - **遠端裝置發佈點位址**

    遠端裝置連線到發佈點所用的IPv4位址。

  - **佈署更新**

    更新被從以下來源分發到受管理裝置：

    - 此發佈點（如果啟用此選項）。
    - 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

    使用發佈點來佈署更新可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以參閱計算發佈點的數量和組態，以決定網路所需的發佈點數量，進而最佳化流量和負載。

    如果停用此選項，管理伺服器上的更新下載和負載數量可能會增加。預設情況下已啟用該選項。

  - **佈署安裝套件**

    安裝套件被從以下來源分發到受管理裝置：

    - 此發佈點（如果啟用此選項）。
    - 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

    使用發佈點來佈署安裝套件可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以參閱計算發佈點的數量和組態，以決定網路所需的發佈點數量，進而最佳化流量和負載。

    如果停用此選項，管理伺服器上的安裝套件下載和負載數量可能會增加。預設情況下已啟用該選項。

- **執行推入伺服器**

  在Open Single Management Platform中，發佈點可以作為透過移動通訊協定管理之裝置和受網路代理管理之裝置的推送伺服器。例如，如果您希望能夠對 KasperskyOS 裝置與管理伺服器進行強制同步，則必須啟用推送伺服器。推送伺服器與啟用推送伺服器的發佈點具有相同的受管理裝置範圍。如果為相同管理群組指派了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

- **推入伺服器連接埠**

  推送伺服器的連接埠號。您可以指定任何未佔用連接埠的編號。

- 在**"範圍"**區域，指定發佈點將向其分發更新的管理群組。

- 在**更新來源**區域，您可以選擇發佈點的更新來源：

  - **更新來源**

    為發佈點選取更新來源：

    - 要允許發佈點從管理伺服器自動接收更新，選取**從管理伺服器接收**。

    - 若要透過工作允許發佈點接收更新，請選取 **使用更新下載工作**，然後指定一個*將更新下載到發佈點的儲存區*工作：

      - 如果裝置上已存在此類工作，請在清單中選擇該工作。

      - 如果裝置上尚不存在此類工作，請按一下**建立工作**連結以建立工作。新工作精靈啟動。遵照精靈的說明。

  - **下載差異檔案**

    該選項啟用下載 diff 檔案功能。

    預設情況下已啟用該選項。

- 如果您的發佈點在連線到網際網路時使用代理伺服器，則可以在**網際網路連線設定**子部分中指定以下設定：

  - **使用代理伺服器**

    如果選取此核取方塊，將使用網際網路代理伺服器將發佈點連線至卡巴斯基更新伺服器。您可以在輸入欄位中設定代理伺服器連線。

    預設情況下，此核取方塊已清除。

  - **代理伺服器位址**

    代理伺服器位址。

  - **埠號**

    用於連線的埠號。

  - **略過本機位址的代理伺服器**

    如果啟用此選項，則不使用代理伺服器連線本機網路的裝置。

    預設情況下已停用該選項。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

  預設情況下，此核取方塊已清除。

- **使用者名稱**

  建立連線代理伺服器的使用者帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

- 在 **KSN 代理**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發 KSN 請求：

  - **在發佈點端啟用 KSN 代理**

    KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。

    發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到Kaspersky。

    預設情況下已停用該選項。啟用該選項僅在**使用管理伺服器作為代理伺服器**和**我同意使用卡巴斯基安全網路**選項在管理伺服器內容視窗中被啟用時起作用。

    您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

  - **轉發 KSN 請求到管理伺服器**

    發佈點從受管理裝置轉發 KSN 請求到管理伺服器。

    預設情況下已啟用該選項。

  - **透過網際網路直接存取 KSN 雲端/KPSN**

    發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或 KPSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或 KPSN。

  - **當連線到 KPSN 時略過代理伺服器設定**

    若您已在發佈點內容或網路代理政策中設定代理伺服器設定，但您的網路架構要求您直接使用 KPSN，請啟用此選項。否則，從受管理應用程式的請求無法到達 KPSN。

    如果您選擇**透過網際網路直接存取 KSN 雲端/KPSN**選項，則此選項可用。

  - **連接埠**

    受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

  - **使用 UDP 連接埠**

    如果需要受管理裝置透過 UDP 連接埠連線到 KSN 代理伺服器，啟用**使用 UDP 連接埠**選項，並指定 UDP 連接埠號。預設情況下已啟用該選項。

  - **UDP 連接埠**

    受管理裝置將用於連線到 KSN 代理伺服器的 UDP 埠號。連線到 KSN 代理伺服器的預設 UDP 連接埠是 15111。

  - **使用 HTTPS**

    如果需要受管理裝置透過 HTTPS 連接埠連線到 KSN 代理伺服器，啟用**使用 HTTPS** 選項，並指定 **HTTPS 連接埠**號。連線到 KSN 代理伺服器的預設 HTTPS 連接埠是 17111。

- **HTTPS 連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 HTTPS 埠號。連線到 KSN 代理伺服器的預設 HTTPS 連接埠是 17111。

- 在**"連線閘道"**部分，您可以將發佈點配置為充當網路代理實例和管理伺服器之間連線的閘道：

  - **連線閘道**

    如果由於您的網路組織而無法在管理伺服器和網路代理之間建立直接連線，您可以使用發佈點充當管理伺服器和網路代理之間的連線閘道。

    如果您需要發佈點充當網路代理和管理伺服器之間的連線閘道，請啟用此選項。預設情況下已停用該選項。

  - **從管理伺服器建立連線到閘道（如果閘道位於 DMZ 中）**

    如果管理伺服器位於隔離區域 (DMZ) 之外，在區域網路中，則安裝在遠端裝置上的網路代理無法連線到管理伺服器。您可以使用發佈點作為具有反向連線能力的連線閘道（管理伺服器建立到發佈點的連線）。

    如果您需要將管理伺服器連線到 DMZ 中的連線閘道，請啟用此選項。

  - **為卡巴斯基安全管理中心網頁主控台開啟本機連接埠**

    如果您需要 DMZ 內的連線閘道為位於 DMZ 中或網際網路上的 Web 主控台開啟一個連接埠，請啟用此選項。指定將用於從 Web 主控台連線到發佈點的連接埠號。預設埠號為 13299。

    如果您啟用**從管理伺服器建立連線到閘道（如果閘道位於 DMZ 中）**選項，則此選項可用。

  透過充當連接閘道的發佈點將行動裝置連線到管理伺服器時，您可以啟用以下選項：

  - **為行動裝置開啟連接埠（僅管理伺服器 SSL 身分驗證）**

    如果您需要連線閘道為移動裝置開啟一個連接埠並指定行動裝置將用於連線到發佈點的連接埠號，請啟用此選項。預設埠號為 13292。行動裝置將檢查管理伺服器憑證。建立連線時，只有管理伺服器需經過身分驗證。

  - **為行動裝置開啟連接埠（雙向 SSL 身分驗證）**

    如果您需要連線閘道開啟一個將用於管理伺服器和行動裝置的雙向身分驗證的連接埠，請啟用此選項。行動裝置將檢查管理伺服器憑證，管理伺服器將檢查行動裝置憑證。指定下列設定：

    - 行動裝置將用於連線到發佈點的連接埠號。預設埠號為 13293。
    - 行動裝置將使用的連線閘道的 DNS 網域名稱。用逗號分隔網域名稱。指定的網域名稱將包含在發佈點憑證中。如果行動裝置使用的網域名稱與發佈點憑證中的一般名稱不比對，則行動裝置不會連線到發佈點。

      預設 DNS 網域名稱是連線閘道的 FQDN 名稱。

  在這兩種情況下，憑證僅在發佈點上建立 TLS 工作階段期間接受檢查。憑證不會被轉送給管理伺服器進行檢查。與行動裝置建立 TLS 工作階段後，發佈點會使用管理伺服器憑證建立行動裝置和管理伺服器之間同步的隧道。如果您開啟雙向 SSL 身分驗證連接埠，則分發行動裝置憑證的唯一方法是透過安裝套件。

- 透過Windows的發佈點設定Windows網路輪詢。

  - **Windows 網域**

    您可以啟用 Windows 網域裝置發現並為發現設定排程。

- 配置發佈點的網域控制器輪詢。
  - **網域控制器輪詢**

    您可以對網域控制器啟用裝置發現

    在**輪詢**欄位中，將切換按鈕切換到**已啟用**位置後，您可以選擇要輪詢的網域控制器，也可以為它們指定輪詢排程。

    如果您使用 Linux 發佈點，請在**輪詢指定網域**部分中點擊**新增** ，然後指定網域控制器的位址和使用者憑據。另外，您可以指定要輪詢的網域的類型：Active Directory 或 Samba、FreeIPA、ALD Pro。

    如果您使用 Windows 發佈點，則可以選擇以下選項之一：

    - **輪詢目前網域**
    - **輪詢整個網域樹系**
    - **輪詢指定網域**
- 配置發佈點對 IP 範圍的輪詢。
  - **IP 範圍輪詢**

    您可以為 IPv4 範圍和 IPv6 網路啟用裝置發現。

    如果啟用**啟用範圍輪詢**核取方塊，您可以新增掃已描範圍並為其設定排程。您可以新增 IP 範圍到已掃描範圍清單。

    如果啟用**使用 Zeroconf 來輪詢 IPv6 網路**選項，發佈點將使用零配置網路（也稱為"*Zeroconf*"）自動輪詢 IPv6 網路。在這種情況下，指定的 IP 範圍將被忽略，因為發佈點會輪詢整個網路。如果發佈點執行 Linux，則**使用 Zeroconf 來輪詢 IPv6 網路**選項可用。要使用 Zeroconf IPv6 輪詢，您必須在發佈點上安裝 avahi-browse 公用程式。
- 在**進階**區域，指定發佈點必須使用以儲存發佈資料的資料夾。
  - **使用預設的資料夾**

    如果您選取此選項，應用程式使用發佈點上的網路代理安裝資料夾。
  - **使用指定的資料夾**

    如果您選取該選項，則可以在下面的欄位中指定該資料夾的路徑。它可以是發佈點上的本機資料夾，也可以是企業網路上任何裝置的資料夾。

    發佈點上用於執行網路代理的帳戶必須具有對指定資料夾的存取權限以進行讀寫操作。

10. 點擊**確定**。

所選裝置作為發佈點執行。

修改管理群組的發佈點清單

您可以檢視為特定管理群組分配的發佈點清單並透過新增或刪除發佈點來修改清單。

要檢視和修改分配給管理群組的發佈點清單：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
2. 透過點擊頁面頂部的**顯示階層**按鈕選擇要檢視其指派的發佈點的管理群組，然後在開啟的視窗中按一下所需群組的名稱。

   這將啟用**發佈點**功能表項。

   所選群組的路徑將顯示在頁面頂部。如果需要，您可以在此路徑中按一下帶有管理群組名稱的連結前往該群組。預設情況下，路徑中的最後一個連結不活動。
3. 在主功能表中，轉至 **資產管理 → 發佈點**。
4. 要為管理群組新增新的發佈點，請點擊**指派**按鈕。
5. 要刪除分配的發佈點，請從清單中選擇裝置並點擊**取消指派**按鈕。

根據於您的修改，新發佈點被新增到清單或現有發佈點被從清單刪除。

啟用推送伺服器

在Open Single Management Platform中，發佈點可以作為透過移動通訊協定管理之裝置和受網路代理管理之裝置的推送伺服器。例如，如果您希望能夠對 KasperskyOS 裝置與管理伺服器進行強制同步，則必須啟用推送伺服器。推送伺服器與啟用推送伺服器的發佈點具有相同的受管理裝置範圍。如果為相同管理群組指派了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

您可能希望將發佈點用作推送伺服器，以確保受管理裝置和管理伺服器之間存在持續連線。某些操作需要持續連線，例如執行和停止本機工作、接收受管理應用程式的統計資訊或建立隧道。如果您將發佈點用作推送伺服器，就不必在受管理裝置上使用**不要中斷與管理伺服器的連線**選項，也不必將封包傳送至網路代理的 UDP 連接埠。

推送伺服器支援負載最多 50,000 個同時連線。

要在發佈點上啟用推入伺服器：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊要在其上啟用推入伺服器的發佈點的名稱。

   發佈點內容視窗將開啟。
4. 在**一般**區段上啟用**已啟用**選項。
5. 在 **推入伺服器連接埠** 欄位中，鍵入連接埠編號。您可以指定任何未佔用連接埠的編號。
6. 在 **遠端主機位址** 欄位中，指定發佈點裝置的 IP 位址或名稱。
7. 點擊**確定**。

推入伺服器將在所選發佈點上啟用。

關於裝置狀態

Kaspersky Next XDR Expert 會為每個受管理裝置指派一個狀態。特定狀態會根據是否符合使用者定義的條件而指派。在某些情況下，Kaspersky Next XDR Expert 會在為裝置指派狀態時，將裝置在網路上的可見性旗標納入考量（請參閱下表）。如果 Kaspersky Next XDR Expert 在兩小時內未於網路上找到裝置，該裝置的可見性旗標會設為*不可見*。

這些狀態如下：

- *緊急*或*緊急/可見*
- *警告*或*警告/可見*
- *正常*或*正常/可見*

下表列出在指派給裝置的*緊急*或*警告*狀態時必須符合的預設條件，其中包含所有可能的值。

分配狀態到裝置的條件

條件	條件敘述	可用值
安全應用程式未安裝	網路代理已安裝到裝置，但是安全應用程式未安裝。	• 開關按鈕被開啟。 • 開關按鈕被關閉。
偵測到太多病毒	一些病毒被病毒偵測工作在裝置上發現，例如，惡意軟體掃描工作，且發現的病毒數量超過指定值。	大於 0。
即時保護等級不符合管理員設定的等級	裝置在網路中可見，但即時防護等級與管理員在裝置狀態條件中設定的等級不同。	• 已停止。 • 暫停。 • 執行中。
惡意軟體掃描已長時間未執行	裝置在網路中可見且安全應用程式已安裝到裝置，但*惡意軟體掃描*工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於 1 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於 1 天。
偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。

條件	條件敘述	可用值
自重新啟動以來需要的時間	裝置在網路上可見，但應用程式要求重新啟動的時間已超過指定時間間隔。	多於 0 分鐘。
重新啟動的原因	裝置在網路上可見，但應用程式因所選原因之一需要重新啟動裝置。	• 未知原因 • 應用程式在重新啟動前不會執行 • 需要重新啟動以完成更新；應用程式正在執行 • 需要重新啟動以啟動更新 • 需要重新啟動以完成掃描或解毒 • 需要重新啟動以完成遠端安裝/移除 • 即將完成磁碟的資料加密
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到軟體弱點	裝置在網路中可見且網路代理已安裝到裝置，但*弱點掃描和所需更新*工作在裝置應用程式中偵測到指定嚴重等級的弱點。	• 嚴重 • 高。 • 中等。 • 如果弱點無法被修補則略過。 • 如果為安裝分配了更新則略過。
產品授權已到期	裝置在網路中可見，但產品授權已過期。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
產品授權即將到期	裝置在網路中可見，但裝置上的產品授權即將在指定天數內過期。	少於 0 天。
Windows Update 更新檢查已長時間未執行	裝置在網路中可見，但*尋找弱點和所需更新*工作未在指定時間段內未執行。	多於 1 天。
無效的加密狀態	網路代理已安裝到裝置，但裝置加密結果等於指定值。	• 由於使用者拒絕未遵從政策（僅對外部裝置）。 • 由於錯誤未遵從政策。 • 套用政策時需要重新啟動。 • 未指定加密政策。 • 不支援。 • 當套用政策時。
行動裝置設定與政策不同	行動裝置設定不同於 Kaspersky Endpoint Security for Android 政策中指定的設定。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到未處理的安全問題	裝置上發現了一些未處理的安全問題。安全問題可以透過安裝在使用者端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB。
裝置已不受管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。 在這種情況下，安全應用程式的狀態為*stopped*或*failure*，不同於下列狀態：*starting*、*running*或*suspended*。	多於 0 分鐘。
安全應用程式沒有執行	裝置在網路中可見且安全應用程式已安裝到裝置，但其未在執行。	• 開關按鈕被關閉。 • 開關按鈕被開啟。

Kaspersky Next XDR Expert 可讓您設定在符合指定條件時，自動切換管理群組中裝置的狀態。當滿足指定條件時，用戶端裝置會被分配以下狀態之一：*緊急*或*警告*。當不滿足指定條件時，用戶端裝置會被分配*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，預設情況下，若**資料庫已過期**條件的值為**多於 3 天**，則用戶端裝置會被指派*警告*狀態；若值為**多於 7 天**，則會被指派*緊急*狀態。

當 Kaspersky Next XDR Expert 為裝置指派狀態時，對於某些條件（請參閱上表中的「條件說明」欄），會將可見性標記納入考量。例如，若受管理裝置因符合資料庫已過期條件而被指派*緊急*狀態，之後能見度標記也已針對該裝置設定，則裝置會被指派*正常*狀態。

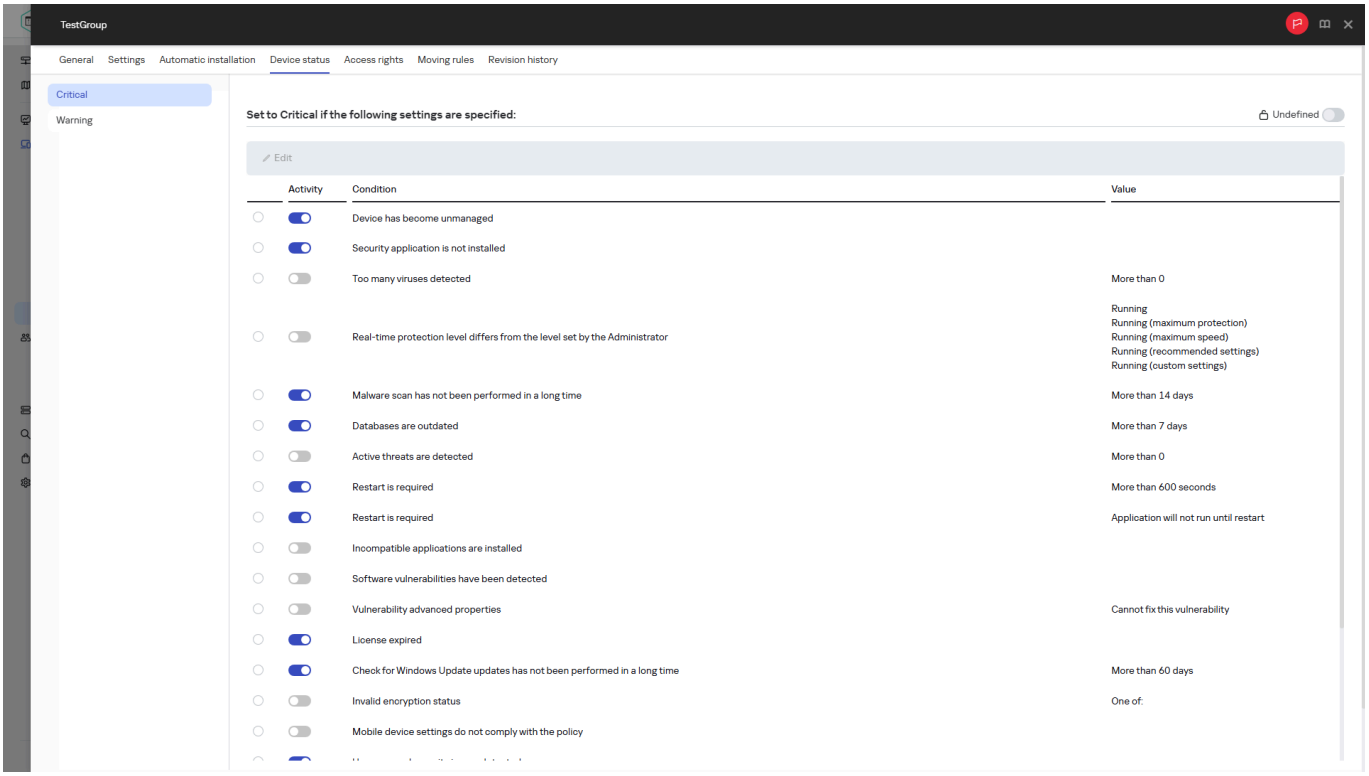
設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 透過以下方式之一，前往要變更切換裝置狀態的管理群組內容：
   - 點擊管理群組的名稱。
   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。

   管理群組內容視窗將開啟。
3. 在屬性視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**緊急**。
5. 在右方窗格中的**如果指定了以下設定，則設定為「緊急」**區段，啟用將裝置切換為*緊急*狀態的條件。



然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。
10. 按一下**儲存**以儲存變更。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**警告**。
5. 在右方窗格中的**如果指定了以下設定則設定為「警告」**區段，啟用將裝置切換為*警告*狀態的條件。

然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。
10. 按一下**儲存**以儲存變更。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

裝置分類

*裝置分類*是根據特定條件篩選裝置的工具。您可以使用裝置分類管理幾個裝置：例如，檢視僅檢視這些裝置的報告或移動所有這些裝置到其他群組。

Open Single Management Platform提供一系列的*預設選項*（例如，**處於「緊急」狀態的裝置**、**防護已停用**、**偵測到活動威脅**）。預先定義分類無法被刪除。您也可以建立和配置附加*使用者定義分類*。

在使用者定義分類中，您可以設定搜尋範圍並選取所有裝置、受管理裝置、或者未配置的裝置。搜尋參數在條件中指定。在裝置分類中，您可以建立帶有不同搜尋參數的多個條件。例如，您可以建立兩個條件並指定不同的 IP 範圍。如果多個條件被指定，分類顯示滿足任意條件的裝置。相比之下，條件中的搜尋參數是附加的。如果 IP 範圍和已安裝應用程式名稱都被指定在一個條件，僅安裝了應用程式且 IP 位址處於指定範圍的裝置被顯示。

從裝置分類中檢視裝置清單

Open Single Management Platform允許您從裝置分類中檢視裝置清單。

從裝置分類中檢視裝置清單：

1. 在主功能表中，轉到**資產管理 → 裝置分類** or **發現和佈署 → 裝置分類**區域。
2. 在選項清單中，按一下裝置分類的名稱。
   該頁面會顯示一個表格，其中包含有關裝置分類中包含的裝置的資訊。
3. 您可以按如下方式對裝置表格資料進行分組和篩選：
   - 點擊設定圖示 ( )，然後選擇要在表中顯示的列。
   - 點擊篩選圖示 ( ), 然後在喚起的功能表中指定並套用篩選條件。
     顯示篩選後的裝置表格。

您可以在裝置分類中選擇一個或多個裝置，然後點擊**新工作**按鈕以建立將套用於這些裝置的工作。

要將裝置分類中的選定裝置移動到另一個管理群組，請點擊**移至群組**按鈕，然後選擇目標管理群組。

建立裝置分類

要建立裝置分類，請執行以下操作：

1. 在主功能表中，轉至 **資產管理 → 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 點擊**新增**。
   裝置分類設定視窗開啟。
3. 輸入新選項的名稱。
4. 指定包含要包括在裝置分類中的裝置的群組：
   - **尋找任何裝置**— 搜尋符合選擇標準並被包含在**受管理裝置**或未**未指派的裝置**群組中的裝置。
   - **尋找受管理裝置** — 搜尋符合選擇標準並被包含在**受管理裝置**群組中的裝置。
   - **尋找未指派的裝置**— 搜尋符合選擇標準並被包含在**未指派的裝置**群組中的裝置。

   您可以啟用**包含來自從屬管理伺服器的資料**核取方塊以啟用搜尋滿足選擇條件並由從屬管理伺服器管理的裝置。
5. 點擊**新增**。

6. 在開啟的視窗中，指定將裝置納入此裝置分類所必須符合的條件，然後按一下 **儲存** 按鈕。
7. 點擊**儲存**按鈕。

   裝置選項已建立並新增到裝置選項清單中。

配置裝置分類

要配置裝置分類：

1. 在主功能表中，轉至 **資產管理 → 裝置分類**。

   裝置選項清單頁面隨即顯示。
2. 選擇相關的使用者自定義裝置分類，然後點擊**內容**按鈕。

   裝置分類設定視窗開啟。
3. 在**一般**標籤上，點擊**新條件**連接。
4. 指定包含裝置到該分類所必須滿足的條件。
5. 點擊**儲存**按鈕。

   裝置被套用並儲存。

以下是分配裝置到分類的條件敘述。多個條件使用 OR 邏輯運算子組合在一起：分類範圍將包含至少符合列出的一個條件的裝置。

一般

在**一般**區域，您可以變更分類條件的名稱，指定是否必須倒轉條件：

反轉分類條件

預設情況下已停用該選項。

如果啟用此選項，指定的分類條件將倒轉。此分類將包含所有不符合該條件的裝置。

以下範例展示了反轉工作的邏輯：

- **條件**：您的裝置上安裝了 Linux 類型且內部版本號為 00.0.000 的作業系統。
- **反轉條件**：您的裝置上安裝了非 Linux 類型且內部版本號為 00.0.000 的作業系統，這等價於：

  安裝了非 Linux 類型或內部版本號非 00.0.000 的作業系統。

因此，分類將包括安裝了 Windows 類型且內部版本號為 00.0.000 的裝置，或安裝了 Linux 類型但內部版本號不為 00.0.000 的裝置。

網路基礎架構

在**網路**子區域，您可以指定依據網路資料裝置納入分類的標準：

- **裝置名稱**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **網域**

  顯示指定的工作組中包括的所有裝置。

- **管理群組**

  顯示指定的管理群組中包括的裝置。

- **描述**

  裝置內容視窗中的文字：在**描述**區域的**一般**欄位。
  您可以使用以下特徵說明**描述**欄位中的文字：

  - 在單詞中：

    - *****。用任意數量的字元更換任何字串。

    例如：
    要敘述單詞 **Server** 或 **Server's**，您可以輸入 **Server***。

    - **?**。更換任意單個字元。

    例如：
    若要描述短語，例如 **SUSE Linux 企業伺服器 12** 或者 **SUSE Linux 企業伺服器 15**, 你可以輸入 **SUSE Linux 企業伺服器 1?**。
    星號 **(*)** 或問號 **(?)** 不能用於查詢中的第一個字元。

  - 要尋找多個單詞：

    - 空格。顯示所有在其敘述中包含列出的任何單詞的裝置。

    例如：
    要尋找在其敘述中包含**從屬**或**虛擬**單詞的短語，您可以在查詢中包含**從屬虛擬**等字。

    - **+**。當單詞帶有加號前綴時，所有搜尋結果都將包含該單詞。

    例如：
    要搜尋同時包含**從屬**和**虛擬**的短語，請輸入**+從屬+虛擬**查詢。

    - **-**。當單詞帶有減號前綴時，所有搜尋結果都不包含該單詞。

    例如：
    要尋找包含**從屬**但不包含**虛擬**的短語，請輸入**+從屬-虛擬**查詢。

    - **「<某些文字>」**。引號中圍繞的文字必須存在文字中。

例如：

要尋找包含**從屬伺服器**單詞群組合的短語，您可以在查詢中輸入**「從屬伺服器」**。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。

  預設情況下已停用該選項。

- **由不同管理伺服器管理**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅套用於由其他管理伺服器管理的用戶端裝置。這些伺服器與您配置裝置移動規則的伺服器不同。
  - **否**。裝置移動規則僅套用於由目前管理伺服器管理的用戶端裝置。
  - **未選取值**。該條件不適用。

在**網域控制器**子區域，您可以根據網域成員身分設定將裝置納入分類的標準：

- **裝置在網域組織單元中**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的網域組織單元中的裝置。

  預設情況下已停用該選項。

- **該裝置是網域安全群組成員**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的網域安全群組中的裝置。

  預設情況下已停用該選項。

在**網路活動**子區域，您可以根據網路活動指定將裝置納入分類的標準：

- **作為發佈點**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。選取範圍將包括充當發佈點的裝置。
  - **否**。分類不包含作為發佈點的裝置。
  - **未選取值**。將不套用標準。

- **不斷開與管理伺服器的連線**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **已啟用**。分類將包含已選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **已停用**。分類將包含未選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **未選取值**。將不套用標準。

- **連線設定檔已轉換**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。該分類將包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **否**。該分類將不包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **未選取值**。將不套用標準。

- **上一次連線到管理伺服器**

  您可使用此方塊設定按上一次連線到管理伺服器的時間搜尋裝置的標準。

  如果選取該方塊，則在輸入欄位中，您可以指定在用戶端裝置上安裝的網路代理和管理伺服器之間建立上一次連線的時間間隔（日期和時間）。選取將包括位於指定間隔的裝置。

  如果清除此方塊，則將不會套用標準。

  預設情況下，此核取方塊已清除。

- **網路輪詢時偵測到新裝置**

  搜尋最近幾天透過網路輪詢偵測到的新裝置。

  如果選取此核取方塊，分類將只包括在**偵測週期（天）**欄位中指定的天數內透過裝置發現偵測到的新裝置。

  如果停用此選項，分類將包括透過裝置發現偵測到的所有裝置。

  預設情況下已停用該選項。

- **裝置可見**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。程式在分類中包括網路中目前可見的裝置。
  - **否**。應用程式在分類中包括網路中目前不顯示的裝置。
  - **未選取值**。將不套用標準。

裝置狀態

在**受管理裝置狀態**子區域，您可以根據受管理應用程式的裝置狀態的敘述設定將裝置納入分類的標準：

- **裝置狀態**

  在該下拉清單中，您可以選取下列裝置狀態之一：*確定*、*緊急*或*警告*。

- **即時防護狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

- **裝置狀態敘述**

  在此欄位中，您可以選取條件旁邊的核取方塊，若滿足這些條件，程式會為裝置分配下列狀態之一：*確定*、*緊急*或*警告*。

在**受管理應用程式元件的狀態**子區域中，您可以根據受管理應用程式元件狀態設定將裝置納入分類的標準：

- **資料洩漏防護狀態**

  根據資料外洩防護的狀態搜尋裝置（*未知*, *已停止*, *正在啟動*, *已暫停*, *執行中*, *失敗*）。

- **協作伺服器防護狀態**

  根據伺服器協作防護狀態搜尋裝置（*未知*, *已停止*、*正在啟動*、*已暫停*, *執行中*、*失敗*）。

- **郵件伺服器的病毒防護狀態**

  根據郵件伺服器防護狀態搜尋裝置（*未知*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*失敗*）。

- **端點感應器狀態**

  根據端點感應器元件狀態搜尋裝置（*未知*、*已停止*、*正在啟動*、*已暫停*、*執行中失敗*）。

在**影響受管理應用程式狀態的問題**子區域，您可以根據由受管理應用程式偵測到的可能問題清單指定將裝置納入分類的標準。如果至少一個您選取的問題存在於裝置，裝置將被包含到分類。當您選取幾個應用程式的問題時，您可以選取在所有清單中自動選取該問題。

您可以選取受管理應用程式狀態敘述的核取方塊；接收這些狀態時，裝置將被包含在分類。當您選取幾個應用程式的狀態時，您可以選取在所有清單中自動選取該狀態。

系統詳情

在**作業系統**區域，您可以根據作業系統指定將裝置納入分類的標準。

- **平台類型**

  如果選中該方塊，您可以從清單中選取一個作業系統。安裝了指定作業系統的裝置會包含在搜尋結果中。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **作業系統架構**

  在該下拉清單中可選取作業系統的架構，這將決定將移動規則套用到裝置（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。預設情況下，不選取清單中的任何選項，這樣就不會對作業系統的架構進行定義。

- **作業系統組建版本**

  該設定僅套用到 Windows 作業系統。

  作業系統版本號。您可以指定所選作業系統是否必須具有相等、更早或更晚的發行版本號。您也可以設定對所有版本號的搜尋，除了指定的值。

- **作業系統發佈號**

  該設定僅套用到 Windows 作業系統。

  作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

在**虛擬機**區域中，您可以根據它們是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來指定將裝置納入分類的標準：

- **這是一台虛擬機**

  在此下拉清單中，您可以選取以下選項：

  - **未定義**。
  - **否**。尋找不是虛擬機的裝置。
  - **是**。搜尋虛擬機裝置。

- **虛擬機類型**

  在該下拉清單中，您可以選取虛擬機製造商。

  若在**是**下清單中選取**不重要**或**這是一台虛擬機**值，則可使用此下拉清單。

- **虛擬桌面基礎架構的一部分**

  在此下拉清單中，您可以選取以下選項：

  - **未定義**。
  - **否**。尋找不是虛擬桌面基礎架構一部分的裝置。
  - **是**。搜尋屬於虛擬桌面基礎架構 (VDI) 一部分的裝置。

在**硬體登錄資料**子區域，您可以根據所安裝的硬體設定將裝置納入分類的標準：

確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

- **裝置**

  在該下拉清單中，您可以選取單元類型。所有帶有該單元的裝置被包含在搜尋結果。

  該欄位支援完整文字搜尋。

- **供應商**

  在該下拉清單中，您可以選取單元生產商的名稱。所有帶有該單元的裝置被包含在搜尋結果。

  該欄位支援完整文字搜尋。

- **裝置名稱**

  具有指定名稱的裝置將包括在該分類中。

- **描述**

  裝置或硬體單元的敘述。帶有該欄位中指定的敘述的裝置將包括在分類範圍內。

  可在裝置的內容視窗輸入任何格式的裝置敘述。該欄位支援完整文字搜尋。

- **裝置製造商**

  裝置製造商的名稱。被指定生產商製造的裝置將包括在分類範圍內。

  您可以在裝置的內容視窗中輸入製造商的名稱。

- **序號**

  帶該欄位中指定序號的所有硬體裝置將包括在該分類中。

- **庫存編號**

  帶有該欄位中指定的清單編號的裝置將包括在選取範圍內。

- **使用者**

  該欄位中指定使用者的所有硬體裝置都將包括在該分類中。

- **位置**

  裝置或硬體單元的位置（例如，在總部或分公司）。在該欄位中指定的位置佈署的電腦或其他裝置將包括在該分類中。

  您可以在該裝置的內容視窗中以任何格式敘述裝置的位置。

- **CPU 時鐘頻率 (MHz)，從**

  CPU 的最小時鐘速率。CPU 與輸入欄位中指定的時鐘速率範圍（含）比對的裝置將被包含在分類中。

- **CPU 時鐘頻率 (MHz)，到**

  CPU 的最大時鐘速率。CPU 與輸入欄位中指定的時鐘速率範圍（含）比對的裝置將被包含在分類中。

- **虛擬 CPU 內核數量，從**

  虛擬 CPU 核心的最小數量。CPU 與輸入欄位中指定的虛擬核心數範圍（含）比對的裝置將被包含在分類中。

- **虛擬 CPU 內核數量，到**

  虛擬 CPU 核心的最大數量。CPU 與輸入欄位中指定的虛擬核心數範圍（含）比對的裝置將被包含在分類中。

- **硬碟磁區，以 GB 為單位，從**

  裝置上硬碟磁碟機的最小容量。硬碟磁碟機與這些輸入欄位中指定的容量範圍（含）比對的裝置將包括在分類範圍內。

- **硬碟磁區，以 GB 為單位，到**

  裝置上硬碟磁碟機的最大容量。硬碟磁碟機與這些輸入欄位中指定的容量範圍（含）比對的裝置將包括在分類範圍內。

- **RAM 大小 (MB)，從**

  裝置 RAM 的最小容量。RAM 容量與輸入欄位中的數值範圍（含）相符的裝置將包括在分類範圍內。

- **RAM 大小 (MB)**

  裝置 RAM 的最大容量。RAM 容量與輸入欄位中的數值範圍（含）相符的裝置將包括在分類範圍內。

第三方軟體詳情

在**應用程式登錄資料**子區域，您可以根據已安裝的應用程式設定搜尋裝置的標準：

- **應用程式名稱**

  在該下拉清單中，您可以選取應用程式。安裝有指定應用程式的裝置將包括在選取範圍中。

- **應用程式版本**

  在該輸入欄位中，您可以指定選定應用程式的版本。

- **供應商**

  在該下拉清單中，您可以選取已安裝應用程式的生產商。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **根據更新尋找**

  如果啟用此選項，則搜尋操作將使用相關裝置內應用程式更新的有關資訊來執行。選取核取方塊後，**應用程式名稱**、**應用程式版本**與**應用程式狀態**欄位會各自變成**更新名稱**、**更新版本**和**狀態**。

  預設情況下已停用該選項。

- **不相容安全應用程式名稱**

  在該下拉清單中，您可以選取協力廠商安全應用程式。在搜尋過程中，安裝有指定程式的裝置將包括在選取範圍中。

- **應用程式標籤**

  在該下拉清單中，您可以選取應用程式標籤。所有安裝了敘述中帶有所選標籤的應用程式的裝置都被包含在裝置分類。

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，分類將包含未帶有所選標籤的敘述的裝置。

  如果停用該選項，則不套用標準。

  預設情況下已停用該選項。

在**弱點與更新**子區域中，您可以根據 Windows 更新來源指定將裝置納入分類的標準：

WUA 已轉換到管理伺服器

您可以在下拉清單中選取以下搜尋選項之一：

- **是**。如果選中該選項，搜尋結果會包含從管理伺服器收到 Windows Update 更新的裝置。
- **否**。如果選中該選項，結果會包含從其他來源收到 Windows Update 更新的裝置。

卡巴斯基應用程式詳情

在 **卡巴斯基應用程式**子區域中，您可以根據所選的受管理應用程式設定將裝置納入分類的標準：

- **應用程式名稱**

  在下拉清單中，可設定按 Kaspersky 應用程式名稱執行搜尋時在分類中包括裝置的標準。

  清單僅提供管理員工作站上已安裝管理外掛程式的應用程式的名稱。

  如果未選取任何應用程式，則將不會套用該標準。

- **應用程式版本**

  在輸入欄位，可設定按 Kaspersky 應用程式版本號執行搜尋時在分類中包括裝置的標準。

  如果未指定版本號，則將不會套用該標準。

- **重大更新名稱**

  在輸入欄位中，可設定按應用程式名稱或更新套件編號執行搜尋時在分類中包括裝置的標準。

  如果欄位留空，則將不會套用該標準。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **選取上次更新模組的期間**

  您可以使用此選項來設定按這些裝置上安裝的程式模組上次更新的時間搜尋裝置的標準。

  如果選中此方塊，則您可以在輸入欄位中指定執行這些裝置上安裝的程式模組的上一次更新的時間間隔（日期和時間）。

  如果清除此方塊，則將不會套用標準。

  預設情況下，此核取方塊已清除。

- **裝置透過管理伺服器進行管理**

  在下拉清單中，您可以將透過 Kaspersky Next XDR Expert 管理的裝置包含在分類中：

  - **是**。應用程式會將透過 Kaspersky Next XDR Expert 管理的裝置包含在分類中。
  - **否**。如果裝置不是透過 Kaspersky Next XDR Expert 管理，應用程式會將其包含在分類中。
  - **未選取值**。將不套用標準。

- **安全應用程式已安裝**

  在該下拉清單，您可以包含已安裝安全應用程式的裝置到分類：

  - **是**。應用程式包含安裝了安全應用程式的裝置到分類。
  - **否**。應用程式會在分類中包含未安裝安全應用程式的裝置。
  - **未選取值**。將不套用標準。

在**病毒防護**子區域，您可以根據防護狀態設定將裝置納入分類的標準：

- **資料庫發佈日期**

  如果啟用此選項，您可以按病毒資料庫發佈日期搜尋用戶端裝置。在該輸入欄位中，您可以設定執行搜尋的時間間隔。

  預設情況下已停用該選項。

- **資料庫記錄數**

  如果啟用此選項，您可以依據資料庫記錄數量來搜尋用戶端裝置。在輸入欄位中，您可以設定病毒資料庫記錄數的上限值和下限值。

  預設情況下已停用該選項。

- **上一次掃描**

  如果啟用此選項，您可以按上次惡意軟體掃描時間來搜尋用戶端裝置。在該輸入欄位中，您可以指定執行上一次惡意軟體掃描的時段。

  預設情況下已停用該選項。

- **偵測到的威脅**

  如果啟用此選項，您可以依據發現的病毒數量來搜尋用戶端裝置。在輸入欄位中，您可以設定發現病毒總數的上限值和下限值。

  預設情況下已停用該選項。

在**加密**子區域中，您可以根據所選的加密演算法設定將裝置納入分類的標準：

加密演算法

進階加密標準 (AES) 對稱區塊編碼器演算法。在下拉清單中，您可以選取加密金鑰大小（56-bit、128-bit、192-bit 或 256-bit）。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

應用程式元件子區域會針對在OSMP主控台中安裝了專用管理外掛程式的應用程式，列出該應用程式的元件。

在**應用程式元件**子區域中，您可以根據所選應用程式元件的狀態和版本編號指定將裝置納入分類的標準：

- **狀態**

  根據應用程式傳送到管理伺服器的元件狀態搜尋裝置。您可以選擇以下狀態之一：*N/A*、*Stopped*、*Paused*、*Starting*、*Running*、*Failed*、*Not installed*、*Not supported by license*。如果安裝在受管理裝置上的應用程式的所選元件具有指定狀態，裝置被包含到裝置分類。

由應用程式傳送的狀態：

- *已停止* - 元件被停用且不在工作。
- *已暫停* - 元件被暫停，例如，在使用者在受管理應用程式上停止了防護後。
- *正在啟動* - 元件處於初始化處理程序中。
- *執行中* - 元件被啟用且在正常工作。
- *失敗* – 元件操作中發生錯誤。
- *未安裝* - 當設定應用程式自訂安裝時，使用者未選取該元件以安裝。
- *不受產品授權支援* – 產品授權不涵蓋所選元件。

不同於其他狀態，裝置上*N/A* 狀態不由應用程式傳送。該選項顯示應用程式沒有所選元件狀態的資訊。例如，這可能發生在所選元件不屬於任何在裝置上安裝的應用程式時，或裝置關閉時。

- **版本**

  根據您在清單中選取的版本號搜尋裝置。您可以輸入版本號，例如 `3.4.1.0`，然後指定所選元件是否必須具有相同、更早或更新版本。您也可以設定對所有版本的搜尋，除了指定的值。

標籤

在**標籤**區域中，您可以根據先前新增到受管理裝置的敘述的關鍵字（標籤）設定將裝置納入分類的標準：

如果有至少一個指定的標籤符合則套用

如果啟用此選項，搜尋結果將顯示包含帶有所選標籤的敘述的裝置。

如果停用此選項，搜尋結果將僅顯示包含帶有所有標籤的敘述的裝置。

預設情況下已停用該選項。

要將標籤新增到條件，請點擊**新增**按鈕，然後點擊**標籤**輸入欄位來選擇標籤。指定是否在裝置分類中包括或排除具有所選標籤的裝置。

- **帶此標籤的所有裝置**

  如果選取了該選項，搜尋結果將顯示帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

  預設情況下已選定此選項。

- **不帶此標籤的所有裝置**

  如果選取了該選項，搜尋結果將顯示不帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

使用者

在**使用者**區域中，您可以根據登入到作業系統的使用者帳戶設定將裝置納入分類的標準。

- **最後一次登入系統的使用者**

  如果啟用此選項，您可以選擇用於配置標準的使用者帳戶。搜尋結果包含所選使用者上一次登入係統的裝置。

- **登入系統至少一次的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含指定使用者至少登入一次的裝置。

裝置所有者

在**裝置所有者**區域中，您可以根據裝置的註冊所有者、其角色及其在安全性群組中的成員資格，設定標準以將裝置包含在選擇中：

- **裝置所有者**

  從內部安全群組中選擇裝置所有者的使用者名稱。在本節中了解有關使用者和使用者角色的更多資訊。

  > 最多只能有一名使用者註冊為裝置所有者。

- **裝置所有者列入 Active Directory 安全群組**

  選擇裝置所有者所屬的外部 Active Directory 安全群組。

  > 使用者可以是 Active Directory 安全群組的一部分，也可以是此 Active Directory 安全群組中包含的群組的一部分。

- **裝置所有者角色**

  選擇裝置所有者的指派角色。在本文中了解有關使用者角色的更多資訊。

- **裝置所有者在內部安全群組中之成員資格**

  選擇裝置所有者所屬的內部安全群組。

從裝置分類中匯出裝置清單

Open Single Management Platform允許您將裝置分類中的裝置資訊匯出為CSV或TXT檔案。

從裝置分類中匯出裝置清單：

1. 從裝置分類中開啟包含裝置的表格。
2. 使用以下方法之一選擇要匯出的裝置：
   - 要選擇特定裝置，請選取它們旁邊的核取方塊。
   - 要從當前表頁面選擇所有裝置，請選取裝置表標頭中的核取方塊，然後選取**全選當前頁面**核取方塊。
   - 要從表中選擇所有裝置，請選取裝置表標頭中的核取方塊，然後選擇**全選**核取方塊。
3. 按一下 **匯出到 CSV**或 **匯出到 TXT**按鈕。表中包含的有關所選裝置的所有資訊都將被匯出。

請注意，如果您將篩選條件套用於裝置表，則只有來自顯示列的篩選資料將被匯出。

在分類中從管理群組中刪除裝置

在使用裝置分類時，你可以直接從管理群組中刪除裝置，而不是轉換到包含這些裝置的管理群組。

要從管理群組刪除裝置，請執行以下操作：

1. 在主功能表中，轉到**資產管理 → 裝置分類** or **發現和佈署 → 裝置分類**。
2. 在選項清單中，按一下裝置分類的名稱。
   該頁面會顯示一個表格，其中包含有關裝置分類中包含的裝置的資訊。
3. 選取您要移除的裝置，之後點擊**刪除**。
   所選裝置即從對應管理群組中刪除。

裝置標籤

該部分描述了裝置標籤，提供了建立和修改它們以及手動或自動標記裝置的說明。

裝置標籤

Open Single Management Platform可讓您*標記*裝置。標籤是用來分組、敘述或查找裝置的字串值。分配到裝置的標籤可以用於建立分類、尋找裝置以及分發裝置到管理群組。

您可以手動或自動標記裝置。如果您想標記單一裝置，可以使用手動標記。Open Single Management Platform透過以下方式之一執行自動標記：

- 按照指定的標記規則。
- 透過應用程式。

不建議使用不同的標記方式來指派相同的標籤。例如，若某種標籤是按規則指派，則不建議手動將此標籤指派給裝置。

如果某種標籤是按規則指派，則在滿足指定規則時就會自動為裝置做標記。單個規則對應於每個標記。規則應用到裝置網路內容、作業系統、裝置上安裝的應用程式以及其他裝置內容。例如，您可以設定規則以指派 `[CentOS]` 標籤到執行 CentOS 作業系統的所有裝置。然後，您可以在建立裝置分類時使用該標籤；這將說明您整理所有 CentOS 裝置並給它們指派工作。

每個標籤只能新增一條自動標記規則。如果為相同標籤建立新規則，則會取代先前的規則。

在以下情況下標籤從裝置上被自動刪除：

- 當裝置停止滿足分配標籤的規則的條件時。
- 當分配標籤的規則被停用或刪除時。

每個管理伺服器的標籤清單和規則清單是獨立的，包括主管理伺服器和從屬虛擬管理伺服器。規則僅被套用到來自建立規則的相同管理伺服器的裝置。

建立裝置標籤

要建立裝置標籤：

1. 在主功能表中，轉至 **資產管理 → 標籤 → 裝置標籤**。
2. 點擊**新增**。

   新標籤視窗開啟。
3. 在**標籤**欄位中，輸入頁籤名稱。
4. 按一下**儲存**以儲存變更。

新標籤出現在裝置標籤清單。

重命名裝置標籤

要重命名裝置標籤：

1. 在主功能表中，轉至 **資產管理 → 標籤 → 裝置標籤**。
2. 點擊您要重命名的標籤名稱。
   標籤內容視窗開啟。
3. 在**標籤**欄位，輸入頁籤名稱。
4. 點擊**儲存**以儲存變更。

更新的標籤出現在裝置標籤清單。

刪除裝置標籤

您只能刪除手動指派的標籤。

要刪除手動指派的裝置標籤：

1. 在主功能表中，轉至 **資產管理 → 標籤 → 裝置標籤**。
   標籤清單隨即顯示。
2. 選取要刪除的裝置標籤。
3. 接著，點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**是**按鈕。

裝置標籤被刪除。刪除的標籤被從其分配的所有裝置上自動刪除。

當您刪除以自動標記規則指派給裝置的標籤時，該規則不會被刪除，並且當裝置首次符合規則條件時，該標籤還將被指派給新裝置。如果您刪除自動標記規則，則規則條件中指定的標籤將從有指派該標籤的所有裝置中刪除，但不會從標籤清單中刪除。如有必要，您可以手動從清單中刪除該標籤。

如果此標記由應用程式或網路代理分配給裝置，則已刪除的標記不會被自動從裝置中刪除。若要刪除此類標籤，請使用klscflag公用程式。

檢視分配了標籤的裝置

要檢視分配了標籤的裝置：

1. 在主功能表中，轉至 **資產管理 → 標籤 → 裝置標籤**。
2. 點擊您要檢視已指派裝置之標籤的**檢視裝置**連結。
   您將被重定向到主功能表的**資產（裝置）**部分，其中裝置按您點擊**檢視裝置**連結的標籤進行篩選。
3. 如果您想要返回裝置標籤清單，點擊您瀏覽器的**後退**按鈕。

檢視分配了標籤的裝置後，您可以建立並指派新標籤，也可以將現有標籤指派給其他裝置。在這種情況下，您必須按標籤刪除過濾器，選擇裝置，然後指派標籤。

檢視分配到裝置的標籤

要檢視分配到裝置的標籤：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
2. 點擊您要檢視其標籤的裝置名稱。
3. 在開啟的裝置內容視窗中，選取**標籤**頁籤。

   分配給所選裝置的標籤清單被顯示。在**指派的標籤**列中，您可以檢視標籤的分配方式。

在工具列中，您可以進行以下操作：

- 為裝置指派另一個標籤。
- 刪除已經指派的標籤。
- 檢視管理伺服器上存在的所有裝置標籤。

> 您無法在裝置上本機檢視已指派的標籤。

手動標記裝置

要手動分配標籤到裝置：

1. 檢視分配到您要分配其他標籤的裝置的標籤。
2. 點擊**新增**。

3. 在開啟的視窗中，執行以下操作之一：

   - 若要建立並指派新標籤，請選取**建立新標籤**，之後指定新標籤的名稱。
   - 若要選取現有標籤，請選取**指派現有標籤**，之後在下拉清單選取必要標籤。

4. 點擊**正常**以套用變更。

5. 按一下**儲存**以儲存變更。

   所選的標籤被分配到裝置。

從裝置上刪除分配的標籤

要從裝置上刪除標籤：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。

2. 點擊您要檢視其標籤的裝置名稱。

3. 在開啟的裝置內容視窗中，選取**標籤**頁籤。

4. 選取您要刪除的項目旁邊的核取方塊。

5. 在清單頂部，點擊**取消指派標籤**按鈕。

6. 在開啟的視窗中，點擊**確定**。

   標籤從裝置上刪除。

未配置的裝置標籤不被刪除。如果您想，您可以手動刪除它。

您不能手動刪除應用程式或網路代理分配給裝置的標籤。若要刪除此類標籤，請使用klscflag公用程式。

檢視自動標記裝置規則

要檢視自動標記裝置規則，

執行以下操作之一：

- 在主功能表中，轉至 **資產管理 → 標籤 → 自動標記規則**。
- 在主功能表中，前往**資產管理 → 標籤 → 裝置標籤**，然後點擊**設定自動標記規則**連結。
- 檢視指派給裝置的標籤，然後點擊**設定自動標記規則**按鈕。

自動標記裝置規則清單出現。

編輯自動標記裝置規則

要編輯自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 點擊您要編輯的規則名稱。
   規則設定視窗開啟。
3. 編輯規則的一般內容：
   a. 在**規則名稱**欄位，輸入規則名稱。
      名稱不能包括 256 個以上字元。
   b. 執行以下操作之一：
      - 透過切換開關按鈕至**規則已啟用**啟用規則。
      - 透過切換開關按鈕至**規則已停用**停用規則。
4. 執行以下操作之一：
   - 如果要新增新條件，請點擊**新增**按鈕，然後在開啟的視窗中指定新條件的設定。
   - 若要編輯現有條件，請點擊您要編輯之條件的名稱，接著編輯條件設定。
   - 若您要刪除條件，請選取您要刪除之條件名稱旁的核取方塊，接著點擊**刪除**。
5. 在條件設定視窗點擊**確定**。
6. 按一下**儲存**以儲存變更。

編輯的規則顯示在清單。

建立自動標記裝置規則

要建立自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 點擊**新增**。
   新規則設定視窗開啟。
3. 配置規則的一般內容：
   a. 在**規則名稱**欄位中，輸入規則名稱。
      名稱不能包括 256 個以上字元。

b. 執行以下操作之一：

- 透過切換開關按鈕至**規則已啟用**啟用規則。
- 透過切換開關按鈕至**規則已停用**停用規則。

c. 在**標籤**欄位中，輸入新裝置標籤名稱或從清單中選取其中一個現有裝置標籤。

名稱不能包括 256 個以上字元。

4. 在條件區段中，點擊**新增**按鈕以新增新條件。

新條件設定視窗開啟。

5. 輸入條件名稱。

名稱不能包括 256 個以上字元。名稱必須在規則內唯一。

6. 設定規則，使其在符合下列條件時觸發（您可以選取多個條件）：

- **網路**— 裝置網路內容，例如裝置的 DNS 名稱，或裝置是否屬於 IP 子網路。

  如果為您用於Open Single Management Platform的資料庫設定了區分大小寫的排序規則，請在指定裝置DNS名稱時保持大小寫。否則，自動標記規則將不起作用。

- **應用程式**—出現在裝置上的網路代理程式、作業系統類型、版本、架構以及套件管理工具。
- **虛擬機**—裝置屬於虛擬機的特定類型。
- **應用程式登錄資料**—裝置上不同供應商應用程式的出現。

7. 點擊**確定**儲存變更。

如果必要，您可以為一個規則設定多個條件。此種情況下，在滿足至少一個條件時，標籤將被分配到裝置。

8. 按一下**儲存**以儲存變更。

新建立的規則會在所選管理伺服器管理的裝置上強制執行。如果裝置的設定滿足規則條件，標籤被分配到裝置。

然後，規則被套用到以下情況：

- 自動和間歇性，取決於伺服器負載
- 在您編輯規則之後
- 當您手動執行規則時
- 在管理伺服器偵測到滿足規則條件的裝置設定的變更或包含此裝置的群組設定的變更後

您可以建立多個標記規則。如果您建立了多個標記規則且規則對應的條件同時被滿足，單個裝置可以被分配多個標籤。您可以在裝置內容中檢視所有分配的標籤清單。

為自動標記裝置執行規則

當規則執行時，規則內容中指定的標籤被分配到滿足相同規則中指定條件的裝置。您僅可以執行活動規則。

要為自動標記裝置執行規則：

1. 檢視自動標記裝置規則。
2. 選取您要執行的活動規則旁邊的核取方塊。
3. 點擊**執行規則**按鈕。

   所選規則被執行。

刪除自動標記裝置規則

要刪除自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 選取您要刪除的規則旁邊的核取方塊。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**。

   所選規則被刪除。規則內容中指定的標籤從所有所分配的裝置上取消分配。

> 未配置的裝置標籤不被刪除。如果您想，您可以手動刪除它。

資料加密與防護

如果您的膝上型電腦或硬碟磁碟機被盜或丟失，資料加密可降低敏感資料和公司資料意外洩露的風險。此外，資料加密還允許您防止未經授權的使用者和應用程式進行存取。

如果您的網路包括安裝了 Kaspersky Endpoint Security for Windows 的 Windows 受管理裝置，您可以使用資料加密功能。在這種情況下，在執行 Windows 作業系統的裝置上，您可以管理以下類型的加密：

- BitLocker 磁碟機加密®
- 卡巴斯基磁碟機加密

> 我們不建議在 VDI 中啟用加密。

例如，透過使用這些 Kaspersky Endpoint Security for Windows 元件，您可以啟用或停用加密、檢視加密磁碟機清單、或產生和檢視有關加密的報告。

若要設定加密，請在Open Single Management Platform中定義Kaspersky Endpoint Security for Windows政策。Kaspersky Endpoint Security for Windows 會根據使用的政策執行加密和解密。關於如何設定規則和加密功能說明的詳細說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

目前在網頁主控台中，無法為管理伺服器的層次結構進行加密管理。請使用主管理伺服器管理加密的裝置。

您可以使用使用者介面設定來顯示或隱藏與加密管理功能相關的某些介面元素。

檢視加密磁碟機的清單

在Open Single Management Platform中，您可以檢視有關加密磁碟機和磁碟機層級加密裝置的詳細資訊。磁碟機上的資訊解密後，該裝置會自動從該清單中移除。

檢視加密磁碟機的清單，

在主功能表中，轉至 **操作 → 資料加密與防護 → 加密磁碟機**。

如果功能表上沒有這個區段，表示它隱藏起來了。在使用者介面設定中，啟用**顯示資料加密與防護**選項即可顯示該區段。

匯出加密磁碟機清單為 CSV 或 TXT 檔案。為此，請點擊**匯出到 CSV**或**匯出到 TXT**按鈕。

檢視加密事件清單

在裝置上執行資料加密或解密工作時，Kaspersky Endpoint Security for Windows會將以下類型的事件傳送給Open Single Management Platform：

- 無法加密或解密檔案，或由於磁碟空間不足無法建立加密的壓縮檔案。
- 無法加密或解密檔案，或由於授權問題無法建立加密的壓縮檔案。
- 無法加密或解密檔案，或由於缺少存取權限無法建立加密的壓縮檔案。
- 該應用程式已被封鎖存取加密檔案。
- 未知錯誤。

若要檢視在裝置上的加密資料時發生的錯誤清單，請執行以下操作：

在主功能表中，轉至 **操作 → 資料加密與防護 → 加密事件**。

如果功能表上沒有這個區段，表示它隱藏起來了。在使用者介面設定中，啟用**顯示資料加密與防護**選項即可顯示該區段。

匯出加密磁碟機清單為 CSV 或 TXT 檔案。為此，請點擊**匯出到 CSV**或**匯出到 TXT**按鈕。

或者，您可以檢查每個受管理裝置的加密事件清單。

若要檢視受管理裝置的加密事件：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
2. 按一下受管理裝置的名稱。
3. 在**一般**頁簽上，轉到**防護**部分。
4. 點擊**檢視資料加密錯誤**連接。

建立和檢視加密報告

您可以建立以下報告：

- 受管理裝置加密狀態報告。此報告提供有關各種受管理裝置的資料加密詳細資訊。例如，該報告顯示套用已設定加密規則之政策的裝置數量。此外，您還可以找出需要重新啟動的裝置數量。該報告還包含每台裝置的加密技術和演算法相關資訊。
- 大容量儲存裝置加密狀態報告。此報告包含的資訊與受管理裝置加密狀態報告類似，但它僅提供大容量儲存裝置和卸除式磁碟機的資料。
- 加密磁碟機存取權限報告。此報告會顯示哪些使用者帳戶可以存取加密磁碟機。
- 檔案加密錯誤報告。此報告包含在裝置上執行資料加密或解密工作時所發生錯誤的相關資訊。
- 封鎖存取加密檔案的報告。該報告包含了封鎖應用程式存取加密檔案的資訊。如果未經授權的使用者或應用程式試圖存取加密檔案或磁碟機，則此報告很有用。

您可在**監控 → 報告**區域中產生任何報告。或者，在**操作→資料加密與防護**區域中，您可以產生以下加密報告：

- 大容量儲存裝置加密狀態報告
- 加密磁碟機存取權限報告
- 檔案加密錯誤報告

*要在**資料加密與防護**部分產生加密報告：*

1. 請確保您在介面選項啟用了**顯示資料加密與防護**選項。
2. 在主功能表中，轉至 **操作 → 資料加密與防護**。
3. 您可以開啟以下其中一個區段：
   - **加密磁碟機**會產生大容量儲存裝置加密狀態報告或加密磁碟機存取權限報告。
   - **加密事件**會產生檔案加密錯誤報告。
4. 按一下您要產生的報告名稱。

報告產生將開始。

以離線模式授予加密磁碟機的存取權限

使用者可要求對加密裝置的存取權限，例如，當 Kaspersky Endpoint Security 未安裝在受管理裝置時。收到要求後，您可建立存取金鑰檔案並將其傳送給使用者。所有使用案例和詳細指示都會在所需平台的 Kaspersky Endpoint Security 說明中提供。

若要在Kaspersky Endpoint Security for Windows中以離線模式授予加密磁碟機的存取權限：

1. 從使用者那裡取得要求存取檔案（副檔名為 FDERTC 的檔案）。按照 Kaspersky Endpoint Security for Windows 說明 中的指示，在 Kaspersky Endpoint Security for Windows 中產生該檔案。
2. 在主功能表中，轉至 **操作 → 資料加密與防護 → 加密磁碟機**。

   加密磁碟機清單隨即顯示。
3. 選取使用者要求存取權限的磁碟機。
4. 點擊**同意存取離線模式下的裝置**按鈕。
5. 在開啟的視窗中，選擇 Kaspersky Endpoint Security for Windows 外掛程式。
6. 按照Kaspersky Endpoint Security for Windows說明 提供的說明操作（請參閱本章節最後的OSMP主控台操作說明）。

之後，使用者套用收到的檔案來存取加密磁碟機，並讀取儲存在磁碟機上的資料。

在管理伺服器之間傳輸加密金鑰

在受管理裝置上啟用資料加密功能後，加密金鑰會儲存在管理伺服器上。加密金鑰會用來存取加密資料以及管理加密政策。

在以下情況下必須將加密金鑰傳輸至其他管理伺服器：

- 在受管理裝置上重新設定網路代理，以指派裝置至其他管理伺服器。若此裝置內含加密資料，則加密金鑰必須傳輸至目標管理伺服器。否則，無法加密資料。
- 加密已連接至裝置 D1 並由管理伺服器 S1 管理的卸除式磁碟機，之後您將此卸除式磁碟機連接至管理伺服器 S2 管理的裝置 D2。若要存取卸除式磁碟機上的資料，必須將加密金鑰從管理伺服器 S1 傳輸至管理伺服器 S2。
- 加密由管理伺服器 S1 管理之裝置 D1 上的檔案，之後您嘗試存取由管理伺服器 S2 管理之裝置 D2 的檔案。若要存取檔案，加密金鑰必須從管理伺服器 S1 傳輸至管理伺服器 S2。

您可以透過下列方式傳輸加密金鑰：

- 系統會自動啟用必須傳輸加密金鑰的兩個管理伺服器內容中的**使用管理伺服器層級獲取加密金鑰**選項。若此選項在其中一個管理伺服器停用，則無法自動傳輸加密金鑰。

  在管理伺服器內容啟用**使用管理伺服器層級獲取加密金鑰**選項後，管理伺服器會將儲存於儲存區的所有加密金鑰傳送至在階層中高一級的主管理伺服器（若有）。

當您嘗試存取加密資料，管理伺服器會先在自己的儲存區搜尋加密金鑰。若啟用**使用管理伺服器層級獲取加密金鑰**選項，且在儲存區中找不到所需的加密金鑰，則管理伺服器會另外將要求傳送至主管理伺服器（若有），以提供所需的加密金鑰。要求將會傳送至所有主管理伺服器，最終傳送至位於階層中最高層級的伺服器。

- 匯出和匯入包含加密金鑰的檔案，以手動從某個管理伺服器傳送至另一個管理伺服器。

  加密金鑰的匯出和匯入是加密金鑰管理功能所包含的操作。要執行這些操作，請如下為Open Single Management Platform使用者設定該功能的存取權限：

  - 將加密金鑰管理功能的**讀取**存取權限授予從從屬管理伺服器匯出加密金鑰的使用者。
  - 將加密金鑰管理功能的**寫入**存取權限授予將加密金鑰匯入目的管理伺服器的使用者。

若要在階層內的管理伺服器之間自動傳輸加密金鑰：

1. 前往所需管理伺服器的屬性：
   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。
   b. 在開啟的導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後點擊設定圖示 (⚙)。
   或者，您可以按一下管理伺服器名稱，然後在主選單中顯示該名稱後，在主選單中按一下它以開啟伺服器屬性視窗。
2. 在開啟的屬性視窗中，選取**加密演算法**部分。
3. 啟用**使用管理伺服器層級獲取加密金鑰**選項。
4. 點擊**儲存**以套用變更。

加密金鑰將會在下次同步時（活動訊號）傳輸至主管理伺服器。此管理伺服器也會在收到要求時，從其儲存區提供加密金鑰給從屬管理伺服器。

若要在管理伺服器之間手動傳輸加密金鑰：

1. 前往要從中匯出加密金鑰的管理伺服器的屬性：
   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。
   b. 在開啟的導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後點擊設定圖示 (⚙)。
   或者，您可以按一下管理伺服器名稱，然後在主選單中顯示該名稱後，在主選單中按一下它以開啟伺服器屬性視窗。
2. 在開啟的屬性視窗中，選取**加密演算法**部分。
3. 點擊**匯出加密金鑰**。
   確保將加密金鑰管理功能的**讀取**存取權限授予從伺服器匯出加密金鑰的使用者。

4. 在**從管理伺服器匯出加密金鑰嗎？**視窗中，執行以下操作：

   a. 指定密碼以防護檔案，避免未獲授權的存取。

   b. 指定檔案的儲存位置。

   記住密碼。無法擷取遺失的密碼。若遺失密碼，您必須重複匯出程序。因此，請記下密碼並放置於方便拿取的地方。

5. 將檔案傳輸至另一個管理伺服器，例如透過共用資料夾或卸除式磁碟機進行。

6. 前往要為其匯入加密金鑰的管理伺服器的屬性。

7. 在內容視窗中，選取**加密演算法**區域。

8. 點擊**匯入加密金鑰**。

   確保將加密金鑰管理功能的**寫入**存取權限授予匯入加密金鑰到伺服器的使用者。

9. 選取包含加密金鑰的檔案。

10. 輸入密碼並點擊**確定**。

    加密金鑰會傳輸至目標管理伺服器。

變更用戶端裝置的管理伺服器

對於特定用戶端裝置，您可以將管理伺服器變更為不同的管理伺服器。為此，請使用*變更管理伺服器*工作。

要變更用戶端裝置連線的管理伺服器：

1. 連線至管理裝置的管理伺服器。

2. 建立管理伺服器變更工作。

   新工作精靈啟動。遵照精靈的說明。在新工作精靈的**新工作**視窗中，選擇**卡巴斯基安全管理中心 16.3**應用程式和**變更管理伺服器**工作類型。之後，指定要變更管理伺服器的裝置：

   - **指派工作給管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

     例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

     如果工作被指派給管理群組，則工作內容視窗中不會顯示**安全**頁籤，因為群組工作受其所套用的群組的安全設定的約束。

   - **手動指定裝置位址或是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。

     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **指派工作給裝置分類**

     該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

3. 執行建立的工作。

在工作完成後，為其建立工作的用戶端裝置將被工作設定中指定的管理伺服器管理。

如果管理伺服器支援加密和資料防護，並且您正在建立*變更管理伺服器*工作，將顯示警告。警告聲明如果有加密資料儲存在裝置，在新伺服器開始管理裝置之後，使用者將僅可以存取他之前使用過的加密資料。在其他情況下，將無法存取加密資料。如需不會提供加密資料存取權限的情況詳細說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

當裝置顯示不活動時檢視和配置操作

如果組中的用戶端裝置不活動，您可以獲取關於它的通知。您也可以自動刪除此類裝置。

要在組中裝置顯示不活動時檢視或設定操作：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 透過下列方式之一轉到所需管理群組的屬性：
   - 點擊管理群組的名稱。
   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。

   管理群組內容視窗將開啟。
3. 在內容視窗中，前往**設定**頁籤。
4. 在**繼承**區段，啟用或停用以下選項：
   - **從父群組繼承**

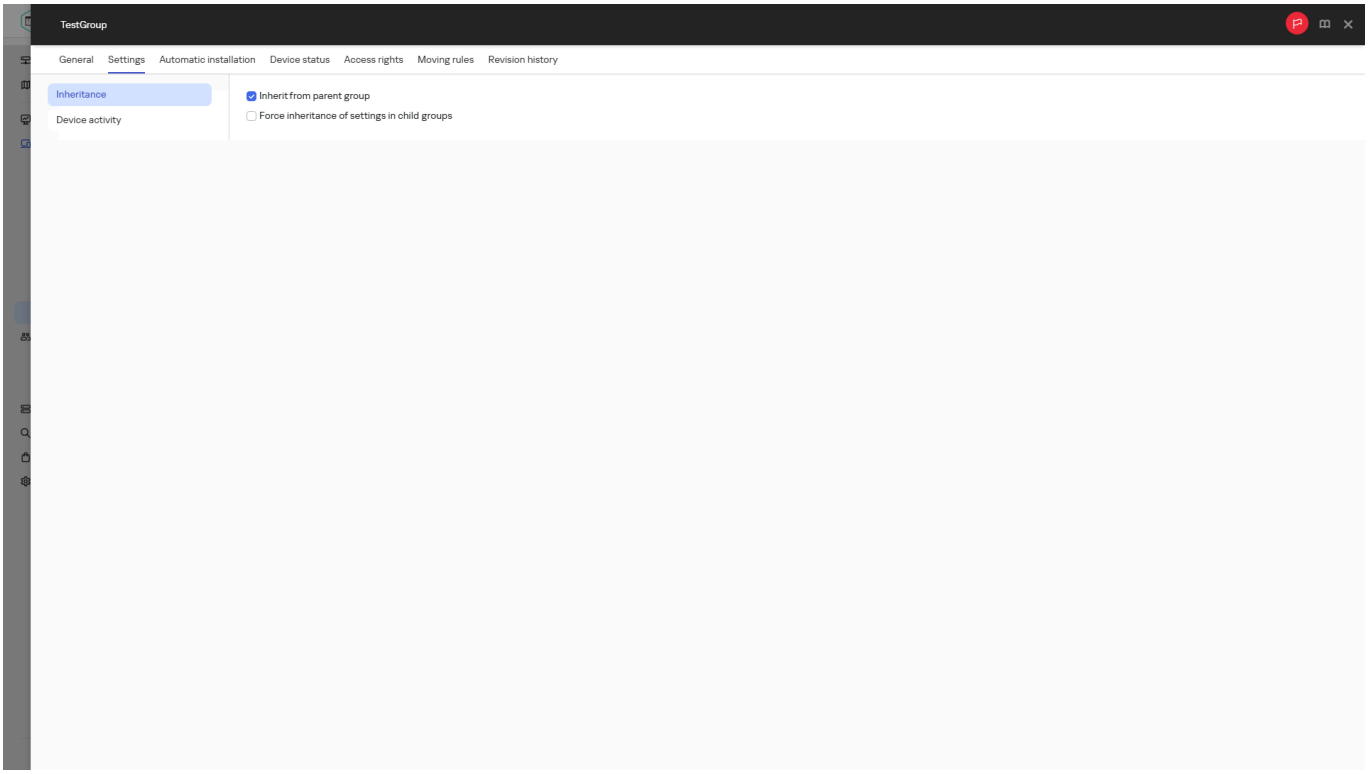
     該區域的設定將從包含用戶端裝置的父群組繼承。如果啟用此選項，**網路中的裝置活動**下的設定會禁止任何變更。

     該選項僅在管理群組擁有父群組時可用。

     預設情況下已啟用該選項。
   - **在子群組中強制繼承設定**

     該設定值將被分發到子群組，但在子群組的內容中這些設定被鎖定。

預設情況下已停用該選項。



管理群組內容

5. 在**裝置活動**區段，啟用或停用以下選項：

- **若裝置未活動超過下列天數，則通知管理員**

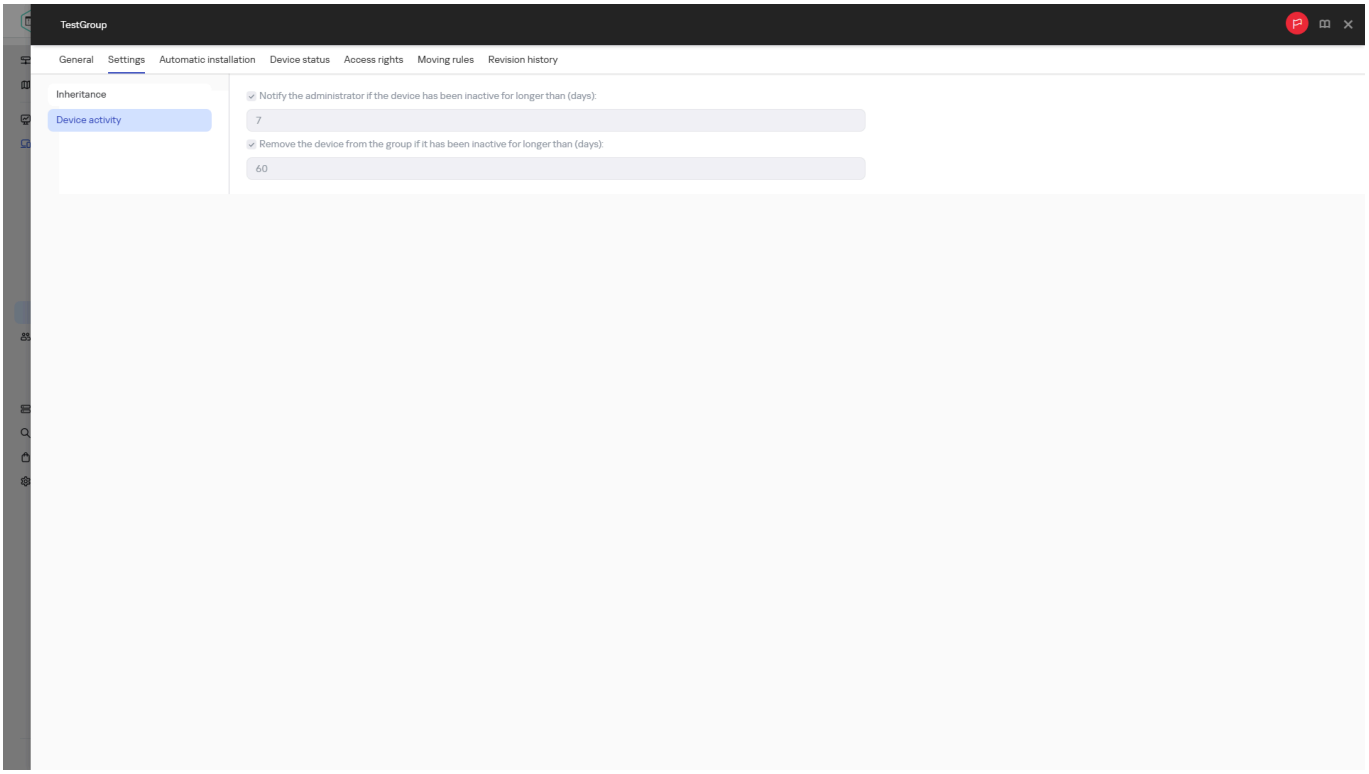
  如果啟用該選項，管理員接收不活動裝置的通知。您可以指定**裝置在網路上已長時間沒有活動**事件被建立的時間間隔。預設時間間隔為 7 天。

  預設情況下已啟用該選項。

- **若裝置未活動超過下列天數，則從群組刪除裝置**

  如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設時間間隔為 60 天。

預設情況下已啟用該選項。



管理群組內容

6. 點擊**儲存**按鈕。

您的變更已儲存並套用。

遠端存取受管理裝置

Open Single Management Platform允許您建立與受管理裝置的遠端連線。管理員可以透過裝置上安裝的網路代理，遠端存取受管理裝置。如果裝置的 TCP 和 UDP 連接埠關閉，也可透過網路代理遠端連線至用戶端裝置。在與裝置建立連線後，管理員會獲取對此裝置上儲存資訊的完全存取權限，以便管理員可以管理其上安裝的應用程式。

建立遠端連線的方法取決於安裝有OSMP主控台的裝置上使用的平台。OSMP主控台可以安裝在管理伺服器裝置以外的裝置上，也就是Windows裝置或Linux裝置上。

從安裝在Linux裝置上的OSMP主控台，您可以建立以下連線：

- 使用以下方式連線到基於 Linux 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - 虛擬網路運算 (VNC)
- 使用以下方式連線到基於 Windows 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - 虛擬網路運算 (VNC)

從安裝在Windows裝置上的OSMP主控台，您可以建立以下連線：

- 使用以下方式連線到基於 Linux 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - 虛擬網路運算 (VNC)
- 使用以下方式連線到基於 Windows 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - Windows 桌面共用 (WDS)

從執行Microsoft Windows on Arm的裝置存取OSMP主控台時，不支援遠端連線到受管理裝置。

若要與裝置建立遠端連線，您必須擁有以下工具：

- klsctunnel 公用程式

  卡巴斯基公用程式用於建立受管理裝置和管理伺服器之間的通道連線。

  Open Single Management Platform允許透過管理伺服器，然後透過網路代理程式從OSMP主控台到受管理裝置上指定連接埠的隧道連線。網路隧道功能用於將安裝了OSMP主控台的裝置上的用戶端應用程式連線到受管理裝置上的TCP連接埠 — 如果OSMP主控台和目標裝置之間無法直接連線。

  如果用於連線到管理伺服器的連接埠在裝置上不可用，則需要遠端用戶端裝置和管理伺服器之間的連線隧道。在以下情況下裝置連接埠可能無法使用：

  - 遠端裝置使用 NAT 機制連線到本機網路。
  - 遠端裝置是本機網路管理伺服器的一部分，但是它的連接埠已被防火牆關閉。

  透過OSMP主控台或手動建立遠端連線後，即可下載該公用程式。klsctunnel 公用程式安裝在管理伺服器裝置上。

  klsctunnel 公用程式用於所有類型的遠端連線（RDP、VNC、WDS）。

- RDP 或 VNC 用戶端

  RDP 或 VNC 用戶端安裝在管理伺服器裝置上。此用戶端允許您使用 klsctunnel 公用程式提供的本機連線的位址和連接埠，取得對受管理裝置的遠端存取權。

  在使用者不知道的情況下，以 RDP 連線方式連線到使用者目前的遠端桌面。一旦管理員連線到工作階段，裝置使用者將在未通知的情況下中斷與工作階段的連線。

- Windows 桌面共用（僅適用於基於 Windows 的受管理裝置）

  此功能允許您連線到用戶端裝置上的現有工作階段，而不使該工作階段中的使用者中斷連線。在此情況下，裝置上的管理員和使用者連線將桌面共用存取。

  當連線到遠端桌面的現有連線時，裝置上的連線使用者會收到來自管理員的連線請求。Kaspersky Next XDR Expert 建立的報告中不會儲存裝置上遠端活動及其結果的任何資訊。

  管理員可以在遠端用戶端裝置上設定使用者活動稽核。在稽核期間，應用程式會儲存用戶端裝置上經管理員開啟並/或修改過之檔案的資訊。

從安裝有OSMP主控台的Linux裝置遠端存取受管理的Linux裝置

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Linux 的受管理裝置上，安裝了網路代理版本 15.3 或更高版本。
- 在執行 Linux 的受管理裝置上，安裝了 RDP 伺服器（如果您使用遠端桌面連線功能連線到受管理裝置）。
- 在執行 Linux 的受管理裝置上，安裝了 VNC 伺服器（如果您使用虛擬網路運算功能連線到受管理裝置）。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線（如果您使用遠端桌面連線功能連線到受管理裝置）。
- 管理員具有**建立通道**權限，可以建立VNC通道連線（如果您使用虛擬網路運算功能連線到受管理裝置）。

若要透過在Linux裝置上開啟的OSMP主控台使用RDP或VNC連線到受管理的Linux裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多個裝置、一個行動裝置或一個執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後運行它。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。
   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的/var/opt/kaspersky/klnagent目錄中。
4. 在**連線到遠端桌面**視窗中，指定連線連接埠。預設埠號為 3389。
5. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
6. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   klsctunnel 公用程式顯示遠端存取用戶端的本機連線的位址和連接埠。

該公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

7. 執行遠端存取用戶端（RDP 或 VNC），並使用 klsctunnel 公用程式提供的位址和連接埠將其連线到受管理裝置。

已建立與受管理裝置的連線。可在遠端存取用戶端視窗中使用桌面。

從安裝有OSMP主控台的Linux裝置遠端存取受管理的Windows裝置

遠端桌面連線 (RDP)

先決條件

在您開始之前，確保您已做了如下：

- 受管理裝置的作業系統設定中允許遠端連線。
- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線。

若要透過在Linux裝置上開啟的OSMP主控台使用RDP連線到受管理的Windows裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取 **RDP** 連線類型。
4. 如果受管理裝置的作業系統設定中不允許遠端連線，請點擊**變更設定**按鈕以集中允許遠端連線。

   如果設定正確套用，則會顯示通知。另外，在受管理裝置上，在**設定 → 系統 → 遠端桌面**區段中，**啟用遠端桌面**選項已啟用。

   如果受管理裝置的作業系統設定中允許遠端連線，則不會顯示**變更設定**按鈕。
5. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式。
6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   klsctunnel 公用程式顯示與遠端裝置的連線的位址和連接埠。

該公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

8. 執行 RDP 用戶端並使用 klsctunnel 公用程式提供的位址和連接埠將其連線到受管理裝置。

已建立與受管理裝置的連線。可在 RDP 用戶端視窗中使用桌面。

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線到工作階段，裝置使用者將在無通知的情況下中斷與工作階段的連線。

虛擬網路運算系統 (VNC)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 在執行 Windows 的受管理裝置上，安裝了 VNC 伺服器。
- 管理員具有**建立通道**權限，可以為 VNC 建立通道連線。

若要透過在Linux裝置上開啟的OSMP主控台使用VNC連線到受管理的Windows裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取連線類型 **VNC**。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。
   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的 /var/opt/kaspersky/klnagent 目錄中。
5. 在**連線到遠端桌面**視窗中，指定 VNC 連線連接埠。預設埠號為 5900。
6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   klsctunnel 公用程式顯示 VNC 用戶端本機連線的位址和連接埠。

該公用程式允許遠端用戶關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

8. 執行 VNC 用戶端並使用 klsctunnel 公用程式提供的位址和連接埠將其連線到受管理裝置。

已建立與受管理裝置的連線。桌面可在 VNC 用戶端視窗中使用。

從安裝有OSMP主控台的Windows裝置遠端存取受管理的Linux裝置

遠端桌面連線 (RDP)

先決條件

在您開始之前，確保您已做了如下：

- 在運行 Linux 的受管理裝置上，安裝了 RDP 伺服器。
- 在執行 Linux 的受管理裝置上，安裝了網路代理版本 15.3 或更高版本。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線。

若要透過在Windows裝置上開啟的OSMP網頁主控台使用RDP連線到受管理的Linux裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取 **RDP** 連線類型。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式。
5. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
6. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。
7. 點擊**開啟連接埠**按鈕。

   「遠端桌面連線」登入視窗隨即開啟。
8. 指定您目前用來登入OSMP主控台的帳戶憑證，然後連線到受管理裝置。

   klsctunnel 公用程式顯示與遠端裝置的連線的位址和連接埠。

   該公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

與裝置建立連線後，您將能在 Microsoft Windows 的遠端連線視窗中使用桌面。

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線到工作階段，裝置使用者將在無通知的情況下中斷與工作階段的連線。

虛擬網路運算系統 (VNC)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Linux 的受管理裝置上，安裝了網路代理版本 15.3 或更高版本。
- 在執行 Linux 的受管理裝置上，安裝了 VNC 伺服器。
- 管理員具有**建立通道**權限，可以為 VNC 建立通道連線。

若要透過在Windows裝置上開啟的OSMP主控台使用VNC連線到受管理的Linux裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取連線類型 **VNC**。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。
   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的 /var/opt/kaspersky/klnagent 目錄中。
5. 在**連線到遠端桌面**視窗中，指定 VNC 連線連接埠。預設埠號為 5900。
6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。
8. 點擊**開啟連接埠**按鈕。

   klsctunnel 公用程式顯示 VNC 用戶端本機連線的位址和連接埠。

該公用程式允許遠端用戶關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

9. 執行 VNC 用戶端並使用 klsctunnel 公用程式提供的位址和連接埠將其連線到受管理裝置。

已建立與受管理裝置的連線。桌面可在 VNC 用戶端視窗中使用。

從安裝有OSMP主控台的Windows裝置遠端存取受管理的Windows裝置

遠端桌面連線 (RDP)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線。
- 受管理裝置的作業系統設定中允許遠端連線。

若要透過在Windows裝置上開啟的OSMP主控台使用RDP連線到受管理的Windows裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取**遠端桌面連線**連線類型。
4. 如果受管理裝置的作業系統設定中不允許遠端連線，請點擊**變更設定**按鈕以集中允許遠端連線。

   如果設定正確套用，則會顯示通知。另外，在受管理裝置上，在**設定 → 系統 → 遠端桌面**區段中，**啟用遠端桌面**選項已啟用。

   如果受管理裝置的作業系統設定中允許遠端連線，則不會顯示**變更設定**按鈕。
5. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式。
6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。
8. 點擊**開啟連接埠**按鈕。

   「遠端桌面連線」登入視窗隨即開啟。

9. 指定您目前用來登入OSMP主控台的帳戶憑證，然後連線到受管理裝置。

   klsctunnel 公用程式顯示與遠端裝置的連線的位址和連接埠。

   該公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

與裝置建立連線後，您將能在 Microsoft Windows 的遠端連線視窗中使用桌面。

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線到工作階段，裝置使用者將在無通知的情況下中斷與工作階段的連線。

Windows 桌面共用 (WDS)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 管理員具有**連線到現有 RDP 連線**權限，可以建立 WDS 連線。
- 弱點和修補程式管理的產品授權可用。
- 管理員工作站上已安裝 Microsoft Windows Vista® 或更新版本。管理伺服器裝置作業系統的類型對透過 Windows 桌面共用進行連線沒有限制。

  檢查 Windows 桌面共用功能是否隨附於您的 Windows 版本中，並確保 Windows 登錄檔中包含 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 金鑰。
- 用戶端裝置安裝了 Microsoft Windows Vista 或更新版本。

若要透過在Windows裝置上開啟的OSMP主控台使用VNC連線到受管理的Windows裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取連線類型 **Windows 桌面共用**。

   如果弱點和修補程式管理的產品授權不可用，則會顯示錯誤訊息。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。
   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的 /var/opt/kaspersky/klnagent 目錄中。

5. 在選定裝置上的可用活動使用者工作階段清單中，選取要連線的工作階段。

   遠端使用者必須允許連線。如果遠端使用者拒絕連線或遠端使用者在逾時期限內不允許連線，則會顯示錯誤訊息。

6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。

8. 點擊**開啟連接埠**按鈕。

   klsctunnel 公用程式顯示 VNC 用戶端本機連線的位址和連接埠。

   該公用程式允許遠端用戶關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

桌面共用會在新視窗啟動。若您要與裝置互動，請點擊視窗左上角的功能表圖示 ( )，接著選取**互動模式**。

管理資產

資產代表組織的電腦。您可以將資產新增至OSMP；在這種情況下，OSMP在擴充事件時會自動新增資產ID，並且當您分析事件時，您可以獲得有關組織中電腦的其他資訊。

您可以透過以下方式將資產新增至OSMP：

- 匯入資產：
  - 從 MaxPatrol VM 匯入。
  - 依照排程從**卡巴斯基安全管理中心**和KICS for Networks匯入。

    受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

    KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

    - 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
    - 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

    若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

    1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
    2. 按一下**匯入**，然後選擇以下操作之一：
       - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。

         這將開啟**匯入KSC資產**視窗。

- 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。

  這將開啟**匯入KSC資產屬性**視窗。

3. 在下拉清單，選取要為其執行匯入的租用戶。

   在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。

   如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。

4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

預設情況下，每12小時匯入一次資產，此頻率可以設定。也可以按需匯入資產；這種按需匯入不影響排程匯入時間。OSMP從卡巴斯基安全管理中心資料庫匯入安裝了卡巴斯基安全管理中心網路代理程式且已連線至卡巴斯基安全管理中心的裝置的資訊，即SQL資料庫中具有非空的「連線時間」欄位。OSMP匯入有關電腦的以下資訊：名稱、位址、連線到卡巴斯基安全管理中心的時間、有關硬體和軟體的資訊，包括作業系統以及弱點，即從卡巴斯基安全管理中心網路代理程式接收的資訊。

- 透過網頁介面或API手動建立資產。

  您可以手動新增資產。在這種情況下，您必須手動指定下列資訊：位址、FQDN、作業系統名稱和版本、硬體資訊。無法透過網頁介面新增資產的弱點資訊。如果您使用API新增資產，則可以提供有關弱點的資訊。

您可以管理OSMP資產：檢視資產資訊、搜尋資產、新增、編輯或刪除資產，以及將資產資料匯出到CSV檔案。

從資產新增至 OSMP 起，大約需要 2 分鐘，解決方案才能開始使用此資產擴充事件資訊。例如，如果在新增資產後兩分鐘內發生關聯事件，產生的警示中將不會顯示此資產。

資產類別

您可以將資產分類，然後在篩選條件或關聯規則中使用這些類別。例如，您可以為來自較高嚴重等級類別的資產建立較高嚴重等級的警示。預設情況下，所有資產都屬於**未分類資產**類別。一個裝置可以新增到多個類別。

預設情況下，OSMP會為資產類別指派以下嚴重等級：低、中、高、緊急。您可以建立自訂類別，類別可顯示為巢狀結構。

類別可以透過以下方式填入：

- **手動**
- **活動**：如果資產**符合指定條件**，則為動態。例如，當資產升級到指定的作業系統版本或放置在指定的子網路中時，資產將會移至指定的類別。

1. 在**重複分類間隔**下拉清單中，指定資產連結到類別的頻率。您可以選擇從每小時一次到每24小時一次不等的值。

   您可以透過在類別快顯功能表中選擇**啟動分類**來強制啟動分類。

2. 在**條件**下，指定篩選條件，以比對要附加至資產類別的資產。

   您可以透過點選**新增條件**按鈕來新增條件。您可以透過點選**新增群組**按鈕來新增條件群組。群組運算子可以在**AND** 、 **OR**和**NOT**值之間切換。

分類篩選器運算元和運算子

運算元	運算子	註解
版本編號	>, >=, =, <=, <	
作業系統	=, like	「like」運算子可確保搜尋不區分大小寫。
IP位址	inSubnet, inRange	IP位址以CIDR標記法表示（例如：192.168.0.0/24）。 選擇inRange運算子時，您只能指示來自私有IP位址範圍的位址（例如：10.0.0.0–10.255.255.255）。兩個地址必須在同一範圍內。
FQDN	=, like	「like」運算子可確保搜尋不區分大小寫。
CVE	=, in	「in」操作員可讓您指定一個值陣列。
軟體	=, like	
CII	in	可以選擇多個值。
病毒資料庫上次更新日期	>=,<=	
資訊的上次更新時間	>=,<=	
防護上次更新時間	>=,<=	
系統上次啟動	>=,<=	
KSC擴充狀態	in	裝置的擴充狀態。 可以選擇多個值。
即時防護狀態	=	受管理裝置上安裝的卡巴斯基應用程式的狀態。
加密狀態	=	
垃圾郵件防護狀態	=	
郵件伺服器的病毒防護狀態	=	
資料外洩防護狀態	=	
KSC擴充狀態ID	=	
Endpoint Sensor 狀態	=	
最後一次出現於	>=,<=	

3. 使用**測試條件**按鈕確保指定的篩選器正確無誤。點選此按鈕後，您將看到**給定條件的資產**視窗，其中包含滿足搜尋條件的資產清單。

- **響應式**- 當觸發關聯規則時，資產將移動到指定的群組。

在OSMP中，資產依租用戶和類別分類。資產以樹狀結構排列，其中租用戶位於根目錄，資產類別從其分支出來。您可以在OSMP主控台的**資產→所有資產**部分中檢視租用戶和類別的樹狀結構。選擇一個樹節點後，指派給此節點的資產將顯示在視窗的右側。如果您指定要遞迴顯示資產，則會顯示所選類別子類別中的資產。您可以選取要檢視其資產的租用戶旁的核取方塊。

若要開啟某個類別的快顯功能表，請將滑鼠遊標停留在此類別上，然後按一下類別名稱右側顯示的省略號圖示。快顯功能表中提供以下操作：

類別快顯功能表項目

操作	描述
顯示資產	在視窗右側顯示所選類別的資產。
遞迴顯示資產	檢視所選類別子類別的資產。如果要退出遞迴檢視模式，請選擇其他類別進行檢視。
顯示資訊	在網頁介面視窗右側顯示的**類別資訊**詳情區域中檢視有關所選類別的資訊。
啟動分類	啟動將資產自動連結到所選類別。此選項適用於具有活動分類的類別。

操作	描述
新增子類別	為所選類別新增子類別。
編輯類別	編輯所選類別。
刪除類別	刪除所選類別。您只能刪除沒有資產或子類別的類別。否則，**刪除類別**選項將處於非活動狀態。
固定為頁籤	在單獨的頁籤上顯示所選類別。您可以透過在相關類別的快顯功能表中選擇**取消固定為頁籤**來撤銷此操作。

新增資產類別

若要新增資產類別：

1. 在主功能表中，**資產管理 → 資產（裝置） → 偵測和響應**。
2. 開啟類別建立視窗：
   - 按一下**新增類別**按鈕。
   - 如果要建立子類別，請在父類別的快顯功能表中選擇**新增子類別** 。

   主控台視窗右側將顯示**新增類別**詳情區域。
3. 若要新增類別資訊：
   - 在**名稱**欄位中，輸入類別的名稱。此名稱必須包含1到128個Unicode字元。
   - 在**父級**欄位中，指明類別在類別樹層次結構中的位置：
     a. 按一下按鈕。
     這將開啟**選擇類別**視窗，其中顯示類別樹。如果您要建立新類別而非子類別，則此視窗可能會顯示多個資產類別樹，每個租用戶對應一個。您在此視窗中選擇的租用戶無法撤銷。
     b. 選擇您正在建立的類別的父級類別。
     c. 按一下**儲存**按鈕。

     所選類別將顯示在**父級**欄位中。
   - **租用戶**欄位會顯示您在其結構中選擇父級類別的租用戶。租用戶類別無法變更。
   - 在**優先順序**下拉清單中為類別指派嚴重等級。
   - 如有必要，您可以在**描述**欄位中新增最多包含256個Unicode字元的注釋。
4. 在**分類類型**下拉清單中，選擇如何以資產填入類別。根據您的選擇，您可能需要指定其他設定：
   - **手動** - 資產只能手動連結到類別。
   - **活動**– 如果資產符合定義的篩選條件，則會定期將其指派到某個類別。

活動的資產類別

1. 在**重複分類間隔**下拉清單中，指定資產連結到類別的頻率。您可以選擇從每小時一次到每24小時一次不等的值。

   您可以透過在類別快顯功能表中選擇**啟動分類**來強制啟動分類。

2. 在**條件**下，指定篩選條件，以比對要附加至資產類別的資產。

   您可以透過點選**新增條件**按鈕來新增條件。您可以透過點選**新增群組**按鈕來新增條件群組。群組運算子可以在**AND** 、 **OR**和**NOT**值之間切換。

   分類篩選器運算元和運算子

運算元	運算子	註解
版本編號	>, >=, =, <=, <	
作業系統	=, like	「like」運算子可確保搜尋不區分大小寫。
IP位址	inSubnet, inRange	IP位址以CIDR標記法表示（例如：192.168.0.0/24）。 選擇inRange運算子時，您只能指示來自私有IP位址範圍的位址（例如：10.0.0.0–10.255.255.255）。兩個地址必須在同一範圍內。
FQDN	=, like	「like」運算子可確保搜尋不區分大小寫。
CVE	=, in	「in」操作員可讓您指定一個值陣列。
軟體	=, like	
CII	in	可以選擇多個值。
病毒資料庫上次更新日期	>=,<=	
資訊的上次更新時間	>=,<=	
防護上次更新時間	>=,<=	
系統上次啟動	>=,<=	
KSC擴充狀態	in	裝置的擴充狀態。 可以選擇多個值。
即時防護狀態	=	受管理裝置上安裝的卡巴斯基應用程式的狀態。
加密狀態	=	
垃圾郵件防護狀態	=	
郵件伺服器的病毒防護狀態	=	
資料外洩防護狀態	=	
KSC擴充狀態ID	=	
Endpoint Sensor 狀態	=	
最後一次出現於	>=,<=	

3. 使用**測試條件**按鈕確保指定的篩選器正確無誤。點選此按鈕後，您將看到**給定條件的資產**視窗，其中包含滿足搜尋條件的資產清單。

- **響應式**– 類別將使用關聯規則填入資產。

5. 按一下**儲存**按鈕。

新類別將新增至資產類別樹。

設定資產表

在OSMP中，您可以設定資產表中顯示的欄位的內容和順序。這些設定儲存在您的本機裝置上。

若要配置顯示資產表的設定：

1. 在主功能表中，**資產管理 → 資產（裝置） → 偵測和響應**。
2. 點按資產表右上角的**設定**圖示（ ）。
3. 在下拉清單中，選取要在表格中檢視的參數旁的核取方塊：
   - **名稱**
   - **FQDN**
   - **IP位址**
   - **類別**
   - **Mac 位址**
   - **資產來源**
   - **作業系統**
   - **建立者**
   - **更新日期**
   - **最後一次出現於**
   - **租用戶**—選取此核取方塊並將該列顯示在資產表中時，**租用戶**直欄的下拉清單中將提供下列資產篩選選項：
     - **僅顯示子實例**—僅顯示所選租用戶層級結構中子實例的資產。
     - **僅顯示父實例**—僅顯示所選租用戶層級結構中父實例的資產。

       這些選項可讓您根據資產所屬層級結構的位置篩選資產，從而幫助您專注於更高層級（父實例）或更低層級（子實例）的實例。所選篩選條件將立即應用於資產表。
   - **CII類別**
   - **已歸檔**—選取此核取方塊並將此列顯示在資產表中時，**已歸檔**直欄的下拉清單中將提供下列資產篩選選項：
     - **是**—僅顯示已歸檔的資產。
     - **否**—僅顯示活動資產。
   - **權重**

- **KSC群組**
- **遙測資料接收於**
- **遙測狀態**
- **EDR狀態**
- **與KSC的上次連線時間**
- **與EDR的上次連線時間**
- **EDR產品授權**
- **EDR代理程式版本**
- **EDR隔離度**
- **AI分數**

選取核取方塊後，資產表將會更新並新增欄位。清除核取方塊後，此直欄將消失。可以根據多直欄對表單進行排序。

4. 如果需要變更直欄的順序，請在列名上按一下滑鼠左鍵，然後將其拖曳到表中的所需位置。

資產表顯示設定已配置。

搜尋資產

OSMP有兩種資產搜尋模式。您可以點選視窗左上角的按鈕在搜尋模式之間切換：

- – 透過以下資產設定進行簡單搜尋：**名稱**、**FQDN**、**IP 位址**、**MAC 位址**和**所有者**。
- – 使用依條件和條件群組篩選的進階資產搜尋。

您可以選取找到的資產旁的核取方塊，將其資料匯出到CSV檔案。

簡單搜尋

若要使用簡單搜尋尋找資產，

請在 **資產管理 → 資產（裝置） → 偵測和響應**區段的**搜尋**欄位中輸入搜尋查詢。

表單顯示符合搜尋條件的資產，其**名稱**、 **FQDN**、 **IP位址**、 **MAC位址**和**所有者**設定均符合。

進階搜尋

若要使用進階搜尋找尋資產：

1. 在 **資產管理 → 資產（裝置） → 偵測和響應**區段中，按一下漏斗圖示（ ）。
   資產篩選設定顯示在視窗上部。

2. 指定資產篩選設定，然後按一下**搜尋**按鈕。
   有關資產篩選設定的詳細資訊，請參見下表。

表單顯示符合搜尋條件的資產。

進階資產搜尋使用可在視窗上部指定的篩選條件進行：

- 您可以點選**新增條件**按鈕來新增包含用於識別條件的欄位的字串。
- 您可以點選**新增群組**按鈕來新增篩選器群組。群組運算子可以在**AND** 、 **OR**和**NOT**之間切換。
- 可以使用滑鼠拖曳條件和條件群組。
- 可以透過點選 按鈕刪除條件、群組和篩選器。
- 您可以點選**折疊**按鈕折疊篩選選項。在這種情況下，將顯示產生的搜尋運算式。點選此按鈕將再次顯示完整的搜尋條件。
- 您可以點選**清除**按鈕重設篩選選項。
- 右運算元的條件運算子和可用值取決於所選的左運算元：

左運算元	可用運算子	右運算元
版本編號	=, ilike	任意值。
作業系統	=, ilike	任意值。
IP位址	inSubnet, inRange	任意值或值的範圍。 若左運算元中的 IP 位址包含於右運算元所指定的子網路中，則符合 inSubnet 運算子的篩選條件。例如，IP 位址 10.80.16.206 的子網路應於右運算元中以斜線標記法指定如下：`10.80.16.206/25`。
FQDN	=, ilike	任意值。
CVE	=, in	任意值。 **in** 運算子可讓您指定 CVE（常見弱點與披露）ID 陣列，例如 `CVE-2017-0143`。
CVSS	>, >=, =, <=, <	0到10之間的數字（資產CVE弱點的可能嚴重程度）。 不適用於來自Open Single Management Platform的弱點。

CVE數量	>, >=, =, <=, <	數字。資產中具有CVE屬性的獨特弱點數量。沒有CVE的弱點不計入此數字。
		如果將 `0` 指定為右運算元，並且選擇 `=` 或 `<=` 運算子，搜尋結果將包括沒有CVE弱點的資產。
		若要以特定嚴重等級的CVE數量進行分類，可以使用組合條件。例如：
		`CVE count >= 1`
		`CVSS >= 6.5`

軟體	=, ilike	任意值。

軟體版本	=, ilike, in	任意值。資產上安裝的軟體版本（內部版本）編號。
資產來源	in	• Open Single Management Platform。 • KICS/KATA。 • 已手動建立
CII	in	• 資訊資源不是CII物件。 • 沒有重要性類別的CII物件。 • 第三類重要性的CII物件。 • 第二類重要性的CII物件。 • 第一類重要性的CII物件。
RAM（位元組）	=, >, >=, <, <=	數字。
磁碟的數量。	=, >, >=, <, <=	數字。
網路卡數量	=, >, >=, <, <=	數字。
磁碟可用位元組	=, >, >=, <, <=	數字。
KSC群組	=, ilike	任意值。資產所屬的Open Single Management Platform管理群組名稱。
病毒資料庫上次更新時間	>=, <=	對於搜尋，時間指定為UTC時間，然後在KUMA介面中轉換為瀏覽器中設定的本機時區。 您可以透過以下方式之一指定此運算元的日期和時間： • 在日曆中選擇確切的日期。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對時間段，或兩者的組合。 有關詳細資訊，請參閱下面的*使用時間值*子部分。
資訊上次更新時間	>=, <=	對於搜尋，時間指定為UTC時間，然後在KUMA介面中轉換為瀏覽器中設定的本機時區。 您可以透過以下方式之一指定此運算元的日期和時間： • 在日曆中選擇確切的日期。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對時間段，或兩者的組合。 有關詳細資訊，請參閱下面的*使用時間值*子部分。
防護上次更新時間	>=, <=	對於搜尋，時間指定為UTC時間，然後在KUMA介面中轉換為瀏覽器中設定的本機時區。 您可以透過以下方式之一指定此運算元的日期和時間： • 在日曆中選擇確切的日期。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對時間段，或兩者的組合。 有關詳細資訊，請參閱下面的*使用時間值*子部分。

系統上次啟動	>=, <=	對於搜尋，時間指定為UTC時間，然後在KUMA介面中轉換為瀏覽器中設定的本機時區。 您可以透過以下方式之一指定此運算元的日期和時間： • 在日曆中選擇確切的日期。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對時間段，或兩者的組合。 有關詳細資訊，請參閱下面的*使用時間值*子部分。
KSC擴充狀態	in	• 安裝了網路代理程式的主機已連線到網路，但網路代理程式未啟動 • 防毒應用程式已安裝，但實時防護沒有運行。 • 防毒應用程式已安裝，但沒有運行。 • 偵測到的病毒數量過多。 • 防毒應用程式已安裝，但實時防護狀態與安全管理員設定的狀態不同。 • 防毒應用程式未安裝。 • 太久未進行全面病毒掃描。 • 病毒資料庫太久未更新。 • 網路代理程式太久未活動。 • 舊產品授權。 • 未修復物件數量過多。 • 需要重新啟動。 • 主機上安裝了不相容的應用程式 • 主機存在一個或多個弱點。 • 在主機上掃描作業系統更新太久未執行了 • 主機的加密狀態無效 • 行動裝置設定不符合安全政策需求。 • 存在未處理事件。 • 主機狀態由受管理的應用程式建議。 • 主機上的磁碟空間不足。發生同步錯誤，或磁碟空間不足
即時防護狀態	=	• 未知。 • 已停止。 • 暫停。 • 啟動中。 • 執行中（如果防毒應用程式不支援「執行中」狀態類別）。 • 執行中（追求最大防護）。 • 執行中（追求最大速度）。 • 執行中（使用建議設定）。 • 執行中（使用自訂設定）。 • 錯誤。
加密狀態	=	• 主機上未設定加密規則。 • 工作正在執行中 • 加密已被使用者取消。 • 發生錯誤。 • 滿足所有主機加密規則。 • 加密正在執行中，必須重新啟動主機。 • 在主機上偵測到未指定加密規則的加密檔案。
垃圾郵件防護狀態	=	• 未知。 • 已停止。 • 暫停。 • 啟動中。 • 執行中。 • 錯誤。 • 未安裝。 • 無產品授權。
郵件伺服器的病毒防護狀態	=	• 未知。 • 已停止。 • 暫停。 • 啟動中。 • 執行中。 • 錯誤。 • 未安裝。 • 無產品授權。
資料外洩防護狀態	=	• 未知。 • 已停止。 • 暫停。 • 啟動中。 • 執行中。 • 錯誤。 • 未安裝。 • 無產品授權。
KSC擴充狀態ID	=	• 確定 • 緊急。 • 警告。

Endpoint Sensor 狀態	=	• 未知。 • 已停止。 • 暫停。 • 啟動中。 • 執行中。 • 錯誤。 • 未安裝。 • 無產品授權。
上一次可見	>=, <=	對於搜尋，時間指定為UTC時間，然後在KUMA介面中轉換為瀏覽器中設定的本機時區。 您可以透過以下方式之一指定此運算元的日期和時間： • 在日曆中選擇確切的日期。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對時間段，或兩者的組合。 有關詳細資訊，請參閱下面的*使用時間值*子部分。
分數ML	=, >, >=, <, <=	數字。AI服務指派的資產分數。
狀態	=, in	AI服務指派的資產狀態： • 低。 • 中等。 • 高。 • 緊急。
自訂資產欄位	=, ilike	任意值。搜尋資產的自訂欄位。

使用時間值

某些條件（例如**病毒資料庫上次更新時間**或**系統上次啟動時間**）使用日期和時間作為運算元值。對於這些條件，您可以使用確切日期和時間或相對時間段。

若要指定日期和時間值：

1. 選擇一個運算元和一個運算子，然後點選日期欄位。
2. 執行以下操作之一：

   - 在日曆中選擇確切的日期。

     預設情況下，目前時間會自動新增到所選日期，精確度為毫秒。更改日曆中的日期不會變更指定的時間。日期和時間會顯示在瀏覽器的時區。您可以根據需要在欄位中編輯日期和時間。

   - 在**相對時間段**清單中，選擇一個相對時間段。

     該期間是相對於當前搜尋的開始時間計算的，並考慮到了當時最新的資產資訊。例如，對於**病毒資料庫上次更新時間**條件，您可以選擇**1小時**和**>=**運算子，找到那些病毒資料庫沒有更新超過1小時的資產。

   - 在日期和時間欄位中，手動輸入一個值。

     您可以以**DD.MM.YYYY HH:mm:ss.SSS**格式（對於俄文在地化）和**YYYY-MM-DD HH:mm:** ss.SSS 格式（對於英文在地化）輸入確切的日期和時間，或者以公式的形式輸入相對時間段。您也可以根據需要結合使用這些方法。

     如果在輸入確切日期時未指定毫秒，則會自動替換為000。

     在相對時間段公式中，您可以使用**now**參數表示當前日期和時間以及間隔參數化語言：**+**、**-**、**/**（四捨五入到最接近的數），以及時間單位：**y**（年）、**M**（月）、**w**（週）、**d**（天）、**h**（小時）、**m**（分鐘）、**s**（秒）。

     例如，對於**資訊上次更新時間**條件，您可以指定**now-2d**搭配**>=**操作員，並指定**now-1d**搭配**>=**操作員，以尋找資訊上次更新時間為搜尋開始前一天的資產；或者，您可以指定**now/w**搭配**<=**操作員，以尋找資訊上次更新時間介於本週第一天開始時間（00:00:00:000 UTC）與目前時間**now**之間的資產。

KUMA以UTC格式儲存時間值，但在使用者介面中，時間會轉換為瀏覽器的時區。這與相對時間段相關：**今天**、**昨天**、**本週**和**本月**。例如，如果您瀏覽器中的時區是UTC+3，並且您選擇**今天**作為時間段，則類別將涵蓋從03:00:00.000到現在的資產，而不是從00:00:00.000到現在的資產。

如果您想在選擇相對時間段（例如**今天**、**昨天**、**本週**或**本月**）時考慮您的時區，則需要在日期和時間字段中手動新增時間偏移量，即加上或減去正確的小時數。例如，如果您瀏覽器的時區是UTC+3，並且您希望分類涵蓋**昨天**時段，則需要將數值變更為**now-1d/d-3h**。如果您希望分類涵蓋**今天**時間段，請將數值變更為**now/d-3h**。

匯出資產資料

您可以將資產表中顯示的資產資料匯出為CSV檔案。

若要匯出資產資料：

1. 設定資產表。

   僅表中指定的資料會寫入檔案。資產表直欄的顯示順序將保留在匯出的檔案中。

2. 找到所需的資產並選中它們旁邊的核取方塊。

   您可以透過選取資產表標頭左側的核取方塊來一次選取表中的所有資產。

3. 按一下**匯出CSV**按鈕。

資產資料將寫入assets_<export date>_<export time>.csv檔案。此檔案根據您的瀏覽器設定下載。

檢視資產詳細資訊

若要檢視有關資產的資訊，請透過以下其中一種方式開啟資產資訊視窗：

- 在主選單中，選擇**資產管理**部分→選擇一個包含相關資產的類別→選擇一個資產。
- 在主選單中，選擇**警示**→按一下包含相關警示的連結→在**相關端點**區段中選擇資產。
- 在主選單中，選擇**事件**部分→搜尋和篩選事件→選擇相關事件→點擊以下欄位之一的連結：SourceAssetID、DestinationAssetID或DeviceAssetID。

資產詳情視窗中可能會顯示以下資訊：

- **名稱**、**ID** — 資產名稱和ID。

  匯入到OSMP的資產保留在來源中指派給它們的名稱。您可以在 OSMP Web 介面中變更這些資產名稱。

- **租用戶** — 擁有資產的租用戶的名稱。
- **已歸檔**— 資產的歸檔狀態。可能的值： Yes、 No。
- **KSC群組**— 資產所屬的KSC伺服器群組。
- **資產來源**— 有關資產的資訊來源。可能有多個來源。例如，可以在OSMP網頁介面中或使用API新增資訊，也可以從Open Single Management Platform和KICS/KATA匯入資訊。

  當使用多個來源將有關相同資產的資訊新增至OSMP時，您應該考慮合併資產資料的規則。

- **建立時間** — 資產新增至OSMP的日期和時間。
- **更新時間** — 資產資訊的最近修改日期和時間。
- **擁有者**— 資產的所有者（如果提供）。
- **IP位址**— 資產的IP位址（如果有）。

  如果OSMP中有多個具有相同IP位址的資產，則透過IP位址搜尋資產時，請務必傳回最新新增的資產。如果具有相同IP位址的資產可以在組織網路中共存，請進行相應規劃並使用其他屬性來識別這些資產。例如，這在關聯過程中可能非常重要。

- **FQDN** —資產的完全限定網域名稱（如有）。
- **Mac 位址**— 資產的MAC位址（如有）。
- **作業系統**— 資產的作業系統。
- **分數 AI**—個數值，用於量化資產活動的非典型程度，以及是否值得關注。**AI狀態**欄位的可能值為：**低**、**中**、**高**、**緊急**。AI分數的值範圍為0到1。
- **隔離狀態**是指資產的網路隔離狀態。您可以點擊狀態旁的**設定**連結來檢視和變更裝置的網路隔離狀態。如果資產（裝置）上安裝了內建代理程式的Kaspersky Endpoint Security應用程式，則會顯示此欄位。
- **CII 類別**—資產是否為關鍵資訊基礎設施 (CII) 物件的相關資訊。
- **相關警示**— 與資產相關的警示（如有）。

  若要檢視與資產相關的警示清單，請點選**在警示中找尋**連結。這將打開**警示**頁籤，其中設定的搜尋運算式用於篩選具有相應資產ID的所有資產。

- **軟體資訊**和**硬體資訊**— 如果提供了資產軟體和硬體參數，則它們將顯示在此區段。
- 資產弱點資訊：
  - **卡巴斯基安全管理中心弱點**— 資產的弱點（如果提供）。此資訊適用於從Open Single Management Platform匯入的資產。

    您可以透過點選圖示來了解有關弱點的更多資訊，該圖示會開啟 Kaspersky Threats Portal。您也可以透過點擊**更新**連結並從卡巴斯基安全管理中心要求更新的資訊來更新弱點清單。

  - **KICS/KATA弱點**— 資產的弱點（如果提供）。此資訊適用於從KICS/KATA匯入的資產。
- 資產來源資訊：
  - **上次出現時間**— 上次從Open Single Management Platform收到有關資產的資訊的時間。此資訊適用於從Open Single Management Platform匯入的資產。
  - **主機 ID**— 從中接收資產資訊的Open Single Management Platform*網路代理程式*的ID。此資訊適用於從Open Single Management Platform匯入的資產。此ID用於確定資產在Open Single Management Platform中的唯一性。
  - **KICS/KATA 伺服器 IP 位址**和**KICS/KATA 連接器 ID** — 有關匯入資產的KICS/KATA實例的資料。
- **自訂欄位**—寫入資產自訂欄位的資料。

- 有關安裝了Kaspersky Endpoint Security for Windows或Kaspersky Endpoint Security for Linux的資產防護設定的其他資訊：
  - **KSC 延伸狀態 ID** — 資產狀態。它可以具有以下值：
    - 確定
    - 嚴重
    - 警告
  - **KSC 延伸狀態**— 有關資產狀態的資訊。例如，**病毒資料庫太久未更新了**。
  - **即時防護狀態**— 安裝在資產上的卡巴斯基應用程式的狀態。例如：**運行中（如果防毒應用程式不支援「運行中」狀態類別）**。
  - **加密狀態**— 有關資產加密的資訊。例如：**主機沒有任何加密規則**。
  - **垃圾郵件防護狀態**— 反垃圾郵件防護的狀態。例如，**啟動中**。
  - **郵件伺服器的病毒防護狀態**— 郵件伺服器的病毒防護狀態。例如，**啟動中**。
  - **資料外洩防護狀態**— 資料外洩防護的狀態。例如，**啟動中**。
  - **端點感測器狀態** — 資料外洩防護的狀態。例如，**啟動中**。
  - **病毒資料庫上次更新時間**- 已下載病毒資料庫的版本。
  - **防護上次更新時間**- 病毒資料庫上次更新的時間。
  - **系統上次啟動時間**—系統上次啟動的時間。
  - **資訊上次更新時間**是資產上次出現在網路上的時間。對於搜尋，時間指定為UTC時間，然後在KUMA介面中轉換為瀏覽器中設定的本機時區。

  如果資產是從Open Single Management Platform匯入的，則會顯示此資訊。
- **類別**— 與資產關聯的類別（如果有）。

點選**移至 KSC 群組**按鈕，即可在 Open Single Management Platform 管理群組之間移動正在檢視的資產。您也可以點選**啟動工作**下拉清單來執行資產上可用的工作：

- 點選**KSC 回應**按鈕，即可在資產上啟動Open Single Management Platform工作；
- 點選**KEDR 回應**按鈕，即可在資產上執行Kaspersky Endpoint Detection and Response工作。
- 點擊**重新整理 KSC 資產**按鈕，即可執行工作以從Open Single Management Platform刷新有關該資產的資訊。

這些工作可在與 Open Single Management Platform 整合及與 Kaspersky Endpoint Detection and Response 整合時使用。

新增資產

您可以透過以下方式新增資產資訊：

- 手動。

  您可以使用KUMA主控台或API新增資產。

- 匯入資產。

  您可以**從卡巴斯基安全管理中心**、KICS for Networks和 MaxPatrol VM 匯入資產。

  受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

  KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

  - 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
  - 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

  若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

  1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
  2. 按一下**匯入**，然後選擇以下操作之一：
     - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。

       這將開啟**匯入KSC資產**視窗。
     - 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。

       這將開啟**匯入KSC資產屬性**視窗。
  3. 在下拉清單，選取要為其執行匯入的租用戶。

     在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。

     如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。
  4. 點擊**匯入**按鈕。

  將匯入資產資訊。

  此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

當新增資產時，OSMP中已經存在的資產可以與正在新增的資產合併。

資產合併演算法：

1. 檢查卡巴斯基安全管理中心或KICS for Networks資產的唯一性。

   - 從卡巴斯基安全管理中心匯入的資產的唯一性由**主機ID**參數決定，此參數包含卡巴斯基安全管理中心*網路代理程式*識別碼。如果兩個資產的ID不同，則它們將被視為單獨的資產，不會合併。
   - 從KICS for Networks匯入的資產的唯一性由**IP位址**、**KICS for Networks伺服器IP位址**和**KICS for Networks連接器ID**參數的組合決定。如果兩個資產的任何參數不同，則它們將被視為單獨的資產，不會合併。

   如果比較的資產相符，則進一步執行演算法。

2. 確保**IP**、**MAC**和**FQDN**欄位中的值相符。

   如果至少兩個指定欄位相符，則合併資產，前提是其他欄位為空。

   可能的相符項：

   - 資產的FQDN和IP位址相符。**MAC**欄位為空。

     檢查針對整個IP位址值陣列執行。如果資產的IP位址包含在FQDN中，則認為值相符。

   - 資產的FQDN和MAC位址相符。**IP**欄位為空。

     檢查針對整個MAC位址值陣列執行。如果陣列中至少有一個值與FQDN完全相符，則認為值相符。

   - 資產的IP位址和MAC位址相符。**FQDN**欄位為空。

     檢查針對整個IP位址和MAC位址值陣列執行。如果陣列中至少有一個值完全相符，則認為值相符。

3. 確保**IP**、**MAC**或**FQDN**欄位中至少一個的值相符，前提是其中一個或兩個資產的另外兩個欄位未填入。

   如果欄位中的值相符，則資產會合併。例如，如果為KUMA資產指定了FQDN和IP位址，但為匯入的資產僅指定了具有相同值的IP位址，則欄位相符。在這種情況下，資產會合併。

   對於每個欄位，驗證將單獨執行，並在第一個相符時結束。

資產欄位比較範例顯示於此處。

資產資訊可以從各種來源產生。如果新增的資產和OSMP資產包含從相同來源接收的資料，則會覆蓋此資料。例如，卡巴斯基安全管理中心資產在匯入OSMP時會收到完全限定網域名稱、軟體資訊和主機ID。從卡巴斯基安全管理中心匯入具有相同完全限定域名的資產時，所有這些資料都將被覆蓋（如果已為新增的資產定義了這些資料）。所有可以重新整理資料的欄位都列在可更新資料表中。

可更新資料

欄位名稱	更新程式
名稱	根據以下優先順序選擇： • 手動定義。 • 從卡巴斯基安全管理中心收到。 • 由KICS for Networks接收。
擁有者	根據下列優先順序選擇來自來源的第一個值： • 從卡巴斯基安全管理中心收到。 • 手動定義。
IP位址	資料已合併。 如果位址陣列包含相同的位址，則會刪除重複位址的副本。

欄位名稱	更新程式
FQDN	根據下列優先順序選擇來自來源的第一個值： • 從卡巴斯基安全管理中心收到。 • 由KICS for Networks接收。 • 手動定義。
Mac 位址	資料已合併。 如果位址陣列包含相同的位址，則會刪除其中一個重複位址。
作業系統	根據下列優先順序選擇來自來源的第一個值： • 從卡巴斯基安全管理中心收到。 • 由KICS for Networks接收。 • 手動定義。
弱點	KUMA資產資料會透過新增的資產資訊進行補充。在資產詳細資訊中，資料會依來源名稱分組。 將分別消除每個來源的弱點。
軟體資訊	始終記錄來自KICS for Networks的資料（如果可用）。 對於其他來源，將根據以下優先順序選擇第一個值： • 從卡巴斯基安全管理中心收到。 • 手動定義。
硬體資訊	根據下列優先順序選擇來自來源的第一個值： • 從卡巴斯基安全管理中心收到。 • 透過API定義。

更新後的資料將顯示在資產詳情中。您可以在KUMA主控台中檢視資產詳情。

新增資產時，此資料可能會被覆蓋。如果用於產生資產資訊的資料超過30天未從來源更新，則會刪除此資產。下次從相同來源新增資產時，將建立新資產。

如果您使用KUMA主控台來編輯從卡巴斯基安全管理中心或KICS for Networks收到的資產資訊，則可以編輯以下資產資料：

- 名稱。
- 類別。

如果資產資訊是手動新增的，則可以在OSMP主控台中編輯這些資產時編輯以下資產資料：

- 名稱。
- 擁有資產的租用戶的名稱。
- IP位址。
- 完全限定網域名稱。
- MAC位址。
- 擁有者。
- 類別。
- 作業系統。
- 硬體資訊。

無法透過REST API編輯資產資料。從REST API匯入時，資料將根據上面提供的合併資產詳情的規則進行更新。

在OSMP中新增資產資訊

若要在OSMP中新增資產：

1. 在主功能表中，轉到**資產管理→資產（裝置）→偵測和響應**，然後點擊**新增**。
   新增資產詳情區域將在視窗右側開啟。
2. 若要輸入資產參數：
   - **資產名稱**（必填）
   - **租用戶**（必填）
   - **IP 位址**和/或 **FQDN**（必填）您可以按一下**新增 FQDN**來指定多個 FQDN。
   - **MAC位址。**
   - **擁有者。**
3. 如有必要，請管理下列索引標籤上的設定：
   - **附加** 索引標籤包含資產擁有者、類別和作業系統的資訊。
   - **硬體**索引標籤包含資產硬體的資訊。
4. 按一下**新增**。

   資產在指派給它的類別或**未分類資產**類別的資產表中建立和顯示。

從卡巴斯基安全管理中心匯入資產資訊

受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

- 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
- 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 按一下**匯入**，然後選擇以下操作之一：
   - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。
     這將開啟**匯入KSC資產**視窗。

- 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。

  這將開啟**匯入KSC資產屬性**視窗。

3. 在下拉清單，選取要為其執行匯入的租用戶。

   在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。

   如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。

4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

從MaxPatrol匯入資產資訊

您可以將資產資訊從MaxPatrol VM匯入XDR。匯入的資產顯示在**資產**群組中。您可以根據需要編輯資產的設定。

從MaxPatrol VM匯入資產資訊

OSMP分發套件包含kuma-ptvm公用程序，此公用程式由一個可執行檔和一個組態檔組成。此公用程式支援Windows和Linux作業系統。此公用程式可讓您連線到MaxPatrol VM API以獲取有關裝置及其屬性（包括弱點）的資料，還允許您編輯資產資料並使用XDR API匯入資料。MaxPatrol VM版本1.1至2.7（含）支援匯入資料。

設定將資產資訊從MaxPatrol VM匯入到KUMA Core涉及以下步驟：

1. 準備XDR和MaxPatrol VM。

   您必須為API操作建立使用者帳戶和XDR權杖。

2. 建立包含資料匯出和匯入設定的組態檔。

3. 使用kuma-ptvm公用程式將資產資料匯入KUMA Core：

   a. 資料從MaxPatrol VM匯出並儲存在公用程式的目錄中。每個租用戶的資訊都以JSON格式儲存到單獨的檔案中。

      您可以根據需要編輯收到的檔案。

   b. 檔案中的資訊會被匯入KUMA Core。

重新匯入現有資產時，KUMA Core中已存在的資產將會被覆蓋。透過這種方式，修復的弱點就被消除了。

已知限制：

- 如果為兩個具有不同 FQDN 的資產指定相同的 IP 位址，KUMA Core 會將這類資產匯入為兩個不同的資產。這些資產不會合併。

- 如果一個資產在名稱、版本、供應商欄位中有兩個具有相同資料的軟體，KUMA Core會將這些資料匯入為一個軟體，儘管資產中的軟體安裝路徑不同。

- 如果資產的 FQDN 包含空格或底線 (_)，則不會將這類資產的資料匯入 KUMA Core。事件記錄會指出匯入時已略過這些資產。
- 如果匯入過程中發生錯誤，則會記錄錯誤詳情並停止匯入。

準備操作：

1. 在XDR和MaxPatrol VM中建立一個單獨的使用者帳戶，並賦予其使用API請求所需的最低權限。
2. 建立稍後將為其產生API權杖的使用者帳戶。

   對產生API權杖的帳戶的需求：

   - 主管理員、租用戶管理員、二級分析師或一級分析師角色。
   - 存取將匯入資產的租用戶。
   - 在使用者帳戶的API存取權限下，選取POST /xdr/api/v2.1/kuma/assets/import核取方塊。
3. 產生用於存取XDR REST API的權杖。
4. 將kuma-ptvm公用程式複製到託管KUMA Core的伺服器，並透過執行以下命令使該公用程式的檔案可執行：

   ```
   chmod +x <path to the kuma-ptvm file on the server hosting the KUMA Core>
   ```

若要建立組態檔：

1. 轉至KUMA公用程式資料夾：

   ```
   cd /opt/kaspersky/kuma/utils/
   ```

2. 複製kuma-ptvm-config-template.yaml範本以建立名為kuma-ptvm-config.yaml的組態檔：

   ```
   cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
   ```

3. 編輯kuma-ptvm-config.yaml組態檔中的設定。
4. 將變更儲存到檔案。

組態檔隨即建立。

若要匯入資產資訊：

1. 若要將資產資訊從MaxPatrol VM匯入KUMA Core，而不會對匯出的資料進行中間驗證，請使用下列選項執行kuma-ptvm公用程式：

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download --upload`

2. 若要從MaxPatrol VM匯出的資料匯入KUMA Core之前檢查其正確性：

   a. 請使用下列選項執行kuma-ptvm公用程式：

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download`

對於組態檔中指定的每個租用戶，將建立一個單獨的檔案，其名稱為<租用戶ID>.JSON。此外，在匯出期間，將建立一個「租用戶」檔案，其中包含要上傳到KUMA Core的JSON檔案清單。所有檔案都儲存在公用程式的目錄中。

b. 檢查匯出的資產檔案，請根據需要進行以下編輯：

- 將資產指派給相應的租用戶。
- 手動將資產資料從「預設」租用戶檔案傳輸到相關租用戶的檔案。
- 在「租用戶」檔案中，編輯要將其資產匯入KUMA Core的租用戶清單。

c. 將資產資訊匯入KUMA Core：

```
kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --upload
```

若要檢視此公用程式可用命令的資訊，請執行--help命令。

資產資訊將從MaxPatrol VM匯入KUMA Core。主控台顯示有關新資產和更新資產數量的資訊。

可能發生的錯誤：

執行kuma-ptvm公用程式時，可能會傳回`tls: failed to verify certificate: x509: certificate is valid for localhost`錯誤。

若要解決此問題：

- 根據MaxPatrol說明文件簽發憑證。我們建議透過這種方式解決錯誤。
- 禁用憑證驗證。

  若要停用憑證驗證，請在組態檔的「MaxPatrol設定」部分中新增下列行：

  ```
  ignore_server_cert: true
  ```

因此，公用程式啟動時不會發生錯誤。

從MaxPatrol VM匯入資產資訊

OSMP分發套件包含kuma-ptvm公用程序，此公用程式由一個可執行檔和一個組態檔組成。此公用程式支援Windows和Linux作業系統。此公用程式可讓您連線至 MaxPatrol VM API，以取得裝置及其屬性（包括弱點）的相關資料，還可讓您編輯資產資料，並使用 KUMA API 匯入資料。MaxPatrol VM版本1.1至2.7（含）支援匯入資料。

設定從 MaxPatrol VM 將資產資訊匯入 OSMP 包括以下步驟：

1. 準備 KUMA 和 MaxPatrol VM。

   您必須建立使用者帳戶和 OSMP 權杖，才能執行 API 作業。

2. 建立包含資料匯出和匯入設定的組態檔。

3. 使用 kuma-ptvm 公用程式將資產資料匯入 OSMP：

   a. 資料從MaxPatrol VM匯出並儲存在公用程式的目錄中。每個租用戶的資訊都以JSON格式儲存到單獨的檔案中。

   您可以根據需要編輯收到的檔案。

   b. 將檔案中的資訊匯入 OSMP。

重新匯入現有資產時，OSMP 中已存在的資產會遭到覆寫。透過這種方式，修復的弱點就被消除了。

已知限制

如果為 FQDN 不同的兩個資產指定相同的 IP 位址，OSMP 會將其匯入為兩個不同的資產，而不會合併這些資產。

如果某個資產包含兩個軟體，且其名稱、版本和供應商欄位中的資料相同，則 OSMP 會將這些資料匯入為同一個軟體，即使這些軟體在資產中的安裝路徑不同。

如果您在 kuma-ptvm-config.yaml 組態檔中將 `strict_import` 設為 false，則會從 MaxPatrol 匯入所有資產的資料，包括缺少 OSMP 必要欄位的資產，以及欄位值不受 OSMP 允許的資產。如果資產的 FQDN 包含空格或底線 ("_")，則不會將此類資產的資料匯入 OSMP，且日誌會指出匯入期間已略過這些資產。

如果匯入過程中發生錯誤，則會記錄錯誤詳情並停止匯入。

準備工作

1. 在 OSMP 和 MaxPatrol VM 中分別建立專用的使用者帳戶，並授予使用 API 要求所需的最低權限。
2. 建立稍後要為其產生 API 權杖的使用者帳戶。

   對產生API權杖的帳戶的需求：

   - 主管理員、租用戶管理員、二級分析師或一級分析師角色。
   - 存取將匯入資產的租用戶。
   - 在使用者帳戶的 **API 存取權限** 下，選取 POST/api/v1/assets/import 的核取方塊。
3. 產生用於存取 OSMP REST API 的權杖。

建立組態檔

若要建立組態檔：

1. 執行下列命令，前往 OSMP 清單檔案中 utils 區段所指定主機的目錄：

   ```
   cd /opt/kaspersky/kuma/utils/
   ```

2. 執行下列命令解壓縮 kuma-ptvm.tar.gz 壓縮檔案：

   `tar -xvf kuma-ptvm.tar.gz`

3. 根據您要匯入資產的方式建立組態檔：

   - 若要匯入所有資產，請複製 `kuma-ptvm-config-template.yaml` 範本，以建立名為 `kuma-ptvm-config.yaml` 的組態檔：

     ```
     cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
     ```

   - 若要僅匯入符合篩選條件的資產，請複製 `kuma-ptvm-vulnerable-assets-config-template.yaml` 範本，以建立名為 `kuma-ptvm-vulnerable-assets-config.yaml` 的組態檔：

     ```
     cp kuma-ptvm-vulnerable-assets-config-template.yaml kuma-ptvm-vulnerable-assets-config.yaml
     ```

4. 根據所選的資產匯入方式，編輯 kuma-ptvm-config.yaml 組態檔中的設定，或編輯 kuma-ptvm-vulnerable-assets-config-template.yaml 組態檔中的設定。

5. 將變更儲存到檔案。

組態檔隨即建立。前往「匯入資產資料」步驟。

匯入資產資料

若要將資產資訊從 MaxPatrol VM 匯入 OSMP，請搭配上一步建立的組態檔使用 kuma-ptvm 公用程式。

若要匯入資產資訊：

1. 如果您要將資產資訊從 MaxPatrol VM 匯入 OSMP，而不先驗證匯出的資料，請根據所選的資產匯入方式，使用下列選項執行 kuma-ptvm 公用程式：

   - 若要匯入所有資產：

     ```
     ./kuma-ptvm --config <path> --download --upload
     ```

     其中：

     <path> 是 `kuma-ptvm-config.yaml` 組態檔的完整路徑。

   - 若要匯入依組態檔中指定參數篩選的資產：

     ```
     kuma-ptvm vulnerable-assets-api --config <path> --download --upload
     ```

     其中：

     <path> 是 `kuma-ptvm-vulnerable-assets-config.yaml` 組態檔的完整路徑。

2. 若要在將從 MaxPatrol VM 匯出的資料匯入 OSMP 前驗證該資料，請根據所選的資產匯入方式，執行下列其中一個命令：

   - 若要匯入所有資產，請使用下列選項執行 kuma-ptvm 公用程式：

     ```
     ./kuma-ptvm --config <path> --download
     ```

- 若要匯入依組態檔中指定參數篩選的資產：

```
kuma-ptvm vulnerable-assets-api --config <path> --download
```

其中：

<path> 是對應組態檔的完整路徑：`kuma-ptvm-config.yaml` 或 `kuma-ptvm-vulnerable-assets-config.yaml`。

如有需要，您可以使用 `--cvss-version <CVSS version number>` 選項，指定要載入哪個 CVSS 版本的資產弱點值。可用值：

- `2` 僅載入 CVSS 版本 2 的值。
- `3` 僅載入 CVSS 版本 3 的值。如果弱點僅有版本 2 的說明，CVSS 欄位會是空白。
- `latest`（預設）載入最新可用 CVSS 版本的值。如果弱點沒有 CVSS 版本 3 的值，則會使用版本 2 的值。

例如：

```
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 2 --download
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 3 --download
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version latest --download
```

其中：

<path> 是對應組態檔的完整路徑：`kuma-ptvm-config.yaml` 或 `kuma-ptvm-vulnerable-assets-config.yaml`。

系統會為組態檔中指定的每個租用戶建立一個名為 <OSMP_tenant_ID>.json 的個別檔案。此外，系統還會建立一個「tenants」檔案，其中包含要上傳至 OSMP 的 JSON 檔案清單。所有檔案都儲存在公用程式的目錄中。

a. 檢查匯出的資產檔案，請根據需要進行以下編輯：

- 將資產指派給相應的租用戶。
- 手動將資產資料從「預設」租用戶檔案傳輸到相關租用戶的檔案。
- 在「tenants」檔案中，編輯要將其資產匯入 OSMP 的租用戶清單。

b. 執行下列其中一個命令，將資產資訊匯入 OSMP：

- 若要匯入所有資產：

```
./kuma-ptvm --config <path> --upload
```

- 若要匯入依組態檔中指定參數篩選的資產：

```
kuma-ptvm vulnerable-assets-api --config <path> --upload
```

其中：

<path> 是對應組態檔的完整路徑：`kuma-ptvm-config.yaml` 或 `kuma-ptvm-vulnerable-assets-config.yaml`。

若要檢視公用程式的可用命令資訊，請執行 `--help` 命令。

資產資訊會從 MaxPatrol VM 匯入 OSMP。主控台顯示有關新資產和更新資產數量的資訊。

可能發生的錯誤

執行kuma-ptvm公用程式時，可能會傳回`tls: failed to verify certificate: x509: certificate is valid for localhost`錯誤。

解決方案。

- 根據MaxPatrol說明文件簽發憑證。我們建議透過這種方式解決錯誤。
- 禁用憑證驗證。
  若要停用憑證驗證，請在設定檔的`MaxPatrol settings`區段中新增以下一行：
  `ignore_server_cert: true`

因此，公用程式啟動時不會發生錯誤。

kuma–ptvm–config.yaml 組態檔的設定

下表列出您可以在 `kuma-ptvm-vulnerable-assets-config-template.yaml` 檔案中指定的設定。

kuma-ptvm-vulnerable-assets-config-template.yaml 組態檔中的設定說明

設定	描述	值
`General settings` 區段		
`log_level`	可選設定。 日誌記錄等級。	可用值： • `trace` • `info` • `warning` • `error` 預設設定：`info`。
`period`	可選設定。 在指定期間內更改的資產資料隨即從MaxPatrol匯出。	沒有限制。 預設設定：`30d`。
`strict_import`	可選設定。 從MaxPatrol匯出資產時，請檢查KUMA的必填欄位是否已填寫。請勿從MaxPatrol匯出未經驗證的資產。	可用值： • `true` 表示會檢查 KUMA 所需欄位是否存在。 • `false` 表示會略過檢查 KUMA 所需欄位是否存在。 預設值為 `false`。 建議從 MaxPatrol 匯出資產時指定 `true`，以便在將資產匯入 KUMA 前偵測並修正 JSON 檔案中可能的錯誤。
`parallel_downloading`	可選設定。 設定從 MaxPatrol 匯入資料時的下載模式。	可用值： • `true` 會平行下載 CSV 檔案。 • `false` 會循序下載 CSV 檔案，以減少 MaxPatrol 的負載。 預設設定為 `true`。 如果需要在資料匯入期間減少 MaxPatrol 的負載，建議指定 `false`。
`KUMA settings` 區段		
`endpoint`	必需設定。 KUMA API 伺服器的 URL。例如：kuma.example.com:7223	–

設定	描述	值
`token`	必需設定。 KUMA API 權杖。	–
`ignore_server_cert`	可選設定。 KUMA 憑證驗證。	可用值： • `true` 可停用 KUMA 憑證驗證。 • `false` 可啟用 KUMA 憑證驗證。 組態檔範本中未包含此設定。您可以手動新增此設定並將其值設為true，這將封鎖kuma-ptvm公用程式在啟動時驗證憑證。
`MaxPatrol settings` 區段		
`endpoint`	必需設定。 MaxPatrol API伺服器的URL。	–
`user`	可選設定。 MaxPatrol API使用者名稱。	–
`password`	可選設定。 MaxPatrol API使用者密碼。	–
`secret`	可選設定。 MaxPatrol API密鑰。	–
`token`	可選設定。 MaxPatrol API權杖。	若要透過 API 存取 MaxPatrol 伺服器，請指定 `user`、`password` 和 `secret` 參數的值，或 `token` 參數的值。
`ignore_server_cert`	可選設定。 驗證MaxPatrol憑證。	可用值： • `true` 表示停用MaxPatrol憑證驗證。 • `true` 表示啟用MaxPatrol憑證驗證。 組態檔範本中未包含此設定。如果發生 `tls: failed to verify certificate: x509: certificate is valid for localhost` 錯誤，您可以手動新增此設定，並將其值設為 true。在這種情況下，kuma-ptvm 實用程式不會在啟動時驗證憑證。 我們建議依照MaxPatrol文件簽發憑證，這是解決此錯誤的首選方法。
`Vulnerable Assets API Parameters` 區段 有一項限制：目前的 Swagger 合約中提供 `from` 和 `to` 參數，但是否支援這些參數取決於您部署的 PTVM 版本。		
`groups`	可選設定。 用於篩選的資產群組 ID 清單。匯入時僅包含屬於指定群組的資產。	範例： 4b7d711f-ae35-4c94-8625-4cfabf5fb99e
`statuses`	可選設定。 要篩選的資產弱點狀態。	可用值： • `new`表示弱點是新的。 • `inProgress`表示弱點正在修復。 • `awaitingFix`表示弱點正在等待修復。 • `excluded`表示弱點已從處理中排除。 • `fixed`表示弱點已修復。 • `overdue`表示弱點已超過修復期限。 • `stale`表示弱點已過時。
`severities`	可選設定。 用於篩選的資產弱點嚴重程度。	可用值： • `none`表示未設定嚴重程度。 • `low` • `medium` • `high` • `critical`
`from`	可選設定。 依資產上次稽核日期進行篩選時的開始日期和時間（含）。UTC。	範例： [待定]
`to`	可選設定。 依資產上次稽核日期進行篩選時的結束日期和時間（含）。UTC。	範例： [待定]
`Vulnerability filter` 區段		

設定	描述	值
`only_exploitable`	可選設定。 僅從MaxPatrol匯出已知漏洞利用的弱點資產。	可用值： • `true` 表示僅匯出存在已知弱點利用程式的資產。 • `false` 表示匯出所有資產。 預設設定：`false`。
`min_severity`	可選設定。 僅匯入指定等級或更高等級的弱點。	可用值： • `low` • `medium` • `high` • `critical` 預設值：`low`。
`Tenant map` 區段		
`id`	必需設定。 KUMA 中的租用戶 ID。 資產將按照組態檔中租用戶指定的順序指派給租用戶：租用戶在清單中的位置越高，其優先順序越高。這表示您可以指定重疊的子網路。	–
`fqdn`	可選設定。 用於搜尋資產FQDN的規則運算式。	–
`networks`	可選設定。 一個或多個子網路。	–
`default_tenant`	可選設定。 用於無法配置給「租用戶」區段中所指定租用戶之資產資料的預設 KUMA 租用戶。	–

從KICS for Networks匯入資產資訊

受KICS for Networks保護的資產資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

設定KICS for Networks整合後，會自動建立以取得KICS for Networks資產資料的工作。執行時間：

- 建立新整合後立即執行。
- 更改現有整合設定後立即執行。
- 根據常規排程，每隔幾小時。預設情況下，每12小時。可以更改排程。

可以手動建立帳戶資料更新工作。

若要設定工作來更新租用戶的KICS for Networks資產資料：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要匯入KICS/KATA資產的租用戶。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤的**偵測與回應**下，按一下**資產設定**。
4. 在**KICS/KATA匯入**頁籤上，確保**狀態**切換開關已開啟。

5. 設定資產資料匯入：

- 若要安排定期匯入，請在**匯入間隔（小時）**欄位中指定OSMP更新KICS/KATA資產資料的時間間隔。
- 若要手動執行導入，請按一下**匯入**按鈕。

從選定租用戶接收帳戶資料的**工作**將會新增至OSMP主控台的工作管理器部分。

匯入過程中資產欄位比較的範例

每個匯入的資產都會與相符的OSMP資產進行比較。

檢查IP、 MAC和FQDN欄位中的兩個欄位值是否符合

比較的資產	比較的欄位		
	FQDN	IP	MAC
KUMA資產	是	是	空
匯入的資產1	是，相符	是，相符	是
匯入的資產2	是，相符	是，相符	空
匯入的資產3	是，相符	空	是
匯入的資產4	空	是，相符	是
匯入的資產5	是，相符	空	空
匯入的資產6	空	空	是

比較結果：

- 匯入的資產1與OSMP資產：FQDN和IP欄位已填入且相符，兩個資產的MAC欄位不衝突。資產已合併。
- 匯入的資產2與OSMP資產：FQDN和IP欄位已填入且相符。資產已合併。
- 匯入的資產3與OSMP資產：FQDN和MAC欄位已填入且相符，兩個資產的IP欄位不衝突。資產已合併。
- 導入的資產4和OSMP資產：IP欄位已填入且相符，兩個資產的FQDN和MAC欄位不衝突。資產已合併。
- 匯入的資產5與OSMP資產：FQDN欄位已填入且相符，兩個資產的IP和MAC欄位不衝突。資產已合併。
- 匯入的資產6和OSMP資產：無符合欄位。資產未合併。

檢查IP、MAC和FQDN欄位中的單一欄位值是否相符

比較的資產	比較的欄位		
	FQDN	IP	MAC
OSMP資產	空	是	空
匯入的資產1	是	是，相符	是
匯入的資產2	是	是，相符	空

比較的資產	比較的欄位		
	FQDN	IP	MAC
匯入的資產3	是	空	是
匯入的資產4	空	空	是

比較結果：

- 匯入的資產1與OSMP資產：IP欄位已填入且相符，兩個資產的FQDN和MAC欄位不衝突。資產已合併。
- 導入的資產2和OSMP資產：IP欄位已填入且相符，兩個資產的FQDN和MAC欄位不衝突。資產已合併。
- 匯入的資產3和OSMP資產：無符合欄位。資產未合併。
- 匯入的資產4和OSMP資產：沒有相符的欄位。資產未合併。

kuma-ptvm-config.yaml組態檔的設定

下表列出了您可以在kuma-ptvm-config.yaml檔案中指定的設定。

設定	描述	值
`General settings` 群組		
`log_level`	可選設定。 日誌記錄等級。	可用值： • `trace` • `info` • `warning` • `error` 預設設定：`info`。
`period`	可選設定。 在指定期間內更改的資產資料隨即從MaxPatrol匯出。	沒有限制。 預設設定：30天。
`strict_import`	可選設定。 從MaxPatrol匯出資產時，請檢查KUMA的必填欄位是否已填寫。請勿從MaxPatrol匯出未經驗證的資產。	可用值： • `true` 表示會檢查 KUMA 所需欄位是否存在。 • `false` 表示會略過檢查 KUMA 所需欄位是否存在。 預設設定：`false`。 我們建議從 MaxPatrol 匯出資產時將其設為 true。如此一來，便可在將資產匯入 XDR 前偵測並修正 JSON 檔案中可能存在的錯誤。
`KUMA settings` 群組		
`endpoint`	必需設定。 XDR API 伺服器的 URL。例如，`api.<XDR FQDN>/xdr/`	-
`token`	必需設定。 XDR API權杖。	-
`ignore_server_cert`	可選設定。 驗證XDR憑證。	可用值： `true` 表示停用憑證驗證。 `false` 表示啟用憑證驗證。 組態檔範本中未包含此設定。您可以手動新增此設定，並將其值設為 true。kuma-ptvm 公用程式在啟動時不會驗證憑證。
`MaxPatrol settings` 群組		
`endpoint`	必需設定。 MaxPatrol API伺服器的URL。	-
`user`	可選設定。 MaxPatrol API使用者名稱。	-

`password`	可選設定。 MaxPatrol API使用者密碼。	-
`secret`	可選設定。 MaxPatrol API密鑰。	-
`token`	可選設定。 MaxPatrol API權杖。	若要透過API存取MaxPatrol伺服器，請指定`user`、`password`和`secret`設定的值，或指定`token`設定的值。
`ignore_server_cert`	可選設定。 驗證MaxPatrol憑證。	可用值： • `true`表示停用MaxPatrol憑證驗證。 • `false`表示啟用MaxPatrol憑證驗證。 組態檔範本中未包含此設定。如果發生`tls: failed to verify certificate: x509: certificate is valid for localhost`錯誤，您可以手動新增此設定，並將其值設為`true`。在這種情況下，kuma-ptvm 實用程式不會在啟動時驗證憑證。 我們建議依照MaxPatrol文件簽發憑證，這是解決此錯誤的首選方法。
`Vulnerability filter`群組		
`only_exploitable`	可選設定。 僅從MaxPatrol匯出已知漏洞利用的弱點資產。	可用值： `true`表示僅匯出存在已知弱點利用程式的資產。 `false`表示匯出所有資產。 預設設定：`false`。
`min_severity`	可選設定。 僅匯入指定等級或更高等級的弱點。	可用值： • `low` • `medium` • `high` • `critical` 預設值：`low`。
`Tenant map`群組		
`id`	必需設定。 XDR中的租用戶ID。 資產將按照組態檔中租用戶指定的順序指派給租用戶：租用戶在清單中的位置越高，其優先順序越高。這表示您可以指定重疊的子網路。	-
`fqdn`	可選設定。 用於搜尋資產FQDN的規則運算式。	-
`networks`	可選設定。 一個或多個子網路。	-
`default_tenant`	可選設定。 用於儲存無法指派給「租用戶」設定群組中指定的租用戶的資產資料的預設XDR租用戶。	-

為資產指派類別

在資產屬性中為單一資產指派類別

此方法不適用於為 KSC 或 KICS 資產指派類別。請依照指示，為一個或多個資產指派類別。

若要為一個資產指派類別：

1. 在主功能表中，前往 **資產管理** → **資產（裝置）** → **偵測和響應**。
2. 點選**顯示導覽**按鈕，然後選取租用戶以及包含所需資產的類別。
   資產表隨即顯示。
3. 選取一個資產，然後在功能表中選取**顯示更多**。
4. 在開啟的視窗中，按一下**編輯**按鈕。
5. 在**附加**索引標籤的**類別**欄位中，選取類別。

   如果要將資產移至**未分類的資產**部分，則必須透過按一下 ✕ 按鈕刪除資產的現有類別。

6. 按一下**儲存**按鈕。

類別將會被指派。

為一個或多個資產指派類別

若要為一個或多個資產指派類別：

1. 在主功能表中，前往 **資產管理** → **資產（裝置）** → **偵測和響應**。
2. 點選**顯示導覽**按鈕，然後選取租用戶以及包含所需資產的類別。
   資產表隨即顯示。
3. 選取您要更改類別的資產旁邊的核取方塊。
4. 按一下**連結到類別**按鈕。
5. 在開啟的視窗中，選擇一個類別。
6. 按一下**綁定**按鈕。

類別將會被指派。

不要將`Categorized assets`類別指派給資產。

將一組資產關聯到一個類別

若要將一組資產關聯到一個類別：

1. 在**資產管理**部分，選取資產表標題中的核取方塊。
2. 選擇頁面上所有可見的資源，或選擇符合選擇條件的所有資源。
   關聯到類別按鈕隨即變成活動，並開啟可用的類別。
3. 點擊**關聯到類別**按鈕，然後選擇一個或多個要關聯到的類別。
4. 點擊**確定**。
   資產隨即與選定的類別或資料夾關聯。

將一組資產從一個類別中取消關聯

若要將一組資產從一個類別中取消關聯：

1. 在導覽窗格中選擇一個類別（租用戶）。
   該類別下的資產清單隨即顯示。
   資料夾屬性中已新增**清理類別**按鈕。
2. 在裝置的快顯表單中，選取**清理類別**。
   螢幕上會顯示一個對話方塊，其中包含確認提示以及將要取消關聯的資產數量。
   此選項可讓您取消關聯所選類別中的所有資產，而不僅僅是頁面上可見的資產。子類別中的資產並未解除關聯。
3. 在對話方塊中，按一下**確定**。
   所有選定的資產隨即從選定的類別中取消關聯。

編輯資產參數

在OSMP中，您可以編輯資產參數。所有手動新增的資產的參數都可以編輯。對於從卡巴斯基安全管理中心匯入的資產，您只能變更資產的名稱及其類別。

若要變更資產的參數：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 選擇包含相關資產的類別。
   資產表隨即顯示。
3. 選擇資產，然後按一下**詳細資訊**。

4. 在開啟的視窗中，按一下**編輯**按鈕。

   編輯資產視窗開啟。

5. 在可用欄位中進行所需的變更：

   - **資產名稱**（必填）如果資產是從卡巴斯基安全管理中心或 KICS for Networks 匯入，此欄位是唯一可編輯的欄位。
   - **IP 位址**和/或 **FQDN**（必填）。您可以指定多個以逗號分隔的 FQDN。
   - **MAC位址。**
   - **擁有者。**
   - **軟體資訊**：
     - **作業系統名稱**
     - **作業系統版本**
   - **硬體資訊**：

     硬體參數

     您可以將資產硬體的資訊新增至**硬體資訊**部分：

     用於描述資產CPU的可用欄位：

     - **CPU名稱**
     - **CPU頻率**
     - **CPU核心數**

       您可以使用**新增 CPU**按鈕為資產新增 CPU。

     用於描述資產磁碟的可用欄位：

     - **磁碟可用位元組**
     - **磁碟空間**

       您可以使用**新增磁碟**按鈕為資產新增磁碟。

     用於描述資產RAM的可用欄位：

     - **RAM頻率**
     - **RAM總位元組數**

用於描述資產網卡的可用欄位：

- **網卡名稱**
- **網卡製造商**
- **網卡驅動程式版本**

您可以使用**新增網卡**按鈕為資產新增網卡。

- **自訂欄位**。
- **CII類別**。

6. 在**附加**索引標籤的**類別**欄位中，選取類別。

您也可以選擇資產，然後將其拖曳到相關類別中。此類別將會新增至資產類別清單。

請勿將`Categorized assets`類別指派給資產。

7. 按一下**儲存**按鈕。

資產參數已變更。

歸檔資產

在OSMP中，歸檔功能適用於以下類型的資產：

- 從卡巴斯基安全管理中心和KICS匯入的資產。

  如果 OSMP 在嘗試匯入十次後仍無法取得資產資訊，該資產將自動歸檔，並依照您在 **歸檔資產的 TTL（天）** 設定中指定的時間儲存於資料庫中。預設設定為0天。這意味著歸檔資產將無限期儲存。如果OSMP在已歸檔資產的保存期限到期之前從來源收到有關資產的資產，則已歸檔資產將變為活動狀態。

- 合併資產

  匯入時，OSMP會檢查從卡巴斯基安全管理中心和KICS匯入的資產以及手動新增的資產之間的唯一性。如果匯入的資產和手動新增的資產的欄位相符，則這些資產將合併為一個資產，該資產被視為已匯入並可歸檔。

- 在主控台中手動新增或使用 API 新增的資產將歸檔並儲存在資料庫中，儲存時間由**已歸檔資產的TTL（天數）**設定指定。預設設定為0天。這意味著歸檔資產將無限期儲存。如果您希望在已歸檔資產的保留期限到期前活動該資產，可以使用**取消歸檔資產**選項。

資產在以下條件下被歸檔：

- 對於在主控台中手動建立或使用API建立的資產，請使用**歸檔資產**選項。
- OSMP 嘗試匯入十次後，仍無法從卡巴斯基安全管理中心或 KICS for Networks 取得該資產的資訊。
- 已停用與卡巴斯基安全管理中心的整合。

  如果您停用與卡巴斯基安全管理中心的整合，則資產將被視為活動狀態30天。30天后，資產將自動歸檔，並儲存在資料庫中，儲存期間在**已歸檔資產的TTL（以天為單位）**欄位中指定。

以下情況不會更新資產：

- 關於卡巴斯基安全中心資產的資訊在已歸檔資產的保存期限內沒有更新。
- 卡巴斯基安全中心或KICS for Networks中不存在有關該資產的資訊。
- 與卡巴斯基安全中心伺服器的連線已超過30天。

若要變更手動建立的資產或資產組的歸檔狀態：

1. 在主功能表中，**資產管理→資產（裝置）→分析與回應**。
   這將開啟資產表。
2. 在資產表中，選取手動建立的資產旁的核取方塊，即可變更其歸檔狀態。
3. 在資產表上方的工具列中，按一下下列按鈕之一：
   - **歸檔資產**以歸檔選定的資產。
   - **取消歸檔資產**以恢復選定的已歸檔資產。

   資產的歸檔狀態已變更。您可以在資產表中的**已歸檔**直欄的下拉清單中按歸檔狀態篩選資產，方法是選擇**是**以僅顯示已歸檔資產，或選擇**否**以僅顯示活動資產。

若要設定已歸檔資產保存期限：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇您要更改歸檔資產保留期的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤上，按一下**資產設定**。
4. 在**常規**頁籤上，在**已歸檔資產的 TTL（以天為單位）**欄位中，輸入新值。
   預設設定為30天。輸入 0 即可無限期保留已歸檔資產。
5. 按一下**儲存**按鈕。

   已歸檔資產保存期限已設定。

有關已歸檔資產的資訊仍然可以在警示和事件卡中檢視。

若要檢視已歸檔資產卡：

1. 在主功能表的**監控**下，選擇**警示**或**事件**部分。
   警示或事件清單隨即顯示。
2. 開啟連結到已歸檔資產的警示或事件卡。
   您可以在已歸檔資產卡中查看資訊。

移除資產

您可以在**管理和防護**頁籤中刪除資產。在**偵測和響應**頁籤中，OSMP 僅會自動刪除已歸檔的資產。您無法手動刪除資產。如果資產資訊的未更新時間超過已歸檔資產保存期限，OSMP會刪除該資產。

刪除資產類別

類別刪除分兩個階段進行：歸檔和永久刪除。歸檔階段允許您在將類別從系統中永久移除之前，請驗證該類別是否仍被任何資源引用。

當在OSMP父實例上歸檔某個類別時，所有OSMP子實例上的對應類別也會被歸檔。然後，系統會檢查是否仍有任何資源引用已歸檔的類別。如果沒有引用，則永久刪除該類別。

若要刪除資產類別：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 在類別樹狀圖中，按一下要刪除的類別旁邊的（⋮）圖示。
3. 在快顯表單中，選擇**歸檔**。
4. 在**刪除類別？**對話方塊中，按一下**確定**進行確認。

如果資源仍然關聯到該類別，則該類別將保持歸檔狀態，直到所有引用都被刪除。

已歸檔的類別不會出現在類別清單中，但仍可能在引用該類別的篩選器中可用。類別內容仍然可用，並且可以移除資源關聯。除類別名稱外，禁止修改類別內容。

包含子類別的類別還有其他限制：

- 如果父類別至少包含一個未歸檔的子類別，則無法歸檔或刪除該父類別。
- 必須先歸檔或永久刪除所有子類別，才能刪除父類別。
- 所有子類別歸檔後，父類別將遵循標準的歸檔和刪除流程。

只有當所有對類別的引用都被移除且所有層次結構約束都已滿足時，類別才會永久刪除。

批次刪除資產

在OSMP網頁介面中，您可以使用篩選器選擇多個資產並刪除所有選定的資產。

若要刪除資產，您必須擁有刪除資產的權限。

批次刪除資產

若要刪除所有選定的資產：

1. 在應用程式的主選單中，轉至**資產管理**部分並選擇資產類別。
   資產表隨即顯示。

2. 選取資產表標題中的核取方塊。
   您可以刪除所有資產，或刪除頁面上目前顯示的所有資產。

3. 點選**頁面中全選**或**全選**。
   刪除按鈕變為活動。

4. 點擊**刪除**按鈕。
   這將開啟一個窗口，提示您確認刪除，並告知您已刪除的資產將不會在警示、事件和小工具中可用。
   頁面下方會顯示已選取刪除的資產數量。

5. 點擊**確定**。
   如果您點選了**全選**，則必須將顯示的產生字串輸入到視窗中的文字方塊中以確認刪除。

所有選定的資產隨即刪除。

刪除資產資料夾

要刪除資料夾，您可以先取消所有資源與該資料夾的關聯（這會取消資源的關聯，但不會刪除它們），然後再刪除該資料夾本身；或者，您可以先刪除所有資源，然後再刪除該資料夾。

更新協力廠商應用程式並修復卡巴斯基安全管理中心資產上的弱點

您可以更新安裝在卡巴斯基安全管理中心資產上的協力廠商應用程式（包括Microsoft應用程式），並修復這些應用程式中的弱點。

首先，您需要在選定的卡巴斯基安全管理中心管理伺服器上使用下列設定建立*安裝必要更新並修復弱點*工作：

- 應用程式—卡巴斯基安全管理中心。
- 工作類型—*安裝必要更新並修復弱點*。
- 將被指派工作的裝置—您需要將工作指派給根管理群組。

- 安裝更新的規則：
  - 僅安裝已核准的更新。
  - 修復嚴重等級等於或高於（可選設定）的弱點。
    如果啟用該選項，更新僅修復卡巴斯基設定的嚴重等級等於或高於清單中選定的值（*中*、*高*或*嚴重*）的弱點。嚴重等級低於選定值的弱點不被修復。
- 排程啟動 - 工作執行排程。

有關如何建立工作的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

*安裝必要更新和修復弱點*工作僅在有弱點和修補程式管理產品授權下才可使用。

接下來，您需要安裝協力廠商應用程式的更新並修復OSMP中資產的弱點。

若要在OSMP的資產上安裝更新並修復協力廠商應用程式的漏洞：

1. 透過以下方式之一開啟資產詳情視窗：
   - 在主功能表中，轉到**資產管理→資產（裝置）→偵測和響應**，選擇一個包含相關資產的類別，然後選擇一個資產，然後點擊**詳情**。
   - 在主功能表中，前往**監控 → 威脅搜尋**。搜尋並篩選事件。然後選取所需的事件，並點選下列其中一個欄位中的連結：SourceAssetID、DestinationAssetID 或 DeviceAssetID。
2. 在資產詳情視窗中，延伸**卡巴斯基安全管理中心弱點**清單。
3. 選取您要更新的應用程式旁邊的核取方塊。
4. 按一下**上傳更新**連結。
5. 在開啟的視窗中，選取要修復的弱點ID旁的核取方塊。
6. 如果所選ID的**EULA已接受**直欄中顯示**否**，請按一下**核准更新**按鈕。
7. 點選**EULA URL**直欄中的連結，仔細閱讀最終使用者產品授權協議的文字。
8. 如果您同意，請按一下**接受所選EULA**。
   已接受EULA的弱點ID在**EULA已成功接受**直欄中顯示**是**。
9. 對於每個必要的弱點ID，重複步驟7-10。
10. 點擊**確定**。

更新將上傳並安裝到啟動工作的管理伺服器所管理的資產以及所有從屬管理伺服器的資產。

每台從屬管理伺服器必須分別接受最終使用者產品授權協議中關於更新和弱點修補程式的條款。

更新將安裝在偵測到弱點的資產上。

您可以在資產詳情視窗中點選**更新**連結來更新資產的弱點清單。

將資產移至選定管理群組

您可以將資產移至卡巴斯基安全管理中心的選定管理群組。在這種情況下，群組政策和工作將應用於資產。有關卡巴斯基安全管理中心任務和政策的更多詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

在**從卡巴斯基安全管理中心匯入資產**期間載入層次結構時，管理群組將會新增至OSMP。首先，您需要設定OSMP與卡巴斯基安全管理中心的整合。

受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

- 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
- 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 按一下**匯入**，然後選擇以下操作之一：
   - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。
     這將開啟**匯入KSC資產**視窗。
   - 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。
     這將開啟**匯入KSC資產屬性**視窗。
3. 在下拉清單，選取要為其執行匯入的租用戶。
   在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。
   如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。
4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

若要將資產移至選定管理群組：

1. 透過以下方式之一開啟資產詳情視窗：
   - 在主功能表中，轉到**資產管理→資產（裝置）→偵測和響應**，選擇一個包含相關資產的類別，然後選擇一個資產，然後點擊**詳情**。
   - 在主功能表中，轉至**監控 → 警示**，按一下相關警示的連結，然後在**資產**部分選擇資產，然後按一下**檢視內容**。

2. 在資產詳情視窗中，按一下**回應→移至群組**按鈕。

3. 在開啟的視窗中選擇群組。

   選定的群組必須與資產屬於同一租用戶。

4. 按一下**儲存**按鈕。

   選定的資產將被移動。

若要將多個資產移至選定的管理群組：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。

2. 選擇包含相關資產的類別。

3. 選取您要移至不同群組之裝置旁的核取方塊。

4. 點選**回應 → 移至群組**。

   如果所有選定資產都屬於同一管理伺服器，則該按鈕處於活動狀態。

5. 在開啟的視窗中選擇群組。

6. 按一下**儲存**按鈕。

   選定的資產將被移動。

資產所屬的特定群組會顯示在資產詳細資料中。

從卡巴斯基安全管理中心匯入資產資訊時，卡巴斯基安全管理中心資產資訊會在OSMP中更新。這表示可能會出現資產在卡巴斯基安全管理中心的管理群組之間移動，但資訊尚未顯示在OSMP中的情況。當嘗試將此類資產移至它已經在的管理群組時，OSMP會傳回**將資產移至另一個 KSC 群組失敗**錯誤。

資產稽核

OSMP可設定為在以下條件下產生資產稽核事件：

- 資產已新增至OSMP。該應用程式監控手動資產建立，以及透過REST API匯入期間和從**卡巴斯基安全管理中心**或KICS for Networks匯入期間的建立。

  受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

- 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
- 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 按一下**匯入**，然後選擇以下操作之一：
   - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。
     這將開啟**匯入KSC資產**視窗。
   - 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。
     這將開啟**匯入KSC資產屬性**視窗。
3. 在下拉清單，選取要為其執行匯入的租用戶。
   在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。
   如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。
4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

- 資產參數已變更。監控以下資產欄位值的變更：
  - 名稱
  - IP位址
  - MAC位址。
  - FQDN
  - 系統

  匯入期間更新資產時，欄位可能會變更。
- 資產已從OSMP中刪除。該程式監控資產的手動刪除情況，以及從卡巴斯基安全中心和KICS for Networks匯入的資產的自動刪除情況，其資料不再被接收。
- 弱點資訊已新增至資產。該程式監控資產新弱點資料的出現。例如，從卡巴斯基安全管理中心或KICS for Networks匯入資產時，可以將弱點資訊新增至資產。
- 資產弱點已解決。應用程式會監控從資產中移除弱點資訊的情況。如果不再從任何先前獲取弱點發生資訊的來源收到有關此弱點的資料，則認為該弱點已解決。

- 資產已新增至類別。應用程式會監控將資產類別指派給資產的情況。
- 資產已從類別中移除。應用程式會監控從資產類別中移除資產的情況。

預設情況下，若啟用了資產稽核功能，在上述條件下，OSMP 不僅會建立稽核事件 (`Type = 4`)，也會產生基礎事件 (`Type = 1`)。

例如，資產稽核事件可以傳送到儲存體或關聯器。

設定資產稽核

若要設定資產稽核：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇您要設定資產稽核的租用戶。

   這會開啟租用戶內容視窗。

   如果要為新租用戶設定資產審核，請先建立租用戶。
3. 在**設定**頁籤上的**偵測與回應**下，按一下**資產稽核**。
4. 對於產生資產稽核事件的每個條件，選擇要將建立的事件傳送到的目標：

   a. 在相關類型的資產稽核事件的設定區塊中，使用**新增目標**下拉清單選擇要將建立的事件傳送到的目標類型：

   - 如果要將事件傳送到儲存體，請選擇**儲存體**。
   - 如果要將事件傳送到關聯器，請選擇**關聯器**。
   - 如果要選擇不同的目標，請選擇**其他**。

     此類資源包括在該程式的先前版本中建立的關聯器和儲存體服務。

   在開啟的**新增目標**視窗中，您必須定義事件轉送的設定。

   b. 使用**目標**下拉清單選擇現有目標，或如果要建立新目標，請選擇**建立**。

   如果您要建立新目標，請依照目標描述中所示的設定進行填入。

   c. 按一下**儲存**按鈕。

   已將目標新增至產生資產稽核事件的條件。每個條件可以新增多個目標。
5. 按一下**儲存**按鈕。

資產稽核已設定完畢。將為已新增目標的條件產生資產稽核事件。按一下**儲存**按鈕。

儲存和搜尋資產稽核事件

資產稽核事件視為基礎事件，且不會取代稽核事件（稽核事件、稽核事件）。可依據下列參數搜尋資產稽核事件：

事件欄位	值
DeviceVendor	"Kaspersky"
DeviceProduct	KUMA
DeviceEventCategory	Audit assets

啟用和停用資產稽核

您可以啟用或停用租用戶的資產稽核：

若要啟用或停用租用戶的資產稽核：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要啟用或停用資產稽核的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤上的**偵測與回應**下，按一下**資產稽核**。
4. 啟用或停用**稽核事件收集**切換開關。
5. 按一下**儲存**按鈕。

預設情況下，當啟用資產稽核時，當出現稽核條件時，會同時建立兩種類型的事件：基礎事件和稽核事件。

您可以停用帶有稽核事件的基礎事件的產生。

若要啟用或停用為單一條件建立基本事件：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇要啟用或停用產生資產稽核事件條件的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤上的**偵測與回應**下，按一下**資產稽核**。
4. 按一下條件操作名稱可啟用或停用對應基礎事件的建立。
5. 按一下**儲存**按鈕。

對於已停用的條件，僅建立稽核事件，而不建立基礎事件。

自訂資產欄位

除了資產資料模型的現有欄位外，您還可以建立自訂欄位。檢視有關資產的資訊時，會顯示來自自訂欄位的資料。您可以手動或使用 API 在自訂欄位中輸入資料。

您可以在OSMP主控台的**資產**部分的**自訂欄位**表中建立或編輯自訂欄位。此表包含以下直欄：

- **名稱**– 檢視有關資產的資訊時顯示的自訂欄位的名稱。
- **預設值**– 將資產新增至KUMA時寫入自訂欄位的值。
- **遮罩**– 自訂欄位中的值必須符合的規則運算式。

若要建立自訂資產欄位：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇您要更改歸檔資產保留期的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤上，按一下**資產設定**。
4. 在**一般**頁籤上，於**自訂欄位**欄位下方按一下**新增**按鈕。
   自訂欄位表中會新增一個空白行。您可以透過自訂欄位設定一次新增多個行。
5. 若要透過自訂欄位設定填入以下直欄：
   - **名稱**（必填）- 1至128個Unicode字元。
   - **預設值**——1至1,024個Unicode字元。
   - **遮罩**——1至1,024個Unicode字元。
6. 按一下**儲存**按鈕。

自訂欄位已新增至資產資料模型。

若要刪除或編輯自訂資產欄位：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選擇您要更改歸檔資產保留期的租用戶。
   這會開啟租用戶內容視窗。
3. 在**設定**頁籤上，按一下**資產設定**。

4. 在**常規**頁籤上，對**自訂欄位**表進行必要的變更：

   - 若要刪除自訂欄位，請選取所需欄位旁的核取方塊，然後按一下**刪除**按鈕。刪除欄位也會刪除該欄位中寫入的所有資產的資料。
   - 您可以變更欄位設定的值。更改預設值不會影響先前寫入資產欄位的資料。
   - 若要變更欄位的顯示順序，請使用**上移**和**下移**按鈕。

5. 按一下**儲存**按鈕。

更改已完成。

關鍵資訊基礎設施資產

在OSMP中，您可以標記與俄羅斯聯邦關鍵資訊基礎設施（CII）相關的資產。這可讓您限制OSMP使用者處理與CII物件相關資產關聯的警示和事件的能力。

如果OSMP中GosSOPKA模組的產品授權處於活動狀態，則可以將CII類別指派給資產。

主管理員和在其設定檔中**選取**存取CII設施核取方塊的使用者可以將CII類別指派給資產。如果不符合上述任何條件，則對使用者適用以下限制：

- **CII類別**設定群組不會顯示在**資產詳情**和**編輯資產**視窗中。您無法檢視或變更資產的CII類別。
- 不可檢視與CII類別的資產關聯的警示和事件。您無法對此類警示和事件執行任何操作；它們不會顯示在警示和事件表中。
- **CII**欄不會顯示在警示和事件表中。
- 無法使用 REST API 搜尋或關閉警示。

資產的CII類別顯示在**CII類別**設定群組的**資產詳情**視窗中。

若要變更資產的CII類別：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 選擇包含相關資產的類別。

   資產表隨即顯示。
3. 選擇資產，然後按一下**詳細資訊**。

   資產詳情視窗隨即開啟。
4. 按一下**編輯**按鈕並在下拉清單中選取其中一值。

   - **資訊資源不是CII物件**— 預設值，表示該資產沒有CII類別。在設定檔中清除了**訪問CII設施**核取方塊的使用者可以使用此類資產以及與這些資產相關的警示和事件。
   - **不具重要性類別的CII物件**。
   - **重要性類別為第三類的CII物件**。

- **重要性類別為第二類的CII物件**。
- **重要性類別為第一類的CII物件**。

5. 按一下**儲存**按鈕。

佈署 Kaspersky 應用程式

本部分說明如何透過OSMP主控台在貴組織內的用戶端裝置上佈署卡巴斯基應用程式。

案例：卡巴斯基應用程式部署

此情境說明如何透過OSMP主控台佈署卡巴斯基應用程式。您可以使用防護佈署精靈，或者您可以手動完成所有必要步驟。

階段

Kaspersky 應用程式佈署分步驟進行：

1. **下載並建立安裝套件**

   手動下載軟體包。

   如果您無法透過 Kaspersky Next XDR Expert 在某些裝置（例如遠端員工的裝置）上安裝 Kaspersky 應用程式，您可以為應用程式建立獨立安裝套件。如果您使用獨立軟體套件安裝 Kaspersky 應用程式，則不必建立和執行遠端安裝工作，也不必為 Kaspersky Endpoint Security for Windows 建立和配置工作。

   或者，您可以從卡巴斯基網站下載網路代理和安全應用程式的分發套件。如果由於某種原因無法遠端安裝應用程式，您可以使用下載的分發套件本機安裝應用程式。

2. **建立、配置和執行遠端安裝工作**

   該步驟是防護部署精靈的一部分。如果您選取不執行防護佈署精靈，您必須手動建立該工作並手動配置它。

   您也可以為不同管理群組或不同裝置分類手動建立幾個遠端安裝工作。您可以在這些工作中佈署應用程式的不同版本。

   請確保搜尋到網路上所有裝置，之後執行遠端安裝工作。

   > 如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

3. **建立和配置工作**

   必須配置 Kaspersky Endpoint Security 的*更新*工作。

   手動建立此工作並手動配置。請確保工作排程滿足您的需要。（預設情況下，工作的排定開始時間設定為**手動**，但您可以選擇其他選項。）

4. **正在建立政策**

   手動建立卡巴斯基Endpoint Security政策。您可以使用預設政策設定。您也可以隨時根據您的需要修改政策的預設設定。

5. **驗證結果**

   確保佈署成功完成：您的每個應用程式都擁有政策和工作，這些應用程式被安裝到受管理裝置。

結果

完成情境可以導致如下：

- 所選應用程式的所有所需政策和工作被建立。
- 工作排程根據您的需要被配置。
- 所選應用程式被佈署，或者排程在所選用戶端裝置上佈署。

防護佈署精靈

要安裝 Kaspersky 應用程式，您可以使用防護佈署精靈。防護佈署精靈允許使用特別建立的安裝套件或直接從分發套件來遠端安裝應用程式。

防護佈署精靈會執行以下操作：

- 為應用程式安裝下載安裝套件（如果之前未建立）。安裝套件位於**軟體管理 → 安裝套件**。您可以使用這些套件進行遠端安裝。
- 您可以為您指定的裝置或是管理群組，建立並啟動遠端安裝工作。新建立的遠端安裝工作會儲存在**工作**區段。您可以稍後自行執行此工作。工作類型為**遠端安裝應用程式**。

如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

步驟 1：開始防護佈署精靈

您可以隨時手動啟動防護佈署精靈。

要手動啟動防護佈署精靈，

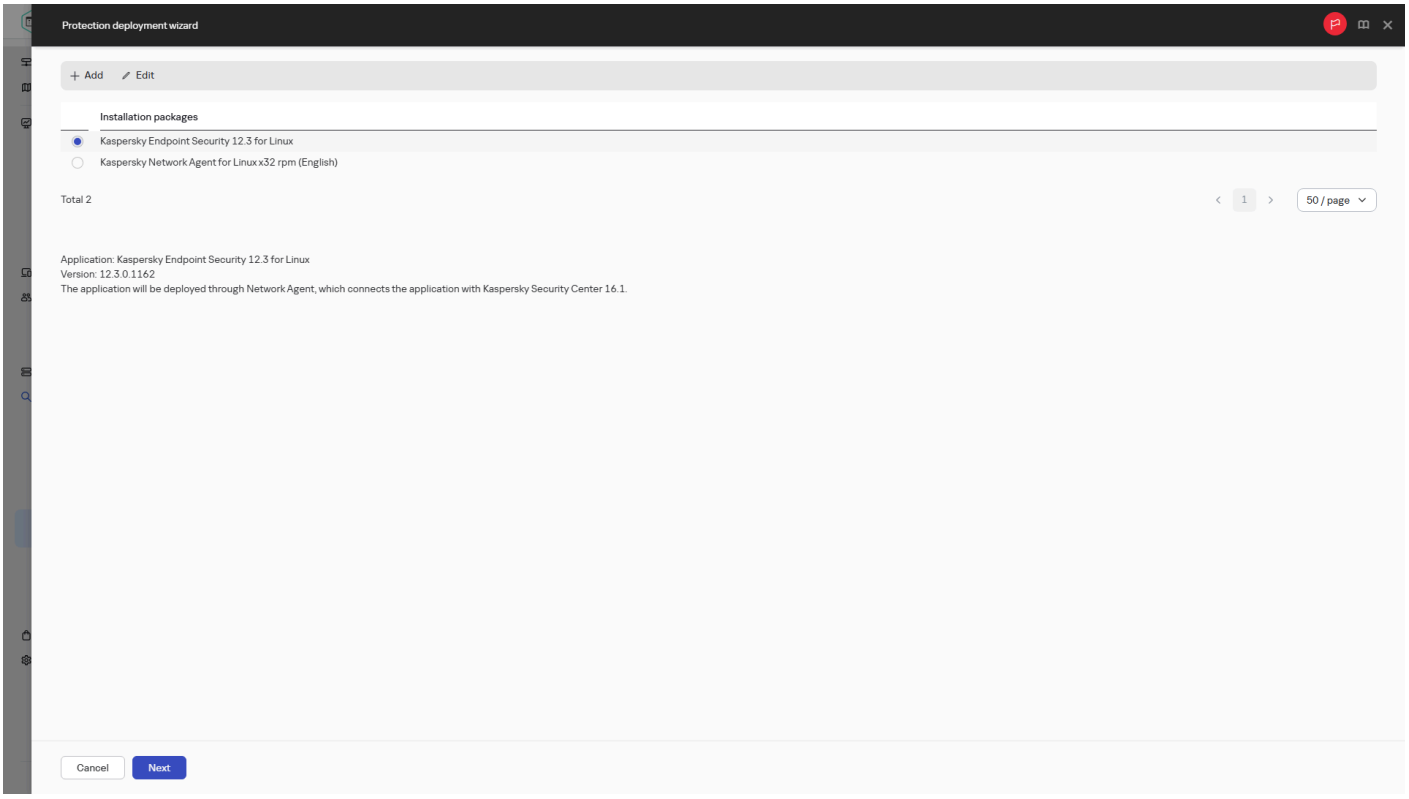
在主功能表中，轉至**發現和佈署 → 佈署和指派 → 防護佈署精靈**。

防護佈署精靈啟動。使用**下一步**按鈕進行精靈。

步驟 2：選取安裝套件

選取您要安裝的應用程式安裝套件。

若未列出必要應用程式的安裝套件，請點擊**新增**按鈕，接著從清單中選取應用程式。



選取安裝套件

步驟 3：選取金鑰檔案或啟動碼的發佈方式

選取金鑰檔案或啟動碼的發佈方式：

- **不新增產品授權金鑰到安裝套件**

  金鑰被自動分發到所相容的所有裝置：

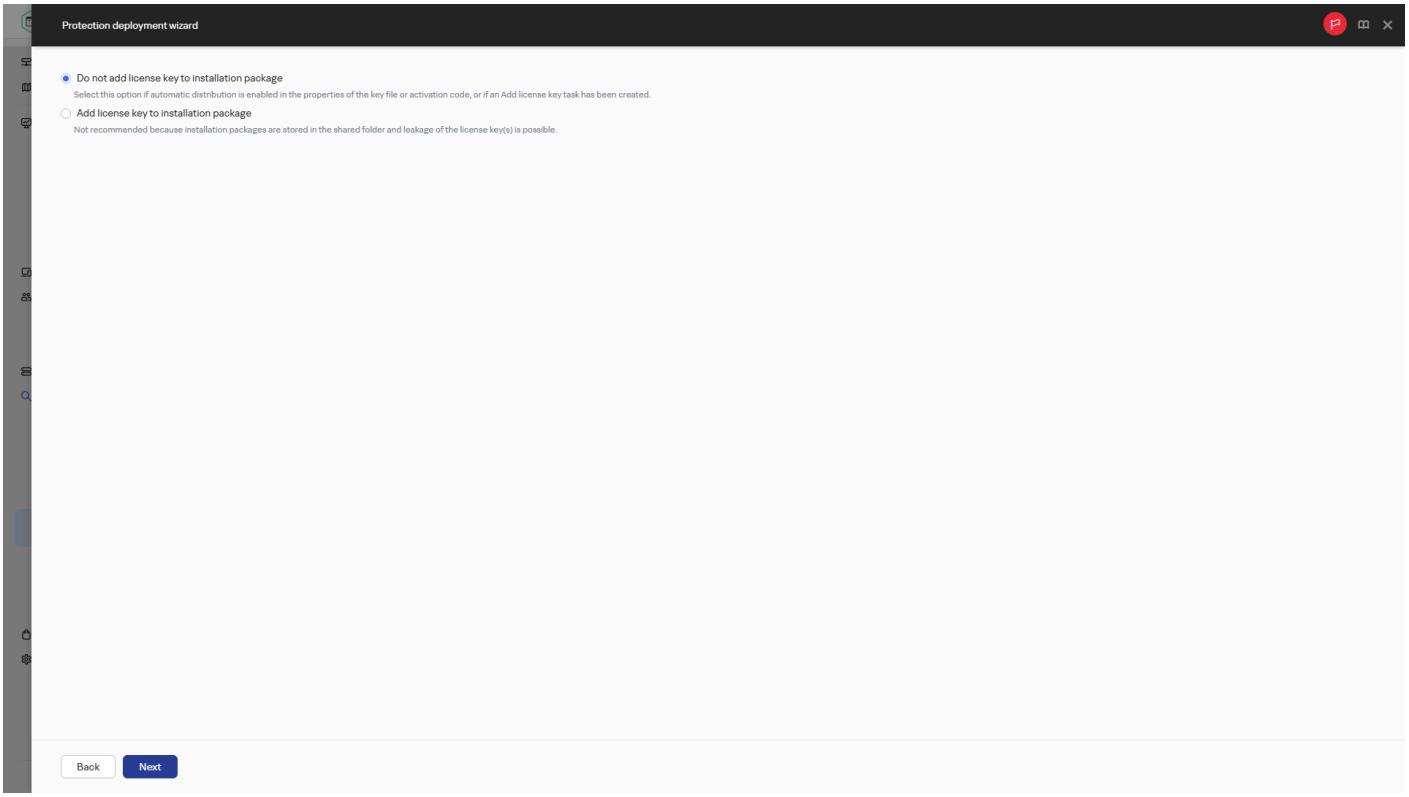
  - 如果自動分發已在金鑰內容中啟用。
  - 如果已建立**新增金鑰**。

- **新增產品授權金鑰到安裝套件**

  金鑰與安裝套件一起被分發到裝置。

  我們不建議您使用該方法分發金鑰，因為共用讀取存取權限已被啟用到安裝套件儲存區。

若安裝套件已包含金鑰檔案或啟動碼，此視窗隨即顯示、但僅會包含產品授權金鑰的資訊。

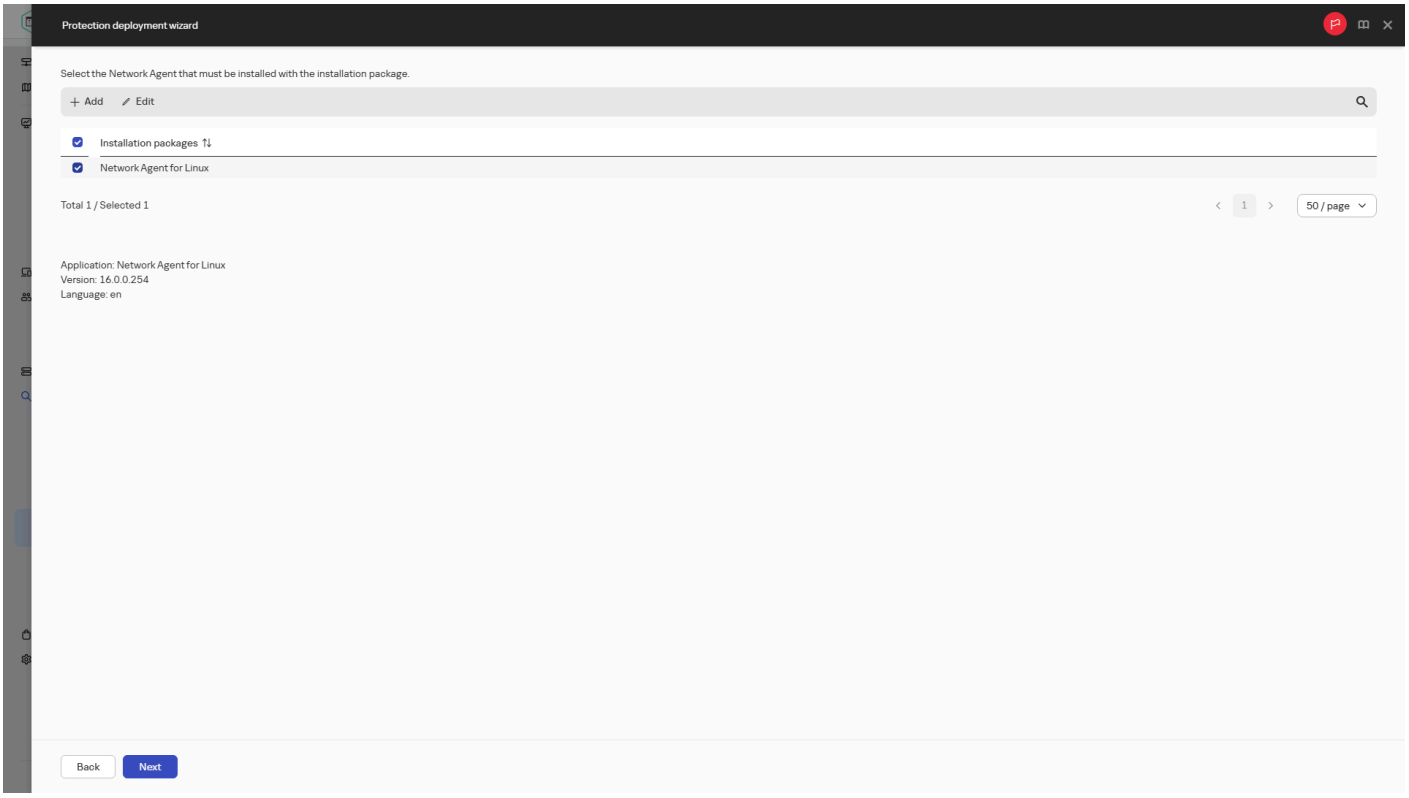


選取金鑰檔案或啟動碼的發佈方式

步驟 4：選取網路代理版本

如果您選取了非網路代理安裝套件，您也必須安裝網路代理，它連線應用程式到管理伺服器。

選取網路代理的最新版本。



選取網路代理版本

步驟 5：選取裝置

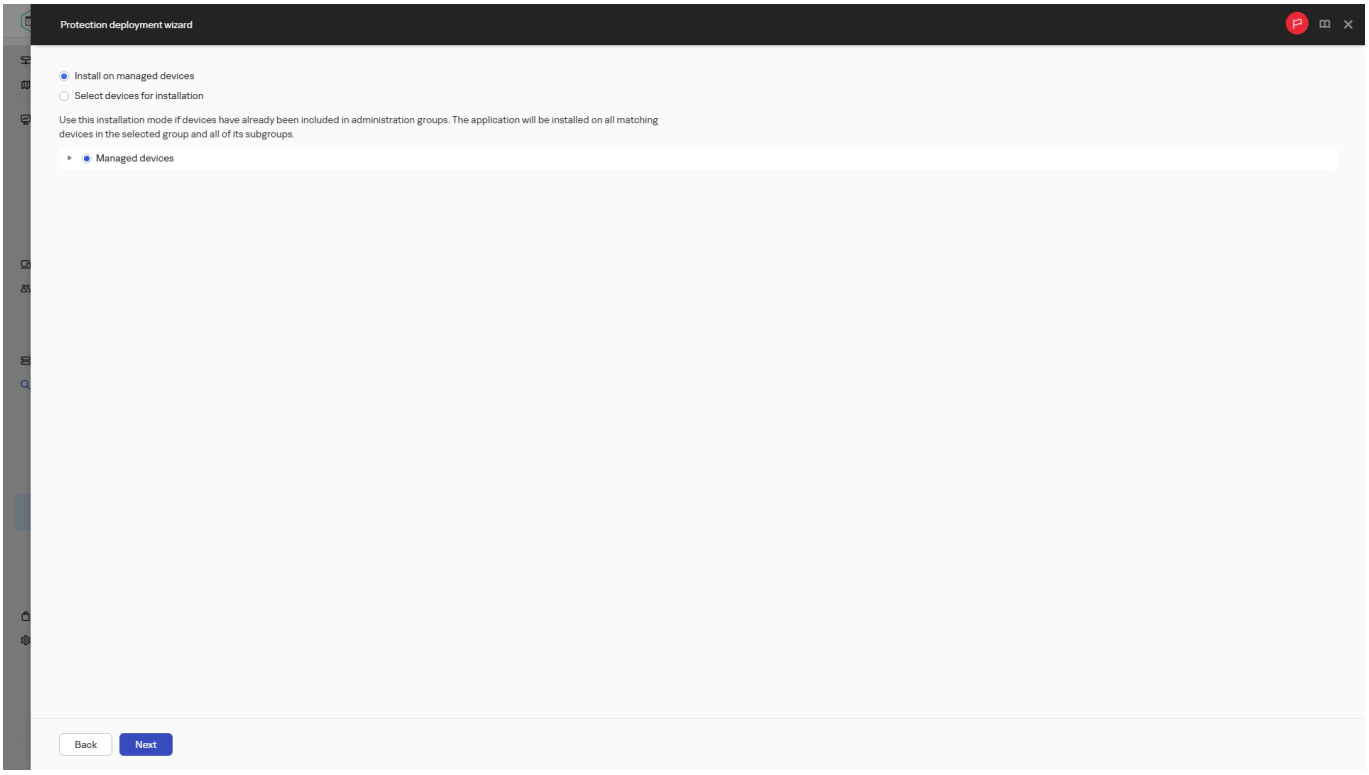
指定要安裝應用程式的裝置清單：

- **安裝到受管理裝置**

  如果選取該選項，程式將為該裝置群組建立遠端安裝工作。

- **選取需要安裝的裝置**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。
  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。



指定要在上面安裝應用程式的裝置清單

步驟 6：指定遠端安裝工作設定

在**遠端安裝工作設定**頁面，指定應用程式遠端安裝設定。

在**強制下載安裝套件**設定群組中，指定如何將安裝應用程式所需的檔案分發到用戶端裝置中：

- **使用網路代理**

  如果啟用此選項，安裝套件透過安裝在裝置上的網路代理傳送到用戶端裝置。
  如果停用此選項，則會使用用戶端裝置的作業系統工具傳送安裝套件。
  如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。
  預設情況下已啟用該選項。

- **透過發佈點使用作業系統資源**

  如果啟用此選項，安裝套件使用作業系統工具透過發佈點傳送到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取本選項。

  如果選取**使用網路代理**方塊，僅在網路代理工具不可用時才透過作業系統工具傳送檔案。

  預設情況下，已經為虛擬管理伺服器上建立的遠端安裝工作選取該選項。

  在未安裝網路代理的裝置上安裝 Windows 應用程式（包括 Windows 網路代理）的唯一方法是使用基於 Windows 的發佈點。因此，當您安裝 Windows 應用程式時：

  - 選擇此選項。
  - 確保為目標用戶端裝置分配了發佈點。
  - 確保發佈點基於 Windows。

- **透過管理伺服器使用作業系統資源**

  如果啟用此選項，檔案將使用用戶端裝置的作業系統工具透過管理伺服器傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

  預設情況下已啟用該選項。

定義附加設定：

- **如果已經安裝應用程式則不再重新安裝**

  如果啟用此選項，則如果選定的應用程式已安裝到該用戶端裝置上，將不再重新安裝它。

  如果停用此選項，系統仍將安裝應用程式。

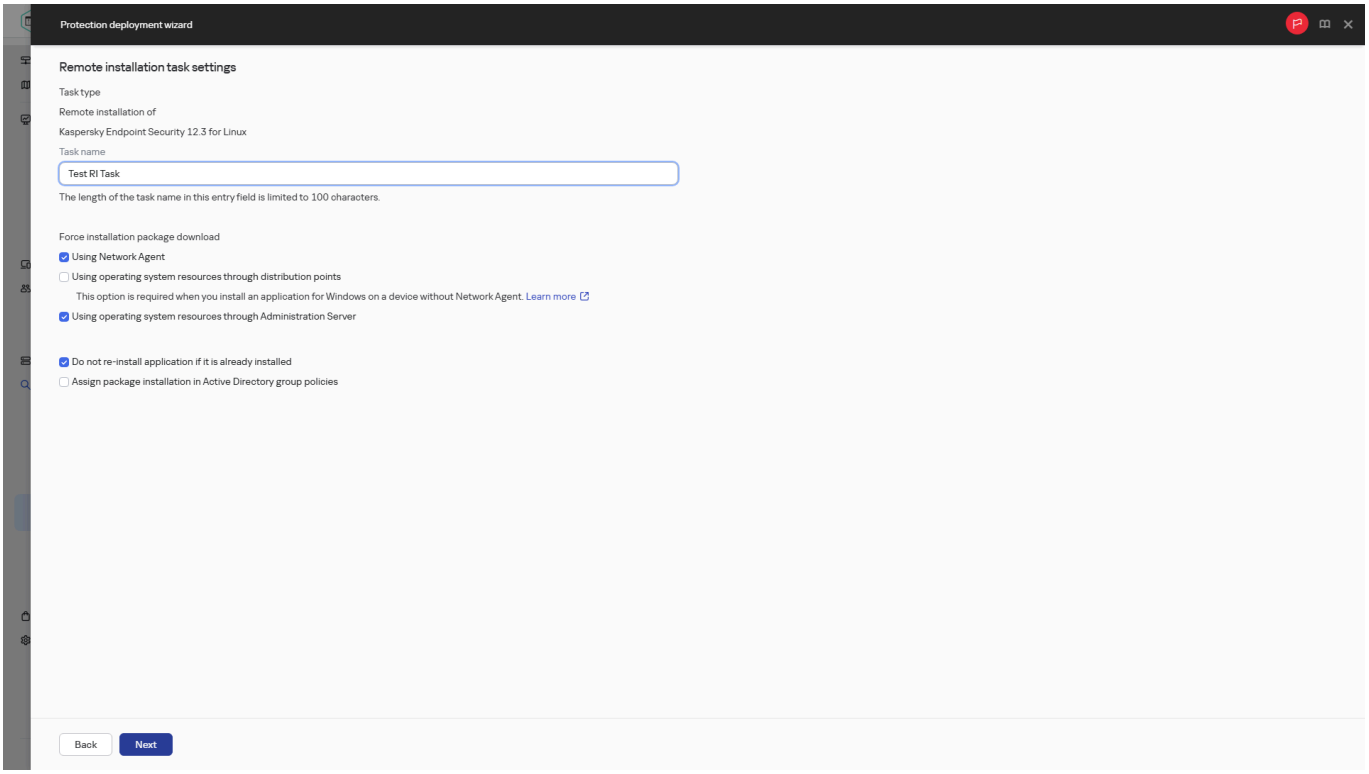
  預設情況下已啟用該選項。

- **在 Active Directory 群組政策中指派安裝套件的安裝**

  如果選取此方塊，安裝套件會使用 Active Directory 的群組政策安裝。

  如果選取網路代理安裝套件，則該方塊可用。

預設情況下已停用該選項。



指定遠端安裝工作設定

步驟 7：重新啟動管理

如果安裝應用程式時作業系統必須重新啟動，指定要執行的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者動作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

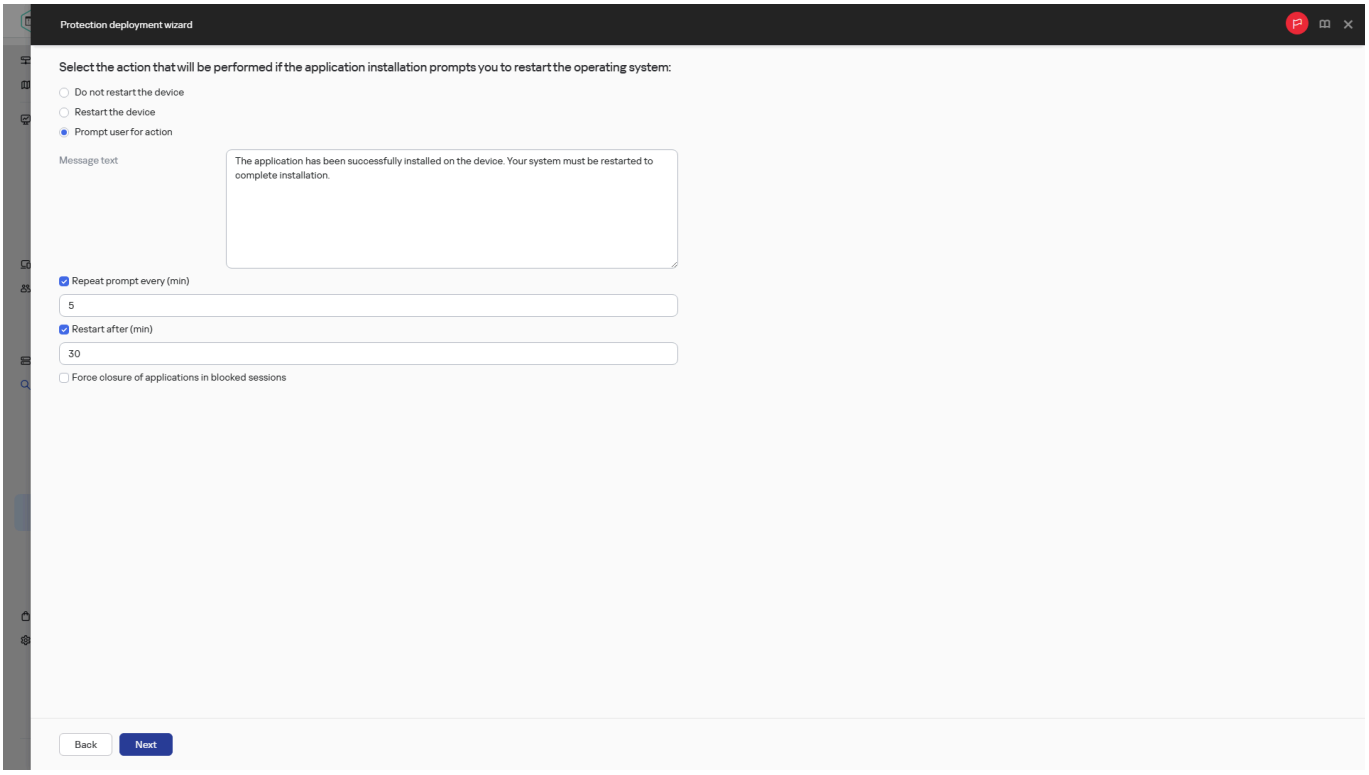
- **強制關閉被封鎖工作階段中的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。



選取作業系統重新啟動選項

步驟 8：安裝前移除不相容的應用程式

該步驟僅在您佈署的應用程式已知與其他應用程式不相容時才顯示。

如果您希望 Kaspersky Next XDR Expert 自動移除與您所佈署的應用程式不相容的應用程式，請選取此選項。

不相容應用程式清單也被顯示。

如果您不選取該選項，應用程式將僅被安裝到沒有不相容應用程式的裝置。

步驟 9：移動裝置到受管理裝置

指定裝置是否在安裝網路代理後必須被移動到管理群組。

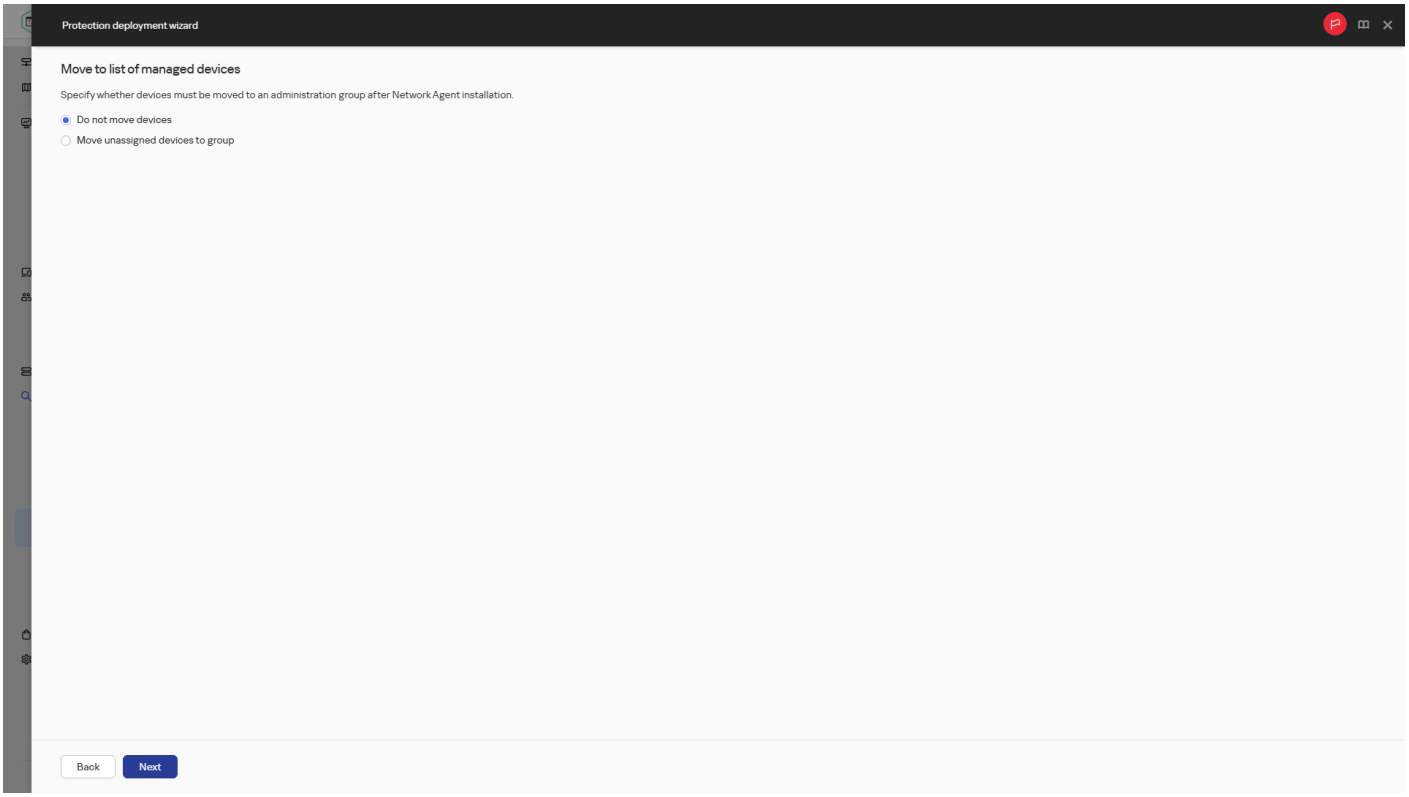
- **不移動裝置**

  裝置保留在目前所在群組中。未被放置在任何群組的裝置保持未分配。

- **將未指派的裝置移動到群組**

  裝置被移動到您選取的管理群組。

預設情況下已選取**不移動裝置** 選項。為了安全，您可能會希望手動移動裝置。



選擇將裝置移至管理群組的選項

步驟 10：選取存取裝置的帳戶

如果必要，新增要用於啟動遠端安裝工作的帳戶。

- **不需要帳戶（網路代理已安裝）**

  如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

  如果網路代理未安裝在用戶端裝置，該選項不可用。

- **需要帳戶（不使用網路代理）**

  如果您為其分配遠端安裝工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶或 SSH 憑證來安裝應用程式。

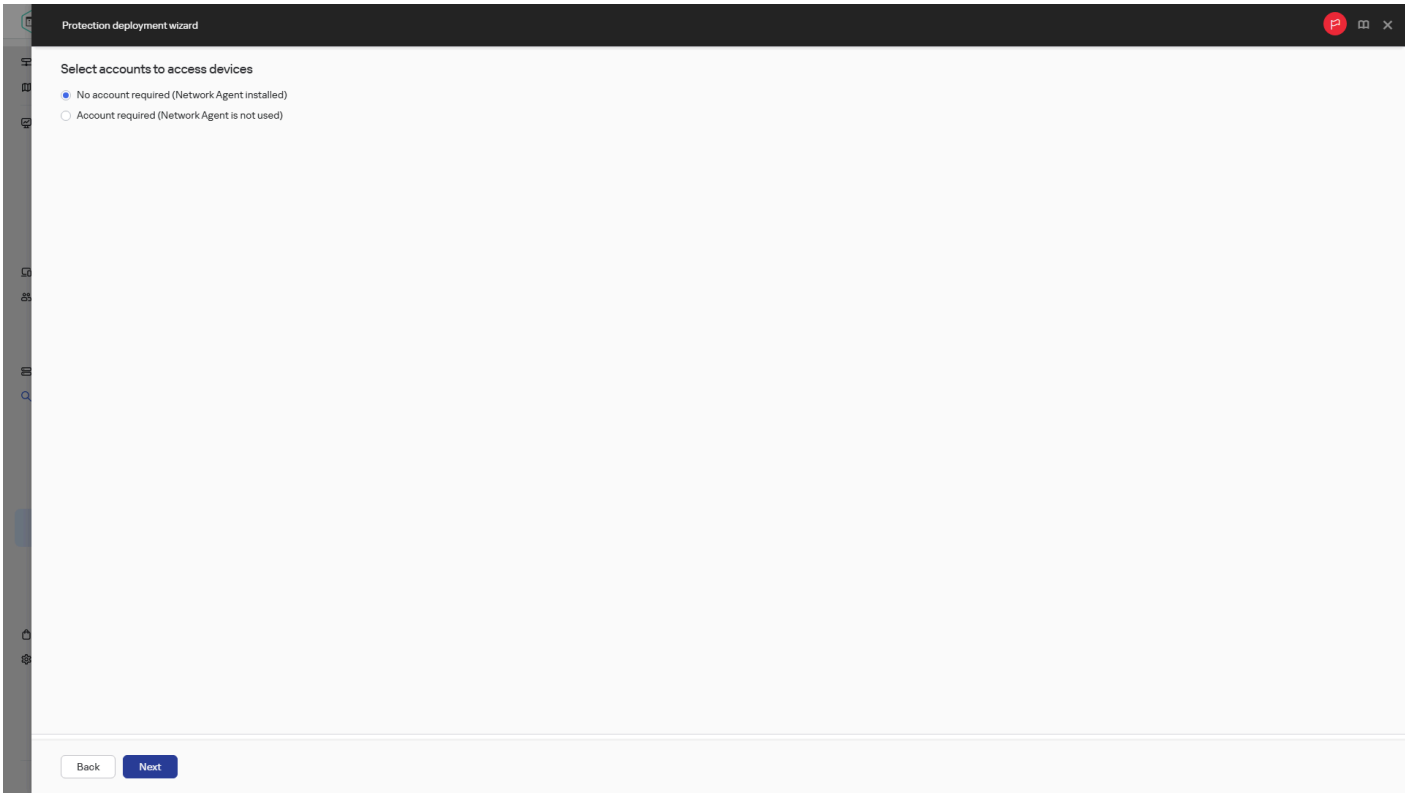
  - **本機或網域帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機或網域帳戶**，然後指定使用者帳戶憑據。

    您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

  - **SSH 憑證**。如果要在 Linux 用戶端裝置上安裝應用程式，您可以指定 SSH 憑證而不是指定使用者帳戶。按一下**新增**按鈕，選擇**SSH 憑證**，然後指定憑證的私鑰和公鑰。

    如要產生私密金鑰，您可以使用 ssh-keygen 公用程式。請注意，Open Single Management Platform支援PEM格式的私密金鑰，但ssh-keygen公用程式預設為產生OPENSSH格式的SSH金鑰。Open Single Management Platform不支援OPENSSH格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 -m PEM 選項。例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵箱 >"
    ```



選取存取裝置的帳戶

步驟 11：啟動安裝

該頁面是精靈的最後一步。在該步驟，**遠端安裝工作**已被成功建立並配置。

預設不會選取**精靈完成時執行工作**選項。如果您選取該選項，**遠端安裝工作**將在您完成精靈後立即啟動。如果您不選取該選項，**遠端安裝工作**不會啟動。您可以稍後自行執行此工作。

點擊**確定**以完成防護佈署精靈的最終步驟。

新增卡巴斯基應用程式的管理外掛程式

要使用OSMP主控台遠端管理卡巴斯基應用程序，您必須安裝管理网页外掛程式。部署Kaspersky Next XDR Expert後，可安裝管理网页外掛程式。

如果需要手動重新安裝管理网页外掛程式，請聯絡卡巴斯基技術支援以取得包含所需管理外掛程式的存檔。

要為卡巴斯基應用程式下載管理网页外掛程式：

1. 將管理網頁外掛程式存檔移至KDT公用程式所在的管理員主機。
2. 如有必要，請在管理員主機上匯出當前版本的設定檔。

   如果沒有新增或修改安裝參數，則無需匯出設定檔。
3. 執行以下命令以安裝外掛程式：

   ```
   ./kdt apply -k <path_to_plugin_archive> -i <path_to_configuration_file>
   ```

   在命令中，指定外掛程式存檔的路徑和目前組態檔的路徑。如果沒有新增或修改安裝參數，則無需在命令中指定設定檔的路徑。

管理網頁外掛程式已安裝。重新載入OSMP主控台以顯示外掛程式。

您可以使用KDT檢視與OSMP相關的元件清單（包括管理Web外掛程式）。此外，您還可以檢視OSMP主控台版本和已安裝的管理Web外掛程式清單。為此，請在OSMP主控台的主功能表中，轉至您的帳戶設定，然後選擇**關於**。

移除管理Web外掛程式

您可以移除為Kaspersky Next XDR Expert提供附加功能的卡巴斯基應用程式的管理Web外掛程式。Kaspersky Next XDR Expert服務外掛程式用於確保Kaspersky Next XDR Expert的正常運作，因此無法移除（例如，事件回應平台外掛程式）。

若要刪除管理網頁外掛程式：

1. 根據需要，請執行下列命令來取得要移除的外掛程式名稱：

   ```
   ./kdt state
   ```

   元件清單隨即顯示。
2. 在管理員主機上，執行下列命令：指定要移除的外掛程式名稱：

   ```
   ./kdt remove --cnab <plug-in_name>
   ```

指定的管理網頁外掛程式隨即由KDT移除。

檢視整合在Open Single Management Platform中的元件清單

您可以使用KDT檢視OSMP中整合的元件清單（包括管理網頁外掛程式）。

若要檢視元件清單，

在KDT所在的管理員主機上，執行以下命令：

```
./kdt state
```

OSMP中整合的元件清單（包括管理網頁外掛程式）顯示在命令列視窗中。

檢視卡巴斯基Next XDR Expert元件的名稱、參數和自訂操作

KDT可讓您檢視傳輸存檔中包含的Kaspersky Next XDR Expert元件清單，以及已安裝元件的清單。此外，您還可以檢視Kaspersky Next XDR Expert元件的參數清單和自訂操作清單。如果元件有可用的自訂操作，您也可以使用KDT檢視指定自訂操作的描述和參數。

*自訂操作*可讓您執行針對Kaspersky Next XDR Expert元件的其他操作（安裝、更新、刪除除外）。例如，恢復管理伺服器資料以及增加管理伺服器及其日誌使用的磁碟空間容量，都是透過自訂操作執行的。

自訂操作使用KDT執行，如下所示：

```
./kdt invoke <component_name> --action <custom_action> --param
<custom_action_parameter>
```

若要檢視傳輸存檔中包含的Kaspersky Next XDR Expert元件清單，

請在KDT公用程式所在的管理員主機上執行下列命令。在命令中，指定傳輸存檔的路徑及其名稱：

```
./kdt describe -k <transport_archive_name_with_path>
```

若要檢視Kaspersky Next XDR Expert元件清單，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt describe
```

Kaspersky Next XDR Expert元件清單隨即顯示。

若要檢視Kaspersky Next XDR Expert元件的參數清單和自訂操作清單，

請在KDT公用程式所在的管理員主機上執行下列命令並指定Kaspersky Next XDR Expert元件的名稱：

```
./kdt describe <component_name>
```

指定元件可用的參數和自訂操作清單隨即顯示。

若要檢視自訂操作的描述和參數清單，

請在KDT公用程式所在的管理員主機上執行下列命令並指定Kaspersky Next XDR Expert元件名稱及其命令：

```
./kdt describe <component_name> <custom_action>
```

指定元件自訂操作的描述和參數清單隨即顯示。

下載和建立 Kaspersky 應用程式的安裝套件

若您的管理伺服器有網際網路的存取權，您可從 Kaspersky 網路伺服器建立 Kaspersky 應用程式的安裝套件。

下載和建立 Kaspersky 應用程式的安裝套件：

1. 在主功能表中，轉至**軟體管理→安裝套件**。

   您也可在螢幕通知清單中檢視通知關於 Kaspersky 應用程式新套件的通知。如果有關於新安裝套件的通知，您可以按一下通知旁邊的連結並轉到可用安裝套件清單。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 點擊**新增**。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 選擇**為卡巴斯基應用程式建立安裝套件**。

   Kaspersky 網路伺服器可用安裝套件清單隨即顯示。該清單僅包含與當前版本的Open Single Management Platform相容的應用程式的安裝套件。預設情況下，清單僅顯示與介面語言相符的應用程式。若要顯示其他語言，請按一下**篩選**並配置篩選設定。

4. 按一下安裝套件的名稱，例如 Kaspersky Endpoint Security for Linux。

   帶有安裝套件資訊的視窗開啟。

   > 如果符合適用的法律和規定，您可以下載並使用包含加密工具以實施強加密的安裝套件。若要下載符合您組織需要的 Kaspersky Endpoint Security for Windows 安裝套件，請諮詢組織用戶端裝置所在的國家或地區的法務部門。

5. 閱讀資訊，然後按一下**下載並建立安裝套件**按鈕。

   若分發套件無法轉換為安裝套件，**下載並建立安裝套件**按鈕則會取代 **下載分發套件**顯示。

   下載安裝套件到管理伺服器開始。您可以關閉精靈視窗。在這種情況下，下載程序將在背景模式下繼續。您可以在**套件狀態**欄中追蹤安裝套件的下載狀態並對狀態進行篩選和排序。

   如果下載程序停止並且下載狀態切換為**接受 EULA**，則點擊安裝套件名稱，然後繼續進行指示的步驟 6。依預設，狀態為**進行中**和**接受 EULA**的安裝套件會放在清單的開頭。

   > 若包含在所選分發套件的資料大小超過目前限制，便會顯示錯誤訊息。您可變更限制值，接著繼續建立安裝套件。

6. 對於一些 Kaspersky 應用程式，下載過程中，**顯示 EULA**按鈕被顯示。如果它不顯示，做以下操作：

   a. 點擊**顯示 EULA**按鈕以閱讀最終使用者產品授權協議 (EULA)。

   b. 閱讀螢幕顯示的 EULA，並再次點擊**同意**。

   您接受 EULA 後下載便會繼續。若您點擊**拒絕**，下載便會暫停。

7. 下載完成後，按一下**關閉**按鈕。

安裝套件會顯示在安裝套件清單中。

從檔案建立安裝套件

您可使用自訂安裝套件進行以下操作：

- 在用戶端裝置安裝應用程式（如文字編輯器），例如根據工作方式。
- 建立獨立安裝套件。

自訂安裝套件是有一組檔案的資料夾。建立自訂安裝套件的來源是*封存檔案*。封存檔案內含檔案或必須包含在自訂安裝套件的檔案。

建立自訂安裝套件期間，您可指定命令行參數，例如在靜默模式中安裝應用程式。

若要建立應用程式安裝套件：

1. 在主功能表中，轉至**軟體管理→安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 點擊**新增**。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 選擇 **從檔案建立安裝套件**。

4. 指定套件名稱並按一下**瀏覽**按鈕。

5. 在開啟的視窗中，選擇位於可用磁盤上的封存檔案。

   您可以上傳 ZIP、CAB、TAR 或 TAR.GZ 封存。您無法從 SFX（自行解壓封存）檔案來建立安裝套件。

   檔案上傳到管理伺服器開始。

6. 如果您指定了卡巴斯基應用程式的檔案，系統可能會提示您閱讀並接受應用程式的最終使用者產品授權協議 (EULA)。要繼續，您必須接受 EULA。僅當您已完全閱讀、理解並接受 EULA 的條款後再選擇**接受此最終使用者產品授權協議的條款和條件**選項。

   此外，系統可能會提示您閱讀並接受隱私政策。要繼續，您必須接受隱私政策。只有在您理解並同意您的資料將受到處理與傳輸（包含傳送至第三國家/地區）（如隱私政策所述）時，才選擇**我接受隱私政策**選項。

7. 選取檔案（從已選封存檔案擷取的檔案清單），接著指定可執行檔命令列參數。

   您可指定命令行參數以靜默模式從安裝應用程式來安裝套件。您可選擇指定命令行參數。

   系統會啟動建立安裝套件的程序。

   精靈會通知您程序已完成。

若未建立安裝套件，系統會顯示適合的訊息。

8. 點擊**完成**按鈕以關閉精靈。

該安裝套件會出現在安裝套件清單中。

在管理伺服器可用之安裝套件的清單中，透過點擊自訂安裝套件名稱的連結，您可：

- 檢視安裝套件的以下內容：
  - **名稱**。自訂安裝檔案名稱。
  - **套件狀態**。安裝套件下載狀態。
  - **來源**。應用程式供應商名稱。
  - **應用程式**。封裝在自訂安裝套件的應用程式名稱。
  - **版本**。應用程式版本。
  - **語言**。封裝在自訂安裝套件的應用程式語言。
  - **大小 (MB)**。安裝套件大小。
  - **作業系統**。適用安裝套件的作業系統類型。
  - **建立日期**。安裝套件建立日期。
  - **修改日期**。安裝套件修改日期。
  - **類型**。安裝套件的類型。
- 變更命令行參數。

建立獨立安裝套件

貴組織中您與裝置使用者可使用獨立安裝套件在裝置上手動安裝應用程式。

獨立安裝套件是可執行檔，您可將其儲存在網頁伺服器或共用資料夾、由電子郵件傳送，或以其他方式傳輸至用戶端裝置。在用戶端裝置上，使用者可在本機執行收到的檔案以安裝應用程式，而不需使用 Kaspersky Next XDR Expert。您可以為 Kaspersky 應用程式或協力廠商應用程式建立獨立安裝套件。若要建立協力廠商的應用程式獨立安裝套件，您必須建立自訂安裝套件。

如果管理伺服器可以存取網際網路，則使用**將更新下載至管理伺服器儲存區**工作下載建立網路代理程式獨立安裝套件所需的依賴項。如果管理伺服器無法存取網際網路，請執行下列步驟：

1. 執行以下命令建立 RIUtilsArchiveDirUsed 標誌：

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. 執行以下命令以重新啟動管理伺服器服務：

   ```
   systemctl restart kladminserver_srv.service
   ```

3. 從卡巴斯基網站下載以下壓縮包，並將壓縮包放置在 /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives 資料夾中：

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   請勿重新命名歸檔檔案。

管理伺服器現在已具備所需的依賴項。

請確保第三人無法取得獨立安裝套件。

若要建立獨立安裝套件：

1. 在主功能表中，轉至**軟體管理→安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 在安裝套件的清單中，選取安裝套件並在上列清單中，點擊**佈署**按鈕。

3. 選擇**使用獨立安裝套件**選項。

   獨立安裝套件建立精靈啟動。使用**下一步**按鈕進行精靈。

4. 若您要隨所選的應用程式安裝網路代理，請確認**隨此應用程式一起安裝網路代理**選項已啟用。

   顯示的選項取決於您為其建立獨立安裝套件的應用程式。

   預設情況下已啟用該選項。若您不確認裝置是否安裝網路代理，建議啟用此選項。若網路代理已在裝置上安裝，在安裝含網路代理的獨立安裝套件後，網路代理將會更新至新版本。

   若您停用此選項，網路代理將不會安裝在裝置上，且裝置不會受到管理。

   若管理伺服器已存在所選應用程式的獨立安裝套件，精靈會告知您此資訊。在此情況下，您必須選取以下其中一個動作：

   - **建立獨立安裝套件**。若您要針對新應用程式版本建立獨立安裝套件，並同時希望保留針對先前應用程式版本建立的獨立安裝套件，請選取此選項。新獨立安裝套件會放在另一個資料夾中。
   - **使用存在的獨立安裝套件**。若要使用現有獨立安裝套件，請選取此選項。建立套件的程序將不會啟動。
   - **重新建立已經存在的獨立安裝套件**。如果您要再次針對相同應用程式建立獨立安裝套件，請選取此選項。獨立安裝套件會放在相同資料夾。

5. 在**移動到受管理裝置清單**步驟，預設會選取**不移動裝置**選項。若您在網路代理安裝後不要移動用戶端裝置至任何管理群組，請不要變更選擇的選項。

   如果要在網路代理安裝後移動用戶端裝置，請選取**將未指派的裝置移動到此群組**選項並指定要將用戶端裝置移動到的管理群組。依預設，裝置會移至**受管理裝置**群組。

6. 獨立安裝套件建立完成後，按一下**完成**按鈕。

   獨立安裝套件建立精靈即會關閉。

獨立安裝套件已建立並放置在Web伺服器上。您可透過點擊在安裝套件清單上的**檢視獨立安裝套件清單**按鈕檢視獨立安裝套件的清單。

變更自訂安裝套件資料大小限制

在建立自訂安裝套件期間解壓縮資料的總大小有所限制。預設限制為 1 GB。

若您嘗試上傳的封存檔案內有超過目前限制的資料，則會顯示錯誤訊息。從大型分發套件建立安裝套件時，您可能需要增加此限制值。

若要變更自訂安裝套件大小的限制值：

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
MaxArchivePkgSize -t d -v <位元組數>'
```

其中 <number of bytes> 是十六進位或十進位格式的字元組數。

例如，如果要求的限制為 2 GB，您可以指定十進制值 2147483648 或十六進制值 0x80000000。在這種情況下，要進行管理伺服器的本機安裝時，您可以使用以下命令：

```
./kdt invoke ksc --action klscflag --param klscflag_param=' -fset -pv klserver -n
MaxArchivePkgSize -t d -v 2147483648'
```

自訂安裝套件資料的大小限制隨即變更。

準備 Linux 裝置以安裝網路代理

在 Linux 裝置上安裝網路代理之前，您必須執行任何 Linux 裝置所需的準備步驟。

要準備執行 Linux 的裝置以遠端安裝網路代理：

1. 請確認您要安裝 Network Agent for Linux 的裝置是執行支援的 Linux 版本。
2. 如果要在AltOS上以封閉軟體環境模式安裝網路代理程式，請停用封閉軟體環境模式，直到安裝完成。
3. 使用網頁主控台下載網路代理安裝套件，或使用應用程式發佈套件。

   如果您需要在執行含glibc 2.5的Linux作業系統的裝置上安裝網路代理程式，則必須使用網頁主控台介面或從卡巴斯基網站下載 *Kaspersky Network Agent for Linux Legacy*安裝套件。
4. 確保目標 Linux 裝置上已安裝下列軟體：
   - Sudo（對於 Ubuntu 10.04，Sudo 版本為 1.7.2p1 或者更高）
   - Perl 語言解譯器 5.10 或更高版本
   - ps公用程式
5. 測試裝置配置：
   a. 檢查是否您可以透過 SSH 用戶端（例如 PuTTY）連線到裝置。

如果您無法連線到裝置，請開啟 `/etc/ssh/sshd_config` 檔案，並確保下列設定具有以下列出的對應值：

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

如果您可以毫無問題地連線到裝置，請不要修改 /etc/ssh/sshd_config 檔案；否則在執行遠端安裝工作時可能會遇到 SSH 認證失敗的情況。

儲存檔案（如有必要），並使用 `sudo service ssh restart` 命令重新啟動 SSH 服務。

b. 確保TCP連接埠 22在未指派的Linux裝置上處於開放和可存取。

若要成功安裝Linux的網路代理程式，必須啟用TCP連接埠22。

c. 停用要連線裝置的使用者帳戶的 sudo 密碼。

d. 使用 sudo 的 `visudo` 指令開啟 sudoers 設定檔。

在開啟的檔案中，將以下一行新增到檔案結尾：`<username> ALL = (ALL) NOPASSWD: ALL`。此種情況下，`<username>` 是用於透過 SSH 進行裝置連線的使用者帳戶。如果您使用的是 Astra Linux 作業系統，請在 /etc/sudoers 檔案的最後一行新增以下文字：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. 儲存並關閉 sudoers 檔案。

f. 透過 SSH 再次連線到裝置，並確保 Sudo 服務不會提示您輸入密碼；您可以使用 `sudo whoami` 命令來執行此操作。

6. 如果要在執行包含 systemd 初始化系統之作業系統的裝置上遠端安裝網路代理，請開啟 `/etc/systemd/logind.conf` 檔案，然後執行下列操作之一：

- 指定 no 作為 `KillUserProcesses` 設定的值：`KillUserProcesses=no`。
- 對於 `KillExcludeUsers` 設定，請輸入執行遠端安裝所使用帳戶的使用者名稱，例如 `KillExcludeUsers=root`。

Astra Linux 目標裝置

如果目標裝置執行 Astra Linux，請在 `/home/<username>/.bashrc` 檔案中新增 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 字串，其中 `<username>` 是用於透過 SSH 進行裝置連線的使用者帳戶。

OSnova 目標裝置

如果目標裝置執行 OSnova，請做以下操作：

a. 開啟 `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` 檔案，然後將 `#KillUserProcess=yes` 行註解掉。

b. 開啟 `/usr/lib/NESS/pam-user-session` 檔案，然後將 `#loginctl terminate-session "$XDG_SESSION_ID"` 行註解掉。

若要套用變更的設定，請重新啟動 Linux 裝置或執行以下命令：

```
sudo systemctl restart systemd-logind.service
```

7. 如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

8. 如果要在封閉軟體環境模式下執行 Astra Linux 作業系統的裝置上安裝網路代理，請執行額外的步驟來準備 Astra Linux 裝置。

9. 如果要在執行Ubuntu Server或Ubuntu Desktop版本10.04的裝置上安裝網路代理，請執行其他步驟來準備這些裝置。

10. 如果要在執行 Linux 作業系統且安裝有 glibc 2.5 的裝置上安裝網路代理，請執行額外步驟來準備目標裝置。

11. 如果您在AltOS上以封閉軟體環境模式安裝網路代理程式，請重新啟用封閉軟體環境模式。

12. 如果要在作業系統為RED OS 7.3.4或更高版本或者MSVSPHERE 9.2或更高版本的裝置上安裝網路代理，請安裝libxcrypt-compat套件以便網路代理正確運作。

Linux 裝置已準備好安裝網路代理。您可以遠端、以互動模式或靜默模式安裝網路代理程式。

準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理

在執行 SUSE Linux 的裝置上安裝網路代理之前，您必須執行兩個準備過程：下面說明中的一個和適用於任何 Linux 裝置的一般準備步驟。

要在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理：

在安裝網路代理之前，執行以下指令：

```
sudo zypper install insserv-compat
```

這使您能夠安裝 insserv-compat 套件並正確配置網路代理。

執行 `rpm -q insserv-compat` 命令即可檢查套件是否已經安裝。

如果您的網路包含大量執行 SUSE Linux Enterprise Server 15 的裝置，您可以使用用來配置和管理公司基礎結構的特殊軟體。透過使用此軟體，您可以一次在所有必要的裝置上自動安裝 insserv-compat 套件。例如，您可以使用 Puppet®、Ansible®、Chef®，也可以自行編寫指令碼—請使用任何方便的方法。

若裝置沒有 SUSE Linux Enterprise 的 GPG 簽名金鑰，您可能會遇到以下警告：`Package header is not signed!`。選取 `i` 選項即可略過該警告。

準備好Linux裝置後，您可以以遠端、互動模式或靜默模式安裝網路代理程式。

準備好用於遠端安裝的 Windows 裝置

遠端安裝應用程式到用戶端裝置時可能會因下列原因發生錯誤：

- 安裝的工作已經成功在此裝置上執行。

  在此狀況下，工作無須再重複執行。

- 工作開始後，裝置被關閉。

  在此情況下，開啟裝置，然後重新啟動工作。

- 用戶端的網路代理與管理伺服器並無連線。

  要確定問題原因，請使用用戶端裝置的遠端診斷實用程式 (klactgui)。

- 如果網路代理未安裝在裝置上，遠端安裝過程中可能會發生以下狀況：

  - 網路錯誤
  - 作業系統配置錯誤
  - 遠端安裝任務中的帳戶權限配置不正確

  為避免在未安裝網路代理程式的用戶端裝置上安裝應用程式時可能出現的問題，您必須使用Open Single Management Platform的遠端安裝任務強制安裝選定的安裝套件 - 前提是每台裝置都擁有一個具有本機管理員權限的使用者帳戶。

之前，riprep公用程式用來為Windows裝置準備遠端安裝。現在，這被認為是過時的作業系統配置方法。不建議在比 Windows XP 和 Windows Server 2003 R2 更新的作業系統上使用 riprep 公用程式。

如果管理伺服器無法直接存取裝置，也可以使用強制安裝。例如，如果裝置位於隔離網路或本機網路中，而管理伺服器位於DMZ區域。在這種情況下，需要一個發佈點來佈署到此類裝置。

當在子網中的裝置通過窄通道通道與管理伺服器通訊，而同一子網內的裝置之間可使用較寬頻通道時，將發佈點作為本機安裝中心進行安裝也可能非常有用。

在初始部署的情況下，不會安裝網路代理。因此，在遠端安裝工作的設定中，您無法選擇使用網路代理進行應用程式安裝所需的檔案分發。您只能透過管理伺服器或發佈點選擇使用作業系統資源來分發檔案。

您應該在遠端安裝任務的設定中指定一個具有訪問admin$共享權限的帳戶。

您可以透過明確指定（使用清單）、選取它們所屬的Open Single Management Platform群組，或根據特定條件建立裝置選擇清單來指定目標裝置。安裝開始時間定義在工作排程中。如果工作內容中啟用了**執行錯過的工作**，工作可以在裝置開啟時立即執行，或裝置被移動到目的管理群組時立即執行。

強制安裝套件包括傳送安裝套件到目的裝置、隨後複製檔案到每個目的裝置的 admin$ 資源，和在這些裝置上遠端註冊支援服務。透過Open Single Management Platform功能將安裝套件傳送到目標裝置，以確保網路互動。以下條件必須在此種情況下被滿足：

- 目標裝置可以從Windows作業系統的發佈點訪問，將從該發行點對用戶端裝置進行遠端安裝，並且此發佈點已被選為目標裝置的發佈點。
- 目的裝置的名稱解析在網路中正常運作。
- 裝置上的管理分享 (admin$) 保持啟用。
- 目標裝置上正在執行以下系統服務：

  - 伺服器 (LanmanServer)

    預設情況下，該服務正在執行。

  - DCOM 伺服器處理程序啟動器 (DcomLaunch)

- RPC Endpoint Mapper (RpcEptMapper)
- 遠端過程呼叫 (RpcS)

- 目標裝置上開啟了連接埠TCP 445，以便透過Windows工具啟用遠端存取。

  TCP 139、UDP 137 和 UDP 138 由舊協定使用，目前應用程式不再需要。

  防火牆必須允許動態出站存取埠，以便從發佈點到目標設備的連接。

- 在部署網路代理期間，Active Directory 網域政策安全性設定被允許提供 NTLM 協定的操作。
- 在執行 Microsoft Windows XP 的目的裝置上，簡單檔案共用模式被停用。
- 在目標裝置上，存取共用和安全模型被設定為*經典 - 本機使用者以自身身分進行驗證*。它絕不可能是*僅限訪客 - 本機使用者以訪客身分進行身分驗證*。
- 目的裝置是網域成員，或帶有管理員權限的統一帳戶提前在目的裝置上被建立。

若要將網路代理或其他應用程式成功部署到未加入Windows Server 2003或更高版本Active Directory網域的裝置，必須在該裝置上停用遠端UAC。遠端 UAC 是阻止本機管理帳戶存取 admin$ 的原因之一，這對於強制部署網路代理或其他應用程式必不可少。停用遠端 UAC 不會影響本機 UAC。

在未配置到任何Open Single Management Platform管理群組的新裝置上進行安裝時，您可以打開遠端安裝工作內容，並指定裝置在網路代理安裝後將被移動到的管理群組。

當建立群組工作時，記住每個群組工作都影響所選群組的潛逃群組中的所有裝置。因此，您必須避免在子群組中的重複安裝工作。

建立強制安裝應用程式工作的一種簡化方法是自動安裝。為此，您必須開啟管理群組內容，開啟安裝套件清單，然後選取必須在該群組中的裝置上安裝的套件。結果，所選安裝套件將被自動安裝在該群組和其所有子群組中的所有裝置上。套件被安裝的時間間隔取決於網路吞吐量和網路裝置總數。

您可以使用多個發佈點來減少在向目標裝置傳送安裝套件時的負載。注意，該安裝方法給作為發佈點的裝置增加了大量負載。如果您使用發佈點，必須確保它們存在於託管目的裝置的每個隔離子網路中。

含有%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit資料夾的分割區中的可用磁碟空間必須遠超已安裝應用程式安裝包的總大小。

準備在封閉軟體環境模式下執行 Astra Linux 的裝置以安裝網路代理

在封閉軟體環境模式下執行 Astra Linux 的裝置上安裝網路代理之前，您必須執行兩個準備過程：下面說明中的一個和適用於任何 Linux 裝置的常規準備步驟。

在具有 root 權限的帳戶下執行本指令中提供的命令。

準備在封閉軟件環境模式下執行 Astra Linux 的裝置以安裝網路代理：

1. 開啟 `/etc/digsig/digsig_initramfs.conf` 檔案，然後指定以下設定：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在指令行中，執行以下指令來安裝相容套件：

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

3. 為應用程式金鑰建立一個目錄：

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

4. 將應用程式金鑰 /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg 放在上一步建立的目錄中：

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

   > 如果 Open Single Management Platform 分發套件不包含 kaspersky_astra_pub_key.gpg 應用程式金鑰，您可以點擊以下連結下載：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. 更新 RAM 瓷碟：

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

   重新啟動系統。

Linux 裝置已準備好安裝網路代理。您可以遠端、以互動模式或靜默模式安裝網路代理程式。

以靜默模式安裝適用於 Linux 的網路代理（搭配回應檔案）

您可在 Linux 裝置上使用回應檔案設定檔安裝網路代理，此檔案內含自訂的安裝參數：變數與其各自的值。使用此回應檔案可讓您以靜默模式執行安裝，意即使用者無須參與。

在基於 Linux 的裝置上安裝網路代理之前，您必須完成所有基於 Linux 的裝置所需的一般準備步驟。

完成一般步驟後，您可以按照特定於您的作業系統的附加說明進行操作：

- 準備執行 SUSE Linux Enterprise Server 15 的裝置
- 準備一部在封閉軟體環境模式下執行 Astra Linux 的裝置
- 準備一部執行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的裝置
- 準備一個執行 Linux 作業系統且安裝有 glibc 2.5 的裝置

若要以靜默模式安裝適用於 Linux 的網路代理：

1. 參閱最終使用者產品授權協議。只有在您理解並接受最終使用者產品授權協議的條款時，才遵循以下步驟操作。

2. 建立應答檔案（TXT 格式）。將採取 VARIABLE_NAME=variable_value 格式的變數清單（個別列於單獨字行）加入至回應檔案。

   正確使用回應檔案，您必須在其中包含三個必要變數的最小集合：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

您也可新增任何選用變數來使用您遠端安裝更特定的變數。下表列出可包含在回應檔案中的所有變數：

回應檔案的變數會作為以靜默模式安裝網路代理的參數使用。

回應檔案的變數會作為以靜默模式安裝網路代理的參數使用。

變數名稱	必要	敘述	可能的值
KLNAGENT_SERVER	是	包含管理伺服器名稱，以完全合格的網域名稱 (FQDN) 或 IP 位址呈現。	DNS 名稱或 IP 位址。
KLNAGENT_AUTOINSTALL	是	定義是否啟用靜默的安裝模式。	1—啟用靜默模式；使用者在安裝期間未收到要採取任何行動的提示。 其他—停用靜默模式；使用者可能會在安裝期間收到要採取行動的提示。
EULA_ACCEPTED	是	定義使用者是否接受網路代理的最終使用者產品授權協議 (EULA)；遺失時，可解讀為未接受 EULA。	1—本人確認已完全閱讀、理解並接受本最終使用者授權協議的條款和條件。 其他值或未指定 — 表示我不接受產品授權協議的條款（將不會執行安裝）。
KLNAGENT_PROXY_USE	否	定義與管理伺服器的連線是否會使用代理設定。預設值是 0。	1—使用代理設定。 其他—未使用代理設定。
KLNAGENT_PROXY_ADDR	否	定義用來與管理伺服器連線的代理伺服器位址。	DNS 名稱或 IP 位址。
KLNAGENT_PROXY_LOGIN	否	定義用來登入代理伺服器的使用者名稱。	任何現有的使用者名稱。
KLNAGENT_PROXY_PASSWORD	否	定義用來登入代理伺服器的使用者密碼。	作業系統中密碼格式允許使用的任何英數字元集。
KLNAGENT_VM_VDI	否	定義網路代理是否已安裝在建立動態虛擬機器的映像檔。	1—網路代理會安裝在映像擋上，這在之後會用來建立動態虛擬機器。 其他—安裝期間沒有使用映像檔。
KLNAGENT_VM_OPTIMIZE	否	定義網路代理設定是否最適用於 hypervisor。	1—網路代理的預設本機設定已修改，以使其最佳運用 hypervisor。
KLNAGENT_TAGS	否	列出指派給網路代理實例的標籤。	由分號區隔的一或多個頁籤名稱。
KLNAGENT_UDP_PORT	否	定義由網路代理使用的 UDP 連接埠。預設值是 15000。	任何現有的埠號。
KLNAGENT_PORT	否	定義網路代理使用的非 TLS 連接埠。預設值是 14000。	任何現有的埠號。
KLNAGENT_SSLPORT	否	定義網路代理使用的 TLS 連接埠。預設值是 13000。	任何現有的埠號。
KLNAGENT_USESSL	否	定義連線是否使用傳輸層安全 (TLS)。	1（預設）—使用 TLS。 其他—不使用 TLS。
KLNAGENT_GW_MODE	否	定義是否使用連線閘道。	1（預設）—不修改目前設定（在初次呼叫中，不指定任何連線閘道）。 2—不使用任何連線閘道。 3—使用連線閘道。需要 KLNAGENT_GW_ADDRESS。 4—網路代理實例會在隔離區域 (DMZ) 作為連線閘道使用。需要伺服器憑證。
KLNAGENT_GW_新增RESS	否	定義連線閘道的位址。僅在 KLNAGENT_GW_MODE=3 時適用該值。	DNS 名稱或 IP 位址。

KLNAGENT_DEVICEOWNER_REGISTRATION_START	否	允許在網路代理安裝後作為裝置所有者公用程式執行使用者註冊。如果關閉，則使用者無法註冊為裝置所有者。	1 — 使用者註冊為裝置所有者公用程式將在網路代理安裝後執行。 其他—已關閉。
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	否	定義是否為網路代理自動安裝已下載但處於*未定義*狀態的更新。	true（預設）：更新會被自動安裝。 false：更新不會被自動安裝。

3. 執行網路代理安裝。KLAUTOANSWERS 環境變數指定應答檔案的路徑，並傳遞給安裝指令。執行以下指令：

   - 要將網路代理從 RPM 套件安裝到 32 位元作業系統，請執行以下指令：
     `sudo KLAUTOANSWERS=<應答檔案的路徑> yum install ./klnagent-<版本號>.i386.rpm`
   - 要將網路代理從 RPM 套件安裝到 64 位元作業系統，請執行以下指令：
     `sudo KLAUTOANSWERS=<應答檔案的路徑> yum install ./klnagent64-<版本號>.x86_64.rpm`
   - 要將網路代理從 RPM 套件安裝到 Arm 架構的 64 位元作業系統，請執行以下指令：
     `sudo KLAUTOANSWERS=<應答檔案的路徑> yum install ./klnagent64-<版本號>.aarch64.rpm`
   - 要將網路代理從 DEB 套件安裝到 32 位元作業系統，請執行以下指令：
     `sudo KLAUTOANSWERS=<應答檔案的路徑> apt install ./klnagent_<版本號>_i386.deb`
   - 要將網路代理從 DEB 套件安裝到 64 位元作業系統，請執行以下指令：
     `sudo KLAUTOANSWERS=<應答檔案的路徑> apt install ./klnagent64_<版本號>_amd64.deb`
   - 要將網路代理從 DEB 套件安裝到 Arm 架構的 64 位元作業系統，請執行以下指令：
     `sudo KLAUTOANSWERS=<應答檔案的路徑> apt install ./klnagent64_<版本號>_arm64.deb`

   根據作業系統配置，您也可以使用 rpm、dpkg 或 dnf 套件管理器來安裝網路代理。

Linux 的網路代理安裝會以靜默模式啟動；使用者在程序期間不會收到採取任何操作的提示。

檢視獨立安裝套件清單

您可檢視獨立安裝套件的清單以及各獨立安裝套件的內容。

若要所有安裝套件的獨立安裝套件清單：

在上述清單中，點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中，其屬性顯示如下：

- **套件名稱**。自動形成為包含在套件與應用程式版本中之應用程式名稱的獨立安裝套件名稱。
- **應用程式名稱**。包含在獨立安裝套件中的應用程式名稱。
- **應用程式版本**。
- **網路代理的安裝套件名稱**。僅在網路代理包含在獨立安裝套件中時才會顯示內容。
- **網路代理版本**。僅在網路代理包含在獨立安裝套件中時才會顯示內容。
- **大小**。檔案大小為 MB。

- **群組**。網路代理安裝後要將用戶端裝置移動過去的群組名稱。
- **建立日期**。建立獨立安裝套件的日期和時間。
- **修改日期**。修改獨立安裝套件的日期和時間。
- **路徑**。獨立安裝套件所在資料夾的完整路徑。
- **網址**。獨立安裝套件位置的網址。
- **檔案雜湊值**。該內容會用來驗證獨立安裝套件不是由協力廠商變更，且使用者有您建立與傳輸給使用者的相同檔案。

網路代理獨立套件或在虛擬管理伺服器上建立的任何套件的安裝套件清單中沒有關於大小、檔案雜湊和路徑的資訊。這些獨立套件在下載時產生。

若要檢視特定安裝套件的獨立安裝套件清單：

選取清單中的安裝套件，並在清單上點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中，您可執行以下操作：

- 點擊**發佈**按鈕，在網路伺服器上發佈獨立安裝套件。收到您傳送之獨立安裝套件連結的使用者，可下載已發佈的獨立安裝套件。
- 點擊**取消發佈**按鈕，取消網路伺服器上獨立安裝套件的發佈。只有您與其他管理員可下載取消發佈的獨立安裝套件。
- 點擊**下載**按鈕，下載獨立安裝套件至您的裝置。
- 點擊**透過電子郵件傳送**按鈕，傳送含有連至獨立安裝套件的連結。
- 點擊**移除**按鈕，移除獨立安裝套件。

分發安裝套件至從屬管理伺服器

Open Single Management Platform可讓您為卡巴斯基應用程式和協力廠商應用程式建立安裝套件，以及將套件分發到用戶端裝置並安裝軟體套件中的應用程式。要最佳化主管理伺服器上的負載，您可以將安裝套件分發到從屬管理伺服器。之後，從屬伺服器將套件傳輸到用戶端裝置，然後您可以在用戶端裝置上執行應用程式的遠端安裝。

若要分發安裝套件至從屬管理伺服器：

1. 請確定，從屬管理伺服器已連線到主管理伺服器。
2. 在主功能表中，轉至 **工作**。

   工作清單隨即顯示。
3. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。

4. 在**新工作設定**頁面上，從**應用程式**下拉清單中，選擇**卡巴斯基安全管理中心**。然後，從**工作類型**下拉清單中選擇**發佈安裝套件**，然後指定工作名稱。

5. 在 **工作範圍**頁面，透過以下方式之一選擇要將工作分配到哪些裝置：

   - 如果您要為管理群組中的所有從屬管理伺服器建立工作，您可以選取該群組，然後為其建立群組工作。
   - 如果要為特定的從屬管理伺服器建立工作，請選取這些伺服器，然後為其建立工作。

6. 在**發佈的安裝套件**頁面，選擇要複製到從屬管理伺服器的安裝套件。

7. 指定一個帳戶，以便在這個帳戶下執行*分發安裝套件*工作。您可以使用您的帳戶並保持**預設帳戶**選項處於啟用狀態。或者，您可以指定工作應在具有必要存取權限的另一個帳戶下執行。為此，請選擇**指定帳戶**選項，然後輸入該帳戶的憑據。

8. 在**完成工作建立**頁面上，您可以啟用**建立完成時開啟工作詳情**選項以開啟工作屬性視窗，然後修改預設工作設定。否則，您可以稍後隨時配置工作設定。

9. 點擊**完成**按鈕。

   為了將安裝套件分發到從屬管理伺服器而建立的工作，會顯示在工作清單中。

10. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

工作完成後，所選的安裝套件將複製到指定的從屬管理伺服器。

同時部署 Kaspersky Next XDR Expert 與 Kaspersky Endpoint Security for Linux

本節說明如何在由六部裝置組成的叢集中，同時部署 Kaspersky Next XDR Expert 與 Kaspersky Endpoint Security 12.5 for Linux。Kaspersky Endpoint Security for Linux 12.5 會以標準模式安裝在已安裝 OSMP 元件的裝置上。您可以透過命令列管理 Kaspersky Endpoint Security for Linux，無須安裝圖形介面。所有裝置都必須安裝網路代理。

為確保 Kaspersky Next XDR Expert 與 Kaspersky Endpoint Security for Linux 之間的最佳互通性，建議您設定 Kaspersky Endpoint Security for Linux 排除項目。

若要同時部署 Kaspersky Next XDR Expert 與 Kaspersky Endpoint Security 12.5 for Linux

1. 準備一個由六部裝置組成的叢集。

   此階段請勿安裝 Kaspersky Next XDR Expert。

2. 從Kaspersky 網站下載 Kaspersky Endpoint Security for Linux 分發套件。

3. 在叢集中的每部裝置上：

   a. 將下載的檔案（例如 kesl_12.5.0-1569_amd64.deb）放在 /root 目錄中。

   b. 執行以下命令安裝 Kaspersky Endpoint Security：

```
apt install /root/kesl_12.5.0-1569_amd64.deb
```

c. 執行以下命令啟動組態精靈：

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

d. 使用組態精靈指定安裝參數：

- 您要以 Light Agent 模式使用 Kaspersky Endpoint Security 嗎？[n]: **Enter**
- 您要以 Endpoint Detection and Response 代理模式使用 Kaspersky Endpoint Security 嗎？[n]: **Enter**
- 您要使用 EDR Expert Cloud 元件嗎？**Enter**
- [ru_RU.UTF-8]: **Enter**
- 按 Enter 鍵顯示最終使用者產品授權協議和隱私權政策：y **Enter**
  若要退出協議閱讀模式，請按 **q**。
- 我確認我已完整閱讀、理解並接受此最終使用者產品授權協議的條款和條件 [y/n]：y **Enter**
- 我瞭解並同意按照隱私政策所述來處理和傳輸我的資料(包括傳輸到協力廠商國家/地區)。我確認我已完整閱讀並理解隱私權政策 [y/n]：y **Enter**
- 我確認我已完整閱讀、理解並接受卡巴斯基安全網路聲明的條款和條件（KSN 聲明的內容位於 /opt/kaspersky/kesl/doc/ksn_license.en 檔案中）[y/n]：y **Enter**
- 輸入您要授予管理員角色的使用者名稱。若要跳過此步驟，請按 Enter 鍵：**Enter**
- 應用程式可以使用可更新的核心模組或 fanotify 技術來攔截系統事件。您要使用可更新的核心模組嗎？[n]: **Enter**
- 指定更新來源。可用值：KLServers|SCServer|<customsource> [KLServers]: **Enter**
- 如果您未使用代理伺服器，請輸入 [n]：**Enter**
- 您要立即下載最新的應用程式資料庫更新嗎？[y]: **Enter**
- 您要啟用應用程式資料庫自動更新嗎？[y]: **Enter**
- 您必須啟用應用程式才能使用。若要立即啟用應用程式，請輸入金鑰檔案的路徑或啟動碼。若要使用試用金鑰啟用應用程式，請按 Enter 鍵：**<your_activation_code> Enter**

e. 依序執行下列命令，建立 Kaspersky Endpoint Security 設定的備份副本：

```
kesl-control --get-app-settings > kesl_app_before.txt
kesl-control --get-settings File_Threat_Protection > kesl_ftp_before.txt
kesl-control --get-settings Behavior_Detection > kesl_bd_before.txt
kesl-control --get-settings System_Integrity_Monitoring > kesl_fim_before.txt
findmnt -o TARGET,SOURCE,FSTYPE > mounts_before.txt
```

f. 將包含設定和排除項目的檔案放在 /root 目錄中。

g. 依序執行下列命令，套用檔案中的排除項目：

- `kesl-control --set-app-settings --file /root/kesl_app.txt`

kesl_app.txt 檔案範例：

```
SambaConfigPath=/etc/samba/smb.conf
NfsExportPath=/etc/exports
TraceFolder=/var/log/kaspersky/kesl/
TraceLevel=None
TraceMaxFileCount=10
TraceMaxFileSize=500
BlockFilesGreaterMaxFileNamePath=16384
DetectOtherObjects=No
UseKSN=Extended
CloudMode=Yes
UseMDR=No
UseEdrOptimum=No
UseProxy=No
ProxyServer=
ProxyBypass=
ProxyBypassEdr=No
ProxyBypassSandbox=No
ProxyBypassNdr=No
MaxEventsNumber=500000
LimitNumberOfScanFileTasks=5
UseSyslog=Yes
EventsStoragePath=/var/opt/kaspersky/kesl/private/storage/events.db
FileBlockDuringScan=Yes
NamespaceMonitoring=No
PowerSaveMode=Yes
UseOnDemandCPULimit=No
OnDemandCPULimit=100
BackupSizeLimit=1024
BackupDaysToLive=30
QuarantineSizeLimit=200
QuarantineFillingNotification=90
QuarantineBackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
ShowPopUpNotifications=Yes
InterceptorMode=UseFanotify
InterceptorFallbackStrategy=FallbackToFanotify
InterceptorApplyStrategy=RestartServiceManually
SystemEventsTransmission=No
ExcludedMountPoint.item_0000=/run/netns/**
ExcludedMountPoint.item_0001=/run/k0s/containerd/io.containerd.grpc.v1.cri/sandboxes/**
ExcludedMountPoint.item_0002=/run/k0s/containerd/io.containerd.runtime.v2.task/**
ExcludedMountPoint.item_0003=/var/lib/k0s/kubelet/pods/**
ExcludedMountPoint.item_0004=/var/lib/k0s/kubelet/plugins/**
ExcludedMountPoint.item_0005=/opt/kaspersky/**
ExcludedMountPoint.item_0006=/var/log/pods
ExcludedMountPoint.item_0007=/var/tmp/alert-rules
ExcludedMountPoint.item_0008=/var/tmp/scripts
ExcludedMountPoint.item_0009=/*-metrics-data
ExcludedMountPoint.item_0010=/var/run/nats
ExcludedMountPoint.item_0011=/data
ExcludedMountPoint.item_0012=/storage
ExcludedMountPoint.item_0013=/var/loki
ExcludedMountPoint.item_0014=/var/lib/ksc64
ExcludedMountPoint.item_0015=/var/lib/grafana
ExcludedMountPoint.item_0016=/tmp/apttmp
```

- `kesl-control --set-settings File_Threat_Protection --file /root/kesl_ftp.txt`

  kesl_ftp.txt 檔案範例：

```
ScanArchived=No
ScanSfxArchived=No
ScanMailBases=No
ScanPlainMail=No
TimeLimit=60
SizeLimit=8
ActionOnThreat=DisinfectDeleteIfNotPossible
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanByAccessType=SmartCheck
```

```
SkipPlainTextFiles=No
SkipDatabaseJournals=No
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0000]
AreaDesc=postgres
UseScanArea=Yes
Path=/var/lib/postgresql
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0001]
AreaDesc=Host_Kuber
UseScanArea=Yes
Path=/var/lib/k0s/kubelet
AreaMask.item_0000='*'
[ExcludedFromScanScope.item_0003]
AreaDesc=Host_TMP
UseScanArea=Yes
Path=/tmp
AreaMask.item_0000='*'
[ExcludedFromScanScope.item_0004]
AreaDesc=KUMA
UseScanArea=Yes
Path=/opt/kaspersky/kuma
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0005]
AreaDesc=CONT_TMP
UseScanArea=Yes
Path=/tmp/tmp**
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0006]
AreaDesc=CONT_TMP
UseScanArea=Yes
Path=/tmp/resultworker**
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0007]
AreaDesc=k0s_runtime
UseScanArea=Yes
Path=/run/k0s
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0008]
AreaDesc=containerd_runtime
UseScanArea=Yes
Path=/run/containerd
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0009]
AreaDesc=pod_logs
UseScanArea=Yes
Path=/var/log/pods
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0010]
AreaDesc=container_logs
UseScanArea=Yes
Path=/var/log/containers
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0011]
AreaDesc=calico_logs
UseScanArea=Yes
Path=/var/log/calico
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0012]
AreaDesc=kaspersky_logs
UseScanArea=Yes
Path=/var/log/kaspersky
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0013]
AreaDesc=kaspersky_data
UseScanArea=Yes
Path=/var/opt/kaspersky
AreaMask.item_0000=*
[ExcludedForProgram.item_0000]
ProgramPath=/var/lib/k0s/bin/containerd
ApplyToDescendants=Yes
AreaDesc=k0s_containerd
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
[ExcludedForProgram.item_0001]
ProgramPath=/var/lib/k0s/bin/containerd-shim-runc-v2
ApplyToDescendants=Yes
```

```
AreaDesc=k0s_shim
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
[ExcludedForProgram.item_0002]
ProgramPath=/var/lib/k0s/bin/runc
ApplyToDescendants=Yes
AreaDesc=k0s_runc
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
[ExcludedForProgram.item_0003]
ProgramPath=/opt/kaspersky/kuma
ApplyToDescendants=No
AreaDesc=KUMA
UseExcludedForProgram=Yes
Path=/
AreaMask.item_0000=*
```

- `kesl-control --set-settings Behavior_Detection --file /root/kesl_bd.txt`

  kesl_bd.txt 檔案範例：

```
UseTrustedPrograms=Yes
TaskMode=Block
UseAEP=No
AEPMode=Block
UseTelemetryMonopolyMode=Yes
TelemetrySource=Default
[TrustedPrograms.item_0000]
ProgramPath=/var/lib/k0s/bin/containerd
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=k0s_containerd
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0001]
ProgramPath=/var/lib/k0s/bin/runc
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=k0s_runc
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0002]
ProgramPath=/var/lib/k0s/bin/containerd-shim-runc-v2
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=k0s_shim
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0003]
ProgramPath=/usr/sbin/iptables-legacy
ApplyToDescendants=No
UseTrustedProgram=Yes
ProgramDesc=calico_iptables
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0004]
ProgramPath=/usr/sbin/xtables-nft-multi
ApplyToDescendants=No
UseTrustedProgram=Yes
ProgramDesc=calico_xtables
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
[TrustedPrograms.item_0005]
ProgramPath=/usr/bin/calico-node
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=calico_node
UseTrustedProgramForDetects=Yes
[TrustedPrograms.item_0006]
ProgramPath=/opt/kaspersky/kuma
ApplyToDescendants=Yes
UseTrustedProgram=Yes
ProgramDesc=
UseTrustedProgramForDetects=Yes
UseTrustedProgramForMDRAndEDR=No
```

- `kesl-control --set-settings System_Integrity_Monitoring --file /root/kesl_fim.txt`

  kesl_fim.txt 檔案範例：

```
UseExcludeMasks=No
[ScanScope.item_0000]
AreaDesc=Kaspersky internal objects
UseScanArea=Yes
Path=/opt/kaspersky/kesl/
AreaMask.item_0000=*
[ScanScope.item_0001]
AreaDesc=etc
UseScanArea=Yes
Path=/etc
AreaMask.item_0000=*
[ScanScope.item_0002]
AreaDesc=ksc
UseScanArea=Yes
Path=/opt/kaspersky/ksc64
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0000]
AreaDesc=klnagent_flags
UseScanArea=Yes
Path=/etc/opt/kaspersky/klnagent
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0001]
AreaDesc=cni_config
UseScanArea=Yes
Path=/etc/cni/net.d
AreaMask.item_0000=*
```

h. 套用排除項後，依序執行下列指令，建立 Kaspersky Endpoint Security 設定的快照：

```
kesl-control --get-app-settings > kesl_app_after.txt
kesl-control --get-settings File_Threat_Protection > kesl_ftp_after.txt
kesl-control --get-settings Behavior_Detection > kesl_bd_after.txt
kesl-control --get-settings System_Integrity_Monitoring > kesl_fim_after.txt
findmnt -o TARGET,SOURCE,FSTYPE > mounts_after.txt
```

i. 執行下列指令，停止 Kaspersky Endpoint Security：

```
systemctl stop kesl-control
```

4. 在 Kaspersky Next XDR Expert 操作員的裝置上執行下列指令，以安裝 Kaspersky Next XDR Expert：

```
./xdr/kdt/bin/kdt apply -k xdr/<full_path_to_transport_archive> -i xdr/param.yml --accept-eula
```

如果在使用 KDT 部署 Kaspersky Next XDR Expert 時發生錯誤，請指定不含 `-i` 旗標的設定檔路徑，以重新開始部署。

5. 在叢集中的所有裝置上執行下列指令，啟動 Kaspersky Endpoint Security 服務：

```
systemctl start kesl
```

6. 在 Kaspersky Next XDR Expert 主控台中，下載並建立安裝套件。

7. 在 **軟體管理 → 下載並建立安裝套件** 中，選取您建立的安裝套件，然後按一下 **佈署**。

8. 選取 **使用獨立安裝套件**，然後選取 **下載獨立安裝套件**。

9. 在每個叢集裝置上，將下載的檔案（例如 klnagent64_16.3.0-1207_amd64.sh）放入 /root 目錄，將其設為可執行，然後執行該檔案：

```
./klnagent64_16.3.0-1207_amd64.sh
```

10. 在 Kaspersky Next XDR Expert 主控台中，前往 **資產管理 → 資產（裝置） → 管理和防護** 區段，確認表格中有一項資產，其名稱與安裝了網路代理的裝置名稱相同。

11. 前往 **資產管理 → 資產（裝置） → Detection and response**，按一下三點按鈕，選取 **匯入 → 匯入 KSC 資產 → 全部**，然後按一下 **匯入**。

12. 前往 **資產管理 → 資產（裝置） → Detection and response**，按一下三點按鈕，選取 **匯入 → 匯入 KSC 資產屬性 → 全部**，然後按一下 **匯入**。

    該資產會顯示在 **資產管理 → 資產（裝置） → Detection and response** 區段中。

13. 前往 **資產管理 → 政策** 區段，然後按一下 **新增**。

14. 選取 **Kaspersky Endpoint Security for Linux 12.5**，然後選取 **標準模式**。

15. 如果您想使用卡巴斯基安全網路，請接受 KSN 聲明。

16. 設定 Kaspersky Endpoint Security 政策。

    如何設定 Kaspersky Endpoint Security 政策

    1. 前往 **應用程式設定** 索引標籤，然後執行下列操作：

       a. 解鎖下列區段中的所有設定：

       - **主機威脅防護 → 檔案威脅防護**。
       - **主機威脅防護 → 行為分析 → 行為偵測**。
       - **信任區域**。
       - **一般設定 → 容器掃描**。

       b. 在 **主機威脅防護 → 行為分析 → 弱點利用防禦** 區段中，解鎖 **弱點利用防禦** 設定。

       c. 在 **通訊與 Web 防護 → 郵件威脅防護** 區段中，將切換開關設為 **郵件威脅防護已停用**。

       d. 在 **通訊與 Web 防護 → Web 威脅防護** 區段中，將切換開關設為 **Web 威脅防護已停用**。

       e. 在 **通訊與 Web 防護 → 網路威脅防護** 區段中，將切換開關設為 **網路威脅防護已停用**。

       f. 在 **通訊與 Web 防護 → 防火牆** 區段中，將切換開關設為 **防火牆已關閉**。

       g. 在 **安全控制 → 系統完整性監控** 中，將切換開關設為 **系統完整性監控已停用**。

       h. 在 **一般設定 → 偵測設定** 中，解鎖 **檔案操作攔截模式** 設定。

       i. 在 **一般** 索引標籤上，將 **政策狀態** 設為 **作用中**，然後按一下 **傳送並關閉**。

    政策完全套用約需 20 分鐘。

17. 若要在政策中設定 EDR 遙測，請選取 **應用程式設定 → 內置代理設定 → Endpoint Detection and Response Expert（內部部署）** 索引標籤，然後按一下 **設定**。

18. 啟用 **Endpoint Detection and Response Expert（內部部署）**。

19. 選取 **[[HmgP9nbh]]Endpoint Detection and Response Expert（8.0 或更新版本）** 模式。

20. 在 **連線至遙測收集伺服器** 下，按一下 **新增 → 選取伺服器**，然後選取唯一可用的位址。

21. 在 **連線至回應伺服器** 下，按一下 **新增 → 選取伺服器**，然後選取唯一可用的位址。

22. 按一下**儲存並關閉**。

有關管理Kaspersky Endpoint Security for Linux 的詳細資訊，請參閱線上說明：

- 安裝、移除及更新應用程式。
- 使用命令列管理應用程式。
- 使用卡巴斯基安全管理中心管理應用程式。

使用遠端軟體安裝工作安裝應用程式

Kaspersky Next XDR Expert 可讓您使用遠端安裝工作，在裝置上遠端安裝應用程式。那些工作透過專門精靈被建立被分配到裝置。要更快和更便捷地分配工作，您可以在精靈視窗中指定裝置（最多 1000 台裝置），使用以下方式之一：

- **指派工作給管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。
- **手動指定裝置位址或是從清單匯入位址**。您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。
- **指派工作給裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預設分類或您所建立的自訂分類。您最多只能選擇 1000 個裝置。

為避免在未安裝網路代理程式的用戶端裝置上安裝應用程式時可能出現的問題，您必須按照透過Open Single Management Platform的遠端安裝工作強制部署中所述進行操作。

遠端安裝應用程式

本節包含有關如何在管理群組、具有特定位址的裝置或選擇的裝置上遠端安裝應用程式的資訊。

若要安裝應用程式到特定裝置：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。
3. 在**工作類型**欄位中，選擇**遠端安裝應用程式**。

4. 您可以選取以下其中一個方法：

- **指派工作給管理群組**

  工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

  例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

  如果工作被指派給管理群組，則工作內容視窗中不會顯示**安全**頁籤，因為群組工作受其所套用的群組的安全設定的約束。

- **手動指定裝置位址或是從清單匯入位址**

  您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。

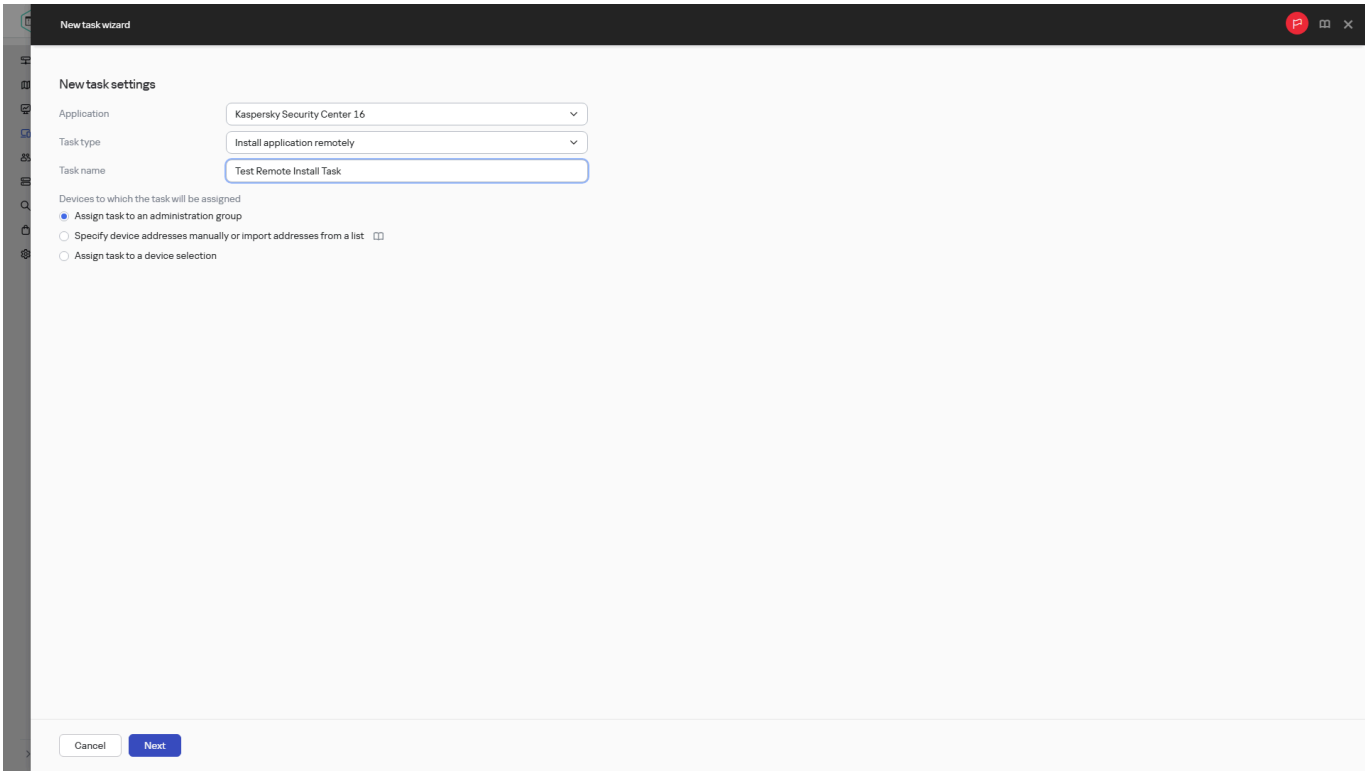
  您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

- **指派工作給裝置分類**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

*遠端安裝應用程式*工作得以為指定裝置建立。如果您選擇了**指派工作給管理群組**選項，工作將是一個組工作。



建立遠端安裝應用程式工作

5. 在**工作範圍**步驟，指定管理群組、具有特定位址的裝置或裝置選擇。

   可用設定取決於在上一步中選擇的選項。

6. 在**安裝套件**步驟中，指定以下設定：

- 在**選取安裝套件**欄位中，選擇要安裝的應用程式的安裝套件。
- 在**強制下載安裝套件**設定群組中，指定如何將安裝應用程式所需的檔案分發到用戶端裝置中：
  - **使用網路代理**

    如果啟用此選項，安裝套件透過安裝在裝置上的網路代理傳送到用戶端裝置。

    如果停用此選項，則會使用用戶端裝置的作業系統工具傳送安裝套件。

    如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。

    預設情況下已啟用該選項。

  - **透過發佈點使用作業系統資源**

    如果啟用此選項，安裝套件使用作業系統工具透過發佈點傳送到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取本選項。

    如果選取**使用網路代理**方塊，僅在網路代理工具不可用時才透過作業系統工具傳送檔案。

    預設情況下，已經為虛擬管理伺服器上建立的遠端安裝工作選取該選項。

    在未安裝網路代理的裝置上安裝 Windows 應用程式（包括 Windows 網路代理）的唯一方法是使用基於 Windows 的發佈點。因此，當您安裝 Windows 應用程式時：

    - 選擇此選項。
    - 確保為目標用戶端裝置分配了發佈點。
    - 確保發佈點基於 Windows。

  - **透過管理伺服器使用作業系統資源**

    如果啟用此選項，檔案將使用用戶端裝置的作業系統工具透過管理伺服器傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

    預設情況下已啟用該選項。

- 在**同時下載的最大數量**欄位中，指定管理伺服器可以同時向其傳輸檔案的最大用戶端裝置數量。
- 在**安裝嘗試次數上限**欄位中，指定安裝程式執行的最大允許次數。

  如果超過參數中指定的嘗試次數，Kaspersky Next XDR Expert 將不再在裝置上啟動安裝程式。若要重新啟動*遠端安裝應用程式*工作，請增加**安裝嘗試次數上限**參數的值並啟動工作。或者，您可以建立新的"*遠端安裝應用程式*"工作。

- 如果您從一個卡巴斯基應用程式移轉到另一個卡巴斯基應用程式，並且當前應用程式受密碼保護，請在**用來解除安裝目前卡巴斯基應用程式的密碼**中輸入密碼。請注意，在移轉過程中，將會解除安裝您目前的卡巴斯基應用程式。

僅當您在**用來解除安裝目前卡巴斯基應用程式的密碼**設定群組中選擇**使用網路代理**選項時，才可使用**強制下載安裝套件**欄位。

使用遠端安裝應用程式工作安裝 Kaspersky Endpoint Security for Windows 時，您只能在從 Kaspersky Security for Windows Server 到 Kaspersky Endpoint Security for Windows 遷移方案中使用移除密碼。安裝其他元件時使用移除密碼可能會導致安裝錯誤。

若要成功完成移轉情境，請確保滿足以下先決條件：

- 您使用的是適用於 Windows 的卡巴斯基安全管理中心網路代理 14.2 或更高版本。
- 您正在執行 Windows 的裝置上安裝應用程式。

- 定義附加設定：
  - **如果已經安裝應用程式則不再重新安裝**

    如果啟用此選項，則如果選定的應用程式已安裝到該用戶端裝置上，將不再重新安裝它。

    如果停用此選項，系統仍將安裝應用程式。

    預設情況下已啟用該選項。

  - **下載之前驗證作業系統類型**

    在將檔案傳輸到用戶端裝置之前，Open Single Management Platform將檢查「安裝公用程式」設定是否適用於用戶端裝置的作業系統。如果設定不適用，則Open Single Management Platform不會傳輸檔案，也不會嘗試安裝應用程式。例如，要將某些應用程式安裝到包括執行各種作業系統之裝置的管理群組裝置，您可以將安裝工作指派給管理群組，然後啟用此選項以跳過執行不是要求的作業系統的裝置。

    無論**下載之前驗證作業系統類型**的設定為何，當您在未指派的裝置上遠端安裝網路代理程式時，Open Single Management Platform 或分發點會自動確定裝置的作業系統類型。

  - **在 Active Directory 群組政策中指派安裝套件的安裝**

    如果選取此方塊，安裝套件會使用 Active Directory 的群組政策安裝。

    如果選取網路代理安裝套件，則該方塊可用。

    預設情況下已停用該選項。

  - **提示使用者關閉執行中的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

- 選擇要在哪些裝置上安裝應用程式：
  - **在所有裝置上安裝**

    應用程式將被安裝到由其他管理伺服器管理的裝置。

    預設情況下已選取此選項。如果您在網路中只有一個管理伺服器，您不必變更該設定。

  - **僅安裝到透過該管理伺服器管理的裝置**

    應用程式將僅被安裝到由該管理伺服器管理的裝置。如果您在網路中有多個管理伺服器且需要避免它們之間的衝突，請選取該選項。

- 指定裝置是否在安裝後必須被移動到管理群組：

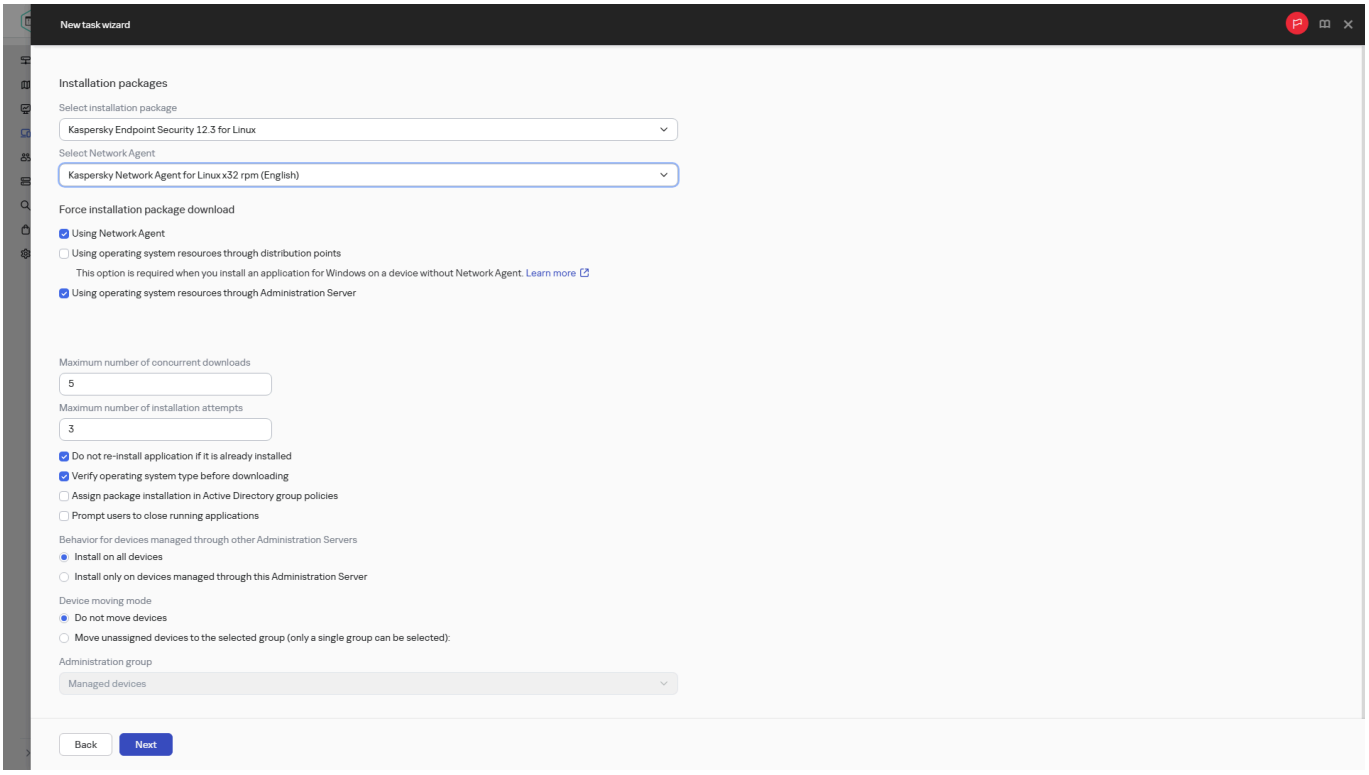
  - **不移動裝置**

    裝置保留在目前所在群組中。未被放置在任何群組的裝置保持未分配。

  - **移動未指派的裝置到所選群組（僅可以選取單一群組）**

    裝置被移動到您選取的管理群組。

  請注意，預設情況下已選取**不移動裝置**選項。為了安全，您可能會希望手動移動裝置。



指定工作設定

7. 在精靈的這一步，指定在安裝應用程式期間是否必須重新啟動裝置：

   - **不重新啟動裝置**

     如果選取該選項，安全應用程式安裝後裝置不被重新啟動。

   - **重新啟動裝置**

     如果選取該選項，安全應用程式安裝後裝置將被重新啟動。

8. 如有必要，在**選取帳戶以存取裝置**步驟，新增將用於啟*動遠端安裝應用程式*工作的帳戶 ：

   - **不需要帳戶（網路代理已安裝）**

     如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

     如果網路代理未安裝在用戶端裝置，該選項不可用。

- **需要帳戶（不使用網路代理）**

  如果您為其分配遠端安裝工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶或 SSH 憑證來安裝應用程式。

  - **本機或網域帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機或網域帳戶**，然後指定使用者帳戶憑據。

    您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

  - **SSH 憑證**。如果要在 Linux 用戶端裝置上安裝應用程式，您可以指定 SSH 憑證而不是指定使用者帳戶。按一下**新增**按鈕，選擇**SSH 憑證**，然後指定憑證的私鑰和公鑰。

    如要產生私密金鑰，您可以使用 ssh-keygen 公用程式。請注意，Open Single Management Platform支援PEM格式的私密金鑰，但ssh-keygen公用程式預設為產生OPENSSH格式的SSH金鑰。Open Single Management Platform不支援OPENSSH格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 -m PEM 選項。例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵箱 >"
    ```

9. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   若您啟用**建立完成時開啟工作詳情**選項，工作設定視窗隨即開啟。在此視窗中，您可以檢查工作參數、修改它們或配置工作啟動排程（如有必要）。

10. 在工作清單中，選擇您建立的工作，然後點擊**開始**。

    或者，等候工作按照您在工作設定中指定的排程啟動。

遠端安裝工作完成後，所選應用程式將安裝在指定裝置上。

在從屬管理伺服器上安裝應用程式

如果您的管理伺服器版本為 15.4 或更高版本，則只能在從屬管理伺服器上安裝應用程式，前提是從屬管理伺服器的版本為 15.4 或更高版本。

在從屬管理伺服器上安裝應用程式：

1. 與控制相關從屬管理伺服器的管理伺服器建立連線。

2. 請您確定每台從屬管理伺服器都必須有要安裝的應用程式套件。如果在任何從屬伺服器上都找不到安裝套件，請發佈它。為此，建立一個工作類型為**發佈安裝套件**的工作。

3. 在從屬管理伺服器上建立一個遠端應用程式安裝工作。選擇**將應用程式遠端安裝到從屬管理伺服器**工作類型。

   新工作精靈會在特定的從屬管理伺服器上建立精靈中所選應用程式的遠端安裝工作。

4. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

遠端安裝工作完成後，所選應用程式將安裝在從屬管理伺服器上。

指定在 Unix 裝置上進行遠端安裝的設定

當您使用遠端安裝工作在 Unix™ 裝置上安裝應用程式時，可以為該工作指定 Unix 特定設定。建立工作後，這些設定可在工作屬性中使用。

要為遠端安裝工作指定特定於 Unix 的設定，請執行以下操作：

1. 在主功能表中，轉至 **工作**。
2. 按一下您要為其指定 Unix 特定設定的遠端安裝工作名稱。

   工作內容視窗隨即開啟。
3. 前往**應用程式設定 → Unix 特定設定**。
4. 指定下列設定：

   - **設定根帳戶密碼（僅適用於透過 SSH 佈署）**

     若未指定密碼即無法在目標裝置上使用 sudo 命令，請選取此選項，然後指定 root 帳戶的密碼。Kaspersky Next XDR Expert 會以加密形式將密碼傳送到目標裝置，解密該密碼後，再使用指定的密碼以根帳戶身分啟動安裝程序。

     > Kaspersky Next XDR Expert不會使用該帳戶或指定的密碼來建立SSH連線。

   - **指定前往暫存資料夾的路徑，具有目標裝置上的執行權限（僅適用於透過 SSH 佈署）**

     如果目標裝置上的 /tmp 目錄沒有執行權限，請選擇此選項，然後指定具有執行權限的目錄路徑。Kaspersky Next XDR Expert使用指定的目錄作為透過SSH存取的暫存目錄。應用程式會將安裝套件放在目錄中並執行安裝程序。
5. 點擊**儲存**按鈕。

隨即儲存指定的工作設定。

啟動和停止卡巴斯基應用程式

您可以使用*啟動或停止應用程式*工作來啟動和停止受管理裝置上的卡巴斯基應用程式。

若要建立啟動或停止應用程式工作：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**應用程式**下拉清單，選取要為其建立工作的應用程式。
4. 在**工作類型**清單中，選取**啟動或停止應用程式**工作。

5. 在**工作名稱**欄位，指定新工作的名稱。

   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

6. 選取要對其分配工作的裝置：

7. 在**應用程式**視窗，執行以下操作：

   - 選取要為其建立工作的應用程式名稱旁的核取方塊。
   - 選擇**啟動應用程式**或**停止應用程式**選項。

8. 若要修改預設工作設定，請啟用**建立完成時開啟工作詳情**步驟的**完成工作建立**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時變更預設設定。

9. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 在工作內容視窗中，依需求指定一般工作設定，然後儲存設定。

    工作被建立和配置。

若要執行工作，請在工作清單選取該工作，然後點擊**開始**按鈕。

取代協力廠商安全應用程式

透過 Kaspersky Next XDR Expert 安裝 Kaspersky 安全應用程式時，可能需要移除與所安裝應用程式不相容的協力廠商軟體。Open Single Management Platform提供了多種移除協力廠商應用程式的方法。

當配置應用程式遠端安裝時移除不相容應用程式

您可以在防護部署精靈中配置安全應用程式遠端安裝時，啟用**自動解除安裝不相容的應用程式**選項。啟用此選項後，Open Single Management Platform會在管理裝置上安裝安全應用程式前，先移除不相容的應用程式。

透過專用工作移除不相容的應用程式

若要透過工作移除不相容的應用程式，請使用*遠端解除安裝應用程式*工作。該工作應該在安全應用程式安裝工作執行之前執行在裝置。例如，在安裝工作中，您可以選取**在完成其它工作時**作為排程類型，其中的其他工作為*遠端解除安裝應用程式*。

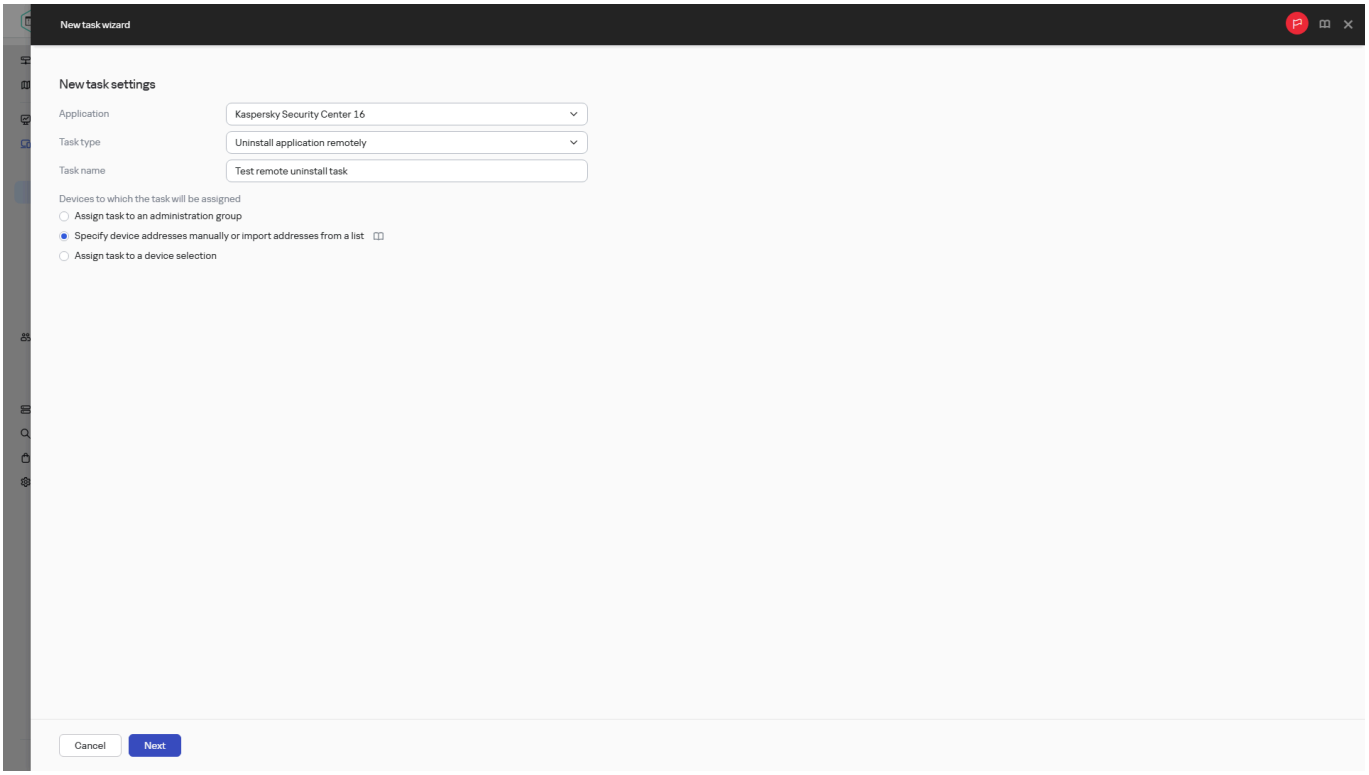
該移除方法在安全應用程式無法正確移除不相容應用程式時是很有用的。

遠端移除應用程式或軟體更新

您只能使用網路代理刪除遠端執行 Linux 的受管理裝置上的應用程式或軟體更新。

要從所選裝置遠端刪除應用程式或軟體更新，請執行以下操作：

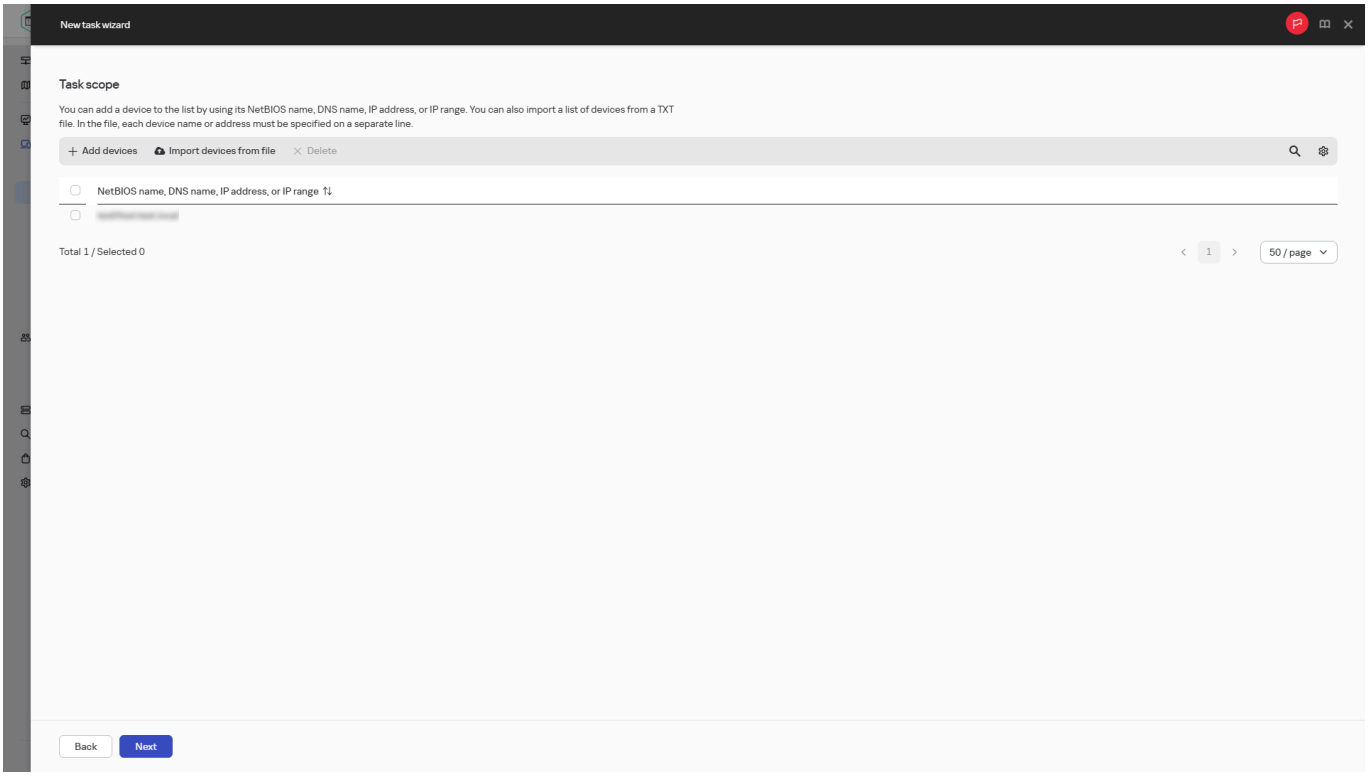
1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**應用程式**下拉式清單中，選擇 Kaspersky Next XDR Expert。
4. 在**工作類型**清單中，選擇**遠端解除安裝應用程式**工作類型。
5. 在**工作名稱**欄位，指定新工作的名稱。
   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。



建立遠端解除安裝應用程式工作

6. 選取要對其分配工作的裝置：

轉到精靈的下一個步驟。



指定工作範圍

7. 選擇要刪除的軟體類型，然後選擇要刪除的特定應用程式，更新或修補程式：

- **解除安裝受管理應用程式**

  顯示 Kaspersky 應用程式清單。選取您要移除的弱點。

  確認受管理應用程式的**使用解除安裝密碼**政策設定已停用。

- **解除安裝不相容的應用程式**

  顯示與卡巴斯基安全應用程式或Open Single Management Platform不相容的應用程式清單。選取您要刪除之項目旁的核取方塊。

- **從應用程式登錄資料中解除安裝應用程式**

  預設情況下，網路代理會傳送管理伺服器有關受管理裝置上安裝的應用程式資訊。已安裝的應用程式清單會儲存在應用程式登錄資料中。

  要從應用程式登錄資料中選取一個應用程式：

  a. 點擊**要解除安裝的應用程式**欄位，然後選擇要刪除的應用程式。

  如果您選擇卡巴斯基安全管理中心網路代理，則當您執行工作時，狀態*已成功完成*會顯示刪除過程已開始。如果卡巴斯基安全管理中心網路代理被移除，則狀態不會變更。如果工作失敗，狀態將變更為*失敗*。

b. 指定移除選項：

- **解除安裝模式**

  選取您要如何移除該應用程式：

  - **自動定義解除安裝指令**

    如果應用程式具有應用程式供應商定義的解除安裝命令，則Open Single Management Platform將使用此命令。我們建議您選取此選項。

  - **指定解除安裝指令**

    如果要為解除安裝應用程式指定自己的命令，請選取此選項。

    > 建議您先嘗試使用**自動定義解除安裝指令**選項。如果透過自動定義的解除安裝命令失敗，請使用自己的命令。

    在該欄位中鍵入安裝命令，然後指定以下選項：

    除非未自動偵測預設指令，否則將使用此指令進行解除安裝

    Open Single Management Platform會檢查所選應用程式是否具有應用程式供應商定義的解除安裝命令。如果找到該命令，則Open Single Management Platform將使用該命令，而不是**應用程式解除安裝指令**欄位中指定的命令。

    我們建議您啟用該選項。

- **應用程式成功解除安裝後執行重新啟動**

  如果應用程式要求成功移除後在受管理裝置上重新啟動作業系統，則作業系統將會自動重新啟動。

- **解除安裝指定的應用程式更新、修補程式或其他應用程式**

  顯示更新、修補程式和協力廠商應用程式的清單。選取您要移除的項目。

  顯示的清單是應用程式和更新的常規清單，並不對應於受管理裝置上安裝的應用程式和更新。選取項目之前，建議您確保在工作範圍中定義的裝置上安裝了應用程式或更新。您可以透過內容視窗檢視安裝了應用程式或更新的裝置清單。

  若要檢視裝置清單：

  a. 按一下應用程式名稱或更新。

  內容視窗隨即開啟。

  b. 開啟**裝置**區段。

  您還可以在裝置內容視窗中檢視已安裝的應用程式和更新的清單。

8. 指定用戶端裝置將如何下載解除安裝公用程式：

- **使用網路代理**

  檔案會透過安裝在這些用戶端裝置上的網路代理傳遞到用戶端裝置。

  如果停用此選項，則會使用 Linux 作業系統工具傳送檔案。

  如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。

- **透過管理伺服器使用作業系統資源**

  該選項已過時。請改用**使用網路代理**或**透過發佈點使用作業系統資源**選項。

  使用管理伺服器作業系統工具將檔案傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

- **透過發佈點使用作業系統資源**

  使用作業系統工具透過發佈點將檔案傳輸到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取此選項。

  如果啟用**使用網路代理**方塊，僅在網路代理工具不可使用時才會透過作業系統工具傳送檔案。

- **同時下載的最大數量**

  管理伺服器可以同時向其傳輸檔案的最大用戶端裝置數量。此數字越大，應用程式解除安裝的速度越快，但是管理伺服器上的負載會更高。

- **解除安裝嘗試次數上限**

  若是在執行*遠端解除安裝應用程式*工作時，Open Single Management Platform解除安裝受管理裝置的應用程式失敗超過指定次數，Open Single Management Platform會停止傳送解除安裝公用程式到該受管理裝置，且不再在該裝置上啟動安裝程式。

  解除安裝嘗試次數上限參數允許您節省受管理裝置資源，以及減少流量（移除、MSI 檔案執行和錯誤訊息）。

  重複的工作啟動嘗試可能提示裝置具有妨礙解除安裝的問題。管理員應在指定的移除嘗試次數內解決問題，然後重新啟動工作（手動或按排程）。

  如果解除安裝始終未完成，問題被視為無法解決且後續工作啟動被認為是不必要的資源和流量浪費。

  建立該工作時，嘗試次數計數器會設定為 `0`。返回錯誤的安裝程式的每次執行都增加計數。

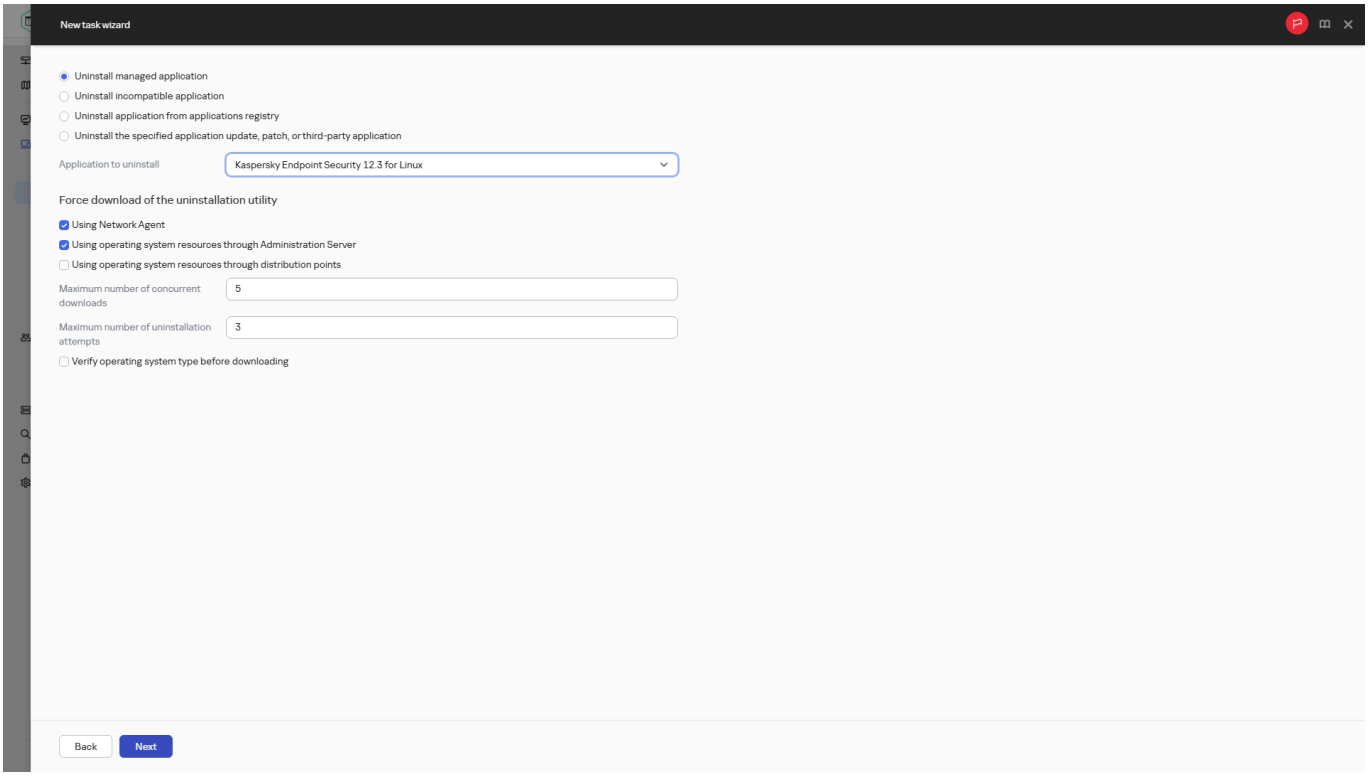
  如果超過指定的嘗試次數且裝置已準備好解除安裝應用程式，您可以增加**解除安裝嘗試次數上限**參數的值並啟動工作以解除安裝應用程式。或者，您可以建立新的*遠端解除安裝應用程式*工作。

- **下載之前驗證作業系統類型**

  在將檔案傳輸到用戶端裝置之前，Open Single Management Platform將檢查「安裝公用程式」設定是否適用於用戶端裝置的作業系統。如果設定不適用，則Open Single Management Platform不會傳輸檔案，也不會嘗試安裝應用程式。例如，要將某些應用程式安裝到包括執行各種作業系統之裝置的管理群組裝置，您可以將安裝工作指派給管理群組，然後啟用此選項以跳過執行不是要求的作業系統的裝置。

  無論**下載之前驗證作業系統類型**的設定為何，當您在未指派的裝置上遠端安裝網路代理程式時，Open Single Management Platform 或分發點會自動確定裝置的作業系統類型。

轉到精靈的下一個步驟。



指定工作設定

9. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者動作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**
  - **在該時間後重新啟動（分鐘）**

- **強制關閉被封鎖工作階段中的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

預設情況下已停用該選項。

轉到精靈的下一個步驟。

10. 如果必要，請新增要用於啟動遠端解除安裝工作的帳戶：

- **不需要帳戶（網路代理已安裝）**

  如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

  如果網路代理未安裝在用戶端裝置，該選項不可用。

- **需要帳戶（不使用網路代理）**

  如果您為其分配*遠端解除安裝應用程式*工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶或 SSH 憑證來取消安裝應用程式。

  - **本機或網域帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機或網域帳戶**，然後指定使用者帳戶憑據。

    您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

  - **SSH 憑證**。如果要在 Linux 型用戶端裝置上安裝應用程式，您可以指定 SSH 憑證而不是指定使用者帳戶。按一下**新增**按鈕，選擇**SSH 憑證**，然後指定憑證的私鑰和公鑰。

    如要產生私密金鑰，您可以使用 ssh-keygen 公用程式。請注意，Open Single Management Platform支援PEM格式的私密金鑰，但ssh-keygen公用程式預設為產生OPENSSH格式的SSH金鑰。Open Single Management Platform不支援OPENSSH格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 -m PEM 選項。

    例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵箱 >"
    ```

11. 如果您在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項，即可編輯工作的預設設定。

    如果您不啟用該選項，工作使用預設設定建立。您可以稍後再修改預設設定。

12. 點擊**完成**按鈕。

    精靈即會建立物件。如果您啟用了**建立完成時開啟工作詳情**選項，工作內容視窗即會自動開啟。在此視窗中，您可以指定一般工作設定，並視需要變更在工作建立期間指定的設定。

    > 您也可以透過在工作清單中點擊所建立工作的名稱，開啟工作內容視窗。

    工作隨即建立、設定，並顯示在**工作**的工作清單中。

13. 若要執行工作，請在工作清單選取該工作，然後點擊**開始**按鈕。

    您也可以在工作內容視窗的**排程**頁籤上，設定工作啟動排程。

    如需排程啟動設定的詳細說明，請參閱一般工作設定。

工作完成後，選中的應用程式會被從所選裝置中移除。

遠端解除安裝問題

有時遠端解除安裝協力廠商應用程式可能會在結束時出現以下警告：“遠端解除安裝已在該裝置上完成，但有警告：要移除的應用程式未安裝。”當要解除安裝的應用程式已被解除安裝或者僅為單個使用者安裝時，會發生該問題。如果使用者未登入，則為單個使用者安裝的應用程式（也稱為按照使用者發放的應用程式）不可見或者無法進行遠端解除安裝。

該行為與同一裝置上供多名使用者使用的應用程式（也稱為按照裝置發放的應用程式）不同。按照裝置發放的應用程式可供裝置的所有使用者看見和存取。

因此，僅當使用者登入時才可解除安裝按照使用者發放的應用程式。

有關已安裝應用程式的資訊來源

網路代理從以下登錄機碼提取關於安裝在 Windows 裝置上的軟體的資訊：

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為所有使用者安裝的應用程式的資訊。
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為所有使用者安裝的應用程式的資訊。
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為目前使用者安裝的應用程式的資訊。
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為特定使用者安裝的應用程式的資訊。

配置卡巴斯基應用程式

本節包含有關政策和工作的手動配置、使用者角色、建構管理群組結構和工作階層的資訊。

情境：配置網路防護

建立和配置網路所需的政策和工作。

先決條件

在您開始之前，確保您已做了如下：

- 已安裝管理伺服器
- 已安裝OSMP主控台
- 已完成Open Single Management Platform主安裝程式方案

設定要以階段進行的網路防護：

1. **設定和傳播 Kaspersky 應用程式政策和政策設定檔**

   要為安裝在受管理裝置上的 Kaspersky 應用程式配置和傳播設定，您可以使用兩種不同的安全管理方法—以裝置為中心或以使用者為中心。這兩種方法也可以被合併。

2. **配置工作以遠端管理 Kaspersky 應用程式**

   在**受管理裝置**管理群組中手動建立並配置以下政策和工作：

   - Kaspersky Endpoint Security政策
   - 更新 Kaspersky Endpoint Security 的群組工作
   - 網路代理政策

   操作說明：設定更新 Kaspersky Endpoint Security 的群組工作。

   如果必要，建立附加工作以管理安裝在用戶端裝置上的 Kaspersky 應用程式。

3. **評估和限制資料庫上的事件負載**

   受管應用程式操作相關的事件資訊將被從用戶端電腦上傳輸並記錄至管理伺服器資料庫。要降低管理伺服器負載，評估和限制可以儲存在資料庫的最大事件數量。

   操作說明：設定事件最大數量。

結果

當您完成該情境時，您將透過配置 Kaspersky 應用程式、工作和管理伺服器接收的事件來防護您的網路：

- Kaspersky 應用程式會根據政策與政策設定檔設定。
- 應用程式會透過一組工作管理。
- 儲存在資料庫的事件數量上限已設定。

當網路防護配置完成時，您可以繼續配置 Kaspersky 資料庫和應用程式的一般更新。

關於以裝置為中心和以使用者為中心的安全管理方法

您可以從裝置功能的立場和從使用者角色的立場管理安全設定。第一種方法叫做*以裝置為中心的安全管理*，第二種叫做*以使用者為中心的安全管理*。要應用不同的應用程式設定到不同的裝置，您可以使用兩種方法的任意一種或其組合。

裝置特定安全性管理可讓您根據裝置特定的功能，套用不同的安全應用程式設定至受管理裝置。例如，您可套用不同設定至分配在不同管理群組中的裝置。

以使用者為中心的安全性管理可讓您套用不同安全應用程式設定至不同的使用者角色。您可建立一些使用者角色，將適當的使用者角色指派給每位使用者，並將不同的應用程式設定定義至不同角色使用者擁有的裝置。例如，您可能要應用不同的應用程式設定到會計和人力資源 (HR) 人員的裝置。結果，當實現了以使用者為中心的安全管理時，每個部門—財務部門和人事部門—具有自己的 Kaspersky 應用程式設定配置。設定配置定義了哪些應用程式設定可以被使用者變更以及哪些被強制設定並被管理員鎖定。

透過使用以使用者為中心的安全管理，您可以應用特定的應用程式設定到單個使用者。這可能用在員工在公司有獨一角色或您要監控與個別人的裝置相關的安全問題時。取決於該員工在公司的角色，您可以延伸或限制該員工變更應用程式設定的權限。例如，您可能要延伸在本機辦公室管理用戶端裝置的系統管理員的權限。

您也可以組合以裝置為中心的安全管理和以使用者為中心的安全管理方法。例如，您可以為每個管理群組設定特別的應用程式政策，然後為一個或幾個使用者角色建立政策設定檔。在此情況下，政策和政策設定檔會按照以下優先順序加以套用：

1. 為以裝置為中心的安全管理建立的政策被應用。
2. 政策設定檔會根據政策設定檔優先順序內容加以修改。
3. 政策被與使用者角色關聯的政策設定檔修改。

政策設定和傳播：以裝置為中心的方法

當您完成該方案後，應用程式將在所有受管理裝置上被設定，與您定義的應用程式政策和政策設定檔一致。

先決條件

在開始之前，請確保您已經安裝了管理伺服器和 OSMP 主控台。您也可能要考慮以使用者為中心的安全管理作為以用於以裝置為中心的方法的附加選項。瞭解更多兩個管理方法的詳情。

階段

以裝置為中心的 Kaspersky 應用程式管理情境包含以下步驟：

1 管理應用程式政策

透過為每個應用程式建立政策來配置安裝在受管理裝置上的 Kaspersky 應用程式設定。政策集將被傳播到用戶端裝置。

如果您有幾個管理伺服器和/或管理群組的層級結構，次要管理伺服器和子管理伺服器預設從主要管理伺服器繼承政策。您可以強制子群組和從屬管理伺服器的繼承以防止上流政策設定的修改。如果您僅要一部分設定被強制繼承，您可以在上游政策中鎖定它們。剩餘未鎖定的設定將可以在下流政策中修改。建立的政策層級將允許您有效管理管理群組中的裝置。

說明：建立一個政策

2 **建立政策設定檔（可選）**

如果您想讓單一管理群組中的裝置在不同政策設定下執行，為這些裝置建立政策設定檔。政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在受管理裝置上活動。

透過使用設定檔啟動條件您可以套用不同的政策設定檔（例如）具有特別硬體設定或被特別標籤標記的裝置。使用標籤篩選滿足特別標準的裝置。例如，您可以建立叫做 *CentOS* 的標籤，使用該標籤標記所有執行 CentOS 作業系統的裝置，然後指定該標籤作為政策設定檔啟動條件。結果，安裝在所有執行 CentOS 裝置上的卡巴斯基應用程式將被使用它們自己的政策設定檔管理。

說明：

- 建立政策設定檔
- 建立政策設定檔啟動規則

3 **傳播政策和政策設定檔到受管理裝置**

預設情況下，管理伺服器每 15 分鐘自動與受管理裝置同步一次。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。您可以避免自動同步並透過使用強制同步指令手動執行同步。一旦同步完成，政策和政策設定檔被傳送和應用到安裝的 Kaspersky 應用程式。

您可以檢查政策和政策設定檔是否被傳送到了裝置。Open Single Management Platform在裝置屬性中指定傳送日期和時間。

說明：強制同步

結果

當以裝置為中心的情境完成時，Kaspersky 應用程式根據指定的設定被設定並透過政策層級傳播。

設定的應用程式政策和政策設定檔將被自動應用到新增到管理群組的新裝置。

政策設定和傳播：以使用者為中心的方法

該部分敘述了以使用者為中心的集中配置安裝到受管理裝置上的 Kaspersky 應用程式的方案。當您完成該方案後，應用程式將在所有受管理裝置上被設定，與您定義的應用程式政策和政策設定檔一致。

先決條件

在開始之前，請確保您已成功安裝管理服務器和 OSMP 主控台，並完成主要部署方案。您也可能要考慮以裝置為中心的安全管理作為以用於為中心的方案的附加選項。瞭解更多兩個管理方法的詳情。

過程

以使用者為中心的 Kaspersky 應用程式管理方案包含以下步驟：

1. **管理應用程式政策**

   透過為每個應用程式建立政策來配置安裝在受管理裝置上的 Kaspersky 應用程式設定。政策集將被傳播到用戶端裝置。

   如果您有幾個管理伺服器和/或管理群組的層級結構，次要管理伺服器和子管理伺服器預設從主要管理伺服器繼承政策。您可以強制子群組和從屬管理伺服器的繼承以防止上流政策設定的修改。如果您僅要一部分設定被強制繼承，您可以在上游政策中鎖定它們。剩餘未鎖定的設定將可以在下流政策中修改。建立的政策層級將允許您有效管理管理群組中的裝置。

   說明：建立一個政策

2. **指定裝置所有者**

   分配受管理裝置到對應使用者。

   說明：指派使用者作為裝置所有者

3. **為您的企業定義使用者角色**

   聯想您企業的員工所做的不同工作。您必須根據他們的角色劃分所有員工。例如，您可以按照部門、專業或職位劃分他們。然後您將需要為每個群組建立使用者角色。記住，每個使用者角色將擁有其自己的政策設定檔，包含該角色特有的應用程式設定。

4. **建立使用者角色**

   為每個員工群組建立和配置使用者角色或使用預定義使用者角色。使用者角色將包含到應用程式功能的存取權限群組。

   說明：建立一個使用者角色

5. **定義每個使用者角色範圍**

   對於每個建立的使用者角色，定義使用者和/或安全群組以及管理群組。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

   說明：編輯使用者角色範圍

6. **建立政策設定檔**

   為您企業中的每個使用者角色建立政策設定檔。政策設定檔決定了哪些設定將被根據使用者角色套用到使用者裝置上的應用程式。

   說明：建立一個政策設定檔

7. **關聯政策設定檔與使用者角色**

   關聯建立的政策設定檔與使用者角色。此後：政策設定檔對具有特定角色的使用者活動。政策設定檔中配置的設定將被套用到安裝於使用者裝置上的 Kaspersky 應用程式。

   說明：關聯政策設定檔到角色

8. **傳播政策和政策設定檔到受管理裝置**

   預設情況下，Open Single Management Platform會每15分鐘自動將管理伺服器與受管理裝置同步。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。您可以避免自動同步並透過使用強制同步指令手動執行同步。一旦同步完成，政策和政策設定檔被傳送和應用到安裝的 Kaspersky 應用程式。

您可以檢查政策和政策設定檔是否被傳送到了裝置。Open Single Management Platform在裝置屬性中指定傳送日期和時間。

說明：強制同步

結果

當以使用者為中心的方案完成時，Kaspersky 應用程式根據指定的設定被配置並透過政策和政策設定檔層級傳播。

對於新使用者，您將必須建立新帳戶，分配一個建立的使用者角色，並分配裝置到使用者。配置的應用程式政策和政策設定檔將被自動套用到該使用者的新裝置。

關於將網路代理切換到其他管理伺服器

如果網路的下列設定已變更，Kaspersky Next XDR Expert 可讓您將用戶端裝置上的網路代理切換到其他管理伺服器：

- **DHCP 伺服器位址條件** — 網路 Dynamic Host Configuration Protocol (DHCP) 伺服器的 IP 位址已變更。

  DHCP 伺服器位址條件設定目前無法使用。

- **預設連線閘道位址條件** — 主要網路閘道的位址已變更。
- **DNS 網域條件** — 子網路的 DNS 後置詞已變更。
- **DNS 伺服器位址條件** — 網路 DNS 伺服器的 IP 位址已變更。
- **WINS 伺服器位址條件** — 網路 WINS 伺服器的 IP 位址已變更。此設定僅適用於執行 Windows 的裝置。
- **名稱可解析性條件** — 用戶端裝置的 DNS 或 NetBIOS 名稱已變更。
- **子網路條件** — 可變更子網路位址和遮罩。
- **Windows 網域可存取性條件** — 可變更用戶端裝置連線到的 Windows 網域的狀態。此設定僅適用於執行 Windows 的裝置。
- **SSL 連線位址可存取性條件** — 用戶端裝置可以或無法（取決於您選取的選項）與指定伺服器（名稱：連接埠）建立SSL連線。您必須使用專用伺服器，並且軟體能夠處理高負載和頻繁的網路代理請求。請勿指定管理伺服器的連接埠。對於每個伺服器，您還可以指定 SSL 憑證。在這種情況下，除了檢查 SSL 連線的功能之外，網路代理還會驗證伺服器憑證。如果憑證不相符，則連線會失敗。

網路代理連線至管理伺服器的初始設定在安裝網路代理時定義。此後，如果建立了將網路代理轉換至其他管理伺服器的規則，網路代理將以下列方式回應網路設定的變更：

- 如果網路設定符合已建立的規則之一，網路代理將連線至該規則中指定的管理伺服器。如果該規則中已經啟用漫遊轉換政策，用戶端裝置上的應用程式將轉換至漫遊政策。
- 如果未套用任何規則，網路代理將回溯至安裝過程中指定的管理伺服器連線預設設定。用戶端裝置上安裝的應用程式將回溯至活動政策。
- 如果無法存取管理伺服器，網路代理將使用使用者漫遊政策。

網路代理只會在網路代理政策設定中的**當管理伺服器不可用時啟用漫遊模式**選項啟用時才會切換至漫遊政策。

網路代理連線至管理伺服器的設定儲存在連線設定檔中。在連線設定檔中，您可以建立將用戶端裝置轉換至漫遊政策的規則，並可對設定檔進行設定，使其僅可用於下載更新。

為漫遊使用者建立連線設定檔

若要為漫遊使用者建立網路代理連線至管理伺服器的連線設定檔，請執行以下操作：

1. 如果要為一組受管理裝置建立連線設定檔，請開啟該群組的網路代理政策。為此，請執行以下操作：
   a. 在主功能表中，轉至 **資產管理 → 政策**。
   b. 選擇要為其建立連線設定檔的管理群組：
      - 對於根群組，您可以繼續下一步。
      - 對於子群組，請按一下頁面頂部的**顯示階層**按鈕，然後在開啟的視窗中按一下所需子群組的名稱。

      所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。
   c. 為受管理裝置群組新增網路代理政策。如果您已經建立它，請點擊網路代理政策名稱以開啟政策內容。
2. 如果要為特定受管理裝置建立連線設定檔，請執行以下操作：
   a. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
   b. 點擊受管理裝置的名稱。
   c. 在開啟的受管理裝置內容視窗中，轉至**應用程式**頁簽。
   d. 點擊僅適用於選定受管理裝置的網路代理政策的名稱。
3. 在開啟的內容視窗中，轉到**應用程式設定→連線→連線設定檔。**
4. 在**管理伺服器連線設定檔**區域中，點擊**新增**按鈕。

   預設下，連線設定檔清單包含<離線模式>和<歸屬管理伺服器>設定檔。您不能編輯或刪除設定檔。

<離線模式>設定檔不指定任何伺服器以連線。因此，網路代理，當切換到該設定檔時，當用戶端裝置上的應用程式工作在漫遊政策下時不試圖連線到任何管理伺服器。如果裝置與網路斷開連線，可以使用<離線模式>設定檔。

<歸屬管理伺服器>設定檔指定在網路代理安裝過程中管理伺服器的連線。當裝置在外部網路中執行了一段時間後重新連線到管理伺服器時，<歸屬管理伺服器>設定檔被套用。

5. 在開啟的**設定設定檔**視窗中，配置連線設定檔：

- **設定檔名稱**

  在該輸入欄位中，您可以檢視或變更連線設定檔名稱。

- **管理伺服器位址**

  用戶端裝置在設定檔啟動期間必須連線的管理伺服器位址。

- **連接埠號**

  用於連線的埠號。

- **SSL 連接埠**

  使用 SSL 協定時的埠號。

- **使用 SSL 連線**

  如果啟用此選項，則使用 SSL 協定透過安全埠建立連線。

  預設情況下已啟用該選項。我們建議您不要停用此選項，以便您的連線保持安全。

- 如果您要在連線到網際網路時使用代理伺服器，選取**使用代理伺服器**選項。如果選取此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

  - **位址**

    Kaspersky Next XDR Expert 連線至網際網路時所使用的代理伺服器位址。

  - **連接埠號**

    Kaspersky Next XDR Expert 代理連線將透過其建立的連接埠號碼。

  - **代理伺服器身分驗證**

    如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

  - **使用者名稱**

    用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

  - **密碼**

    其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

    若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

- **連線閘道位址**

  透過用戶端裝置連線至管理伺服器的閘道位址。

- **當管理伺服器不可用時啟用漫遊模式**

  選取該核取方塊允許用戶端裝置上安裝的應用程式在在不可使用管理伺服器進行的任何離線嘗試時，以漫遊模式使用政策設定檔和漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

  如果停用此選項，則應用程式將使用已啟動的政策。

  預設情況下，此核取方塊已清除。

- **僅用來接收更新**

  如果啟用此選項，則該設定檔將僅被用戶端裝置上安裝的應用程式用來下載更新。對於其他操作，程式將使用在網路代理安裝過程中定義的初始連線設定連線管理伺服器。

  預設情況下已啟用該選項。

- **在此設定檔中同步連線設定和管理伺服器設定**

  如果停用此選項，網路代理將使用設定檔屬性中指定的設定連線至管理伺服器。

  如果停用此選項，網路代理將使用安裝期間已指定的原始設定連線至管理伺服器。

  如果停用**僅用來接收更新**選項，則此選項可用。

  預設情況下已停用該選項。

程式將為漫遊使用者建立一個用於將網路代理連線至管理伺服器的設定檔。當使用此設定檔將網路代理連線至管理伺服器後，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策，或漫遊政策。

政策和政策設定檔

在OSMP控制台中，您可以為卡巴斯基應用程式創建政策。該部分描述了政策和政策設定檔，並提供建立和修改它們的說明。

關於政策和政策設定檔

*政策*是一組應用於管理群組及其子群組的卡巴斯基應用程式設定。您可以在管理群組的裝置上安裝多個 Kaspersky 應用程式。Kaspersky Next XDR Expert 為管理群組中的每個 Kaspersky 應用程式提供單一政策。政策會有下列其中一種狀態：

政策狀態

州	敘述
活動	套用至裝置的目前政策。每個管理群組中的 Kaspersky 應用程式只能啟用一個政策。裝置將為卡巴斯基應用程式套用活動政策的設定值。
不啟用	目前未將政策套用至裝置。
漫遊	如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

政策會根據以下規則執行：

- 您可以為單個應用程式配置擁有不同值的多個政策。
- 對於目前應用程式只有一個政策可以處於啟用狀態。
- 政策可以有子政策。

通常，您可以將政策作為緊急情況 (例如病毒攻擊) 的準備。例如，如果有透過快閃記憶體磁碟機的攻擊，則可以啟動阻止存取快閃記憶體磁碟機的政策。在這種情況下，目前的啟用政策將自動變為非啟用狀態。

為了防止維護多個政策，例如，當不同場合僅假設變更多個設定時，您可以使用政策設定檔。

*政策設定檔*是政策設定值的已命名子集，用於替換政策的設定值。政策設定檔會影響受管理裝置上有效的設定形式。*有效設定*是目前應用於裝置的一組政策設定，政策設定檔設定和本機應用程式設定。

政策設定檔會根據以下規則執行：

- 當特定的啟動條件發生時，政策設定檔會生效。
- 政策設定檔包含與政策設定不同的設定值。
- 政策設定檔的啟動會變更受管理裝置的有效設定。
- 政策可以包含最多 100 個設定檔。

關於鎖定和已鎖定的設定

每個政策設定都有一個鎖定按鈕圖示 ( )。下表顯示鎖定按鈕的狀態：

鎖定按鈕狀態

州	描述
Undefined	如果設定旁邊顯示開啟鎖，並且停用了切換按鈕，則該設定未在政策中指定。使用者可以在受管理應用程式介面中變更這些設定。這些類型的設定稱為*解鎖*。
Enforce	如果設定旁邊顯示關閉的鎖頭，並且啟用了切換按鈕，則該設定將套用於強制執行政策的裝置。使用者無法在受管理應用程式介面中修改這些設定的值。這些類型的設定稱為*鎖定*。

我們強烈建議您關閉要在受管理裝置上套用的政策設定的鎖定。解鎖的政策設定可以由卡巴斯基應用程式設定在受管理裝置上重新分配。

您可以使用鎖定按鈕執行以下操作：

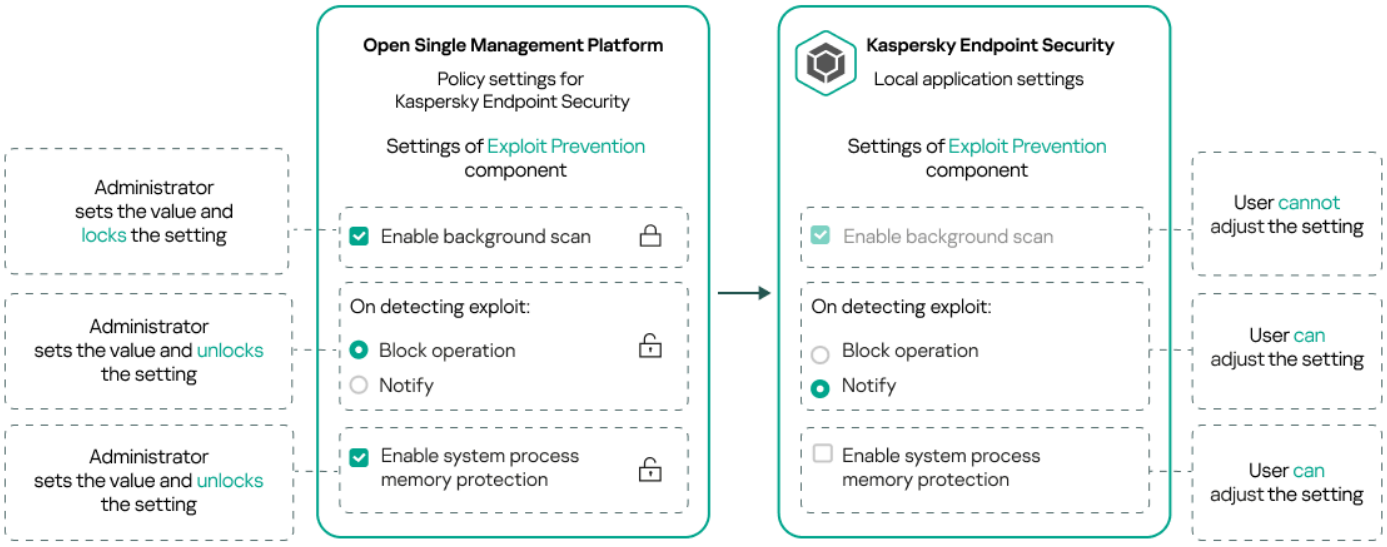
- 鎖定管理子群組政策的設定
- 在受管理裝置上鎖定卡巴斯基應用程式的設定

因此，鎖定設定可用於在受管理裝置上實作有效的設定。

有效設定的實作程序包括以下操作：

- 受管理裝置會套用卡巴斯基應用程式的設定值。
- 受管理裝置會套用政策的鎖定設定值。

政策和受管理卡巴斯基應用程式包含相同的設定集。配置政策設定時，卡巴斯基應用程式設定會變更受管理裝置上的值。您無法調整受管理裝置上的鎖定設定（請參閱下圖）：



鎖定和卡巴斯基應用程式設定

政策繼承和政策設定檔

本節提供政策和政策設定檔的階層和繼承資訊。

政策層級

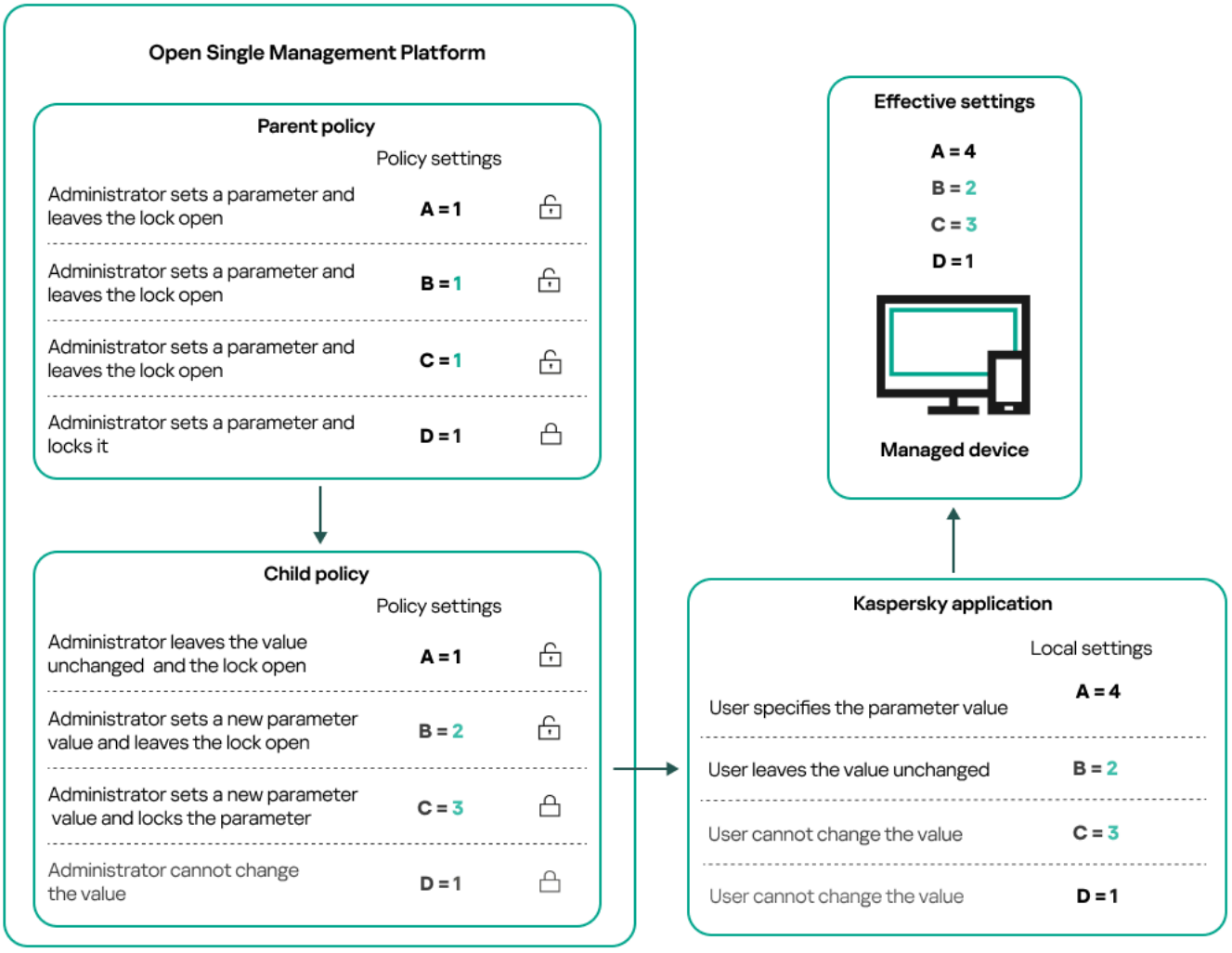
如果不同的裝置需要不同的設定，則可以將裝置組織到管理群組中。

您可以為單一管理群組指定政策。政策設定可以*繼承*。繼承代表從上級（父）管理群組的政策接收子群組（子群組）中的政策設定值。

因此，父群組政策也叫*父政策*。子群組的政策也叫*子政策*。

預設情況下，管理伺服器上至少存在受管理裝置群組。如果要建立自訂組，它們將作為受管理裝置群組內的子群組（子群組）建立。

根據管理群組的層次結構，相同應用程式的政策會互相作用。上級（父）管理群組政策的鎖定設定將重新分配子群組的政策設定值（請參閱下圖）。

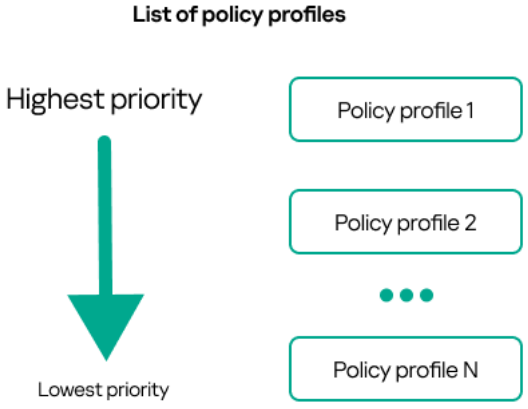


政策層級

政策層次結構中的政策設定檔

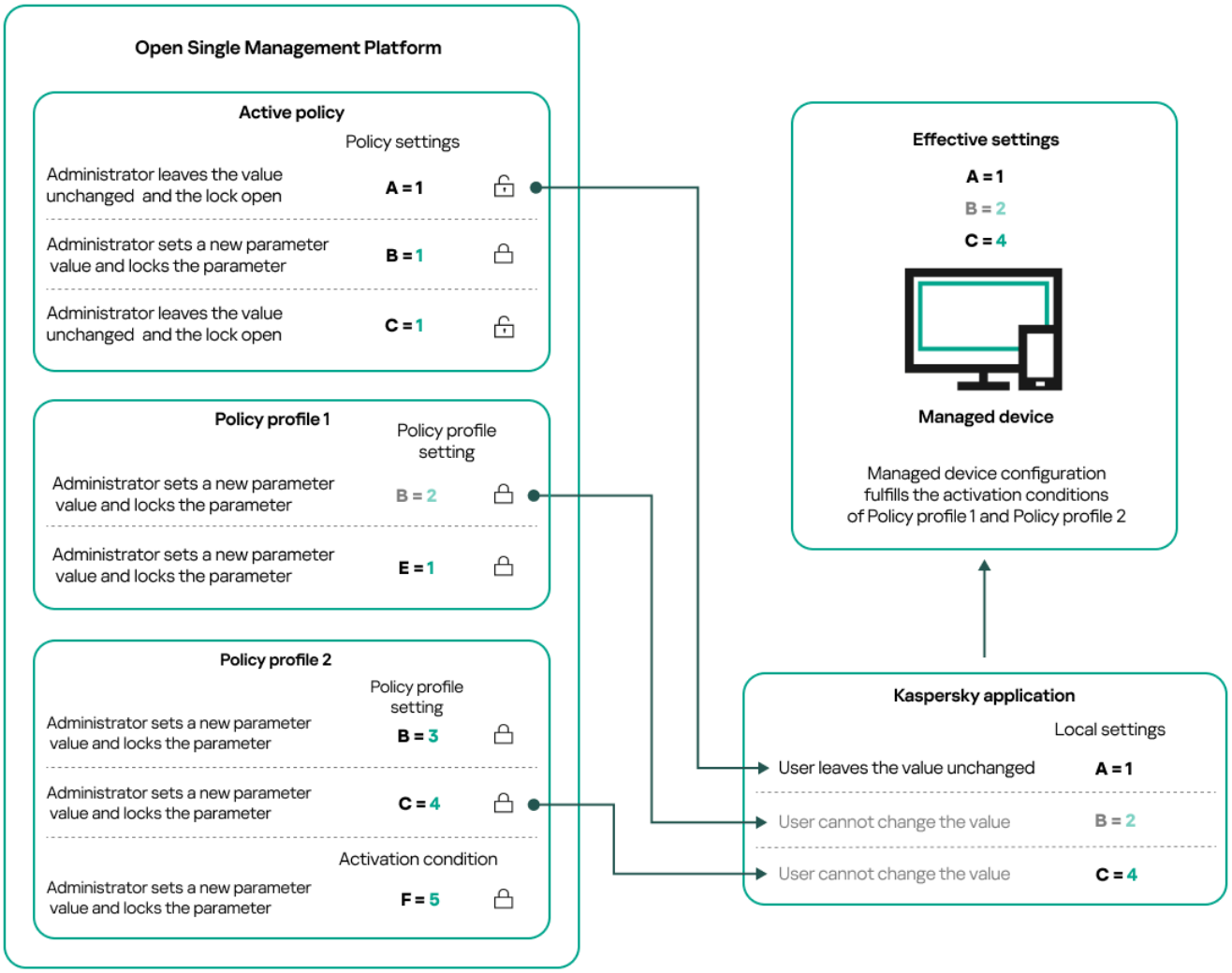
政策設定檔具有以下優先等級分配條件：

- 設定檔在政策設定檔清單中的位置指示其優先等級。您可變更政策設定檔的優先順序。清單中的最高位置表示最高優先等級（請參閱下圖）。



政策設定檔的優先等級定義

- 政策設定檔的啟動條件互不依賴。您可以同時啟動多個政策設定檔。如果多個政策設定檔影響相同設定，則裝置將從政策設定檔中取得具有最高優先等級的設定值（請參閱下圖）。

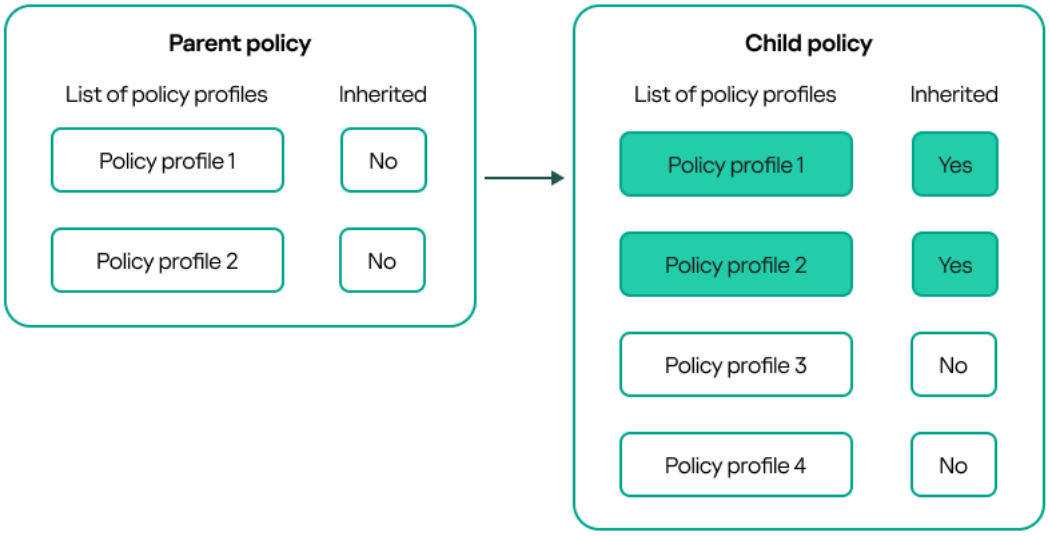


受管理裝置配置滿足幾個政策設定檔的啟動條件

繼承層次結構中的政策設定檔

來自不同層次結構層級政策的政策設定檔符合以下條件：

- 較低層級的政策從較高層級的政策繼承政策設定檔。從較高級政策繼承的政策設定檔比原始政策設定檔的層級具有更高的優先等級（請參閱下圖）。
- 您不能變更繼承之政策設定檔的優先等級（請參見下圖）。

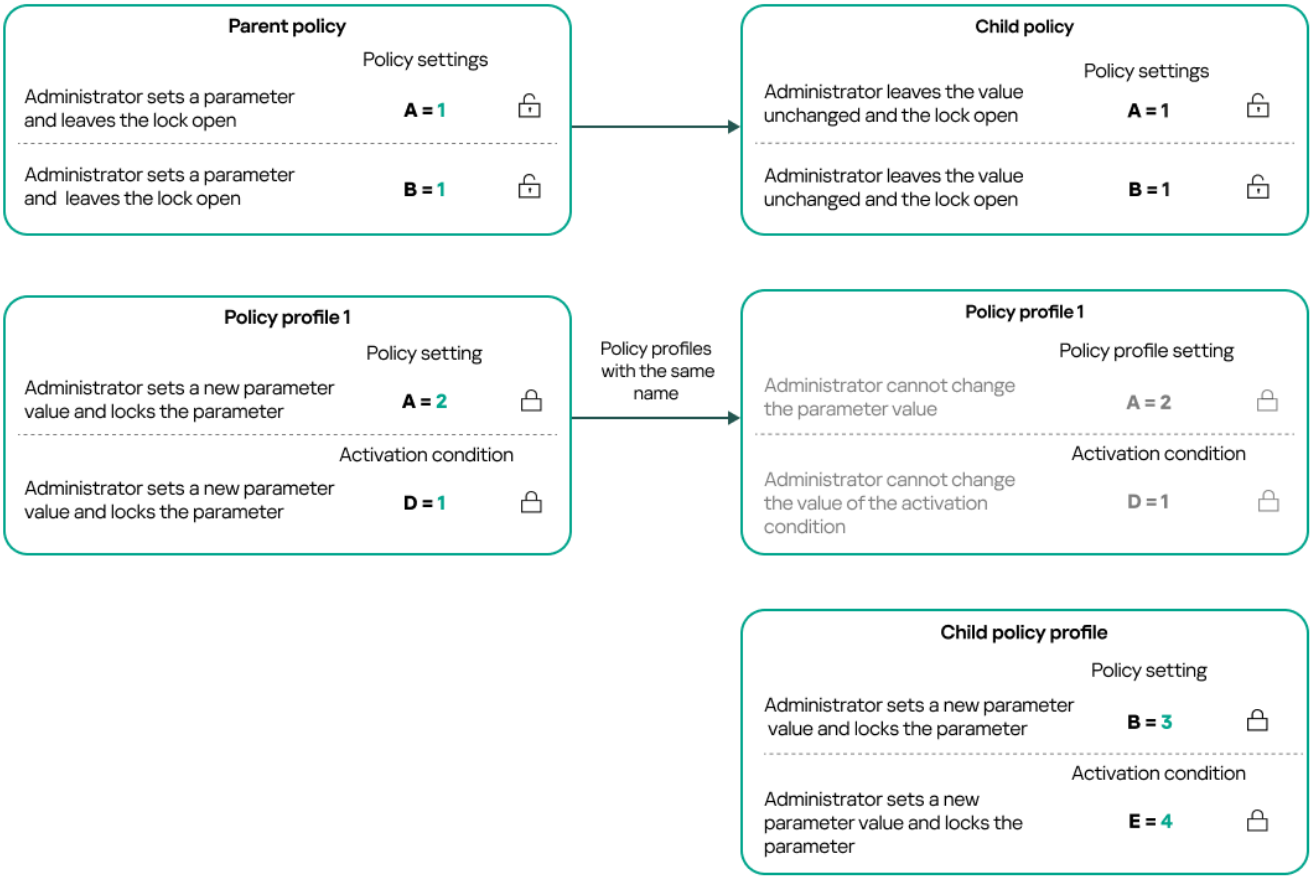


政策設定檔繼承

具有相同名稱的政策設定檔

如果在不同的層次結構層級中有兩個名稱相同的政策，則這些政策將根據以下規則執行：

- 上級政策設定檔的鎖定設定和設定檔啟動條件會變更下級政策設定檔的設定和設定檔啟動條件（請參閱下圖）。



子設定檔從父政策設定檔繼承設定值

- 上級政策設定檔的解鎖設定和設定檔啟動條件不會變更下級政策設定檔的設定和設定檔啟動條件。

如何在受管理裝置上實作設定

以下提供在受管理裝置上實作有效設定的說明：

- 所有未被鎖定的設定值都取自於政策。
- 然後，這將被受管理應用程式設定的值覆寫。
- 接著，將套用有效政策中被鎖定的設定值。鎖定的設定值會變更未鎖定的有效設定值。

管理政策

本節說明管理政策，並提供檢視政策清單、建立政策、修改政策、複製政策、移動政策、強制同步、檢視政策分發狀態圖，以及刪除政策的資訊。

檢視政策清單

您可以檢視為管理伺服器或任何管理群組建立的政策清單。

要檢視政策清單，請執行以下操作：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 在管理群組結構中，選擇您要檢視其政策清單的管理群組。

政策清單以表格格式出現。如果沒有政策，表格為空。您可以顯示或隱藏表格的列，變更它們的順序，僅檢視包含指定值的行，或者使用尋找。

建立新政策

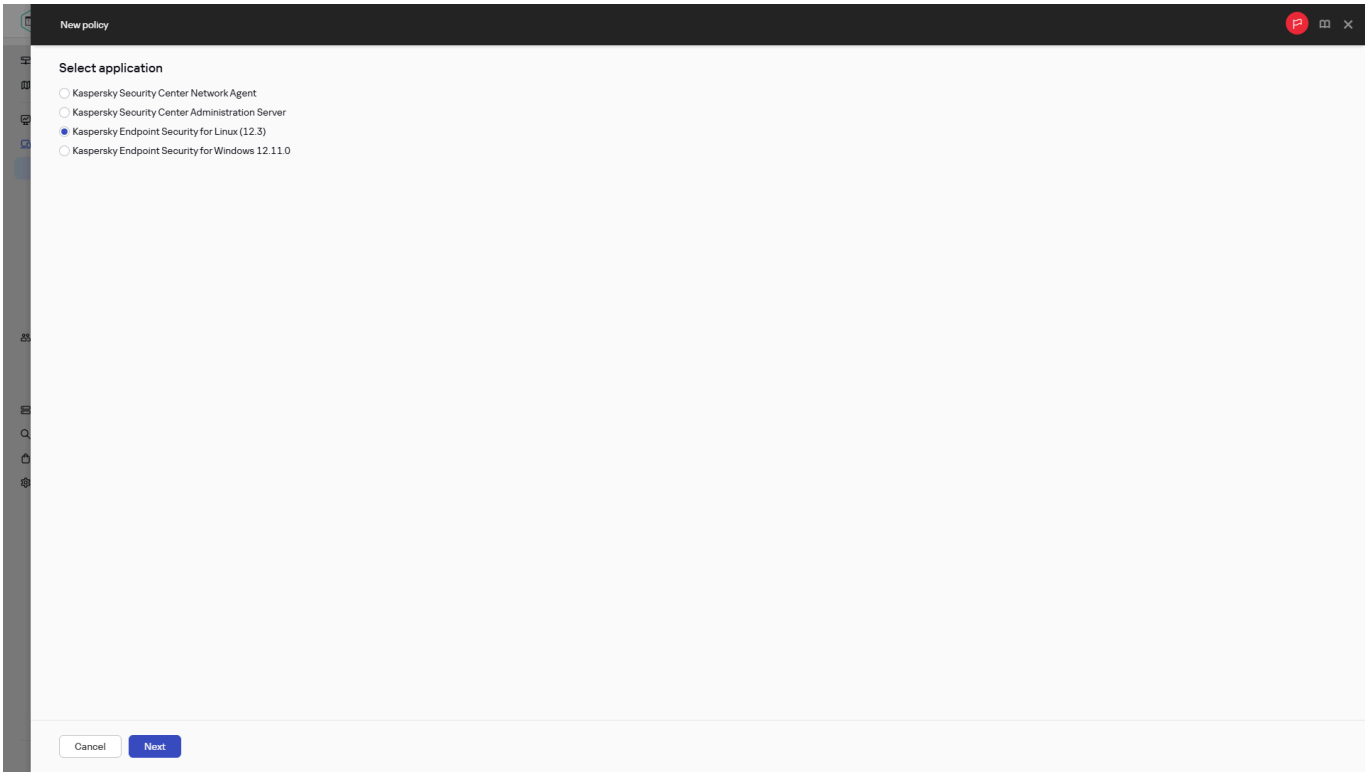
您可以建立政策；您也可以修改和刪除現有政策。

要建立政策：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 選擇要為其建立政策的管理群組：
   - 對於根群組。
     在這種情況下，您可以繼續執行下一步。
   - 對於子群組：
     a. 點擊頁面頂部的**顯示階層**按鈕。
     b. 按鈕名稱將變更為**隱藏階層**。
     c. 在開啟的視窗中，按一下所需子群組的名稱。

   所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。
3. 點擊**新增**。

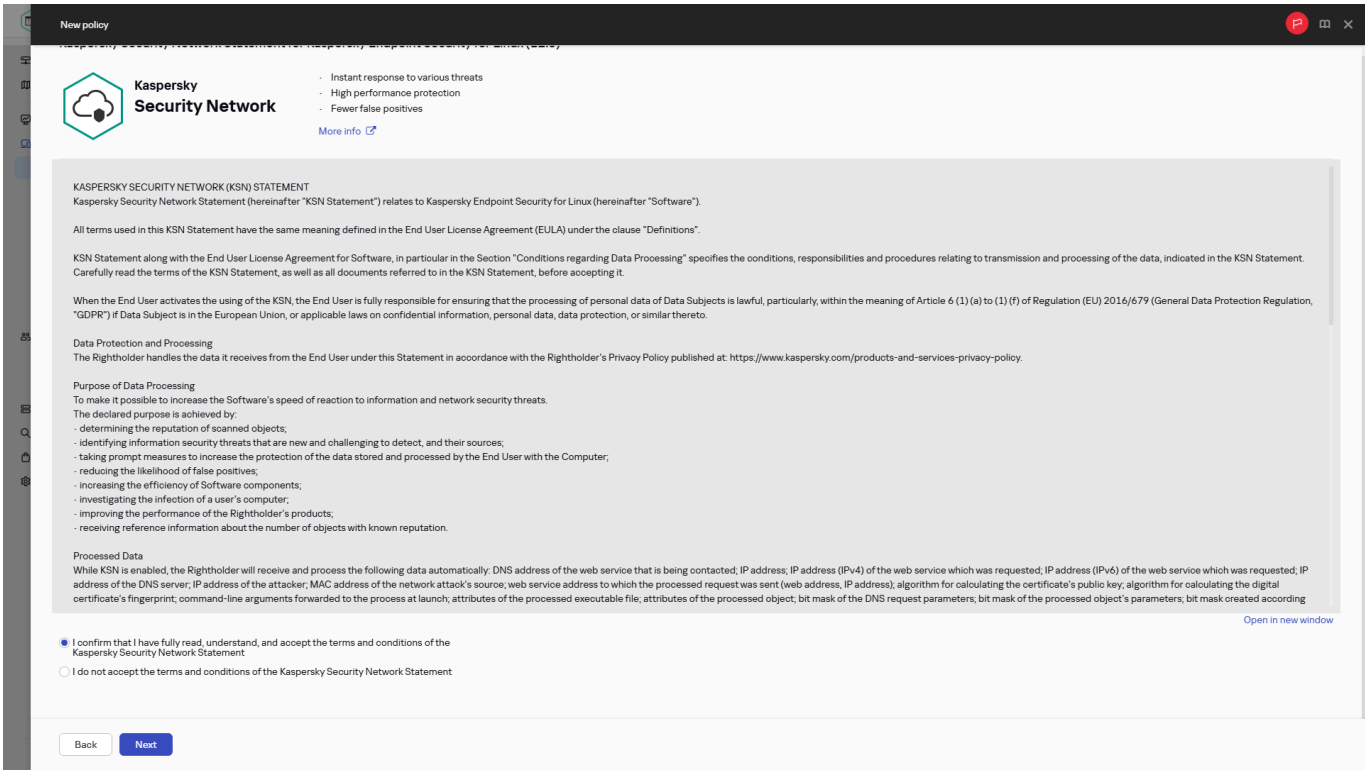
選取應用程式視窗將開啟。



建立新政策

4. 選取您要建立政策的應用程式。

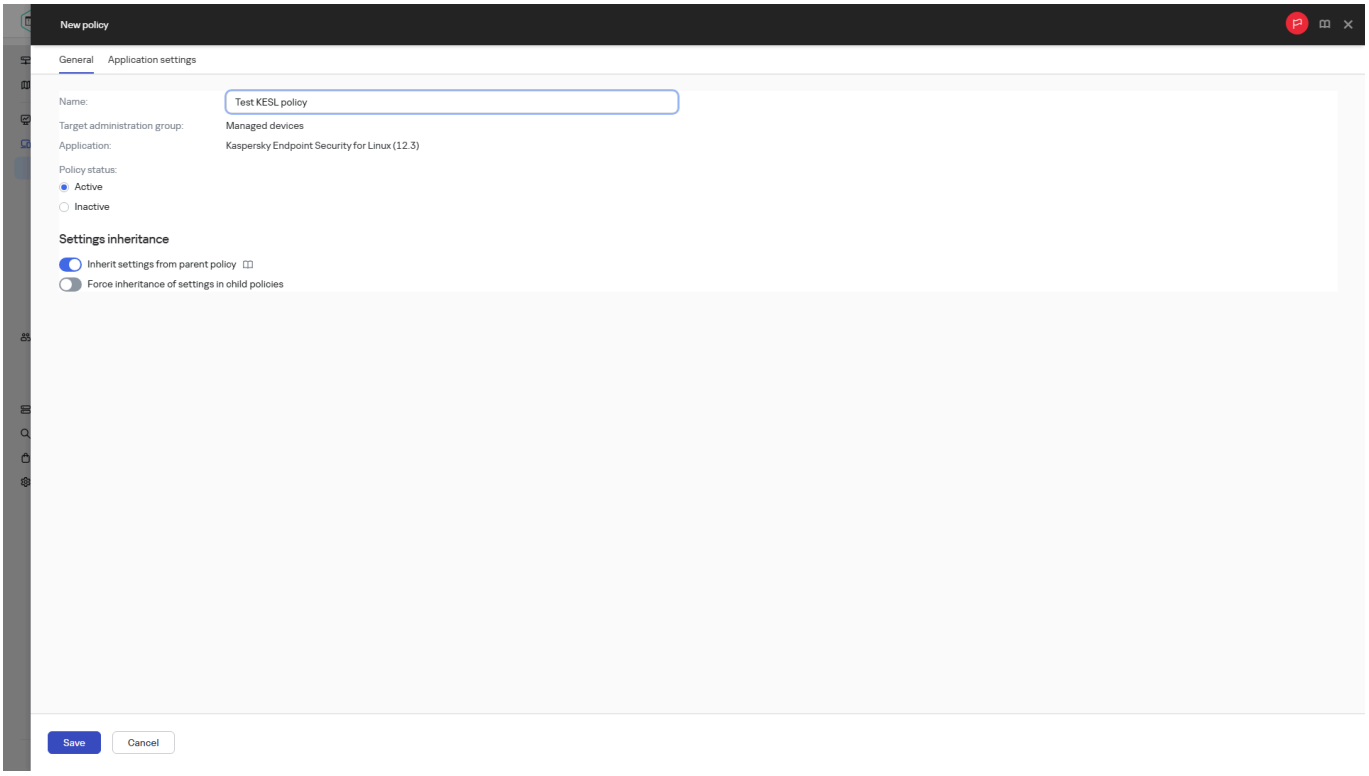
5. 如果您正在為其建立政策的卡巴斯基應用程式支援卡巴斯基安全網路，系統將提示您接受 KSN 聲明。如果您想使用卡巴斯基安全網路，請接受 KSN 聲明。



接受 KSN 聲明

6. 點擊**"下一步"**。

新政策設定視窗會開啟，並含有所選的**一般**頁籤。如果您需要，變更政策的預設名稱、預設狀態和預設繼承設定。



新政策設定視窗

7. 選取 **應用程式設定**頁籤。

   或者，您可點擊**儲存**並結束。政策將出現在政策清單，且您可以稍後編輯其設定。

8. 在**應用程式設定**頁籤的左窗格中選取您需要的類別，在優方的結果窗格中編輯政策的設定。您可以在每個類別中（區域）編輯政策設定。

   設定集會以您建立政策的應用程式為依據。如需詳細資訊，請參閱以下內容：

   - 設定管理伺服器
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Linux 說明
   - Kaspersky Endpoint Security for Windows 說明

   如需設定其他安全應用程式設定的詳細資訊，請參閱對應應用程至的文件。

   編輯設定時，您可點擊**取消**來取消最後的操作。

9. 點擊**儲存**儲存政策。

   系統會顯示包含以下訊息的通知：**正在儲存政策並透過管理伺服器階層分發**。

   如果政策通過驗證，則會顯示以下通知：**政策已儲存**。

   如果政策驗證失敗，則會顯示以下通知：**無法儲存政策 並透過管理伺服器階層分發。請聯絡技術支援**。您可以檢閱並修訂政策設定，然後再試一次。如果問題持續存在，請聯絡技術支援。

該政策將顯示在政策清單中。政策建立後，如果已啟用此選項，政策變更事件會匯出至 SIEM 系統。

一般政策設定

一般

在**一般**區域，您可以修改政策狀態並指定政策設定的繼承：

- 在**政策狀態**區塊中，您可以選取一種政策模式：
  - **作用中**

    如果選取該選項，政策將變為啟用狀態。

    預設情況下已選定此選項。
  - **漫遊**

    如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。
  - **非作用中**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。
- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。

    預設情況下已啟用該選項。
  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。

    預設情況下已停用該選項。

事件組態

事件組態區域可讓您配置事件記錄和事件通知。事件根據嚴重等級用下面的標籤分佈：

- **緊急**

  緊急頁籤不會顯示在網路代理政策內容中。
- **功能失效**
- **警告**
- **資訊**

在每個區域，清單顯示在管理伺服器上事件類型和預設事件儲存的週期（天）。點擊事件類型允許您指定以下設定：

- **事件註冊**

  您可以指定儲存事件的天數和選取儲存事件的位置：

  - **使用 Syslog 匯出到 SIEM 系統**
  - **儲存在裝置上的作業系統事件記錄中**
  - **儲存在管理伺服器上的作業系統事件記錄中**

- **事件通知**

  您可以選取您是否想由以下方法之一被通知事件：

  - **透過電子郵件通知**
  - **透過 SMS 通知**
  - **透過執行可執行檔或指令碼來進行通知**
  - **透過 SNMP 通知**

  預設下，使用在管理伺服器內容標籤中指定的通知設定（例如收件者位址）。如有需要，您可在**電子郵件**、**SMS**與**要執行的可執行檔**頁籤變更這些設定。

此外，當新增新的事件類型（例如，在新版本的應用程式中）時，**事件組態**頁簽會顯示通知，並允許您透過點擊**儲存**或**儲存並關閉**按鈕來套用新設定。

變更歷史

變更歷史頁籤允許您檢視政策修訂版本的清單，比較政策修訂版本，並在必要時恢復對政策所做的變更。

修改政策

要修改政策：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 點擊您要修改的政策。

   政策設定視窗隨即開啟。
3. 指定通用設定和為其建立政策的應用程式的設定。如需詳細資訊，請參閱以下內容：

   - 設定管理伺服器
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Windows 文件

   如需設定其他安全應用程式設定的詳細資訊，請參閱對應應用程式的文件。
4. 點擊**儲存**按鈕。

系統會顯示包含以下訊息的通知：**正在儲存政策並透過管理伺服器階層分發**。

如果政策通過驗證，則會顯示以下通知：**政策已儲存**。

如果政策驗證失敗，則會顯示以下通知：**無法儲存政策 並透過管理伺服器階層分發。請聯絡技術支援**。您可以檢閱並修訂政策設定，然後再試一次。如果問題持續存在，請聯絡技術支援。

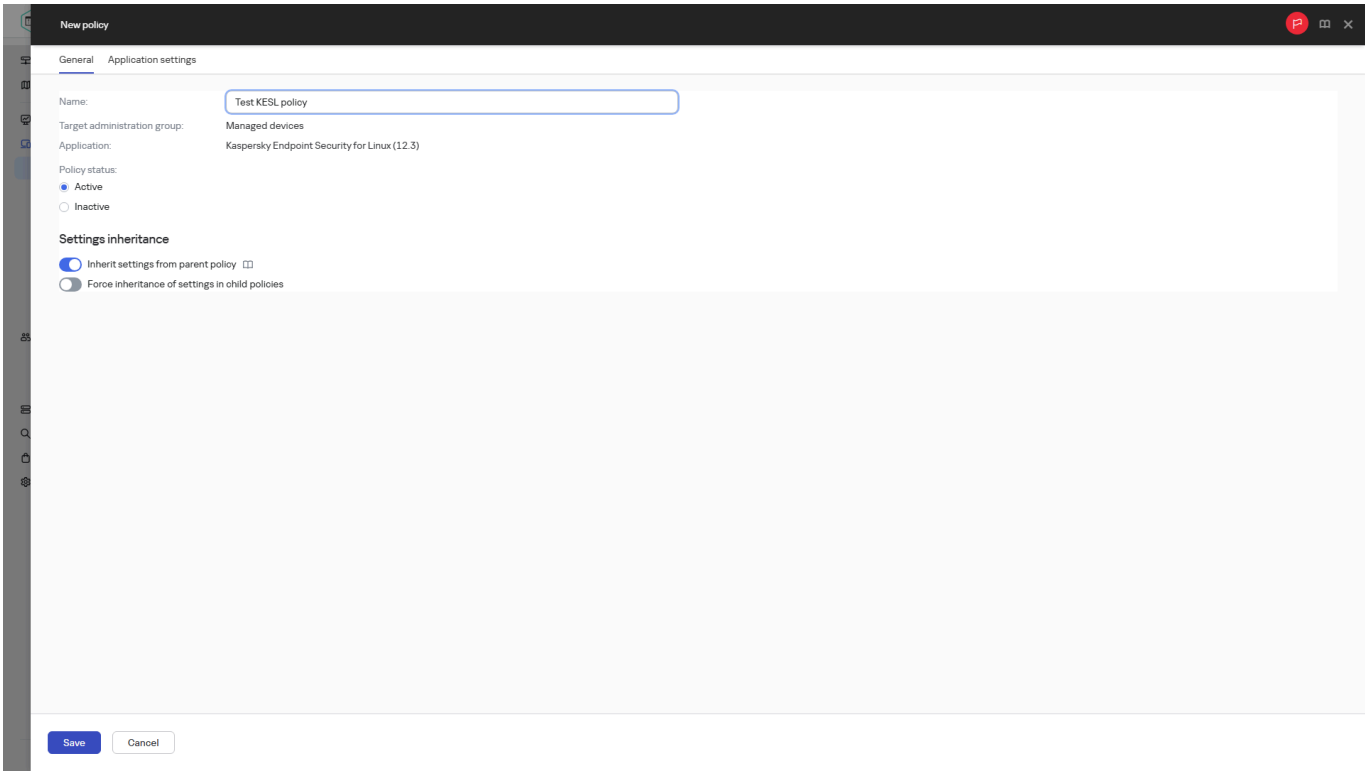
對政策所做的變更將儲存在政策內容中，並且會顯示在**變更歷史**區段。修改政策後，如果已啟用此選項，政策變更事件會匯出至 SIEM 系統。

如有必要，您可以比較政策修訂版本。此選項適用於管理伺服器、網路代理程式、Kaspersky Endpoint Security for Windows（從14.0網頁外掛程式版本開始）和Kaspersky Endpoint Security for Mac（從12.2.1 Patch A網頁外掛程式版本開始）的政策。

啟用和停用政策繼承選項

若要啟用或停用政策中的繼承選項：

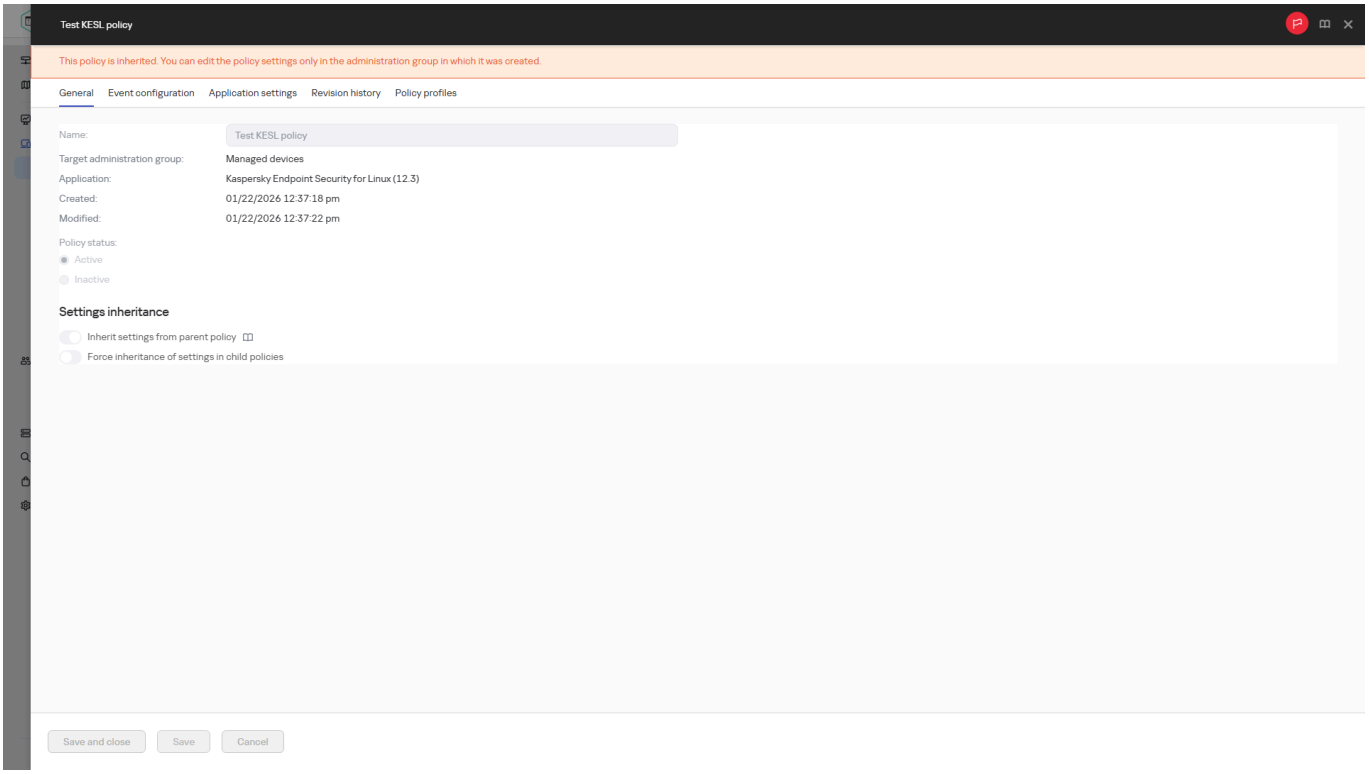
1. 開啟所需的政策。
2. 開啟**一般**標籤。



建立新政策

3. 啟用或停用政策繼承：

   - 如果您對子群組啟用**從父政策繼承設定**，並在父政策中鎖定一些設定，那麼您無法在子政策中變更這些設定。
   - 如果您對子政策停用**從父政策繼承設定**，那麼您可以變更子政策中的所有設定，即便一些設定在父政策中是鎖定的。
   - 如果您在父群組啟用**在子政策中強制繼承設定**，這將為每個子政策啟用**從父政策繼承設定**。此種情況下，您無法為任何子政策停用該選項。所有在父政策中被鎖定的設定被強制繼承到子群組，且您無法在子群組中變更這些設定。



鎖定的政策設定

4. 點擊**儲存**按鈕儲存變更，或點擊**取消**按鈕拒絕變更。

依預設，政策會啟用**從父政策繼承設定**選項。

如果政策有設定檔，所有子政策都會繼承這些設定檔。

複製政策

您可以從一個管理群組複製政策到另一個。

要複製政策到其他管理群組：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 選取您要複製的政策旁邊的核取方塊。
3. 點擊**複製**。

   在螢幕的右側，管理群組樹狀目錄被顯示。

4. 在樹狀目錄中，選取目的群組，意即您要複製政策到該群組。

5. 點擊畫面底部的**複製**按鈕。

6. 點擊**確定**以確認操作。

政策將連帶其所有設定檔被複製到目的群組。目標群組中各個複製的政策將會**非作用中**。您可隨時變更狀態至**作用中**。

如果目的群組中已包含名稱與新移動政策的名稱一致的政策，那麼會在新移動政策的名稱後附加一個（<下一個序號>）的索引，例如：（1）。

移動政策

您可以從一個管理群組移動政策到另一個。例如，您要刪除一個群組，但您要為其他群組使用其政策。在此情況下，您可能要先將政策從舊群組移動至新群組，再刪除舊群組。

將政策移至另一個管理群組時，政策的修訂歷程記錄將被清除。「**變更歷史**」頁籤僅顯示有關最新變更的資訊。

要移動政策到其他管理群組：

1. 在主功能表中，轉至 **資產管理** → **政策**。

2. 選取您要移動的政策旁邊的核取方塊。

3. 點擊**移動**按鈕。

   在螢幕的右側，管理群組樹狀目錄被顯示。

4. 在樹狀目錄中，選取目的群組，例如，您要將政策移動到該群組。

5. 點擊畫面底部的**移動**按鈕。

6. 點擊**確定**以確認操作。

   如果政策不是從資源群組繼承的，它連帶所有設定檔被移動到目的群組。目標群組中的政策狀態是**非作用中**。您可隨時變更狀態至**作用中**。

   如果政策繼承自資源群組，它將保持在資源群組中。它連帶所有其設定檔被複製到目的群組。目標群組中的政策狀態是**非作用中**。您可隨時變更狀態至**作用中**。

如果目的群組中已包含名稱與新移動政策的名稱一致的政策，那麼會在新移動政策的名稱後附加一個（<下一個序號>）的索引，例如：（1）。

匯出政策

Open Single Management Platform允許您將政策及其設定和政策設定檔儲存到KLP檔案。您可以使用此 KLP 檔案匯入儲存的政策到卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux。

要匯出政策，請執行以下操作：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 選取您要匯出之政策旁邊的核取方塊。

   您不能同時匯出多個政策。如果您選擇了多個政策，**匯出**按鈕將被停用。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存新檔**視窗中，指定政策檔案的名稱和路徑。按一下**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，政策檔案會自動儲存在**下載**資料夾。

匯入政策

Open Single Management Platform允許您從KLP檔案匯入政策。KLP 檔案包含匯出的政策及其設定和政策設定檔。

要匯入政策，請執行以下操作：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 點擊**匯入**按鈕。
3. 點擊**瀏覽**按鈕選擇要匯入的政策檔案。
4. 在開啟的視窗中，指定 KLP 政策檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個政策檔案。

   政策處理開始。
5. 政策處理完畢後，選擇要將政策套用到哪些管理群組。
6. 點擊**完成**按鈕以完成政策匯入。

此時會顯示匯入結果通知。如果政策匯入成功，您可以按一下**詳細資訊**連結以檢視政策內容。

匯入成功後，政策會顯示在政策清單中。政策的設定和設定檔也會一併匯入。無論匯出期間選取的政策狀態如何，匯入的政策都處於非使用中狀態。您可以在政策內容中變更政策狀態。

如果新匯入政策的名稱與現有政策的名稱相同，則匯入政策的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

強制同步

雖然 Kaspersky Next XDR Expert 會自動同步受管理裝置的狀態、設定、工作和政策，但在某些情況下，管理員必須確切得知在特定時間是否已針對指定裝置執行同步。

同步單一裝置

要強制同步管理伺服器和受管理裝置：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
2. 點擊要與管理伺服器同步的裝置名稱。
   政策內容視窗會開啟，並含有所選的**一般**區段。
3. 點擊**強制同步**按鈕。

應用程式將所選裝置與管理伺服器同步。

同步多部裝置

強制同步管理伺服器和受管理裝置：

1. 開啟管理群組的裝置清單或裝置分類：
   - 執行裝置分類以檢視裝置清單。
   - 在主功能表中，前往**資產管理 → 資產（裝置）**，然後選取要同步的裝置所在的管理群組：
     - 對於根群組，您可以繼續下一步。
     - 對於子群組，請按一下頁面頂部的**顯示階層**按鈕，然後在開啟的視窗中按一下子群組的名稱。
       所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。
2. 選取您要與管理伺服器同步之裝置旁的核取方塊。
3. 在受管理裝置清單上方，按一下省略符號按鈕（...），然後按一下**強制同步**按鈕。
   應用程式將所選裝置與管理伺服器同步。
4. 在裝置清單中，檢視上次連線管理伺服器的時間已針對選取的裝置變更為目前時間。若時間未變更，請點擊**重新整理**按鈕更新頁面內容。

所選裝置會與管理伺服器同步。

檢視政策交付的時間

在管理伺服器上變更 Kaspersky 應用程式政策後，管理員可以檢查是否被變更的政策被傳輸到了特定受管理裝置。政策可以在定期同步或者強制同步中傳輸。

若要檢視應用程式政策交付至受管理裝置的日期與時間：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
2. 點擊要與管理伺服器同步的裝置名稱。
   政策內容視窗會開啟，並含有所選的**一般**區段。
3. 點擊**應用程式**標籤。

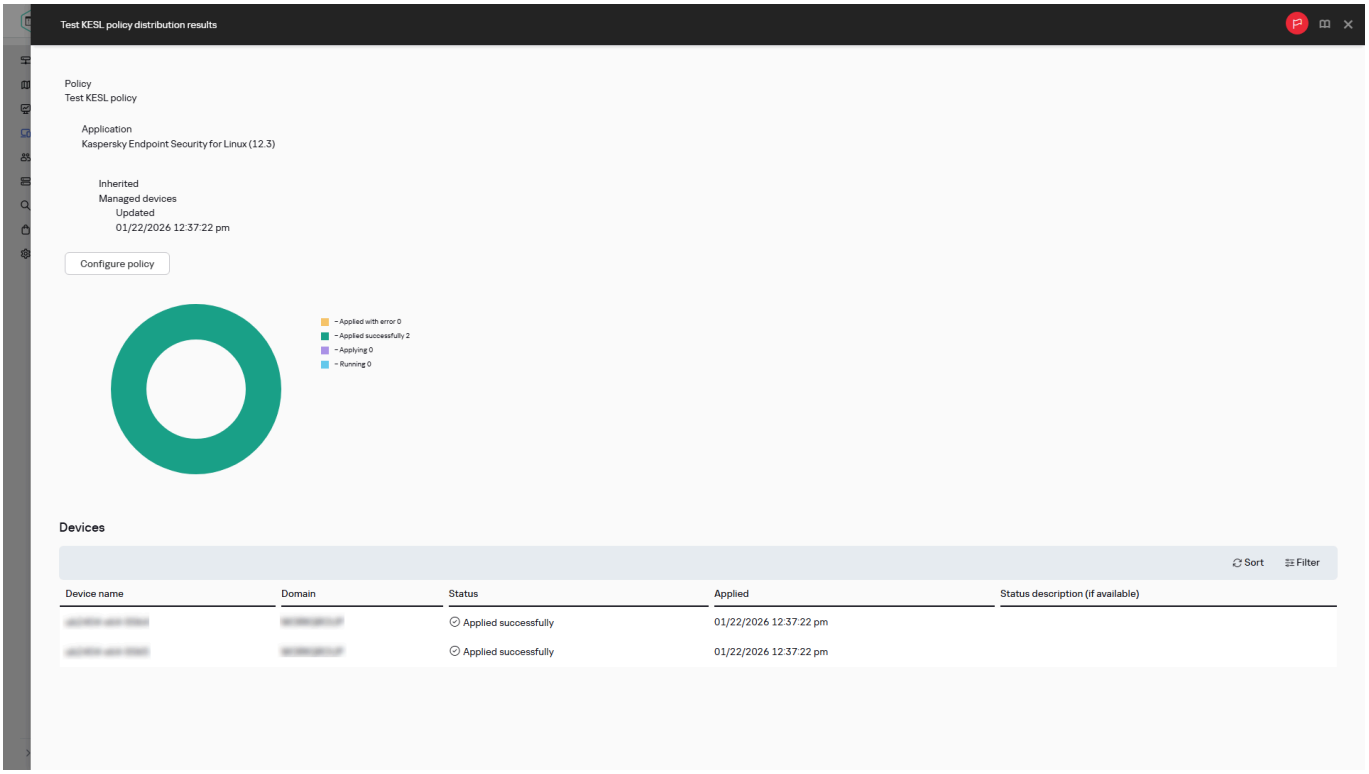
4. 選取您要檢視政策同步日期的應用程式。
   應用程式政策視窗會開啟，並含有所選的**一般**區段，並且顯示政策交付日期與時間。

檢視政策發佈狀態圖表

在Open Single Management Platform中，您可以在政策分發狀態圖中查看每個裝置上政策應用程式的狀態。

要檢視每個裝置上的政策發佈狀態：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 選取要在裝置上檢視分配狀態之政策名稱旁的核取方塊。
3. 在出現的選單中，選取**分發**連結。
   <政策名稱>分發結果視窗隨即開啟。



政策分發狀態圖

4. 在開啟的**<政策名稱>分發結果**視窗中，顯示政策的**狀態描述**。

您可以使用政策分發變更清單中顯示的結果數量。裝置最高數量是 100,000。

若要使用政策發佈結果變更清單中顯示的裝置數量：

1. 在主功能表中，轉至**設定 → 介面選項**。
2. 在**政策分發結果中顯示的裝置限制**中，輸入裝置數量（最多 100,000）。
   預設情況下，數量為 5000。
3. 點擊**儲存**按鈕。
   設定已儲存並套用。

在出現病毒爆發事件時自動啟用政策

要使政策在出現病毒爆發事件時自動啟用，請執行以下操作：

1. 在主功能表中，按一下管理伺服器名稱。

   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 選擇**病毒爆發**區段。

3. 在右側面板中，點擊**設定在病毒爆發事件發生時要啟動的政策**連結。

   啟動政策視窗將開啟。

4. 在與偵測到病毒爆發的該元件相關區段中—適用於工作站與檔案伺服器的防毒軟體、適用於郵件伺服器的防毒軟體，或適用於週邊防護的防毒軟體—選取您要輸入項旁的選項按鈕，之後點擊**新增**。

   內含**受管理裝置**管理群組的視窗隨即開啟。

5. 點擊**受管理裝置**旁的 V 型圖示（ ）。

   管理群組層級和它們的政策被顯示。

6. 在管理群組層級和它們的政策中，點擊政策名稱或偵測到病毒爆發時啟動的政策的名稱。

   要在清單或群組中選擇所有政策，選擇所需名稱旁邊的核取方塊。

7. 點擊**儲存**按鈕。

   管理群組層級和它們的政策的視窗被關閉。

所選的政策被新增到偵測到病毒爆發時啟動的政策清單。所選政策在病毒爆發中被啟動，無論它們是活動的還是非活動的。

如果政策在病毒爆發事件中啟動，您僅可以使用手動模式返回到先前政策。

刪除政策

如果您不再需要一個政策，您可以刪除它。您僅可以刪除一個在指定管理群組中繼承的政策。如果一個政策是繼承的，您僅可以在其被建立的上級群組刪除它。

要刪除政策，請執行以下操作：

1. 在主功能表中，轉至 **資產管理 → 政策**。

2. 選取您要刪除之政策旁的核取方塊並點擊**刪除**。

   若您選取繼承的政策，則**刪除**按鈕會變成無法使用（暗顯）。

3. 點擊**確定**以確認操作。

政策連帶其所有設定檔被刪除。政策刪除後，如果此選項已啟用，政策變更事件會匯出至 SIEM 系統。

管理政策設定檔

本節說明如何管理政策設定檔，並提供有關檢視政策設定檔、變更政策設定檔優先順序、建立政策設定檔、複製政策設定檔、建立政策設定檔啟用規則、刪除以及匯出和匯入政策設定檔的資訊。

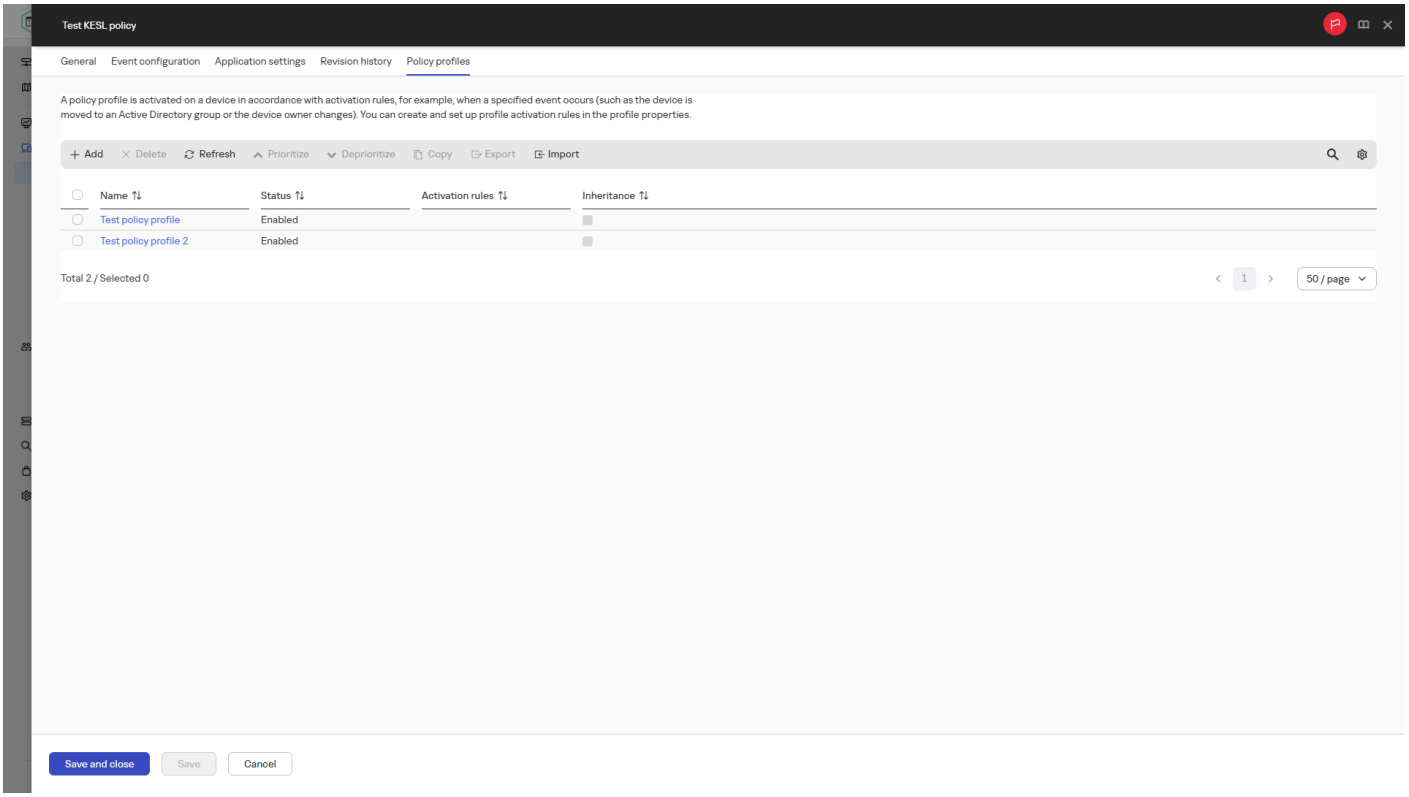
檢視政策設定檔

要檢視政策設定檔：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 點擊您要檢視其設定檔的政策名稱。

   政策內容視窗會開啟，並含有所選的**一般**頁籤。
3. 開啟**政策設定檔**頁籤。

政策設定檔清單以表格格式出現。如果政策沒有設定檔，將顯示空表。



政策設定檔清單

變更政策設定檔優先順序

要變更政策設定檔優先順序：

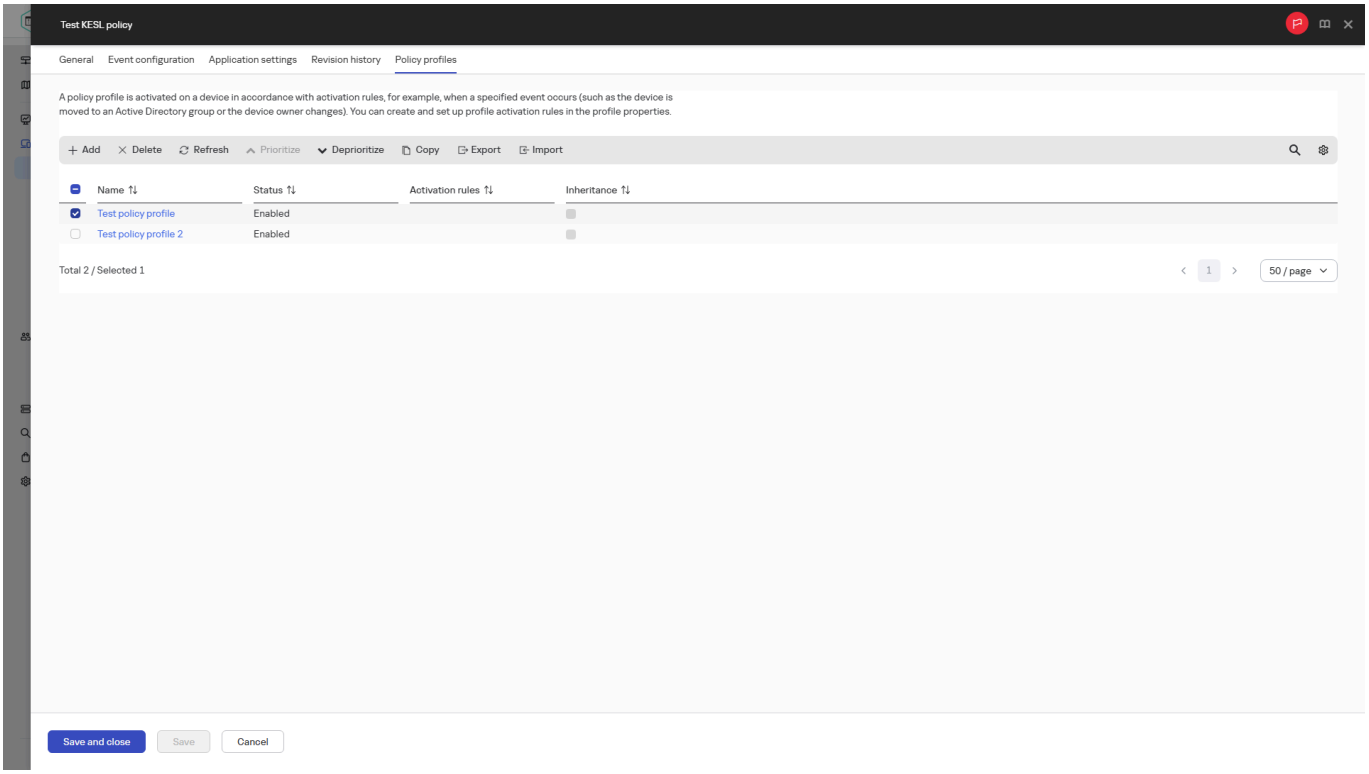
1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。

2. 在**政策設定檔**頁籤，選取您要變更優先權之政策設定檔旁的核取方塊。

3. 透過點擊**提高優先順序**或**降低優先順序**，在清單中設定政策設定檔的新位置。

   政策設定檔在清單中的位置越高，其優先順序越高。



4. 點擊**儲存**按鈕。

   所選政策設定檔的優先順序被變更並套用。

建立政策設定檔

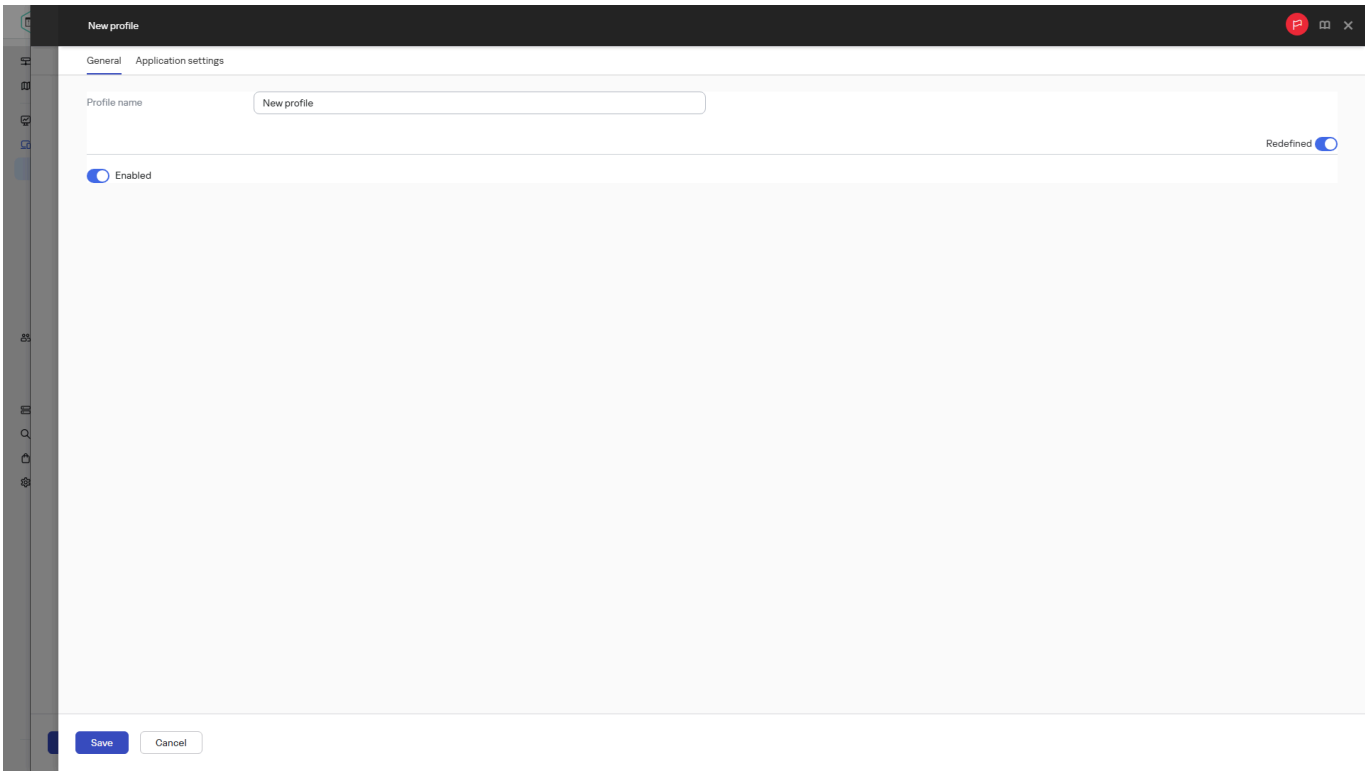
要建立政策設定檔：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。如果政策沒有設定檔，將顯示空表。

2. 點擊**新增**。

3. 如果您需要，變更設定檔的預設名稱和預設繼承設定。



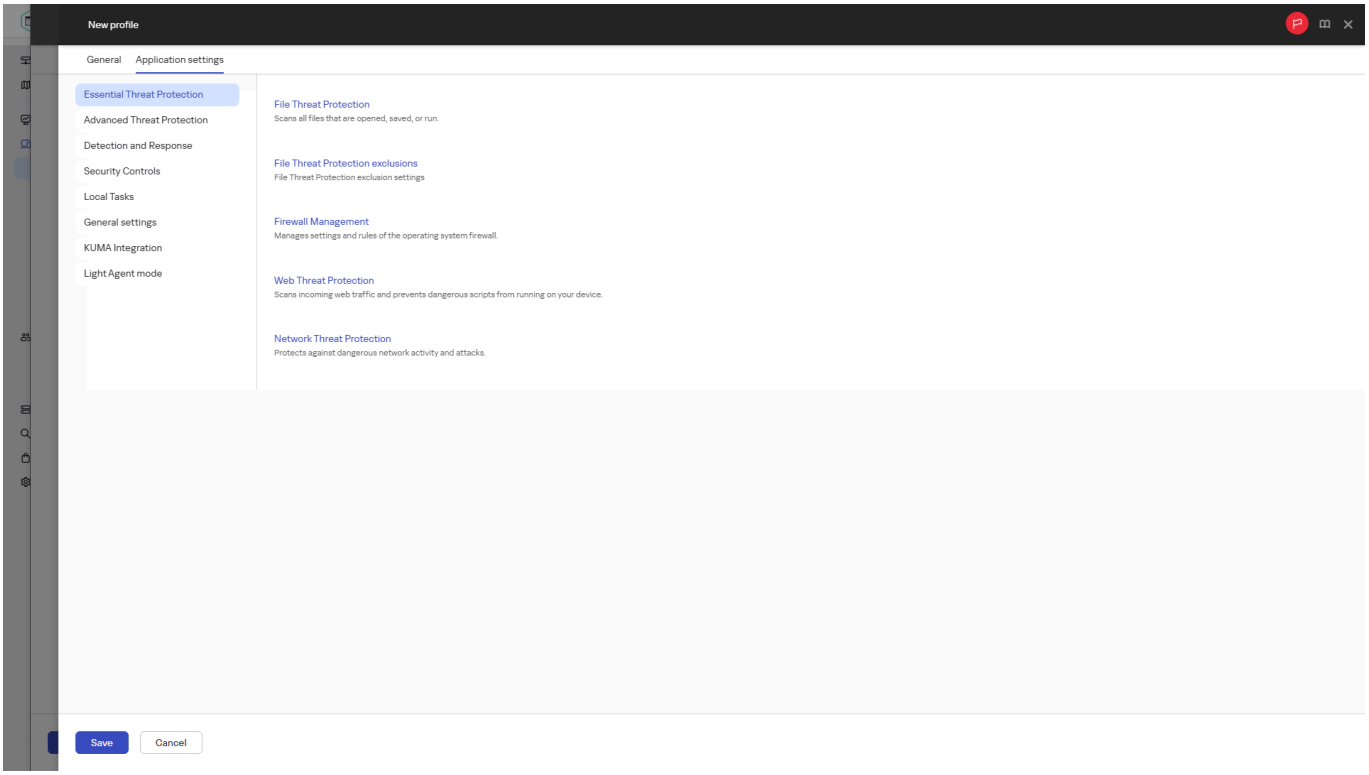
建立政策設定檔

4. 選取 **應用程式設定**頁籤。

   或者，您可點擊 **儲存**並結束。您建立的設定檔將出現在政策設定檔清單，且您可以稍後編輯其設定。

5. 在**應用程式設定**頁籤的左窗格與右邊的結果窗格中選取您要的類別，接著編輯設定檔的設定。您可以在每個類別中（區域）編輯政策設定檔設定。

   編輯設定時，您可點擊**取消**來取消最後的操作。



指定政策設定檔設定

6. 點擊**儲存**以儲存設定檔。

該設定檔顯示在政策設定檔清單中。

複製政策設定檔

您可以複製政策設定檔到目前政策或其他政策，例如，如果您要對不同政策擁有相同設定檔。您也可以使用複製，如果您想擁有兩個或更多僅在少數設定不同的設定檔。

要複製政策設定檔：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。如果政策沒有設定檔，將顯示空表。

2. 在**政策設定檔**頁籤，選取您要複製的政策設定檔。

3. 點擊**複製**。

4. 在開啟的視窗中，選取您要複製設定檔的政策。

   您可以複製政策設定檔到相同政策或您指定的政策。

5. 點擊**複製**。

   政策設定檔被複製到您選取的政策。新複製的設定檔具有最低優先順序。如果您複製設定檔到相同政策，新複製的設定檔名稱將附加（ ）索引，例如：（1）、（2）。

您稍後可以變更政策設定檔的設定，包括其名稱和優先順序。在此情況下，原始政策設定檔不會變更。

建立政策設定檔啟動規則

要建立政策設定檔啟動規則：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。

2. 在**政策設定檔**頁籤，點擊您需在其中建立啟動規則的政策設定檔。

   如果政策設定檔清單為空，您可以建立政策設定檔。

3. 在**啟動規則**標籤上，點擊**新增**按鈕。

   政策設定檔啟動規則視窗開啟。

4. 指定規則的名稱。

5. 選取影響您目前建立的政策設定檔的啟動的條件的核取方塊：

   - **政策設定檔啟動一般規則**

     選取該核取方塊依據裝置行動模式狀態設定裝置上的政策設定檔啟動規則、連線管理伺服器規則和分配給裝置的標記。

對於該選項，指定在下一步：

- **裝置狀態**

  定義裝置出現在網路的條件：

  - **線上**—裝置位在網路中，因此可使用管理伺服器。
  - **離線**—裝置位在網路外，因此無法使用管理伺服器。
  - **N/A**—將不套用標準。

- **裝置網路位置**

  選取政策設定檔啟動條件（規則是否被執行）並選取規則名稱。

  規則定義裝置網路位置以便連線到管理伺服器，它的條件必須被滿足（或不滿足）以便啟動政策設定檔。

  用於連線到管理伺服器的裝置網路位置敘述可以在網路代理轉換規則中被建立或設定。

- **特定裝置所有者規則**

  對於該選項，指定在下一步：

  - **裝置所有者**

    啟用此選項依據裝置所有者在其上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 裝置屬於指定的擁有者（“=”符號）。
    - 裝置不屬於指定的擁有者（“#”符號）。

      如果啟用該選項，設定檔根據配置的標準在裝置上啟動。啟用此選項時，您可以指定裝置所有者。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **裝置所有者在內部安全群組中**

    啟用此選項可設定並啟用規則，根據裝置所有者是否為 Kaspersky Next XDR Expert 內部安全群組的成員，在裝置上啟動設定檔。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 裝置所有者是指定安全群組的成員（“=”符號）。
    - 裝置所有者不是指定安全群組的成員（“#”符號）。

      如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定 Kaspersky Next XDR Expert 的安全群組。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **硬體規格規則**

  選取該核取方塊依據記憶體和邏輯處理器數量設定裝置上的政策設定檔啟動規則。

對於該選項，指定在下一步：

- **RAM 大小 (MB)**

  啟用此選項透過裝置上可用 RAM 容量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

  - 該裝置記憶體大小小於指定值（"<" 符號）。
  - 該裝置記憶體大小大於指定值（">" 符號）。

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的 RAM 容量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **邏輯處理器數量**

  啟用此選項透過裝置上邏輯處理器數量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

  - 裝置上邏輯處理器數量少於或等於指定值（“<”符號）。
  - 裝置上邏輯處理器數量大於或等於指定值（“>”符號）。

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的邏輯處理器數量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **角色指派規則**

  對於該選項，指定在下一步：

  - **由裝置所有者特定角色啟動政策設定檔**

    選取該選項以在裝置上根據所有者角色配置和啟用設定檔啟動規則。從現有角色清單手動新增角色。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。

- **標籤使用規則**

  選取該核取方塊根據分配到裝置的標籤設定裝置上的政策設定檔啟動規則。您可以在有選取標籤或沒有選取標籤的裝置啟動政策設定檔。

  對於該選項，指定在下一步：

  - **標籤清單**

    在標籤清單中，透過選中與相應標籤對應的方塊，可以指定政策設定檔中的裝置包含規則。

    您可以透過清單上方的欄位新增新標籤到清單，並點擊**新增**按鈕。

    政策設定檔包含具有選定標籤的裝置。如果清除方塊，則將不套用該標準。預設情況下已清除這些方塊。

  - **套用到沒有指定標籤的裝置**

    如果您必須轉換您的標籤選項則啟用此選項。

    如果啟用此選項，政策設定檔將包含未帶有所選標籤的敘述的裝置。如果停用該選項，則不套用標準。

    預設情況下已停用該選項。

- **Active Directory 使用規則**

  選取該核取方塊依據裝置在 Active Directory 組織單元中的出現或者裝置在 Active Directory 安全性群組中的成員關係設定裝置上的政策設定檔啟動規則。

對於該選項，指定在下一步：

- **裝置所有者在 Active Directory 安全群組中的身分**

  如果啟用此選項，當裝置屬於指定的安全群組或指定安全群組的子群組時，裝置上的政策設定檔被啟動。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **裝置列入 Active Directory 安全群組**

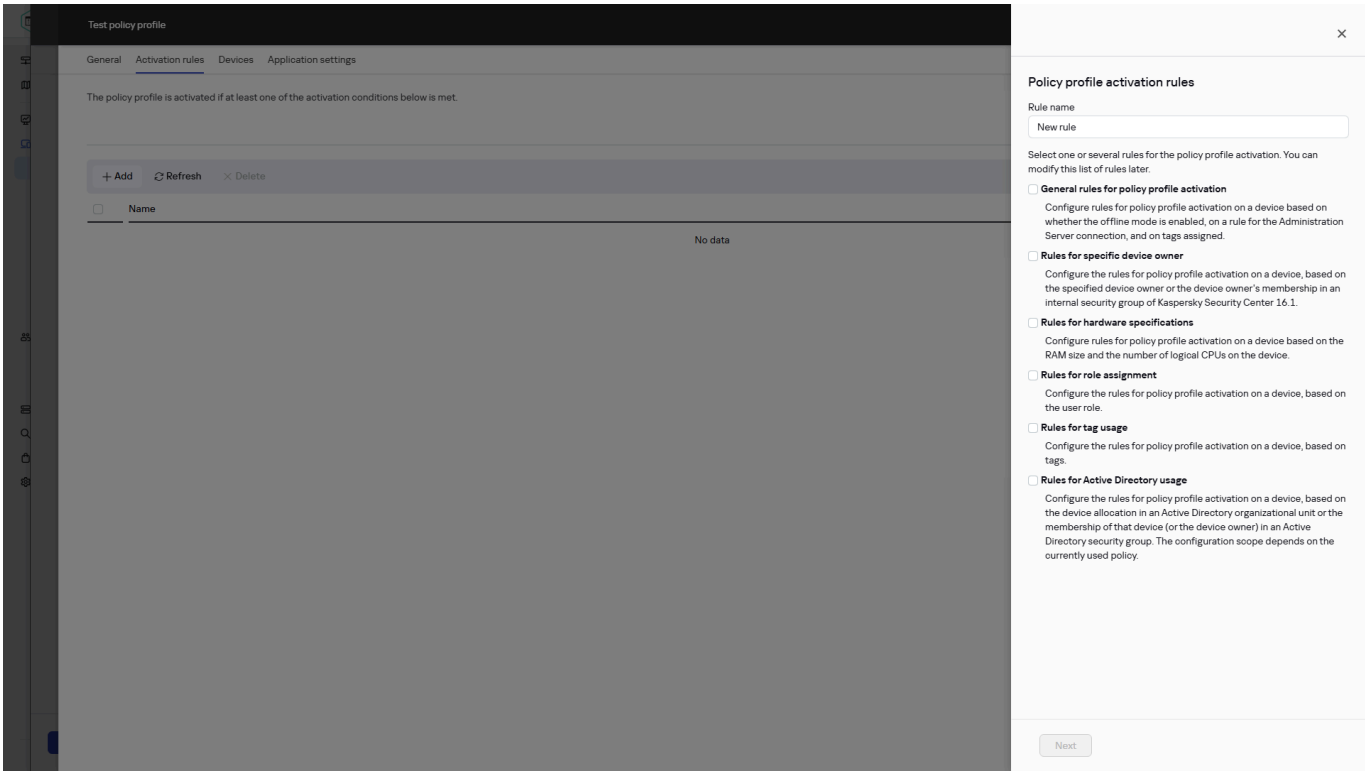
  如果選取此核取方塊，則會在裝置上啟動政策設定檔。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **在 Active Directory 組織單元中的裝置分配**

  如果啟用此選項，包含在指定 Active Directory 組織單元 (OU) 中的裝置上的政策設定檔將會啟動。如果停用此選項，則不套用設定檔啟動標準。

  預設情況下已停用該選項。

精靈的附加頁面數量取決於您在第一步選取的設定。您可以稍後修改政策設定檔啟動規則。



建立政策設定檔啟動規則

6. 檢查所配置參數的清單。若清單正確，請點擊**建立**。

設定檔將被儲存。當觸發啟動規則時，將在裝置上啟動該設定檔。

針對顯示在**啟動規則**頁籤中政策設定檔內容的設定檔，所建立的政策設定檔啟動規則。您可以修改或刪除任何政策設定檔啟動規則。

多個啟動規則可以被一起觸發。

刪除政策設定檔

要刪除政策設定檔：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤上，選取要刪除之政策設定檔旁的核取方塊，接著點擊**刪除**。
3. 在開啟的視窗中，再次點擊**刪除**按鈕。

政策設定檔被刪除。如果政策從低級別群組繼承，設定檔保持在該群組，但變成該群組的政策設定檔。這可以消除低級別群組裝置上安裝的受管理應用程式的設定的顯著修改。

匯出和匯入政策設定檔

無需匯出政策，即可將政策設定檔儲存到 KLPROF 檔案，然後使用此 KLPROF 檔案將已儲存的設定檔匯入到政策。

這可讓您快速恢復策略設定檔設定，而不是再設定它們。

政策設定檔會匯入到與匯出該設定檔的應用程式版本相同的政策中。對於支援政策向後相容的應用程式（例如，Kaspersky Endpoint Security for Windows），您可以將政策設定檔匯入到不同版本的政策中。

要匯出政策設定檔，請執行以下操作：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在「**政策設定檔**」索引標籤上，點擊要匯出的政策設定檔。
3. 在工具列上，點擊「**匯出**」按鈕。
4. 在開啟的視窗中，指定要儲存包含政策設定檔之檔案的目錄。
   如有必要，可變更檔案名稱。
5. 按一下**儲存**按鈕。

如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

要匯入政策設定檔，請執行以下操作：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在工具列上，點擊「**匯入**」按鈕。

3. 在開啟的視窗中，選取包含所需政策設定檔的 KLPROF 檔案，然後點擊「**開啟**」按鈕。
   匯入檔案的大小上限為 4 GB。

如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

政策設定檔會以匯出時的名稱匯入，而不是以 KLPROF 檔案的名稱匯入。
檔案會以「**已停用**」狀態和最低優先順序匯入，無論政策設定檔在匯出前的優先順序為何。

在以下情況下無法執行匯入：

- 政策中已存在同名設定檔。
- 政策中的設定檔數量已達 100 個。

網路代理政策設定

若設定網路代理政策：

1. 在應用程式的主選單中，前往 **資產管理 → 政策**。
2. 按一下網路代理政策的名稱。
   網路代理政策的內容視窗開啟。內容視窗包含如下所述的頁簽和設定。

請參閱以下比較表，它詳情描述了如何根據使用的作業係統類型套用設定。

一般

在此頁籤上，您可以修改政策名稱、政策狀態並指定政策設定的繼承：

- 在**名稱**欄位中，您可以修改政策名稱。
- 在**政策狀態**區塊中，您可以選取一種政策模式：
  - **作用中**

    如果選取該選項，政策將變為啟用狀態。
    預設情況下已選定此選項。
  - **非作用中**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。

- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。
    預設情況下已啟用該選項。
  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。
    預設情況下已停用該選項。

事件組態

在此頁簽上，您可以配置事件記錄和事件通知。事件根據重要性等級分佈在以下部分：

- **功能失效**
- **警告**
- **資訊**

在每個區域，清單顯示在管理伺服器上事件類型和預設事件儲存的週期（天）。點擊事件類型後，您可以指定清單中已選中的事件記錄和通知設定。預設下，為整個管理伺服器指定的通用通知設定被用於所有事件類型。然後，您可以變更所需事件類型的特別設定。

例如，在**警告**區域，您可以配置**發生了安全問題**事件類型。例如，當發佈點的可用磁碟空間小於 2 GB（遠端安裝應用程式和下載更新至少需要 4 GB）時，此類事件可能發生。若要配置**發生了安全問題**事件，按一下它並指定儲存發生的事件的位置以及如何通知它們。

> 如果網路代理偵測到安全問題，您可以使用受管理裝置設定管理該問題。

應用程式設定

設定

在**設定**區域，您可以配置網路代理政策：

- **僅透過發佈點分發檔案**

  如果啟用此選項，受管理裝置上的網路代理僅從發佈點擷取更新。

如果停用此選項，受管理裝置上的網路代理從發佈點或從管理伺服器擷取更新。

請注意，受管理裝置上的安全應用程式從每個安全應用程式的更新工作中的來源集中擷取更新。如果您啟用**僅透過發佈點分發檔案**選項，請確保在更新工作中將Open Single Management Platform設定為更新來源。

預設情況下已停用該選項。

- **事件佇列最大值(MB)**

  在該欄位中，您可以指定事件佇列可在磁碟機上佔據的最大空間。

  預設值為 2 MB。

- **應用程式被允許在裝置上獲取政策延伸資料**

  安裝在受管理裝置的網路代理會傳輸已套用安全應用程式政策的相關資訊至安全應用程式（例如 Kaspersky Endpoint Security for Linux）。您可在安全應用程式介面檢視已傳輸的資訊。

  網路代理會傳輸以下資訊：

  - 政策傳送至受管理裝置的時間。
  - 政策傳送至受管理裝置時啟用中政策的名稱。
  - 政策傳送至受管理裝置時漫遊政策的名稱（對於 Linux 版網路代理不可用）。
  - 政策傳送至受管理裝置時，受管理裝置包含的管理群組名稱與連結路徑。
  - 政策傳送至受管理裝置時包含名稱和優先順序的活動政策設定檔的清單。

  您也可使用資訊確保套用正確政策至裝置和用於疑難排解。預設情況下已停用該選項。

- **保護網路代理服務免遭未經授權的移除或終止，並防止設定遭到變更**

  如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

  啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

  預設情況下已停用該選項。

- **使用解除安裝密碼**

  如果啟用了此選項，透過單擊**修改**按鈕，您可以指定klmover公用程式的密碼。

  預設情況下已停用該選項。

  停用此選項可遠端解除安裝網路代理程式。

儲存區

在**儲存區**區域，您可以選取將其資訊從網路代理傳送到管理伺服器的物件類型：

- **已安裝應用程式詳情**

  如果啟用此選項，會將安裝在用戶端裝置上的應用程式資訊傳送至管理伺服器。

  預設情況下已啟用該選項。

- **包括修補程式資訊**

  安裝在用戶端裝置的應用程式修補程式的資訊會傳送至管理伺服器。啟用此選項可能增加管理伺服器和 DBMS 的負載，並造成資料庫的流量增加。

  預設情況下已啟用該選項。它僅適用於 Windows。

- **Windows Update 更新詳情**

  如果啟用此選項，會將用戶端裝置上必須安裝的 Microsoft Windows Update 更新資訊傳送至管理伺服器。

  預設情況下已啟用該選項。它僅適用於 Windows。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **軟體弱點和對應更新的詳情**

  若啟用此選項，協力廠商的弱點（包含 Microsoft 軟體）、受管理裝置上偵測到的資訊以及修復協力廠商弱點的軟體更新資訊（不含 Microsoft 軟體）都會傳送至管理伺服器。

  選取此選項（**軟體弱點和對應更新的詳情**）會增加網路負載、管理伺服器磁碟負載和網路代理的資源消耗。

  預設情況下已啟用該選項。它僅適用於 Windows。

  若要管理 Microsoft 軟體更新，請使用**Windows Update 更新詳情**選項。

- **硬體登錄資料詳細資訊**

  安裝在裝置上的網路代理會向管理伺服器傳送關於裝置硬體的資訊。您可以在裝置內容中檢視硬體詳細資訊。

  確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

如果網路代理政策禁止本區域中某些設定，則您無法修改這些設定。

軟體更新和弱點

在**軟體更新和弱點**區域，您可以啟用可執行檔的弱點掃描：

- **當執行可執行檔時掃描其弱點**

  如果啟用此選項，系統將在執行可執行檔時掃描弱點。

  預設情況下已啟用該選項。

重新啟動管理

如果您的作業系統必須在您使用、安裝或移除安裝應用程式時重新啟動受管理裝置，請在**重新啟動管理**區域指定執行的操作：

- **不要重新啟動作業系統**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **如果必要，自動重新啟動作業系統**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者動作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在指定時間後強制重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

  - **強制關閉被封鎖工作階段中的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

管理修補程式和更新

在管理修補程式和更新區域，您可以設定受管理裝置上的更新下載和發佈，以及修補程式安裝：

- **自動為處於「未定義」狀態的元件安裝適用的更新與修補程式**

  如果啟用此選項，帶有*未定義*批准狀態的 Kaspersky 應用程式在從更新伺服器下載後將被自動安裝在受管理裝置。

  如果停用此選項，被下載和標注為*未定義*狀態的卡巴斯基修補程式將僅在您改變其狀態為*已核准*是被安裝。

  預設情況下已啟用該選項。

- **提前從管理伺服器下載更新和病毒資料庫（建議）**

  如果啟用此選項，離線模式更新下載被使用。當管理伺服器接收更新時，它通知網路代理（安裝網路代理的裝置）將用於受管理應用程式的更新。當網路代理接收更新的資訊後，它提前從管理伺服器下載相關檔案。在第一次連線網路代理時，管理伺服器發起更新下載。網路代理下載所有更新到用戶端裝置後，更新對該裝置上的應用程式可用。

  當用戶端裝置上的受管理應用程式嘗試存取網路代理以更新時，該網路代理檢查其是否具有所有所需的更新。如果在受管理應用程式請求更新之前 25 小時內，更新已從管理伺服器收到，則網路代理不連線到管理伺服器，而是從本機快取提供更新給受管理應用程式。當網路代理提供更新到用戶端裝置上的應用程式時，可能不會建立到管理伺服器的連線，但是更新不需要連線。

  如果停用此選項，離線模式更新下載不被使用。更新依據更新下載工作的排程被發佈。

  預設情況下已啟用該選項。

連線

連線區域包含三個子區域：

- **網路**
- **連線設定檔**
- **連線排程**

在**網路**子區域，您可以設定到管理伺服器的連線、啟用 UDP 連接埠，和指定 UDP 連接埠號。

- 在**連線至管理伺服器**設定群組中，您可以設定到管理伺服器的連線，並指定同步用戶端裝置和管理伺服器的時間間隔：
  - **同步間隔（分鐘）**

    網路代理同步管理伺服器的受管理裝置。我們建議您設定同步間隔（也叫心跳）為每 10,000 台受管理裝置 15 分鐘。

  - **壓縮網路流量**

    如果啟用此選項，則透過減少所傳輸的流量進而減少管理伺服器的負載來提高網路代理的資料傳輸速度。

    用戶端裝置上的 CPU 負載可能會增加。

預設情況下會啟用此核取方塊。

- **在 Microsoft Windows 防火牆上開啟網路代理連接埠**

  如果啟用此選項，網路代理工作所需的連接埠將新增到 Microsoft Windows 防火牆排除清單中。

  預設情況下已啟用該選項。

- **使用 SSL 連線**

  如果啟用此選項，則使用 SSL 通訊協定透過安全連接埠連線管理伺服器。

  預設情況下已啟用該選項。

- **以預設連線設定在發佈點（如果可用）上使用連線閘道**

  如果啟用此選項，發佈點上的連線閘道在管理群組屬性指定的設定下使用。

  預設情況下已啟用該選項。

- **使用 UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

- **UDP 連接埠號**

  在該欄位中，您可以輸入 UDP 連接埠號。預設埠號為 15000。

  使用十進位系統記錄。

- **使用發佈點強制連線到管理伺服器**

  如果您選取了**將此發佈點用作推送伺服器**發佈點設定視窗中的選項。否則，發佈點將不會作為推送伺服器。

在**連線設定檔**子區域中，您可以指定網路位置設定，並在管理伺服器不可用時啟用不在辦公室模式：

- **網路位置設定**

  網路位置設定定義用戶端裝置所連線的網路內容，並指定當網路內容改變時，網路代理從一個管理伺服器連線設定檔轉換到另一個的規則。

- **管理伺服器連線設定檔**

  您可以檢視和設定網路代理至管理伺服器的連線。在該區域，您也可以建立當以下事件發生時，轉換網路代理到不同管理伺服器的規則：

  - 當用戶端裝置連線到另一個本機網路時
  - 當裝置與組織的本機網路遺失連線時
  - 當連線閘道的位址變更或 DNS 伺服器位址修改時

- **當管理伺服器不可用時啟用漫遊模式**

  如果啟用此選項，則在透過該設定檔連線的情況下，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策設定檔，以及漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

  如果停用此選項，則應用程式將使用已啟動的政策。

  預設情況下已停用該選項。

在**連線排程**子區域中，可以指定網路代理傳送資料到管理伺服器的時間間隔：

- **必要時連線**

  如果選中此選項，當網路代理需要傳送資料到管理伺服器時連線才被建立。

  預設情況下已選定此選項。

- **在指定時間間隔連線**

  如果選中此選項，網路代理在指定時間連線到管理伺服器。您可以新增若干個連線時間段。

透過發佈點的網路輪詢

在**透過發佈點的網路輪詢**區域，您可以設定網路自動輪詢。您可以使用以下選項啟用輪詢並設定其頻率：

- **Windows 網路**

  此選項僅適用於Windows的分發點。

  如果啟用此選項，則管理伺服器將按照您按一下**設定快速輪詢排程**和**設定完整輪詢排程**連結所配置的排程自動輪詢網路。

  如果停用此選項，管理伺服器將以**網路輪詢頻率（分鐘）**欄位中指定的時間間隔輪詢網路。

  網路代理程式版本的裝置發現間隔可以在**Windows 網域的輪詢頻率（分鐘）**（用於快速的Windows網路輪詢）和**網路輪詢頻率（分鐘）**（用於完整的Windows網路輪詢）欄位中進行設定。

  預設情況下已停用該選項。

- **IP 範圍**

  如果啟用此選項，則發佈點將按照您按一下**設定輪詢排程**按鈕所配置的排程自動輪詢 IP 範圍。

  如果停用此選項，則發佈點將不輪詢 IP 範圍。

  在 10.2 版之前的網路代理中，可在**輪詢間隔（分鐘）**欄位中配置 IP 範圍的輪詢頻率。若啟用該選項，可使用區域。

  預設情況下已停用該選項。

- **Zeroconf**

  如果啟用此選項，發佈點將使用零配置網路（也稱為 *Zeroconf*）用 IPv6 裝置自動輪詢網路。在這種情況下，啟用的 IP 範圍輪詢將被忽略，因為發佈點會輪詢整個網路。

  要開始使用 Zeroconf，必須滿足以下條件：

  - 發佈點必須執行 Linux。
  - 您必須在發佈點上安裝 avahi-browse 公用程式。

  如果停用此選項，則發佈點不會使用 IPv6 裝置輪詢網路。

  預設情況下已停用該選項。

- **網域控制器**

  如果啟用此選項，則發佈點將按照您按一下**Set polling schedule**按鈕設定輪詢排程自動輪詢網域控制器。

  如果停用此選項，則發佈點將不輪詢網域控制器。

在 10.2 版之前的網路代理中，可在**輪詢間隔（分鐘）**欄位中配置網域控制器的輪詢頻率。如果啟用此選項，則該欄位可用。

預設情況下已停用該選項。

發佈點網路設定

在**發佈點網路設定**區域中，您可以指定網際網路存取設定：

- **使用代理伺服器**

  如果啟用此選項，將使用網際網路代理伺服器將發佈點連線至卡巴斯基更新伺服器。

- **位址**

- **連接埠號**

- **略過本機位址的代理伺服器**

  如果啟用此選項，則不使用代理伺服器連線本機網路的裝置。
  預設情況下已停用該選項。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。
  預設情況下，此核取方塊已清除。

KSN 代理（發佈點）

在 **KSN 代理（發佈點）**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發卡巴斯基安全網路 (KSN) 請求。

- **在發佈點端啟用 KSN 代理**

  KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。
  發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到Kaspersky。
  預設情況下已停用該選項。啟用該選項僅在**使用管理伺服器作為代理伺服器**和**我同意使用卡巴斯基安全網路**選項在管理伺服器內容視窗中被啟用時起作用。
  您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

- **轉發 KSN 請求到管理伺服器**

  發佈點從受管理裝置轉發 KSN 請求到管理伺服器。
  預設情況下已啟用該選項。

- **透過網際網路直接存取 KSN 雲端/KPSN**

  發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或 KPSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或 KPSN。

- **TCP 連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

- **UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

- **HTTPS 連接埠**

  如果您需要受管裝置透過 HTTPS 連接埠連線至 KSN 代理伺服器，請啟用**使用 HTTPS**選項，然後在**HTTPS 連接埠**欄位中指定連接埠號碼。預設情況下已停用該選項。連線到 KSN 代理伺服器的預設 HTTPS 連接埠是 17111。

更新（發佈點）

在**更新（發佈點）**部分，您可以啟用下載差異檔案功能，以便發佈點以差異檔案的形式從卡巴斯基更新伺服器獲取更新。

本機帳戶管理（僅限 Linux）

本機帳戶管理（僅限 Linux）區域包括三個子區域：

- **使用者憑證管理**
- **新增或編輯適用的本機管理員群組**
- **上傳參考檔案以防護使用者裝置上的 sudoers 檔案免受變更**

在**使用者憑證管理**子區域中，您可以指定要安裝的根憑證。例如，這些憑證可用於驗證網站或網頁伺服器的真確性。

- **安裝根憑證**

  如果啟用此選項，則新增至表格中的憑證將安裝在指定的裝置上。

  如果停用此選項，則不會在指定裝置上安裝任何憑證。

  預設情況下已停用該選項。

- **新增**

  點擊此按鈕將開啟一個視窗，您可以在其中新增憑證。

  憑證必須小於 10 MB。

  卡巴斯基安全管理中心支援具有 CER、CRT、CERT、PEM 和 KEY 副檔名的憑證。

在**新增或編輯適用的本機管理員群組**子區域中，您可以管理本機管理員群組。例如，在撤銷本機管理員權限時就會用到這些群組。您也可以使用**特權裝置使用者報告（僅限 Linux）**檢查特權使用者帳戶清單。

- **新增**

  點擊此按鈕將開啟一個視窗，您可以在其中新增本機管理員群組。

- **編輯**

  點擊此按鈕將開啟一個視窗，您可以在其中編輯本機管理員群組。

  如果選取本機管理員群組旁邊的核取方塊，則可使用此按鈕。

- **刪除**

  點擊此按鈕即從表格中刪除已選取的本機管理員群組。

  如果選取本機管理員群組旁邊的核取方塊，則可使用此按鈕。

在**上傳參考檔案以防護使用者裝置上的 sudoers 檔案免受變更**子區域中，您可以設定 sudoers 檔案的控制。特權群組和裝置使用者是由裝置上的 sudoers 檔案定義。sudoers 檔案位於 `/etc/sudoers`。您可以上傳參考 sudoers 檔案，以保護 sudoers 檔案免於變更。這將防止對 sudoers 檔案進行不必要的變更。

無效的參考 sudoers 檔案可能會導致使用者的裝置故障。

- **控制 sudoers 檔案**

  如果啟用此選項，sudoers 檔案將被目前的參考 sudoers 檔案取代。

  如果停用此選項，sudoers 檔案將保持不變。

  預設情況下已停用該選項。

- **參考 sudoers 檔案**

  此欄位顯示上傳的參考 sudoers 檔案名稱。

- **上傳**

  點擊此按鈕將開啟一個視窗，您可以在其中上傳參考 sudoers 檔案。

- **目前的參考 sudoers 檔案**

  點擊此按鈕將顯示目前 sudoers 檔案的內容。

變更歷史

在**變更歷史**頁籤上，您可以：

- 檢視並儲存政策修訂歷程記錄。
- 回溯到政策修訂。

- 新增和編輯政策修訂描述。
- 比較政策修訂版本。

Windows、Linux 和 macOS 網路代理的使用：比較

網路代理的用法因裝置的作業係統而異。網路代理政策和安裝套件設定也根據作業系統不同而不同。下表比較適用於 Windows、Linux 和 macOS 作業系統的網路代理功能和使用情境。

網路代理功能比較

網路代理功能	Windows	Linux	macOS
安裝			
使用協力廠商工具，透過複製帶有作業系統和網路代理的管理員硬碟磁碟機映像安裝	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
使用應用程式遠端安裝的協力廠商工具佈署	✓	✓	✓
在裝置上手動執行應用程式安裝程式安裝	✓	✓	✓
使用靜默模式安裝網路代理	✓	✓	✓
將用戶端裝置手動連線至管理伺服器。klmover 公用程式	✓	✓	✓
自動安裝 Kaspersky Next XDR Expert 元件的更新與修補程式	✓	✓	—
自動發佈金鑰	✓	✓	✓
強制同步	✓	✓	✓ 除推播伺服器外
發佈點			
用作發佈點	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
計算發佈點的數量和配置	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓ 不使用網路位置感知 (NLA)。	✓ 不使用網路位置感知 (NLA)。
行動模式更新下載	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
網路輪詢	✓ • IP 範圍輪詢 • 網域控制器輪詢（Active Directory） 限制：不支援 Microsoft Windows on Arm的網路代理程式。	✓ IP 範圍輪詢 Zeroconf 輪詢 網域控制器輪詢（Microsoft Active Directory、Samba 4 Active Directory、FreeIPA、ALD Pro）	—
在發佈點端執行 KSN 代理服務	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	—

網路代理功能	Windows	Linux	macOS
通過 Kaspersky 更新伺服器將更新下載到將更新發佈到受管理裝置的發佈點儲存區	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	– (若一或多個執行 Linux 或 macOS 的裝置位於下載更新至發佈點儲存區工作範圍內，該工作會以失敗狀態完成，即使工作已在所有 Windows 裝置上成功完成。)
應用程式的推送安裝	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	受限制：無法使用 Linux 發佈點在 Windows 裝置上執行推送安裝。	受限制：無法使用 macOS 發佈點在 Windows 裝置上執行推送安裝。
作為推送伺服器使用	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	–
處理協力廠商應用程式			
在裝置上遠端安裝應用程式	✓	✓	✓ 有關詳細資訊，請參閱以下文章：在macOS裝置上遠端安裝應用程式。
在網路代理政策中配置作業系統更新	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	–	–
檢視軟體弱點資訊	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	–	–
掃描應用程式以尋找弱點	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	–	–
軟體更新	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	–	–
清查裝置上所安裝的軟體	✓	✓	–
虛擬機			
在虛擬機上安裝網路代理	✓	✓	✓
虛擬桌面基礎結構 (VDI) 的最佳化設定	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
對動態虛擬機的支援	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
其他			
在遠端用戶端裝置使用 Windows 共用桌面稽核操作	✓	–	–
監控防毒防護狀態	✓	✓	✓
管理裝置重新啟動	✓	–	–
支援檔案系統復原	✓	✓	✓
使用該網路代理作為連線閘道	✓	✓	✓
連線管理員	✓	✓	✓
漫遊使用者的連線設定檔	✓	✓	✓

網路代理功能	Windows	Linux	macOS
從一部管理伺服器切換至另一部的網路代理（依網路位置自動進行）	✓	✓	✓
檢查用戶端裝置與管理伺服器之間的連線。Klnagchk 公用程式	✓	✓	✓
用戶端裝置的遠端桌面連線	✓	✓	✓ 透過使用虛擬網路計算 (VNC) 系統。
透過移轉精靈下載獨立安裝套件	✓	✓	✓
檢視用戶端裝置硬體的資訊	✓	✓ 安裝在這些裝置上的網路代理傳送給管理伺服器的 Linux 裝置硬體資訊僅限於受管理裝置設定說明中指定的資訊。	✓ 安裝在這些裝置上的網路代理向管理伺服器傳送的有關 macOS 裝置硬體的資訊僅限於受管理裝置設定說明中指定的資訊。

按作業系統比較網路代理設定

下表顯示了可用的網路代理政策設定，具體取決於安裝網路代理的受管理裝置的作業系統。

網路代理設定：按作業系統比較

設定部分	Windows	Linux	macOS
一般	✓	✓	✓
事件組態	✓	✓	✓
設定	✓	✓ 提供以下功能： • **僅透過發佈點分發檔案** • **事件佇列最大值(MB)** • **應用程式被允許在裝置上獲取政策延伸資料**	✓
儲存區	✓	✓ 提供以下功能： • **已安裝應用程式詳情** • **硬體登錄資料詳細資訊**	✓ **硬體登錄資料詳細資訊**選項可用。
連線→網路	✓	✓ 除了**在 Microsoft Windows 防火牆上開啟網路代理連接埠** 選項。	✓
連線→連線設定檔	✓	✓	✓
連線→連線排程	✓	✓	✓
透過發佈點的網路輪詢	✓ 提供以下功能： • **Windows 網路** • **IP 範圍** • **網域控制器**	✓ 提供以下功能： • **Zeroconf** • **IP 範圍** • **網域控制器**	—
發佈點網路設定	✓	✓	✓
KSN 代理（發佈點）	✓	✓	—
更新（發佈點）	✓	✓	—
變更歷史	✓	✓	✓

配置受管理應用程式的防護設定

若要配置受管理卡巴斯基應用程式的防護設定，您可以使用政策。

有關配置 Kaspersky Endpoint Security 政策的詳細資訊，請參閱對應說明：

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

Kaspersky Endpoint Security 更新群組工作的手動設定

Kaspersky Endpoint Security 的最佳化和建議排程選項是**當新更新下載至儲存區時**時，當**使用工作啟動自動隨機化延遲**核取方塊被選中時。

卡巴斯基安全網路和卡巴斯基私人安全網路

本節說明卡巴斯基安全網路 (KSN) 和卡巴斯基私人安全網路 (KPSN) 線上服務基礎架構的使用方式。本節提供 KSN 和 KPSN 的相關資訊，以及如何啟用 KPSN、設定 KPSN 的存取權限和檢視 KSN 代理伺服器使用統計資料的說明。

經認證的應用程式版本僅允許使用 KPSN。不允許使用 KSN，因為這會導致應用程式失去認證狀態。我們建議使用 KPSN，或避免使用 KSN。

關於 KSN

卡巴斯基安全網路 (KSN) 是一種線上服務組織結構，可提供對 Kaspersky 網路知識庫的存取，其中包含與檔案信譽、網路資源和軟體相關的資訊。使用來自卡巴斯基安全網路的資料可確保卡巴斯基應用程式更快地回應威脅、提高某些防護元件的有效性並降低誤報風險。KSN 允許您使用 Kaspersky 的信譽資料庫檢索有關安裝在受管理裝置上的應用程式資訊。

參與卡巴斯基安全網路，即表示您同意自動向卡巴斯基提供相關資訊，說明安裝在透過 Open Single Management Platform 管理的電腦和行動裝置上的安全應用程式運作情況。依照目前 KSN 存取設定傳送資訊。

使用卡巴斯基安全網路會導致應用程式失去認證狀態。您必須使用卡巴斯基私人安全網路，或避免使用 KSN。

Open Single Management Platform支援以下KSN基礎設施解決方案：

- *全球 KSN*是一種允許您與卡巴斯基安全網路交換資訊的解決方案。一旦加入KSN，即表示您同意以自動模式將透過Open Single Management Platform管理的用戶端裝置上安裝的卡巴斯基程式的相關操作資訊傳送到卡巴斯基。依照目前 KSN 存取設定傳送資訊。卡巴斯基分析師會另外分析收到的資訊，並將其包含在卡巴斯基安全網路的信譽和統計資料庫中。Open Single Management Platform預設使用此解決方案。

- *卡巴斯基私有安全網路 (KPSN)* 是一種解決方案，可讓已安裝卡巴斯基應用程式的裝置使用者存取卡巴斯基安全網路的信譽資料庫和其他統計資料，而不必從自己的電腦傳送資料給 KSN。KPSN用於由於以下原因無法加入Kaspersky Security Network的企業用戶端：

  - 使用者裝置未連線到網際網路。

  - 傳輸任何資料到國家/地區以外或企業區域網路以外被法律或企業安全政策禁止。

  您可以在管理伺服器內容視窗的**KSN Proxy settings**區段中，KSN 代理。

您可以隨時開始或停止使用KSN。

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在更新或升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的先前版本繼續使用 KSN。

啟用KSN後，Open Single Management Platform會檢查KSN伺服器是否可存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保維護受管理裝置的安全級別。

管理伺服器管理的用戶端裝置透過 KSN 代理伺服器與 KSN 互動。KSN 代理伺服器提供以下功能：

- 即使無法直接連線網際網路，用戶端裝置也可向 KSN 傳送請求以及向 KSN 傳送資訊。

- KSN 代理可暫存已處理的資料，進而減少對外頻寬消耗以及用戶端裝置等待 KSN 回覆而花費的時間。

您可以在**管理伺服器內容視窗**的KSN 代理區域中設定 KSN 代理伺服器。

設定對 KSN 的存取

您可以在管理伺服器和發佈點上設定到卡巴斯基安全網路 (KSN) 的存取。

KSN功能僅適用於當前的Kaspersky EDR Expert授權許可。

要設定管理伺服器到 KSN 的存取：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤上，選取**KSN 代理**區段。

3. 將切換按鈕切換到**在管理伺服器上啟用 KSN 代理 已啟用**位置。

   資料被從用戶端裝置傳送到 KSN，與在這些用戶端裝置上活動的 Kaspersky Endpoint Security 政策一致。如果清除此核取方塊，管理伺服器和用戶端裝置將不會透過 Kaspersky Next XDR Expert 將任何資料傳送至 KSN。不過，用戶端裝置可依其各自的設定，直接將資料傳送至 KSN（略過 Kaspersky Next XDR Expert）。用戶端裝置上啟用的 Kaspersky Endpoint Security 政策會決定哪些資料將從這些裝置直接傳送至 KSN（略過 Kaspersky Next XDR Expert）。

4. 將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。

   如果啟用了此選項，用戶端裝置將傳送修補程式安裝結果到 Kaspersky。啟用此選項時，請確保閱讀並接受 KSN 聲明的條款。

   如果您正使用 KPSN，將切換按鈕切換到**使用卡巴斯基私人安全網路 已啟用**位置並點擊**選取包含 KSN 代理設定的檔案**按鈕以下載 KPSN 設定（帶有 pkcs7 和 pem 副檔名的檔案）。下載完設定之後，介面會顯示提供商的名稱和聯絡人，以及 KPSN 設定檔的建立日期。

   當您將切換按鈕切換到**使用卡巴斯基私人安全網路 已啟用**位置，將顯示一則含有有關 KPSN 詳細資料的訊息。

   以下卡巴斯基應用程式支援 KPSN：

   - Kaspersky Next XDR Expert
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   如果您在 Kaspersky Next XDR Expert 中啟用 KPSN，這些應用程式將收到支援 KPSN 的相關資訊。在應用程式設定視窗，在**進階威脅防護**區域的**卡巴斯基安全網路**子區域中，將顯示關於所選 KSN 提供者的資訊 — KSN 或 KPSN。

   > 如果已在管理伺服器內容視窗的**KSN 代理**區段中設定 KPSN，Kaspersky Next XDR Expert 不會將任何統計資料傳送至卡巴斯基安全網路。

5. 若您已在管理伺服器內容中設定代理伺服器設定，但您的網路架構要求您直接使用 KPSN，請啟用**當連線到 KPSN 時略過代理伺服器設定**選項。否則，從受管理應用程式的請求無法到達 KPSN。

6. 在**連線設定**下，配置與KSN代理服務的管理伺服器連線：

   - TCP連接埠13111用於連線到KSN代理伺服器。對於根管理伺服器，此連接埠號碼無法變更。
   - 如果您要讓管理伺服器透過UDP連接埠連線到KSN代理伺服器，啟用**使用 UDP 連接埠**選項。預設下，會停用此選項，並使用 TCP 連接埠。如果啟用此選項，則預設使用UDP連接埠 15111。對於根管理伺服器，此連接埠號碼無法變更。

7. 將切換按鈕切換到**透過主管理伺服器將從屬管理伺服器連線到 KSN 已啟用**位置 。

   如果啟用此選項，從屬管理伺服器使用主管理伺服器作為 KSN 代理伺服器。如果停用此選項，從屬管理伺服器會自己連線到 KSN。該情況下，受管理裝置使用從屬管理伺服器作為 KSN 代理伺服器。

   > 如果在**KSN 代理**區段的右側面板中，從屬管理伺服器內容的切換按鈕是切換到**在管理伺服器上啟用 KSN 代理 已啟用**位置，則從屬管理伺服器會使用主管理伺服器作為代理伺服器。

8. 點擊**儲存**按鈕。

KSN 存取設定將被儲存。

您也可以設定發佈點存取 KSN，例如，如果您想降低管理伺服器負載。作為 KSN 代理伺服器的發佈點從受管理裝置直接傳送 KSN 請求到 Kaspersky，不使用管理伺服器。

要設定發佈點到卡巴斯基安全網路 (KSN) 的存取：

1. 確保發佈點是手動分配。
2. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
3. 在**一般**頁籤，選取**發佈點**區段。
4. 按一下發佈點的名稱以開啟工作內容視窗。
5. 在發佈點內容視窗中的**KSN 代理**區段，啟用**在發佈點端啟用 KSN 代理**選項，然後啟用**透過網際網路直接存取 KSN 雲端/KPSN**選項。
6. 點擊**確定**。

該發佈點將作為 KSN 代理伺服器。

請注意，發佈點不支援使用 NTLM 協定進行受管理裝置身分驗證。

啟用和停用 KSN 的使用

您可以在管理伺服器設定中啟用 KSN 的使用。若要為整合解決方案啟用 KSN 的使用，您也必須在 OSMP 設定中啟用它。

在管理伺服器設定中啟用和停用 KSN 的使用

若要啟用 KSN 的使用：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤上，選取**KSN 代理**區段。
3. 將切換按鈕切換到**在管理伺服器上啟用 KSN 代理 已啟用**位置。

KSN 代理伺服器已啟用，並將資料傳送至 KSN，以提升 Kaspersky Next XDR Expert 元件的效率及改善 Kaspersky 應用程式的效能。

1. 根據您使用的KSN 基礎架構解決方案，啟用對應的切換按鈕。
   - 如果您使用的是全球 KSN，請將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。
     現在可以向 KSN 傳送資料。啟用此選項時，您必須閱讀並接受 KSN 聲明的條款。

- 如果您使用的是 KPSN，請將切換按鈕切換到**使用卡巴斯基私人安全網路 已啟用**位置，然後按一下**選取包含 KSN 代理設定的檔案**按鈕，以下載 KPSN 設定（副檔名為 pkcs7 和 pem 的檔案）。下載完設定之後，介面會顯示提供商的名稱和聯絡人，以及 KPSN 設定檔的建立日期。

  當您將切換按鈕切換到**使用卡巴斯基私人安全網路 已啟用**位置，將顯示一則含有有關 KPSN 詳細資料的訊息。

2. 點擊**儲存**按鈕。

若要停用 KSN：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤上，選取**KSN 代理**區段。

3. 將切換按鈕切換到**在管理伺服器上啟用 KSN 代理 已停用**位置以停用 KSN 代理服務。

4. 點擊**儲存**按鈕。

在 OSMP 設定中啟用和停用 KSN 的使用

具有以下角色的使用者可以在 OSMP 設定中檢視和編輯參與 KSN 和 KPSN 的狀態：

- 總管理員
- SOC管理員
- 租用戶管理員（編輯狀態功能僅適用於根租用戶，對於層級結構中的其他租用戶，設定將自動套用）。

具有稽核員角色的使用者只能檢視參與 KSN 和 KPSN 的狀態。

若要在 OSMP 設定中啟用 KSN 的使用：

1. 在主選單中，前往**設定 → 卡巴斯基安全網路**。

2. 在 **Kaspersky EDR Expert** 區段中，選擇 **KSN** 連線模式。

3. 開啟**參與 KSN** 切換按鈕。

4. 請仔細閱讀KSN聲明。

5. 如果您同意 KSN 聲明的條款與條件，請選擇**本人確認已完整閱讀、理解並接受 KSN 聲明的條款和條件**選項，然後按一下**同意**。

   KSN隨即啟用，Open Single Management Platform會將統計資料傳送至KSN，供卡巴斯基專家進行分析。

6. 如果您不同意 KSN 聲明的條款與條件，請按一下**拒絕**。

   KSN將不會啟用。

若要在 OSMP 設定中啟用 KPSN 的使用：

1. 在主選單中，前往**設定 → 卡巴斯基安全網路**。
2. 在 **Kaspersky EDR Expert** 區段中，選擇 **KPSN** 連線模式。
3. 開啟**參與 KPSN** 切換按鈕。
4. 按一下**上傳**按鈕，選擇 KPSN 設定檔（副檔名為 .pkcs7 或 .pem 的檔案），然後按一下**開啟**。

   加入KPSN功能隨即啟用。

若要在 OSMP 設定中停用 KSN 或 KPSN 的使用：

1. 在主選單中，前往**設定→卡巴斯基安全網路**。
2. 如果要停用加入 KSN 功能，請選擇 **KSN** 連線模式，然後關閉**參與 KSN** 切換按鈕。
   加入KSN功能隨即停用。
3. 如果要停用加入 KPSN 功能，請選擇 **KPSN** 連線模式，然後關閉**參與 KPSN** 切換按鈕。

   加入KPSN功能隨即停用。

設定與KPSN本機信譽資料庫的連線

Kaspersky Next XDR Expert可以將沙盒元件警示資訊儲存到KPSN 的本機信譽資料庫。在這種情況下，物件將被賦予*不受信任*狀態。本機信譽資料庫的資料僅供公司區域網路電腦存取。

該應用程式允許具有以下角色的使用者檢視和編輯Kaspersky Private Security Network API整合設定：

- 總管理員
- SOC管理員
- 租用戶管理員（設定編輯功能僅適用於根租用戶，對於層級結構中的其他租用戶，設定將自動套用）。

具有稽核員角色的使用者只能檢視Kaspersky Private Security Network API整合設定。

若要設定Kaspersky Next XDR Expert與KPSN本機信譽資料庫的連線：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 按一下**根租用戶**，然後轉至**設定→KPSN本機信譽資料庫**子區段。
3. 在**資產**欄位中，指定儲存KPSN本機信譽評比資料庫的KPSN伺服器的IP位址。
4. 按一下**使用者憑證公鑰**欄位右側的**上傳**，然後選擇所需的.pem憑證。
5. 按一下**使用者憑證私鑰**欄位右側的**上傳**，然後選擇所需的.pem憑證。

6. 按一下**KPSN伺服器受信任根受信任憑證**欄位右側的**上傳**，然後選擇所需的.pem憑證。

7. 按一下**儲存**按鈕。

與KPSN本機信譽資料庫的連線隨即設定。

檢視接受的 KSN 聲明

啟用卡巴斯基安全網路 (KSN) 時，必須閱讀並接受 KSN 聲明。您可以隨時檢視已接受的 KSN 聲明。

若要檢視已接受的 KSN 聲明：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。

2. 在**一般**標籤上，選取**KSN 代理**區段。

3. 點擊**檢視卡巴斯基安全網路聲明**連接。

在開啟的視窗中，您可以檢視接受的 KSN 聲明的文字。

接受更新的 KSN 聲明

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的版本繼續使用 KSN。

升級管理伺服器版本後，會自動顯示更新的 KSN 聲明。如果您拒絕更新的 KSN 聲明，則以後仍然可以檢視並接受它。

要檢視然後接受或拒絕更新的 KSN 聲明，請執行以下操作：

1. 點擊**檢視通知**主應用程式視窗右上角的連結。
   通知 視窗隨即開啟。

2. 點擊**檢視更新的 KSN 聲明**連結。
   卡巴斯基安全網路聲明更新視窗開啟。

3. 閱讀 KSN 聲明，然後透過按一下以下其中一個按鈕做出決定：

   - **我接受更新的 KSN 聲明**
   - **在舊聲明下使用 KSN**

根據您的選擇，KSN 會按照目前或更新的 KSN 聲明條款繼續有效。您可以隨時在管理伺服器屬性中檢視已接受的 KSN 聲明文字。

檢查發佈點是否作為 KSN 代理伺服器運作

在分配作為發佈點運作的受管理裝置上，可以啟用卡巴斯基安全網路 (KSN) 代理。當 ksnproxy 服務在裝置上執行時，受管理裝置會作為 KSN 代理伺服器運作。您可以在本機裝置上檢查、開啟或關閉此服務。

您可以將基於 Windows 或基於 Linux 的裝置分配為發佈點。檢查發佈點的方法取決於該發佈點的作業系統。

若要檢查基於 Linux 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上，執行 `ps aux` 命令以顯示正在執行的處理程序清單。
2. 在正在執行的處理程序清單中，檢查 `/opt/kaspersky/klnagent64/sbin/ksnproxy` 處理程序是否正在執行。

如果 `/opt/kaspersky/klnagent64/sbin/ksnproxy` 處理程序正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所包含的受管理裝置的 KSN 代理伺服器運作。

若要檢查基於 Windows 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上的 Windows 系統中，開啟**服務**（**所有程序 → 管理工具 → 服務**）。
2. 在服務清單，檢查 ksnproxy 服務是否正在執行。

   如果 ksnproxy 服務正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

如果您想，您可以關閉 ksnproxy 服務。在這種情況下，發佈點上的網路代理程式停止加入Kaspersky Security Network。該需要本機管理員權限。

檢視 KSN 代理伺服器統計

OSMP主控台可讓您檢視KSN代理伺服器的使用統計資料。

統計資料包括以下參數：

- 與 KSN 的連線狀態
- 快取記錄數
- 快取中處理的封包數量
- 收到的封包數量

如果您使用 KPSN 作為基礎架構解決方案，則會顯示 KPSN 的使用統計資料。

檢視統計資料：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選擇**KSN 代理**部分，然後開啟**統計**頁簽。

   該頁簽顯示 KSN 代理伺服器使用的實際統計。統計資料每 15 秒重新整理一次。

您可以透過點擊**複製到剪貼簿**按鈕來複製統計資料。

管理端點防護工作

該部分介紹Open Single Management Platform使用的任務。

關於工作

Open Single Management Platform透過建立和執行*任務*來管理安裝在裝置上的卡巴斯基安全應用程式。安裝、啟用和停用應用程式、掃描檔案、更新病毒資料庫和軟體模組以及應用程式的其他行為均需要使用工作來完成。

只有在OSMP主控台伺服器上安裝了該應用程式的管理外掛程式後，才能使用OSMP主控台為特定應用程式創建任務。

工作可以在管理伺服器和裝置上執行。

管理伺服器上執行的工作包含以下：

- 自動發佈報告
- 將更新下載至儲存區
- 備份管理伺服器資料
- 資料庫維護

以下類型的工作在裝置上執行：

- *本機工作* — 在特定裝置上執行的工作。

  本機工作可以被管理員透過OSMP主控台修改，或者被遠端裝置使用者修改（例如，透過安全應用程式介面）。如果本機工作同時被管理員和受管理裝置使用者修改，管理員的修改將生效，因為其具有更高優先順序。

- *群組工作* — 在特定裝置上執行的工作。

  除非在工作內容中指定了其他項目，群組工作也影響所選群組的所有子群組。群組工作也影響（可選）佈署在其群組或子群組的連線到從屬和虛擬管理伺服器的裝置。

- *全域工作* — 選取指定裝置來執行的工作，與裝置屬於哪個管理群組無關。

您可以為每個應用程式建立任意數量群組工作、全域工作或本機工作。

您可以修改工作設定、檢視工作進度、複製、匯出、匯入和刪除工作。

只有當裝置上應用程式被執行，建立之工作才會執行。

工作執行結果儲存在每台裝置的作業系統事件記錄、管理伺服器作業系統事件記錄和管理伺服器資料庫中。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

關於工作範圍

*工作範圍*是執行工作的裝置集合。範圍的類型包括以下：

- 對於*本機工作*，範圍是裝置本身。
- 對於*管理伺服器工作*，範圍是管理伺服器。
- 對於*群組工作*，範圍是包含在群組中的裝置清單。

當建立*全域工作*時，您可以使用以下方法指定範圍：

- 手動指定特定裝置。

  您可以使用 IP 位址（或 IP 範圍）或 DNS 名稱作為該裝置的位址。您還可以選擇由管理伺服器偵測到的聯網裝置。

- 從包含有要新增的裝置位址的 .txt 檔案來匯入裝置清單（每一個電腦位址必須單獨一行）。

  如果透過檔案匯入裝置清單或手動建立裝置清單，且如果裝置是以名稱定義，則清單可以只包含其資訊已被輸入到管理伺服器資料庫中的裝置。而且，資訊必須在裝置被連線或裝置發現中輸入。

- 指定裝置分類。

  後續，工作範圍隨著包含在分類中的裝置集的變更而變更。裝置分類可以基於裝置內容（包含安裝在裝置上的軟體）建立，也可以基於分配到裝置的標籤來建立。裝置分類是指定工作範圍的最靈活的方法。

  裝置分類的工作總是按管理伺服器排程執行。這些工作無法執行在缺少管理伺服器連線的裝置上。使用其他方法指定範圍的工作直接執行在裝置上，且因此不取決於到管理伺服器的裝置連線。

  裝置分類的工作不會按裝置本機時間執行；相反，它們將按照管理伺服器本機時間執行。使用其他方法指定範圍的工作以裝置本機時間執行。

建立工作

要建立工作：

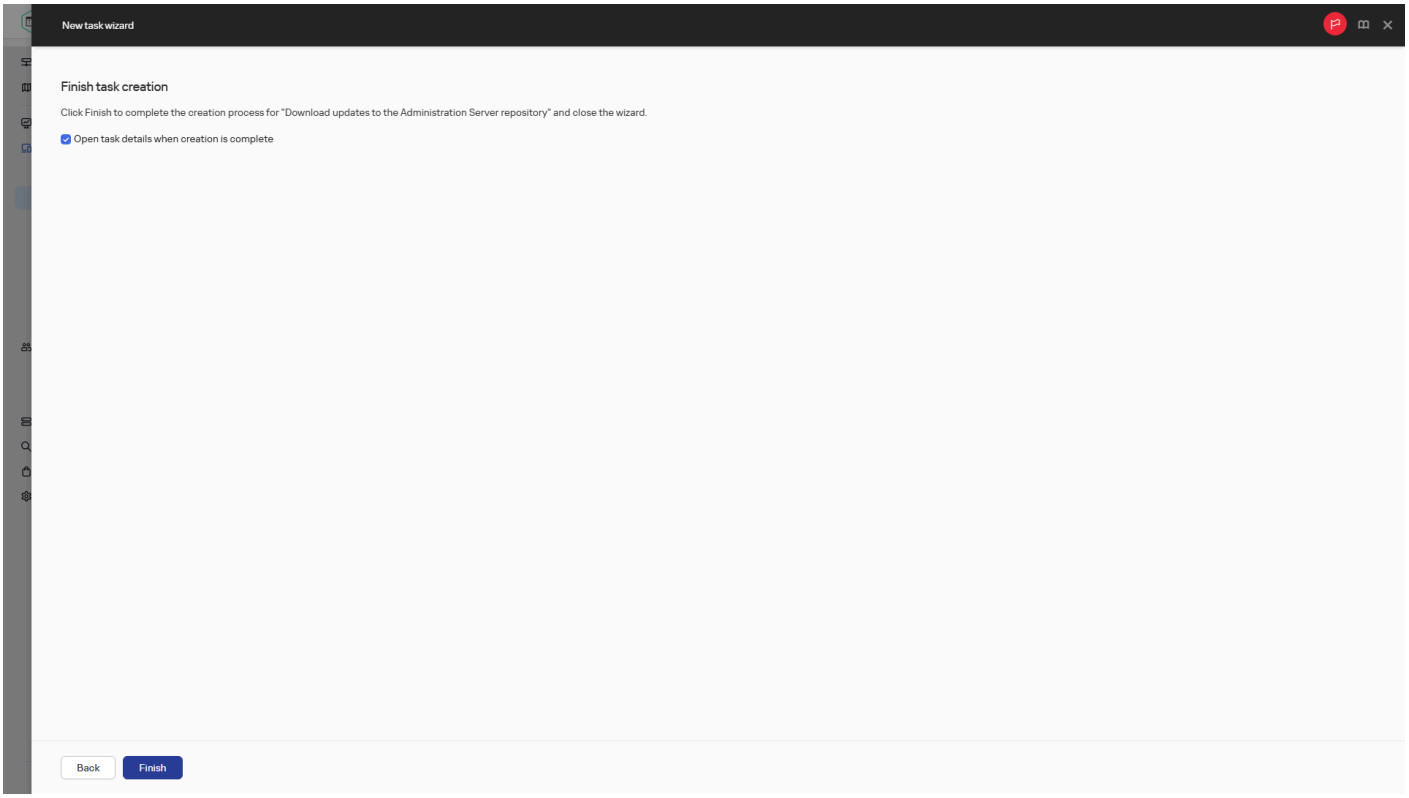
1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵循其說明。

3. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時變更預設設定。

4. 點擊**完成**按鈕。

工作被建立並顯示在工作清單。



完成工作建立

若要建立分配給所選裝置的新工作：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。

   受管理裝置清單隨即顯示。

2. 在受管理裝置清單中，選取裝置旁的核取方塊以為其執行工作。您可以使用搜尋和過濾功能來查找您正在尋找的裝置。

3. 點擊**執行工作**按鈕，然後選擇**新增一個新工作**。

   新工作精靈啟動。

   在精靈的第一步中，您可以刪除被選擇包含在工作範圍中的裝置。請按照精靈的步驟進行操作。

4. 點擊**完成**按鈕。

該工作是為選定的裝置建立的。

手動啟動工作

該應用程式會根據在各工作內容中指定的排程設定啟動工作。您可以隨時從工作清單中手動啟動工作。或者，您也可以在**資產（裝置）**清單中選取裝置，然後對這些裝置啟動現有工作。

若要手動啟動工作：

1. 在主功能表中，轉至 **工作**。
2. 在工作清單中，請選取您要啟動之工作旁的核取方塊。
3. 按一下**開始**按鈕。

工作啟動。您可在**狀態**欄中檢視工作狀態或點擊**結果**按鈕。

為選取的裝置啟動工作

您可以在裝置清單中選擇一台或多台用戶端裝置，然後啟動先前為它們建立的工作。這可讓您執行先前為一組特定裝置建立的工作。

這會變更套用工作的裝置清單。
舊的工作範圍會遭到刪除，並由選取的範圍取代。

為選取的裝置啟動工作：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，選取要執行工作的裝置所對應的核取方塊。您可以使用搜尋和過濾功能來查找您正在尋找的裝置。
3. 按一下**執行工作**按鈕，然後選擇**套用現有工作**。

   現有工作清單隨即顯示。
4. 所選裝置顯示在工作清單上方。如有必要，您可以從此清單中刪除裝置。您可以刪除除一台裝置之外的所有裝置。
5. 在清單中選擇所需的工作。您可以使用清單上方的搜尋框按名稱搜尋所需的工作。只能選擇一項工作。
6. 按一下**儲存並啟動工作**。

所選工作將立即為所選裝置啟動。工作中的排程啟動設定不會變更。

檢視工作清單

您可以檢視在 Kaspersky Next XDR Expert 中建立的工作清單。

若要檢視工作清單，

在主功能表中，轉至 **工作**。

工作清單隨即顯示。工作會依與應用程式名稱的關聯來分組。例如，*遠端安裝應用程式*工作會與管理伺服器相關，*更新*工作則指 Kaspersky Endpoint Security。

若要檢視工作內容，

請按一下工作的名稱。

工作內容視窗會一起顯示數個命名的頁籤。例如，**工作類型**會顯示在**一般**頁籤，以及工作排程–位於**排程**頁籤。

一般工作設定

此區段包含您可檢視與為大多數工作配置的清單。可用設定清單取決於您正在配置的工作。

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- 作業系統重新啟動設定：
  - **不重新啟動裝置**

    用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

  - **重新啟動裝置**

    如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

  - **強制關閉被封鎖工作階段中的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

- 工作排程設定：

  排程類型可能因工作而異。

某些類型的計劃可能不適用於其他卡巴斯基應用程式。

- **開始工作設定：**
  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **按每週中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

    工作定期執行，在指定月日的指定時間。

    在缺少指定日的月份，工作在最後一天執行。

    預設下，工作在每月的第一天執行，在目前系統時間。

  - **手動**

    工作不自動執行。您僅可以手動啟動。

    預設情況下已選定此選項。

  - **一次**

    此任務在指定的日期和時間（預設情況下，在建立工作的當天）執行一次。

  - **立即**

    工作在其設定儲存後立即執行。

  - **每月於選定的週間日**

    工作定期在指定月日的指定時間執行。

    預設情況下，開始時間為18:00，且未選擇當月的任何日期。

    請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

您可以選擇一週中的多個日期。

- **當新更新下載至儲存區時**

  工作會在更新下載至儲存區時執行。例如，您可能希望使用此排程進行*更新*工作。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。
    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機化延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

- 要分配工作的裝置：

  - **選取管理伺服器偵測到的網路裝置**

    工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

    例如，您可能要在安裝網路代理到未配置的裝置的工作中使用該選項。

- **手動指定裝置位址或從清單匯入位址**

  您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。

  您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

- **分配工作到裝置分類**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

- **分配工作到管理群組**

  工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

  例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

  如果工作被指派給管理群組，則工作內容視窗中不會顯示**安全**頁籤，因為群組工作受其所套用的群組的安全設定的約束。

- 帳戶設定：

  - **預設帳戶**

    在與執行該工作的應用程式相同的帳戶下執行該工作。

    預設情況下已選定此選項。

  - **指定帳戶**

    填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **登入。**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

工作建立後指定的設定

您可以在建立工作後指定以下設定。

- 群組工作設定：

  - **分發到子群組**

    此選項僅在群組工作的設定中可用。

    啟用此選項時，工作範圍包括：

    - 您在建立工作時選擇的管理群組。
    - 依據群組層次結構從屬於所選管理群組的任何級別下的管理群組。

    停用此選項時，工作範圍僅包括您在建立工作時選擇的管理群組。

    預設情況下已啟用該選項。

- **分發到從屬和虛擬管理伺服器**

  啟用此選項時，在主管理伺服器上有效的工作也將套用於從屬管理伺服器（包括虛擬伺服器）。如果從屬管理伺服器上已經存在相同類型的工作，則這兩個工作都將套用到從屬管理伺服器上 — 現有的工作和從主管理伺服器繼承的工作。

  此選項僅在**分發到子群組**選項已啟用的情況下可用。

  預設情況下已停用該選項。

- 進階排程設定：

  - **在啟動工作之前，使用 Wake-On-LAN 功能開啟裝置**

    裝置上的作業系統在工作開始之前的指定時間啟動。預設時間段為五分鐘。

    如果您想要工作在工作範圍內的所有用戶端裝置上執行，包括工作要啟動時關閉的裝置，則啟用該選項。

    若要裝置在工作完成後自動關閉，請啟用**完成工作後將裝置關機**選項。此選項可在相同視窗中找到。

    預設情況下已停用該選項。

  - **完成工作後將裝置關機**

    例如，您可能想為每週五工作時間後安裝更新到用戶端裝置的更新安裝工作啟用該選項，然後在週末關閉這些裝置。

    預設情況下已停用該選項。

  - **停止工作，若執行時間超過**

    在指定時間段過後，工作被自動停止，無論它是否完成。

    如果您想要中斷或停止執行時間太長的工作，則啟用該選項。

    預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

- 通知設定：

  - **儲存工作歷程記錄**塊:

    - **儲存在管理伺服器資料庫中（天）**

      有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件在指定的天數內被儲存在管理伺服器。當該時間段過後，資訊被從管理伺服器刪除。

      預設情況下已啟用該選項。

    - **儲存在裝置上的作業系統事件記錄中**

      有關工作執行的應用程式事件被本機儲存在每個用戶端裝置的 Syslog 事件記錄中。

      預設情況下已停用該選項。

    - **儲存在管理伺服器上的作業系統事件記錄中**

      有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件被集中儲存在管理伺服器作業系統的 Syslog 事件記錄中。

      預設情況下已停用該選項。

- **儲存所有事件**

  如果選取該選項，所有工作相關事件被儲存到事件記錄。

- **儲存工作進度相關事件**

  如果選取該選項，僅工作執行相關事件被儲存到事件記錄。

- **僅儲存工作執行結果**

  如果選取該選項，僅工作結果相關事件被儲存到事件記錄。

- **通知管理員工作執行的結果**

  您可以選取管理員接收工作執行通知的方法：透過電子郵件、透過 SMS 和透過執行可執行檔。若要配置通知，請點擊**設定**連結。

  預設下，所有通知方法被停用。

- **僅通知錯誤**

  如果該選項被啟用，管理員僅在工作執行完成但帶有錯誤時被通知。

  如果該選項被停用，管理員在每次工作執行完成後被通知。

  預設情況下已啟用該選項。

- 安全設定。

- 工作範圍設定。
  取決於工作範圍決定的方式，以下設定被展現：

  - **裝置**

    如果工作範圍由管理群組決定，您可以檢視該群組。這裡不可以變更。但您可設定**工作範圍排除項目**。

    如果工作範圍由裝置清單決定，您可以透過新增和刪除裝置修改該清單。

  - **裝置分類**

    您可以變更應用程式工作的裝置分類。

  - **工作範圍排除項目**

    您可以指定套用工作的裝置群組。要排除的群組僅可以是套用工作的管理群組的子群組。

- **變更歷程**。

匯出工作

Open Single Management Platform允許您將工作及其設定儲存到KLT檔案。您可以使用此 KLT 檔案匯入儲存的工作到卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux。

要匯出工作，請執行以下操作：

1. 在主功能表中，轉至 **工作**。
2. 選取您要匯出之工作旁邊的核取方塊。

   您不能同時匯出多個工作。如果您選擇了多個工作，**匯出**按鈕將被停用。此外，管理伺服器工作也不供匯出。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存新檔**視窗中，指定工作檔案的名稱和路徑。按一下**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，工作檔案會自動儲存在**下載**資料夾。

匯入工作

Open Single Management Platform允許您從KLT檔案匯入工作。KLT 檔案包含匯出工作及其設定。

為了正確匯入卡巴斯基應用程式工作，您必須安裝相應的管理外掛程式。

要匯入工作，請執行以下操作：

1. 在主功能表中，轉至 **工作**。
2. 點擊**匯入**按鈕。
3. 點擊**瀏覽**按鈕選擇要匯入的工作檔案。
4. 在開啟的視窗中，指定 KLT 工作檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個工作檔案。

   工作處理開始。
5. 工作處理成功後，選擇要將工作分配到哪些裝置。如要這麼做，請選擇以下選項之一：

   - **指派工作給管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

     例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

     如果工作被指派給管理群組，則工作內容視窗中不會顯示**安全**頁籤，因為群組工作受其所套用的群組的安全設定的約束。

   - **手動指定裝置位址或是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。

     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **指派工作給裝置分類**

     該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

     例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

6. 指定工作範圍。

7. 點擊**完成**按鈕以完成工作匯入。

此時會顯示匯入結果通知。如果工作匯入成功，您可以按一下**詳細資訊**連結以檢視工作內容。

匯入成功後，工作會顯示在工作清單中。工作設定和排程也會一起匯入。工作將根據其排程來啟動。

如果新匯入的工作與現有工作的名稱相同，則匯入工作的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

啟動變更工作密碼精靈

對於非本機工作，您可在指定必須在其下執行工作的帳戶。您可在建立工作期間或在現有工作的內容中指定帳戶。若根據組織安全指示使用指定帳戶，這些指示可能不實需要變更帳戶密碼。當帳戶密碼過期且您設定了新密碼，工作將無法啟動直到您在工作內容中指定新的有效密碼。

變更工作密碼精靈可讓您自動在指定帳戶的所有工作中以新密碼取代密碼。或者，您可在各工作的內容中手動變更此密碼。

若要啟動變更工作密碼精靈：

1. 在主功能表中，轉至 **工作**。

2. 點擊**管理啟動工作的帳戶憑證**。

   遵照精靈的說明。

步驟 1。指定憑證

指定目前在您的系統中有效的新憑據。當您切換至精靈的下一步時，Open Single Management Platform會檢查指定帳戶名稱是否符合各個非本機工作內容中的帳戶名稱。若帳戶名稱相符，則工作內容中的密碼將自動取代為新的。

若要指定新帳戶，請選取選項：

- **使用目前帳戶**

  精靈會使用您目前登入OSMP主控台的帳戶名稱。接著在**在工作中使用的目前密碼**欄位手動指定帳戶密碼。

- **指定不同帳戶**

  指定必須啟動工作的帳戶名稱。接著在**在工作中使用的目前密碼**欄位指定帳戶密碼。

若您填寫**先前密碼(可選，如果您要使用目前密碼更換它)**欄位，Open Single Management Platform僅會對已找到帳戶名稱與密碼的工作取代密碼。取代會自動執行。在所有其他情況下，您必須選擇進行精靈的下個步驟。

步驟 2：選取要採取的動作

若您未在精靈的第一步指定舊密碼或指定的舊密碼與工作內容中的密碼不符，您必須對已找到的工作選擇要採取的動作。

若要為工作選擇操作：

1. 選取您要為其選擇操作之工作旁邊的核取方塊。
2. 執行以下操作之一：
   - 若要移除工作內容中的密碼，請點擊**刪除憑證**。
     工作會切換為在預設帳戶下執行。
   - 若要用新的密碼取代，請點擊**即便舊密碼錯誤或未指定也強制密碼變更**。
   - 若要取消密碼變更，請點擊**未選取行動**。

所選操作會在您移至精靈的下一步時套用。

步驟 3：檢視結果

在精靈的最後步驟中，檢視各個已找到工作的結果。要完成精靈，請點擊**完成**按鈕。

檢視儲存在管理伺服器中的工作執行結果

Kaspersky Next XDR Expert 可讓您檢視群組工作、特定裝置的工作及管理伺服器工作的結果。

要檢視工作結果：

在工作屬性視窗中，前往 **結果** 索引標籤。

查看從屬管理伺服器的工作結果：

1. 在工作內容視窗中，選取**一般**區域。
2. 點擊**結果**連結開啟**工作結果**視窗。
3. 點擊**來自從屬伺服器的統計資訊**。
4. 選取要顯示其**工作結果**視窗的次要伺服器。

Kaspersky Endpoint Security 裝置掃描群組工作的手動設定

如果自動指定的群組掃描工作排程不適合您的組織，您必須根據組織採用的工作場所規則手動設定最方便的排程。

例如，工作被分配**在星期五下午 7:00 執行**排程，並且不選取**執行錯過的工作**核取方塊。這意味著如果組織中的裝置在星期五關閉，例如在下午 6:30，裝置掃描工作將永遠不會被執行。在這種情況下，您需要手動設定群組掃描工作。

管理偵測和回應工作

管理程式主控台時，您可以使用工作來執行各種操作。例如，您可以匯入資產或將KUMA事件資訊匯出到TSV檔案。

檢視工作表

工作表包含已建立工作的清單，位於程式主控台視窗的 **工作 → Detection and Response** 區段。您可以檢視您（目前使用者）所建立的工作。

具有主管理員角色的使用者可以檢視所有使用者的工作。

工作表包含以下資訊：

- **狀態**— 工作的狀態。可以為工作指派下列狀態之一：
  - *綠點閃爍*— 工作處於作用中狀態。
  - **已完成**— 工作已完成。
  - **取消**— 使用者取消了工作。
  - **錯誤**— 由於錯誤，工作未完成。如果將滑鼠停留在感嘆號圖示上，則會顯示錯誤訊息。
- **工作**—工作類型。程式提供以下類型的工作：
  - **匯出事件**— 匯出事件。
  - **在後台執行查詢** - 在後台執行SQL查詢。
  - **Threat Lookup**— 請求Kaspersky Threat Intelligence Portal的資料。
  - **回溯掃瞄** — 重播事件的工作。
  - **OSMP資產匯入**— 從卡巴斯基安全管理中心伺服器匯入資產資料。
  - **匯入帳戶**— 從Active Directory匯入使用者資料。
  - **KICS for Networks資產匯入**— 從KICS for Networks匯入資產資料。
  - **儲存庫更新**— 更新KUMA儲存庫以從設定中指定的來源接收資源包。
  - **分割區備份** 備份分割區，並將備份檔案儲存至指定路徑。
  - **從備份還原分割區** 從備份副本還原分割區。
  - **匯入分割區** 從外部 KUMA 安裝匯入分割區。

- **建立者**— 建立工作的使用者。如果工作是自動建立的，則此直欄將顯示**排定的工作**。
  此直欄僅對具有一般管理員和租用戶管理員角色的使用者顯示。
- **建立時間**— 工作建立時間。
- **更新時間** — 工作上次更新的時間。
- **租用戶**— 啟動工作的租用戶名稱。

工作日期格式取決於應用程式設定中選擇的在地化語言。可用的日期格式選項：

- 英文在地化：YYYY-MM-DD。
- 俄文在地化：DD.MM.YYYY。

檢視工作執行結果

若要檢視工組的結果：

1. 在主功能表中，前往 **工作 → Detection and Response**。
   工作表隨即顯示。
2. 按一下**工作**直欄中包含工作類型的連結。
   將顯示此工作類型可用的操作清單。
3. 選擇**顯示結果**。

   工作結果視窗隨即開啟。

重新啟動工作

若重新啟動工作：

1. 在主功能表中，前往 **工作 → Detection and Response**。
   工作表隨即顯示。
2. 選取您要重新啟動的工作旁邊的核取方塊。
3. 點擊**重新啟動**按鈕。

   工作將重新啟動。

應用程式標籤

Kaspersky Next XDR Expert 可讓您為應用程式登錄資料中的應用程式加上標籤。標籤是應用程式標誌，可以用於分組或尋找應用程式。分配給應用程式的標籤可以作為裝置分類中的條件。

例如，您可以建立 [瀏覽器] 標籤，並將其指派給所有瀏覽器，例如 Microsoft Internet Explorer®、Google Chrome、Mozilla Firefox。

建立應用程式標籤

要建立應用程式標籤：

1. 在主功能表中，轉至 **軟體管理 → 第三方應用程式 → 應用程式標籤**。
2. 點擊**新增**。
   新標籤視窗開啟。
3. 輸入標籤名稱。
4. 點擊**確定**儲存變更。

新標籤出現在應用程式標籤清單。

重命名應用程式標籤

要重命名應用程式標籤：

1. 在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式標籤**。
2. 選取您要重新命名之標籤旁的核取方塊，接著點擊**編輯**。
   標籤內容視窗開啟。
3. 變更標籤名稱。
4. 點擊**確定**儲存變更。

更新的標籤出現在應用程式標籤清單。

分配標籤到應用程式

要分配一個或多個標籤到一個應用程式：

1. 在主功能表中，轉至 **軟體管理 → 第三方應用程式 → 應用程式登錄資料**。
2. 點擊您要分配標籤的應用程式名稱。
3. 選取**標籤**頁簽。
   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**指派的標籤**欄中的核取方塊。

4. 對於要指派的標籤，請在**指派的標籤**欄中選取核取方塊。
5. 按一下**儲存**以儲存變更。

標籤被分配到應用程式。

從應用程式上刪除分配的標籤

要從應用程式刪除一個或多個標籤：

1. 在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式登錄資料**。
2. 點擊您要刪除標籤的應用程式名稱。
3. 選取**標籤**頁簽。

   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**指派的標籤**欄中的核取方塊。
4. 對於您要移除的標記，請不要選取**指派的標籤**欄中的核取方塊。
5. 按一下**儲存**以儲存變更。

標籤被從應用程式刪除。

已移除應用程式的標籤不被刪除。如果您想，您可以手動刪除它們。

刪除應用程式標籤

要刪除應用程式標籤：

1. 在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式標籤**。
2. 在清單中，選取您想要刪除的應用程式標籤。
3. 接著，點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**。

應用程式標籤被刪除。刪除的標籤被從其分配的所有應用程式上自動刪除。

在OSMP主控台中註冊卡巴斯基Industrial CyberSecurity for Networks應用程式

若要透過OSMP主控台開始使用Kaspersky Industrial CyberSecurity for Networks應用程式，必須先在OSMP主控台中註冊它。

要註冊 Kaspersky Industrial CyberSecurity for Networks 應用程式：

1. 確保完成以下操作：

   - 已下載並安裝 Kaspersky Industrial CyberSecurity for Networks Web 外掛程式。

     您可以稍後在等待 Kaspersky Industrial CyberSecurity for Networks Server 與管理伺服器同步時執行此操作。下載並安裝外掛程式後，OSMP主控台主功能表中將顯示**KICS for Networks**部分。

   - 在 Kaspersky Industrial CyberSecurity for Networks Web 介面中，已設定並啟用與 Kaspersky Next XDR Expert 的互動。詳情請參閱 Kaspersky Industrial CyberSecurity for Networks 線上說明。

2. 將安裝 Kaspersky Industrial CyberSecurity for Networks Server 的裝置從未分配裝置群組移動到受管理裝置群組：

   a. 在主功能表中，轉至 **資產管理 → 未指派的裝置**。

   b. 選中安裝了 Kaspersky Industrial CyberSecurity for Networks Server 的裝置旁邊的核取方塊。

   c. 點擊**移至群組**按鈕。

   d. 在管理群組層次結構中，選中**受管理裝置**群組旁邊的核取方塊。

   e. 點擊**移動**按鈕。

3. 開啟安裝了 Kaspersky Industrial CyberSecurity for Networks Server 的裝置的內容視窗。

4. 在裝置內容頁面的**一般**區域，選擇**不要中斷與管理伺服器的連線**選項，然後按一下**儲存**按鈕。

5. 在裝置內容頁面上，選擇**"應用程式"**區域。

6. 在**應用程式**區域中，選擇卡巴斯基安全管理中心網路代理。

7. 如果應用程式的目前狀態是*已停止*，等到它變為*正在執行*。

   這大約需要 15 分鐘。如果您尚未安裝 Kaspersky Industrial CyberSecurity for Networks Web 外掛程式，可以立即安裝。

8. 如果您想檢視 Kaspersky Industrial CyberSecurity for Networks 的統計資訊，您可以在儀表板上新增小部件。要新增小部件，請執行以下操作：

   a. 在主功能表中，「**監控**」→「**儀表板**」。

   b. 在儀表板上，點擊**新增或者還原網頁小部件**按鈕。

   c. 在開啟的小部件功能表中，選取**其它**。

   d. 選取您要新增的小部件：

      - KICS for Networks 部署圖
      - 有關 KICS for Networks 伺服器的資訊
      - KICS for Networks 的最新事件
      - KICS for Networks 中存在問題的裝置

- KICS for Networks 中的緊急事件
- KICS for Networks 中的狀態

9. 要繼續前往 Kaspersky Industrial CyberSecurity for Networks 網頁介面，請執行以下操作：

   a. 在主功能表中，轉至**KICS for Networks→ 搜尋**。

   b. 點擊**查找事件或裝置**按鈕。

   c. 在開啟的**查詢參數**視窗中，點擊**伺服器**欄位。

   d. 從與 Kaspersky Next XDR Expert 整合的伺服器下拉式清單中選擇 Kaspersky Industrial CyberSecurity for Networks 伺服器，然後點擊**尋找**按鈕。

   e. 點選Kaspersky Industrial CyberSecurity for Networks伺服器名稱旁邊的**轉至伺服器**連結。

   Kaspersky Industrial CyberSecurity for Networks 登入頁面將顯示。

   要登入 Kaspersky Industrial CyberSecurity for Networks 網頁介面，您需要提供應用程式使用者帳戶憑據。

管理使用者和使用者角色

該部分描述了使用者和使用者角色，並提供建立和修改它們、分配角色和群組到使用者以及關聯政策設定檔到角色的說明。

關於使用者帳戶

Kaspersky Next XDR Expert 可讓您管理使用者帳戶和安全群組。該應用程式支援四種帳戶類型：

- 組織員工的帳戶。在輪詢組織的網域控制器時管理伺服器擷取資料的網域使用者帳戶。
- 本機使用者帳戶。受管理裝置上的本機帳戶，以及安裝了管理伺服器的裝置上的本機帳戶。
- Kaspersky Next XDR Expert 的內部使用者帳戶。您可以建立內部使用者的帳戶。這些帳戶僅在 Kaspersky Next XDR Expert 內使用。
- 服務帳戶。這些帳戶僅用於將Kaspersky Next XDR Expert服務連線到管理伺服器。服務帳戶在解決方案已部署時自動新增，無法刪除或變更。這些帳戶的權限和角色也無法變更。您無法使用服務帳號登入OSMP主控台。

Linux 作業系統中的本機使用者帳戶和 kladmins 本機群組無法用於存取 Open Single Management Platform 中的 OSMP 主控台。kladmins群組只能包含用於啟動Open Single Management Platform服務的帳戶。組織員工在設定網域身分驗證後，即可使用自己的使用者帳戶登入。

OSMP主控台中的預設身分驗證方法是輸入使用者名稱、密碼以及用於雙因素驗證的附加一次性安全代碼。從Kaspersky Next XDR Expert 2.0開始，雙因素驗證會自動啟用，並且預設停用登入時設定雙因素驗證的選項。

您可以透過Kerberos協定設定網域身分驗證。網域身份驗證可讓您在OSMP主控台中啟用安全身份驗證，而無需在企業網路上重新輸入密碼（單一登入）。

要檢視使用者帳戶和安全群組表：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**。
2. 選擇**使用者**或**群組**頁簽。

使用者或安全群組表將開啟。

如果要僅使用內部、本機或網域使用者或群組檢視表格，請將**帳戶類型**篩選條件設定為相應的值。

如果使用者表包含超過 50,000 個使用者，則僅顯示前 50,000 個使用者，其餘使用者將不顯示。

關於用於角色

使用者角色（也叫*角色*）是包含一組權限集的物件。角色可以與安裝在使用者裝置上的 Kaspersky 應用程式設定關聯。您可以在管理伺服器階層中任何層級或在指定物件層級，指派角色給使用者集或安全群組集。

如果您透過包含虛擬管理伺服器的管理伺服器階層管理裝置，請注意您只能從實體管理伺服器建立、修改或刪除使用者角色。然後，您可以將使用者角色傳播到從屬管理伺服器，包括虛擬伺服器。

您可以關聯使用者角色到政策設定檔。若使用者獲派一個角色，此使用者會取得執行工作職能必要的安全設定。

一個使用者角色可以與特定管理群組中的裝置使用者關聯。

使用者角色範圍

*使用者角色範圍*是使用者和管理群組的組合。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

使用角色的好處

使用角色的好處之一是您不必為每個受管理裝置或使用者指定安全設定。公司中的使用者和裝置數量可能相當龐大，但需要不同安全設定的職務說明數量則少得多。

與使用政策設定檔的不同點

政策設定檔是為每個 Kaspersky 應用程式建立的政策的內容。角色與許多為不同應用程式建立的政策設定檔相關聯。因此，角色是聯合特定使用者類型的設定到一處的方法。

設定應用程式功能的存取權限。角色型存取控制

Kaspersky Next XDR Expert 提供角色型存取控制功能，可控制對 Kaspersky Next XDR Expert 功能及受管理 Kaspersky 應用程式的存取權限。

您可以透過下列其中一種方式，為 Kaspersky Next XDR Expert 使用者設定應用程式功能的存取權限：

- 透過為每個使用者或使用者群組單獨設定權限。
- 透過使用一群組預先定義的權限建立標準使用者角色並根據使用者的職責範圍將這些角色分配給使用者。

使用者角色的應用旨在簡化和縮短配置使用者對應應用程式功能存取權限的常規過程。角色內的存取權限根據標準工作和使用者的職責範圍設定。

可為使用者角色分配與其各自的目的對應的名稱。您可在程式中建立無限數量的角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色並自己配置所需的權限。

應用程式功能的存取權

下表顯示 Kaspersky Next XDR Expert 的功能，以及管理相關工作、報告及設定和執行相關使用者操作的存取權限。

要執行表中列出的使用者操作，使用者必須具有操作旁邊指定的權限。

讀取、**寫入**和**執行**權限適用於任何工作、報告或設定。除了這些權限外，使用者還必須具有**對裝置分類執行操作**的權限，才能管理裝置分類上的工作、報告或設定。

表中缺少的所有工作、報告、設定和安裝套件均屬於**一般功能：基本功能**的功能區域。

應用程式功能的存取權

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：對管理群組的管理功能	**寫入**	• 將裝置新增到管理群組：**寫入** • 從管理群組中刪除裝置：**寫入** • 將管理群組新增到另一個管理群組：**寫入** • 從另一個管理群組中刪除管理群組：**寫入**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：存取物件而不考慮它們的 ACL	**讀取**	獲得對所有物件的存取權限：**讀取**	沒有	沒有	**一般功能：存取物件而不考慮它們的 ACLs**功能區域均旨在用於稽核目的。此功能區域中的 **讀取** 權限可授予對所有物件的完整**讀取**存取權限。我們建議謹慎地將這些權利授予需要這些權利來履行正式職責的有限使用者。 無論其他權限如何，系統都會授予存取權限，即使已禁止對特定物件的讀取存取。
一般功能：基本功能	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 虛擬伺服器的裝置移動規則（建立、修改或刪除）：**寫入**、**對裝置分類執行操作** • 取得行動 (LWNGT) 通訊協定自訂憑證：**讀取** • 設定行動 (LWNGT) 通訊協定自訂憑證：**寫入** • 獲取 NLA 定義的網路清單：**讀取** • 新增、修改或刪除 NLA 定義的網路清單：**寫入** • 檢視群組的存取控制清單：**讀取** • 檢視作業系統記錄：**讀取**	• 「將更新下載至管理伺服器儲存區」 • 「提交報告」 • 「分發安裝套件」 • 「在從屬管理伺服器上遠端安裝應用程式」	• 「防護狀態報告」 • 「威脅報告」 • 「受感染最嚴重的裝置報告」 • 「病毒資料庫狀態報告」 • 「錯誤報告」 • 「網路攻擊報告」 • 「已安裝的外圍防禦應用程式的摘要報告」 • 「已安裝的應用程式類型概要報告」 • 「受感染的裝置使用者報告」 • 「事件報告」 • 「事件報告」 • 「發佈點活動報告」 • 「從屬管理伺服器的報告」 • 「裝置控制項事件報告」 • 「弱點報告」 • 「禁止的應用程式報告」 • 「Web控制項報告」 • 「受管理裝置加密狀態報告」 • 「大容量儲存裝置加密狀態報告」 • "加密磁碟機存取權限報告" • 「檔案加密錯誤報告」 • 「封鎖存取加密檔案的報告」 • 「有效使用者權限報告」 • 「權限報告」	沒有
一般功能：刪除的物件	• **讀取** • **寫入**	• 檢視資源回收桶中已刪除的物件：**讀取** • 從資源回收桶中刪除物件：**寫入**	沒有	沒有	沒有
一般功能：事件處理	• **刪除事件** • **編輯事件通知設定** • **編輯事件記錄設定** • **寫入**	• 變更事件註冊設定：**編輯事件記錄設定** • 變更事件通知設定：**編輯事件通知設定** • 刪除事件：**刪除事件**	沒有	沒有	設定： • 儲存在資料庫中的最大事件數量 • 儲存已刪除裝置中的事件時段
一般功能：管理伺服器上的操作	• **讀取** • **寫入** • **執行**	• 指定適用於網路代理連線之管理伺服器的管理連接埠：**寫入**	• 「備份管理伺服器資料」 • 「資料庫	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
	• **修改物件 ACL** • **對裝置分類執行操作**	• 指定在管理伺服器上啟動的啟動代理連接埠：**寫入** • 指定在管理伺服器上啟動的行動啟動代理連接埠：**寫入** • 指定用於發佈獨立套件之網頁伺服器的連接埠：**寫入** • 指定用於發佈 MDM 設定檔的網頁伺服器的連接埠：**寫入** • 指定管理伺服器的SSL連接埠以透過OSMP主控台進行連線：**寫入** • 指定用於行動連線之管理伺服器的管理連接埠：**寫入** • 指定儲存在管理伺服器資料庫的事件最大數量：**寫入** • 指定管理伺服器可以傳送的最大事件數：**寫入** • 指定管理伺服器可以傳送事件的時段：**寫入**	維護」		
一般功能：**Kaspersky 軟體部署**	• **管理 Kaspersky 修補程式** • **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	核准或拒絕安裝修補程式：**管理 Kaspersky 修補程式**	沒有	• 「虛擬管理伺服器產品授權金鑰使用報告」 • 「Kaspersky 軟體版本報告」 • 「不相容的應用程式報告」 • 「Kaspersky 軟體模組更新版本報告」 • 「防護部署報告」	安裝套件： "Kaspersky"
一般功能：**金鑰管理**	• **匯出金鑰檔案** • **寫入**	• 匯出金鑰檔案：**匯出金鑰檔案** • 修改管理伺服器產品授權金鑰設定：**寫入**	沒有	沒有	沒有
一般功能：**強制報告管理**	• **讀取** • **寫入**	• 建立報告，而不考慮其 ACL：**寫入** • 不論報告的 ACL 為何都加以執行：**讀取**	沒有	沒有	沒有
一般功能：**管理伺服器的層次結構**	**配置管理伺服器的層次結構**	• 註冊、更新或刪除從屬管理伺服器：**配置管理伺服器的層次結構**	沒有	沒有	沒有
一般功能：**使用者權限**	**修改物件 ACL**	• 變更任何物件的「安全性」屬性：**修改物件 ACL** • 管理使用者角色：**修改物件 ACL** • 管理內部使用者：**修改物件 ACL** • 管理安全群組：**修改物件 ACL** • 管理別名：**修改物件 ACL**	沒有	沒有	沒有
一般功能：**虛擬管理伺服器**	• **管理虛擬管理伺服器** • **讀取** • **寫入**	• 取得理虛擬管理伺服器的清單：**讀取** • 取得虛擬管理伺服器的資訊：**讀取**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
	• **執行** • **對裝置分類執行操作**	• 建立、更新或刪除虛擬管理伺服器：**管理虛擬管理伺服器** • 將虛擬管理伺服器移動到另一個群組：**管理虛擬管理伺服器** • 設定管理虛擬伺服器權限：**管理虛擬管理伺服器**			
一般功能：**加密金鑰管理**	**寫入**	核准在訓練模式下啟動常規程式加密金鑰：**寫入**	沒有	沒有	沒有
系統管理：**弱點和修補程式管理**	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 檢視協力廠商修補程式屬性：**讀取** • 變更協力廠商修補程式屬性：**寫入**	• 「修復弱點」 • 「安裝必要更新並修復弱點」	「軟體更新報告」	沒有

預先定義的使用者角色

指派給 Kaspersky Next XDR Expert 使用者的使用者角色，可為這些使用者提供一組應用程式功能的存取權限。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色並自己配置所需的權限。Kaspersky Next XDR Expert 中部分預先定義的使用者角色可與特定職位相關聯，例如 **稽核員**、**安全官**、**主管**。這些角色的存取權限會根據標準工作和相關職位的職責範圍預先配置。下表顯示角色可以如何與特定職位建立關聯。

特定職位的角色範例

角色	敘述
稽核員	允許對所有類型報告的所有操作、所有檢視操作，包含檢視已刪除的物件（在**已刪除的物件**區域授予**讀取**與**寫入**權限）。不允許進行其他操作。您可以分配該角色到執行您組織的稽核的人。
管理者	允許所有檢視操作，不允許其他操作。您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
安全官	允許所有檢視操作，允許報告管理；在**系統管理**：**連線**區域授予有限的權限。您可以分配該角色到負責您組織的 IT 安全的安全官。

下表顯示指派給每個預先定義使用者角色的存取權限。

預先定義使用者角色的存取權限

角色	敘述
基本角色	
管理伺服器管理員	允許在以下功能區域中進行所有操作： • **一般功能**： • **基本功能** • **加密金鑰管理** • **事件處理** • **管理伺服器的層次結構** • **虛擬管理伺服器** • **系統管理**： • **連線** • **設備清查** • **軟體清查**

角色	敘述
管理伺服器憑證運算子	授予以下所有功能區域的**讀取**和**執行**權限： • **一般功能**： • **基本功能** • **加密金鑰管理** • **虛擬管理伺服器** • **系統管理**： • **連線** • **設備清查** • **軟體清查**
稽核員	允許在以下功能區域中進行所有操作，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **刪除物件** • **管理報告** 您可以分配該角色到執行您組織的稽核的人。
安裝管理員	允許在以下功能區域中進行所有操作，在**一般功能**： • **基本功能** • **佈署 Kaspersky 應用程式** • **產品授權金鑰管理** 在**一般功能：虛擬管理伺服器**功能區域中授予**讀取**和**執行**權限。
安裝運算子	授予以下所有功能區域的**讀取**和**執行**權限，位於**一般功能**中： • **基本功能** • **Kaspersky 軟體部署**（也會在此區域授予**管理 Kaspersky Lab 修補程式**權限） • **虛擬管理伺服器**
Kaspersky Endpoint Security 管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。
Kaspersky Endpoint Security 運算子	授予以下所有功能區域的**讀取**和**執行**權限： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能
一般管理員	允許功能區域內的所有操作，以下區域*除外*，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **管理報告** 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。
主要運算子	授予以下所有功能區域的**讀取**和**執行**（如適用）權限： • **一般功能**： • **基本功能** • **刪除物件** • **管理伺服器操作** • **佈署 Kaspersky 應用程式** • **虛擬管理伺服器** • Kaspersky Endpoint Security 區域，包括所有功能
行動裝置管理管理員	允許在**一般功能：基本功能**功能區域中的所有操作。
安全官	允許在以下功能區域中進行所有操作，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **管理報告** 在**系統管理：連線**功能區域中，授予**讀取**、**寫入**、**執行**、**將來自裝置的檔案儲存到管理員的工作站**以及**對裝置分類執行操作**的權限。 您可以分配該角色到負責您組織的 IT 安全的安全官。
自助服務入口使用者	允許**行動裝置管理：自助服務入口**功能區域中的所有操作。此功能僅適用於卡巴斯基安全管理中心 11 或更新版本。

角色	敘述
管理者	在**一般功能**：**不受 ACL 限制地存取物件**及**一般功能**：**強制報告管理**功能區域中，授予**讀取**權限。 您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
XDR角色	
一般管理員	允許在以下XDR功能區域中進行所有操作： • **警示和事件** • **偵測和回應** • **常規程式和回應** • **管理資產** • **IAM** • **租用戶** • **卡巴斯基整合** • **協力廠商整合** • **產品授權**
租用戶管理員	允許在以下XDR功能區域中進行所有操作： • **警示和事件** • **偵測和回應** • **常規程式和回應** • **管理資產** • **IAM** • **租用戶** • **卡巴斯基整合** • **協力廠商整合** • **產品授權** 此角色相當於主管理員角色，但有一項限制。在KUMA中，租用戶管理員對預設物件的存取權限有限。
SOC管理員	授予XDR功能區域中的以下權限： • **偵測和回應**：**讀取**、**寫入** • **常規程式和回應**：**讀取**、**寫入**、**刪除** • **IAM**：**讀取使用者和角色**、**分配角色**和**列出使用者** • **租用戶**：**讀取**、**寫入** • **卡巴斯基整合**：**讀取**、**寫入** • **協力廠商整合**：**讀取**、**寫入** • **產品授權**：**讀取** • **資產管理**：**讀取**、**寫入**、**刪除**

角色	敘述
初級分析師	授予XDR功能區域中的以下權限： • **警示和事件**：**讀取**和**寫入** • **偵測和回應**：**讀取** • **資產管理**：**讀取** **檢視詳情** 讀取： • 檢視類別清單。 • 按類別新增裝置清單。 • 以CSV格式匯出裝置。 • 檢視符合活動分類標準的裝置。 • 檢視資產卡。 • 檢視自訂欄位清單。 • 檢視已歸檔裝置的事件保留期間（TTL）。 • 檢視資產稽核設定。 • 檢視與 Kaspersky Next XDR Expert 的整合設定。 • 檢視用於定義裝置活動狀態的閾值設定。 寫入： • 新增類別。 • 修改類別。 • 新增裝置。 • 修改裝置（包括類別）。 • 對 Kaspersky Next XDR Expert 裝置執行強制同步。 • 手動執行活動分類。 • 新增資產自訂欄位。 • 修改資產自訂欄位。 • 修改已歸檔裝置的事件保留期間（TTL）。 • 新增資產審核設定。 • 修改資產審核設定。 • 複製資產審核設定。 • 新增與 Kaspersky Next XDR Expert 的整合設定。 • 修改與 Kaspersky Next XDR Expert 的整合設定。 • 修改用於定義裝置活動狀態的閾值設定。 刪除： • 刪除類別。 • 將裝置歸檔。 • 刪除資產自訂欄位。 • 刪除資產稽核設定。 • **IAM** ：**讀取使用者和角色**和**列出使用者** • **租用戶**：**讀取** • **卡巴斯基整合**：**讀取** • **協力廠商整合**：**讀取** • **產品授權**：**讀取**

角色	敘述
二級分析師	授予XDR功能區域中的以下權限： • **警示和事件**：**讀取**和**寫入** • **偵測和回應**：**讀取** • **常規程式與回應**：**讀取**、**寫入**、**執行** • **管理資產** • **IAM** ：**讀取使用者和角色**和**列出使用者** • **租用戶**：**讀取** • **卡巴斯基整合**：**讀取** • **協力廠商整合**：**讀取** • **產品授權**：**讀取**
一級分析師	授予XDR功能區域中的以下權限： • **警示和事件**：**讀取**和**寫入** • **偵測和回應**：**讀取** • **常規程式與回應**：**讀取**、**寫入**、**執行** • **資產管理。** • **IAM** ：**讀取使用者和角色**和**列出使用者** • **租用戶**：**讀取** • **卡巴斯基整合**：**讀取** • **協力廠商整合**：**讀取** • **產品授權**：**讀取** 此角色對應於二級分析師角色，但有限制。在KUMA中，一級分析師只能修改自己的物件。

角色	敘述
SOC管理員	授予XDR功能區域中的以下權限： • **警示和事件**：**讀取**和**寫入** • **偵測和回應**：**讀取** • **常規程式和回應**：**讀取** • **資產管理**：**讀取** **檢視詳情** 讀取： • 檢視類別清單。 • 按類別新增裝置清單。 • 以CSV格式匯出裝置。 • 檢視符合活動分類標準的裝置。 • 檢視資產卡。 • 檢視自訂欄位清單。 • 檢視已歸檔裝置的事件保留期間（TTL）。 • 檢視資產稽核設定。 • 檢視與 Kaspersky Next XDR Expert 的整合設定。 • 檢視用於定義裝置活動狀態的閾值設定。 寫入： • 新增類別。 • 修改類別。 • 新增裝置。 • 修改裝置（包括類別）。 • 對 Kaspersky Next XDR Expert 裝置執行強制同步。 • 手動執行活動分類。 • 新增資產自訂欄位。 • 修改資產自訂欄位。 • 修改已歸檔裝置的事件保留期間（TTL）。 • 新增資產審核設定。 • 修改資產審核設定。 • 複製資產審核設定。 • 新增與 Kaspersky Next XDR Expert 的整合設定。 • 修改與 Kaspersky Next XDR Expert 的整合設定。 • 修改用於定義裝置活動狀態的閾值設定。 刪除： • 刪除類別。 • 將裝置歸檔。 • 刪除資產自訂欄位。 • 刪除資產稽核設定。 • **IAM** ：**讀取使用者和角色**和**列出使用者** • **租用戶**：**讀取** • **卡巴斯基整合**：**讀取** • **協力廠商整合**：**讀取** • **產品授權**：**讀取**

角色	敘述
批准人	授予XDR功能區域中的以下權限： • **警示和事件**：**讀取**、**寫入**、**關閉** • **偵測和回應**：**讀取** • **常規程式和回應**：**讀取**和**回應確認** • **資產管理**：**讀取** **檢視詳情** 讀取： • 檢視類別清單。 • 按類別新增裝置清單。 • 以CSV格式匯出裝置。 • 檢視符合活動分類標準的裝置。 • 檢視資產卡。 • 檢視自訂欄位清單。 • 檢視已歸檔裝置的事件保留期間（TTL）。 • 檢視資產稽核設定。 • 檢視與 Kaspersky Next XDR Expert 的整合設定。 • 檢視用於定義裝置活動狀態的閾值設定。 寫入： • 新增類別。 • 修改類別。 • 新增裝置。 • 修改裝置（包括類別）。 • 對 Kaspersky Next XDR Expert 裝置執行強制同步。 • 手動執行活動分類。 • 新增資產自訂欄位。 • 修改資產自訂欄位。 • 修改已歸檔裝置的事件保留期間（TTL）。 • 新增資產審核設定。 • 修改資產審核設定。 • 複製資產審核設定。 • 新增與 Kaspersky Next XDR Expert 的整合設定。 • 修改與 Kaspersky Next XDR Expert 的整合設定。 • 修改用於定義裝置活動狀態的閾值設定。 刪除： • 刪除類別。 • 將裝置歸檔。 • 刪除資產自訂欄位。 • 刪除資產稽核設定。 • **IAM**：**讀取使用者和角色以及列出使用者**。 • **租用戶**：**讀取** • **卡巴斯基整合**：**讀取** • **協力廠商整合**：**讀取** • **產品授權**：**讀取**

角色	敘述
稽核員	授予XDR功能區域中的以下權限： • **警示和事件**：**讀取** • **偵測和回應**：**讀取** • **常規程式和回應**：**讀取** • **資產管理**：**讀取** **檢視詳情** 讀取： • 檢視類別清單。 • 按類別新增裝置清單。 • 以CSV格式匯出裝置。 • 檢視符合活動分類標準的裝置。 • 檢視資產卡。 • 檢視自訂欄位清單。 • 檢視已歸檔裝置的事件保留期間（TTL）。 • 檢視資產稽核設定。 • 檢視與 Kaspersky Next XDR Expert 的整合設定。 • 檢視用於定義裝置活動狀態的閾值設定。 寫入： • 新增類別。 • 修改類別。 • 新增裝置。 • 修改裝置（包括類別）。 • 對 Kaspersky Next XDR Expert 裝置執行強制同步。 • 手動執行活動分類。 • 新增資產自訂欄位。 • 修改資產自訂欄位。 • 修改已歸檔裝置的事件保留期間（TTL）。 • 新增資產審核設定。 • 修改資產審核設定。 • 複製資產審核設定。 • 新增與 Kaspersky Next XDR Expert 的整合設定。 • 修改與 Kaspersky Next XDR Expert 的整合設定。 • 修改用於定義裝置活動狀態的閾值設定。 刪除： • 刪除類別。 • 將裝置歸檔。 • 刪除資產自訂欄位。 • 刪除資產稽核設定。 • **IAM** ：**讀取使用者和角色**和**列出使用者** • **租用戶**：**讀取** • **卡巴斯基整合**：**讀取** • **協力廠商整合**：**讀取** • **產品授權**：**讀取**

角色	敘述
與子事件的互動	授予XDR功能區域中的以下權限： • **子事件**：**讀取**和**寫入** • **IAM**：**讀取使用者和角色以及列出使用者**。 除了此角色之外，您還必須擁有以下其中一個XDR角色：主要管理員、租用戶管理員、初級分析師、二級分析師、一級分析師、SOC管理員、核准人、稽核員。
管理共享資源	授予編輯對共享租用戶中共享資源的存取權限。 除了此角色之外，您還必須擁有以下其中一個XDR角色：主管理員、租用戶管理員、初級分析師、二級分析師、一級分析師、SOC管理員、核准人。
讀取共享資源	授予讀取對共享租用戶中共享資源的存取權限。 除了此角色之外，您還必須擁有以下其中一個XDR角色：主管理員、租用戶管理員、初級分析師、二級分析師、一級分析師、SOC管理員、核准人。
SLA管理	授予編輯事件剩餘SLA時間的權限。 除了此角色之外，您還必須擁有以下其中一個XDR角色：主管理員、租用戶管理員、初級分析師、二級分析師、一級分析師、SOC管理員、核准人。
檢視通用儀表板版面配置	授予檢視通用儀表板版面配置的權限。 除了此角色之外，您還必須擁有以下其中一個XDR角色：主管理員、租用戶管理員、初級分析師、二級分析師、一級分析師、SOC管理員、核准人。
服務角色	
自動威脅響應器	授予服務帳戶響應威脅的權限。 存取權限根據 卡巴斯基安全管理中心 Linux 和受管理卡巴斯基應用程式基於角色的存取控制政策進行自動配置。 您只能將此角色分配給服務帳戶。 該角色無法編輯。

為特定物件分配存取權限

除了分配伺服器層級的存取權限，您可以設定對特定物件的存取，例如，對特定工作的存取。該應用程式允許您指定對以下物件類型的存取權限：

- 管理群組
- 工作
- 報告
- 裝置分類
- 事件分類

若要為特定物件分配存取權限：

1. 根據物件類型，在主功能表中，轉至相對應的部分：
   - **資產管理 → 群組的階層**
   - **工作**
   - **監控→報告**
   - **資產管理→裝置分類**
   - **監控 → 事件分類**
2. 開啟物件的內容，以將存取權限指派給物件。

   要開啟管理群組或工作的內容視窗，請按一下物件名稱。您可以使用工具列上的按鈕開啟其他物件的內容。
3. 在內容視窗中，開啟**存取權限**部分。

   使用者清單開啟。列出的使用者和安全群組具有物件的存取權限。預設情況下，如果您使用管理群組或伺服器的層次結構，則清單和存取權限是從父管理群組或主伺服器繼承的。
4. 為了能夠修改清單，啟用**使用自訂權限**選項。
5. 設定存取權限：
   - 使用**新增**和**刪除**按鈕修改清單。
   - 指定使用者或安全群組的存取權限。執行以下操作之一：
     - 如果要手動指定存取權限，請選擇使用者或安全群組，按一下**存取權限**按鈕，然後指定存取權限。
     - 如果你想分配使用者角色到使用者或安全群組，請選擇使用者或安全群組，按一下**角色**按鈕，然後選擇要分配的角色。
6. 點擊**儲存**按鈕。

物件的存取權限已設定好。

分配權限到使用者和群組

您可以授予使用者和安全群組對管理伺服器及您擁有管理外掛的卡巴斯基應用程式（例如，Windows版卡巴斯基 Endpoint Security）的不同功能的存取權限。

要將權限分配給使用者或使用者群組：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。
2. 在"**存取權限**"頁簽上，選中要對其分配權限的使用者或安全群組名稱旁邊的核取方塊，然後點擊"**存取權限**"按鈕。

   您不能同時選擇多個使用者或安全群組。如果您選擇了多個項目，**存取權限**按鈕將被停用。

3. 配置使用者或群組的權限集：

   a. 使用管理伺服器或其他卡巴斯基應用程式的功能擴展節點。

   b. 選擇所需功能或存取權限旁邊的**允許**或**拒絕**核取方塊。

      *示例 1：*選中**應用程式集成**節點旁邊的**允許**核取方塊，向使用者或群組授予對應用程式集成功能（**讀取**、**寫入**和**執行**）的所有可用存取權限。

      *示例 2：*展開**加密金鑰管理**節點，然後選中寫入權限旁邊**的允許**核取方塊，以授予使用者或群組對加密金鑰管理功能的**寫入**存取權限。

4. 配置存取權限集合後，點擊**確定**。

使用者或使用者群組的權限集將被設定。

管理伺服器（或管理群組）的權限被分成以下部分：

- 一般功能：
  - 對管理群組進行管理
  - 存取物件而不考慮它們的 ACLs
  - 基本功能
  - 刪除物件
  - 加密金鑰管理
  - 事件處理
  - 管理伺服器操作
  - 裝置標籤
  - 佈署 Kaspersky 應用程式
  - 產品授權金鑰管理
  - 管理報告
  - 伺服器層級
  - 使用者角色權限
  - 虛擬管理伺服器
- 行動裝置管理：
  - 一般
- 系統管理：
  - 連線
  - 設備清查

- 網路存取控制
- 作業系統部署
- 管理弱點和修補程式
- 遠端安裝
- 軟體清查

如果對權限未選取**允許**或**拒絕**，權限被認為是*未定義*：它在對使用者明確拒絕或允許之前被拒絕。

使用者權限是以下的集合：

- 使用者自己的權限
- 指派給該使用者的所有角色的權限
- 使用者所屬的所有安全群組的權限
- 指派給使用者所屬安全群組的所有角色的權限

如果至少一個權限集對權限**拒絕**，那麼使用者被拒絕該權限，即便其他集允許它或保持未定義。

您也可以將使用者和安全群組新增至使用者角色的範圍以使用管理伺服器的不同功能。與使用者角色相關聯的設定只會套用到屬於此角色的使用者的裝置，並且僅當這些裝置屬於與此角色相關聯的群組（包括子群組）時才會生效。

新增內部使用者帳戶

若要將新的內部使用者帳戶新增至 Kaspersky Next XDR Expert：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 點擊**新增**。
3. 在開啟的**新增使用者**視窗中，指定新使用者帳戶設定：
   - **名稱**。
   - **密碼**，供使用者連線至 Kaspersky Next XDR Expert 使用。
     密碼必須符合以下規則：
     - 密碼必須是 10 到 256 位字元長度。
     - 密碼必須包含以下組中三組的字元：
       - 大寫字母（A-Z）
       - 小寫字母 (a-z)

- 數字（0-9）
- 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- 密碼不得包含任何空白字元、Unicode 字元，或「.」在「@」之前的「.」與「@」組合。

若要檢視您輸入的字元，請按住**顯示**按鈕。

輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 3。您可以管理允許的密碼輸入嘗試次數，敘述在"變更允許的密碼輸入嘗試次數"。

如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。您僅可以透過變更密碼解鎖封鎖使用者。

4. 按一下**儲存**以儲存變更。
5. 如有必要，請為租用戶中建立的內部使用者帳戶指派角色。

新的使用者帳戶被新增到使用者清單中。

若要使用在OSMP主控台上建立的內部使用者帳戶登入，必須為該使用者帳戶指派角色。登入前，請確保內部使用者帳戶已被指派角色。否則，將會出現登入錯誤。

建立安全群組

要建立安全群組：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**群組**頁簽。
2. 點擊**新增**。
3. 在開啟的**建立安全群組**視窗中，為新安全群組指定以下設定：
   - **群組名稱**
   - **描述**
4. 按一下**儲存**以儲存變更。

新的安全群組被新增到群組清單中。

編輯內部使用者帳戶

若要在 Kaspersky Next XDR Expert 中編輯內部使用者帳戶：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 點擊您要編輯的使用者帳戶名稱。
3. 在開啟的使用者設定視窗中的**一般**頁籤，變更使用者帳戶設定：
   - **描述**
   - **完整名稱**
   - **電子郵件地址**
   - **主電話**
   - 為使用者連線至 Kaspersky Next XDR Expert **設定新密碼**。
     密碼必須符合以下規則：
     - 密碼必須是 10 到 256 位字元長度。
     - 密碼必須包含以下組中三組的字元：
       - 大寫字母（ A-Z ）
       - 小寫字母 (a-z)
       - 數字（ 0-9 ）
       - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密碼不得包含任何空白字元、Unicode 字元，或「.」在「@」之前的「.」與「@」組合。

     若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

     > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 3。您可以變更允許的嘗試次數；但是，出於安全原因，我們不建議您減少此數字。如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。您僅可以透過變更密碼解鎖封鎖使用者。
   - 如有必要，請切換開關按鈕至**已停用**，以禁止使用者連線到應用程式。您可以停用帳戶，例如，在員工離職後。
4. 在**雙步驟驗證**頁籤中，您可以指定此帳戶的安全設定。
5. 在**群組**頁籤，您可新增使用者至安全群組。
6. 在**裝置**頁籤，您可指派裝置給使用者。

7. 在**角色**頁籤，您可指派角色給使用者。

8. 按一下**儲存**以儲存變更。

更新的使用者帳戶出現在使用者清單。

變更使用者工作狀態

使用者工作狀態顯示您是否可以將警示和事件指派給該使用者。

使用者可以具有以下幾種狀態之一：

- **可用** - 使用者已準備好處理警示和事件。
- **忙碌**– 使用者尚未準備好處理警示和事件。警示和事件無法自動指派給該使用者。

預設情況下，當使用者登入OSMP主控台或KUMA主控台時，使用者的工作狀態會自動更新為**可用**。

您可以手動變更自己的工作狀態或目前登入使用者的工作狀態。

變更您自己帳戶的工作狀態

如果狀態為**可用**，則在帳戶名稱旁邊的主功能表中顯示為綠點（ ），如果狀態為**忙碌**，則顯示為紅點（ ）。

如果您想要變更目前工作狀態，請在上方窗格中，轉至帳戶設定，然後選擇要指派給帳戶的狀態。

變更內部使用者帳戶的工作狀態

只有當使用者目前已登入 OSMP Console 或 KUMA Console 時，才會在使用者設定視窗中顯示**工作狀態**欄位。
若要變更內部使用者的工作狀態，您必須具有以下其中一種XDR 角色：主管理員、租用戶管理員、SOC 管理員。

若要變更內部使用者的工作狀態：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**使用者**頁簽。
使用者清單開啟。

2. 按一下您要變更狀態的使用者帳戶名稱。
使用者設定視窗隨即開啟，並含有所選的**一般**頁籤。

3. 在**工作狀態**欄位中，選擇要指派的狀態：**可用**或**忙碌**。

4. 點擊**儲存**按鈕。

視窗隨即關閉，使用者的工作狀態將變更。

編輯安全群組

要編輯安全群組：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**群組**頁簽。
2. 點擊您要編輯的安全群組名稱。
3. 在開啟的群組設定視窗中，變更安全群組設定：
   - 在**一般**頁簽上，您可以變更**名稱**和**描述**設定。這些設定僅適用於內部安全群組。
   - 在**使用者**頁籤上，您可以進行以下操作：
     - 檢視群組使用者表格。
     - 將使用者新增至安全群組。為此，請按一下**新增**按鈕，然後在開啟的**新增使用者**窗格中，選取要新增的使用者帳戶旁的核取方塊，然後按一下**儲存**。

       在**新增使用者**窗格中，您可以依租用戶篩選使用者。為此，請將**租用戶所有者**篩選條件設定為所需值。

       只有內部使用者和內部安全群組才能將使用者新增至安全群組。

     - 從安全群組中刪除使用者。為此，請選取使用者帳戶名稱旁的核取方塊，按一下**刪除**，然後確認操作。
   - 在**角色**頁籤，您可指派角色給安全群組。
4. 按一下**儲存**以儲存變更。

變更被套用於安全群組。

為使用者或安全群組分配角色

對使用者或安全群組分配角色：

1. 在主功能表中，轉至**使用者和角色→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選擇要對其分配角色的使用者或安全群組的名稱。

   您可以選取多個名稱。
3. 在功能表行中，點擊**指派角色**按鈕。

   角色分配精靈啟動。
4. 按照精靈的說明進行操作：選擇要分配給所選使用者或安全群組的角色，然後選擇角色的範圍。

   *使用者角色範圍*是使用者和管理群組的組合。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

擁有處理管理伺服器權限集合的角色將被指派給使用者（或者多個使用者，或者安全群組）。在使用者或安全群組清單中，**已指派角色**列中會出現一個核取方塊。

新增使用者帳戶到內部安全群組

您僅可以新增內部使用者帳戶到內部安全群組。

要新增使用者帳戶到內部安全群組：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 選取您要新增到安全群組的使用者帳戶旁邊的核取方塊。
3. 點擊**指派群組**按鈕。
4. 在開啟的**指派群組**視窗中，選取您要向其新增使用者帳戶的安全群組。
5. 點擊**儲存**按鈕。

使用者帳戶被新增到安全群組。您還可以使用群組設定將內部使用者新增到安全群組。

將使用者指派為裝置所有者

有關將使用者指派為行動裝置所有者的資訊，請參閱Kaspersky Security for Mobile說明。

若要將使用者指派為裝置所有者：

1. 如果要指派連線到虛擬管理伺服器的裝置所有者，請先切換到虛擬管理伺服器：
   a. 在主功能表中，按一下目前管理伺服器名稱右側的 v 形箭號圖示（ ）。
   b. 選取所需的管理伺服器。
2. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
   使用者清單開啟。如果您目前已連線到虛擬管理伺服器，該清單會包括來自目前虛擬管理伺服器和主管理伺服器的使用者。
3. 按一下您要指派為裝置所有者的使用者帳戶名稱。
4. 在開啟的使用者設定視窗中，選擇**裝置**頁籤。
5. 點擊**新增**。
6. 從裝置清單中，選取您要分配給使用者的裝置。
7. 點擊**確定**。

所選的裝置被新增到分配給使用者的裝置清單。

您可在**資產管理 → 資產（裝置）**執行相同操作，方法是點擊您要指派之裝置的名稱，之後點擊**管理裝置所有者**連結。

設定雙步驟驗證

從Kaspersky Next XDR Expert 2.0開始，雙步驟驗證將自動啟用。不支援全域停用雙因素驗證的選項。此情景提供了在首次登入時配置雙因素驗證以及在管理伺服器上配置雙因素驗證設定的步驟。

階段

雙因素驗證的設定分階段進行：

1. **在裝置上安裝驗證應用程式**

   您可以安裝任何支援基於時間的一次性密碼演算法 (TOTP) 的應用程式，例如：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 驗證器
   - Aladdin 2FA
   - Rutoken OTP

   若要檢查Kaspersky Next XDR Expert是否支援您要使用的身分驗證應用程式，請為所有使用者或特定使用者啟用雙步驟驗證。

   其中步驟之一建議您指定由身分驗證器應用程式產生的安全代碼。如果成功，則Kaspersky Next XDR Expert支援選定的身分驗證器。

   > 我們強烈建議不要在與管理伺服器建立連線的同一台裝置上安裝身分驗證應用程式。

2. **將身分驗證器應用程式裝置上的時間與安裝了管理伺服器的裝置的時間同步**

   確保具有身分驗證應用程式的裝置上的時間和具有管理伺服器的裝置上的時間與UTC同步。為了提高準確性，我們建議在整個基礎設施中使用相同的NTP伺服器。否則，在設定雙因素驗證時可能會發生故障。

3. **為使用者帳號登入網頁主控台時設定雙因素驗證**

   登入網頁主控台並設定雙步驟驗證。

   如果您無法設定雙因素驗證，請聯絡具有一般功能：使用者權限功能區中**修改物件ACL**權限且已設定雙因素驗證的使用者，將您的帳戶新增至雙因素驗證允許清單中。

4. **在管理伺服器上設定雙因素驗證設定**

如果您已設定雙步驟驗證並具有**常規功能**：**一般功能**功能區域中使用者權限權限，則可以如下在管理伺服器上配置雙步驟驗證設定：

1. 檢視可在登入時設定雙步驟驗證的使用者清單：

   - 若要從頭開始安裝卡巴斯基Next XDR Expert 2.0：將所需的使用者新增到雙步驟身份驗證允許清單中，以便他們在首次登入時設定雙步驟身份驗證。
   - 要升級到Kaspersky Next XDR Expert 2.0：檢視雙步驟身份驗證允許清單，並刪除必須無法訪問管理伺服器的帳戶。

2. 排除不需要啟用雙因素驗證的使用者帳戶（可選）

   將使用者帳戶從雙因素驗證中排除，以便即使他們未設定雙因素驗證，也能登入管理伺服器。對於在身分驗證期間無法提供安全碼的整合帳戶，可能需要將帳戶從雙因素驗證中排除。整合帳戶用於透過OpenAPI執行指令碼。

3. 重設或刪除雙因素驗證密鑰（可選）

   當使用者無法存取其雙因素驗證裝置，或需要在新裝置上設定雙因素驗證時，您可以重設雙因素驗證密鑰。您也可以重設自己帳戶的密鑰。

   您可以刪除密鑰以完全阻止使用者登入網頁主控台並阻止其存取管理伺服器。

4. 編輯安全碼簽發者的名稱（可選）

   如果您有多個具有相似名稱的管理伺服器，則可能必須變更安全碼簽發者的名稱，以便更進一步識別不同的管理伺服器。

結果

完成此情境後：

- 雙因素驗證設定適用於您自己的帳戶以及需要存取管理伺服器的其他使用者帳戶。
- 整合帳戶將排除在雙因素驗證之外。

關於帳戶的雙因素驗證

Kaspersky Next XDR Expert為OSMP主控台的使用者提供雙步驟身分驗證。雙因素驗證基於RFC 6238標準執行（TOTP：基於時間的一次性密碼演算法）。

每次登入OSMP主控台時，都需要輸入使用者名稱、密碼和一次性安全碼。若要接收一次性安全碼，電腦或行動裝置上必須具有身分驗證器應用程式。

任何支援時效型一次性密碼演算法 (TOTP) 的身分驗證軟體都可以用作身分驗證應用程式，例如Google Authenticator。為了產生一次性安全碼，您必須將裝置上透過身分驗證應用程式設定的時間與管理伺服器裝置上設定的時間同步。為了提高準確性，我們建議在整個基礎設施中使用相同的NTP伺服器。

若要檢查Kaspersky Next XDR Expert是否支援您要使用的身分驗證應用程式，請嘗試使用此身分驗證應用程式設定雙步驟驗證。

其中步驟之一建議您指定由身分驗證應用程式產生的安全碼。如果成功，則Kaspersky Next XDR Expert支援選定的身分驗證器。

使用身分驗證應用程式產生密碼

驗證應用程式將產生安全碼，如下所示：

1. 管理伺服器會產生一個特殊的秘密金鑰和 QR 碼。
2. 您將產生的秘密金鑰或 QR 碼傳遞給驗證應用程式。
3. 驗證應用程式產生一次性使用的安全碼，您將其傳遞到管理伺服器的身分驗證視窗。

安全碼具有名為*簽發者名稱*的識別碼。安全碼簽發者名稱用作驗證應用程式中管理伺服器的識別碼。您可以變更安全碼簽發者名稱的名稱。安全碼簽發者名稱的預設值與管理伺服器的名稱相同。下次登入後，新的安全碼簽發者名稱將指派給管理伺服器。安全碼為一次性，有效期最長為 30 秒（具體時間可能會有所不同）。

強烈建議將秘密金鑰（或 QR 碼）儲存在安全的地方。如果您丟失了行動裝置，這將有助於您恢復對OSMP主控台的存取。

雙因素驗證具有以下功能：

- 從Kaspersky Next XDR Expert 2.0開始，雙步驟身分驗證將自動啟用，並且預設停用登入時配置雙步驟身分驗證的選項。只有包含在雙因素驗證允許清單中的使用者才能設定登入時執行雙因素驗證。
- 使用者僅可以為其帳戶啟用雙步驟身分驗證。
- 使用者可以從雙因素驗證中排除帳戶。對於無法接收一次性身份驗證安全碼的整合帳戶來說，這可能是必要的。整合帳戶用於透過OpenAPI執行指令碼以及執行KUMA指令碼。
- 若要重新產生雙因素身分驗證密鑰，使用者必須重設其自身帳戶的密鑰。
- 若要重設或刪除其他使用者帳戶的雙步驟身分驗證密鑰，該使用者必須擁有已設定雙步驟身分驗證的帳戶，並且在**常規功能**：**一般功能**功能區域中擁有使用者權限權限。
- 若要將其他使用者的帳戶從雙因素驗證中排除，或修改雙因素驗證允許清單，使用者必須擁有已設定雙因素驗證的帳戶，並且在**一般功能**: **一般功能**功能區域中擁有使用者權限的權限。
- 應該始終至少有一個使用者配置了雙因素驗證，以便該使用者可以管理雙因素驗證允許清單和排除清單。
- 雙步驟身分驗證僅在Kaspersky Next XDR Expert 2.0或更高版本中自動啟用。如果其他主管理伺服器或輔助管理伺服器執行的是1.4或更早版本，則它們的雙因素驗證設定將保持不變。
- 虛擬管理伺服器會繼承實體管理伺服器的雙因素驗證設定，因此，如果實體管理伺服器啟用了雙因素驗證，虛擬管理伺服器也會啟用該功能。您無法在虛擬管理伺服器上配置雙因素驗證設定。

為了確保使用雙因素驗證提供全面保護，不僅需要保護管理伺服器，還需要保護安裝該伺服器的裝置。為此，請參考強化指南建議。

在OSMP主控台登入時設定雙因素驗證密鑰

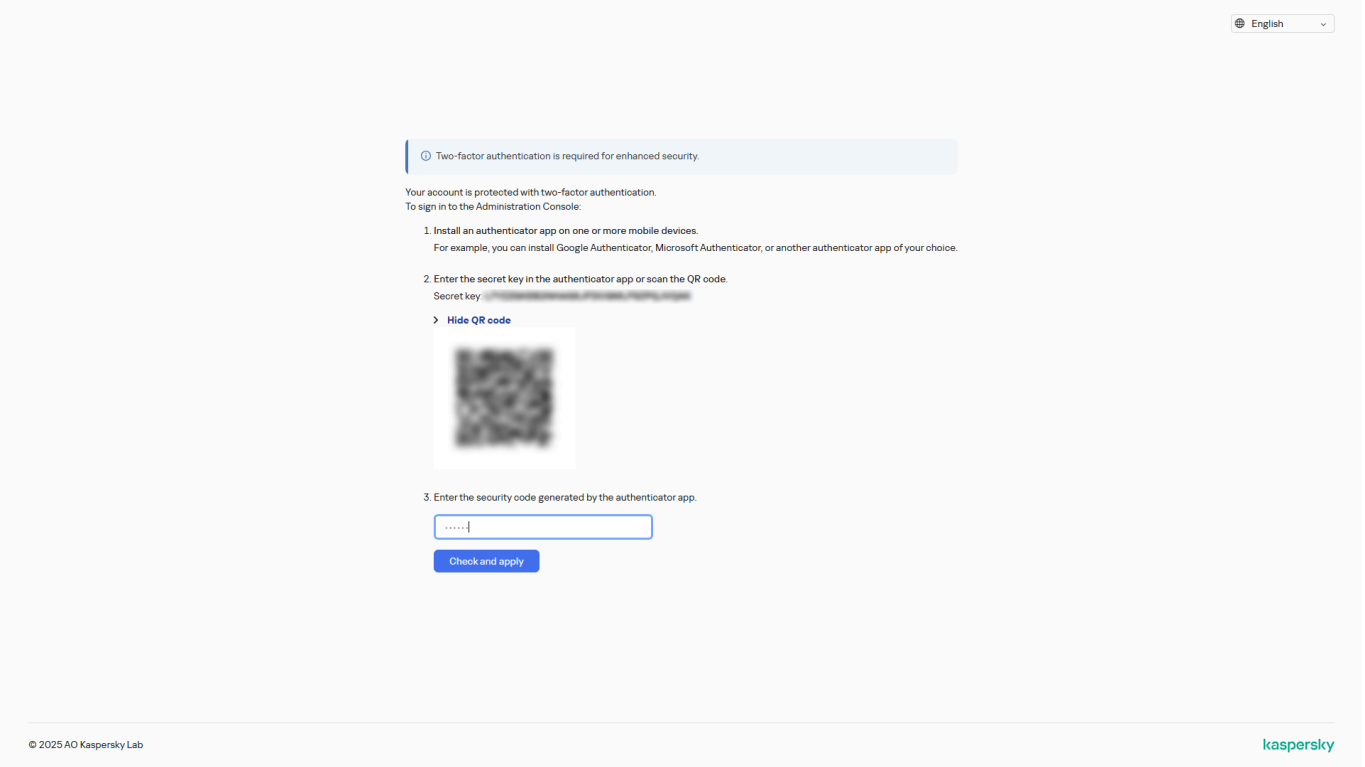
首次登入Kaspersky Next XDR Expert 2.0或更高版本時，將開啟設定雙步驟身份驗證的視窗。

要為帳戶設定雙因素驗證，請執行以下操作：

1. 請在行動裝置或電腦上安裝任何支援基於時間的一次性密碼演算法（TOTP）的應用程式，例如：
   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 驗證器
   - Aladdin 2FA
   - Rutoken OTP

   我們強烈建議不要在與管理伺服器建立連線的同一台裝置上安裝身分驗證應用程式。
2. 確保具有身分驗證應用程式的裝置上的時間和具有管理伺服器的裝置上的時間與UTC同步。為了提高準確性，我們建議在整個基礎設施中使用相同的NTP伺服器。
3. 使用行動裝置或電腦上的身份驗證應用程式生成一次性安全碼。為此，請執行下列其中一個步驟：
   - 在身分驗證應用程式中手動輸入雙步驟身分驗證密鑰。
   - 點擊**檢視 QR 碼**並使用身分驗證器應用程式掃描 QR 代碼。

行動裝置上將顯示一個6位數的一次性安全碼。



在OSMP主控台登入時設定雙因素驗證密鑰

4. 在開啟的**雙步驟驗證**視窗中，指定由身分驗證應用程式產生的安全碼，然後點擊**確認並套用**按鈕。

Rutoken OTP 設定

若您使用 Rutoken OTP，則需要一台已安裝 Rutoken OTP 應用程式的 Android 行動裝置。Android 行動裝置須滿足以下要求：

- 作業系統為 Android 7 或更新版本。
- NFC 模組可用且已啟用

在 Rutoken OTP 應用程式中，必須設定以下參數：

- 掃描雙步驟設定精靈中顯示的 QR 碼。
- 將時間間隔設定為 30 秒。
- 選取 SHA1 作為演算法。

若要設定 Rutoken OTP：

1. 將 Rutoken OTP 裝置放在有 NFC 模組的行動裝置旁。
2. 在 Rutoken OTP 應用程式中，按**連線權杖**。
3. 在 Rutoken OTP 應用程式中，按**配置設定**，然後按**儲存秘密金鑰**。

如果權杖成功連線到行動裝置，Rutoken OTP 應用程式將顯示下列狀態訊息：

- **權杖已連線。**
- **設定已配置。**
- **秘密金鑰已儲存。**

4. 在 Rutoken OTP 裝置上，按下按鈕。
   一個安全碼會顯示在此裝置上。
5. 在 OSMP 主控台的雙因素驗證視窗中，輸入安全碼。

至此，帳戶已完雙因素驗證設定。您可以根據您的權限存取管理伺服器。

如果您無法設定雙因素驗證，請聯絡在「**General features**: **一般功能**」功能區域中擁有使用者權限 權限且已設定雙因素驗證的使用者，將您的帳戶新增至雙因素驗證允許清單中。

允許使用者配置雙因素驗證

雙因素驗證允許清單是一份使用者清單，這些使用者可以在登入網頁主控台時對雙因素驗證進行初始設定。此清單包含未配置雙因素驗證的使用者帳戶。預設情況下，新使用者帳戶不包含在雙因素驗證允許清單中，這些帳戶必須由管理員新增至清單。如果新帳戶是用於執行OpenAPI指令碼的整合帳戶，則必須被從雙因素驗證中排除。

當使用者帳戶設定了雙因素驗證或被排除在雙因素驗證之外時，該帳戶將自動從雙因素驗證允許清單中刪除。

對於已設定雙因素驗證且在「**General features**: **一般功能**」功能區域中擁有使用者權限 權限的帳戶，可以手動修改雙因素驗證允許清單。

手動將使用者帳戶新增至允許清單：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在內容視窗的**雙步驟驗證**頁簽上，在**允許產生秘密金鑰的使用者**表中，按一下**新增**按鈕。
3. 在開啟的視窗中：
   a. 選取您要新增的使用者帳戶。
      只有未被排除在雙因素驗證之外且沒有雙因素驗證秘密金鑰的使用者才能被新增至允許清單。
   b. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。
   c. 儲存您的變更。

選定的使用者帳戶將新增到雙因素驗證允許清單中。下次登入時，用戶將能夠產生秘密金鑰。

在為使用者帳戶設定雙因素驗證之前，可以從雙因素驗證允許清單中刪除該帳戶。

手動從雙因素驗證允許清單中刪除使用者帳戶：

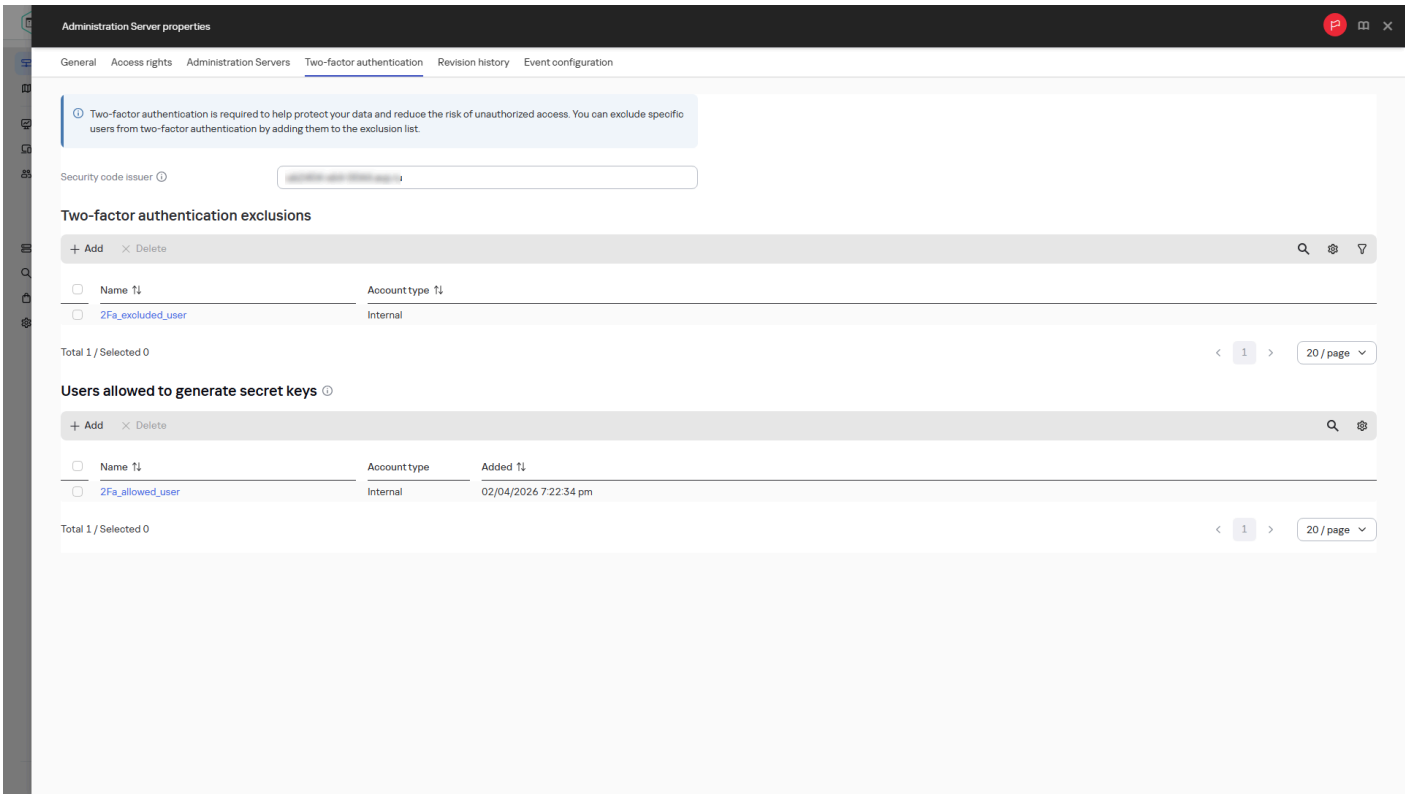
1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**頁籤上的**允許產生秘密金鑰的使用者**表中，選擇要刪除的使用者帳戶，然後按一下**刪除**。

3. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

選定的使用者帳戶將被從允許清單中刪除。



設定雙因素驗證允許清單

如果在管理伺服器上的活動工作階段期間，您的雙因素驗證秘密金鑰被其他使用者刪除，或者您自己重設了金鑰但沒有建立新金鑰，則修改允許清單的功能將被封鎖。

使用者帳戶也可以自動新增到雙因素驗證允許清單或從中刪除。

為其他帳戶重設雙因素身份驗證金鑰時，他們的帳戶會自動新增到雙因素身份驗證允許清單中，以便他們可以生成新的金鑰。

將 Kaspersky Next XDR Expert 從 1.4 版升級至 2.0 版或更新版本時，如果符合以下所有條件，使用者帳戶會自動新增至雙因素驗證允許清單：

- 使用者在功能區域 *一般功能：基本功能*中擁有"讀取"權限，該權限被直接（而非透過安全性群組）指派給使用者。具有此權限的使用者角色範圍必須包含所有受管理和未指派的裝置，並且必須在管理伺服器層級設定。
- 使用者未被排除在雙因素驗證之外。

- 使用者沒有雙因素驗證秘密金鑰。
- 先前版本的管理伺服器上未對所有使用者啟用雙重身分驗證。

即使僅未滿足其中一項條件，使用者也無法新增到雙因素驗證允許清單中。

> 升級或還原後，我們建議確保允許清單僅包含必須有權存取管理伺服器的使用者帳戶。審核允許清單並從中刪除任何其他帳戶。將用於透過 OpenAPI 執行指令碼的整合帳戶新增至排除清單中，以防止指令碼失敗。

如果滿足以下所有條件，則使用者帳戶在升級或恢復後將失去對管理伺服器的存取權限：

- 使用者在功能區 *一般功能：基本功能* 擁有透過安全性群組（不是直接指派給使用者）指派的"讀取"權限，或者根本沒有此權限。
- 使用者未被排除在雙因素驗證之外。
- 使用者沒有雙因素驗證秘密金鑰。
- 在舊版管理伺服器上，並未為所有使用者啟用雙因素驗證。

如有需要，可手動將這些帳戶新增至雙因素驗證允許清單中。

重置和刪除雙因素驗證秘密金鑰

當使用者無法存取其雙因素驗證裝置或需要在新裝置上設定雙因素驗證時，您可以重置秘密金鑰。重置秘密金鑰後，使用者可以再次登入網頁主控台並產生新的秘密金鑰。

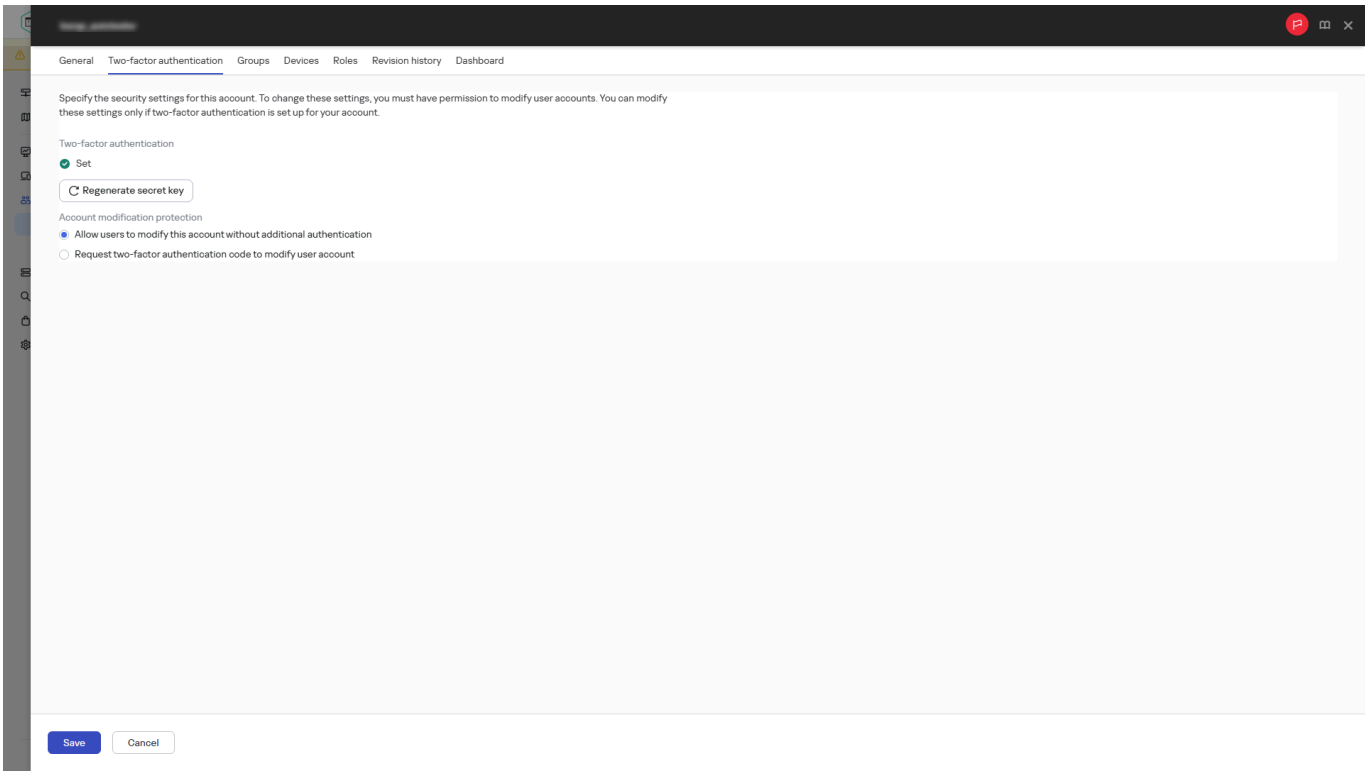
> 只有當您配置了雙因素驗證，並且在一般功能**一般功能**使用者權限**使用者權限修改物件 ACL**權限時，才能重置或刪除其他使用者帳戶的雙因素驗證秘密金鑰。您也可以重新產生自己的秘密金鑰。

重置帳戶的秘密金鑰：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 按一下您要為其重置秘密金鑰的使用者帳戶名稱。

3. 如果您想重置帳戶的秘密金鑰：

a. 在**雙步驟驗證**頁簽上，按一下**重新產生秘密金鑰**按鈕。

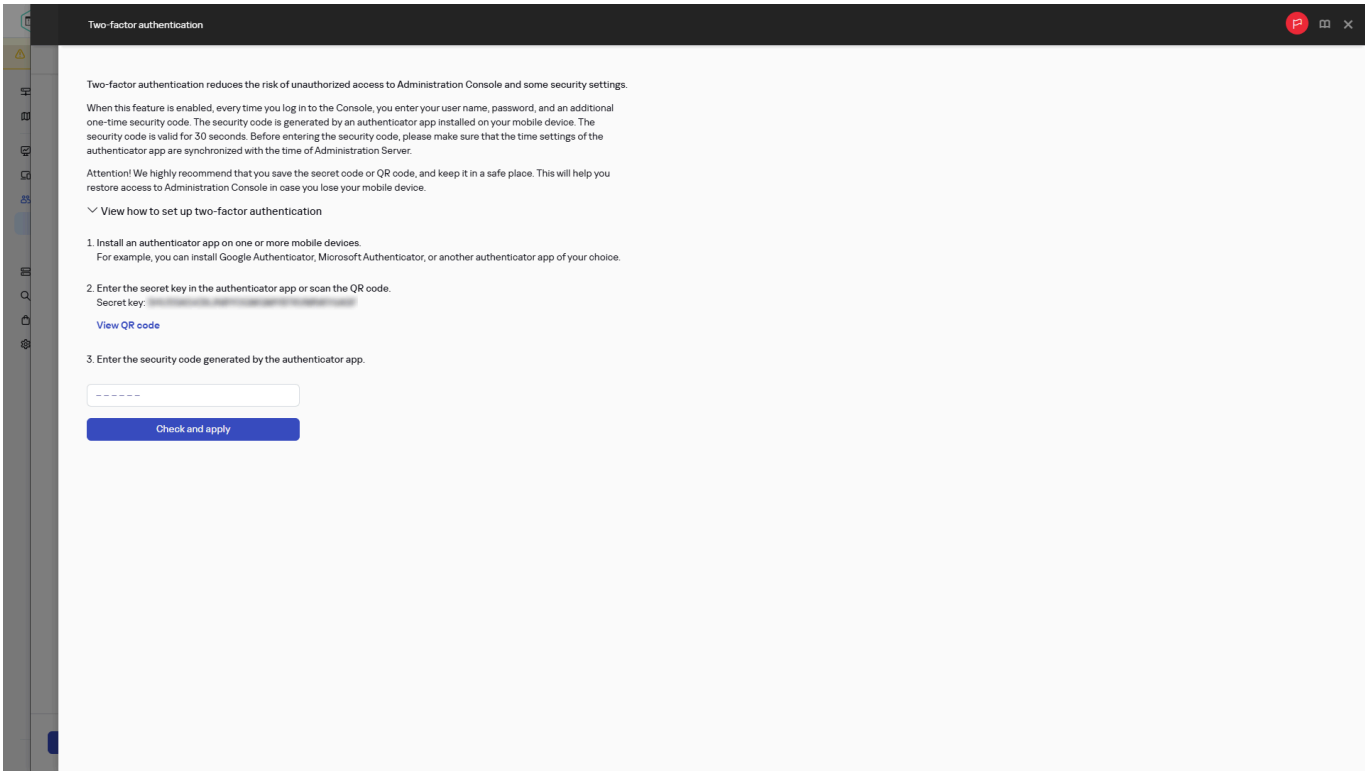


為目前使用者帳戶重新產生雙因素驗證秘密金鑰

a. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證代碼。

b. 在**雙步驟驗證**視窗中，點擊**檢視設定雙步驟驗證的方式**，然後點擊**檢視 QR 碼**。

c. 使用行動裝置上的身分驗證器應用程式掃描 QR 代碼和接收一次性安全碼。



a. 在**雙步驟驗證**視窗中，指定由身分驗證器應用程式產生的一次性安全碼，點擊**確認並套用**按鈕，然後保存變更。

Rutoken OTP 設定

若您使用 Rutoken OTP，則需要一台已安裝 Rutoken OTP 應用程式的 Android 行動裝置。Android 行動裝置須滿足以下要求：

- 作業系統為 Android 7 或更新版本。
- NFC 模組可用且已啟用

在 Rutoken OTP 應用程式中，必須設定以下參數：

- 掃描雙步驟設定精靈中顯示的 QR 碼。
- 將時間間隔設定為 30 秒。
- 選取 SHA1 作為演算法。

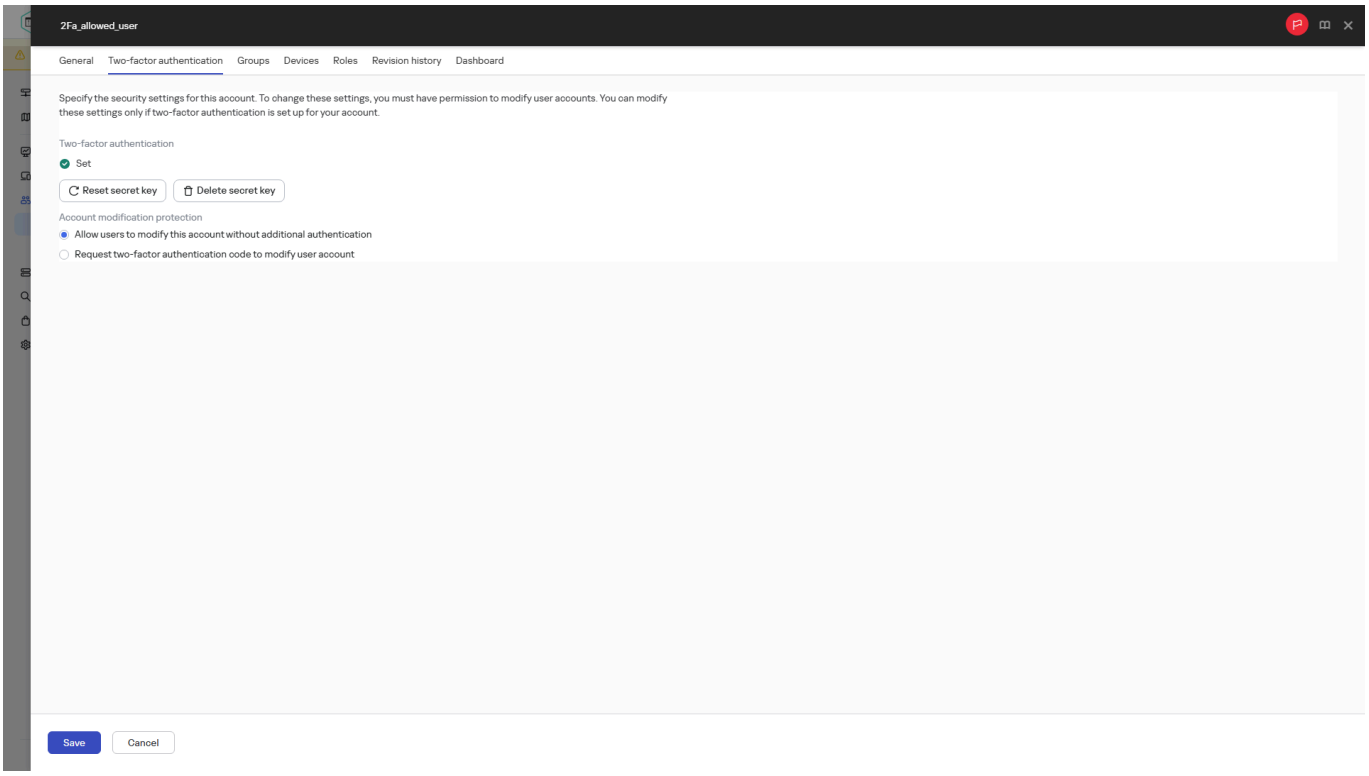
若要設定 Rutoken OTP：

1. 將 Rutoken OTP 裝置放在有 NFC 模組的行動裝置旁。
2. 在 Rutoken OTP 應用程式中，按**連線權杖**。
3. 在 Rutoken OTP 應用程式中，按**配置設定**，然後按**儲存秘密金鑰**。
   如果權杖成功連線到行動裝置，Rutoken OTP 應用程式將顯示下列狀態訊息：
   - **權杖已連線。**
   - **設定已配置。**
   - **秘密金鑰已儲存。**
4. 在 Rutoken OTP 裝置上，按下按鈕。
   一個安全碼會顯示在此裝置上。
5. 在OSMP主控台的雙因素驗證視窗中，輸入安全碼。

您的帳戶秘密金鑰已變更。

4. 如果您想重置其他帳戶的秘密金鑰：

   a. 在**雙步驟驗證**頁簽上，按一下**重設秘密金鑰**按鈕。



為其他使用者帳戶重設雙因素驗證秘密金鑰

   a. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

   b. 確認重置秘密金鑰，然後儲存變更。

   當為另一個帳戶重置秘密金鑰時，現有秘密金鑰將被刪除，並且使用者帳戶將被新增到「管理伺服器」內容中的雙因素身份驗證允許清單中。下次登入時，使用者將能夠產生新的秘密金鑰。

   使用者帳戶的秘密金鑰已重置。

您可以刪除密鑰以完全阻止使用者登入網頁主控台並阻止其存取管理伺服器。

若要刪除秘密金鑰：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。

2. 按一下您要刪除其秘密金鑰的內部使用者帳戶名稱。

   > 您無法刪除自己帳戶的秘密金鑰。

3. 在**雙步驟驗證**頁簽上，按一下**刪除秘密金鑰**按鈕。

4. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

5. 確認刪除秘密金鑰，然後儲存變更。

   使用者帳戶的秘密金鑰被刪除。

您可以透過在管理伺服器內容中將使用者新增至雙因素驗證允許清單中來還原存取權限。在此情況下，下次登入時，使用者將能夠產生新的秘密金鑰。

從雙因素驗證中排除帳戶

您可以將使用者帳戶排除在雙因素驗證之外，以允許他們登入管理伺服器，即使他們沒有設定雙因素驗證。對於在身份驗證期間無法提供一次性安全碼的整合帳戶，可能需要將帳戶排除在雙因素驗證之外。整合帳戶用於透過OpenAPI執行指令碼以及執行KUMA指令碼。

如果您的帳戶已設定雙因素驗證，並且您在**常規功能**：**一般功能**功能區中擁有使用者權限權限，則可以修改排除清單。

若要從雙因素驗證中排除使用者帳戶：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**選項卡上，在**雙步驟驗證排除項目**中，按一下**新增**按鈕。

3. 在開啟的視窗中：

   a. 選取您要排除的使用者帳戶。

   b. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

   c. 儲存您的變更。

選定的使用者帳戶將被排除在雙因素驗證之外，並且如果存在，其密鑰將被刪除。當您將Kaspersky Next XDR Expert升級到2.0或更高版本時，排除的帳戶清單不會變更。如果排除清單中的帳戶在上一個版本的Kaspersky Next XDR Expert中有密鑰，這些密鑰將在2.0中刪除。

您可以從排除清單中刪除使用者帳戶，以完全阻止使用者登入網頁主控台並阻止使用者存取管理伺服器。

若要從排除清單中刪除使用者帳戶：

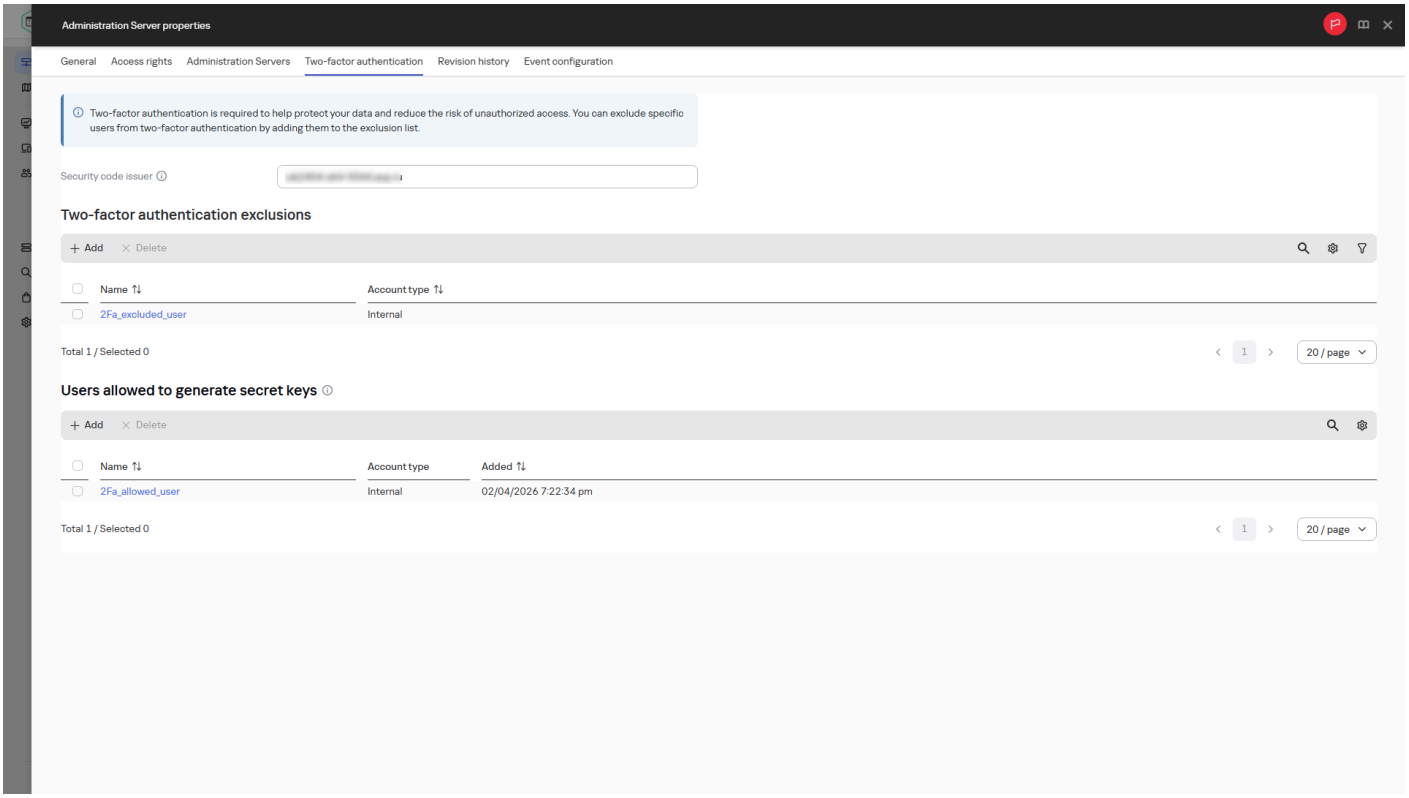
1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**頁籤上的**雙步驟驗證排除項目**表中，選擇要刪除的使用者帳戶，然後按一下**刪除**。

3. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

選定的使用者帳戶將從排除清單中移除。



設定雙因素驗證排除項目清單

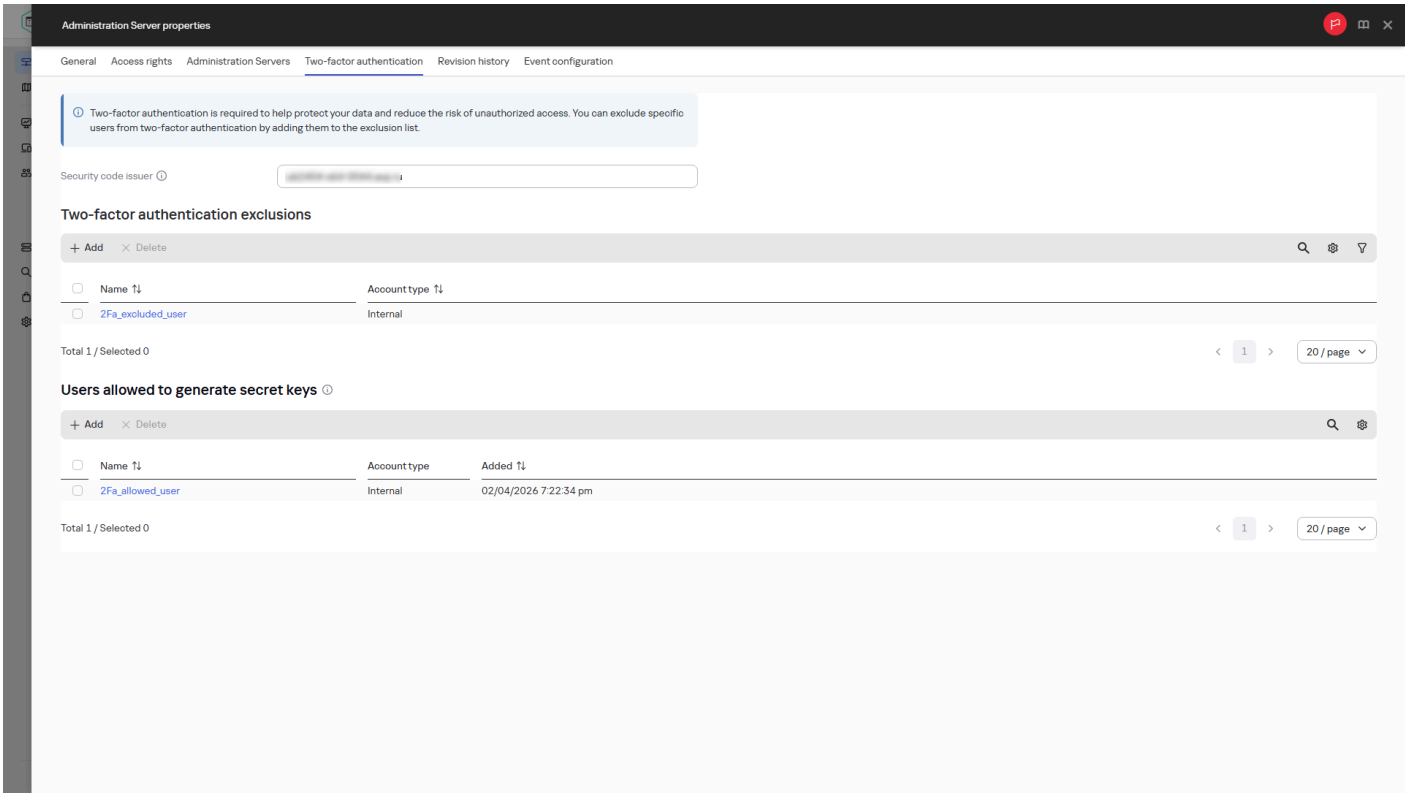
編輯安全碼簽發者的名稱

您可以為不同的管理伺服器使用多個識別碼（這稱為簽發者）。您可以更改安全碼簽發者的名稱以防萬一，例如，管理伺服器已經為另一台管理伺服器使用了類似的安全碼簽發者名稱。預設情況下，安全碼簽發者的名稱與管理伺服器的名稱相同。

若要指定安全碼簽發者的新名稱，請執行以下操作：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在內容視窗的**雙步驟驗證**頁籤中，在**安全碼簽發者**欄位中輸入新名稱，然後儲存變更。

下次登入後，新的安全碼簽發者名稱將指派給管理伺服器。



指定安全碼簽發者的名稱

允許的密碼輸入嘗試次數

Kaspersky Next XDR Expert 使用者輸入無效密碼的次數有限。達到限制後，使用者帳戶被鎖定一小時。

預設下，允許的最大密碼輸入嘗試次數是 3。此數字是固定的，無法更改。

設定使用者 SSO 工作階段和身分驗證權杖的存留期

權杖（或使用者工作階段）的存留期是指權杖或工作階段保持有效並可用於身分驗證的一段時間。當該時段結束時，權杖或工作階段會自動過期，並需要更新或重新登入。Kaspersky Next XDR Expert 可讓您設定存取權杖、用於更新存取權杖的更新權杖，以及閒置的單一登入 (SSO) 工作階段的存留期。將權杖或 SSO 工作階段的存留期設定得較短，可降低權杖遭洩露時發生未經授權存取的風險。

您也可以在多節點和單節點部署 Kaspersky Next XDR Expert 之前，使用設定檔中的對應參數（`tokenhub_access_token`、`tokenhub_refresh_token`、`credentials_session_ttl`），設定權杖的存留期和 SSO 工作階段的閒置時間。如果部署期間未指定這些設定，則會使用以下預設值：

- 存取權杖（`tokenhub_access_token`）：1 小時
- 更新權杖（`tokenhub_refresh_token`）：24 小時
- 閒置的 SSO 工作階段（`credentials_session_ttl`）：1 小時。

若要變更已部署解決方案中的設定，請使用 KDT 命令。

若要檢查目前的存留期值：

在管理員主機上，執行下列命令：

```
./kdt invoke iam -a getAuthTTLs
```

命令輸出會以 < 小時數 >h< 分鐘數 >m< 秒數 >s 格式顯示存取權杖、更新權杖及 SSO 工作階段閒置時間目前的存留期值，例如：

- `2h`
- `23h30m`
- `12h55m`

若要設定存取權杖的存留期：

在管理員主機上，執行下列命令：

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_access_token=< 時間長度 >
```

其中，`< time_period >` 是所需的時間長度，以小時、分鐘及秒為單位。例如，`1h` 或 `1h30m`。存取權杖的 `< time_period >` 最小值為 `5m`，最大值為 `2h`。

若要設定重新整理權杖的存留期：

在管理員主機上，執行下列命令：

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_refresh_token=< time_period >
```

其中，`< time_period >` 是所需的時間長度，以小時、分鐘及秒為單位。例如，`24h` 或 `720h30m`。重新整理權杖的 < 時間長度 > 最小值為 `12m`，最大值為 `4320h`。

若要設定閒置單一登入工作階段的存留期：

在管理員主機上，執行下列命令：

```
./kdt invoke iam -a setAuthTTLs --param credentials_session_ttl=< time_period >
```

其中，`<time_period>` 是所需的時間長度，以小時、分鐘及秒為單位。例如，`2h` 或 `1h30m`。閒置 SSO 工作階段的 `<` 時間長度 `>` 最小值為 `5m`，最大值為 `96h`。

若要一次設定所有參數的存留期：

在管理員主機上，執行下列命令：

```
./kdt invoke iam -a setAuthTTLs --param tokenhub_access_token=<time_period> --param
tokenhub_refresh_token=<time_period> --param credentials_session_ttl=<time_period>
```

其中，`<time_period>` 是所需的時間長度，以小時、分鐘及秒為單位。

驗證權杖和 SSO 工作階段的存留期已設定。如果您輸入的值超出最小值和最大值限制，該值會取代為預設值。

新設定的存留期僅適用於儲存變更後建立的權杖和工作階段。作用中的權杖和工作階段將根據其核發時生效的存留期參數值到期。

刪除使用者或安全群組

您僅可以刪除內部使用者或內部安全群組。

要刪除使用者或安全群組：

1. 在主功能表中，轉至**使用者和角色→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選取您要刪除的使用者或安全群組旁邊的核取方塊。

   應該始終至少有一個使用者配置了雙因素驗證，以便該使用者可以管理雙因素驗證允許清單和排除清單。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**正常**。

使用者或安全群組被刪除。

變更使用者帳戶密碼

如果當前密碼即將過期，或者您想將其更改為更安全的密碼，您可能需要更改使用者帳戶的密碼。

密碼必須符合以下規則：

- 密碼必須是 10 到 256 位字元長度。
- 密碼必須包含下列群組中的字元：
  - 大寫字母（A-Z）
  - 小寫字母 (a-z)
  - 數字（0-9）
  - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ~ " ( ) < > ;)
- 密碼不得包含任何空白字元或 Unicode 字元。

變更內部使用者帳戶的密碼

若要編輯內部使用者帳戶的密碼：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**使用者**頁簽。
2. 點擊您要編輯的使用者帳戶名稱。
3. 在開啟的使用者設定視窗中的**一般**頁簽上，按一下**變更密碼**按鈕。
4. 為使用者連線到Open Single Management Platform設定新密碼。
   若要查看輸入的密碼，請按一下。
5. 如果使用者帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，在一般功能：使用者權限功能區域中指定具有修改物件 ACL權限的帳戶的憑據。
6. 輸入身分驗證器應用程式在行動裝置上產生的一次性安全碼。

在首次登入時強制變更密碼

您可以要求使用者在首次登入 Open Single Management Platform 主控台時變更密碼。如果為多個新帳戶設定了相同的暫時密碼，建議使用此選項，因為這可確保每位使用者在首次登入時設定自己的密碼。

若要強制使用者在首次登入時變更密碼：

1. 在主選單中，前往**設定** → **身分驗證政策**，然後啟用**首次登入時強制執行密碼變更**選項。
2. 儲存您的變更。

首次登入時強制變更密碼已啟用。

是否強制變更密碼是在建立使用者帳戶時決定，且不會回溯套用：

- 在啟用此選項時建立的帳戶，在首次登入後一律需要變更密碼，即使日後停用此選項亦然。
- 在停用此選項時建立的帳戶，在首次登入後不需要變更密碼，即使日後啟用此選項亦然。

設定密碼有效期限

您可以設定使用者帳戶的密碼有效期限，以確保更頻繁地變更密碼。預設情況下已啟用該選項。

若要變更密碼有效期限：

1. 在主選單中，前往**設定 → 身分驗證政策**，然後啟用**強制執行定期密碼變更**選項。
2. 在**密碼存留時間（天）**輸入欄位中，指定密碼到期前的期間。預設密碼有效期限為 365 天。
3. 儲存您的變更。

密碼有效期限已變更。

在登入頁面新增自訂消息區塊

您可以在登入頁面新增自訂訊息區塊，以便在使用者授權前向其顯示重要資訊。例如，您可以告知使用者為確保資訊安全所採取的措施。

要新增自訂訊息區塊：

1. **建立訊息區塊字串**。

   若要建立訊息區塊字串：

   1. 為您的訊息區塊編寫HTML程式，例如：

      ```
      <div>
        <h4>Protected system of ACME Corporation </h4>
        <p>Only authorized employees are allowed to work with the system.</p>
      </div>
      ```

      不支援新增圖像。

      將此程式碼儲存到一個檔案中，例如markup.html。

2. 使用Base64編碼您的HTML。在Linux中，編碼命令如下：

```
base64 -w 0 markup.html > banner.b64
```

此命令傳回一個編碼字串，例如：

```
PGRpdj4KPGg0PtCX0LDRidC40YnQtdC90L3QsNGPINGB0LjRgdGC0LXQvNCwINCe0J7QniDCq9Cg0L7QvNCw0YjQutCwwrs8aDQ+CjxwPtCaIN(
```

2. 將該字串加入Kaspersky Next XDR Expert組態。您可以透過不同的方式將訊息區塊字串新增至設定：

- **在初始設定期間新增訊息區塊**

  要在初始設定期間新增訊息區塊：

  1. 在執行Kaspersky Next XDR Expert安裝之前，請將以下行新增至param.yaml檔案的`parameters`區段：

     ```
     - name: login_markup_b64
       source:
       value: "<以Base64編碼的訊息區塊字串>"
     ```

  2. 執行Kaspersky Next XDR Expert安裝程式。

- **在更新期間新增訊息區塊**

  要在更新期間新增訊息區塊：

  1. 在管理員主機上，使用以下命令匯出目前的組態檔：

     ```
     ./kdt ec -e <configuration_file_name_with_path>
     ```

     目前版本的組態檔將以指定名稱儲存到指定目錄。

  2. 在匯出的組態檔的`parameters`區段中，新增以下行：

     ```
     - name: login_markup_b64
       source:
       value: "<以Base64編碼的訊息區塊字串>"
     ```

  3. 更新Kaspersky Next XDR Expert和Bootstrap元件。執行更新命令時，使用`-i`旗標指定步驟1中匯出的組態檔完整路徑：

     ```
     ./kdt apply -k <XDR更新封存檔的完整路徑> --force --accept-eula -i <包含路徑的組態檔名稱>
     ```

- **透過命令列新增訊息區塊**

  要透過命令列新增訊息區塊：

  1. 將ConfigMap匯出到檔案：

     ```
     kubectl get configmap credentials -n iam -o yaml > credentials.yaml
     ```

     Credentials.yaml檔案包含您需要修改的初始組態。

2. 將您的編碼訊息區塊字串插入到creents.yaml中：

```
sed -i 's|public:\\n|public:\\n      login_markup_b64: \\"'"$(sed 's|[\/&\\]|\\&|g'
banner.b64)"'\\"\\n|' credentials.yaml
```

此命令會尋找包含「public:\n」的行，並在其後立即插入`login_markup_b64`欄位。

3. 使用任何文字編輯器，確保`login_markup_b64`參數前後各正好有6個空格字元，且引號已正確逸出。範例：

```
前面6個空格字元login_markup_b64:
\"PGRpdj4KICA8aDQ+WW91ckNvbXBhbnkgU2VjdXJlIFN5c3RlbTwvaDQ+CiAgPHA+T25seSBhdXRob3JpemVkIGVtcGxveWVlcyBhcmUgY
後面6個空格字元
```

4. 將本地變更套用到Kubernetes叢集：

```
kubectl apply -f credentials.yaml
kubectl -n iam rollout restart deployment credentials
```

如果您之後想要編輯或刪除訊息區塊：

1. 執行以下指令：

```
kubectl edit configmap credentials -n iam
```

2. 變更`login_markup_b64`參數的值，或刪除該參數。

3. 將本地變更套用到Kubernetes叢集：

```
kubectl apply -f credentials.yaml
kubectl -n iam rollout restart deployment credentials
```

- **透過IDE Lens新增訊息區塊**

要透過IDE Lens新增訊息區塊：

1. 下載並安裝IDE Lens。

2. 複製`~/.kdt/cluster.config`檔案的內容。

3. 在 Lens IDE 中，前往**本機 Kubeconfigs → + → 透過貼上新增 kubeconfig**區段，並貼上`cluster.config`檔案的內容。

4. 開啟已新增的命名空間（`iam`），然後前往**組態 → 組態映射**，並找到`credentials`組態映射。

5. 開啟`credentials`組態映射，並在結尾新增以下行（不含縮排）：

```
credentials.server.public.login_markup_b64: "<您的訊息區塊字串以Base64編碼>"
```

範例：

```
credentials.server.public.login_markup_b64:
"PGRpdiBzdHlsZT0idGV4dC1hbGlnbjogY2VudGVyOyI+CiAgPGltZyBzcmM9ImZpbGU6Ly8vaG9tZS90b29yLzUwLmpwZyIgYWx0PSJTZW
```

6. 按一下**儲存**按鈕。
7. 重新載入pod：

```
kubectl -n iam rollout restart deployment credentials
```

要稍後編輯或刪除訊息區塊：

1. 重複上述步驟1到4。
2. 開啟`credentials`組態映射，並編輯或刪除`login_markup_b64`參數。
3. 按一下**儲存**按鈕。
4. 重新載入pod：

```
kubectl -n iam rollout restart deployment credentials
```

套用新組態後，您的自訂訊息區塊將顯示在登入頁面上。

建立使用者角色

要建立使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 點擊**新增**。
3. 在開啟的**新角色名稱**視窗中，輸入新角色的名稱。
4. 點擊**正常**以套用變更。
5. 在開啟的角色內容視窗中，變更角色設定：
   - 在**一般**頁籤，編輯角色名稱。
     您無法編輯預定義角色名稱。

- 在**設定**頁籤，編輯角色範圍和政策以及與角色相關的設定檔。
- 在**存取權限**頁籤，編輯存取 Kaspersky 應用程式的權限。

6. 按一下**儲存**以儲存變更。

新角色出現在使用者角色清單。

編輯使用者角色

要編輯使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 點擊您要編輯的角色名稱。
3. 在開啟的角色內容視窗中，變更角色設定：
   - 在**一般**頁籤，編輯角色名稱。
     您無法編輯預定義角色名稱。
   - 在**設定**頁籤，編輯角色範圍和政策以及與角色相關的設定檔。
   - 在**存取權限**頁籤，編輯存取 Kaspersky 應用程式的權限。
4. 按一下**儲存**以儲存變更。

更新的角色出現在使用者角色清單。

編輯使用者角色範圍

*使用者角色範圍*是使用者和管理群組的組合。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

要新增使用者、安全群組和管理群組到使用者角色範圍，您可以使用以下其中一種方法：

方法 1：

1. 在主功能表中，轉至**使用者和角色→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選取您要新增到使用者角色範圍的使用者或安全群組旁邊的核取方塊。
3. 點擊**指派角色**按鈕。
   角色分配精靈啟動。使用**下一步**按鈕進行精靈。
4. 在**選取角色**步驟，選取您要指派的使用者角色。

5. 在**定義範圍**步驟，選取您要新增至使用者角色範圍的管理群組。

6. 點擊**指派角色**按鈕以關閉視窗。

所選使用者或安全群組和所選管理群組被新增到使用者角色範圍。

方法 2：

1. 在主功能表中，轉至 **使用者和角色** → **角色**。

2. 按一下您要定義範圍的角色名稱。

3. 在開啟的角色內容頁面中，選擇**設定**頁籤。

4. 在**角色範圍**區段中，點擊**新增**。
角色分配精靈啟動。使用**下一步**按鈕進行精靈。

5. 在**定義範圍**步驟，選取您要新增至使用者角色範圍的管理群組。

6. 在**選取使用者**步驟，選取您要新增到使用者角色範圍的使用者和安全群組。

7. 點擊**指派角色**按鈕以關閉視窗。

8. 按一下**關閉**按鈕 (⨉) 以關閉角色內容視窗。

所選使用者或安全群組和所選管理群組被新增到使用者角色範圍。

方法 3：

1. 在主選單中，按一下管理伺服器名稱。
管理伺服器內容視窗將開啟。

2. 在**"存取權限"**頁簽上，選中要新增到使用者角色範圍的使用者或安全群組名稱旁邊的核取方塊，然後點擊**"角色"**按鈕。
您不能同時選擇多個使用者或安全群組。如果您選擇了多個項目，**角色**按鈕將被停用。

3. 在**角色**視窗中，選擇要指派的使用者角色，然後套用並儲存變更。
所選使用者或安全群組被新增到使用者角色範圍。

刪除使用者角色

要刪除使用者角色：

1. 在主功能表中，轉至 **使用者和角色** → **角色**。

2. 選取您要刪除的角色旁邊的核取方塊。

3. 點擊**刪除**按鈕。

4. 在開啟的視窗中，點擊**正常**。

使用者角色被刪除。

關聯政策設定檔到角色

您可以關聯使用者角色到政策設定檔。此種情況下，該政策設定檔的啟動規則基於角色：政策設定檔對具有指定角色的使用者可用。

例如，政策禁止在管理群組的所有裝置上執行 GPS 導航軟體。GPS 導航軟體僅在"使用者"管理群組中的單個裝置上是必須的——該裝置屬於導遊。此種情況下，您可以分配"導遊"角色給其所有者，然後建立一個政策設定檔，允許 GPS 導航軟體僅在分配了"導遊"角色的使用者的裝置上執行。所有其他政策設定被保留。僅帶有"導遊"角色的使用者將被允許執行 GPS 導航軟體。然後，如果其他員工被分配了"導遊"角色，該新員工也在組織的裝置上執行導航軟體。執行 GPS 導航軟體在相同管理群組的其他裝置上仍將被禁止。

要關聯角色到政策設定檔：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。

2. 選取您要關聯政策設定檔的角色名稱。

   角色內容視窗會開啟，並含有所選的**一般**頁籤。

3. 選取**設定**頁籤，之後向下捲動至**政策**區段。

4. 點擊**編輯**。

5. 要關聯角色到：

   - **現有政策設定檔**—點擊所學政策名稱旁邊的臂章圖示（ ）），然後選取您要關聯角色的設定檔旁邊的核取方塊。
   - **新政策設定檔**：

     a. 選取您要建立設定檔的政策旁邊的核取方塊。

     b. 點擊**新政策設定檔**。

     c. 為新設定檔指定名稱並配置設定檔設定。

     d. 點擊**儲存**按鈕。

     e. 選取新設定檔旁邊的核取方塊。

6. 點擊**指派到角色**。

設定檔被關聯到角色並顯示在角色內容中。設定檔自動應用到分配了該角色的使用者的任意裝置。

設定 Kerberos 網域身分驗證

Kaspersky Next XDR Expert 可讓您透過 Kerberos 通訊協定使用網域身分驗證。網域身份驗證可讓您在OSMP主控台中啟用安全身份驗證，而無需在企業網路上重新輸入密碼（單一登入）。

您必須先設定您的網域控制器以使用 Kerberos 並產生 keytab 檔案。有關更多資訊，請參閱網域控制器文件。

Microsoft Active Directory 支援 SCRIL（互動式登入需要智慧卡）。

為 FreeIPA 和 AldPro 產生 keytab 檔案

要產生 keytab 檔案，請執行以下操作：

1. 建立一個使用者帳戶，供 IAM 用於存取網域控制器。
2. 如果管理伺服器位於FreeIPA/AldPro網域之外，請新增DNS記錄項目和主機項目：

```
ipa dnsrecord-add <zoneName> <recordName> --a-rec <Administration Server IP address>
ipa host-add --password=<password> <Administration Server host address>
```

3. 為管理伺服器建立 HTTP 服務時，請指定 PAC 類型：

```
ipa service-add HTTP/<console_host>.<smp_domain>@<DOMAIN WRITTEN IN CAPITAL LETTERS> --ok-to-auth-as-
delegate=true --pac-type PAD
```

在此，`<console_host>` 是服務主機名稱，`<smp_domain>` 是網域名稱。服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 `console_host` 變數的值為 `console`，而 `smp_domain` 變數的值為 `smp.local`，則提供 OSMP 主控台存取權的服務完整名稱為 `console.smp.local`。

4. 指定用於身分驗證的使用者帳戶：

```
ipa service-allow-retrieve-keytab HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN CAPITAL LETTERS>
--user=<user>
```

5. 匯出 keytab 檔案：

```
ipa-getkeytab -s <domain controller address> -p HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN
CAPITAL LETTERS> -k /tmp/h.keytab
```

為 Microsoft Active Directory 產生 keytab 檔案

要產生 keytab 檔案，請執行以下操作：

1. 建立一個使用者帳戶，供 IAM 用於與網域控制器通訊。
2. 為使用者帳戶啟用以下選項：
   - **使用者無法變更密碼**
   - **Kerberos AES 256 位元加密**

   您可以啟用「**密碼永不過期**」選項，避免每次密碼過期時重新簽發 keytab 檔案。
3. 為使用者帳戶新增服務主體名稱 (SPN)：

```
setspn -S HTTP/<> <DOMAIN WRITTEN IN CAPITAL LETTERS>\<user>
```

4. 匯出 keytab 檔案：

```
ktpass -out C:\<folder>\<keytab file name> -princ HTTP/<console_host>.<smp_domain>@<DOMAIN WRITTEN IN CAPITAL
LETTERS> -mapuser <user>@<DOMAIN WRITTEN IN CAPITAL LETTERS> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
<user password> -mapop set
```

在此，`<console_host>` 是服務主機名稱，`<smp_domain>` 是網域名稱。服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 `console_host` 變數的值為 `console`，而 `smp_domain` 變數的值為 `smp.local`，則提供 OSMP 主控台存取權的服務完整名稱為 `console.smp.local`。

為 Samba 產生 keytab 檔案

要產生 keytab 檔案，請執行以下操作：

1. 建立一個使用者帳戶，供 IAM 用於與網域控制器通訊：

```
samba-tool user add <user>
```

2. 將 SPN 新增到使用者帳戶：

```
samba-tool spn add HTTP/<console_host>.<smp_domain> <user>
```

在此，`<console_host>` 是服務主機名稱，`<smp_domain>` 是網域名稱。服務主機名稱與網域名稱皆為服務FQDN的組成部分。例如，如果 `console_host` 變數的值為 `console`，而 `smp_domain` 變數的值為 `smp.local`，則提供 OSMP 主控台存取權的服務完整名稱為 `console.smp.local`。

3. 匯出 keytab 檔案：

```
samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<console_host>.<smp_domain>
```

設定 Kerberos 網域身分驗證

若要啟用 Kerberos 網域身分驗證：

1. 執行網域控制器輪詢。
2. 在主選單中，前往 **設定** → **單一登入** 區段。
3. 啟用**Kerberos 身分驗證**選項。
4. 上傳 keytab 檔案。
5. 為允許存取OSMP主控台的網域使用者指派角色。
   至此，已為網域使用者啟用 Kerberos 網域身分驗證。

更新 Kaspersky 資料庫和應用程式

您只能安裝已通過認證程序的應用程式模組更新。啟用模組自動更新會導致應用程式失去認證狀態。

依照既定程序安裝未通過認證測試的 Kaspersky 應用程式可執行模組更新（消除已知弱點的更新除外），會導致應用程式失去認證狀態。

該部分敘述了定期更新以下內容必須採取的步驟：

- 卡巴斯基資料庫和軟體模組
- 已安裝卡巴斯基應用程序，包括Open Single Management Platform元件和安全應用程式

在美國使用的軟體將無法提供更新功能（包括防毒軟體簽章更新和程式碼庫更新）和 KSN 功能。

情境：定期更新 Kaspersky 資料庫與應用程式

該部分提供了定期更新 Kaspersky 資料庫、軟體模組和應用程式的情境。完成設定網路防護情境後，您必須維持防護系統的可靠性，確保管理伺服器和受管理裝置受到多種威脅的防護，包含病毒、網路攻擊與釣魚攻擊。

網路防護透過更新以下內容保持最新：

- 卡巴斯基資料庫和軟體模組
- 已安裝的 Kaspersky 應用程式，包括 Kaspersky Next XDR Expert 元件和安全應用程式

當您完成此情境，您可確保以下事項：

- 您的網路受到最新 Kaspersky 軟體的防護，包括 Kaspersky Next XDR Expert 元件和安全應用程式。
- 對網路安全關鍵的病毒資料庫和其他 Kaspersky 資料庫保持最新。

先決條件

受管理裝置必須有與管理伺服器的連線。若沒有連線，請考慮手動更新卡巴斯基資料庫和軟體模組，或直接從卡巴斯基更新伺服器更新。

管理伺服器必須具有到網際網路的連線。

在您開始之前，確保您已做了如下：

1. 根據通過OSMP主控台部署卡巴斯基應用程序的情境，已將卡巴斯基安全應用程序部署到受管裝置上。
2. 建立了配置了所有所需政策、政策設定檔和工作，根據網路防護配置情境。
3. 分配了適當數量的發佈點，與受管理裝置和網路拓撲一致。

更新 Kaspersky 資料庫和應用程式分步驟進行：

1 選取更新方案

您可使用多種方案為Open Single Management Platform元件和安全應用程式安裝更新。選取一個或多個滿足您網路需求的方案。

2 建立管理伺服器的「將更新下載至儲存區」工作

手動建立*將更新下載至管理伺服器儲存區*工作。

此工作需要從卡巴斯基更新服務器下載更新到管理伺服器的儲存區，以及更新Open Single Management Platform的卡巴斯基資料庫和軟體模組。更新被下載後，它們可以被傳播到受管理裝置。

如果您的網路被分配了發佈點，更新被從管理伺服器儲存區自動下載到發佈點儲存區。此種情況下，發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。

操作說明：建立管理伺服器的「將更新下載至儲存區」工作

3 建立「將更新下載至發佈點儲存區」工作（可選）

預設下，更新被從管理伺服器下載到發佈點。您可以配置Open Single Management Platform，直接從卡巴斯基更新伺服器下載更新到發佈點。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

當您的網路獲得指派的發佈點並且建立了*將更新下載至發佈點儲存區*工作後，發佈點會從 Kaspersky 更新伺服器下載更新，而非管理伺服器儲存區。

操作說明：建立「將更新下載至發佈點儲存區」工作

4 配置發佈點

當您的網路有指派的發佈點時，請確保**已啟用**選項已在所有必要發佈點中啟用。當該選項對發佈點停用時，包含在發佈點範圍中的裝置從管理伺服器儲存區下載更新。

5 使用差異檔案最佳化更新過程（可選）

您可以使用以下差異檔案最佳化管理伺服器和受管理裝置之間的流量。當該功能被啟用時，管理伺服器或發佈點下載 diff 檔案，而不是整個 Kaspersky 資料庫或軟體模組檔案。diff 檔案敘述了資料庫或軟體模組的檔案的兩個版本之間的差異。因此，diff 檔案比整個檔案佔用更少的空間。這導致降低管理伺服器之間或發佈點和受管理裝置之間的流量。若要使用此功能，請啟用*將更新下載至管理伺服器儲存區*工作和/或*將更新下載至發佈點儲存區*工作內容中的**下載差異檔案**選項。

如何使用 diff 檔案：使用 diff 檔案更新 Kaspersky 資料庫和軟體模組

6 為安全應用程式配置更新的自動安裝

為受管理應用程式建立*更新*工作，以提供對軟體模組和卡巴斯基資料庫（包括病毒資料庫）的及時更新。為了確保定期更新，建議您在配置工作排程時選取**當新更新下載至儲存區時**選項。

如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。此後，更新可以被傳播到受管理裝置。

7 核准和拒絕受管理卡巴斯基應用程式的更新

預設下，下載的軟體更新具有*未定義*狀態。您可以變更狀態到*已批准*或*已拒絕*。批准的更新總是被安裝。如果受管理卡巴斯基應用程式更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受該條款。此後，更新可以被傳播到受管理裝置。您設定了*已拒絕*狀態的更新將不被安裝到裝置。若先前安裝了已被拒絕的受管理應用程式更新，Open Single Management Platform將嘗試從所有裝置解除安裝該更新。

核准和拒絕更新僅適用於安裝在 Windows 型用戶端裝置上安裝的網路代理和受管理卡巴斯基應用程式。不支援管理伺服器、OSMP主控台和管理Web外掛程式的無縫更新。

操作說明：核准與拒絕軟體更新

有時，網路代理更新後，您可能會被提示重新啟動受管理裝置。如果顯示所需重啟通知，按一下通知中的**檢視裝置**連接，選取要重新啟動的裝置旁的核取方塊，然後按一下**重新啟動**按鈕以完成網路代理更新。

結果

完成此情境後，Kaspersky Next XDR Expert 會設定為在更新下載至管理伺服器的儲存庫後，更新 Kaspersky 資料庫。您然後可以繼續監控網路狀態。

關於更新 Kaspersky 資料庫、軟體模組和應用程式

為了確保管理伺服器和受管理裝置的防護是最新的，您必須提供以下內容的定期更新：

- 卡巴斯基資料庫和軟體模組

  在下載卡巴斯基資料庫和軟體模組之前，Open Single Management Platform會檢查卡巴斯基伺服器是否可以存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保更新病毒資料庫並維護受管裝置的安全級別。

- 已安裝卡巴斯基應用程序，包括Open Single Management Platform元件和安全應用程式

  Open Single Management Platform可讓您自動更新安裝在Windows用戶端裝置上的網路代理程式和卡巴斯基應用程式。不支援管理伺服器、OSMP主控台和管理Web外掛程式的無縫更新。若要更新這些元件，您必須從卡巴斯基網站下載最新版本，然後手動安裝它們。

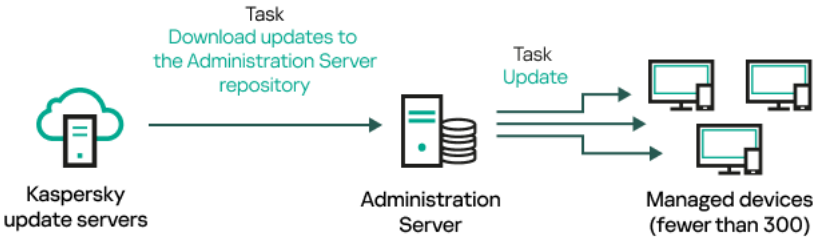
取決於您網路的配置，您可以使用以下方案來下載和分發所需更新到受管理裝置：

- 通過使用單個工作：*將更新下載至管理伺服器儲存區*
- 透過使用兩個工作：
  - *將更新下載至管理伺服器儲存區*工作
  - *將更新下載至發佈點儲存區*工作
- 透過共用資料夾或FTP伺服器手動。

- 直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security
- 如果管理伺服器沒有網際網路連線，則透過網路資料夾

使用將更新下載至管理伺服器儲存區工作

在此方案中，Open Single Management Platform會透過*將更新下載至管理伺服器儲存區*工作下載更新。在單一網段包含少於 300 台受管理裝置或每個網段包含少於 10 台受管理裝置的小網路中，更新直接從管理伺服器儲存區被分發到受管理裝置（參見下圖）。



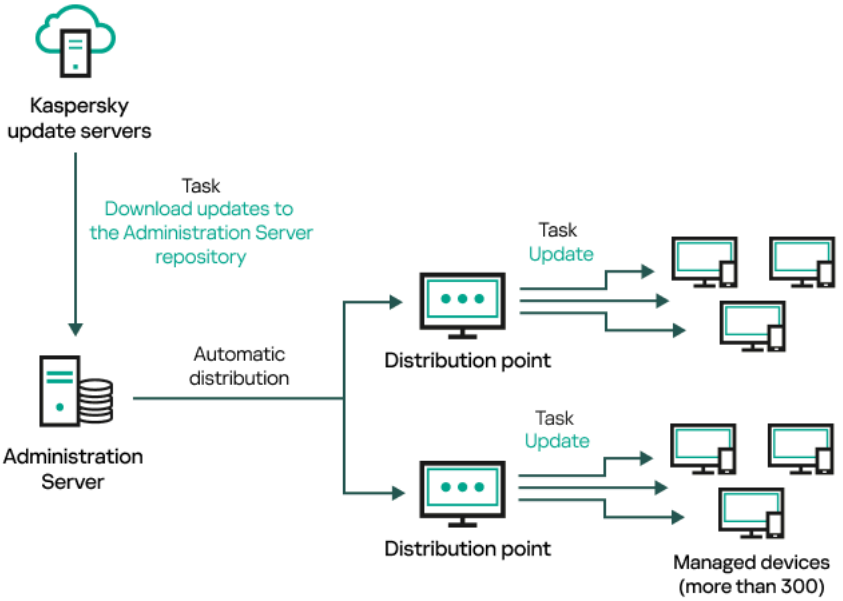
使用*將更新下載至管理伺服器儲存區*工作在沒有發佈點狀態下更新

作為更新的來源，您不僅可以使用卡巴斯基更新伺服器，還可以使用網路資料夾。

預設下，管理伺服器與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器使用 HTTP 協定，而不是 HTTPS。

如果您的網路中單一網段包含 300 台或更多受管理裝置，或您的網路由多個網段組成，每個網段包含多於 9 台受管理裝置，我們建議您使用發佈點傳播更新到受管理裝置（參見下圖）。發佈點降低管理伺服器負載並最佳化管理伺服器和受管理裝置之間的流量。您可以計算數字並配置您網路所需的發佈點。

此種方案中，更新被從管理伺服器儲存區自動下載到發佈點儲存區。發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。



使用*將更新下載至管理伺服器儲存區*工作搭配發佈點更新

當*將更新下載至管理伺服器儲存區*工作完成後，Kaspersky Endpoint Security 的卡巴斯基資料庫和軟體模組的更新將下載到管理伺服器儲存區。這些更新透過 Kaspersky Endpoint Security 的*更新*工作安裝。

*將更新下載至管理伺服器儲存區*工作在虛擬管理伺服器上不可用。虛擬管理伺服器的儲存區節點下的更新，將顯示已下載至主管理伺服器的更新。

您可以配置在測試裝置集上進行更新的操作和錯誤驗證。如果驗證成功，更新被分發到其他受管理裝置。

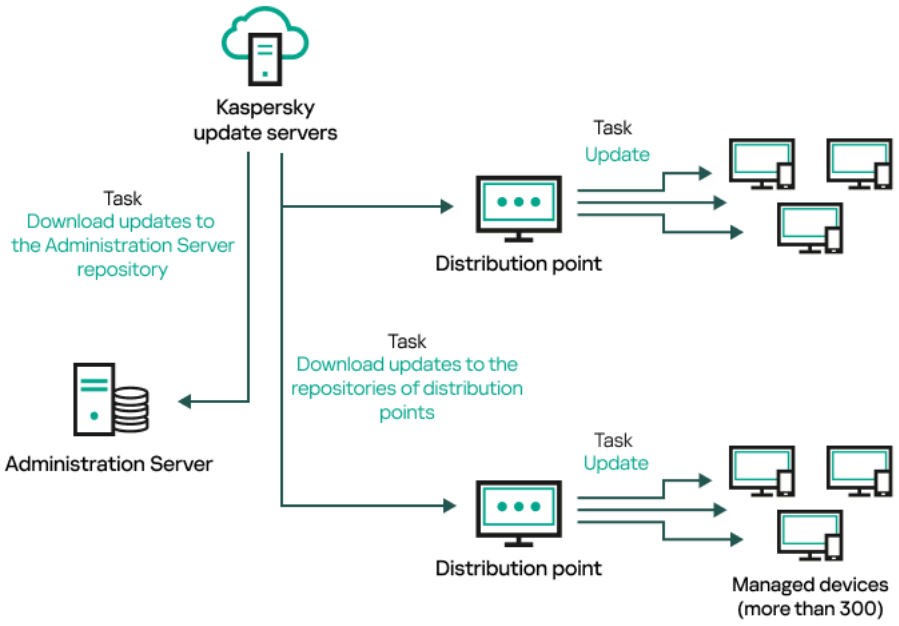
每個 Kaspersky 應用程式都從管理伺服器請求所需更新。管理伺服器集合這些更新並僅下載應用程式請求的更新。這確保了相同更新不被下載多次，且不必要更新不被下載。當執行*將更新下載至管理伺服器儲存區*工作時，管理伺服器自動傳送以下資訊到 Kaspersky 更新伺服器以便確保相關版本的 Kaspersky 資料庫和軟體模組的下載：

- 應用程式 ID 和版本
- 應用程式啟動 ID
- 啟動金鑰 ID
- 「*將更新下載至管理伺服器儲存區*」工作執行 ID

傳輸的資訊均不含個人詳情或其他機密資訊。AO Kaspersky Lab 依照法律需求防護資訊。

使用兩個工作：將更新下載至管理伺服器儲存區工作與將更新下載至發佈點儲存區工作

您可以直接從 Kaspersky 更新伺服器下載更新到發佈點儲存區，而不是從管理伺服器儲存區，然後分發更新到受管理裝置（參見下圖）。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。



使用「*將更新下載至管理伺服器儲存區*」和「*將更新下載至發佈點儲存區*」工作進行更新

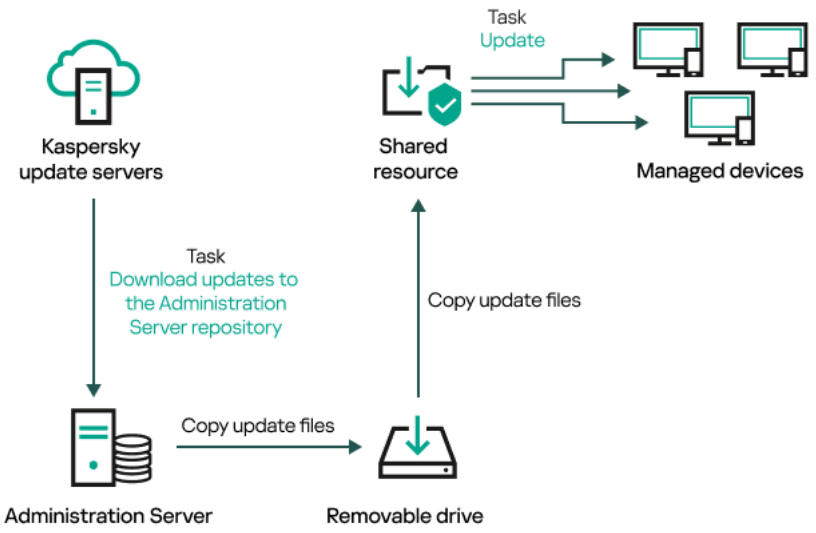
預設下，管理伺服器和發佈點與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器和/或發佈點使用 HTTP 協定，而不是 HTTPS。

若要實現該方案，請在*將更新下載至發佈點儲存區*工作外再建立*將更新下載至管理伺服器儲存區*工作。此後，發佈點將從 Kaspersky 更新伺服器下載更新，而不是從管理伺服器儲存區。

此方案也需要*將更新下載至管理伺服器儲存區*工作，因為該工作被用於下載卡巴斯基資料庫和Open Single Management Platform軟體模組。

透過共用資料夾或FTP伺服器手動。

如果裝置未連線到管理伺服器，您可以使用共用資料夾作為更新卡巴斯基資料庫、軟體模組和應用程式的更新來源。在此方案中，您需要將所需的更新從管理伺服器儲存庫複製到可移動驅動器，然後將更新複製到Kaspersky Endpoint Security設定中指定為更新來源的共用資源（見下圖）。



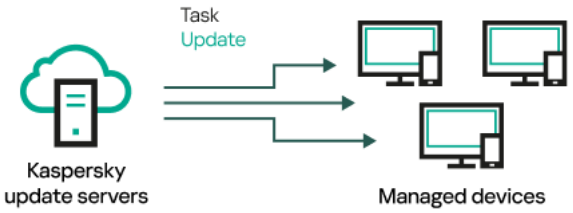
透過共用資料夾或FTP伺服器更新

有關 Kaspersky Endpoint Security 更新來源的更多資訊，請參閱以下說明：

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

直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security

在受管理裝置上，您可以配置 Kaspersky Endpoint Security 直接從卡巴斯基更新伺服器接收更新（參見下圖）。



直接從卡巴斯基更新伺服器更新安全應用程式

在此方案中，安全應用程式不使用Open Single Management Platform提供的儲存庫。要直接從卡巴斯基更新伺服器接收更新，在安全應用程式中指定卡巴斯基更新伺服器作為更新來源。有關這些設定的詳細資訊，請參閱以下說明：

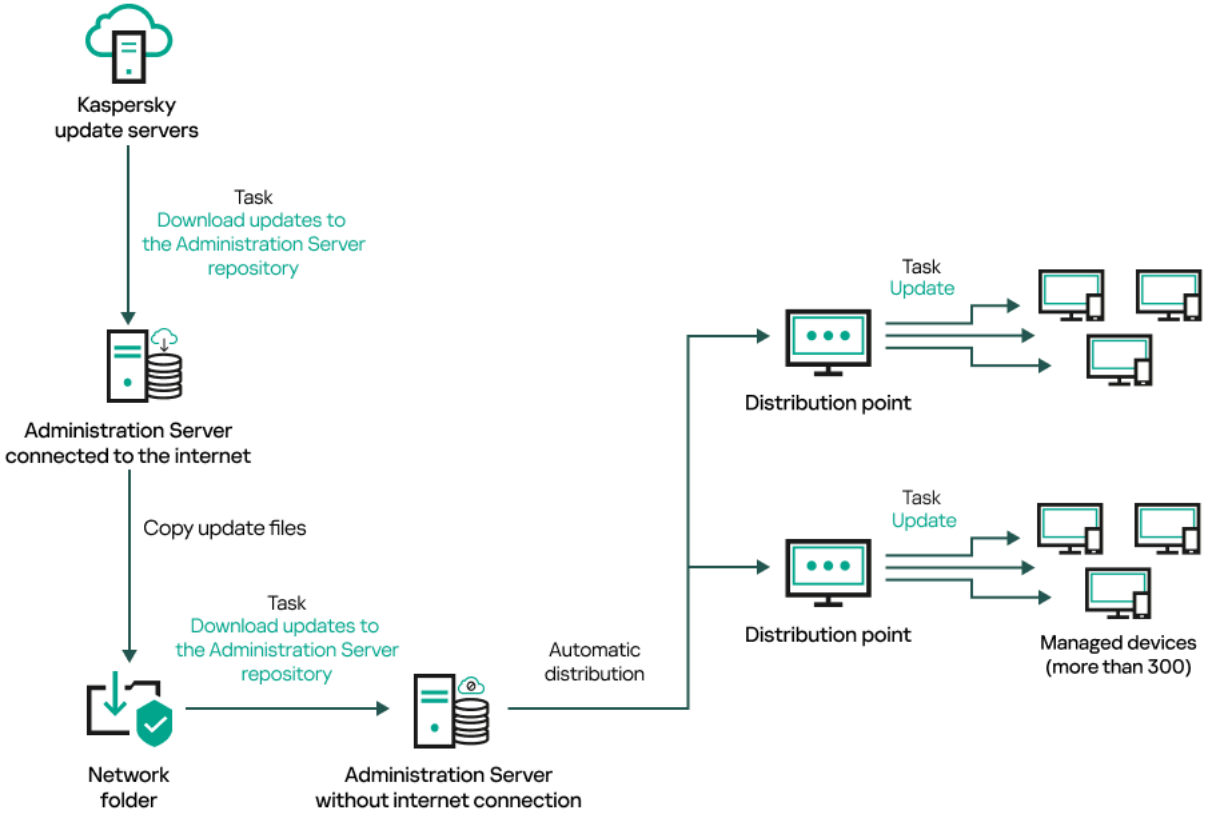
- Kaspersky Endpoint Security for Linux 說明
- Kaspersky Endpoint Security for Windows 說明

如果管理伺服器沒有網際網路連線，則透過網路資料夾

如果管理伺服器沒有網際網路連線，您可以設定*將更新下載至管理伺服器儲存區*工作從網路資料夾下載更新。在這種情況下，您必須不時將所需的更新檔案複製到指定的資料夾中。例如，您可以從以下來源之一複制所需的更新檔案：

- 具有網際網路連線的管理伺服器（參見下圖）

  因為管理伺服器只下載安全應用程式請求的更新，所以管理伺服器管理的安全應用程式集合（一個有網際網路連線，一個沒有網際網路連線）必須比對。



如果管理伺服器沒有網際網路連線，則透過網路資料夾更新

- Kaspersky Update Utility

  由於此公用程式使用舊方案下載更新，請開啟*將更新下載至管理伺服器儲存區*工作的內容，然後啟用*使用舊配置下載更新*選項。如有必要，您還可以設定*自動下載更新請求檔案*選項，以便卡巴斯基更新實用程式僅下載所需的更新。

建立「將更新下載至管理伺服器儲存區」工作

*將更新下載至管理伺服器儲存區*工作可讓您將 Kaspersky Endpoint Security for Linux 的資料庫和軟體模組更新從卡巴斯基更新伺服器下載到管理伺服器儲存區。在工作清單中，只能有一個*將更新下載至管理伺服器儲存區*工作。

*將更新下載至管理伺服器儲存區*工作完成和更新被下載後，它們可以被傳播到受管理裝置。

如果您在叢集中安裝管理伺服器，則會自動建立*將更新下載至管理伺服器儲存區*的工作。

在向受管理裝置分發更新之前，您可以執行*更新驗證*工作。這可讓您確保管理伺服器正確安裝下載的更新，並且安全級別不會因為更新而降低。若要在分發之前驗證它們，請在*將更新下載至管理伺服器儲存區*工作設定中配置**執行更新驗證**選項。

要建立將更新下載至管理伺服器儲存區工作：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。
3. 對於 Kaspersky Next XDR Expert 應用程式，請選擇**將更新下載至管理伺服器儲存區**工作類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 在**完成工作建立**頁面上，您可以啟用**建立完成時開啟工作詳情**選項以開啟工作內容視窗並修改預設工作設定。否則，您可以稍後隨時配置工作設定。
6. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。
7. 點擊建立的工作名稱以開啟屬性視窗。
8. 在開啟的工作內容視窗的**應用程式設定**頁籤，指定以下設定：

   - **更新來源**

     您可以使用卡巴斯基更新伺服器或網路資料夾作為更新來源。如果您要為次要管理伺服器或虛擬管理伺服器建立工作，也可以選擇本機目錄或主管理伺服器作為更新來源。

     在*將更新下載至管理伺服器儲存區*工作和*將更新下載至發佈點的儲存區* 工作中，如果您選擇受密碼防護的本機或網路資料夾作為更新來源，則使用者身分驗證不起作用。要解決此問題，首先掛接受密碼防護的資料夾，然後指定所需的憑據，例如，透過作業系統。之後，您可以選擇此資料夾作為更新下載工作中的更新來源。Open Single Management Platform不需要您輸入憑證。

   - **更新儲存資料夾**

     用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

   - **強制執行從屬管理伺服器的更新**

     如果啟用該選項，當新更新下載後管理伺服器立刻在從屬管理伺服器上啟動更新工作。更新工作透過使用在從屬管理伺服器上的工作屬性中配置的更新來源來啟動。

     如果停用此選項，從屬管理伺服器上的更新工作將根據排程啟動。

     預設情況下已停用該選項。

- **複製下載的更新至其他資料夾**

  管理伺服器接收更新後，它複製它們到指定資料夾。如果您想要在您的網路上手動管理更新的分發，則使用該選項。

  例如，您可能要在以下情況下使用該選項：您組織的網路包含幾個獨立子網路，且每個子網路的裝置不能存取其他子網路。然而，所有子網路中的裝置都可以存取通用網路共用。此種情況下，您在子網路之一設定管理伺服器從 Kaspersky 更新伺服器下載更新，啟用該選項，然後指定該網路共用。對於其他管理伺服器的「將更新下載至儲存區」工作中，指定與更新來源相同的網路共用。

  如果選擇將下載的更新複製到本機資料夾，則必須在已安裝管理伺服器的的裝置上指定資料夾。資料夾路徑取決於裝置的作業系統。由於本機資料夾位於基於 Linux 的管理伺服器上，因此您必須指定 POSIX 路徑。例如 /path/to/dir。

  選取位於基於 Linux 的管理伺服器上的網路資料夾時，必須事先透過掛載該資料夾，來確保安裝有管理伺服器的裝置可以存取該網路資料夾。存取資料夾將透過 SMB 通訊協定實現。

  預設情況下已停用該選項。

- **下載差異檔案**

  該選項啟用下載 diff 檔案功能。

  預設情況下已停用該選項。

- **使用舊配置下載更新**

  Open Single Management Platform使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新**選項。否則，更新下載工作將失敗。

  例如，當指定本機或網路資料夾作為更新來源，且此資料夾中的更新檔案是由使用舊方案下載更新的 Kaspersky Update Utility 所下載時，您必須啟用此選項。

  預設情況下已停用該選項。

- **執行更新驗證**

  管理伺服器會從源下載更新並將其儲存到暫時儲存區，之後執行**更新驗證工作**欄位中定義的工作。如果工作成功完成，系統會從暫時儲存區將更新複製到管理伺服器共用資料夾，然後分發到所有以管理伺服器作為更新來源的裝置（系統會啟動有**當新更新下載至儲存區時**排程類型的工作）。「將更新下載至儲存區」工作僅在*更新驗證*工作完成後結束。

  預設情況下已停用該選項。

- **自動下載更新請求檔案**

  如果您希望Kaspersky Update Utility 僅下載具有適當配置的必要更新，請啟用此選項，並指定卡巴斯基 Next XDR Expert將創建包含要下載的更新資訊的更新請求文件的路徑。更新請求檔案包含用於版本控制的時間戳記和 MD5 雜湊。

  請確保**使用舊配置下載更新**選項已停用。

  此外，還必須配置卡巴斯基更新實用程式中的更新下載 。

預設指定以下路徑：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml。如有必要，您可以變更預設名稱（retranslation_request）和路徑。

請求檔案可以放在本機或共用資料夾中。使用共用資料夾時，您必須確保可疑從安裝了管理伺服器的裝置存取該資料夾。確保存取的方法和使用的工具取決於您的基礎架構。

執行*將更新下載至管理伺服器儲存區*工作時，Kaspersky Next XDR Expert 會在您指定的路徑中建立 XML 格式的更新請求檔案。Kaspersky Update Utility會自動從請求檔案中獲取資訊，然後僅下載所需的更新。如果Kaspersky Update Utility無法自動取得資訊（例如，Kaspersky Update Utility無法存取卡巴斯基Next XDR Expert在其中建立請求檔案的資料夾），您必須使用協力廠商工具傳輸該檔案。

9. 在工作內容視窗的**排程**頁籤，建立工作開始的排程。如果必要，配置以下設定：

- **開始工作**:
  - **手動**（預設選取）

    工作不自動執行。您僅可以手動啟動。

    預設情況下已選定此選項。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期五於目前系統時間執行一次。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。這是 Kaspersky Next XDR Expert 向後相容所必需的。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

- **按每週中的指定日**

  工作定期執行，在每周指定日期的指定時間。

  預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。

  在缺少指定日的月份，工作在最後一天執行。

  預設下，工作在每月的第一天執行，在目前系統時間。

- **每月於選定的週間日**

  工作定期在指定月日的指定時間執行。

  預設情況下，開始時間為18:00，且未選擇當月的任何日期。

  > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

  您可以選擇一週中的多個日期。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

- 其它工作設定：

  - **執行錯過的工作**

    該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

    如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

    如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

    預設情況下已停用該選項。

  - **使用工作啟動自動隨機化延遲**

    如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

- **停止工作，若執行時間超過**

  在指定時間段過後，工作被自動停止，無論它是否完成。

  如果您想要中斷或停止執行時間太長的工作，則啟用該選項。

  預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

10. 點擊**儲存**按鈕。

    工作被建立和配置。

當管理伺服器執行*將更新下載至管理伺服器儲存區*工作時，資料庫和軟體模組更新將從更新來源下載並儲存在管理伺服器共用資料夾中。如果您為管理群組建立此工作，它將僅被套用到包含在指定管理群組中的網路代理。

如果您在連線到網際網路時使用代理伺服器，則必須在管理伺服器屬性中指定代理伺服器位址。否則，*將更新下載至管理伺服器儲存區*工作將無法運行。

瀏覽已下載的更新

當管理伺服器執行*將更新下載至管理伺服器儲存區*工作時，資料庫和軟體模組更新將從更新來源下載並儲存在管理伺服器共用資料夾中。您可以在**卡巴斯基資料庫和軟體模組更新**區域中檢視下載的更新。

要檢視已下載的更新，

在主功能表中，轉至 **軟體管理 → 卡巴斯基應用程式 → 卡巴斯基資料庫和軟體模組更新**。

可用更新清單被顯示。

驗證已下載的更新

安裝更新到受管理裝置之前，您可以先透過*更新驗證*工作檢查更新。*更新驗證*工作會自動作為*將更新下載至管理伺服器儲存區*工作的一部分執行。管理伺服器從更新來源下載更新、將其儲存在臨時儲存區並執行*更新驗證*工作。如果工作成功完成，更新將從臨時儲存區複製到管理伺服器儲存區。它們被分發到所有以該管理伺服器為更新來源的用戶端裝置。

如果在*更新驗證*工作的過程中，位於臨時儲存區的更新不正確，或者*更新驗證*工作以錯誤結束，則這些更新不會被複製到管理伺服器儲存區。管理伺服器保留之前的更新集。此外，有**當新更新下載至儲存區時**排程類型的工作也不會啟動。若新更新的掃描成功完成，這些操作會在*將更新下載至管理伺服器儲存區*工作下次啟動時執行。

如果在一台或多台測試裝置上出現以下情況，那麼更新就被認為是無效的：

- 發生了更新工作錯誤。
- 安全應用程式的即時防護狀態在套用更新後變更。
- 執行自訂掃描工作過程中發現一個被感染的物件。
- Kaspersky 程式出現執行階段錯誤。

如果在任何測試裝置上未出現以上情況，則此更新集就被認為是有效的，*更新驗證*工作被認為已成功完成。

在開始建立*更新驗證*工作之前，執行先決條件：

1. 用幾個測試裝置建立管理群組。您將需要該組來驗證更新。

   我們建議使用網路中防護最可靠、應用程式設定最常用的裝置作為測試裝置。這種方法提高了掃描期間病毒偵測的品質和概率，將誤報的風險降至最低。如果在測試裝置上偵測到病毒，*更新驗證*工作將被判定為不成功。

2. 為Open Single Management Platform支援的應用程式（例如 Kaspersky Endpoint Security for Linux）建立更新和惡意軟體掃描工作。當建立更新和惡意軟體掃描工作時，指定測試裝置的管理群組。

   *更新驗證*工作將在測試裝置上順序執行更新和惡意軟體掃描工作以檢查所有更新是否有效。此外，在建立*更新驗證*工作時，您需要指定更新和惡意軟體掃描工作。

3. 建立*將更新下載至管理伺服器儲存區*工作。

若要讓 Kaspersky Next XDR Expert 在將下載的更新發佈至用戶端裝置之前進行驗證：

1. 在主功能表中，轉至 **工作**。
2. 點擊**將更新下載至管理伺服器儲存區**工作。
3. 在開啟的工作內容視窗中，轉到**應用程式設定**頁簽，然後啟用**執行更新驗證**選項。
4. 如果存在*更新驗證*工作，請點擊**選取工作**按鈕。在開啟的視窗中，在測試裝置的管理群組中選取*更新驗證*工作。
5. 如果您之前沒有建立*更新驗證*工作，請執行以下操作：
   a. 點擊**新工作**按鈕。
   b. 在開啟的新工作精靈中，如果要變更預設名稱，請指定工作名稱。
   c. 選擇您之前建立的具有測試裝置的管理群組。
   d. 首先，選擇Open Single Management Platform支援的所需應用程式的更新工作，然後選擇惡意軟體掃描工作。

之後，將出現以下選項。我們建議啟用它們：

- **在資料庫更新後重新啟動裝置**

  在裝置上更新病毒資料庫後，我們建議重新啟動裝置。

  預設情況下已啟用該選項。

- **在資料庫更新和裝置重新啟動後檢查即時防護狀態**

  如果啟用此選項，則*更新驗證*工作將檢查下載到管理伺服器儲存區的更新是否有效，以及在病毒資料庫更新和裝置重啟後防護等級是否降低了。

  預設情況下已啟用該選項。

e. 指定一個帳戶，*更新驗證*工作將從該帳戶執行。您可以使用您的帳戶並保持**預設帳戶**選項處於啟用狀態。或者，您可以指定工作應在具有必要存取權限的另一個帳戶下執行。為此，請選擇**指定帳戶**選項，然後輸入該帳戶的憑據。

6. 點擊**儲存**關閉*將更新下載至管理伺服器儲存區*工作的內容視窗。

自動更新驗證被啟用。現在，您可以執行*將更新下載至管理伺服器儲存區*工作，它將從更新驗證開始。

建立「將更新下載至發佈點儲存區」工作

您可以為管理群組建立*將更新下載至發佈點儲存區*工作。該工作將為包含在指定管理群組中的發佈點執行。

您可以使用該工作，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

該工作用在從 Kaspersky 更新伺服器下載更新到發佈點儲存區時。更新清單包含：

- Kaspersky 安全應用程式資料庫和軟體模組更新
- Kaspersky Next XDR Expert 元件更新
- Kaspersky 安全應用程式更新

更新被下載後，它們可以被傳播到受管理裝置。

*若要針對選取的管理群組建立**將更新下載至發佈點儲存區**工作：*

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。
3. 針對 Kaspersky Next XDR Expert 應用程式，在**工作類型**欄位中選取**將更新下載至發佈點儲存區**。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取一個選項按鈕以指定管理群組、裝置分類或應用程式工作的裝置。
6. 在**完成工作建立**步驟中，如果要修改預設工作設定，請啟用**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時變更預設設定。

7. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。

8. 按一下建立的工作的名稱以開啟工作內容視窗。

9. 在工作內容視窗的**應用程式設定**頁籤，指定以下設定：

   - **更新來源**

     以下資源可作為發佈點的更新來源：

     - Kaspersky 更新伺服器

       Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

       預設情況下已選取此選項。

     - 本機或網路資料夾

       包含最新更新的本機或網路資料夾。只有已安裝的 SMB 共用才能用作網路資料夾。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

       > 在*將更新下載至管理伺服器儲存區*工作和*將更新下載至發佈點的儲存區*工作中，如果您選擇受密碼防護的本機或網路資料夾作為更新來源，則使用者身分驗證不起作用。要解決此問題，首先掛接受密碼防護的資料夾，然後指定所需的憑據，例如，透過作業系統。之後，您可以選擇此資料夾作為更新下載工作中的更新來源。Open Single Management Platform不需要您輸入憑證。

   - **更新儲存資料夾**

     用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

   - **下載差異檔案**

     該選項啟用下載 diff 檔案功能。

     預設情況下已停用該選項。

   - **使用舊配置下載更新**

     Open Single Management Platform使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新**選項。否則，更新下載工作將失敗。

     例如，當指定本機或網路資料夾作為更新來源，且此資料夾中的更新檔案是由使用舊方案下載更新的 Kaspersky Update Utility 所下載時，您必須啟用此選項。

     預設情況下已停用該選項。

10. 為工作啟動建立排程。如果必要，配置以下設定：

    - **開始工作**:

      - **手動**（預設選取）

        工作不自動執行。您僅可以手動啟動。

        預設情況下已選定此選項。

- **每 N 分鐘**

  工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

  預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

- **每 N 小時**

  工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

  預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

- **每 N 天**

  工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

  預設下，工作每天執行一次，從目前系統日期和時間開始。

- **每 N 星期**

  工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

  預設下，工作每星期五於目前系統時間執行一次。

- **每天（不支援日光節約時間）**

  工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

  我們不建議您使用該排程。這是 Kaspersky Next XDR Expert 向後相容所必需的。

  預設下，工作每天於目前系統時間執行一次。

- **每週**

  工作每週在指定星期和指定時間執行。

- **按每週中的指定日**

  工作定期執行，在每周指定日期的指定時間。

  預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。

  在缺少指定日的月份，工作在最後一天執行。

  預設下，工作在每月的第一天執行，在目前系統時間。

- **每月於選定的週間日**

  工作定期在指定月日的指定時間執行。

  預設情況下，開始時間為18:00，且未選擇當月的任何日期。

  > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

  您可以選擇一週中的多個日期。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機化延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

11. 點擊**儲存**按鈕。

工作被建立和配置。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

執行*將更新下載至發佈點儲存區*工作時，資料庫和軟體模組更新從更新來源下載並儲存在共用資料夾。下載的更新將僅被包含在指定管理群組的發佈點和沒有更新下載工作的更新代理使用。

為將更新下載到管理伺服器儲存區工作新增更新來源

當您建立或使用將更新下載到管理伺服器儲存區的工作時，您可以選擇以下更新來源：

- Kaspersky 更新伺服器
- 主管理伺服器

  該資源套用到為從屬或虛擬管理伺服器建立的工作。
- 本機或網路資料夾

  該資源套用到為從屬或虛擬管理伺服器建立的工作。
- 網路資料夾

在*將更新下載至管理伺服器儲存區*工作和*將更新下載至發佈點的儲存區*工作中，如果您選擇受密碼防護的本機或網路資料夾作為更新來源，則使用者身分驗證不起作用。要解決此問題，首先掛接受密碼防護的資料夾，然後指定所需的憑據，例如，透過作業系統。之後，您可以選擇此資料夾作為更新下載工作中的更新來源。Open Single Management Platform不需要您輸入憑證。

預設使用卡巴斯基更新伺服器，但您也可以從本機或網路資料夾下載更新。如果您的網路無法存取網際網路，您可能希望使用該資料夾。在這種情況下，您可以從卡巴斯基更新伺服器手動下載更新，並將下載的檔案放在必要的資料夾中。

您只能指定一個本機或網路資料夾路徑。作為本機資料夾，您必須指定管理伺服器安裝所在裝置上的資料夾。作為網路資料夾，您可以使用 FTP 或 HTTP 伺服器，或者 SMB 共用。如果 SMB 共用需要身分驗證，則必須提前使用所需的憑據將其安裝在系統中。我們建議不要使用 SMB1 協定，因為它不安全。

如果您同時新增卡巴斯基更新伺服器和本機或網路資料夾，更新將首先從該資料夾下載。如果下載時出錯，將使用卡巴斯基更新伺服器。

如果包含更新的共用資料夾受密碼防護，請啟用**指定帳戶以存取更新來源的共用資料夾（如果有）**選項並輸入存取所需的帳戶憑據。

要新增更新來源：

1. 在主功能表中，轉至 **工作**。
2. 點擊**將更新下載至管理伺服器儲存區**。
3. 轉到**應用程式設定**標籤。
4. 在**更新來源**行中，點擊**設定**按鈕。
5. 在開啟的視窗中，點擊**新增**按鈕。

6. 在更新來源清單中，新增必要的來源。如果您選擇**工作資料夾**或**本機或網路資料夾**核取方塊，請指定資料夾的路徑。

7. 點擊**確定**，然後關閉更新來源內容視窗。

8. 在更新來源視窗中，點擊**確定**。

9. 點擊工作視窗中的**儲存**按鈕。

現在更新被從指定來源下載到管理伺服器儲存區。

批准和拒絕軟體更新

更新安裝工作的設定可能需要對要安裝的更新進行批准。您可以批准必須安裝的更新並拒絕不能安裝的更新。

例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些更新到用戶端裝置。

> 核准和拒絕更新僅適用於安裝在 Windows 型用戶端裝置上的網路代理和受管理應用程式。不支援管理伺服器、OSMP主控台和管理Web外掛程式的無縫更新。若要更新這些元件，您必須手動安裝。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉至**軟體管理→卡巴斯基應用程式→無縫更新**。
   可用更新清單被顯示。

   > 受管理應用程式的更新可能需要安裝卡巴斯基安全管理中心特定的最低版本。如果此版本晚於目前版本，則顯示這些更新，但無法核准。同樣，在升級卡巴斯基安全管理中心之前，無法從此類更新中建立安裝軟體套件。提示您將卡巴斯基安全管理中心執行個體升級到所需的最低版本。

2. 如有必要，請點擊**檢視和接受產品授權協議**按鈕以接受 EULA。

3. 選取您要批准或拒絕的更新。

4. 點擊**批准**以核准選取的更新或**拒絕**以拒絕選取的更新。
   預設值是*未定義*。

您分配了*已批准*狀態的更新被放置在安裝佇列。

您分配了*已拒絕*狀態的更新被從先前將其安裝的裝置上移除（如果可能）。而且，它們將來也不會被安裝到其他裝置。

Kaspersky 應用程式的一些更是無法被移除。如果您為這些更新設定*已拒絕*狀態，Kaspersky Next XDR Expert 將不會從先前已安裝這些更新的裝置上移除這些更新。然而，這些更新將來也不會被安裝到其他裝置。

如果您為協力廠商軟體更新設定了*已拒絕*狀態，則已計畫但未安裝這些更新的裝置將不會安裝這些更新。更新將保持在已將其安裝的裝置上。如果您必須刪除更新，您可以在本機手動刪除它們。

自動安裝 Kaspersky Endpoint Security for Windows 的更新

您可以在用戶端裝置上配置 Kaspersky Endpoint Security for Windows 自動更新資料庫和軟體模組。

要在裝置上配置下載和自動安裝 Kaspersky Endpoint Security for Windows 更新：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。
3. 對於 Kaspersky Endpoint Security for Windows 應用程式，選取**更新**作為工作子類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取工作範圍。
6. 指定管理群組、裝置分類或應用程式工作的裝置。
7. 在**完成工作建立**步驟中，如果要修改預設工作設定，請啟用**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時變更預設設定。
8. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。
9. 按一下建立的工作的名稱以開啟工作內容視窗。
10. 在工作內容視窗的**應用程式設定**頁籤，定義本機或行動模式的更新工作設定：
    - **本機模式**：連線會在裝置和管理伺服器之間建立。
    - **行動模式**：Kaspersky Next XDR Expert 與裝置之間未建立連線（例如，裝置未連線至網際網路時）。
11. 啟用您要用來更新 Kaspersky Endpoint Security for Windows 資料庫與應用程式模組的更新來源。如有必要，請使用**向上移動**與**向下移動**按鈕變更清單中的來源位置。若啟用數個更新來源，Kaspersky Endpoint Security for Windows 會嘗試逐一連線，從清單頂端開始，並透過第一個可用來源的更新套件執行更新工作。
12. 啟用**安裝批准的應用程式模組更新**選項，在更新應用程式資料庫同時下載和安裝軟體模組。

如果啟用該選項，Kaspersky Endpoint Security for Windows 在執行更新工作時，會通知使用者有可用的軟體模組更新並且更新套件包含軟體模組更新。Kaspersky Endpoint Security for Windows 僅安裝您已設為*已批准*狀態的更新；這些更新將透過應用程式介面或 Kaspersky Next XDR Expert 在本機安裝。

您也可以啟用**自動安裝關鍵應用程式模組更新**選項。如果軟體模組有任何更新，Kaspersky Endpoint Security for Windows 自動安裝*關鍵*狀態的更新；其餘的更新會在您批准後安裝。

如果軟體模組更新需要審查並接受產品授權協議的隱私政策，程式將在使用者接受最終使用者產品授權協議的條款和隱私政策後安裝更新。

13. 選取**複製更新到資料夾**核取方塊，程式將已下載的更新儲存到指定的資料夾。

14. 排程工作。若要確保定期更新，建議您選取**當新更新下載至儲存區時**選項。

15. 點擊**儲存**按鈕。

更新工作在執行時，程式傳送請求到 Kaspersky 更新伺服器。

一些更新需要安裝最新版本的管理外掛程式。

關於使用 diff 檔案更新 Kaspersky 資料庫和軟體模組

Kaspersky Next XDR Expert 從卡巴斯基更新伺服器下載更新時，會使用 diff 檔案來最佳化流量。您也可以對從網路中其他裝置（管理伺服器、發佈點和用戶端裝置）獲取更新的裝置啟用對 diff 檔案的使用。

關於下載 diff 檔案功能

diff 檔案敘述了資料庫或軟體模組的檔案的兩個版本之間的差異。使用 diff 檔案節省您公司網路內的流量，因為 diff 檔案相比資料庫和軟體模組的完整檔案佔據更少的空間。如果對管理伺服器或發佈點啟用 *下載 diff 檔案*功能，diff 檔案被儲存到該管理伺服器或發佈點。結果，從該管理伺服器或發佈點獲取更新的裝置可以使用儲存的 diff 檔案更新它們的資料庫和軟體模組。

要最佳化對 diff 檔案的使用，我們建議您根據管理伺服器或發佈點的更新排程同步從管理伺服器或更新代理獲取更新的的裝置的更新排程。然而，即便裝置更新頻率小於從其獲取更新的管理伺服器或發佈點，流量也被節省。

發佈點不對 diff 檔案的自動分發使用 IP 多點傳送。

啟用下載 diff 檔案功能

階段

1. **在管理伺服器上啟用功能。**

   在*將更新下載至管理伺服器儲存區*設定中啟用該功能。

2. **為發佈點啟用該功能**

   對透過"*將更新下載至發佈點儲存區*"工作接收更新的發佈點啟用該功能。

   接著啟用對從管理伺服器接收更新的發佈點的網路代理政策設定中啟用該功能。

   接著啟用對從管理伺服器接收更新的發佈點啟用該功能。

   該功能會在網路代理政策設定中啟用，並且當您手動分配發佈點，而且您要在管理伺服器內容中的**發佈點**區域覆寫政策設定。

要檢查下載 diff 檔案功能是否被成功啟用，您可以在執行方案之前和之後分別測試內部流量。

透過發佈點下載更新

Kaspersky Next XDR Expert 允許發佈點從管理伺服器、Kaspersky 伺服器或本機或網路資料夾接收更新。

要為發佈點設定更新下載：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊將透過其將更新傳送到群組中的用戶端裝置的發佈點的名稱。
4. 在發佈點內容視窗中，選取**更新來源**區域。
5. 為發佈點選取更新來源：

   - **更新來源**

     為發佈點選取更新來源：

     - 要允許發佈點從管理伺服器自動接收更新，選取**從管理伺服器接收**。
     - 若要透過工作允許發佈點接收更新，請選取 **使用更新下載工作**，然後指定一個*將更新下載到發佈點的儲存區*工作：
       - 如果裝置上已存在此類工作，請在清單中選擇該工作。
       - 如果裝置上尚不存在此類工作，請按一下**建立工作**連結以建立工作。新工作精靈啟動。遵照精靈的說明。

- **下載差異檔案**

  該選項啟用下載 diff 檔案功能。

  預設情況下已啟用該選項。

發佈點將從指定的更新來源接收更新。

在離線裝置上更新 Kaspersky 資料庫和軟體模組

依照既定程序安裝未通過認證測試的 Kaspersky 應用程式可執行模組更新（消除已知弱點的更新除外），會導致應用程式失去認證狀態。

在受管理裝置上更新 Kaspersky 資料庫和軟體模組是個重要的工作，它維持裝置的防護以防範病毒和其他威脅。管理員通常透過使用管理伺服器儲存區來配置定期更新。

當您需要在未連線到管理伺服器（主要或次要）、發佈點或網際網路的裝置（或裝置群組）上更新資料庫和軟體模組時，您必須使用其他更新來源，例如 FTP 伺服器或本機資料夾。此種情況下，您必須使用大容量裝置傳送所需更新的檔案，例如快閃記憶體磁碟機或外部硬碟磁碟機。

您可以從這裡複製所需更新：

- 管理伺服器。

  為確保管理伺服器儲存區包含所需的安裝在離線裝置上的安全應用程式的更新，至少一台受管理的線上裝置必須安裝了相同的安全應用程式。您必須設定此應用程式，才可透過*將更新下載至管理伺服器儲存區*工作，從管理伺服器儲存區接收更新。

- 任何安裝了相同安全應用程式的裝置，並配置了從管理伺服器儲存區接收更新，或直接從 Kaspersky 更新伺服器接收更新。

以下是透過從管理伺服器儲存區複製而更新資料庫和軟體模組的例子。

要在離線裝置上更新 Kaspersky 資料庫和軟體模組：

1. 連線卸除式磁碟機到管理伺服器所在裝置。

2. 複製更新檔案到卸除式磁碟機。

   預設下，更新位於： /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   或者，您可以配置Open Single Management Platform定期複製更新到您選取的資料夾。為此，請使用*將更新下載至管理伺服器儲存區*工作內容中的**複製下載的更新至其他資料夾**選項。如果您指定快閃記憶體磁碟機或外部硬碟磁碟機上的資料夾作為該選項的目的資料夾，該大容量裝置將總是包含更新的最新版本。

3. 在離線裝置上，配置 Kaspersky Endpoint Security 以從本機資料夾或共用資料夾接收更新，例如 FTP 伺服器或共用資料夾。

   說明：

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

4. 從卸除式磁碟機複製更新到您想用作更新來源的本機資料夾或共用資源。

5. 在需要更新安裝的離線裝置上，啟動 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的*更新*工作，具體取決於離線裝置的作業系統。

在更新工作完成後，Kaspersky 資料庫和軟體模組在裝置上變為最新。

用戶端裝置的遠端診斷

您可在 Windows 和 Linux 用戶端裝置上遠端執行遠端診斷：

- 啟用和關閉偵錯、變更偵錯等級並下載偵錯檔案
- 下載系統資訊和應用程式設定
- 下載事件記錄
- 為應用程式建立記憶體傾印檔案
- 開始進行診斷並下載診斷報告
- 啟動、停止和重新啟動應用程式

您可以使用從用戶端裝置下載的事件記錄和診斷報告以自行定位問題。同時，若您聯絡 Kaspersky 技術支援，他們可能會請您從用戶端裝置下載偵錯檔案、傾印檔案、事件記錄和診斷報告以讓 Kaspersky 進一步分析。

開啟遠端診斷視窗

若要執行對 Windows 和 Linux 用戶端裝置的遠端診斷，您必須開啟遠端診斷視窗。

開啟遠端診斷視窗：

1. 選取您要開啟遠端診斷視窗的裝置，並執行以下其中一個操作：
   - 若裝置屬於管理群組，請在主功能表中，前往**資產管理 → 資產（裝置）**。
   - 若裝置屬於「未指派的裝置」群組，請在主功能表中，轉至**資產管理→未指派的裝置**。
2. 點擊所需裝置的名稱。
3. 在開啟的裝置內容視窗中，選取**進階**頁籤。
4. 在**進階**頁籤上，按一下**遠端診斷**。

   這會開啟用戶端裝置的**遠端診斷** 視窗。如果管理伺服器和用戶端裝置之間未建立連線，則會顯示錯誤訊息。

或者，如果您需要立即獲取有關基於 Linux 的用戶端裝置的所有診斷資訊，您可以在此裝置上執行 collect.sh 指令碼。

啟用與停用應用程式偵錯

您可啟用和停用對應用程式的偵錯，包含 Xperf 偵錯。

啟用和停用偵錯

在遠端裝置上啟用或停用偵錯：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單上，選取您要啟用或停用偵錯的應用程式。

   遠端診斷選項清單隨即開啟。
4. 若您要啟用偵錯：

   a. 在**偵錯**區域中，點擊**啟用偵錯**。

   b. 在開啟的**修改偵錯等級**視窗中，建議您保留設定的預設值。當需要時，技術支援專家將指導您設定過程。提供以下功能：

   - **偵錯等級**

     偵錯等級定義偵錯檔案包含的詳情資料量。

   - **基於循環的偵錯**

     應用程式覆蓋偵錯資訊以防止偵錯檔案過量增長。指定用於儲存偵錯資訊的檔案最大數量，以及每個檔案的最大大小。如果寫入了最大數量的最大大小的偵錯檔案，最舊的檔案被刪除以便新偵錯檔案可以被寫入。

     此設定僅適用於 Kaspersky Endpoint Security

   c. 點擊**儲存**按鈕。

   偵錯會針對選取的應用程式啟用。某些情況下，要啟用偵錯，必須重新啟動安全應用程式及其工作。

   > 在基於 Linux 的用戶端裝置上，網路代理元件更新程式的偵錯由網路代理設定管理。因此，在執行 Linux 的用戶端裝置上，此元件的**啟用偵錯**和**修改偵錯等級**"選項被停用。

5. 若您要停用對選取的應用程式偵錯，請點擊**停用偵錯**按鈕。

   系統會針對選取的應用程式停用偵錯。

啟用 Xperf 偵錯

對於 Kaspersky Endpoint Security，技術支援專家可能需求您對系統效能資訊啟用 Xperf 偵錯。

要啟用和配置 Xperf 偵錯或停用它：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取 Kaspersky Endpoint Security for Windows。

   適用於 Kaspersky Endpoint Security for Windows 遠端診斷選項的清單隨即顯示。
4. 在**Xperf 偵錯**區域中，點擊**啟用 Xperf 偵錯**。

   若已啟用 Xperf 偵錯，則會改為顯示**停用 Xperf 偵錯**按鈕。如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊此按鈕。
5. 在開啟的**變更 Xperf 偵錯等級**視窗，根據技術支援專員的要求執行以下操作：

   a. 選取以下其中一個偵錯等級：

   - **輕度等級**

     該類型的偵錯檔案包含系統最少量資訊。

     預設情況下已選定此選項。
   - **深度等級**

     相比於*輕度*類型的偵錯檔案，該類型的偵錯檔案包含更多詳細資訊，且可能在*輕度*類型偵錯檔案不足以評估效能時被技術支援專家需求。*深度*偵錯檔案包含關於系統的硬體、作業系統、應用程式的啟動和結束處理程序清單、用於效能評估的事件和來自 Windows System Assessment 工具的事件的技術資訊。

   b. 選取以下其中一個 Xperf 偵錯類型：

   - **基本類型**

     偵錯資訊在 Kaspersky Endpoint Security 應用程式執行期間被接收。

     預設情況下已選定此選項。
   - **重新啟動時類型**

     偵錯資訊在作業系統從受管理裝置上啟動時接收。該偵錯類型在影響系統效能的問題發生時，在裝置被開啟後和 Kaspersky Endpoint Security 啟動之前有效。

   系統可能要求您啟用**循環檔案大小 (MB)**選項，以防止偵錯檔案的過量增長。然後指定偵錯檔案的最大大小。當檔案達到最大大小時，最舊的偵錯資訊被新資訊覆蓋。

   c. 定義輪換檔案大小。

   d. 點擊**儲存**按鈕。

系統會啟用並設定 Xperf 偵錯。

6. 如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊**Xperf 偵錯**區域中的**停用 Xperf 偵錯**。

   Xperf 偵錯已停用。

下載應用程式偵錯檔案

要下載應用程式的偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取您要為其下載偵錯檔案的應用程式。
4. 在**偵錯**部分中，點擊**偵錯檔案**按鈕。

   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。
5. 在偵錯檔案清單中，選取您要下載的檔案。
6. 執行以下操作之一：

   - 點擊**下載**來下載所選檔案。您可以選擇一個或多個檔案進行下載。
   - 下載部分選取的檔案：

     a. 點擊**下載一部分**。

     您無法同時下載多個檔案的部分內容。如果您選擇多個偵錯檔案，**下載一部分**按鈕將被停用。

     b. 在開啟的視窗中，根據您的需求指定要下載的名稱與檔案部分。

     對於基於 Linux 的裝置，無法編輯檔案部分名稱。

     c. 點擊**下載**。

選取的檔案或其部分會下載至您指定的位置。

刪除偵錯檔案

您可刪除不再需要的偵錯檔案。

若要刪除偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，選擇**事件記錄**頁簽。
3. 在**偵錯檔案**區段中，點擊**Windows Update 記錄**或**遠端安裝記錄**，視您要刪除的偵錯檔案而定。

Windows Update 記錄連接僅適用於基於 Windows 的用戶端裝置。

這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。

4. 在偵錯檔案清單中，選取一個或多個您要刪除的檔案。
5. 點擊**移除**按鈕。

選取的偵錯檔案被刪除。

下載應用程式設定

從用戶端裝置下載應用程式設定：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。
3. 在**應用程式設定**區段中，點擊**下載**按鈕，下載用戶端裝置上已安裝應用程式設定的資訊。

包含資訊的 ZIP 存檔將被下載到指定位置。

從用戶端裝置下載系統資訊

從用戶端裝置下載系統資訊：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**系統資訊**頁簽。
3. 點擊**下載**按鈕可下載有關用戶端裝置的系統資訊。
   如果您獲取有關基於 Linux 的裝置的系統資訊，則緊急終止的應用程式的傾印檔案會被新增到結果檔案中。

該封存檔案可能包含純文字形式的敏感資料（例如金鑰和密碼）。建議您在將封存檔案傳送給卡巴斯基技術支援之前，先檢查封存檔案中的檔案並移除此類資料。

包含資訊的檔案將下載到指定位置。

下載事件記錄

要從遠端裝置下載事件記錄：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗的**事件記錄**頁簽上，點擊**所有裝置記錄**。

3. 在**所有裝置記錄**視窗中，選取多個相關記錄。

4. 執行以下操作之一：

   - 點擊**下載整個檔案**來下載所選日誌。
   - 下載部分選取的記錄：

     a. 點擊**下載一部分**。
     您無法同時下載多個日誌的部分內容。如果您選擇多個事件記錄，**下載一部分**按鈕將被停用。

     b. 在開啟的視窗中，根據您的需求指定要下載的名稱與記錄部分。
     對於基於 Linux 的裝置，無法編輯記錄部分名稱。

     c. 點擊**下載**。

選取的事件記錄或其部分，會下載至指定的位置。

啟動、停止、重新啟動應用程式

您可在用戶端裝置啟動、停止、重新啟動應用程式。

若要啟動、停止和重新啟動應用程式，請執行以下操作：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。

3. 在應用程式清單中，選取您要啟動、停止或重新啟動的應用程式。

4. 點擊以下其中一個按鈕以選取操作：

   - **停止應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **重新啟動應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **啟動應用程式**
     此按鈕僅在應用程式不是正在執行時可供使用。

視您選取的操作而定，系統會啟動、停止或重新啟動應用程式。

若您重新啟動網路代理，系統會顯示訊息表示將失去裝置對管理伺服器的目前連線。

執行卡巴斯基安全管理中心網路代理的遠端診斷並下載結果

若要在遠端裝置上啟動卡巴斯基安全管理中心網路代理的診斷並下載結果：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選擇**卡巴斯基安全管理中心網路代理**。

   遠端診斷選項清單隨即開啟。
4. 在**診斷報告**區段中，點擊**執行診斷**按鈕。

   這會啟動遠端診斷程序並產生診斷報告。診斷程序完成時，您就能使用**下載診斷報告**按鈕。
5. 按一下**“ 下載診斷報告”**按鈕下載報告。

報告將下載到指定位置。

在用戶端裝置執行應用程式

您可能需要在用戶端裝置上執行應用程式，若 Kaspersky 支援專家要求您這樣做的時候。您無需在該裝置上安裝該應用程式。

若想在用戶端裝置上執行自訂指令碼，您可以使用 KLACDT_SAVE_SETTING 環境變數來確定儲存執行結果的路徑。例如：

- 對於基於 Windows 的裝置：

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```
- 對於基於 Linux 的裝置：

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

若要在用戶端裝置上執行應用程式：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。
3. 在**物件類型**欄位中，選取要上傳的物件類型：
   - 選取**檔案**以上傳可執行檔。
   - 選取**資料夾**以上傳包含要在用戶端裝置上執行的應用程式的資料夾。

     如果選取此物件類型，則會出現**要執行的可執行檔名稱**欄位。在此欄位中，指定資料夾中可執行檔的名稱。您也可以指定檔案的相對路徑。
   - 選取**存檔** 以上傳包含要在用戶端裝置上執行的應用程式的 ZIP 存檔。

如果選取此物件類型，則會出現**要執行的可執行檔名稱**欄位。在此欄位中，指定資料夾中可執行檔的名稱。您也可以指定檔案的相對路徑。

ZIP 存檔必須包含公用程式資料夾。此資料夾包含要在遠端裝置上執行的可執行檔。

4. 透過在系統視窗中選取物件或將其拖曳到上傳欄位來上傳物件。
5. 如果需要，在**命令列參數**欄位中指定執行可執行檔時要傳遞的命令列參數。
6. 點擊**上傳和執行**按鈕以在用戶端裝置上執行選定的應用程式。
7. 應用程式執行成功完成後，點擊**下載應用程式執行結果**按鈕即可下載執行結果。

會儲存應用程式執行結果，直到您執行新的診斷或關閉視窗。

使用該應用程式對用戶端裝置進行遠端診斷已完成。

為應用程式建立記憶體傾印檔案

應用程式傾印檔案允許您檢視某個時間點在用戶端裝置上執行的應用程式的參數。該檔案還包含有關為應用程式加載的模組的資訊。

不支援獲取來自 Linux 裝置的傾印檔案。

若要透過遠端診斷獲取傾印檔案，請使用 kldumper 公用程式。該公用程式旨在應技術支援專家的要求獲取卡巴斯基應用程式處理程序的傾印檔案。卡巴斯基安全管理中心知識庫中提供了有關使用 kldumper 公用程式的要求的詳細資訊。

要為應用程式建立傾印檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。
3. 在**正在產生處理程序傾印檔案**區域中，指定要為其產生傾印檔案的應用程式的可執行檔。
4. 點選**下載傾印檔案**按鈕。

   包含指定應用程式的傾印檔案的存檔被下載。

   如果指定的應用程式未在用戶端裝置上執行，則下載的存檔中包含的「結果」資料夾將為空。

   如果指定的應用程式正在執行，但下載失敗並出現錯誤，或下載的壓縮檔案中包含的「結果」資料夾為空，請參閱卡巴斯基安全管理中心知識庫。

在基於 Linux 的用戶端裝置上執行遠端診斷

Open Single Management Platform可讓您從用戶端裝置下載基本診斷資訊。或者，您可以使用卡巴斯基的 collect.sh 指令碼獲取關於 Linux 裝置的診斷資訊。此指令碼必須在需要診斷的 Linux 用戶端裝置上執行。接著會建立一個檔案，其中包含診斷資訊、裝置的系統資訊、應用程式偵錯檔案、裝置事件記錄，以及當機和終止程序的傾印檔案。

我們建議您使用 collect.sh 指令碼一次性獲取有關 Linux 用戶端裝置的所有診斷資訊。如果透過Open Single Management Platform遠端下載診斷資訊，您將需要瀏覽遠端診斷介面的所有部分。此外，Linux 裝置的診斷資訊可能無法完全獲得。

如果您需要將產生的包含診斷資訊的檔案傳送給卡巴斯基技術支援，請在傳送檔案之前刪除所有機密資訊。

要使用 collect.sh 指令碼從基於 Linux 的用戶端裝置下載診斷資訊：

1. 下載 collect.sh 指令碼，其封裝在 collect.tar.gz 壓縮檔案中。
2. 將下載的存檔複製到需要診斷的 Linux 用戶端裝置上。
3. 執行以下指令解壓 collect.tar.gz 存檔：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 執行以下指令以指定指令碼執行權限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理員權限的帳戶執行 collect.sh 指令碼：

   ```
   # ./collect.sh
   ```

一個包含診斷資訊的檔案產生並被儲存到 /tmp/$HOST_NAME-collect.tar.gz 資料夾中。

管理用戶端裝置上的協力廠商應用程式和可執行檔

本節說明 Kaspersky Next XDR Expert 中與管理在用戶端裝置上執行的協力廠商應用程式和可執行檔相關的功能。

使用「應用程式控制」來管理可執行檔

您可以使用「應用程式控制」元件來允許或阻止使用者裝置上可執行檔的啟動。「應用程式控制」元件支援基於 Windows 和 Linux 的作業系統。

對於 Linux 作業系統，從 Kaspersky Endpoint Security 11.2 for Linux 開始提供應用程式控制元件。

先決條件

- Kaspersky Next XDR Expert 已部署在您的組織中。
- Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的政策已建立並處於使用中狀態。政策中啟用了「應用程式控制」元件。

階段

應用程式控制使用情境分階段進行：

1. **形成和檢視用戶端裝置上可執行檔的清單**

   此階段可提供您受管理裝置上有哪些可執行檔的資訊。檢視可執行檔清單，並將其與允許和禁止的可執行檔清單比較。對可執行檔使用的限制可能與您組織中的資訊安全政策相關。

   操作說明：取得並檢視儲存在用戶端裝置上的可執行檔清單

2. **為組織中使用的可執行檔建立類別**

   分析受管理裝置上儲存的可執行檔清單。基於分析為可執行檔建立類別。建議您建立涵蓋組織中使用的可執行檔標準集的「工作應用程式」類別。若不同的安全群組在其工作中使用各自的可執行檔集，則可針對各安全群組建立獨立的應用程式類別。

   與任何應用程式控制規則不符的可執行檔啟動的設定，會由該元件選取的操作模式規管：

   - *拒絕清單*。若您要允許啟動所有可執行檔（除了封鎖規則所指定者），則會使用此模式。預設情況下會選取此模式。
   - *允許清單*。若您要封鎖啟動所有可執行檔（除了允許規則所指定者），則會使用此模式。

   應用程式控制規則是透過可執行檔的類別進行實作。Kaspersky Next XDR Expert 中有三種類型的可執行檔類別：

   - 含有手動新增內容的類別。您會定義條件，例如檔案中繼資料、檔案雜湊碼、檔案憑證、檔案路徑，以在類別中包含可執行檔。
   - 包含來自所選服務的可執行檔的類別。您指定之裝置的可執行檔會自動包含在類別中。
   - 包含來自所選資料夾的可執行檔的類別。您指定之資料夾中的可執行檔會自動包含在類別中。

3. **在 Kaspersky Endpoint Security 政策設定應用程式控制**

   使用您在先前階段建立的類別，在 Kaspersky Endpoint Security for Linux 政策中設定「應用程式控制」元件。

   操作說明：在 Kaspersky Endpoint Security for Windows 政策中配置應用程式控制

4. **在測試模式中開啟應用程式控制元件**

   若要確定應用程式控制規則沒有封鎖使用者工作所需的可執行檔，建議啟用應用程式控制規則測試，並在建立新規則後分析其運作。啟用測試後，Kaspersky Endpoint Security for Windows 不會封鎖應用程式控制規則封鎖啟動的可執行檔，但會改為傳送有關其啟動的資訊至管理伺服器。

測試應用程式控制規則時，建議執行以下動作：

- 決定測試期間。測試期間可從數日到兩個月。
- 檢查因應用程式控制作業產生的測試事件。

OSMP 主控台操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制元件 請依照此說明，並在設定過程中啟用**測試模式**選項。

5. **變更「應用程式控制」元件的設定**

   如有必要，請變更應用程式控制設定。根據測試結果，您可於包含手動新增內容的類別中，新增與「應用程式控制」元件事件相關的可執行檔。

   OSMP主控台操作說明：將與事件相關的可執行檔新增到應用程式類別

6. **在操作模式套用應用程式控制規則**

   測試應用程式控制規則且完成類別組態後，您可在操作模式中套用應用程式控制規則。

   OSMP 主控台操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制元件 請依照此說明，並在設定過程中停用**測試模式**選項。

7. **確認應用程式控制組態**

   請確保您已完成以下項目：

   - 為可執行檔建立類別。
   - 使用類別設定「應用程式控制」。
   - 在操作模式中套用應用程式控制規則。

結果

當情境完成時，受管理裝置上的可執行檔啟動會受到控制。使用者僅可啟動組織中允許的這些可執行檔，不可啟動被禁止的可執行檔。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

應用程式控制模式和類別

「應用程式控制」元件監控使用者啟動可執行檔的嘗試。您可以使用應用程式控制規則來控制可執行檔的啟動。

應用程式控制元件適用於 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

與任何應用程式控制規則不符的可執行檔啟動的設定，會由該元件選取的操作模式規管：

- *拒絕清單*。若您要允許啟動所有可執行檔（除了封鎖規則所指定者），則會使用此模式。預設情況下會選取此模式。
- *允許清單*。若您要封鎖啟動所有可執行檔（除了允許規則所指定者），則會使用此模式。

應用程式控制規則是透過可執行檔的類別進行實作。Kaspersky Next XDR Expert 中有三種類型的類別：

- 含有手動新增內容的類別。您會定義條件，例如檔案中繼資料、檔案雜湊碼、檔案憑證、檔案路徑，以在類別中包含可執行檔。
- 包含來自所選服務的可執行檔的類別。您指定之裝置的可執行檔會自動包含在類別中。
- 包含來自所選資料夾的可執行檔的類別。您指定之資料夾中的可執行檔會自動包含在類別中。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

取得並檢視安裝在用戶端裝置的應用程式清單

Kaspersky Next XDR Expert 會清查執行 Linux 和 Windows 的受管理用戶端裝置上安裝的所有軟體。

網路代理編輯安裝在裝置上的應用程式清單，並把該清單傳給管理伺服器。網路代理更新應用程式清單大約需要 10-15 分鐘。

對於 Windows 用戶端裝置，網路代理從 Windows 登錄接收有關已安裝應用程式的大部分資訊。對於 Linux 用戶端裝置，套件管理工具會向網路代理提供有關已安裝應用程式的資訊。

若要檢視安裝在受管理裝置上的應用程式清單：

1. 在主功能表中，轉至 **軟體管理 → 第三方應用程式 → 應用程式登錄資料**。

   該頁面顯示一個表格，其中包含安裝在受管理裝置上的應用程式。選取應用程式以檢視其內容，例如，供應商名稱、版本號、可執行檔清單、安裝了該應用程式的裝置清單、可用軟體更新清單和偵測到的軟體弱點清單。

2. 您可以按如下方式對包含已安裝應用程式的表格資料進行分組和篩選：

   - 按一下表格右上角的設定圖示（ ⚙ ）。

     在叫用的**表格設定**功能表中，選擇要在表格中顯示的欄。要檢視安裝應用程式的用戶端裝置的作業系統類型，請選擇**作業系統類型**欄。

   - 按一下表格右上角的篩選圖示（ ▽ ），然後在叫用的功能表中指定並套用篩選條件。

     顯示篩選後的已安裝應用程式表格。

若要檢視安裝在特定受管理裝置上的應用程式清單：

在主應用程式視窗中，前往 **裝置 → 受管理裝置 → 裝置名稱 → 進階 → 應用程式登錄資料**區段。在此功能表中，您可將應用程式清單匯出為 CSV 檔案或 TXT 檔案。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

取得並檢視儲存在用戶端裝置上的可執行檔清單

您可以透過以下方式之一獲取儲存在用戶端裝置上的可執行檔清單：

- 在 Kaspersky Endpoint Security 政策中啟用應用程式啟動通知。
- 建立清查工作。

在 Kaspersky Endpoint Security 政策中啟用應用程式啟動通知

要啟用有關應用程式啟動的通知：

1. 開啟 Kaspersky Endpoint Security 政策設定，然後轉至**一般設定** → **報告和儲存**。
2. 在**到管理伺服器的資料傳輸**設定群組中，選擇**關於啟動的應用程式**核取方塊，然後保存變更。

當使用者嘗試啟動可執行檔時，關於這些檔案的資訊將被新增到用戶端裝置上的可執行檔清單中。Kaspersky Endpoint Security 會將該資訊傳送到網路代理，然後網路代理會將其傳送到管理伺服器。

建立清查工作

對於 Kaspersky Endpoint Security for Linux，清查可執行檔的功能從 11.2 版本開始可用。

您可以在獲取已安裝應用程式的資訊時降低資料庫的負載。為了節省資料庫空間，請在安裝了標準軟體集合的參考裝置上執行清查工作。建議的裝置數量是 1-3。

要在用戶端裝置上為可執行檔建立清查工作：

1. 在主功能表中，轉至 **工作**。

   工作清單隨即顯示。

2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。

3. 在**新工作設定**頁面的**應用程式**下拉清單中，根據用戶端裝置的作業系統選擇 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows。
4. 在**工作類型**下拉清單中，選取**清單**。
5. 在**完成工作建立**頁面上，點擊**完成**按鈕。

在新工作精靈完成後，**清單**工作隨即建立且設定。如有需要，您可變更已建立工作的設定。新建立的工作會顯示在工作清單。

如須清查工作的詳細描述，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

執行**清單**工作後，會形成儲存在受管理裝置的可執行檔清單，您可檢視該清單。

清查期間可偵測以下格式的可執行檔（取決於您在清查工作內容中選擇的選項）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

檢視受管理裝置上儲存的可執行檔清單

要檢視儲存在用戶端裝置的可執行檔清單：

在主功能表中，轉至**軟體管理→第三方應用程式→可執行檔**。

此頁面會顯示儲存在用戶端裝置上的可執行檔清單。

如有必要，您可以將受管理裝置的可執行檔傳送到OSMP主控台在其中開啟的裝置。

若要傳送可執行檔：

1. 在主功能表中，轉至**軟體管理→第三方應用程式→可執行檔**。
2. 按一下要傳送的可執行檔的連結。
3. 在開啟的視窗中，轉至**裝置**區域，然後選擇要從其傳送可執行檔的受管理裝置的核取方塊。

   在傳送可執行檔之前，請確保受管理裝置已直接連線至管理伺服器，方法是選取**不斷開與管理伺服器的連線**核取方塊。

4. 點擊**傳送**按鈕。

   選定的可執行檔將下載，以便進一步傳送到OSMP主控台在其中開啟的裝置。

建立含有手動新增內容的應用程式類別

您可指定一組準則作為可執行檔的範本，這些範本是您希望在組織中允許或封鎖的啟動範本。根據對應該準則的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

要建立含有手動新增內容的應用程式類別：

1. 在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式類別**。

   應用程式類別清單頁面隨即顯示。

2. 點擊**新增**。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

3. 在**選取類別建立方法**步驟，指定應用程式類別名稱並選擇**含有手動新增內容的類別。可執行檔的資料被手動新增到該類別中**選項。

4. 在**條件**步驟，點擊**新增**按鈕新增條件準則，以在建立的類別中包含檔案。

5. 在「**條件標準**」步驟中，執行以下操作：

   a. 選取要建立類別的規則類型：

   - **從 KL 類別**

     如果選中此選項，作為新增應用程式到使用者類別的條件，您可以為應用程式指定 Kaspersky 類別。來自指定 Kaspersky 類別的應用程式將被新增到自訂應用程式類別。

   - **從儲存區選取憑證**

     如果選中此選項，則可以指定來自儲存區的憑證。類別條件僅符合指定憑證簽署的可執行檔。

     如果您建立並啟動了清查工作，並且在Kaspersky Endpoint Security政策中選取了**關於已啟動的應用程式**核取方塊，則憑證將新增至儲存區。您可以同時執行兩項操作。

     > 只能從 PE 格式（.exe、.dll、.sys）的可執行檔擷取憑證資訊。

   - **指定應用程式路徑（支援遮罩）**

     如果選中此選項，您可以指定包含要新增到使用者應用程式類別的可執行檔的用戶端裝置上的資料夾路徑。

   - **卸除式磁碟機**

     如果選中此選項，您可以指定應用程式在其上執行的媒體類型（任意裝置或行動裝置）。在所選驅動類型上執行的應用程式被新增到使用者應用程式類別。

   - **雜湊、檔案內容或憑證**：

     - **從可執行檔清單選取**

       如果選中此選項，可以使用用戶端裝置上的可執行檔清單來選取應用程式並將其新增到類別。

     - **從應用程式登錄資料選取**

       若已選取此選項，會顯示應用程式登錄資料。從登錄檔中選擇一個應用程式後，視窗將開啟，其中的參數將使用您選擇的應用程式的中繼資料進行填充：

       - 檔案名稱。
       - 檔案版本。您可指定版本的準確值或說明條件，例如「大於 5.0」。
       - 應用程式名稱。
       - 應用程式版本。您可指定版本的準確值或說明條件，例如「大於 5.0」。
       - 供應商。

       請注意，僅阻止滿足指定參數的可執行檔的啟動，而不是阻止您選擇的應用程式的啟動。如果選定的應用程式中繼資料與啟動應用程式時啟動的可執行檔的中繼資料相匹配，則可以繼續下一步。否則，您必須手動變更值以匹配可執行檔的中繼資料。

- **手動指定**

  如果選取此選項，您必須指定檔案雜湊或中繼資料或憑證，以作為新稱應用程式至使用者類別的條件。

  檔案雜湊值

  根據網路中裝置上所安裝安全應用程式的版本，您應選取 Kaspersky Next XDR Expert 用來計算此類別中檔案雜湊值的演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

  SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security for Linux 支援 SHA256 計算。

  請選取以下其中一個選項，讓 Kaspersky Next XDR Expert 計算此類別中檔案的雜湊值：

  - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security for Linux，請選擇 **SHA256**核取方塊。

  - 僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇**MD5 雜湊值**。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

  檔案內容

  若已選取此選項，您可指定檔案中繼資料作為檔案名稱、檔案版本、供應商。類別條件僅匹配具有相同中繼資料的可執行檔。

  憑證

  如果選中此選項，則可以指定來自儲存區的憑證。類別條件僅符合指定憑證簽署的可執行檔。

  如果您建立並啟動了清查工作，並且在Kaspersky Endpoint Security政策中選取了**關於已啟動的應用程式**核取方塊，則憑證將新增至儲存區。您可以同時執行兩項操作。

- **從封存資料夾**

  如果選擇此選項，您可以指定封存資料夾的檔案，然後選擇要使用哪個條件將應用程式新增到使用者類別。封存資料夾將被解壓縮，您選擇的條件將被套用於資料夾中的檔案。作為條件，您可以選取以下標準之一：

  - **檔案雜湊值**

    您選取要用於計算雜湊值的雜湊函數（MD5 或 SHA256）。和封存資料夾裡的檔案具有相同雜湊的應用程式被新增到自訂應用程式類別。

    僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇 MD5 雜湊函數。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

  - **檔案內容**

    您選擇要用作標準的中繼資料。包含相同檔案內容的可執行檔將被新增到自訂應用程式類別。

  - **憑證**

    您選擇要用作標準的憑證內容（憑證主旨、指紋或頒發者）。已用具有同樣內容的憑證簽章的可執行檔將被新增到使用者類別。

  如果您想使用這些標準，必須在上傳檔案或存檔資料夾後手動指定**檔案內容**和**憑證**標準。

  如果選擇此選項，您可以指定封存資料夾的檔案，然後選擇要使用哪個條件將應用程式新增到使用者類別。封存資料夾將被解壓縮，您選擇的條件將被套用於資料夾中的檔案。作為條件，您可以選取以下標準之一：

  - **檔案雜湊值**

    您選取要用於計算雜湊值的雜湊函數（MD5 或 SHA256）。和封存資料夾裡的檔案具有相同雜湊的應用程式被新增到自訂應用程式類別。

僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇 MD5 雜湊函數。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

- **檔案內容**

  您選擇要用作標準的中繼資料。包含相同檔案內容的可執行檔將被新增到自訂應用程式類別。

- **憑證**

  您選擇要用作標準的憑證內容（憑證主旨、指紋或頒發者）。已用具有同樣內容的憑證簽章的可執行檔將被新增到使用者類別。

如果您想使用這些標準，必須在上傳檔案或存檔資料夾後手動指定**檔案內容**和**憑證**標準。

b. 如有必要，可在「**描述**」欄位中新增註解。符號數量不得超過 1000 個。

之後，您將可編輯或刪除該註解。若要執行此操作，請在應用程式類別內容中開啟**條件**頁籤，然後在**條件標準**欄中，按一下您要編輯或刪除其註解的條件連結。

選取「**從 KL 類別**」規則類型時，可以為所有將基於此規則類型建立的條件新增一條註解。可以單獨編輯或刪除每個條件的註解。

選取的準則會新增至條件清單。

可以為正在建立的應用程式類別新增所需的任意數量的條件。

6. 在**排除**步驟，點擊**新增**按鈕新增排除條件準則，以從建立的類別排除檔案。

   如有必要，可以在「**描述**」欄位中新增註解。符號數量不得超過 1000 個。

   之後，您將可編輯或刪除該註解。為此，請在應用程式類別內容中開啟**排除**索引標籤，然後在**條件標準**欄中，按一下要編輯或刪除註解的條件連結。

7. 在**條件標準**步驟，從清單選取規則類型，與您為建立類別選取規則類型的方式一樣。

精靈完成後，應用程式類別即建立完成，並將顯示在應用程式類別清單中。當您設定應用程式控制時，您可使用建立的應用程式類別。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

建立應用程式類別以包含來自所選裝置的可執行檔

您可從選取的裝置使用可執行檔作為您希望允許或封鎖的可執行檔範本。根據選取裝置的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

請確保滿足以下先決條件：

- 在 Kaspersky Endpoint Security 政策中已啟用「應用程式控制」元件。
- 已取得受管理裝置上儲存的可執行檔的清單。

若要建立應用程式類別以包含來自所選裝置的可執行檔：

1. 在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式類別**。

   顯示包含可執行檔類別清單的頁面。

2. 點擊**新增**。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

3. 在**選取類別建立方法**步驟中，指定類別名稱，然後選取**包含所選裝置上可執行檔的類別。這些可執行檔被自動處理，它們的計量被新增到類別中**。

4. 點擊**新增**。

5. 在開啟的視窗中，選取一部裝置，或其中的可執行檔將用來建立應用程式類別的裝置。

6. 指定下列設定：

   - **雜湊值計算方法**

     根據網路中裝置上所安裝安全應用程式的版本，您應選取 Kaspersky Next XDR Expert 用來計算此類別中檔案雜湊值的演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

     SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security for Linux 支援 SHA256 計算。

     請選取以下其中一個選項，讓 Kaspersky Next XDR Expert 計算此類別中檔案的雜湊值：

     - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security for Linux，請選擇**SHA256**核取方塊。

     僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇**MD5 雜湊值**。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

     依預設，系統將選取**為該類別中的檔案計算 SHA256（由 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本支援）**核取方塊。

     為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

   - **與管理伺服器儲存區同步資料**

     選取此選項，若您希望管理伺服器定期在指定資料夾（或資料夾）檢查變更。

     預設情況下已停用該選項。

     若您啟用此選項，請指定時段（小時）以檢查指定資料夾（或資料夾）中的變更。依預設，掃描間隔為 24 小時。

   - **檔案類型**

     在此區段內，您可指定用來建立應用程式類別的檔案類型。

     所有檔案。所有檔案都會在建立類別時納入考量。預設情況下已選定此選項。

     僅應用程式類別之外的檔案。僅應用程式類別外的檔案會在建立類別時納入考量。

   - **資料夾**

     在此區段中，您可要指定已選取裝置中要用來建立應用程式類別的資料夾。

     所有資料夾。所有資料夾都會納入建立類別的考量。預設情況下已選定此選項。

指定資料夾。僅指定的資料夾會納入建立類別的考量。若您選取此選項，您必須指定連至資料夾的路徑。

精靈完成後就會建立可執行檔類別。它顯示在類別清單中。當您設定「應用程式控制」時，可使用已建立的類別。

建立應用程式類別以包含來自所選資料夾的可執行檔

您可從選取的資料夾使用可執行檔，將其作為組織中允許或封鎖的標準。以所選資料夾的可執行檔為依據，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

若要建立類別以包含來自所選資料夾的可執行檔：

1. 在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式類別**。

   類別清單頁面隨即顯示。

2. 點擊**新增**。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

3. 在**選取類別建立方法**步驟，指定類別名稱並選取**包含指定資料夾內可執行檔的類別。複製至指定資料夾的應用程式可執行檔被自動處理，它們的計量被新增到類別中**選項。

4. 指定其可執行檔將用於建立類別的資料夾。

5. 配置下列設定：

   - **包含動態連結程式庫 (DLL) 到該類別**

     應用程式類別包含動態連結程式庫（DLL 格式的檔案），應用程式控制元件記錄系統中執行的此類庫的操作。將 DLL 檔案包含在該類別中可能會降低 Kaspersky Next XDR Expert 的效能。

     預設情況下，此核取方塊已清除。

   - **包含指令碼到該類別**

     應用程式類別包含指令碼資料，指令碼不被 Web 威脅防護封鎖。將指令碼資料包含在該類別中可能會降低 Kaspersky Next XDR Expert 的效能。

     預設情況下，此核取方塊已清除。

   - **雜湊值計算演算法：為該類別中的檔案計算 SHA256（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支援）/ 為該類別中的檔案計算 MD5（在早於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的版本中支援）**

     根據網路中裝置上所安裝安全應用程式的版本，您應選取 Kaspersky Next XDR Expert 用來計算此類別中檔案雜湊值的演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

     SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security for Linux 支援 SHA256 計算。

     請選取以下其中一個選項，讓 Kaspersky Next XDR Expert 計算此類別中檔案的雜湊值：

     - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security for Linux，請選擇**SHA256**核取方塊。

     僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇**MD5 雜湊值**。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

     依預設，系統將選取**為該類別中的檔案計算 SHA256（由 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本支援）**核取方塊。

為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

- **強制掃描資料夾以尋找變更**

  如果啟用此選項，應用程式會定期檢查「類別屬性新增」資料夾的任何變化。您可以在該方塊旁的輸入欄位中指定檢查頻率（小時）。預設情況下，強制檢查的時間間隔為 24 小時。

  如果停用此選項，應用程式不會強制檢查資料夾。如果檔案被修改、新增或刪除，伺服器會嘗試存取這些檔案。

  預設情況下已停用該選項。

精靈完成後就會建立可執行檔類別。該類別顯示在類別清單中。您可在「應用程式控制」組態使用類別。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

檢視應用程式類別清單

您可檢視已設定可執行檔類別清單以及各類別的設定。

要檢視應用程式類別清單，

在主功能表中，轉至**軟體管理 → 第三方應用程式 → 應用程式類別**。

類別清單頁面隨即顯示。

若要檢視應用程式類別內容，

點擊類別的名稱。

類別的內容視窗隨即開啟。內容會在數個頁籤上分組。

在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制

建立應用程式控制類別後，您可將其用來在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制。

若要在 Kaspersky Endpoint Security for Windows 政策設定應用程式控制：

1. 在主功能表中，轉至 **資產管理 → 政策**。
   政策清單頁面隨即顯示。
2. 按一下 **Kaspersky Endpoint Security for Windows** 政策。
   政策設定視窗隨即開啟。

3. 轉到**應用程式設定→安全控制→應用程式控制**。

   含應用程式控制設定的**應用程式控制**視窗隨即顯示。

4. **應用程式控制**選項預設為啟用。切換切換按鈕**應用程式控制已停用**來停用該選項。

5. 在**應用程式控制設定**封鎖設定中，啟用操作模式以套用應用程式控制規則，並允許 Kaspersky Endpoint Security for Windows 封鎖應用程式啟動。

   如果要測試應用程式控制規則，請在**應用程式控制設定**區域啟用測試模式。在測試模式下，Kaspersky Endpoint Security for Windows 不會封鎖應用程式啟動，但會在報告中記錄有關觸發規則的資訊。點擊**檢視報告**連接可檢視此資訊。

6. 若您希望在使用者啟動應用程式時，要 Kaspersky Endpoint Security for Windows 監控 DLL 模組載入情況，請啟用**控制 DLL 模組載入**選項。

   模組與載入模組之應用程式的相關資訊將儲存至報告中。

   選取**控制 DLL 模組載入**選項後，Kaspersky Endpoint Security for Windows 僅會監控 DLL 模組和載入的驅動程式。選取**控制 DLL 模組載入**選項後，若您要 Kaspersky Endpoint Security for Windows 監控所有 DLL 模組和驅動程式，包含那些在 Kaspersky Endpoint Security for Windows 啟動前就已載入的項目，請重新啟動裝置。

7. （選用）在**訊息範本**區塊中，變更應用程式被封鎖啟動時顯示的訊息範本，以及會傳送給您的電子郵件訊息範本。

8. 在**應用程式控制模式**封鎖設定中，選取**拒絕清單**或**允許清單**模式。

   依預設會選取**拒絕清單**模式。

9. 按一下**規則清單設定**連結。

   拒絕清單與允許清單視窗隨即開啟以供您新增應用程式類別。選取**拒絕清單**模式時，依預設會選取**拒絕清單**頁籤，選取**允許清單**模式時會選取**允許清單**頁籤。

10. 在**拒絕清單與允許清單**視窗中，點擊**新增**按鈕。

    應用程式控制規則視窗將啟動。

11. 按一下**請選擇一個類別**連結。

    應用程式類別視窗隨即開啟。

12. 新增您先前建立的應用程式類別。

    您可按一下**編輯**按鈕來編輯已建立類別的設定。

    您可按一下**新增**按鈕建立新類別。

    您可按一下**刪除**按鈕從清單中刪除類別。

13. 完成應用程式類別清單後，請點擊**確定**按鈕。

    應用程式類別視窗隨即關閉。

14. 在**應用程式控制規則**視窗的**物件與其權限**區段中，建立要套用應用程式控制規則的使用者與使用者群組清單。

15. 點擊**確定**按鈕以儲存設定並關閉**應用程式控制規則**視窗。

16. 點擊 **確定** 按鈕以儲存設定並關閉**拒絕清單與允許清單**視窗。

17. 點擊**確定**按鈕以儲存設定並關閉**應用程式控制**視窗。

18. 關閉包含 Kaspersky Endpoint Security for Windows 政策設定的視窗。

應用程式控制已設定。政策填入用戶端裝置後，可執行檔啟動就會受管理。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明 。

新增事件相關的可執行檔到應用程式類別

當您在 Kaspersky Endpoint Security 政策中配置應用程式控制，以下事件會顯示在事件清單中：

- **應用程式遭禁止啟動**（*緊急*事件）。若您已設定應用程式控制來套用規則，則會顯示此事件。
- **應用程式在測試模式中遭禁止啟動**（*資訊*事件）。若您已設定用程式控制來測試規則，則會顯示此事件。
- **向管理員傳送的有關應用程式啟動禁止的訊息**（*警告*事件）。若您已設定應用程式控制來套用規則，則會顯示此事件，並且使用者已要求存取在啟動時遭封鎖的應用程式。

建議您建立事件分類來檢視與應用程式控制操作相關的事件。

您可新增與應用程式控制事件相關的可執行檔至現有應用程式類別或新的應用程式類別。您僅可將可執行檔，新增至透過手動新增內容的應用程式類別。

若要新增與應用程式控制事件相關的可執行檔到應用程式類別：

1. 在主功能表中，轉至 **監控 → 事件分類**。

   事件分類清單已顯示。

2. 選取事件分類來檢視與應用程式控制相關的事件並啟動此事件分類。

   若您尚未建立與應用程式控制相關的事件分類，您可選取並啟動預先定義的分類，例如**最近的事件**。

   事件清單隨即顯示。

3. 選取其中有您要新增至應用程式類別之可執行檔的事件，接著點擊**指派到類別**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

4. 在精靈頁面上，指定相關設定：

   - 在**對事件相關可執行檔採取的名稱**區段，選取以下其中一個選項：

     - **新增到新的應用程式類別**

       如果您需要根據事件相關的可執行檔建立新的應用程式類別，請選取此選項。

       預設情況下已選定此選項。

       若您已選取此選項，請指定新類別名稱。

     - **新增到現有應用程式類別**

       如果您需要新增事件相關可執行檔至現有應用程式類別，請選取此選項。

       預設情況下未選定此選項。

       若您已選取此選項，請選取您要新增可執行檔且有手動新增內容的應用程式類別。

- 在**規則類型**區域，選取以下選項之一：
  - **新增為包含項目的規則**
  - **新增為排除項目的規則**
- 在**用作條件的參數**區段中，選擇以下選項之一：
  - **憑證詳情（如果檔案沒有憑證，則為 SHA256 雜湊）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    每個檔案都有其獨特的 SHA256 雜湊函數。當您選取 SHA256 雜湊函數時，僅一個對應的檔案（例如定義的應用程式版本）組成類別。

    如果您要在類別規則中新增可執行檔的憑證詳情（或無憑證檔案的 SHA256 雜湊），請選取此選項。

    預設情況下已選定此選項。
  - **憑證詳情（沒有憑證的檔案將被略過）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    如果您要新增可執行檔的憑證詳情到類別規則，請選取此選項。如果可執行檔沒有憑證，該檔案將被略過。該檔案的資訊將不被新增到類別。
  - **僅 SHA256（沒有雜湊的檔案將被略過）**

    每個檔案都有其獨特的 SHA256 雜湊函數。當您選取 SHA256 雜湊函數時，僅一個對應的檔案（例如定義的應用程式版本）組成類別。

    如果您要僅新增可執行檔的 SHA256 雜湊函數詳情，請選取此選項。
  - **僅 MD5（停產模式，僅適用於 Kaspersky Endpoint Security 10 Service Pack 1 版本）**

    > 僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇此選項。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

    每個檔案都有單獨的 MD5 雜湊。當您選取 MD5 雜湊時，僅一個對應的檔案，例如，定義的應用程式版本，組成類別。

5. 點擊**"確定"**。

當精靈完成時，系統會新增與應用程式控制事件相關的可執行檔至現有應用程式類別或新的應用程式類別。您可檢視已修改或建立的應用程式類別的設定。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

建立安裝必要更新並修復弱點工作

*安裝所需更新並修復弱點*工作僅在有弱點和修補程式程序管理產品授權下才可使用。

*安裝所需更新並修復弱點*工作會用來更新與修復安裝在受管理裝置上協力廠商軟體中的弱點。此工作可讓您根據工作設定中指定的規則，安裝多個更新並修復多個弱點。

若要使用*安裝所需更新並修復弱點*工作安裝更新或修復弱點，您可進行以下一項操作：

- 執行更新安裝精靈或弱點修復精靈。
- 建立*安裝所需更新並修復弱點*工作。
- 對現有*安裝所需更新並修復弱點*工作新增安裝更新規則。

要建立安裝所需更新並修復弱點工作：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**應用程式**下拉式清單中，選擇 Kaspersky Next XDR Expert。
4. 在**工作類型**清單中，選擇**安裝所需更新並修復弱點**工作類型。

   如果沒有顯示該工作，請檢查您的帳戶是否具有**系統管理**：**弱點和修補程式管理**功能區域的**讀取**、**修改**和**執行**權限。如果沒有這些存取權限，您就不能建立及設定*安裝所需更新並修復弱點*工作。
5. 在**工作名稱**欄位，指定新工作的名稱。

   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
6. 選取要對其分配工作的裝置：
7. 在精靈的**指定安裝更新規則**步驟中，新增更新安裝規則。

   這些規則被套用到用戶端裝置上的更新安裝。如果規則未被指定，工作無可執行。對於具有規則的操作的資訊，請參閱更新安裝規則。

   這些規則被套用到用戶端裝置上的更新安裝。如果您不指定任何規則，則該工作無需執行任何操作。
8. 指定下列設定：

   - **在裝置重新啟動或關閉時開始安裝**

     如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。

     如果安裝更新可能影響裝置效能則使用該選項。

     預設情況下已停用該選項。

- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

- **更新過程中允許安裝新的應用程式版本**

  如果啟用該選項，當更新會導致安裝新版本的軟體應用程式時，則允許進行更新。

  如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

  預設情況下已啟用該選項。

  > 升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

  如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

  Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新到**欄位指定的資料夾。

  如果停用該選項，更新被自動安裝到裝置。

  預設情況下已停用該選項。

  - **下載更新到**

    該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

  如果啟用該功能，即便寫入偵錯檔案在Open Single Management Platform遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

  如果停用該功能，網路代理將根據Open Single Management Platform遠端診斷共用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

  當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

  預設情況下已停用該選項。

  - **進階診斷檔案的最大大小 (MB)**

    預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

轉到精靈的下一個步驟。

9. 指定作業系統重新啟動設定：

   - **不重新啟動裝置**

     用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

   - **重新啟動裝置**

     如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

   - **提示使用者動作**

     用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

     預設情況下已選定此選項。

   - **重複提示間隔（分鐘）**

     如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

     預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

     如果停用該選項，提示僅顯示一次。

   - **在該時間後重新啟動（分鐘）**

     提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

     預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

   - **強制關閉封鎖工作階段中應用程式前的等待時間（分鐘）**

     使用者裝置鎖定時，程式以強制模式關閉（指定不活動間隔之後自動鎖定，或手動鎖定）。

     如果啟用此選項，一旦輸入區域指定的時間間隔結束，鎖定裝置上的程式以強制模式關閉。

     如果停用此選項，鎖定裝置上的程式將不會關閉。

     預設情況下已停用該選項。

10. 在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項，即可修改預設工作設定。

    如果您不啟用該選項，工作使用預設設定建立。您可以稍後再修改預設設定。

11. 點擊**完成**按鈕。

    新工作精靈即會建立工作。如果您啟用了**建立完成時開啟工作詳情**選項，工作內容視窗即會自動開啟。在此視窗中，您可以指定一般工作設定，並視需要變更在工作建立期間指定的設定。

    > 您也可以透過在工作清單中點擊所建立工作的名稱，開啟工作內容視窗。

    工作隨即受到建立、設定，並顯示在工作清單。

12. 若要執行工作，請在工作清單選取該工作，然後點擊**開始**按鈕。

    您也可以在工作內容視窗的**排程**頁籤上，設定工作啟動排程。

    如需排程啟動設定的詳細說明，請參閱一般工作設定。

工作完成後，將安裝所需的更新並修復弱點。

如果您的組織網路中使用了 WSUS 伺服器（本機 WSUS 伺服器），並且您希望將其與管理伺服器一起使用，則必須先確保管理伺服器未用作 WSUS 伺服器，然後執行下列操作：

a. 在執行 Windows 的受管理裝置上，為 Windows 更新伺服器服務指定本機 WSUS 伺服器。您可以在 Windows 登錄檔中手動執行此操作，也可以使用 Windows 群組原則執行此操作。

b. 在本機 WSUS 伺服器上，指定所需的更新分類以及要在其上分發更新的應用程式。

c. 將您的 WSUS 伺服器與上游伺服器同步（這可以是 Microsoft WSUS 伺服器，也可以是另一個本地上游 WSUS 伺服器）。

在裝置上執行*安裝所需更新和修復弱點*工作後，網路代理使用 Windows 更新服務安裝 Windows 更新。Windows 更新服務從登錄檔獲取外部 WSUS 伺服器的位址，並直接從該外部伺服器下載更新。

「弱點掃描和所需更新」工作設定

除了一般工作設定外，您可在建立*弱點掃描和所需更新*工作，或在之後設定已建立工作的內容時，指定以下設定：

- **搜尋 Microsoft 列出的弱點和更新**

  搜尋弱點和更新時，Kaspersky Next XDR Expert 會使用 Microsoft 更新來源目前提供的適用 Microsoft 更新資訊。

  例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

  預設情況下已啟用該選項。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **連線更新伺服器以更新資料**

  受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

  - 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
  - Microsoft Updates 伺服器

  如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

  若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得。

  到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

  預設情況下已啟用該選項。

網路代理政策設定的以下選項組合會定義取得更新的模式：

- 只有在 *弱點掃描和所需更新*工作的內容中啟用**連線更新伺服器以更新資料**設定，並在網路代理政策設定中將**Windows Update 搜尋模式**設為**主動**時，受管理裝置上的 Windows 更新代理才會連線至更新伺服器以接收更新。

- 如果在執行 *弱點掃描*工作時不需要網路代理來啟動與 Microsoft Windows 更新來源的連線並下載更新，則可以將**Windows Update 搜尋模式**選項設為**被動**，同時**連線更新伺服器以更新資料**選項必須保持啟用狀態。這可讓您節省資源並使用先前收到的 Windows 更新來掃描弱點。如果您設定以不同方式接收 Microsoft Windows 更新，則可以使用被動模式。如果未以其他方式設定接收 Microsoft Windows 更新，請勿將**Windows Update 搜尋模式**選項設為**被動**，因為在這種情況下，將永遠不會收到有關更新的資訊。

- 無論**連線更新伺服器以更新資料**選項處於何種狀態（啟用或停用），如果**已停用**選項設為**Windows Update 搜尋模式**，Kaspersky Next XDR Expert 都不會請求任何更新資訊。

如果您的組織網路中使用了 WSUS 伺服器（本機 WSUS 伺服器），並且您希望將其與卡巴斯基安全管理中心管理伺服器一起使用，則必須先確保卡巴斯基安全管理中心管理伺服器未用作 WSUS 伺服器，然後執行下列操作：

1. 在執行 Windows 的受管理裝置上，為 Windows 更新伺服器服務指定本機 WSUS 伺服器。您可以在 Windows 登錄檔中手動執行此操作，也可以使用 Windows 群組原則執行此操作。

2. 在本機 WSUS 伺服器上，指定所需的更新分類以及要在其上分發更新的應用程式。

3. 將您的 WSUS 伺服器與上游伺服器同步（這可以是 Microsoft WSUS 伺服器，也可以是另一個本地上游 WSUS 伺服器）。

在裝置上執行*尋找弱點和所需更新*工作後，網路代理將使用 Windows 更新服務發起適用於該裝置的 Windows 更新請求。Windows 更新服務從登錄檔獲取外部 WSUS 伺服器的位址，並直接從該外部 WSUS 伺服器搜尋更新。然後，Windows 更新服務透過網路代理將此清單轉送到管理伺服器。因此，管理伺服器具有最新的庫。

- **搜尋卡巴斯基列出的第三方弱點和更新**

  如果啟用此選項，Kaspersky Next XDR Expert 會在 Windows 登錄檔以及**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中，搜尋第三方應用程式（由 Kaspersky 和 Microsoft 以外的軟體供應商開發的應用程式）的弱點和所需更新。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

  如果停用此選項，Kaspersky Next XDR Expert 不會搜尋第三方應用程式的弱點和所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

  預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

  Kaspersky Next XDR Expert 會在這些資料夾中搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

  指定應用程式安裝資料夾。預設下，清單包含大多數應用程式所安裝的系統資料夾。

- **啟用進階診斷**

  如果啟用該功能，即便寫入偵錯檔案在Open Single Management Platform遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小(MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

  如果停用該功能，網路代理將根據Open Single Management Platform遠端診斷共用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

工作排程的建議

排程*弱點掃描和所需更新*工作時，請確保啟用**執行錯過的工作**與**使用工作啟動自動隨機化延遲**兩個選項。

依預設，*弱點掃描和所需更新*工作設定為手動啟動。如果組織的工作場所規定要求此時關閉所有裝置，則*弱點掃描和所需更新*工作將在裝置重新開機後執行，也就是隔天早上。此活動可能不是必須的，因為弱點掃描可能增加 CPU 和磁碟子系統負載。您必須根據組織的工作規則為該工作設定最方便的排程。

OPENAPI 參考手冊

本「OpenAPI參考指南」旨在幫助完成以下工作：

- 自動化和客製化。您可以自動化您可能不想手動處理的工作。例如，作為管理員，您可以使用OpenAPI建立和執行指令碼，這些指令碼將有助於開發管理群組的結構，並使該結構保持最新狀態。
- 自訂開發。透過使用 OpenAPI，您可以開發用戶端應用程式。

您可以使用螢幕右側的搜尋欄位，在《OpenAPI 參考手冊》中找出您所需的資訊。

OPENAPI 參考手冊

指令碼範例

OpenAPI 參考指南包含下表中列出的 Python 指令碼範例。這些範例展示如何調用OpenAPI方法並自動完成各種網路防護工作，例如，建立一個「主要/從屬」層次結構，在Open Single Management Platform執行工作，或分配發佈點。您可以按原樣執行範例，也可以根據範例建立自己的指令碼。

使用者應用情境和OpenAPI方法樣本之間的匹配

範例	樣本目的	情景
記錄 KlAkParams	您可以使用 `KlAkParams` 資料結構來擷取與處理資料。該範例顯示如何使用此資料結構。 範例輸出可以以不同的方式呈現。您可以取得資料來傳送 HTTP 方法或在您的程式碼中使用它。	監控和報告
建立和刪除「主要/從屬」層次結構	您可以新增次要管理伺服器，進而建立「主要 / 次要」層級。或者，您可以中斷次要管理伺服器與層次結構的連線。	建立管理伺服器的層次結構，新增從屬管理伺服器，刪除管理伺服器的層次結構
透過連線閘道下載網路清單檔案到指定主機	您可以透過使用連線閘道連線到所需裝置的網路代理，然後將包含網路清單的檔案下載到您的裝置。	發佈點和連線閘道器的調整

範例	樣本目的	情景
將儲存在主管理伺服器儲存區中的產品授權金鑰安裝到從屬管理伺服器上	您可以連線到主管理伺服器，從其下載所需的產品授權金鑰，然後將此金鑰傳輸到層次結構中包含的所有從屬管理伺服器。	受管理應用程式的產品授權
建立有效的使用者權限報告	您可以建立不同的報告。例如，您可以使用此範例產生有效的使用者權限報告。此報告描述了使用者擁有的權限，具體取決於他或她的群組和角色而定。 您可以下載 HTML、PDF 或 Excel 格式的報告。	生成和瀏覽報告
啟動裝置工作	您可以透過使用連線閘道連線到所需裝置上的網路代理，然後執行必要的工作。	手動啟動工作
為群組中的裝置註冊發佈點	您可以將受管理裝置分配為發佈點（以前稱為更新代理）。	更新 Kaspersky 資料庫和應用程式
列舉所有群組	您可以對管理群組採取以下操作。該範例顯示如何執行以下操作： • 取得「受管理裝置」根群組的識別碼 • 在群組層次結構中移動 • 獲取完整的、擴展的群組層次結構及其名稱和巢狀結構	設定管理伺服器
列舉工作、查詢工作統計並執行工作	您可以找到以下資訊： • 工作進度記錄 • 目前工作狀態 • 不同狀態的工作數量 您還可以執行工作。預設情況下，範例會在輸出統計資訊後執行工作。	手動啟動工作
建立並執行工作	您可以建立工作。在範例中指定以下工作參數： • 類型 • 執行方法 • 名稱。 • 將使用工作的裝置群組 預設情況下，範例會建立一個「顯示訊息」類型的工作。您可以為管理伺服器的所有受管理裝置執行此工作。如有需要，您可以指定自己的工作參數。	建立工作
列舉產品授權金鑰	您可以獲得安裝在管理伺服器受管理裝置上之卡巴斯基應用程式的所有啟動產品授權金鑰的清單。該清單包含關於每個產品授權金鑰的詳細資料，例如名稱、類型或到期日期。	產品授權
建立一個自訂類別	您可以使用所需的參數建立應用程式類別。	建立含有手動新增內容的應用程式類別
使用 SrvView 列舉使用者	您可以使用 SrvView 類別向管理伺服器請求詳細資料。例如，您可以使用此範例取得使用者清單。	管理使用者和使用者角色

透過OpenAPI與Open Single Management Platform互動的應用程式

某些應用程式透過OpenAPI與Open Single Management Platform互動。此類應用程式包括，例如Kaspersky Anti Targeted Attack Platform。這也可以是您基於 OpenAPI 開發的自訂用戶端應用程式。

透過OpenAPI與Open Single Management Platform互動的應用程式連接到管理伺服器。要了解您使用的應用程式是否透過OpenAPI工作，請參閱此應用程式的說明。

監控和報告

本節說明 Kaspersky Next XDR Expert 的監控和報告功能。這些功能給您一個基礎架構、防護狀態和統計資訊的總覽。

部署 Kaspersky Next XDR Expert 後或在運作期間，您可以設定監控和報告功能，使其最符合您的需求。

方案：監控和報告

本節提供在 Kaspersky Next XDR Expert 中設定監控和報告功能的方案。

先決條件

在組織網路中部署 Kaspersky Next XDR Expert 後，您可以使用卡巴斯基安全管理中心監控網路的安全狀態並產生報告。

組織網路中的監控和報告分步驟進行：

1. **設定裝置狀態轉換**

   熟悉取決於特定條件的裝置狀態設定。透過變更這些設定，您可以變更帶有*緊急*或*警告*嚴重等級的事件數量。當配置裝置狀態切換時，確保以下：

   - 新設定不與您組織的安全政策資訊衝突。
   - 您可以及時對您組織網路中的重要安全事件做出反應。

2. **配置用戶端裝置上的事件通知**

   說明：

   配置用戶端裝置上的事件通知（透過郵件、SMS 或執行可執行檔）

3. **對嚴重、警告、資訊通知執行建議的操作**

   說明：

   對您的組織網路執行建議的操作

4. **檢視您組織網路的安全狀態**

   說明：

   - 檢閱防護狀態小工具
   - 產生並檢閱防護狀態報告
   - 產生並檢閱錯誤報告

5. **定位不被防護的用戶端裝置**

說明：

- 檢閱新裝置部件
- 產生並檢閱防護佈署報告

6. **檢查用戶端裝置防護**

   說明：

   - 從防護狀態和威脅統計資訊類別產生並檢閱報告
   - 啟動並檢閱緊急事件分類

7. **評估和限制資料庫上的事件負載**

   受管應用程式操作相關的事件資訊將被從用戶端電腦上傳輸並記錄至管理伺服器資料庫。要降低管理伺服器負載，評估和限制可以儲存在資料庫的最大事件數量。

   說明：

   - 限制最大事件數量

8. **檢視產品授權資訊**

   說明：

   - 新增產品授權金鑰使用小工具至控製板並加以檢閱
   - 產生並檢閱產品授權金鑰使用報告

結果

完成方案後，您被通知您組織網路的防護，因此可以為進一步防護排程操作。

關於監控和報告的類型

組織網路的安全事件資訊儲存在管理伺服器資料庫。OSMP主控台在您組織的網路中基於事件提供以下類型的監控和報告：

- 控製板
- 報告
- 事件分類
- 通知

控製板

儀表板透過對資訊進行圖形顯示來允許您監控您組織網路的安全趨勢。

報告

報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

- 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
- 依時間—**最近事件**
- 依類型—**使用者請求**和**稽核事件**

您可以在OSMP主控台介面中，根據可用設定建立並檢視使用者定義的事件選取，以進行配置。

通知

通知會警示您關於事件的資訊，並協助您透過執行建議動作或您認為適當的動作加速回應這些事件。

智慧培訓模式中的規則觸發

該部分提供了用戶端裝置上的 Kaspersky Endpoint Security for Windows 中的適應性異常控制規則執行的偵測資訊。

規則偵測用戶端裝置上的異常行為並可能封鎖它。如果工作為智慧培訓模式，它們將偵測異常行為並傳送每個偵測的報告到管理伺服器。您可以在**儲存區→智慧培訓狀態中的規則觸發器**中檢視有關偵測到的異常行為的報告。您可以確認偵測為正確或新增它們為排除，因此該行為類型不再被認為是異常。

偵測資訊儲存在管理伺服器的事件記錄中（與其他事件一起）和適應性異常控制報告中。

關於適應性異常控制、規則以及它們的模式和狀態的更多資訊，請參閱 Kaspersky Endpoint Security for Windows 說明。

檢視並確認使用自適應異常控制規則執行的偵測

要檢視使用適應性異常控制規則執行的偵測清單：

1. 在主功能表中，轉至**儲存區→智慧培訓狀態中的規則觸發器**。

   清單顯示使用適應性異常控制規則執行的偵測的以下資訊：

   - **管理群組**

     裝置所屬管理群組的名稱。

   - **虛擬管理伺服器**

     管理裝置的虛擬管理伺服器。

   - **裝置名稱**

     套用規則的用戶端裝置名稱。

   - **名稱**

     套用的規則名稱。

   - **狀態**

     正在排除 — 如果管理員處理該項目並新增其到排除規則清單。該狀態保持到下一次用戶端電腦與管理伺服器同步時，同步之後，該項目從清單消失。

     正在確認 — 如果管理員處理該項目並確認。該狀態保持到下一次用戶端電腦與管理伺服器同步時，同步之後，該項目從清單消失。

     空 — 如果管理員不處理該項目。

   - **偵測數量**

     一個啟發式規則中的偵測數量，一個處理程序和一個用戶端裝置。該數量由 Kaspersky Endpoint Security 計算。

   - **使用者名稱**

     執行產生偵測之處理程序的用戶端裝置使用者名稱。

   - **來源處理程序路徑**

     處理程序來源路徑，例如，執行操作的處理程序路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

   - **來源處理程序雜湊**

     處理程序原始檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

   - **來源物件路徑**

     啟動處理程序的物件路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **來源物件雜湊**

  原始檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標處理程序路徑**

  目的處理程序的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標處理程序雜湊**

  目的檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標物件路徑**

  目的物件的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標物件雜湊**

  目的檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **已處理**

  異常被偵測的日期。

檢視偵測內容：

1. 在主功能表中，轉至**儲存區→智慧培訓狀態中的規則觸發器**。
2. 執行以下操作之一：
   - 在**名稱**欄中，點擊包含要檢視的偵測名稱的連結。
   - 在偵測清單中，選取要檢視的偵測旁的核取方塊，然後點擊**內容**按鈕。

   將開啟所選偵測的內容視窗，顯示有關它的資訊。

您可以從自適應異常控制規則的偵測清單或所選偵測的內容視窗中確認任何偵測。

確認偵測：

- 在偵測清單中選取一個或多個偵測，然後點擊**確認**按鈕。
- 開啟選定偵測的內容視窗，然後點擊**確認**按鈕。

  偵測的狀態被變更為**正在確認**。用戶端裝置與管理伺服器下次同步後，偵測將從偵測清單中消失。

  您的確認將有助於規則使用的統計資料。有關詳細資訊，請參閱Kaspersky Endpoint Security for Windows 說明。

從適應性異常控制規則新增排除

"新增到自適應異常控制排除項目"精靈允許您從 Kaspersky Endpoint Security 的自適應異常控制規則中新增排除項目。

使用精靈新增自適應異常控制規則的排除項目：

1. 以下列方式之一啟動精靈：

   - 在主功能表中，轉至**儲存區→智慧培訓狀態中的規則觸發器**，選取一個或多個偵測，然後點擊**排除**按鈕。

     您可以一次新增 1000 個排除項目。

     在將偵測新增至排除項目之前，您可以透過點擊偵測名稱或**內容**按鈕來檢視偵測的屬性。在開啟的偵測內容視窗中，您也可以點擊**排除**按鈕。

   - 在主功能表中，前往**監控 → 事件分類**，點擊所需事件分類的連結，選中要排除的偵測旁邊的核取方塊，然後點擊**從自適應異常控制中排除**按鈕。

   "新增到自適應異常控制排除項目"精靈啟動。使用**下一步**按鈕進行精靈。

2. 選取您要新增排除的政策和設定檔。

   繼承的政策無法被更新。如果您沒有權限修改政策，政策將不被更新。

3. 點擊**完成**關閉精靈。

偵測狀態被變更為**正在排除**。用戶端裝置與管理伺服器下次同步後，偵測將從偵測清單中消失。已配置並套用自適應異常控制規則的排除項。

儀表板和小部件

本部分包含有關儀表板和儀表板提供的小工具的資訊。該部分包括有關如何管理小工具和配置小工具設定的說明。

使用儀表板

儀表板透過對資訊進行圖形顯示來允許您監控您組織網路的安全趨勢。

儀表板可在OSMP控制台中使用，路徑為**監控 → 控制板**。

儀表板提供可以自訂的部件。您可以選取大量不同的部件，顯示為圓形圖、表格、圖表和清單。小工具中顯示的資訊會自動更新，更新周期為一到兩分鐘。更新間隔根據不同部件而不同。您可以隨時透過設定選單手動刷新小工具上的資料。

儀表板包括**管理和保護**和**偵測和回應**頁籤，您可以在其中添加小工具。

管理與保護頁籤

管理與保護頁籤可以包含顯示管理伺服器資料庫中儲存的所有事件資訊的小工具。

在**管理和保護**頁籤中，以下群組的小小工具可用：

- **防護狀態**
- **佈署**
- **更新**
- **威脅統計資訊**
- **其他**

偵測和回應頁籤

偵測和回應標籤可以包含顯示有關偵測到和註冊的警示和事件以及對其採取的回應措施的資訊的小工具。您只能檢視您有權訪問的租戶的資料。

在**偵測和回應**頁籤中，下列群組的小工具可用：

- **事件**
- **活動清單**
- **上下文表**
- **警示**
- **資產**
- **事件**
- **常規程式**
- **事件來源**
- **使用者**

管理和防護小工具

設定儀表板的**管理和防護**頁籤時，您可以新增小工具、隱藏小工具、更改小工具的大小或外觀、移動小工具以及更改其設定。

一些部件具有帶連結的文字資訊。您可以透過點選連結檢視詳細資訊。

儀表板的**管理和防護**頁籤上提供以下小工具群組和小工具：

- **防護狀態**

此組包括以下小工具：

- **軟體弱點歷程記錄**
- **弱點裝置的數量**
- **按照弱點嚴重等級的裝置分發**
- **所選裝置的狀態**
- **防護狀態**

- **佈署**
  此組包括**新裝置**小工具。

- **更新**
  此群組包括以下小工具：
  - **有關Windows Update更新的統計資訊**
  - **病毒資料庫分發**
  - **活動警示**
  - **基於更新類別的更新安裝結果統計資訊**
  - **基於更新類別的更新安裝狀態統計資訊**
  - **更新安裝狀態統計資訊**

- **威脅統計資料**
  此群組包括以下小工具：
  - **指定的應用程式元件偵測到威脅，按解毒結果分發**
  - **被應用程式元件偵測到威脅**
  - **禁止的應用程式**
  - **網路攻擊的類型**
  - **偵測到病毒類型和解毒結果**
  - **隔離歷史**
  - **偵測到疑似被感染物件的記錄**
  - **網路攻擊歷史**
  - **依應用程式類型排序的威脅活動記錄**
  - **威脅活動**
  - **10個被感染最嚴重的裝置的使用者：**

- **被感染最嚴重的裝置**
- **最經常被感染的虛擬管理伺服器**
- **最常見的威脅**
- **感染最頻繁的 Windows 網域**
- **最常感染的群組**
- **警示**

- **其他**
  此群組包括以下小工具：
  - **產品授權金鑰使用**
  - **所選嚴重等級的通知**
  - **資料庫中 10 個最經常發生的事件**
  - **所選管理伺服器工作的目前狀態**
  - **工作歷史**

新增小部件到儀表板

要新增工具到儀表板：

1. 在主功能表中，轉至 **監控 → 控制板**。
2. 點擊**新增或還原小部件**按鈕。
3. 在可用工具清單，選取您要新增到儀表板的工具。
   工具按類別分組。要檢視包含在類別中的工具清單，點擊類別名稱旁邊的臂章圖示（ > ）。
4. 點擊**新增**。

所選的工具被新增到儀表板結尾。

您現在可以編輯所新增工具的展示和參數。

從儀表板隱藏小部件

要從儀表板隱藏工具：

1. 在主功能表中，轉至 **監控 → 控制板**。
2. 點擊您要隱藏的工具旁邊的設定圖示（ ⚙ ）。

3. 選擇**隱藏小部件**。

4. 在開啟的**警告**視窗中，點擊**確定**。

所選工具被隱藏。稍後，您可以再次新增該工具到儀表板。

移動儀表板上的小部件

要移動工具到儀表板：

1. 在主功能表中，轉至 **監控 → 控制板**。

2. 點擊您要移動的工具旁邊的設定圖示（⚙）。

3. 選擇**移動**。

4. 點擊您要移動工具的地方。您僅可以選取其他工具。

所選工具的地方被清掃。

變更部件尺寸或樣子

對於顯示圖表的工具，您可以變更其展示–線條圖或線形圖。對於一些工具，您可以變更其大小：最小、中度或最大。

要變更工具展示：

1. 在主功能表中，轉至 **監控 → 控制板**。

2. 點擊您要編輯的工具旁邊的設定圖示（⚙）。

3. 執行以下操作之一：

   - 若要顯示小工具作為條狀圖，請選取 **圖表類型：長條**。
   - 若要顯示小工具作為直線圖，請選取 **圖表類型：線形**。
   - 若要變更由小工具佔據的區域，請選取其中一個值：
     - **最小**
     - **最小（僅長條）**
     - **中度（餅圖）**
     - **中度（長條圖）**
     - **最大**

所選工具的展示被變更。

變更部件設定

要變更工具設定：

1. 在主功能表中，轉至 **監控 → 控制板**。
2. 點擊您要編輯的工具旁邊的設定圖示（⚙）。
3. 選擇**顯示設定**。
4. 在開啟的工具設定視窗，變更所需的工具設定。
5. 按一下**儲存**以儲存變更。

   所選工具的設定被變更。

設定集合取決於特定工具。以下是一些通用設定：

- **小部件範圍**（小工具顯示資訊的物件集）—例如，管理群組或裝置分類。
- **選取工作**可設定小工具要顯示其資訊的工作。
- **時間間隔**（小工具中顯示資訊的時間間隔）—介於兩個指定日期；從指定日期至當前日期；或從當前日期扣除目前日期的指定天數。
- **如果指定了以下設定，則設定為「緊急」**和**如果指定了以下設定則設定為「警告」**規則控制狀態圖表上的色彩指派方式。

更改小工具設定後，您可以手動重新整理小工具上的資料。

要重新整理小工具上的資料：

1. 在主功能表中，轉至 **監控 → 控制板**。
2. 點擊您要移動的工具旁邊的設定圖示（⚙）。
3. 選擇**重新整理**。

   小工具上的資料已重新整理。

偵測和回應小工具

在**偵測和回應**頁籤上，您可以新增、設定和刪除小工具。

偵測與回應頁籤中使用的一系列小工具稱為*佈局*。所有小部件都必須放置在佈局中。Kaspersky Next XDR Expert 可讓您建立、編輯和刪除佈局。此外，還提供預設的佈局。您可以根據需要在預設的佈局中編輯小工具設定。預設情況下，在**檢測和響應**頁籤上選擇警示概覽**佈局**。

小工具僅為在小工具或佈局設定中選定的租用戶顯示在小工具或佈局設定中選擇的週期的資料。

透過點擊有關事件、警示、事故或活動清單的小部件名稱的連結，您可以轉到Kaspersky Next XDR Expert介面的相應部分。請注意，某些小部件沒有此選項。

儀表板的**偵測和回應**頁籤上提供以下小工具群組和小工具：

- **事件**。用於基於事件建立分析的小工具。
- **活動清單**。用於基於關聯器活動清單建立分析的小工具。
- 警示。與警示相關的分析群組。包括有關Kaspersky Next XDR Expert提供的警示和事件的資訊。
  此群組包括以下小部件：
  - **活動警示**。尚未關閉的警示數。
  - **依租用戶分類的活動警示**。每個租用戶未關閉的警示數。
  - **依租用戶分類的警示**。每個租用戶所有狀態的警示數。
  - **未指派的警示**。沒有受讓人的警示數。
  - **依狀態分類的警示**。狀態為*新建*、*已開啟*、*已指派*或*已升級*的警示數。依狀態分組。
  - **最新警示**。包含佈局中所選租用戶的最近10個未關閉警示訊息的表格。
  - **警示分佈**。為小工具設定的期間內所建立的警示數。
  - **依使用者分類的警示**。狀態為*已指派*的警示數。依帳戶名稱分組。
  - **依群組分類的警示**。指派給每個群組以及群組內分析師的警示數。指派給分析師的警示在其所屬的每個群組中都會被計入。
  - **依嚴重程度分類的警示**。依嚴重程度分組的未關閉警示數。
  - **依規則分組的警示**。按關聯規則分組的未關閉警示數。
  - **依期間分組的警示狀態**。所選期間依狀態分組的警示數量。
  - **依技術分組的警示**。產生警示的防護技術名稱。
  - **依雜湊值分組的警示**。按掃描物件雜湊值分組的警示數量。支援的雜湊值類型：MD5和SHA-256。
  - **依偵測來源分組的警示**。依偵測來源分組的警示數量。
  - **依檔案名稱分組的警示**。依掃描檔案名稱分組的警示數量。
- **資產**。來自已處理事件的資產相關分析群組。此群組包括以下小工具：
  - **警示中受影響的裝置**包含資產和相關租用戶名稱以及與這些資產關聯的未關閉警示數的表格。從小工具移動到具有資產清單的部分不可用。
  - **受影響的資產類別**。連結到未關閉警示的資產類別。
  - **資產數量**。新增到Kaspersky Next XDR Expert的資產數。

- **事件中依租用戶分類的資產**。與未關閉事件關聯的資產數。依租用戶分組。
- **警示中依租用戶分類的資產**。與未關閉警示關聯的資產數，按租用戶分組。

- 事件。與事件相關的分析群組。
  此組包括以下小工具：
  - **活動事件**。尚未關閉的事件數。
  - **未指派的事件**。狀態為*已開啟*的事件數。
  - **事件分佈**。為小工具設定的期間內建立的事件數。
  - **依狀態分類的事件**。依狀態分組的事件數。
  - **依類型分類的事件**依類型分組處於任何狀態的事件數。
  - **依租用戶分類的活動事件**。可供使用者帳戶使用的依租用戶分組的未關閉事件數。
  - **所有事件**。所有狀態的事件數。
  - **依租用戶分類的所有事件**。依租用戶分組的所有狀態的事件數。
  - **事件中受影響的資產類別**。與未關閉事件關聯的資產類別。
  - **最新事件**。包含佈局中選定租用戶的最近10個未關閉事件資訊的表格。
  - **依使用者分類的事件**。狀態為*已指派*的事件數。依使用者帳戶名稱分組。
  - **依群組分類的事件**。指派給每個群組以及群組內分析師的事件數。指派給分析師的事件在其所屬的每個群組中都會被計入。
  - **依嚴重程度分類的事件**依嚴重程度分組的未關閉事件數。
  - **事件中受影響的資產**與未關閉事件關聯的資產數。從小工具移動到具有資產清單的部分不可用。
  - **事件中受影響的使用者**。與事件關聯的使用者。從小工具移動到具有使用者清單的部分不可用。
- **事件來源**。與事件來源相關的分析群組。此組包括以下小工具：
  - **依警示數分類的熱門事件來源**。依事件來源分組的未關閉警示數。
  - **依轉換率分類的熱門事件來源**。與未關閉警示關聯的事件數量。依事件來源分組。

    在某些情況下，來源產生的警示數量可能不準確。為了獲得準確的統計資料，建議在關聯規則中將裝置產品事件欄位指定為唯一，並允許在關聯事件中儲存所有基礎事件。但是，具有這些設定的關聯規則會消耗更多資源。

- **使用者**。用於分析已處理事件中與使用者相關的群組。此組包括以下小工具：
  - **警示中受影響的使用者**。與未關閉警示相關的帳戶數。從小工具移動到具有使用者清單的部分不可用。
  - **AD使用者數量**。為小工具設定的期間內透過LDAP接收的Active Directory帳戶數量。

    在事件表、事件詳情區域、警示視窗和小工具中，資產、帳戶和服務的名稱將取代ID顯示為SourceAssetID、DestinationAssetID、DeviceAssetID、SourceAccountID、DestinationAccountID和ServiceID欄位的值。將事件匯出到檔案時，ID會被儲存，但包含名稱的列會新增到檔案中。當您將滑鼠游標停留在資產、使用者帳戶或服務的名稱上時，也會顯示 ID。
    您只能使用 ID 搜尋含有 ID 的欄位。

- **常規程式**。與常規程式相關的分析群組。

  要查看此群組中的小工具，您必須擁有以下XDR角色之一：主管理員、租用戶管理員、 SOC管理員、SOC經理、一級分析師、二級分析師、核准人、稽核員。

  此組包括以下小工具：

  - **統計MTTR** 。變更在指定時間段內（預設為30天）對警示和事件的首次回應時間。此小工具顯示柱狀圖。
    統計MTTR小工具的以下組態參數可用：
    - **MTTR類型**：
      - **平均時間**。變更對警示和事件首次回應的平均時間。
      - **最短時間**。變更對警示和事件首次回應的最短時間。
      - **最長時間**。變更對警示和事件首次回應的最長時間。
    - **回應模式**：
      - **手動**。僅手動變更首次回應的時間。
      - **自動**。僅自動變更首次回應的時間。
      - **所有**。變更所有首次回應的時間。
    - **範圍**：
      - **警示**。僅變更對警示首次回應的時間
      - **事件**。僅變更對事件首次回應的時間
      - **所有**。變更對警示和事件的首次回應時間
  - **自動和手動啟動常規程式**。在一定時間段內自動和手動啟動常規程式的總次數。此小工具顯示柱狀圖。
    小工具的**啟動類型**參數指定是否僅顯示自動啟動次數、僅顯示手動啟動次數，或是顯示某一時間段內常規程式啟動的總次數。
    對於**統計MTTR**和**常規程式的自動和手動啟動**小工具，您也可以設定**時間分段長度**參數。此參數指定資料分組的時間間隔。您可以依每小時、每4小時或每24小時對資料進行分組。在直條圖上，**時間分段長度**參數指定列寬。

- **常規程式的警示和事件覆蓋範圍**。活動警示和事件的數量。您可以選擇要顯示的元件：事件、警示或全部。

  圓環圖顯示以下部分的警示/事件：

  - 啟動了**自動**運作模式的常規程式的警示/事件。
  - 啟動了**訓練**運作模式的常規程式的警示/事件。
  - 所有其他警示/事件。

- **使用常規程式節省的時間**。啟動所有具有*成功*或*警告*操作狀態的常規程式節省的時間。

  預設情況下不顯示該小工具。

  您可以透過按一下任何常規程式小工具的名稱來查看完整的常規程式清單。

- **觸發沙盒掃描的IOA規則**。導致Kaspersky Anti Targeted Attack Platform提交檔案供沙盒組件掃描的最常觸發的前10個IOA規則。
- **最常觸發的IOA規則**。在目標攻擊分析器（TAA）偵測到的事件中最常觸發的十大IOA規則。
- **觸發IOA規則的裝置**。IOA規則觸發頻率最高的10台裝置。

管理小工具的基礎知識

小工具中資料顯示的原則取決於圖表的類型。KUMA提供以下圖表類型：

- 圓餅圖（ ）。
- 計數器（ ）。
- 表格（ ）。
- 長條圖（ ）。
- 日期直方圖（ ）。
- 折線圖

一般小工具管理的基礎知識

小工具的名稱顯示在小工具的左上角。透過點擊帶有事件、警示或活動清單的小工具名稱的連結，您可以轉到KUMA主控台的相應部分。

小工具名稱下方是顯示資料的租用戶清單。

小工具右上角會顯示小工具上資料的顯示期間（例如 30 天 30d ）。請注意，由於快取，儀表板中顯示的資料可能存在延遲。您可以透過將滑鼠懸停在期間圖示上來檢視上次更新的日期和時間。

如果在小工具屬性中啟用**顯示上一期間的資料**選項，且小工具顯示的是相對期間的資料，則工具提示也會顯示上一期間。上一期間是相對於目前期間計算，方法是從目前期間的開始時間和結束時間減去目前期間的持續時間。例如，如果資料每日更新並顯示一個月，但該月只過去了前10天，則上一期間為上個月的最後10天。

您可以透過點擊期間圖示並在顯示的視窗中選擇確切日期或相對期間來變更小工具的資料顯示期間。若要在小工具顯示佈局中選定期間的資料，請按一下**重設**按鈕。更改佈局中顯示的期間也會更改小工具中顯示的期間。

小工具中的時間以瀏覽器中設定的本機時區顯示。

CSV按鈕位於期間圖示的左側。您可以以CSV格式（UTF-8編碼）下載小工具上顯示的資料。下載的檔案名稱格式為 <小工具名車>_<下載日期(YYYYMMDD)>_<下載日期(HHMMSS)>.CSV。

小工具僅為在小工具或佈局設定中選定的租用戶顯示在小工具或佈局設定中選擇的週期的資料。

如果您在小工具設定中啟用了**顯示總計**切換開關，則小工具會顯示**總計**值，但當您以CSV格式下載小工具時，不會顯示**總計**值。若要在報告中顯示**總計**值，您可以使用Excel公式或手動從小工具複製總計值。

管理圓餅圖的基礎知識

租用戶清單下方顯示了一個帶有圖例的圓餅圖。圖例列出了與圖表中各個扇形對應的類別名稱。您可以左鍵點選圖例中的類別，跳到OSMP主控台中包含相關資料的部分。該部分中的資料依據小工具中指定的篩選器和/或搜尋查詢進行排序。

從小工具圖例跳轉到活動詳情部分時，請注意點擊圖例項目進入事件部分的文字。文字中使用的任何「\」或「'」字元都會在SQL查詢的文字中轉義。但是，「/」字元不會被轉義。

在期間圖示下，將顯示按資料顯示期間的選定標準分組的事件、活動清單、資產、警示或事件的數量。

範例：

- 在**依狀態分組的警示**小工具中，在期間圖示下方，顯示按**新建** 、 **開啟** 、 **已指派**或**已升級**狀態分組的警示數量。
  如果您只想查看**已開啟**和**已指派**狀態的警示的圖例，可以清除**新建**和**已升級**狀態左側的核取方塊。
- 在指定 SQL 查詢 `SELECT count(ID) AS `metric`, Name AS `value` FROM `events` GROUP BY Name ORDER BY `metric` DESC LIMIT 10` 的 **事件** 小工具中，期間圖示下方會顯示 10 個事件，這些事件依名稱分組並按降冪排序。
  如果要在圖例中檢視具有特定名稱的事件，可以清除不想在圖例中看到的事件名稱左側的核取方塊。

管理計數器圖表的基礎知識

此類圖表顯示所選資料的總和。

例子 1
資產數量小工具顯示新增到KUMA的資產總數。
例子 2
如果您想檢視趨勢以將當前資料與過去某個期間的資料進行比較，您可以建立一個顯示向上或向下趨勢的小工具。趨勢可以在以下小工具中進行設定：

- **資產 → 資產數量**。
- **資產 → 自訂小工具**。
- **警報 → 作用中警報**。
- **警報 → 未指派的警報**。
- **事件 → 作用中事件**。
- **事件 → 未指派的事件**。
- **事件 → 所有事件**。
- **使用者 -> AD 使用者數量**。
  若要設定趨勢的顯示，您需要啟用**顯示上一期間的資料**切換開關，然後在「外觀」頁籤上選擇一個趨勢。如果無法計算百分比值，或者如果這些值相等，則會顯示（ — ）圖示。如果選擇**向上更好**，則圖表上以綠色箭頭表示上升趨勢，以紅色箭頭表示下降趨勢。如果選擇**向下更好**，則圖表上以紅色箭頭表示上升趨勢，以綠色箭頭表示下降趨勢。
  您可以點擊該值來變更小工具中資料的顯示方式（例如，顯示絕對值而不是百分比）。當小工具顯示於儀表板且開啟電視模式時，即可使用此功能。

管理表格圖表的基礎知識

此類圖表以表格格式顯示資料。

範例：
在指定 SQL 查詢 `SELECT TenantID , Timestamp , Name , DeviceProduct , DeviceVendor FROM `events` LIMIT 10` 的 **事件** 小工具中，會顯示包含 **TenantID**、**Timestamp**、**Name**、**DeviceProduct** 和 **DeviceVendor** 欄的事件表格。該資料表包含 10 行。

您可以使用雙色（紅色和綠色）或三色（紅色、黃色和綠色）漸層來填滿來自訂表格中資料的顯示。選擇漸層類型後，您可以透過點擊切換方向圖示（⇆）來調整填滿方向並設定閾值。雙色漸層需要指定兩個值，三色漸層需要指定三個值。這些值顯示在圖例中，並決定新增至所選列儲存格中的標記的顏色。**漸變指示器欄位**下拉清單中指定。

管理長條圖的基礎知識

包含圖例的長條圖顯示在租用戶清單下方。圖例列出了與圖表中各長條對應的類別名稱。透過左鍵點選圖例中的類別，您可以轉至OSMP主控台中包含對應資料的部分。該部分中的資料依據小工具中指定的篩選器和/或搜尋查詢進行排序。

從小工具圖例跳轉到活動詳情部分時，請注意點擊圖例項目進入事件部分的文字。文字中使用的任何「\」或「'」字元都會在SQL查詢的文字中轉義。但是，「/」字元不會被轉義。

範例：
在已指定 SQL 查詢 `SELECT sum(BytesIn) AS metric, DestinationAddress AS value FROM `events` WHERE (DeviceProduct = 'netflow' OR DeviceProduct = 'sflow') AND (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16')) GROUP BY DestinationAddress ORDER BY metric DESC LIMIT 10` 的 **Netflow 主要內部 IP** 小工具中，圖表的 x 軸對應於總流量（以位元組為單位），y 軸對應於目標連接埠位址。資料按目標位址分組，並依總流量降序排列。

您也可以使用雙色（紅色和綠色）或三色（紅色、黃色和綠色）漸層來填滿來自訂長條圖的顯示。選擇漸層類型後，您可以透過點擊切換方向圖示（⇆）來調整填滿方向並設定閾值。雙色漸層需要指定兩個值，三色漸層需要指定三個值。這些數值顯示在圖例中，並決定長條圖的顏色。

管理日期直方圖的基礎知識

包含圖例的日期直方圖顯示在租用戶清單下方。圖例列出了與圖表中各長條對應的類別名稱。透過左鍵點選圖例中的類別，您可以轉至OSMP主控台中包含對應資料的部分。該部分中的資料依據小工具中指定的篩選器和/或搜尋查詢進行排序。

從小工具圖例跳轉到活動詳情部分時，請注意點擊圖例項目進入事件部分的文字。文字中使用的任何「\」或「'」字元都會在SQL查詢的文字中轉義。但是，「/」字元不會被轉義。

如果在建立**日期直方圖**類型的小工具時選擇了**長條圖**視圖，則可以使用雙色（紅色和綠色）或三色（紅色、黃色和綠色）漸層來填滿來自訂條形的顯示。選擇漸層類型後，您可以透過點擊切換方向圖示（⇆）來調整填滿方向並設定閾值。雙色漸層需要指定兩個值，三色漸層需要指定三個值。這些數值顯示在圖例中，並決定長條圖的顏色。

範例：

```
SELECT count(ID) AS `metric`, Timestamp AS `value`
FROM `events`
GROUP BY Timestamp
ORDER BY `metric` DESC
LIMIT 250
```

圖表的X軸表示事件建立日期，Y軸表示事件數量。圖表中的長條圖從左到右依事件數量降序排列。

如果在SQL查詢中使用了帶有`category`別名的附加欄位，則長條圖將顯示為堆疊長條圖。在這種情況下，不套用漸層填充。

範例：

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, Type AS `value`
FROM `events`
GROUP BY Timestamp, Type
ORDER BY metric DESC
LIMIT 250
```

X軸表示時間間隔，Y軸表示事件數。長條的每個分段對應於標記為**類型**欄位的值。

如果在建立具有**日期直方圖**類型的小工具時，選擇了**折線圖**視圖，則圖表有兩種顯示選項：單線（如果查詢中僅指定了`metric`和`value`欄位）和多線（如果使用帶有`category`別名的附加欄位）。這允許您比較不同群組的值，具體取決於查詢中用於分組的欄位。例如，可以使用關聯規則、使用者或主機。此類圖表不套用漸層填充。

範例：

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, CorrelationRuleName AS `value`
FROM `events`
WHERE Type = 3
GROUP BY Timestamp, CorrelationRuleName
ORDER BY metric DESC
LIMIT 250
```

圖表會在 X 軸上顯示間隔（指定為 `category` 的欄位）。Y 軸會顯示關聯規則被觸發的次數（標記為 `metric` 的欄位）。圖表上的每條線都對應於 `value` 欄位中的唯一值（在此案例中為關聯規則的名稱）。

您可以使用以下時間欄位在日期直方圖中進行分組：

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> 為方便起見，我們建議使用ClickHouse支援的函式將時間欄位（**時間戳記**）中的值四捨五入，例如四捨五入到1小時或1天。

對於具有**折線圖**視圖的**日期直方圖**小工具，您也可以設定平均值的顯示。為此，請在**外觀**頁籤上的**回歸**設定中選擇**LOESS**。

管理折線圖的基礎知識

包含圖例的折線圖顯示在租用戶清單下方。圖例顯示與圖表上的線條對應的類別名稱。透過左鍵點選圖例中的類別，您可以轉至OSMP主控台中包含對應資料的部分。該部分中的資料依據小工具中指定的篩選器和/或搜尋查詢進行排序。

從小工具圖例跳轉到活動詳情部分時，請注意點擊圖例項目進入事件部分的文字。文字中使用的任何「\」或「'」字元都會在SQL查詢的文字中轉義。但是，「/」字元不會被轉義。

範例：
在指定了 SQL 查詢 `SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY `value` ASC LIMIT 250` 的 **事件** 小工具中，x 軸對應於近似連接埠號碼，y 軸對應於事件數量。資料按連接埠號碼分組，並以升序排列。

對於**折線圖**小工具，您還可以設定平均值的顯示。為此，請在**外觀**頁籤的**回歸**設定中選擇**線性**。如果圖表顯示多個類別，則會顯示每個類別的平均值。

堆疊長條圖類型圖表管理的基礎知識

包含圖例的長條圖顯示在租用戶清單下方。圖例顯示構成每個長條部分的各個類別名稱。每個類別左側都有一個核取方塊，可用於隱藏或顯示該類別。圖表中的長條數量與所選分組中的數值數量相對應。長條帶有標題。長條中對應類別的顏色會自動指派。將滑鼠懸停在長條區域上時，會顯示一個工具提示，其中包含值及其描述。您可以左鍵點選圖例中的類別，跳到OSMP主控台中包含相關資料的部分。

從小工具圖例跳轉到活動詳情部分時，請注意點擊圖例項目進入事件部分的文字。文字中使用的任何「\」或「'」字元都會在SQL查詢的文字中轉義。但是，「/」字元不會被轉義。

長條高度的含義取決於**格式**設定：

- 如果設定了**絕對值**格式，則長條的高度對應於測量值的總和。
- 如果設定了**相對值（%）**格式，則所有長條的高度均為100%，柱狀圖上彩色區域的相對高度與值的比率相對應。

如果在基於堆疊長條圖建立自訂小工具時，您選擇了**顯示上一期間的資料**選項，並且在查詢中使用了標準`value`、`category`、`metric`別名，則圖表會將上一期間的資料顯示為個別長條。但是，如果查詢使用具有非標準別名的自訂指標計算，而不是標準`metric`，則顯示圖表時不會考慮**顯示上一期間的資料**（請參閱以下範例查詢）。

範例：
當根據**事件**小工具的SQL查詢建立**堆疊長條圖**類型的自訂小工具時，適用以下規則：

- 查詢中標記為`value`別名（必填欄位）的欄位在圖表中用作建立圖例並將長條劃分為類別的欄位。
- 查詢中標記為`category`別名（必填欄位）的欄位在圖表中用作定義沿 X 軸排列長條的欄位。
- 查詢中標記為`metric`別名的欄位在圖表中用作定義長條區域計數方式的欄位。在這種情況下，分佈是自動執行的。

但是，您可以使用標準彙總函式（`sum`、`avg`、`min`、`max`、`count`）和您自己的任意命名別名作為指標，而不是標準`metric`別名來管理計數（在這種情況下，不支援顯示上一期間的資料）。

例子 1：
對於**事件**小工具，使用標準別名指定以下SQL查詢，並在建立小工具時選擇**顯示上一期間的資料**選項：

```
SELECT count(ID) AS `metric`,

Type AS `value`,

TenantID AS `category`

FROM `events`

GROUP BY value, category

ORDER BY metric DESC
```

X 軸代表租用戶（標記為`category`的欄位），Y 軸代表特定類型的事件數量（標記為值的欄位）。在每個長條中，特定類型對應的數量以特定顏色表示。圖例中，長條的劃分依據是事件類型名稱，並以類別形式顯示。每個類別在長條上都有自動指派的對應顏色。如果您只想在圖表中查看某些事件類型，可以取消選取或選取圖例中對應事件類型左側的核取方塊。

如果查詢回應中收到了歷史資料，則每個長條旁邊也會顯示一個包含歷史資料的附加長條。

例子 2：
對於**事件**小工具，以下 SQL 查詢標有自訂指標，這些自訂指標標記為 `Base` 和 `Audit` 別名，而不是標準 `metric` 別名：

```
SELECT SUM(IF (Type = 1,1,0)) AS `Base`,

SUM(IF (Type = 4,1,0)) AS `Audit`,

TenantID as `category`

FROM `events`

GROUP BY category
```

X 軸代表租用戶（標記為`category`的欄位），Y 軸代表每種類型的事件數量（標記為 Base 和 Audit 別名的自訂指標）。在每個長條中，特定指標對應的數量以特定顏色表示。圖例中，用於將長條劃分為類別的 `Base` 和 `Audit` 指標，會以類別名稱的形式顯示。每個類別在長條上都有自動指派的對應顏色。如果您只想在圖表中查看與特定指標對應的事件，可以取消選取或取消選取圖例中相關指標左側的核取方塊。

對於包含自訂指標的查詢，即使在建立小工具時選擇了「顯示上一期間資料」選項，也不會顯示包含歷史資料的附加長條。

例子 3：
對於**事件**小工具，使用標準別名指定以下SQL查詢：

```
SELECT count(ID) AS `metric`,

TenantID as `value`,

Type as `category`

FROM events

GROUP BY value, category

ORDER BY metric DESC
```

與例子 1 中的類似查詢相比，在此情況下，X 軸代表事件類型（標記為 `category` 的欄位），而租用戶（標記為 `value` 的欄位）則由長條中（沿 X 軸）的值範圍以及圖例中對應的標題表示。

例子 4：
對於**事件**小工具，使用標準別名指定以下SQL查詢：

```
SELECT count(ID) AS `metric`,

CAST(fromUnixTimestamp64Milli(Timestamp) AS DATE) AS `category`,

Type as `value`

FROM `events`

GROUP BY category, value

ORDER BY category DESC
```

圖表會在 X 軸上顯示月份中的日期（標記為 **category** 的欄位）。Y 軸會顯示特定類型的事件數量（標記為 **value** 的欄位）。

若要建立長條按日期和/或時間排列的類似圖表，請使用依下列 **timestamp** 類型欄位進行分組和排序的查詢：

- Timestamp
- DeviceCustomDate1
- DeviceCustomDate2
- EndTime
- FileCreateTime
- FileModificationTime
- FlexDate1
- OldFileCreateTime
- OldFileModificationTime
- DeviceReceiptTime
- StartTime

> 我們建議使用**日期直方圖**來處理按日期和/或時間排列的資料。

速度計圖表管理的基礎知識

這種類型的圖表顯示所選類型的物件數量與特定期間內物件總數的百分比。**速度計圖**可用於以下物件：

- 滿足特定條件的類別資產與同一類別或未分類資產的資產總數
- 滿足特定條件的警示與特定期間內的警示總數
- 滿足特定條件的事件與事件總數
- 滿足特定條件的事件與特定期間內的事件總數

圖表上的值以百分比形式顯示，顏色與設定的值範圍相符。預設情況下，指定以下範圍：0–30、30–70、70–100。

例子 1：
在**資產**自訂小工具中，使用者選擇一個資產類別，以比較該類別中的資產數量與資產總數。使用者可以為圖表的刻度指定閾值。然後，根據Y軸的一個或多個條件，使用現有的資產資料庫進行計算。

例子 2：
在**警示**小工具中，您可以為**活動**警示和速度計圖類別選擇**速度計圖表**類型。對於警示，需要選擇租用戶和分析期間。預設情況下，這些值與相關儀表板中指定的值一致。在警示總數中，您也可以顯示上一個期間的資料。

活動事件和**未分配事件**類別的百分比值在**事件**小工具中以相同方式計算。

例子 3：
在**事件**小工具中，對於**速度計圖**類型，使用者需要指定租用戶、分析期間和事件資料儲存體。SQL查詢如下所示：

```
SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

在小工具中顯示資料的特殊注意事項

顯示資料的限制

為了提高可讀性，KUMA依據視窗小工具的類型對顯示的資料進行了限制：

- 圓餅圖最多顯示20個扇形區域。
- 長條圖最多顯示40個長條。
- 表格最多顯示500個條目。
- 日期直方圖最多顯示365天。

超過指定限制的資料將顯示在視窗小工具的**其他**類別中。

您可以以CSV格式下載用於在視窗小工具中建立分析的完整資料。

加總資料

日期直方圖、長條圖和圓餅圖上顯示資料總和的格式取決於語言環境：

- 英語語言環境：十進位（每三位數字）以逗號分隔，小數部分以句點分隔。
- 俄語語言環境：十進制（每三位數字）用空格分隔，小數部分用逗號分隔。

建立小工具

您可以在建立或編輯佈局設定時在儀表板佈局中建立小工具。

若要建立小工具：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 建立佈局或切換到所選佈局的編輯模式。
3. 按一下**新增小工具**。

4. 從下拉清單中選擇視窗小工具類型。
   將會開啟包含小工具參數的視窗。
5. 編輯小工具設定。
6. 如果要檢視資料在小工具中的顯示方式，請按一下**預覽**。
7. 按一下**新增**。

小工具將出現在儀表板佈局中。

新增小工具

若要編輯小部件：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 延伸視窗右上角的清單。
3. 將滑鼠遊標停留在相關佈局上。
4. 按一下編輯按鈕（ ）。
   自訂佈局視窗將開啟。
5. 在要編輯的小工具中，按一下設定圖示（ ）。
6. 選擇**編輯**。
   將會開啟包含小工具參數的視窗。
7. 編輯小工具設定。
8. 在小工具設定視窗中，按一下**儲存**。
9. 在**自訂佈局**視窗中，按一下**儲存**。

小工具隨即編輯。

刪除小工具

若要刪除小工具：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 延伸視窗右上角的清單。
3. 將滑鼠遊標停留在相關佈局上。
4. 按一下編輯按鈕（ ）。
   自訂佈局視窗將開啟。
5. 在要刪除的小工具中，按一下設定圖示（ ）。

6. 選擇**刪除**。

7. 在開啟的確認視窗中，按一下**確定**。

8. 按一下**儲存**按鈕。

小工具隨即刪除。

小工具設定

本章節介紹KUMA中所有可用視窗小工具的設定。

事件小工具

您可以使用**事件**小工具來取得基於SQL查詢的分析資料。

在建立此小工具時，您必須指定下表中所述的設定。

一般頁籤

下表描述了**一般**頁籤上的設定。

描述

設定	描述
名稱	小工具的名稱。 以Excel格式儲存報告時，工作表標題中顯示的小工具名稱長度限制為31個字元。我們建議您在命名小工具時注意此限制。
圖表	圖表類型。有下列應用程式類型可用： • **圓餅圖**。 • **長條圖**。 • **計數器**。 • **折線圖**。 • **表格**。 • **日期直方圖**。 • **堆疊長條圖** • **速度計圖**
格式	資料顯示格式：**絕對值**或**相對值（%）**。此設定適用於**堆疊長條圖**。 如果選擇**絕對值**格式，則長條的高度對應於所測量指標值的總和。如果選擇**相對值（%）**格式，所有長條的高度均為100%，長條上彩色區域的相對高度對應於指標值的比率。 預設情況下，選擇**絕對值**。
時間軸檢視畫面	時間資料顯示格式：**長條圖**或**折線圖**。此設定適用於**日期直方圖**類型的圖表。 選擇**長條圖**格式時，資料預設以垂直長條的形式顯示。如果SQL查詢包含一個帶有類別別名的附加欄位，則圖表將成為堆疊長條圖，即每個長條圖根據該欄位的值劃分為條紋。 選擇**折線圖**格式時，資料將顯示為一條或多條（取決於查詢）穿過時間軸上的點的折線。 預設選擇長條圖格式。
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
期間	小工具中顯示資料的期間。預設為**依佈局**，意味著為佈局選定的期間顯示資料。 您也可以透過以下方式之一為小工具指定期間： • 在日曆中選擇期間的確切開始和結束日期和時間，然後按一下**套用**。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對期間，或兩者的組合。 詳情請參閱下面的*設定期間*子部分。
顯示上一期間的資料	啟用同時顯示兩個期間的資料：當前期間和上一個期間。 使用**堆疊長條圖**時，如果查詢包含標準別名：`value`、`category`、`metric`，則會納入考量**顯示上一期間的資料**設定。但是，如果查詢不是使用標準`metric`，而是使用具有非標準別名的自訂指標計算，則不會納入考量**顯示上一期間的資料**設定。

設定	描述
定義的變數	可用於篩選小工具資料的局部變數或全域變數。 按一下**新增**。如果要新增局部變數，請輸入變數的任意名稱，然後輸入變數的值。如果要新增全域變數，請在清單中選擇您在儀表板內容中指定的變數名稱。
儲存體	用於搜尋事件的儲存體。清單顯示了可用空間。您只能選擇一個儲存體，但可以選擇一個或多個空間。**儲存體**欄位中的值與**租用戶**欄位中所選的租用戶無關。此欄位會顯示儲存體和空間，如同**事件**區段中所示。當儲存體中建立新空間時，預設不會在小工具設定中選取此新空間。 您必須手動選取新空間。 如果使用者有權存取小工具中列出的所有空間，小工具便可顯示使用者權限中設定的空間集合內所指定租用戶的事件資訊。 如果使用者沒有對一個或多個儲存空間的存取權限，則小工具無法顯示資訊；使用者無法編輯小工具，但可以使用**複製**按鈕複製小工具。複製操作與空間存取權限無關。如果範本在指定了使用者無法存取的空間的小工具中重複出現，則**儲存體**欄位中的值將會重設。此類小工具會顯示錯誤：存取被拒絕（由於允許和選定的事件空間，操作沒有返回結果）。若要儲存範本，需要在小工具中指定空格。 在具有使用者可存取空間的小工具中，當範本被複製時，**儲存體**欄位的值不會被重設並儲存。 當使用者下載範本時，無法存取之檔案的資料會隱藏在下載的檔案中。 如果使用者的電子郵件地址包含在排程報告的收件者清單中，則無論哪些空間是否可存取，使用者都將取得報告的完整版本。

設定	描述

SQL查詢欄位	用於手動查詢篩選和搜尋事件。您可以透過點擊**使用 SQL 建置器**在建構器中建立查詢。
	您可以使用擴充事件架構欄位來建立**表格**類型的圖表。
	範例
	先決條件：
	事件來自FWSaaS系統。
	10.08.2023 12:12:12 src=10.10.10.10 ReqUrls=[https://google.com, https:/ya.ru]
	10.08.2023 12:12:23 src=10.10.10.20 ReqUrls=[https://google.com, https:/yndex.ru]
	10.08.2023 12:12:33 src=10.10.10.30 ReqUrls=[https://google.com, https:/ya.ru, https://mail.ru]
	KUMA 主管理員已在 KUMA 的**設定 → 其他 → 進階事件架構欄位**區段中新增擴充事件架構欄位。在KUMA規範化器中，為**ReqUrls**和**SA.urls**欄位設定了欄位對應。
	在KUMA中，規範化的事件如下所示：
	DeviceReceiptTime=10.08.2023 12:12:12 SourceAddress=10.10.10.10 SA.urls=[https://google.com, https:/ya.ru]
	DeviceReceiptTime=10.08.2023 12:12:23 SourceAddress=10.10.10.20 SA.urls=[https://google.com, https:/yandex.ru]
	DeviceReceiptTime=10.08.2023 12:12:30 SourceAddress=10.10.10.30 SA.urls=[https://google.com, https:/ya.ru, https://mail.ru]
	你想建立一個「30分鐘內訪問量最高的URL」儀表板。以下是**事件**部分和小工具中的請求範例：
	SELECT res.1 AS url, res.2 AS count FROM (SELECT arrayJoin(groupArray((url, count))) AS res FROM (SELECT url, count() AS count FROM (SELECT SA.urls AS urls FROM `events`) ARRAY JOIN urls AS url GROUP BY url) GROUP BY url)
	結果：
	URL計數
	google.com 3
	ya.ru 2
	mail.ru 1
	yandex.ru 1
	KUMA支援以下允許在查詢中使用陣列的函式：
	• `groupArray` 函式會將 x 引數的所有值打包到陣列中，並在分組資料時用於彙總函式。
	• `arrayJoin` 函式會將陣列展開成個別字串，做為查詢結果。
	您可以在 SQL 查詢中使用變數。只有在手動建立查詢時才能指定變數。SQL建構器中不能使用變數。
	包含變數的範例
	包含局部變數的 SQL 查詢範例
	`SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name) GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250`
	此查詢使用局部變數`$Name`。`Name`事件欄位的值會代入此變數。您可以點擊漏斗圖示（ ）將變數套用在小工具上。這將開啟一個視窗；在該視窗中，您可以為變數指定一個值。小工具會依據`Name`欄位的所選值篩選選取項目。
	請注意，如果在SQL查詢中為取數值的欄位指定變數，則必須將該值轉換為字串。您可以使用`toString`函式執行此操作。否則，SQL查詢將傳回錯誤。
	範例
	`SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250`
	在此查詢中，`SourcePort`事件欄位具有數值，因此會轉換為字串：`toString(SourcePort)`。
	有關在查詢建構函式中建立SQL查詢的詳盡資訊，請參見下文。
	將套用以下限制：
	• 除表格外，任何類型的事件分析小工具的SQL查詢中的`metric`和`value`別名均無法編輯。
	• 在**表格**類型的圖表小工具中的別名可以包含拉丁字母和西里爾字母，以及空格。使用空格或西里爾字母時，別名必須以引號括住：`"An alias with a space"`、`` `Another alias` ``。
	• 不支援`ARRAY JOIN` SQL查詢。
	• 顯示前一期間的資料時，依 `count(ID)` 參數排序可能無法正常運作。建議依`metric`參數排序。例如，`SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`。
	• 在**計數器**類型的圖表小工具中，必須為`SELECT`函式的值指定資料處理方法：`count`、`max`、`min`、`avg`、`sum`。

設定	描述
	• 在**表格**類型的圖表小工具中，漸層是根據SQL查詢中指定的數字或時間欄位（例如，`Timestamp`）的值繪製的。此欄位可從**漸變指示器欄位**下拉清單中選擇（如果查詢包含多個數字或時間欄位，則可以選擇其中任一個）。之後，所選直欄的儲存格將以漸層填滿標記突出顯示。如果查詢中不存在某個欄位，**外觀**頁籤將不會顯示**漸層**和**漸變指示器欄位**欄位。 • 在**堆疊長條圖**小工具中，使用標準查詢時，`Timestamp`值不會顯示在x軸上。如果要沿著x軸顯示時間，我們建議使用**折線圖**。如果需要使用**堆疊長條圖**，則必須將`Timestamp`值轉換為字串：`toString(Timestamp) AS `category``。

設定期間

若要設定資料顯示期間，請執行下列操作之一：

- 如有必要，請按以下方式之一變更**期間**設定中的日期和時間：

  - 若要指定**確切日期**，請在日曆中選取期間的開始日期和結束日期，然後按一下**套用**。

    您可以選擇包括目前日期在內的任意日期。日期和時間格式取決於瀏覽器的設定。如果**範圍始自**或**範圍終至**欄位已有值，且您未手動編輯時間值，則在日曆中選取日期時，**範圍始自**欄位會自動填入`00:00:00,000`，**結束日期**欄位則會填入`23:59:59,999`。如果您已手動刪除**範圍始自**或**範圍終至**欄位中的值，則在日曆中選取日期時，該欄位會自動填入目前時間。在其中一個欄位中選取值後，焦點會切換至另一個欄位。如果**範圍終至**早於**範圍始自**，系統會自動將較早的值填入**範圍始自**欄位。

  - 若要指定**相對期間**，請從**相對期間**清單中選取一個期間。

    期間是相對於當前時間計算的。

  - 若要指定**自訂期間**，請手動設定或編輯**範圍始自**和**範圍終至**欄位的值。

    您可以使用俄文語言版本的`DD.MM.YYYY HH:mm:ss.SSS`格式或英文語言版本的`YYYY-MM-DD HH:mm:ss.SSS`格式輸入確切的日期和時間，也可以使用公式輸入相對於目前時間的期間。您也可以結合使用這些方法。如果輸入確切日期時未指定毫秒，系統會自動代入`000`。如果您已編輯**範圍始自**或**範圍終至**欄位中的時間，在日曆中選取日期不會變更時間部分。

    在相對期間公式中，您可以使用代表目前日期和時間的參數`now`，以及間隔參數化語法：`+`（僅適用於**範圍終至**欄位）、`-`、`/`（四捨五入至最接近的值），還可以使用下列時間單位：`y`（年）、`M`（月）、`w`（週）、`d`（日）、`h`（小時）、`m`（分鐘）、`s`（秒）。例如，您可以指定期間`now-5d`，以取得過去五天的資料；或指定`now/w`，以取得從本週第一天開始時（00:00:00:000 UTC）到目前時間（`now`）的資料。

    > **範圍始自**欄位為必填，且其值不得晚於**範圍終至**欄位的值，也不得早於 1970-01-01（指定確切日期或相對期間時）。**範圍終至**不得早於**範圍始自**。如果您未在**範圍終至**欄位中指定值，系統會自動代入`now`。

Kaspersky SIEM 以 UTC 儲存時間值，但網頁介面會將時間轉換為瀏覽器的時區。這與相對時間段相關：**今天**、**昨天**、**本週**和**本月**。例如，如果瀏覽器中的時區是UTC+3，並且您選擇**今天**作為資料顯示期間，則將顯示從03:00:00.000到現在的資料，而不是從00:00:00.000到現在。

如果您希望在選取**今天**、**昨天**、**本週**或**本月**等相對資料顯示期間時考量您的時區，則需要在**範圍始自**和**範圍終至**（若指定的值不是`now`）中，透過加上或減去適當的小時數，手動加入時間偏移量。例如，如果瀏覽器的時區為 UTC+3，而您想顯示**昨天**的資料，則需要將**範圍始自**變更為`now-1d/d-3h`，並將**結束日期**變更為`now/d-3h`。如果您想顯示**今天**的資料，只需將**範圍始自**欄位的值變更為`now/d-3h`。

> 如果您需要截至昨天23:59:59:999 UTC的結果，可以使用帶有時間戳篩選器的SQL查詢，或指定確切的日期和時間。

期間的邊界包含所有時間：例如，對於**今天**時間範圍，事件顯示範圍從當天開始（00:00:00:00）到當前時間（**now**），包含當前時間；對於**昨天**期間，事件顯示範圍從前一天開始（00:00:00:00）到當天00:00:00:00。將滑鼠懸停在小工具中的期間圖示上，即可查看上次資料更新的日期和時間以及資料顯示的確切期間。

如果小工具啟用了**顯示上一期間資料**設定，且小工具顯示的是相對期間的資料，則工具提示也會顯示上一期間。上一期間是相對於當前期間計算的，計算方法為：當前期間的起始值和結束值減去當前期間的持續時間。例如，如果資料每日更新並顯示一個月，但該月只過去了前10天，則上一期間為上個月的最後10天。

- 若要在小工具顯示佈局中選定期間的資料，請按一下**重設**按鈕。更改佈局中顯示的期間也會更改小工具中顯示的期間。

如何在構建器中建立查詢

若要在構建器中建立查詢：

1. 指定以下參數的值：

   a. **SELECT** — 應傳回的事件欄位。可用欄位的數量取決於所選的圖表類型。

   - 在左側的下拉清單中，選擇要在小工具中顯示資料的事件欄位。
   - 中間欄位顯示所選欄位在小工具中的用途： **metric**或**value** 。

     如果您選擇了**表格**圖表類型，則在中間欄位中，必須使用ANSII-ASCII字元指定直欄名稱。

   - 在右側的下拉清單中，您可以選擇要對資料執行的操作：
     - **計數** —事件計數。此操作僅適用於**ID**事件欄位。預設用於折線圖、圓餅圖、長條圖和計數器。這是日期直方圖的唯一選項。
     - **max**是事件選擇中**事件**欄位的最大值。
     - **min**是事件選擇中**事件**欄位的最小值。
     - **avg**是事件選擇中**事件**欄位的平均值。
     - **sum**是事件選擇中事件欄位值的總和。

   b. **來源**是資料來源的型別。只有**事件**值可供選擇。

   c. **WHERE** —篩選事件的條件。

   - 在左側的下拉清單中，選擇要用於篩選的事件欄位。
   - 從中間的下拉清單中選擇必要的運算子。可用的運算子取決於所選事件欄位的值類型。
   - 在右側的下拉清單中，輸入條件的值。依據所選欄位的類型，您可能需要手動輸入值，從下拉清單中選擇值或在日曆上選擇值。

   您可以點選**新增條件**來新增搜尋條件，或點選✕來移除搜尋條件。

   您也可以透過點擊**新增群組**來新增條件群組。預設情況下，使用**AND**運算子新增條件群組，但您可以根據需要變更它。可用值： **AND**、**OR**、**NOT**。點選**刪除群組**按鈕，即可刪除條件群組。

   d. **GROUP BY** - 用於將傳回的資料分組的事件欄位或別名。此參數不適用於**計數器**圖表類型。

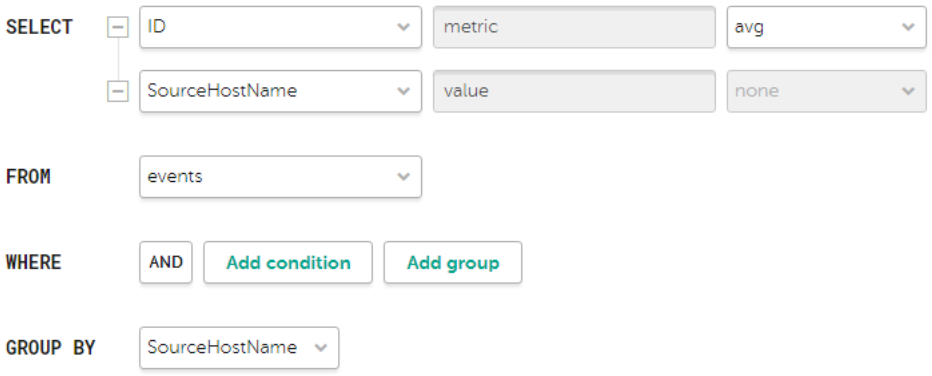
e. **ORDER BY** - 用作對傳回的資料進行排序的基礎的直欄。此參數不適用於**日期直方圖**和**計數器**圖表類型。

- 在左側的下拉清單中，選擇將用於排序的值。
- 從右側的下拉清單中選擇排序順序： **ASC**表示升序， **DESC**表示降序。
- 對於**表格**類型圖表，您可以透過點擊**新增直欄**來新增排序條件。

f. **LIMIT**是小工具的最大資料點數。此參數不適用於**日期直方圖**和**計數器**圖表類型。

2. 點選**套用**。

查詢構建器中的搜尋條件範例



在小工具中顯示每個主機平均位元組數的搜尋條件參數

座標軸頁籤

下表描述了**座標軸**頁籤上的設定。

> 如果您在**一般頁籤的圖表**欄位中選取以下其中一個值，便會顯示此頁籤：**長條圖**、**折線圖**、**日期直方圖**。

描述

設定	描述
點大小	圖表上的點大小。此欄位用於**折線圖**類型。
線寬	圖表上線條的寬度。此欄位用於**折線圖**類型。
Y軸的最小值和最大值	Y軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。
X軸的最小值和最大值	X軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。
小數	顯示數值必須四捨五入到的小數位數。

外觀頁籤

下表描述了**外觀**頁籤上的設定。

設定	描述
描述	小工具的描述。
顯示圖例	顯示用於分析的圖例。切換開關預設為開啟。
在圖例中顯示空值	在分析的圖例中顯示具有空值的參數。切換開關預設為開啟。 僅當啟用**顯示上一期間的資料**設定且目前期間沒有資料，但上一期間有資料時，才會顯示空值。
顏色	用於顯示資訊的顏色： • **預設**為瀏覽器的預設字體顏色 • **綠色** • **紅色** • **藍色** • **黃色** 此設定適用於**長條圖**、**計數器**、**折線圖**、**日期直方圖**等圖表。
漸層	圖表的漸層填充： • 兩種顏色（紅色和綠色） • 三種顏色（紅色、黃色和綠色） 此設定適用於**長條圖**、**日期直方圖**（類型為**長條圖**）、**表格**等圖表。 您可以透過點擊切換方向圖示（⇆）來調整填充方向；您還可以設定閾值。 如果未手動設定，漸層閾值將根據資料自動計算。如果在指定的閾值之間沒有資料，則不會套用漸層。而是使用兩種顏色：一種用於低於下限閾值的值，另一種用於高於上限閾值的值。
漸變指示器欄位	顯示漸層填充指標的直欄。 此設定適用於**表格**類型的圖表。
水平方向	以水平方向而不是垂直方向顯示直方圖。 啟用此選項後，當小工具顯示大量資料時，水平捲動不可用，所有可用資訊都適合小工具的固定大小。如果要顯示大量資料，建議增加小工具的大小。
顯示總和	顯示數值的總和。 數值的捨入方式由**小數位數**設定決定。 此設定適用於**圓餅圖**、**長條圖**和**日期直方圖**類型的圖表。 預設情況下，切換開關是關閉的。
期間分段長度	您要將期間劃分的分段的持續時間。適用於**日期直方圖**類型的圖表。
刻度	用於顯示資料的刻度。適用於**堆疊長條圖**。以下值可用： • **線性** • **平方** • **對數** 預設值為**線性**。
迴歸	在圖表上顯示平均值的選項。以下值可用： • **未設定**。 • **線性** • **LOESS**（使用局部估計散點圖平滑的曲線）。 適用於**日期直方圖**和**折線圖**類型。

操作頁籤

如果您在**一般**頁籤的**圖表**欄位中選取下列其中一個值，則不會顯示此頁籤：**計數器**、**速度計圖**、**表格**。

此頁籤上的設定允許您在小工具的各種元素上設定左鍵點擊操作，例如在圖表分段或圖例項目的文字上。您可以選擇以下操作：

- 轉至事件。
- 依變數篩選。

  這些設定已在篩選多個小工具中的資料情景中進行了描述。

- 深層探究到另一個儀表板。

這些設定已在深層探究到另一個儀表板情景中進行了描述。

活動清單小工具

您可以使用**活動清單**小工具來取得基於SQL查詢的分析資料。

在建立此小工具時，您必須指定下表中所述的設定。

一般頁籤

下表列出了**常用**頁籤上必須指定的設定。

描述

設定	描述
圖表	圖表類型。有下列應用程式類型可用： • **長條圖** • **圓餅圖** • **計數器** • **表格**
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
關聯器	包含要接收其資料的活動清單的關聯器的名稱。
活動清單	要接收其資料的活動清單的名稱。 不同的關聯器可以使用相同的活動清單。但是，每個關聯器都會建立一個單獨的活動清單實體。因此，即使活動清單具有相同的名稱和ID，不同關聯器使用的活動清單的內容也會有所不同。

設定	描述
SQL查詢欄位	該欄位可讓您手動輸入用於篩選和搜尋活動清單資料的查詢。 查詢結構類似於事件搜尋中使用的查詢結構。 建立基於活動清單的查詢時，必須考慮下列事項： • 對於FROM函式，必須指定「records」值。 • 如果您要接收名稱包含空格和西里爾字元的欄位資料，則您也必須在查詢中將這些名稱括在引號中： • 在SELECT函式中，將別名括在雙引號或反引號中："alias"，`another alias`。 • 在ORDER BY函式中，將別名括在反引號中：`another alias`。 • 事件欄位值用直引號括起來：WHERE DeviceProduct = 'Microsoft'。 • 事件欄位名稱無需用引號括起來。 • 如果活動清單欄位的名稱以空格開頭或結尾，則小工具不會顯示這些空格。欄位名稱不能僅包含空格。 • 如果活動清單欄位的值包含尾隨或前導空格，建議使用LIKE '%field value%'函式進行搜尋。 • 在查詢中，您可以使用服務欄位：_key（包含活動清單記錄的鍵欄位）和 _count（此記錄新增至活動清單的次數），以及自訂欄位。 • 除表格外，任何類型的活動清單分析小工具都無法編輯SQL查詢中的「metric」和「value」別名。 • 如果在SQL查詢中使用了日期和時間轉換函式（例如 fromUnixTimestamp64Milli），且正在處理的欄位不包含日期和時間，則小工具中將顯示錯誤。為避免這種情況，請使用可以處理空值的函式。範例：SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250。 • LIMIT函式的值過大可能會導致瀏覽器錯誤。 • 如果選擇計數器作為圖表類型，必須為SELECT函式的值指定資料處理方法：`count`、`max`、`min`、`avg`、`sum`。 • 在圖表為**表格**類型的小工具中，漸層是根據SQL查詢中指定的欄位值繪製的（例如，`_count`、`value`、`temp`或`name`）。此欄位可從**漸變指示器欄位**下拉清單中選擇（如果查詢包含多個數字或時間欄位，則可以選擇其中任一個）。之後，所選直欄的儲存格將以漸層填滿標記突出顯示。如果查詢中不存在某個欄位，**外觀**頁籤將不會顯示**漸層**和**漸變指示器欄位**欄位。 在SQL函數和SELECT中使用別名時需要特別注意，您可以使用雙引號和反引號："、`。 如果您選擇計數器作為圖形類型，別名可以包含拉丁字元和西里爾字元以及空格。使用空格或西里爾字元時，別名必須用引號括起來："具有空格的別名"，`另一個別名`。 顯示前一期間的資料時，依計數（ID）參數可能無法正常運作。建議依metric參數排序。例如，SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250。

您可以在小工具中取得租用戶的名稱，而不是它們的ID。

如果您希望在活動清單小工具中顯示租用戶名稱而非租用戶ID，請在關聯器的關聯規則中設定用於使用對應租用戶資訊填入活動清單的函式。設定流程包括以下步驟：

1. 匯出租用戶清單。
2. 建立一個**表格**類型的字典，並將先前取得的租用戶清單匯入該字典。
3. 在關聯規則中新增一個局部變數，該變數具有用於將租用戶名稱對應到租用戶ID的**dict**函式。

   範例：

   - 變數：`TenantName`
   - 值：`dict ('<Name of the previously created dictionary with tenants>', TenantID)`
4. 在關聯規則中新增活動清單動作。此動作會使用 **Set** 函式，以金鑰-值格式將先前建立的變數值寫入活動清單。將活動清單的欄位（例如 `Tenant`）指定為金鑰，並在**值**欄位中參照先前建立的變數（例如 `$TenantName`）。

當此規則觸發時，由 **dict** 函式從租用戶字典對應至 ID 的租用戶名稱將被置入活動清單。建立活動清單的小工具時，您可以透過參照活動清單欄位的名稱（在上述範例中為 `Tenant`）來取得租用戶名稱。

上述方法可套用於其他具有ID的事件欄位。

基於活動清單接收分析的SQL查詢範例：

- `SELECT * FROM `records` WHERE "Event source" = 'Johannesburg' LIMIT 250`
  此查詢傳回活動清單的鍵，其中欄位名稱為「事件來源」，該清單的值範例為「約翰內斯堡」。
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  查詢圓餅圖，該圓餅圖返回活動清單中的鍵數（「_key」欄位上的「count」彙總）和狀態自定義欄位的所有變體。此小工具顯示一個圓餅圖，其中顯示了活動清單中的記錄總數，並依比例除以**狀態**欄位的可能值的數量。
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  查詢表格，該表格返回**名稱**和**狀態**自訂欄位的值，以及描述自訂欄位值與ILIKE「%ftp%」匹配的活動清單記錄的服務欄位「_count」。此小工具顯示一個包含**狀態**、**名稱**和**數量**欄位的表格。

座標軸頁籤

下表列出了必須在**座標軸**頁籤上指定的設定。

如果在**常用**頁籤上的**圖表**欄位中選擇了**長條圖**，則會顯示此頁籤。

描述

設定	描述
Y軸最小值和Y軸最大值	Y軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。
X軸最小值和X軸最大值	X軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。

外觀頁籤

下表列出了**外觀**頁籤上必須指定的設定。

描述

設定	描述
名稱	小工具的名稱。
描述	小工具的描述。
顏色	用於顯示資訊的顏色： • **預設**為瀏覽器的預設字體顏色 • **綠色** • **紅色** • **藍色** • **黃色**
漸層	圖表的漸層填充： • 兩種顏色（紅色和綠色） • 三種顏色（紅色、黃色和綠色） 此設定適用於長條圖和表格。 您可以透過點擊切換方向圖示（⇆）來調整填充方向；您還可以設定閾值。 如果未手動設定，漸層閾值將根據資料自動計算。如果在指定的閾值之間沒有資料，則不會套用漸層。而是使用兩種顏色：一種用於低於下限閾值的值，另一種用於高於上限閾值的值。
漸變指示器欄位	顯示漸層填充指標的直欄。 此設定適用於**表格**類型的圖表。
水平方向	以水平方向而不是垂直方向顯示直方圖。 啟用此設定後，所有可用資訊都將適合設定的小工具大小。如果資料量很大，您可以增加小工具的大小以獲得最佳顯示效果。
顯示總和	顯示值的總和。

設定	描述
顯示圖例	顯示用於分析的圖例。切換開關預設為開啟。
在圖例中顯示空值	在分析的圖例中顯示具有空值的參數。切換開關預設為開啟。 僅當啟用**顯示上一期間的資料**設定且目前期間沒有資料，但上一期間有資料時，才會顯示空值。

快線表單小工具

您可以使用**快線表單**小工具來取得基於SQL查詢的分析。

建立此類小工具時，必須為以下設定設定值：

頁籤：

下表列出了**常用**頁籤上必須指定的設定。

描述

設定	描述
圖表	有下列應用程式類型可用： • **長條圖** • **圓餅圖** • **計數器** • **表格**
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
關聯器	包含您要接收資訊的快線表單的關聯器的名稱。
快顯表單	您想要接收資訊的快顯表單的名稱。 同一個快顯表單可用於多個關聯器。但是，每個關聯器都會建立一個單獨的快顯表單實體。因此，即使快顯表單具有相同的名稱和ID，不同關聯器使用的快顯表單的內容也是不同的。

設定	描述
SQL查詢欄位	該欄位可讓您手動輸入查詢來篩選和搜尋快顯表單資料。預設情況下，對於每個小工具類型，該欄位都包含一個查詢，該查詢依鍵欄位取得快顯表單模式和金鑰。 查詢結構類似於事件搜尋中使用的查詢結構。 基於快顯表單建立查詢時，必須考慮以下事項： • 對於 FROM 函式，必須指定 `records` 值。 • 您只能取得快顯表單結構中指定欄位的資料。 • 您可以使用ClickHouse的支援功能。 • 如果您要接收名稱包含空格和西里爾字元的欄位資料，則您也必須在查詢中將這些名稱括在引號中： • 在 SELECT 函式中，將別名括在雙引號或反引號中："<別名>"，`<另一個別名>`。 • 在 ORDER BY 函式中，將別名括在反引號中：`<另一個別名>`。 • 事件欄位值會括在直引號中：WHERE DeviceProduct = 'Microsoft'. • 事件欄位名稱無需用引號括起來。 • 如果活動清單欄位的名稱以空格開頭或結尾，則小工具不會顯示這些空格。欄位名稱不能僅包含空格。 • 如果活動清單欄位的值包含尾隨或前導空格，建議使用 LIKE '%< 欄位值 >%' 函式進行搜尋。 • 您可以使用 _count 服務欄位（此記錄已新增至快顯表單的次數）以及自訂欄位。 • 除表格外，任何類型的活動清單分析小工具都無法編輯 SQL 查詢中的 metric 和 value 別名。 • 如果在 SQL 查詢中使用日期和時間轉換函式（例如 fromUnixTimestamp64Milli ），且正在處理的欄位不包含日期和時間，則小工具中將顯示錯誤。為避免這種情況，請使用可以處理空值的函式。範例：SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250 。 • LIMIT 函式的值過大可能會導致瀏覽器錯誤。 • 如果您選擇**計數器**做為圖表類型，則必須為 SELECT 函式的值指定資料處理方法：count 、max 、min 、avg 、sum 。 • 在使用**表格**類型圖表的小工具中，漸層僅適用於**INT**和**FLOAT**類型的欄位，以及**_count**欄位。您可以從**漸變指示器欄位**下拉清單中選擇欄位。之後，所選直欄的儲存格將以漸層填滿標記突出顯示。 在 SQL 函式和 SELECT 陳述式中使用別名時的特殊注意事項：您可以使用雙引號和反引號："、`。 使用空格或西里爾字元時，別名必須用雙引號括住：<含空格的別名>"，值必須用直單引號括住：'<含空格的值>' 顯示上一個期間的資料時，依 count(ID) 參數排序可能無法正常運作。建議依 metric 參數排序。例如，SELECT count(ID) AS "metric" 、Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250 。

您可以在小工具中取得租用戶的名稱，而不是它們的ID。

如果您希望在活動清單小工具中顯示租用戶名稱而非租用戶ID，請在關聯器的關聯規則中設定用於使用對應租用戶資訊填入活動清單的函式。設定流程包括以下步驟：

1. 匯出租用戶清單。
2. 建立一個**表格**類型的字典，並將先前取得的租用戶清單匯入該字典。
3. 在關聯規則中新增一個局部變數，該變數具有用於將租用戶名稱對應到租用戶ID的**dict**函式。

   範例：

   - 變數：TenantName
   - 值：dict ('<Name of the previously created dictionary with tenants>', TenantID)
4. 在關聯規則中新增活動清單動作。此動作會使用 **Set** 函式，以金鑰-值格式將先前建立的變數值寫入活動清單。將活動清單的欄位（例如 Tenant ）指定為金鑰，並在**值**欄位中參照先前建立的變數（例如 $TenantName ）。

   當此規則觸發時，由 **dict** 函式從租用戶字典對應至 ID 的租用戶名稱將被置入活動清單。建立活動清單的小工具時，您可以透過參照活動清單欄位的名稱（在上述範例中為 Tenant ）來取得租用戶名稱。

上述方法可套用於其他具有ID的事件欄位。

基於活動清單接收分析的SQL查詢範例：

- `SELECT * FROM `records` WHERE "Event source" = 'Johannesburg' LIMIT 250`
  此查詢會傳回活動清單的金鑰，其中欄位名稱為「`Event source`」，且此欄位的值為「`Johannesburg`」。
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  圓餅圖查詢，會傳回活動清單中的金鑰數量（「**_key**」欄位上的「`count`」彙總）以及 Status 自訂欄位的所有變體。此小工具顯示一個圓餅圖，其中顯示了活動清單中的記錄總數，並依比例除以**狀態**欄位的可能值的數量。
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  表格查詢，會傳回活動清單中描述自訂欄位的值符合`ILIKE '%ftp%'`的記錄，其**名稱**與**狀態**自訂欄位的值，以及服務欄位「**_count**」。此小工具顯示一個包含**狀態**、**名稱**和**數量**欄位的表格。

頁籤：

下表列出了必須在**座標軸**頁籤上指定的設定。

如果在**常用**頁籤上的**圖表**欄位中選擇了**長條圖**，則會顯示此頁籤。

描述

設定	描述
Y 軸 and 最小值 - 最大值	Y軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。
X 軸 and 最小值 - 最大值	X軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。

頁籤：

下表列出了**外觀**頁籤上必須指定的設定。

描述

設定	描述
名稱	小工具的名稱。
描述	小工具的描述。
顏色	用於顯示資訊的顏色： • **預設**為瀏覽器的預設字體顏色 • **綠色** • **紅色** • **藍色** • **黃色**
漸層	圖表的漸層填充： • 兩種顏色（紅色和綠色） • 三種顏色（紅色、黃色和綠色） 此設定適用於**長條圖**和**表格**。 您可以透過點擊切換方向圖示（⇆）來調整填充方向；您還可以設定閾值。 如果未手動設定，漸層閾值將根據資料自動計算。如果在指定的閾值之間沒有資料，則不會套用漸層。而是使用兩種顏色：一種用於低於下限閾值的值，另一種用於高於上限閾值的值。
漸變指示器欄位	顯示漸層填充指標的直欄。 此設定適用於**表格**類型的圖表。
水平方向	以水平方向而不是垂直方向顯示直方圖。 啟用此設定後，所有可用資訊都將適合設定的小工具大小。如果資料量很大，您可以增加小工具的大小以獲得最佳顯示效果。

設定	描述
顯示總和	顯示值的總和。
顯示圖例	顯示用於分析的圖例。切換開關預設為開啟。
在圖例中顯示空值	在分析的圖例中顯示具有空值的參數。切換開關預設為開啟。 僅當啟用**顯示上一期間的資料**設定且目前期間沒有資料，但上一期間有資料時，才會顯示空值。

資產自訂小工具

您可以使用**資產→自訂小工具**，透過查詢建構器從已處理的事件中取得進階資產分析。在查詢中，您需要指定資產欄位以及用於統計資產的對應條件或條件集（Y軸）。您也可以指定一個或多個附加條件（類別），用於比較每個欄位的資產數量。

為資產建立自訂小部件時，您必須指定下表中描述的設定。

一般頁籤

下表描述了**一般**頁籤上的設定。

描述

設定	描述
名稱	小工具的名稱。 以Excel格式儲存報告時，工作表標題中顯示的小工具名稱長度限制為31個字元。我們建議您在命名小工具時注意此限制。
圖表	圖表類型。有下列應用程式類型可用： • **圓餅圖**。 依指定類別顯示資產分佈情況，適用於所有選定的租用戶。 • **計數器**。 資產基於單一條件進行統計。圖表顯示所有選定租用戶中符合該條件的資產總數。 • **表格**。 資產按所有選定租用戶的指定類別進行統計。圖表中的每個類別都對應一行。類別名稱顯示在**值**欄位中。符合條件的資產數量顯示在**指標**欄位中。 • **堆疊長條圖** 資產依所有選定租用戶的指定類別進行統計，您可以依租用戶對資產進行分組（在這種情況下，各個租用戶沿X軸排列）。每個類別在圖表的長條上都有自己的區域，並以不同的顏色表示。類別名稱顯示在圖例中。您可以使用類別名稱左側的核取方塊來隱藏或顯示長條上的對應區域。 • **速度計圖** 此圖表顯示符合指定條件的資產數量佔資產總數的比例。 圖表中的數值以百分比表示。
格式	此設定適用於**堆疊長條圖**。資料顯示格式：**絕對值**或**相對值（%）**。如果選擇**絕對值**格式，則長條的高度對應於所測量指標值的總和。如果選擇**相對值（%）**格式，所有長條的高度均為100%，長條上彩色區域的相對高度對應於指標值的比率。 預設情況下，選擇**絕對值**。
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
資產類別	小工具顯示其資料的資產類別。
在未分類資產中搜尋	此設定可讓您顯示沒有類別的資產。 預設情況下，此核取方塊已清除。
選取圖表座標軸設定群組	
Y軸	必需設定。資產欄位以及為此欄位指定的條件或條件集，用於定義資產的計數方式。
Y 軸類別	所選欄位的類別。不適用於**計數器**類型的圖表。對於值為列舉的Y軸欄位，此設定是可選的（可以從有限的值清單中選擇）。對於所有其他欄位，此參數是必需的。
依租用戶分組	此設定適用於**堆疊長條圖**類型的圖表。啟用依租用戶對資產進行額外分組。如果選取此核取方塊，圖表上的資產將沿著X軸分成與個別租用戶對應的長條圖。如果取消選取此核取方塊，則所有資產將顯示在同一長條上。預設情況下，此核取方塊已清除。

外觀頁籤

下表描述了**外觀**頁籤上的設定。

設定	描述
描述	小工具的描述。
顯示總和	此設定適用於**圓餅圖**類型的圖表。除了選定的類別外，還可以在圖表中顯示總數。如果啟用此核取方塊，則所有指定類別的值總和將顯示在圓餅圖中心，並在圖例的單獨**總計**直欄中顯示。預設情況下，切換開關是關閉的。
顏色	此設定適用於**計數器**類型的圖表。用於顯示資訊的顏色： • **預設**為瀏覽器的預設字體顏色 • **綠色** • **紅色** • **藍色** • **黃色**
漸層	圖表的漸層填充： • 兩種顏色（紅色和綠色） • 三種顏色（紅色、黃色和綠色） 此設定適用於**表格**類型的圖表。 您可以透過點擊切換方向圖示（⇆）來調整填充方向；您還可以設定閾值。 如果未手動設定，漸層閾值將根據資料自動計算。如果在指定的閾值之間沒有資料，則不會套用漸層。而是使用兩種顏色：一種用於低於下限閾值的值，另一種用於高於上限閾值的值。
漸變指示器欄位	顯示漸層填充指標的直欄。此直欄由下拉清單中所選的**指標**欄位決定。 此設定適用於**表格**類型的圖表。
水平方向	以水平方向而不是垂直方向顯示直方圖。 啟用此選項後，當小工具顯示大量資料時，水平捲動不可用，所有可用資訊都適合小工具的固定大小。如果要顯示大量資料，建議增加小工具的大小。
顯示圖例	顯示用於分析的圖例。切換開關預設為開啟。
在圖例中顯示空值	在分析的圖例中顯示具有空值的參數。切換開關預設為開啟。 僅當啟用**顯示上一期間的資料**設定且目前期間沒有資料，但上一期間有資料時，才會顯示空值。
在圖例中顯示百分比	圖例中顯示百分比值。切換開關預設為開啟。
小數	顯示數值必須四捨五入到的小數位數。
刻度	適用於**堆疊長條圖**。用於顯示資料的刻度。以下值可用： • **線性** • **平方** • **對數** 預設值為**線性**。
閾值	適用於**速度計圖**。預設情況下，指定以下範圍：0–30、30–70、70–100。

其他小工具

本節說明除 **事件**、**作用中清單**、**內容相關表格**和自訂**資產**小工具以外的所有小工具設定。

小工具可用的參數集取決於小工具上顯示的圖表類型。KUMA提供以下圖表類型：

- 圓餅圖（ ）。
- 計數器（ ）。
- 表格（ ）。
- 長條圖（ ）。
- 日期直方圖（ ）。
- 折線圖

圓餅圖的設定

下表列出了**圓餅圖**的設定。

描述

設定	描述
名稱	小工具的名稱。
描述	小工具的描述。
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
期間	小工具中顯示資料的期間。預設為**依佈局**，意味著為佈局選定的期間顯示資料。 您也可以透過以下方式之一為小工具指定期間： • 在日曆中選擇期間的確切開始和結束日期和時間，然後按一下**套用**。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對期間，或兩者的組合。 詳情請參閱下面的*設定期間*子部分。
顯示總和	顯示值的總和。
顯示圖例	顯示用於分析的圖例。切換開關預設為開啟。
在圖例中顯示空值	在分析的圖例中顯示具有空值的參數。切換開關預設為開啟。
小數	顯示數值必須四捨五入到的小數位數。

計數器的設定

下表列出了**計數器**的設定。

描述

設定	描述
名稱	小工具的名稱。
描述	小工具的描述。
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
期間	小工具中顯示資料的期間。預設為**依佈局**，意味著為佈局選定的期間顯示資料。 您也可以透過以下方式之一為小工具指定期間： • 在日曆中選擇期間的確切開始和結束日期和時間，然後按一下**套用**。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對期間，或兩者的組合。 詳情請參閱下面的*設定期間*子部分。

表格的設定

下表列出了**表格**的設定。

描述

設定	描述
名稱	小工具的名稱。
描述	小工具的描述。
租用戶	小工具中顯示資料的租用戶。您可以選取多個租用戶。預設情況下，顯示在佈局設定中選擇的租用戶的資料。
期間	小工具中顯示資料的期間。預設為**依佈局**，意味著為佈局選定的期間顯示資料。 您也可以透過以下方式之一為小工具指定期間： • 在日曆中選擇期間的確切開始和結束日期和時間，然後按一下**套用**。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對期間，或兩者的組合。 詳情請參閱下面的*設定期間*子部分。

設定	描述
漸層	圖表的漸層填充： • 兩種顏色（紅色和綠色） • 三種顏色（紅色、黃色和綠色） 您可以透過點擊切換方向圖示（⇆）來調整填充方向；您還可以設定閾值。 如果未手動設定，漸層閾值將根據資料自動計算。如果在指定的閾值之間沒有資料，則不會套用漸層。而是使用兩種顏色：一種用於低於下限閾值的值，另一種用於高於上限閾值的值。
漸變指示器欄位	顯示漸層填充指標的直欄。 此直欄由下拉清單中所選的欄位決定。欄位類型取決於小工具的類型： • 對於**受影響資產**，它是**頻率**欄位； • 對於**事件中受影響資產**、**KSC資產的即時防護擴充狀態**和**事件中受影響使用者**，它是**計數**欄位。
小數	顯示數值必須四捨五入到的小數位數。

長條圖和日期直方圖的設定

下表列出了**坐標軸**頁籤上的**長條圖**和座標軸類型的圖表的設定。

描述

設定	描述
Y 軸 and 最小值 - 最大值	Y軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。
X 軸 and 最小值 - 最大值	X軸刻度。 圖表軸上可以顯示負值。這是由於小工具上圖表的縮放比例造成的，可以透過將最小圖表值設為零而不是**自動**來解決。
小數	顯示數值必須四捨五入到的小數位數。

下表列出了**外觀**頁籤上的**長條圖**、**堆疊長條圖**和外觀類型的圖表的設定。

描述

設定	描述
名稱	小工具的名稱。
描述	小工具的描述。
期間	小工具中顯示資料的期間。預設為**依佈局**，意味著為佈局選定的期間顯示資料。 您也可以透過以下方式之一為小工具指定期間： • 在日曆中選擇期間的確切開始和結束日期和時間，然後按一下**套用**。 • 在**相對時間段**清單中選擇相對於目前時間的時間段。 • 手動輸入數值：確切的日期和時間或相對期間，或兩者的組合。 詳情請參閱下面的*設定期間*子部分。
格式	資料顯示格式：**絕對值**或**相對值（%）**。此設定適用於**堆疊長條圖**。 如果選擇**絕對值**格式，則長條的高度對應於所測量指標值的總和。如果選擇**相對值（%）**格式，所有長條的高度均為100%，長條上彩色區域的相對高度對應於指標值的比率。 預設情況下，選擇**絕對值**。
時間軸檢視畫面	時間資料顯示格式：**長條圖**或**折線圖**。此設定適用於**日期直方圖**類型的圖表。 選擇**長條圖**格式時，資料預設以垂直長條的形式顯示。如果SQL查詢包含一個帶有類別別名的附加欄位，則圖表將成為堆疊長條圖，即每個長條圖根據該欄位的值劃分為條紋。 選擇**折線圖**格式時，資料將顯示為一條或多條（取決於查詢）穿過時間軸上的點的折線。 預設選擇長條圖格式。
顯示上一期間的資料	啟用同時顯示兩個期間的資料：當前期間和上一個期間。

設定	描述
顏色	用於顯示資訊的顏色： • **預設**為瀏覽器的預設字體顏色 • **綠色** • **紅色** • **藍色** • **黃色**
漸層	圖表的漸層填充： • 兩種顏色（紅色和綠色） • 三種顏色（紅色、黃色和綠色） 您可以透過點擊切換方向圖示（⇆）來調整填充方向；您還可以設定閾值。 如果未手動設定，漸層閾值將根據資料自動計算。如果在指定的閾值之間沒有資料，則不會套用漸層。而是使用兩種顏色：一種用於低於下限閾值的值，另一種用於高於上限閾值的值。 堆疊長條圖不套用漸層填充。在這種情況下，顏色會自動分配。
水平方向	以水平方向而不是垂直方向顯示直方圖。啟用此設定後，所有可用資訊都將適合設定的小工具大小。如果資料量很大，您可以增加小工具的大小以獲得最佳顯示效果。
顯示總和	顯示值的總和。
顯示圖例	顯示用於分析的圖例。切換開關預設為開啟。
在圖例中顯示空值	在分析的圖例中顯示具有空值的參數。切換開關預設為開啟。 僅當啟用**顯示上一期間的資料**設定且目前期間沒有資料，但上一期間有資料時，才會顯示空值。
期間分段長度	您要將期間劃分的分段的持續時間。適用於**日期直方圖**類型的圖表。

速度計圖表的設定

下表列出了**速度計圖**的設定。

> 圖表中的數值以百分比表示。

描述

設定	描述
General頁籤	
名稱	小工具的名稱。
租用戶	其資料顯示在小工具中的租用戶。您只能選擇先前在儀表板設定中選擇的租用戶。
資產類別	將要搜尋值的選定類別的資產。
在未分類資產中搜尋	在圖表中搜尋資產時，系統將忽略資產類別。
Y軸	用於搜尋資產並隨後計算速度計讀數的參數值。 您可以指定多個參數值來搜尋資產。
外觀頁籤	
描述	小工具上顯示的圖表的描述。
閾值	為了幫助您直觀地識別事件的嚴重等級，速度計的錶盤分為三個區域：綠色、黃色和紅色。預設情況下，這些區域設定了以下間隔： • 綠色： 0–30 • 黃色： 30–70 • 紅色： 70–100 您可以根據需要變更範圍。

設定期間

對於**圓餅圖**、**計數器**、**表格**、**長條圖**、**堆疊長條圖**、**日期直方圖**等圖表，您可以使用**期間**設定，設定小工具中資料的顯示期間。預設情況下，小工具的資料顯示期間與儀表板的資料顯示期間相同。

若要設定資料顯示期間，請執行下列操作之一：

- 如有必要，請按以下方式之一變更**期間**設定中的日期和時間：

  - 如果您想要指定確切日期，請在左側行事曆中選擇期間的開始日期和結束日期，然後按一下**套用**。

    您可以選擇包括目前日期在內的任意日期。日期和時間格式取決於瀏覽器的設定。如果**範圍起始**或**範圍結尾**欄位已有值，且您未手動編輯時間值，則當您在行事曆中選擇日期時，**範圍起始**欄位會自動填入00:00:00.000，而**範圍結尾**欄位會自動填入23:59:59.999。如果您已手動刪除**範圍起始**或**範圍結尾**欄位中的值，則當您在日曆中選擇日期時，該欄位會自動填入當前時間。在其中一個欄位中選擇值後，焦點將切換到另一個欄位。如果您的**範圍結尾**早於**範圍起始** ，則較早的值會自動插入到**範圍起始**欄位中。

  - 如果您想要指定相對期間，請在右側的**相對期間**清單中選擇一個可用期間。

    期間是相對於當前時間計算的。

  - 如果要指定自訂期間，請編輯**範圍起始**和**範圍結尾**欄位的值。

    您可以以**DD.MM.YYYY HH:mm:ss.SSS**格式（用於俄文在地化）和**YYYY-MM-DD HH:mm:ss.SSS**格式（用於英文在地化）輸入確切的日期和時間，或者以公式的形式輸入相對期間。您也可以根據需要結合使用這些方法。如果在輸入確切日期時未指定毫秒，則會自動替換為000。如果您已編輯**範圍起始**或**範圍結尾**欄位中的時間，則在日曆中選擇日期不會變更時間部分。

    在相對期間公式中，您可以使用當前日期和時間的**now**參數以及間隔參數化語言：**+**（僅在**範圍結尾**欄位中）、**-**、**/**（四捨五入至最接近的），以及時間單位：**y**（年）、**M**（月）、**w**（周）、**d**（天）、**h**（小時）、**m**（分鐘）、**s**（秒）。例如，您可以指定**now-5d**期間以取得過去五天的資料，或指定**now/w**期間以取得從本週第一天（UTC時間00:00:00:00）到當前時間（**now**）的資料。

    > **範圍起始**欄位為必填項，其值不能超過**範圍結尾**欄位的值，且不能早於1970年1月1日（如果指定確切日期或相對期間）。**範圍結尾**不能早於**範圍起始**。如果未在**範圍結尾**欄位中指定值，則自動指定**now**。

  KUMA以UTC格式儲存時間值，但在使用者介面中，時間會轉換為瀏覽器的時區。這與相對時間段相關：**今天**、**昨天**、**本週**和**本月**。例如，如果瀏覽器中的時區是UTC+3，並且您選擇**今天**作為資料顯示期間，則將顯示從03:00:00.000到現在的資料，而不是從00:00:00.000到現在。

  如果您想在選擇相對資料顯示期間（如**今天**、**昨天**、**本週**或**本月**）時考慮您的時區，則需要透過新增或減去正確的小時數來手動在**範圍起始**和**範圍結尾**（如果指定了現在以外的值）中新增時間偏移。例如，如果您的瀏覽器時區是UTC+3，並且您想要顯示**昨天**的資料，您需要將**範圍起始**變更為**now-1d/d-3h**，並將**結束日期**更改為**now/d-3h**。如果您想顯示**今天**期間的資料，您只需要將**範圍起始**欄位中的值變更為**now/d-3h**。

  > 如果您需要截至昨天23:59:59:999 UTC的結果，可以使用帶有時間戳篩選器的SQL查詢，或指定確切的日期和時間。

  期間的邊界包含所有時間：例如，對於**今天**時間範圍，事件顯示範圍從當天開始（00:00:00:00）到當前時間（**now**），包含當前時間；對於**昨天**期間，事件顯示範圍從前一天開始（00:00:00:00）到當天00:00:00:00。將滑鼠懸停在小工具中的期間圖示上，即可查看上次資料更新的日期和時間以及資料顯示的確切期間。

  如果小工具啟用了顯示上一期間資料設定，且小工具顯示的是相對期間的資料，則工具提示也會顯示上一期間。上一期間是相對於當前期間計算的，計算方法為：當前期間的起始值和結束值減去當前期間的持續時間。例如，如果資料每日更新並顯示一個月，但該月只過去了前10天，則上一期間為上個月的最後10天。

若要在小工具顯示佈局中選定期間的資料，請按一下**重設**按鈕。更改佈局中顯示的期間也會更改小工具中顯示的期間。

篩選小工具資料

KUMA 可讓您透過在儀表板中選取篩選參數，篩選 **事件** 類型小工具中的資料。在以下情況下，您可以篩選資料：

- 在單一小工具上篩選資料

  對於這種類型的篩選，您需要在小工具內容的SQL查詢中指定一個或多個局部變數。變數可讓您透過將儀表板小工具的資料替換到查詢中來修改此SQL查詢。小工具會根據變數的新值篩選資料並重新整理圖表。您無需在小工具內容中手動變更SQL查詢。

  您可以透過點擊小工具中的漏斗圖示（ ）來應用局部變數。這將打開一個窗口，您可以在其中選擇或輸入局部變數的值。

- 在同一儀表板中的多個小工具中篩選資料

  對於這種類型的篩選，您需要在儀表板內容中指定一個或多個全域變數。然後，將全域變數新增至要套用這些全域變數的小工具的SQL查詢。當您為全域變數指派新值時，所有使用此變數的小工具都會根據新值自動重新建構圖表。

  點擊圖表的某個部分或圖例中的文字即可套用全域變數。KUMA將顯示一個選單，其中包含將所選圖表部分或圖例項目的資料類別套用至變數的指令。

- 深層探究到另一個儀表板時，可以使用全域變數傳遞篩選參數

  全域變數可用於將值傳遞到另一個儀表板。從一個儀表板深層探究到另一個儀表板時，KUMA會取代所選變數值和所選期間，並自動重新建構新儀表板的圖表。

  深層探究到另一個儀表板時，不能使用局部變數。

我們不建議在一個儀表板中設定超過五個變數。這可能會導致儀表板運作不穩定。

在單一小工具上篩選資料

KUMA 可讓您在儀表板中選取篩選參數，並在**事件**類型的小工具中篩選資料。

若要對單一小工具的資料進行篩選，需要在小工具內容的SQL查詢中指定一個或多個局部變數。變數可讓您透過將儀表板小工具的資料替換到查詢中來修改此SQL查詢。小工具會根據變數的新值篩選資料並重新整理圖表。您無需在小工具內容中手動變更SQL查詢。

我們不建議在一個儀表板中設定超過五個變數。這可能會導致儀表板運作不穩定。

在單一元件上設定資料篩選

若要在小工具內設定用於資料篩選的局部變數：

1. 在**儀表板**部分，選擇一個儀表板，然後按一下**編輯**按鈕，進入儀表板編輯模式。
2. 選擇現有的**事件**小工具，或按一下**新增小工具**按鈕，然後選擇**事件**小工具類型。
3. 在小工具內容視窗中，選取**一般**頁籤。
4. 在**定義的變數**下，按一下**新增**。
5. 輸入變數的任意名稱，然後指定變數的值。儀表板中的局部變數和全域變數名稱必須唯一。

將value或category指定為變數的值，亦即查詢中使用的欄位別名。如果您想在小工具中篩選資料時手動輸入此變數的值，請將此欄位留空。

對於表格類型的圖表，您可以將事件欄位的名稱指定為變數的值。這樣，您就可以根據此欄位的選定值篩選表格中的資料。事件欄位的名稱會顯示在表格列的標頭中。

6. 在**SQL查詢**欄位的WHERE子句中，加入一個函式來處理這些變數。

   具有特定值的變數的語法如下：

   ```
   filter(<event_field_name> = $variable_name)
   ```

   手動輸入任意值的變數的語法如下：

   ```
   filter(<event_field_name> like $variable_name)
   ```

   在這種情況下，在手動輸入時，您可以使用%元字元來搜尋相符的部分文字。有關詳細資訊，請參閱ClickHouse說明文件。

   > 您不能使用SQL建構器為SQL查詢新增變數。

   查看範例

   含區域變數的 SQL 查詢範例

   ```
   SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name)
   GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250
   ```

   此查詢使用局部變數`$Name`。`Name`事件欄位的值會代入此變數。您可以點擊漏斗圖示（ ）將變數套用在小工具上。這將開啟一個視窗；在該視窗中，您可以為變數指定一個值。小工具會依據`Name`欄位的所選值篩選選取項目。

   請注意，如果在SQL查詢中為取數值的欄位指定變數，則必須將該值轉換為字串。您可以使用`toString`函式執行此操作。否則，SQL查詢將傳回錯誤。

   範例

   ```
   SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like
   $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250
   ```

   在此查詢中，`SourcePort event`欄位的值為數值，因此會將其轉換為字串：`toString(SourcePort)`。

7. 儲存您的變更。

將資料篩選套用至單一小工具

若要在小工具內套用局部變數進行資料篩選：

1. 在**儀表板**部分，選擇包含相關小工具的儀表板。必須在此小工具內容中設定至少一個局部變數。
2. 在小工具上，按一下漏斗圖示（ ）。
3. 這將開啟一個視窗；在該視窗中，選擇要套用的局部變數。
4. 儲存您的變更。

   此元件會根據變數的新值重新構建圖表。

在多個小工具中篩選資料

KUMA 可讓您在儀表板中選取篩選參數，並在**事件**類型的小工具中篩選資料。

要在一個儀表板中的多個小工具中篩選資料，您需要在儀表板內容中指定一個或多個全域變數。然後，將全域變數新增至要套用這些全域變數的小工具的SQL查詢。當您為全域變數指派新值時，所有使用此變數的小工具都會根據新值自動重新建構圖表。

點擊圖表的某個部分或圖例中的文字即可套用全域變數。KUMA將顯示一個選單，其中包含將所選圖表部分或圖例項目的資料類別套用至變數的指令。

> 我們不建議在一個儀表板中設定超過五個變數。這可能會導致儀表板運作不穩定。

在儀表板層級設定多個小工具的資料篩選

若要在儀表板層級設定多個小工具的資料篩選：

1. 在**儀表板**部分，選擇一個儀表板，然後按一下**編輯**按鈕，進入儀表板編輯模式。
2. 點擊**設定**按鈕。
3. 這將打開一個視窗；在該視窗的**變數**部分，選擇**全域變數**頁籤。
4. 按一下**新增**按鈕。
5. 在新行中，輸入變數的名稱。儀表板中的局部變數和全域變數名稱必須唯一。

   所有新增了全域變數的儀表板小工具的名稱都列在**已用於小工具**直欄中。

   當您點擊圖表的分段或圖表圖例中的項目時，全域變數的名稱會顯示在快顯選單的命令中。
6. 儲存您的變更。
7. 選擇現有的**事件**小工具，或按一下**新增小工具**按鈕，然後選擇**事件**小工具類型。在此小工具中，您將設定點擊時的操作。
8. 在小工具內容視窗中，選取**一般**頁籤。
9. 在**定義的變數**部分，新增一個或多個您在儀表板內容中新增的全域變數。
10. 如有必要，請在SQL查詢欄位中使用filter()函式將全域變數新增至WHERE子句。這也會將設定的操作套用到此小部件。
11. 選取**操作**頁籤

    如果您想在點擊圖表的分段時顯示一個帶有命令的選單，以便按選定的分段類別篩選資料：

    a. 在**圖表分段**部分，啟用**依變數篩選**選項。

    b. 在**類別**清單中，選擇要替換 SQL 查詢中指定的 `category` 別名值的變數。

    類別選項僅適用於堆疊長條圖類型。

    c. 在**值**清單中，選擇要替換 SQL 查詢中指定的 `value` 別名值的變數。

如果您想顯示一個帶有命令的選單，以便在點擊圖例項目時依所選值篩選資料：

a. 在**圖例**項目部分，啟用**依變數篩選**選項。

如有必要，請按一下**從圖表分段設定複製**按鈕，將選定的參數值從**圖表分段**設定群組自動傳輸到**圖例項目**設定群組。

b. 在**值**清單中，選擇要替換為圖例項目變數的變數。

12. 在要套用全域變數的其他小工具內容中：

- 在**一般**頁籤的**定義的變數**部分，新增一個或多個全域變數。
- 在小工具的SQL查詢欄位中，使用filter()函式將全域變數新增至WHERE子句。

在儀表板層級對多個小工具套用資料篩選

若要套用全域變數來篩選小工具之間的資料：

1. 在**儀表板**部分，選擇要套用全域變數的小工具所在的儀表板。
2. 找到已設定點擊操作的小工具。按一下圖表的分段或圖例項目旁邊的箭頭圖示（ ⌄ ）以開啟選單。
3. 在選單中，按一下**將類別套用至變數<變數名稱>**或**將值套用至變數<變數名稱>**。

將選定類別或圖例項目的值指派給該變數。在目前儀表板中，所有使用此變數的小工具都會根據該變數的新值重新建構其圖表。此類小工具會標示漏斗圖標（ 1 ），圖標內的數字表示套用的篩選器數量。螢幕上方會顯示已套用的全域變數清單。若要清除小工具的資料篩選，請點選帶有數字的漏斗圖示（ 1 ）。若要清除儀表板所有小工具的資料篩選，請按一下儀表板部的**全部重設**。

深層探究到相關儀表板

KUMA 可讓您在目前儀表板的 **事件** 類型小工具中篩選資料，並深層探究到另一個儀表板，同時保留已設定的篩選參數和期間。

這是透過全域變數實現的。全域變數必須在兩個儀表板以及小工具內容中都進行設定：在目標儀表板中，變數在SQL查詢中指定；在來源儀表板中，變數在管理**深層探究到另一個儀表板**設定時指定。從一個儀表板深層探究到另一個儀表板時，KUMA會自動取代所選變數值和周期，之後再重新建構目標儀表板中的圖表。兩個儀表板必須在同一個租用戶中。

深層探究到另一個儀表板時，不能使用局部變數。

設定目標儀表板

若要設定目標儀表板：

1. 在KUMA網頁介面中，進入**儀表板**部分，選擇一個儀表板並建立一個全域變數。

變數名稱可能只包含英文字母和數字，不得包含空格。

2. 儲存您的變更。
3. 在儀表板，選擇現有的**事件**小工具，或按一下**新增小工具**按鈕，然後選擇**事件**小工具類型。

4. 在**一般**頁籤上，指定先前建立的變數：

   - 在**定義的變數**下
   - 在**SQL 查詢**欄位中，若要讓 SQL 查詢考慮變數的值，請將`filter()`函式新增到`WHERE`子句中。

     具有特定值的變數的語法如下：

     `filter(<event_field_name> = $variable_name)`

     手動輸入任意值的變數語法如下：

     `filter(<event_field_name> like $variable_name)`

     查詢範例

     含有 $ServiceName 變數的查詢：

     ```
     SELECT DestinationHostName AS Host, Name AS Status, Message AS Reason, ServiceName,
     Timestamp AS Time
     FROM events
     WHERE DeviceEventClassID = 'KLSRV_HOST_STATUS_CRITICAL' OR DeviceEventClassID =
     'KLSRV_HOST_STATUS_WARNING' AND filter(ServiceName = $ServiceName)
     ORDER BY Time DESC
     LIMIT 25
     ```

     當向下鑽取至目標儀表板時，如果在 $ServiceName 變數中傳遞值，該值會自動代入查詢中，並篩選資料。如果未指定變數的值，則會像不存在變數一樣執行查詢。

5. 儲存您的變更。

設定來源儀表板

若要設定來源儀表板：

1. 在KUMA網頁介面中，進入**儀表板**部分，選擇一個儀表板並建立一個全域變數。

   變數名稱必須與目標儀表板中建立的變數名稱相同。名稱只能包含英文字母和數字，不能包含空格。

2. 儲存您的變更。
3. 在儀表板，選擇現有的**事件**小工具，或按一下**新增小工具**按鈕，然後選擇**事件**小工具類型。
4. 在**一般**頁籤的**定義的變數**部分，指定先前建立的變數。
5. 在**操作**頁籤中，指定以下設定：

   a. 在**圖表分段**或**圖例項目**部分，啟用**深層探究到另一個儀表板**。

   b. 在**儀表板**下拉清單中，選擇目標儀表板。

   c. 在**值**下拉清單中，選擇要在深層探究到另一個儀表板時傳遞其值的變數。這必須是您之前建立的同一個變數。

   所選變數必須在目標儀表板小工具的SQL查詢中指定，以便在深層探究後自動篩選此小工具上的資料。

6. 儲存您的變更。

從來源儀表板深層探究到目標儀表板

若要從來源儀表板深層探究到目標儀表板：

1. 在KUMA網頁介面中，在**儀表板**下，選擇來源儀表板。

2. 找到已啟用**深層探究到另一個儀表板**選項的小工具。按一下已設定此操作的圖表圖例中的分段或項目。

   這將在新頁籤中開啟目標儀表板。原始小工具的期間自動套用至整個儀表板，從**值**下拉清單中選擇的值會作為變數傳遞給**事件**類型的小工具，在這些小工具中，此變數會透過`filter()`函式用於SQL查詢。其他儀表板小工具中的圖表會根據傳遞的值重新建構。

   如果您變更或刪除目標儀表板板上操作中指定的變數，則仍會執行深層探究操作，但不會傳遞變數的值。

在活動清單類型小工具中顯示租用戶名稱

如果您希望在**活動清單**小工具中顯示租用戶名稱而非租用戶ID，請在關聯器的關聯規則中設定使用對應租用戶資訊填入活動清單的功能。

設定流程包括以下步驟：

1. 匯出租用戶清單。

2. 建立**表格**類型的字典。

3. 將在步驟1中獲得的租用戶清單匯入到在本說明的步驟2中建立的字典中。

4. 將一個具有dict**函式的局部變數**新增至關聯規則中，用於將租用戶名稱對應到租用戶ID。

   範例：

   - 變數：`TenantName`
   - 值：`dict ('<Name of the previously created dictionary with tenants>', TenantID)`

5. 在關聯規則中新增一個**設定**動作，該動作會將先前建立的變數的值以 <key>-<value> 格式寫入活動清單。請指定活動清單的欄位作為金鑰（例如，`Tenant`），並在**值**欄位中指定變數（例如，`$TenantName`）。

當此規則觸發時，由**dict**函式對應到租用戶字典中的ID的租用戶名稱被放置在活動清單中。基於活動清單建立小工具時，小工具將顯示租用戶名稱而不是租用戶ID。

偵測和回應儀表板

在**儀表板**部分，您可以監控組織網路的安全狀態。

儀表板是一組顯示網路安全資料分析的小工具。您只能檢視您有存取權限的租用戶的資料。

儀表板中使用的小工具選擇稱為*佈局*。您可以手動建立佈局或使用預定義佈局。您可以根據需要編輯預定義佈局中的小工具設定。預設情況下，儀表板顯示警示概覽預定義佈局。

只有具有主管理員、租用戶管理員、二級分析師和一級分析師角色的使用者才能建立、編輯或刪除佈局。具有所有角色的使用者帳戶都可以檢視佈局並設定預設佈局。如果將佈局設定為預設佈局，則每次使用者導覽至**儀表板**部分時，都會為該帳戶顯示該佈局。所選的預設佈局將儲存到目前使用者帳戶。

儀表板上的資訊將根據佈局設定中設定的排程進行更新。如有必要，您可以強制更新資料。

為了方便地在儀表板上顯示訊息，您可以啟用TV模式。此模式可讓您以全螢幕模式以全高清解析度檢視儀表板。在TV模式下，您也可以為選定的版面設定投影片顯示。

建立儀表板佈局

若要建立佈局：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 打開視窗右上角的下拉清單，然後選擇**建立佈局**。

   新建佈局視窗將開啟。
3. 在**租用戶**下拉清單中，選擇將擁有已建立佈局的租用戶，其資料將用於填充佈局的小工具。

   如果您要建立通用佈局（步驟8），則此下拉清單中的租用戶選擇無關緊要。
4. 在**時間段**下拉清單中，選擇需要分析的時間段：
   - **1小時**
   - **1天**（預設選擇此值）
   - **7天**
   - **30天**
   - **指定期間**：取得所選期間的分析資料。選取此選項時，系統會顯示日曆，您可使用該日曆設定期間。

     期間的上限不包含在其定義的時間片段中。換句話說，要接收24小時期間的分析資料，您應該將期間設定為第1天00:00:00 – 第2天00:00:00，而不是第1天00:00:00 – 第1天23:59:59。
5. 在**重新整理間隔**下拉清單中，選擇佈局小工具中資料的更新頻率：
   - **1分鐘**
   - **5分鐘**
   - **15分鐘**
   - **1小時**（預設選擇此值）。
   - **24小時**
6. 在**新增小工具**下拉清單中，選擇所需的小工具並配置其設定。

   您可以為佈局新增多個小工具。

   您也可以在視窗中拖曳小工具，並使用將滑鼠游標停留在小工具上時出現的對角線按鈕 (⤡) 調整其大小。

   您可以編輯或刪除新增至佈局的小工具。為此，請點擊設定圖示 (⚙)，然後選擇**編輯**以變更其設定，或選擇**刪除**以將其從佈局中刪除。
7. 在**佈局名稱**欄位中，輸入此佈局的唯一名稱。必須包含1至255個Unicode字元。

   自訂儀表板不能與預定義儀表板同名。

嘗試建立與預定義儀表板同名的儀表板或將自訂儀表板的名稱更改為主租用戶中預定義儀表板的名稱時，會傳回錯誤。在主租用戶以外的其他租用戶中，您可以建立或複製與預定義儀表板儀表板同名的自訂儀表板。

8. 如有需要，請點擊佈局名稱欄位右側的設定圖示 (⚙)，然後選取**通用**設定旁的核取方塊。

   佈局小工具顯示您在左側功能表的**選定租用戶**部分中所選的租用戶的資料。這意味著佈局小工具中的資料將根據您選擇的租用戶而變化，而無需編輯佈局設定。對於通用佈局，不會考慮在**租用戶**下拉清單中所選的租用戶。

   如果清除該核取方塊，佈局小工具將顯示在佈局設定的**租用戶**下拉清單中所選的租用戶的資料。如果您無法使用佈局中選定的任何租用戶，則其資料將不會顯示在佈局小工具中。

> 您無法在通用佈局中使用**活動清單**小工具。
> 只有已獲指派主管理員角色的使用者，才能建立和編輯通用佈局。所有使用者都可以檢視此類佈局。

9. 按一下**儲存**按鈕。

新佈局已建立並顯示在儀表板的**偵測和回應**頁籤上。

選擇儀表板佈局

若要選擇儀表板佈局：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 延伸視窗右上角的清單。
3. 選擇相關佈局。

所選佈局顯示在儀表板的**偵測和回應**頁籤上。

選擇儀表板佈局作為預設佈局

若要將儀表板佈局設定為預設佈局：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 延伸視窗右上角的清單。
3. 將滑鼠遊標停留在相關佈局上。
4. 按一下星形圖示 (☆)。

預設情況下，所選佈局顯示在儀表板的**偵測和回應**頁籤上。

編輯儀表板佈局

若要編輯儀表板佈局：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。
2. 延伸視窗右上角的清單。
3. 將滑鼠遊標停留在相關佈局上。
4. 按一下編輯圖示 (✎)。

   自訂佈局視窗將開啟。

5. 編輯儀表板佈局。可供編輯的設定與建立佈局時可用的設定相同。

6. 按一下**儲存**按鈕。

儀表板佈局在**偵測和回應**頁籤上進行編輯和顯示。

如果在編輯佈局設定時將其刪除或指派給其他租用戶，則按一下**儲存**時會顯示錯誤。佈局將不儲存。重新整理Kaspersky Next XDR Expert介面頁面以在下拉清單中查看可用佈局的清單。

刪除儀表板佈局

若要刪除佈局：

1. 在主功能表中，轉至**監控→控制板**，然後選擇**偵測和回應**頁籤。

2. 延伸視窗右上角的清單。

3. 將滑鼠遊標停留在相關佈局上。

4. 點選刪除圖示 ( ) 並確認此操作。

佈局隨即刪除。

啟用和禁用TV模式

建議建立一個單獨的使用者，並賦予其在TV模式下顯示分析資料所需的最低權限。

若要啟用TV模式：

1. 在KUMA主控台中，選擇**儀表板**部分。

2. 點選右上角的按鈕。
設定視窗隨即開啟。

3. 將**TV模式**切換開關移至**啟用**位置。

4. 若要設定佈局的投影片顯示，請執行下列操作：

   a. 將**投影片**切換開關移至**啟用**位置。

   b. 在**逾時**欄位中，指示切換佈局前等待的秒數。

   c. 在**佇列**下拉清單中，選擇要檢視的佈局。如果未選擇任何佈局，投影片模式將逐一顯示使用者可用的所有佈局。

   d. 如有必要，請按一下按鈕並拖放佈局，以變更佈局的顯示順序。

5. 按一下**儲存**按鈕。

TV模式將啟用。若要恢復使用KUMA主控台，請停用TV模式。

若要停用TV模式：

1. 在KUMA主控台中，選擇**儀表板**部分。
2. 點選右上角的⚙按鈕。
   設定視窗隨即開啟。
3. 將**TV模式**切換開關移至**停用**位置。
4. 按一下**儲存**按鈕。

TV模式將被停用。螢幕左側顯示一個窗格，其中包含KUMA主控台的各個部分。

當為投影片更改選定的佈局時，這些變更將自動套用至活動投影片會話。

預先設定的儀表板佈局

Kaspersky Next XDR Expert包括一組預定義佈局，其中包含以下小部件：

- **警示概覽**佈局（警示概覽）：
  - 活動警示 – 尚未關閉的警示數量。
  - 未指派的警示 – 沒有受讓人的警示數量。
  - 最新警示 – 包含佈局中選定租用戶的最近10個未關閉警示資訊的表格。
  - 警示分佈 – 為小工具設定的時間段內建立的警示數量。
  - 依優先順序分類的警示 – 依優先順序分組的未關閉警示數量。
  - 依使用者分類的警示 – 狀態為**調查中**的警示數量。依帳戶名稱分組。
  - 按狀態分類的警示 – 按狀態分組的警報數量。
  - 依群組分類的警示 – 依使用者群組分類的警示數量。
  - 警示中受影響的使用者 - 與未關閉警示關聯的使用者。
  - 受影響資產是一個表格，包含資產、其重要性等級，以及與其關聯的未關閉警示數量等資訊。資產的重要性等級會根據該資產所屬的類別計算，包括直至階層結構根節點的所有父類別。
  - 受影響資產類別 — 圖表顯示未關閉警示和事件中指定的資產類別數量。對於警示或事件中引用的每個資產，其重要性等級是基於資產所屬類別計算，包括層級結構根節點之前的所有父類別。
  - 依警示數分類的事件來源 - 按產生警示的事件來源分組的未關閉警示數量。

    此小工具最多顯示10個事件來源。

  - 依規則分類的警示 - 按關聯規則分組的未關閉警報數。

未關閉警示是指具有下列狀態之一的警示：**新增**、**調查中**、在**在事件中**。

- **事件概覽**佈局（事件概覽）：
  - 活動事件 - 不處於**已完成**狀態類別的事件數。
  - 未指派的事件 - 無受讓人的事件數。
  - 最新事件 - 包含佈局中選定租戶的最近10個未關閉事件的資訊表格。
  - 事件分佈 - 為小工具設定的時間段內所建立的事件數。
  - 依優先順序分類的事件 - 依優先順序分組的事件數。
  - 依使用者分類的事件 - 狀態為**進行中**的事件數。依使用者帳戶名稱分組。
  - 依狀態分類的事件 - 依狀態分組的事件數。
  - 依群組分類的事件 - 依使用者群組分類的事件數。
  - 事件中受影響的資產 — 顯示與未關閉事件關聯的資產數量的表格。該表格列出了資產及其重要性級別，該級別是根據資產所屬的類別以及直到層次結構根節點的所有父類別來計算的。
  - 事件中受影響的使用者 - 與未關閉事件關聯的使用者。
  - 事件中的受影響資產類別 - 圖表顯示與未關閉在事件中關聯的資產類別數量。對於關聯到事件的每個資產，其重要性等級是基於資產所屬類別計算，包括層級結構根節點之前的所有父類別。
  - 按租用戶分類的活躍事件 - 依租用戶分組的未關閉事件數量。

未關閉事件是指未處於**已完成**狀態類別的事件。

- **網路概覽**佈局（網路活動概覽）：
  - Netflow頂層內部IP - 資產接收的Netflow流量總量（以位元組為單位）。資料依資產的內部IP位址分組。此小工具最多顯示10個IP位址。
  - Netflow頂層外部IP - 資產接收的Netflow流量總量，以位元組為單位。資料依資產的外部IP位址分組。
  - Netflow遠端控制頂層主機 - 與存取下列連接埠之一的嘗試關聯的事件數：3389、22、135。資料依資產名稱分組。
  - 依內部連接埠分類的Netflow總位元組數 - 傳送到資產內部連接埠的位元組數。資料依連接埠號碼分組。
  - 依事件數劃分的頂層日誌來源 - 收到事件數最多的前10個來源。
- **NGFW彙總儀表板**佈局：
  - NGFW。防火牆會話和操作 - 已觸發並設定了日誌記錄選項的防火牆描述檔操作數。
  - NGFW。DNS安全性會話和操作 - 已觸發並設定了日誌記錄選項的DNS安全描述檔操作數。

- NGFW。Web控制會話和操作 - 已觸發並設定了日誌記錄選項的Web控制描述檔操作數。
- NGFW。IDPS會話和操作 - 已觸發並設定了日誌記錄選項的IDPS描述檔操作數。
- NGFW。防毒會話和操作 - 已觸發並設定了日誌記錄選項的防毒描述檔操作數。

- **NGFW IDPS和檔案網頁防毒**佈局：
  - NGFW。IDPS。前5種威脅名稱—IDPS描述檔偵測到的五種最常見的威脅。
  - NGFW。IDPS。前5種MITRE策略和技術——IDPS描述檔偵測到的五種最常見的MITRE ATT&CK策略和技術。
  - NGFW。IDPS。前5種威脅類型 - IDPS描述檔偵測到的五種最常見的威脅類型。
  - NGFW。IDPS。封鎖Web流量最多的前5個目標IP位址 - IDPS描述檔封鎖的Web流量最大的五個目標IP位址。
  - NGFW。IDPS。封鎖Web流量最多的前5個來源IP位址 - IDPS描述檔封鎖的Web流量最大的五個來源IP位址。
  - NGFW。檔案Web防毒。前5種威脅名稱—防毒描述檔偵測到的五種最常見的威脅。
  - NGFW。檔案Web防毒。封鎖Web流量最多的前5個來源IP位址—防毒描述檔封鎖的Web流量最大的五個目標IP位址。
  - NGFW。檔案Web防毒。封鎖Web流量最多的前5個目標IP位址 - 防毒描述檔封鎖的Web流量最大的五個來源IP位址。
- **NGFW DNS安全**佈局：
  - NGFW。DNS安全。封鎖位址的前5個威脅 - 來自DNS安全描述檔封鎖的IP位址的五個最常見的威脅。
  - NGFW。DNS安全。重新導向位址的前5個威脅——來自DNS安全描述檔重新導向的IP位址的五個最常見的威脅。
  - NGFW。DNS安全。封鎖Web流量最多的前5個來源IP位址 - 被DNS安全描述檔封鎖的Web流量最大的五個來源IP位址。
  - NGFW。DNS安全。重新導向主機名前5位 - DNS安全描述檔最常重新導向的五個網域。
  - NGFW。DNS安全。封鎖Web流量最多的前5個目標IP位址 - DNS安全描述檔阻止的Web流量最大的五個目標IP位址。
  - NGFW。DNS安全。重新導向Web流量最多的前5個來源IP位址 - DNS安全描述檔最常重新導向的五個來源IP位址。
- **NGFW Web控制和URL Web防毒**佈局：
  - NGFW。URL Web 防毒。封鎖URL的前5個Web類別 - Web防毒描述檔封鎖的五個最常見的URL類別。
  - NGFW。URL Web 防毒。封鎖Web流量最多的前5個目標IP位址 - Web防毒描述檔封鎖的Web流量最大的五個目標IP位址。
  - NGFW。Web控制警告Web流量最多的前5個網站類別 - Web控制描述檔最常顯示警告的五類網站。

- NGFW。Web控制封鎖網路流量最多的前5類網站——網路防毒描述檔封鎖的網路流量最大的五類網站。
- NGFW。Web控制警告網路流量最多的前5個目標IP位址 - Web控製描述檔中顯示警告最頻繁的五個目標IP位址。
- NGFW。Web控制封鎖的網路流量最多的前5個目標IP位址 - Web控制描述檔封鎖的網路流量最大的五個目標IP位址。
- NGFW。Web控制封鎖位址的前5個Web控制類別來源 - 最常取得封鎖URL類別的五個來源。
- NGFW。Web控制重新導向位址的前5個Web控制類別來源 - 最常取得重新導向URL類別的五個來源。

- **NGFW防火牆**佈局：
  - NGFW。依會話數排名的前5個應用程式服務—依會話數排名的前5個應用程式服務。
  - NGFW。依流量（MB）排名的前5個應用程式服務—依網路流量（MB）排名的前5個應用程式服務。
  - NGFW。依會話數排名的前5個應用程式協定 - 依會話數排名的前5個應用程式協定。
  - NGFW。依流量（MB）排名的前5個應用程式協定 - 按網路流量（MB）排名的前5個應用程式協定。
  - NGFW。依會話數排名的前5個用戶端應用程式 - 按會話數排名的前5個用戶端應用程式。
  - NGFW。依流量（MB）排名前五的用戶端應用程式 - 按網路流量（MB）排名前五的用戶端應用程式。
  - NGFW。依流量（MB）排名前五名的來源IP - 網路流量（MB）最大的五個來源IP位址。
  - NGFW。依流量（MB）排名前五名的目標IP - 網路流量（MB）最大的五個目標IP位址。
  - NGFW。依會話數排名前五的網站 - 會話數最多的五個網站。
  - NGFW。依流量（MB）排名前5名的網站—網路流量（MB）最大的五個網站。

預定義佈局的預設重新整理周期為**從不**。您可以根據需要編輯這些佈局。

關於“僅儀表板”模式

您可以為不管理網路但希望在卡巴斯基安全管理中心中檢視網路防護統計資訊的員工（例如，高級管理員）設定僅儀表板模式。當使用者啟用此模式時，只會向使用者顯示帶有一組預定義小工具的儀表板。因此，他或她可以監控小工具中指定的統計資訊，例如，所有受管理裝置的防護狀態、最近偵測到的威脅數量或網路中最常見的威脅清單。

當使用者在僅儀表板模式下工作時，將套用以下限制：

- 主功能表不向使用者顯示，因此他或她無法變更網路防護設定。
- 使用者不能用小工具執行任何操作，例如，新增或隱藏它們。因此，您需要將使用者所需的所有小工具都放在儀表板上並進行配置，例如，設定計數物件的規則或指定時間間隔。

您不能將僅儀表板模式分配給自己。如果要在此模式下工作，請聯絡系統管理員、受管理服務提供商 (MSP) 或在**一般功能：使用者權限**功能區域中具有**修改物件 ACL** 權限的使用者。

配置“僅儀表板”模式

在開始配置僅儀表板模式之前，請確保滿足以下先決條件：

- 您在**一般功能：使用者權限**功能區域中有**修改物件 ACL** 權限。如果您沒有此權限，則用於配置模式的標籤將缺失。
- 使用者在「**一般功能：基本功能**」功能區域中有**讀取**權限。

如果在您的網路中安排了管理伺服器的層次結構，為了配置僅儀表板模式，請轉到伺服器，其中使用者帳戶可在**使用者 → 使用者和角色** 部分的**使用者和群組**頁簽中使用。它可以是主伺服器或實體從屬伺服器。無法在虛擬伺服器上調整模式。

若要配置僅儀表板模式：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 點擊要使用小工具調整儀表板的使用者帳戶名稱。
3. 在開啟的帳戶設定視窗中，選取**儀表板**標籤。

   在開啟的標籤上，為您和使用者顯示相同的儀表板。
4. 如果**以僅儀表板模式顯示主控台**選項已啟用，用切換按鈕停用它。

   啟用此選項後，您也無法變更儀表板。停用該選項後，您可以管理小工具。
5. 配置儀表板外觀。在**儀表盤**標籤上準備的小工具集合可供具有可自訂帳戶的使用者使用。他或她不能變更小工具的任何設定或大小，也不能從儀表板新增或刪除任何小工具。因此，為使用者調整它們，以便他或她可以檢視網路防護統計資訊。為此，在**儀表板**標籤上，您可以對小工具執行與**監控 → 控制板**區段中相同的操作：
   - 新增小工具到儀表板。
   - 隱藏使用者不需要的小工具。
   - 移動小工具到特定的順序。
   - 變更小工具的大小或外觀。
   - 變更小工具設定。
6. 轉換切換按鈕以啟用**以僅儀表板模式顯示主控台**選項。

   之後，只有儀表板可供使用者使用。他或她可以監控統計資料，但不能變更網路防護設定和儀表板外觀。由於為您顯示的儀表板與為使用者顯示的儀表板相同，您也無法變更儀表板。

   如果您保持停用該選項，則會為使用者顯示主功能表，因此他或她可以在Open Single Management Platform中執行各種操作，包括變更安全設定和小工具。
7. 完成配置僅儀表板模式後按一下**儲存**按鈕。只有在那之後，準備好的儀表板才會顯示給使用者。
8. 如果使用者想要檢視受支援的卡巴斯基應用程式的統計資訊並且需要存取權限來執行此操作，請為使用者配置權限。之後，卡巴斯基應用程式資料將在這些應用程式的小工具中顯示給使用者。

現在使用者可以在自訂帳戶下登入Open Single Management Platform並在僅儀表板模式下監控網路防護統計資訊。

管理和防護報告

本節介紹如何使用報告、管理自定義報告範本、使用報告範本產生新報告以及建立報告交付工作。

使用報告

報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

報告功能可在OSMP主控台使用，路徑為**監控—>報告**。

預設下，報告包含 30 天內的資訊。

Kaspersky Next XDR Expert 預設提供以下類別的報告：

- **防護狀態**
- **佈署**
- **更新**
- **威脅統計資訊**
- **其他**

您可以建立自訂報告範本、編輯報告範本和刪除它們。

您可以基於現有範本建立報告、匯出報告到檔案和建立報告傳送工作。

報告範本

報告範本用於指定報告所依據的條件和資料，以及報告週期。具有主管理員、租用戶管理員、二級分析師和一級分析師角色的使用者可以建立、編輯或刪除報告範本。使用報告範本產生的報告顯示在**已產生的報告**頁籤中。

報告報告位於**報告**部分的**範本**頁籤中，其中顯示了現有範本的表格。該表包含以下資訊：

- **名稱**為報告範本的名稱。
  您可以透過點按直欄標頭中的排序圖示 ⌄ 並選擇**升序**或**降序**來對報告範本進行排序。
  您也可以使用表格上方的**搜尋**欄位搜尋報表範本。

  > 搜尋報告範本時使用規則運算式。

- **租用戶**為擁有該報告範本的租用戶名稱。

- **更新時間**為資源範本上次更新的日期和時間。

  您可以透過點按直欄標頭中的排序圖示 ⌄ 並選擇**升序**或**降序**來按此直欄對表格進行排序。

- **建立者**為建立報告範本的使用者名稱。

- **描述**為關於報告範本的可選資訊。

- **標籤**用於找尋報告範本。您可以透過點按直欄標頭中的排序圖示 ⌄ 、在**搜尋**欄位中指定要搜尋的值，或使用核取方塊選擇標籤，來搜尋報告範本。

- **排程**為使用範本產生報告的頻率。若未設定報告排程，則會顯示 `disabled` 值。

- **上一份報告**為上次根據報告範本產生報告的日期和時間。

- **套件名稱**是用來處理事件的工具套件的名稱。

- **透過電子郵件傳送**表示已設定為對產生的報告發送電子郵件通知。

如有需要，您可以點按齒輪圖示來自訂直欄。

在清單中選擇報告範本後，您可以點按選單圖示⋮以開啟可用操作的下拉清單：

- **顯示依賴項**會開啟所選報表範本的依賴項圖表視窗。如有必要，您可以在該圖表中下載SVG格式的依賴項資料，並設定要套用至圖表中顯示的依賴項的篩選器。

- **檢視版本歷程記錄**會顯示報告範本的版本歷程記錄。如有必要，您可以在側邊欄中比較版本並還原到先前的版本。

- **執行報告**會產生報告。產生的報告顯示在**已產生的報告**頁籤上。

- **檢視所有已產生的報告**會顯示為所選報告範本產生的所有報告清單。如有必要，您可以將所選報告儲存為支援的格式之一，或將其刪除。

- **編輯排程**可讓您設定報告排程，並選擇要接收有關已產生報告的電子郵件通知的使用者。

您也可以在**資源 → 清單**區段中檢視您可用的報告範本清單。為此，請在**資源類型**直欄中選擇資源種類。

建立報告範本

若要建立報告範本，請執行以下操作：

1. 在主功能表中，轉至 **監控 → 報告**。

2. 點擊**新增**。

   程式將啟動"新報告範本精靈"。使用**下一步**按鈕進行精靈。

3. 輸入報告名稱並選擇報告類型。

4. 在精靈的**範圍**步驟，選取根據此報告範本，其資料會顯示在報告中的用戶端裝置集（管理群組、裝置分類、選取的裝置，或所有網路裝置）。

5. 在精靈的**報告週期**步驟，指定報告期間。可用值：

   - 在兩個指定日期之間
   - 從指定日期到報告建立日期
   - 從報告建立日期減去指定天數

   該頁對一些報告可能不顯示。

6. 點擊**確定**以關閉精靈。

7. 執行以下操作之一：

   - 點擊**儲存和執行**按鈕以儲存新報告範本並據此執行報告。
     報告範本被儲存。報告被生成。
   - 點擊**儲存**按鈕以儲存新報告範本精靈。
     報告範本被儲存。

您可以使用新範本來生成和檢視報告。

檢視和編輯報告範本內容

您可以檢視和編輯報告範本的基本內容，例如，報告範本名稱或顯示在報告中的欄位。

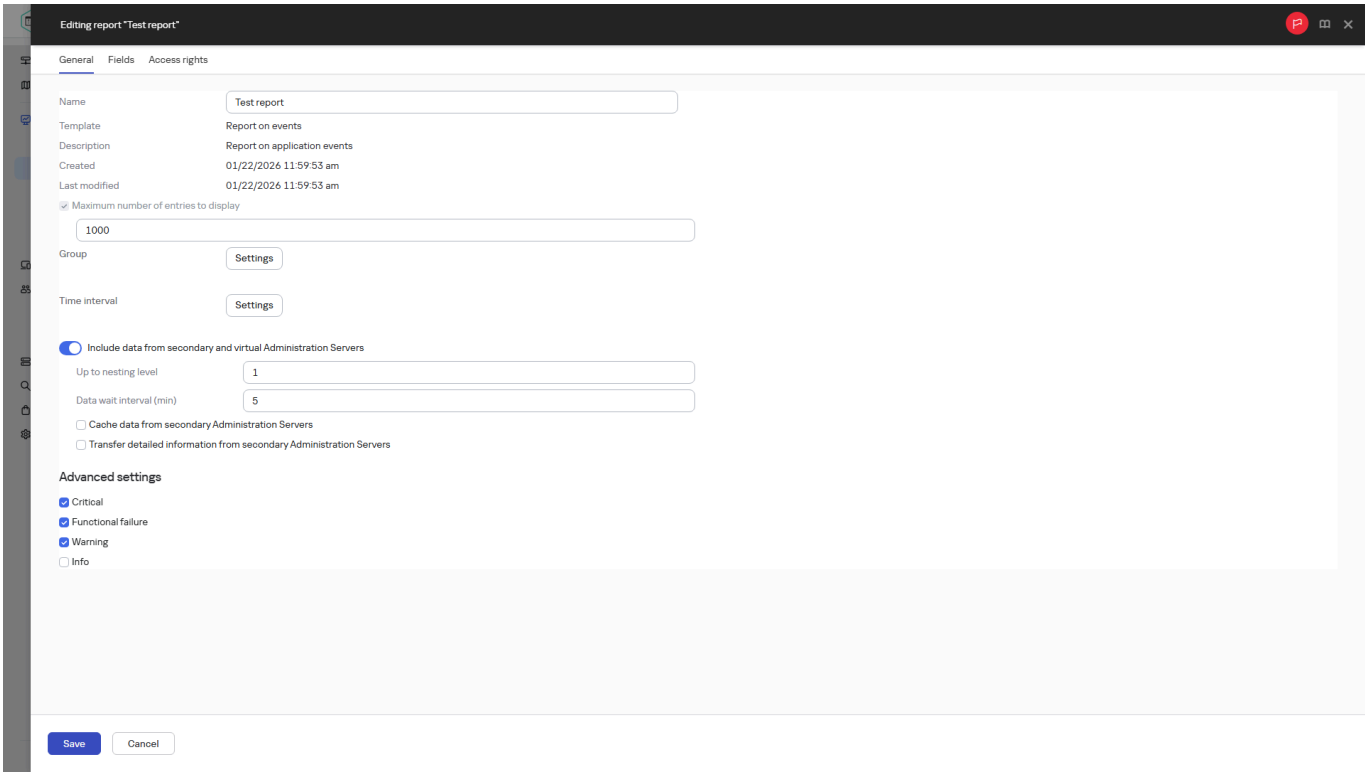
要檢視和編輯報告範本內容：

1. 在主功能表中，轉至 **監控 → 報告**。

2. 選取您要檢視並編輯其內容的報告範本旁邊的核取方塊。
   或者，您可以先產生報告，然後點擊**編輯**按鈕。

3. 點擊**開啟報告範本內容**按鈕。

編輯報告 <報告名稱>視窗會開啟，並含有所選的**一般**頁籤。



報告範本內容

4. 編輯報告範本內容：

- **一般**頁籤：
  - 報告範本名稱
  - **顯示的項目數量上限**

    如果啟用該選項，顯示在表格中的帶有詳細報告資料的項目數量不會超過指定值。請注意，此選項不會影響將報告匯出到檔案時可包含在報告中的最大事件數。

    報告項目首先根據指定在報告範本內容的**欄位 → 詳細資料欄位**區域的規則被儲存，然後僅第一個結果項目被儲存。帶有詳細報告資料的表頭展示顯示的項目數量和比對其他報告範本設定的可用項目總數。

    如果停用該選項，帶有詳細報告資料的表顯示所有可用項目。我們不建議您停用該選項。限制顯示的報告項目數量會降低資料庫管理系統 (DBMS) 負載，也會降低產生和匯出報告所需的時間。一些報告包含太多項目。如果是這樣，您可能難於閱讀和分析所有。此外，裝置在產生此類報告時可能會耗盡記憶體。這可能會導致您無法檢視報告。

    預設情況下已啟用該選項。預設值是 1000。
  - **群組**

    點擊**設定**按鈕以變更建立報告的用戶端裝置集。對於一些報告類型，按鈕可能不可用。實際設定取決於建立報告範本時指定的設定。
  - **時間間隔**

    點擊**設定**按鈕以修改報告時段。對於一些報告類型，按鈕可能不可用。可用值：
    - 在兩個指定日期之間
    - 從指定日期到報告建立日期
    - 從報告建立日期減去指定天數

- **包含來自從屬管理伺服器和虛擬管理伺服器的資料**

  如果啟用該選項，報告包含屬於建立範本的管理伺服器的從屬和虛擬管理伺服器的資訊。

  如果您要僅從目前管理伺服器檢視資料，停用該選項。

  預設情況下已啟用該選項。

- **最大嵌套層級**

  報告包含位於目前管理伺服器下小於或等於指定巢狀等級的從屬和虛擬管理伺服器的資料。

  預設值是1。如果您必須從樹中位於低等級的從屬管理伺服器接收資訊，您可能要變更該值。

- **資料等待間隔（分鐘）**

  在產生報告之前，建立報告範本的管理伺服器等待從屬管理伺服器的資料指定分鐘數。如果在該時間段後未從從屬管理伺服器接收到資料，報告依然執行。除了實際資料，報告也會顯示從快取接收的資料（如果**快取來自從屬管理伺服器的資料**選項已啟用），否則為 **N/A**（不可用）。

  預設值是5分鐘。

- **快取來自從屬管理伺服器的資料**

  從屬管理伺服器定期傳輸資料到建立報告範本的管理伺服器。傳輸的資料儲存在快取。

  如果在產生報告時目前管理伺服器無法從從屬管理伺服器接收資料，報告顯示從快取接收的資料。資料傳輸到快取的日期也被顯示。

  啟用該選項允許您檢視從屬管理伺服器資訊，即便即時資料無法被獲取。然而，所顯示資料可能過期。

  預設情況下已停用該選項。

- **快取更新頻率（小時）**

  從屬管理伺服器會在一定間隔時間傳輸資料到建立報告範本的管理伺服器。您可以以小時為單位指定此期間。如果指定值是 0 小時，資料僅會在產生報告時被傳輸。

  預設值是 0。

- **從從屬管理伺服器傳輸詳細資訊**

  在產生的報告中，帶有詳細報告資料的表格包含建立報告範本的管理伺服器的從屬管理伺服器的資料。

  啟用該選項會減慢報告產生並增加管理伺服器之間的流量。然而，您可以在一個報告中檢視所有資料。

  除了啟用該選項，您可能想分析詳細報告資料以偵測故障從屬管理伺服器，然後僅為該故障管理伺服器產生相同報告。

  預設情況下已停用該選項。

- **欄位**頁籤

  選取您要在報告中顯示的欄位。使用 **向上移動** 和 **向下移動** 按鈕變更欄位的顯示順序。使用**新增**按鈕或**編輯** 按鈕指定報告中的資訊是否必須根據每個欄位排序或篩選。

  在**詳細欄位篩選器**區段，您也可以點擊**轉換篩選器**按鈕以開始使用延伸的篩選格式。此格式使您可以使用邏輯 OR 運算子來組合在各個欄位中指定的篩選條件。點擊該按鈕後，會開啟 **轉換篩選器** 面板。點擊 **轉換篩選器** 按鈕以確認轉換。現在，您可以使用邏輯 OR 運算子從套用的 **詳細資料欄位** 區段定義轉換篩選條件。

  將報告轉換為支援複雜篩選條件的格式將使該報告與卡巴斯基安全管理中心的早期版本（11 和更早版本）不相容。另外，轉換後的報告將不包含來自執行此類不相容版本的從屬管理伺服器的任何資料。

5. 點擊**儲存**以儲存變更。

6. 關閉**編輯報告<報告名稱>**視窗。

更新的報告範本顯示在報告範本清單。

刪除報告範本

要刪除一個或幾個報告範本：

1. 在主功能表中，轉至 **監控 → 報告**。

2. 選取您要刪除的報告範本旁邊的核取方塊。

3. 接著，點擊**刪除**按鈕。

4. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

所選報告範本被刪除。如果這些報告範本被包含在報告傳送工作中，它們也被從工作刪除。

通用報告範本

在KUMA中，如果報告範本是在共用租用戶中建立的，則該範本被視為通用範本。在其他租用戶中建立的報告範本為非通用範本。

若要管理通用報告範本，使用者需要以下角色：

- 建立、管理或刪除報告範本需要「管理共用資源」角色。此角色權限授予對所有共用資源的存取權限。

  如果使用者的角色涉及管理CII資源，則任何具有「管理共用資源」角色的使用者都可以設定CII屬性。

- 「讀取共用資源」角色允許檢視通用報告範本清單。擁有此類權限後，使用者擁有所有共用資源的讀取權限。

通用報告範本中的小工具會根據以下規則顯示：

- 根據使用者對租用戶的存取權限、全域租用戶篩選器以及報告範本或小工具的設定，顯示租用戶的小工具資料。

- 您可以點選**更新預覽**按鈕，在管理報告範本設定時檢視小工具資料。

- 根據使用者的空間設定從資料庫接收事件小部件資料。如果在產生報告時，發現使用者沒有權限存取一個或多個租用戶的空間，KUMA將產生空白報告，並顯示一則訊息，指出由於缺乏對相關空間的存取權限，無法提供其他結果。

- 報告中的小工具資料可以包含或排除關鍵資訊基礎設施（CII）。若要存取包含CII資料的報告，使用者必須具有「與CII互動」角色。

- 活動清單和快顯表單小工具的限制適用於通用報告。

匯出報告到檔案

您可以將一份或多份報告儲存為 XML、HTML 或 PDF。Open Single Management Platform允許您同時將最多10份報告匯出為指定格式的檔案。

僅當您連接到OSMP主控台中的從屬管理伺服器時，PDF格式才可用。

要匯出報告到檔案：

1. 在主功能表中，轉至 **監控 → 報告**。
2. 選擇您要匯出的報告。

   如果您選擇超過 10 個報告，**匯出報告**按鈕將被停用。
3. 點擊**匯出報告**按鈕。
4. 在開啟的視窗中，指定以下匯出參數：

   - **檔案名稱**。

     如果您選擇匯出一份報告，請指定報告檔案名稱。

     如果您選擇多個報告，報告檔案名稱將與所選報告模板的名稱一致。

   - **項目數量上限**。

     指定報告檔案中包含的最大項目數。預設值是 10,000。

     您可以匯出包含無限數量項目的報告。請注意，如果您的報告包含大量項目，則產生和匯出報告所需的時間會增加。

   - **檔案格式**。

     選取報告檔案格式：XML、HTML 或 PDF。如果匯出多個報告，所有選定的報告都會以指定的格式儲存為單獨檔案。

     僅當您連接到OSMP主控台中的從屬管理伺服器時，PDF格式才可用。

     需要使用 wkhtmltopdf 工具將報告轉換為 PDF。當您選擇PDF選項時，從屬管理伺服器會檢查裝置上是否已安裝wkhtmltopdf工具。如果未安裝該工具，應用程式會顯示一條訊息，說明必須在管理伺服器裝置上安裝該工具。手動安裝該工具，然後繼續下一步。
5. 點擊**匯出報告**按鈕。

報告以指定格式儲存到檔案中。

生成和瀏覽報告

要建立和瀏覽報告，請執行以下操作：

1. 在主功能表中，轉至 **監控 → 報告**。
2. 點擊要用來建立報告的報告範本名稱。

   會產生並顯示使用所選範本的報告。

報告資料根據為管理伺服器設定的當地語係化顯示。

在產生的報告中，某些字體可能無法正確顯示在圖表上。要解決此問題，請安裝 fontconfig 庫。另外，請檢查作業系統中是否安裝了與您的作業系統區域設定相對應的字體。

此報告將顯示下列資料：

- 在**概要**頁籤：
  - 報告名稱和類型、簡要說明和報告時間區段，以及該報告為哪個裝置群組產生的相關資訊。
  - 圖表顯示最有代表性的報告資料。
  - 帶有計算好的報告指示器的加固表格。
- 在**詳細資訊**頁籤會顯示包含詳細報告資料的表格。

建立報告傳送工作

您可以建立傳送所選報告的工作。

要建立報告傳送工作：

1. 在主功能表中，轉至 **監控 → 報告**。
2. 選取您要建立報告傳送工作之報告範本旁邊的核取方塊。
3. 點擊**建立交付工作**按鈕。
   新工作精靈啟動。使用下一步按鈕進行精靈。
4. 在精靈的**新工作設定**步驟中，輸入工作名稱。
   預設名稱是「**傳送報告」。**如果具有此名稱的工作已存在，則序號 (<N>) 會新增到工作名稱。

5. 在精靈的**報告組態**步驟中，指定以下設定：

   a. 要使用工作傳送的報告範本。

   b. 報告格式：HTML、XLS 或 PDF。

      需要使用 wkhtmltopdf 工具將報告轉換為 PDF。當您選擇 PDF 選項時，管理伺服器會檢查裝置上是否安裝了 wkhtmltopdf 工具。如果未安裝該工具，應用程式會顯示一條訊息，說明必須在管理伺服器裝置上安裝該工具。手動安裝該工具，然後繼續下一步。

   c. 報告是否使用電子郵件連同郵件通知設定一起傳送。

      您最多可以指定 20 個電子郵件地址。若要分開電子郵件地址，請按 **Enter**。您也可以貼上以逗號分隔的電子郵件地址清單，然後按 **Enter**。

   d. 是否將報告以及相應的設定儲存到資料夾中。

      啟用 **儲存到資料夾**選項後，您必須指定該資料夾的 POSIX 路徑。如果要將報告儲存到共用資料夾，您還必須選取**指定帳戶以存取共用資料夾**核取方塊，然後指定用於存取此資料夾的使用者帳戶和密碼。

      > 如果選擇將報告儲存到共用資料夾，則必須確保可用從安裝了管理伺服器的裝置存取該資料夾。確保存取的方法和使用的工具取決於您的基礎架構。

      將報告儲存到本機資料夾時，通常不需要憑據，因為執行管理伺服器的帳戶可以存取此資料夾。如有必要，您可以在精靈的**選取要執行此工作的帳戶**步驟中指定使用者憑據。

      無論選擇哪個資料夾，如果您希望新的報告檔案覆蓋上次工作啟動時儲存在報告資料夾中的檔案，您也可以選取**"覆蓋相同類型的舊報告**核取方塊。

6. 在精靈的**設定工作排程**步驟中，選取工作啟動排程。

   可使用下方的工作排程選項：

   - **手動**

     工作不自動執行。您僅可以手動啟動。

     預設情況下已選定此選項。

   - **每 N 分鐘**

     工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

     預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

   - **每 N 小時**

     工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

     預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

   - **每 N 天**

     工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

     預設下，工作每天執行一次，從目前系統日期和時間開始。

   - **每 N 星期**

     工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

預設下，工作每星期五於目前系統時間執行一次。

- **每月**

  工作定期執行，在指定月日的指定時間。

  在缺少指定日的月份，工作在最後一天執行。

  預設下，工作在每月的第一天執行，在目前系統時間。

- **在指定日期**

  工作定期在指定月日的指定時間執行。

  預設情況下，開始時間為18:00，且未選擇當月的任何日期。

  > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

  您可以選擇一週中的多個日期。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

7. 在精靈的這個步驟中，設定其他工作排程設定：

- 在**工作排程**區域中，檢查或重新設定先前選取的排程並設定時間間隔、每月或每週的天數、設定病毒爆發條件或完成另一個工作作為啟動工作的觸發條件。如果選擇了適用的排程，也可以在此區域中指定開始時間。

- 在**其他設定**區域中，指定下方設定：

  - **執行錯過的工作**

    該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

    如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

    如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

    預設情況下已停用該選項。

  - **使用工作啟動自動隨機化延遲**

    如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

    當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

    如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  - **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

    如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

    如果該選項被停用，工作依據排程在用戶端裝置上啟動。

    預設情況下已停用該選項。預設時間間隔為一分鐘。

  - **停止工作，若執行時間超過**

    在指定時間段過後，工作被自動停止，無論它是否完成。

    如果您想要中斷或停止執行時間太長的工作，則啟用該選項。

    預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

8. 在精靈的**選取要執行此工作的帳戶**步驟中，指定用於執行工作的使用者帳戶憑證。

9. 如果您要在建立工作後修改其他工作設定，請在精靈的**完成工作建立**步驟中，啟用**建立完成時開啟工作詳情**選項。預設情況下已啟用該選項。

10. 點擊**完成**按鈕以建立工作並關閉精靈。

報告傳送工作被建立。如果啟用**建立完成時開啟工作詳情**選項，則工作設定視窗隨即開啟。

偵測和回應報告

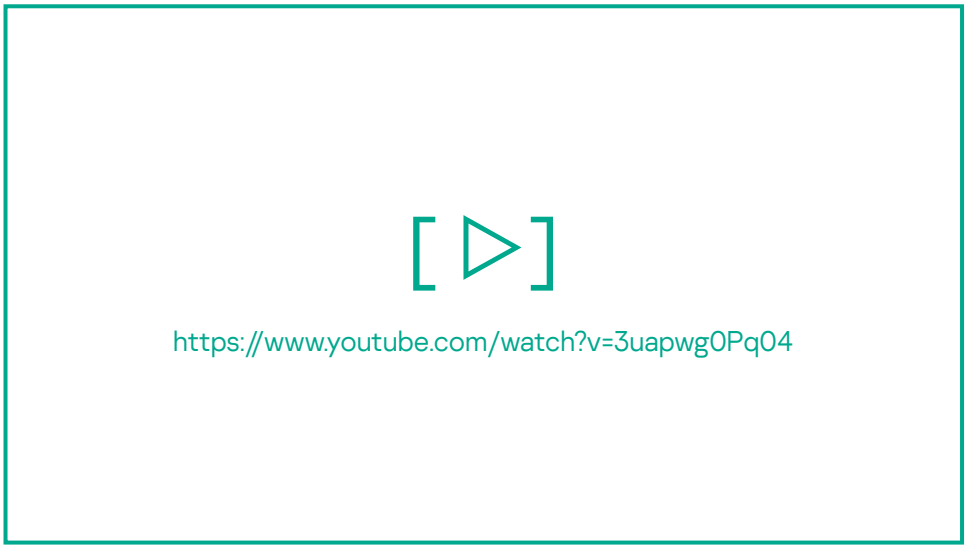
您可以在KUMA中安排產生進程和物件狀態報告。

報告使用*報告範本產生*。您可以在**範本**頁籤的**報告**部分找到報告範本。

您可以在已產生的報告頁籤的**報告**部分找到**已產生的報告**。

若要將產生的報告儲存為HTML和PDF格式，請在裝有KUMA Core的裝置上安裝所需的軟體套件。

在高可用性版本中部署KUMA時，KUMA Core伺服器的時區和使用者瀏覽器中的時間可能會有所不同。這種差異表現為依排程產生的報告中的時間與用戶可以從小工具導出的資料之間的差異。為避免這種差異，建議在設定報告產生排程時考慮使用者時區與UTC之間的差異。



報告範本

報告範本用於指定報告所依據的條件和資料，以及報告週期。具有主管理員、租用戶管理員、二級分析師和一級分析師角色的使用者可以建立、編輯或刪除報告範本。使用報告範本產生的報告顯示在**已產生的報告**頁籤中。

報告報告位於**報告**部分的**範本**頁籤中，其中顯示了現有範本的表格。該表包含以下資訊：

- **名稱**為報告範本的名稱。

  您可以透過點按直欄標頭中的排序圖示 ⌄ 並選擇**升序**或**降序**來對報告範本進行排序。

  您也可以使用表格上方的**搜尋**欄位搜尋報表範本。

  搜尋報告範本時使用規則運算式。

- **租用戶**為擁有該報告範本的租用戶名稱。
- **更新時間**為資源範本上次更新的日期和時間。

  您可以透過點按直欄標頭中的排序圖示 ⌄ 並選擇**升序**或**降序**來按此直欄對表格進行排序。

- **建立者**為建立報告範本的使用者名稱。
- **描述**為關於報告範本的可選資訊。
- **標籤**用於找尋報告範本。您可以透過點按直欄標頭中的排序圖示 ⌄ 、在**搜尋**欄位中指定要搜尋的值，或使用核取方塊選擇標籤，來搜尋報告範本。

- **排程**為使用範本產生報告的頻率。若未設定報告排程，則會顯示 `disabled` 值。
- **上一份報告**為上次根據報告範本產生報告的日期和時間。
- **套件名稱**是用來處理事件的工具套件的名稱。
- **透過電子郵件傳送**表示已設定為對產生的報告發送電子郵件通知。

如有需要，您可以點按齒輪圖示來自訂直欄。

在清單中選擇報告範本後，您可以點按選單圖示以開啟可用操作的下拉清單：

- **顯示依賴項**會開啟所選報表範本的依賴項圖表視窗。如有必要，您可以在該圖表中下載SVG格式的依賴項資料，並設定要套用至圖表中顯示的依賴項的篩選器。
- **檢視版本歷程記錄**會顯示報告範本的版本歷程記錄。如有必要，您可以在側邊欄中比較版本並還原到先前的版本。
- **執行報告**會產生報告。產生的報告顯示在**已產生的報告**頁籤上。
- **檢視所有已產生的報告**會顯示為所選報告範本產生的所有報告清單。如有必要，您可以將所選報告儲存為支援的格式之一，或將其刪除。
- **編輯排程**可讓您設定報告排程，並選擇要接收有關已產生報告的電子郵件通知的使用者。

您也可以在**資源 → 清單**區段中檢視您可用的報告範本清單。為此，請在**資源種類**直欄中選擇**報告範本**。

建立報告範本

若要建立報告範本，請執行以下操作：

1. 開啟OSMP主控台，然後轉至下列部分之一：
   - **報告 → 範本**
   - **資源 → 清單**
     如果您選擇了此部分，為了便於檢視物件，您可以在表格的**資源類型**直欄中選擇資源種類。
2. 根據所選部分，執行下列其中一項操作：
   - 在**報告 → 範本**部分中，按一下報告範本表格上方的**新建**按鈕。
   - 在**資源→清單**部分，按一下**新建**按鈕，然後在資源清單中選擇**報告範本**。
3. 這將開啟一個視窗；在該視窗中，輸入報告範本的唯一名稱。此名稱必須包含1到128個Unicode字元。
   在主租用戶中，自訂報告範本不能與預設報告範本同名。
   在主租用戶中，如果您嘗試建立與預定義報告範本相同名稱的報告範本，或將預定義報告範本的名稱分配給自訂報告模板，則會傳回錯誤。在主租用戶以外的其他租用戶中，您可以建立或複製與預定義報告範本同名的自訂報告範本。我們建議為自訂報告範本使用自訂名稱。
4. 在**範本租用戶**下拉清單中，選擇將擁有正在建立之報告範本的租用戶。
5. 在**從租用戶收集資料**下拉清單中，選擇一個或多個租用戶。系統會根據所選租用戶的資料產生報告。

6. 如有必要，請在**期間**下拉清單中選擇要取得分析資料的期間，方法如下：

   - 如果您想要指定確切日期，請在左側行事曆中選擇期間的開始日期和結束日期，然後按一下**套用**。

     您可以選擇包括目前日期在內的任意日期。日期和時間格式取決於瀏覽器的設定。如果**範圍起始**或**範圍結尾**欄位已有值，且您未手動編輯時間值，則當您在行事曆中選擇日期時，**範圍起始**欄位會自動填入00:00:00.000，而**範圍結尾**欄位會自動填入23:59:59.999。如果您已手動刪除**範圍起始**或**範圍結尾**欄位中的值，當您在行事曆中選擇日期時，該欄位會自動填入目前時間。在其中一個欄位中選擇值後，焦點將切換到另一個欄位。如果**範圍結尾**早於**範圍起始**，系統會自動將這個較早的值填入**範圍起始**欄位。

   - 如果您想要指定相對期間，請在右側的**相對期間**清單中選擇一個可用期間。

     期間是相對於當前時間計算的。

   - 如果您想要指定自訂期間，請編輯**範圍起始**和**範圍結尾**欄位的值。

     您可以以**DD.MM.YYYY HH:mm:ss.SSS**格式（用於俄文在地化）和**YYYY-MM-DD HH:mm:ss.SSS**格式（用於英文在地化）輸入確切的日期和時間，或者以公式的形式輸入相對期間。您也可以根據需要結合使用這些方法。如果在輸入確切日期時未指定毫秒，則會自動替換為000。如果您已編輯**範圍起始**或**範圍結尾**欄位中的時間，在行事曆中選擇日期時不會變更時間部分。

     在相對期間公式中，您可以使用當前日期和時間的**now**參數以及間隔參數化語言：**+**（僅在**範圍結尾**欄位中）、**-**、**/**（四捨五入至最接近的），以及時間單位：**yMM**（月）、**w**（周）、**d**（天）、**h**（小時）、**m**（分鐘）、**s**（秒）。例如，您可以指定**now-5d**期間以取得過去五天的資料，或指定**now/w**期間以取得從本週第一天（UTC時間00:00:00:00）到當前時間（**now**）的資料。

     > **範圍起始**欄位為必填項，其值不能超過**範圍結尾**欄位的值，且不能早於1970年1月1日（如果指定確切日期或相對期間）。**範圍結尾**不能早於**範圍起始**。如果未在**範圍結尾**欄位中指定值，則自動指定**now**。

   預設情況下，選擇**1天（now-1d）**相對期間。期間的起始和結束時間均包含在內。例如，對於**今天**時間範圍，事件會顯示從當天開始時間（00:00:00:000）到目前時間（**now**）（含）為止；對於**昨天**期間，事件會顯示從前一天的開始時間（00:00:00:000）到當天的00:00:00:000為止。

   KUMA以UTC格式儲存時間值，但在使用者介面中，時間會轉換為瀏覽器的時區。這與相對時間段相關：**今天**、**昨天**、**本週**和**本月**。例如，如果瀏覽器中的時區是UTC+3，並且您選擇**今天**作為資料顯示期間，則將顯示從03:00:00.000到現在的資料，而不是從00:00:00.000到現在。

   如果您想在選擇相對資料顯示期間（如**今天**、**昨天**、**本週**或**本月**）時考慮您的時區，則需要透過新增或減去正確的小時數來手動在**範圍起始**和**範圍結尾**（如果指定了現在以外的值）中新增時間偏移。例如，如果您的瀏覽器時區是UTC+3，並且您想要顯示**昨天**的資料，您需要將**範圍起始**變更為**now-1d/d-3h**，並將**結束日期**更改為**now/d-3h**。如果您想要顯示**今天**期間的資料，只需將**範圍起始**欄位中的值變更為**now/d-3h**。

   > 如果您需要截至昨天23:59:59:999 UTC的結果，可以使用帶有時間戳篩選器的SQL查詢，或指定確切的日期和時間。

7. 根據需要，在**保留期間**欄位中，指定要儲存根據此範本生成的報告的多長時間。

   預設值是3個月。

8. 如有必要，請從**標籤**下拉清單中選擇報告範本的標籤。

9. 如有必要，請新增報告範本的描述。

10. 使用**CII狀態**切換開關可啟用顯示與關鍵資訊基礎設施（CII）相關的資產、警示和事件資訊。啟用後，只有在設定中選取**存取CII設施**核取方塊的使用者才能檢視計算資料包含CII資訊的報告。

    如果此切換開關已停用，即使使用者擁有CII設施的存取權限，報告的小工具也不會顯示與關鍵資訊基礎設施（CII）相關的資產、警示和事件資訊。

11. 按一下**儲存**按鈕。

12. 這將開啟一個視窗；在該視窗中，您可以點擊**上傳檔案**連結來更改報告範本的徽標。在檔案選擇視窗中，選擇徽標的圖像檔案。圖像格式必須為 JPEG、PNG 或 GIF，且大小不得超過 3 MB。

    新增的標識將顯示在報告中，而不是KUMA標識。

13. 點擊**新增小工具**按鈕並選擇一個小工具。這將開啟一個視窗；在該視窗中，設定所選小工具。

14. 您可以新增多個小工具。您可以透過小工具左上角的手把圖示（ ⠿ ）在視窗中拖動小工具。如果您需要調整小工具的大小，您可以使用將滑鼠懸停在小工具右下角時顯示的調整大小圖示（ ⤡ ）。

15. 以下限制適用於**圓餅圖**、**長條圖**、**折線圖**、**計數器**和**日期直方圖**圖表類型的小工具：

    - 在`SELECT`查詢中，您可以使用`String`、`Number`和`Float`類型的擴充事件結構欄位。
    - 在`WHERE`查詢中，您可以使用所有類型的擴充事件結構欄位（`String`、`Number`、`Float`、`Array of strings`、`Array of numbers`和`Array of floats`）。

    對於`Table`圖表類型的小工具，在`SELECT`查詢中，您可以使用所有類型的擴充事件結構欄位（`String`、`Number`、`Float`、`Array of strings`、`Array of numbers`和`Array of floats`）。

16. 透過點擊小工具右上角的選單⋮圖示，您可以執行以下操作：

    - 管理小工具設定
    - 建立小工具副本
    - 移除小工具
    - 以CSV格式下載小工具資料

17. 點擊**建立**按鈕。

    新的報表範本會顯示在OSMP主控台的**報告→範本**和**資源→清單**頁籤中。您可以手動執行此報告。若要自動產生報告，則必須為此設定排程。

設定報告排程

若要設定報告排程：

1. 開啟KUMA網頁介面，選擇**報告→範本**。
2. 在包含報告範本清單的表格中，選擇一個報告範本並點擊選單圖示⋮。
3. 在下拉式清單中，選取**編輯排程**。

   這將開啟**編輯排程**視窗。

4. 如果希望定期產生報告：

   a. 啟用**依排程傳送報告**切換開關。

   b. 在**產生頻率**下，指定報告的產生頻率。

      您可以依天、週、月或年指定產生報告的頻率。依據選定的期間，您應該指定報告產生的時間、星期幾、月份或日期。

c. 在**時間**欄位中，輸入必須產生報告的時間。

d. 在**時區**下拉清單中，選擇報告產生時間的時區。

5. 在**通知設定**下，指定以下內容：

a. 在**通知範本**下拉清單中，選擇要依排程傳送給使用者的通知表單。

b. 在**傳送至**設定群組中，按一下**新增**。

c. 這將開啟一個視窗；在該視窗中，新增要接收報告的使用者群組並選擇格式。為此：

- 在**電子郵件**下拉清單中，選擇報告收件者的電子郵件地址。
- 在**格式**下拉清單中，選擇報告的格式：可提供以下格式：PDF、HTML、CSV、分割CSV、Excel。

您可以點選**新增群組**按鈕新增多個報告接收者群組。

每次手動產生報告時，報告都會傳送到指定的電子郵件地址，或者KUMA會依排程自動產生報告。

> 若要透過電子郵件傳送產生的報告，則需要設定SMTP連線。

如果電子郵件報告的收件人是KUMA使用者，他們可以透過點擊電子郵件中的連結來下載或檢視報告。如果收件人不是KUMA使用者，他們可以點擊連結，但無法登入 KUMA，因此只能查看附件。

我們建議透過點擊網頁介面中的連結來查看HTML報告，因為在某些螢幕解析度下，附件中的HTML報告可能無法正確顯示。

如果您傳送了沒有附件的電子郵件，收件人只能透過連結獲取報告，並且只有在他們可以在KUMA中授權的情況下，對角色或租用戶沒有限制。

d. 按一下**新增**按鈕。

6. 按一下**儲存**按鈕。

報告排程已設定。

編輯報告範本

若要編輯報告範本：

1. 開啟KUMA網頁介面，並轉至以下部分之一：

- **報告 → 範本**
- **資源 → 清單**

如果您選擇了此部分，為了便於檢視物件，您可以在表格的**資源類型**直欄中選擇資源種類。

2. 根據所選部分，執行下列其中一項操作：

- 在**報告 → 範本**部分中，點按報告範本表格中的報告範本名稱。
- 在**資源→清單**部分中，點按資源清單中報告範本名稱旁邊的編輯設定圖示 ()。

這將打開**編輯範本**視窗。

您也可以在「報告」→「已產生的報告」頁籤中開啟此窗口，方法是選擇現有報告並點選「編輯範本」按鈕。

> 您也可以在**報告 → 已產生的報告**頁籤中開啟此視窗，方法是選擇現有報告並點按**編輯報告**按鈕。

3. 做必要的變更：

   - 變更報告範本的名稱。
   - 修改為報告傳送資料的租用戶清單。
   - 點擊**設定**按鈕可變更取得分析資料的期間、保留期限、標籤和報告範本描述。
   - 點選**新增小工具**按鈕可新增小工具至報告範本。
   - 點擊選單圖示（⋮）檢視此範本產生的報告清單，或刪除報告範本。
   - 透過點擊**上傳檔案**連結並上傳新徽標來更改報告徽標。如果範本已包含標識，則必須先刪除。
   - 透過拖曳來更改小工具的位置。
   - 使用將滑鼠游標懸停在小工具上時顯示的調整大小（⤡）圖示來調整小工具大小。
   - 點擊小工具上的選單圖示（⋮）來管理小工具設定、複製小工具、刪除小工具或以 CSV 格式下載小工具資料。

4. 按一下**儲存**按鈕。

報表範本隨即修改和顯示在KUMA網頁介面的**報告→範本**和**資源→清單**頁籤中。

複製報告範本

若要建立報告範本的副本：

1. 開啟KUMA網頁介面，並轉至以下部分之一：

   - **報告 → 範本**
   - **資源 → 清單**

     如果您選擇了此部分，為了便於檢視物件，您可以在表格的**資源種類**直欄中選擇**報告範本**。

2. 在表格中，選擇一個報告範本，然後按一下表格上方的**複製**按鈕。
3. 這將開啟一個視窗；在該視窗中，輸入報告範本的名稱。複製報告範本時，報告名稱會註明它是副本。
4. 在**範本租用戶**下拉清單中，選擇將擁有所建立報告範本的租用戶。
5. 在**從租用戶收集資料**下拉清單中，選擇一個或多個租用戶，以在報告範本中顯示其資料。

6. 根據需要變更以下設定：

   - 報告產生期間。
   - 報告保留期間。
   - 報告範本的標籤。
   - 報告範本的描述。
   - 使用CII資訊產生報告資料。

7. 按一下**儲存**按鈕。

報告範本副本隨即建立，並顯示在KUMA網頁介面的**報告→範本**和**資源→清單**頁籤中。

刪除報告範本

若要刪除報告範本：

1. 開啟KUMA網頁介面，並轉至以下部分之一：

   - **報告 → 範本**
   - **資源 → 清單**
     如果您選擇了此部分，為了便於檢視物件，您可以在表格的**資源種類**直欄中選擇**報告範本**。

2. 在報告範本表格中，選取報告範本的核取方塊，然後按一下表格上方的**刪除**按鈕。
   確認視窗隨即開啟。

3. 執行以下操作之一：

   - 如果只想刪除報告範本，請按一下**刪除**按鈕。
   - 如果您要刪除報告範本以及使用該範本產生的所有報告，請按一下**隨報告一起刪除**按鈕。

報告範本隨即被刪除。

匯出或匯入報告範本

若要匯出報告範本：

1. 開啟KUMA網頁介面，並轉至以下部分之一：

   - **報告 → 範本**
   - **資源 → 清單**
     如果您選擇了此部分，為了便於檢視物件，您可以在表格的**資源種類**直欄中選擇**報告範本**。

這將打開一個窗口，其中列出了KUMA中所有可用的報告範本。

2. 使用核取方塊選擇要匯出的報告範本。

3. 點選報告範本表格上方的**匯出**按鈕。

4. 在顯示的側邊欄中：

   a. 請輸入匯出資源檔案的密碼。該名稱必須符合以下要求：

      - 至少包含16個字元。
      - 至少包含一個小寫字母。
      - 至少包含一個大寫字母。
      - 至少包含一個數字。
      - 至少包含一個特殊字元。

   b. 在**租用戶**下拉列表中，選擇要從中匯出所選資源的租用戶。

   c. 選取核取方塊以指定要匯出的資源。
   如果選取**所有資源**核取方塊，則會匯出所選租用戶資料夾中的所有資源。

5. 按一下**匯出**按鈕。

匯出報表範本時，請考慮以下事項：

- 報告範本匯出時不包含租用戶、儲存體和空間資訊，因為這些參數是針對每個 KUMA部署單獨配置的。
- 報告範本小工具匯出時也不包含租用戶、儲存體和空間資訊。

若要匯入報告範本：

1. 開啟KUMA網頁介面，並轉至以下部分之一：

   - **報告 → 範本**
   - **資源 → 清單**
   如果您選擇了此部分，為了便於檢視物件，您可以在表格的**資源種類**直欄中選擇**報告範本**。

   這將打開一個窗口，其中列出了KUMA中所有可用的報告範本。

2. 使用核取方塊選擇要匯入的報告範本。

3. 點選資源表格上方的**匯入**按鈕。

4. 在側邊欄的**租用戶**下拉清單中，選擇要將報告範本匯入的租用戶。

5. 選擇匯入來源：**檔案**或**儲存庫**。

6. 根據所選的匯入來源，請執行下列步驟：

   a. 如果您將**檔案**選為了匯入來源，請執行下列步驟：

      - 指定匯入檔案的密碼。
      - 按一下**選取檔案**按鈕，選擇要匯入的檔案。
      - 選取要匯入的資源的核取方塊。

   b. 如果您將**儲存庫**選為了匯入來源，請在顯示的表格中選擇一個或多個儲存庫套件。

7. 點擊**匯入**按鈕。

8. 如有必要，請解決從檔案中匯入的資源與現有資源之間的衝突。

匯入報告範本時，請注意下列事項：

- 如果將報表範本匯入任何租用戶，則匯入的報表範本的租用戶將被指定為資源租用戶和資料來源租用戶。
- 匯入資源後，您需要為帶有事件的小工具指定空間，並根據需要延伸租用戶清單。

通用報告範本

在KUMA中，如果報告範本是在共用租用戶中建立的，則該範本被視為通用範本。在其他租用戶中建立的報告範本為非通用範本。

若要管理通用報告範本，使用者需要以下角色：

- 建立、管理或刪除報告範本需要「管理共用資源」角色。此角色權限授予對所有共用資源的存取權限。
  如果使用者的角色涉及管理CII資源，則任何具有「管理共用資源」角色的使用者都可以設定CII屬性。
- 「讀取共用資源」角色允許檢視通用報告範本清單。擁有此類權限後，使用者擁有所有共用資源的讀取權限。

通用報告範本中的小工具會根據以下規則顯示：

- 根據使用者對租用戶的存取權限、全域租用戶篩選器以及報告範本或小工具的設定，顯示租用戶的小工具資料。
- 您可以點選**更新預覽**按鈕，在管理報告範本設定時檢視小工具資料。
- 根據使用者的空間設定從資料庫接收事件小部件資料。如果在產生報告時，發現使用者沒有權限存取一個或多個租用戶的空間，KUMA將產生空白報告，並顯示一則訊息，指出由於缺乏對相關空間的存取權限，無法提供其他結果。
- 報告中的小工具資料可以包含或排除關鍵資訊基礎設施（CII）。若要存取包含CII資料的報告，使用者必須具有「與CII互動」角色。
- 活動清單和快顯表單小工具的限制適用於通用報告。

產生的報告

所有報告均使用報告範本產生。產生的報告可在**報告**部分的**產生的報告**頁籤中找到，並顯示在表格中，其中包含以下資訊：

- **名稱**— 報告範本的名稱。

  您可以透過點按直欄標頭中的排序圖示 ⌄並選擇**升序**或**降序**來對報告範本進行排序。

  您也可以使用表格上方的**搜尋**欄位以名稱搜尋報表範本。

- **期間** - 提取報告分析的期間。

- **上次報告** - 產生上次報告的日期和時間。

- 您可以透過點按直欄標頭中的排序圖示 ⌄並選擇**升序**或**降序**，依此直欄對表格進行排序。

- **租用戶** - 擁有報告的租用戶的名稱。

- **使用者** - 手動產生報告的使用者的名稱。如果報告是依排程產生的，則該值為空。如果報告是在KUMA 2.1以下版本中產生的，則該值為空。

如有需要，您可以點按齒輪圖示⚙來自訂直欄。

在產生的報告清單中選擇報告後，您可以：

- 建立報告。
- 開啟和檢視報告。
- 將產生的報告儲存為特定格式。可用格式：HTML、PDF、CSV、分割CSV、Excel。預設情況下，所有格式均顯示250行。PDF和HTML格式的表格行的最大數量為500。如果要在報告中輸出超過500行，請在SQL查詢中設定LIMIT參數的值，並將報告儲存為CSV格式。
- 管理報告範本的設定。
- 刪除報告。

檢視報告

若要開啟報告：

1. 開啟KUMA網頁介面，選擇**報告→產生的報告**。
2. 在報告清單中，點選已產生的報告名稱。

   將開啟新的瀏覽器視窗，其中的小工具顯示報告分析資料。如果小工具顯示有關事件、警示或活動清單的資料，則可以按一下其標頭以開啟KUMA網頁介面的相應部分，其中包含用於顯示小工具資料的活動篩選器和/或搜尋查詢。預設值已套用至小工具。

   若要檢視完整資料，請使用請求中指定的設定下載CSV格式的報告。

如果您在小工具設定中啟用了**顯示總計**開關，則小工具會顯示**總計**值；但當您以CSV或擴充CSV格式附加或上傳報告時，**總計**值不會顯示。若要顯示報告中的**總計**值，您可以使用Excel公式，或從小工具複製並貼上總計值，或使用PDF或HTML附件。

3. 如有必要，請點按**另存為**按鈕，以所選格式儲存報告。

產生報告

您可以手動產生報告，也可以設定自動產生報告的排程。

若要手動產生報告：

1. 開啟KUMA網頁介面，並轉至**報告**部分。
2. 執行以下操作之一：
   a. 在**已產生的報告**頁籤上：
      - 在報告清單中選取報告的核取方塊。
      - 點擊表格上方的**產生報告**按鈕。
   b. 在**範本**頁籤上：
      - 在報表範本清單中選取報表的核取方塊。
      - 點擊選單圖示⋮，然後從下拉清單中選擇**產生報告**。

15秒內，報告將產生並顯示在「報告」→「已產生的報告」頁籤中。

您也可以設定報告產生排程，以自動產生報告。

儲存報告

若要以所需的格式儲存報告：

1. 開啟KUMA網頁介面，選擇**報告→已產生的報告**。
2. 在已產生報告清單中，選取所需報告的核取方塊。
3. 在表格上方的**另存為**下拉式清單中，選取格式：HTML、PDF、CSV、分割 CSV、Excel。
   報告將會儲存到瀏覽器中設定的下載資料夾中。

您也可以在檢視報告時以所需的格式儲存報告。

更新報告

若要更新已產生的報告：

1. 開啟 KUMA 網頁介面，然後前往 **報告** → **已產生的報告**區段。
2. 在已產生的報告清單中，選擇一份報告。
3. 點擊表格上方的**產生報告**按鈕。
   報告會在 15 秒內更新，並可在 **報告** → **已產生的報告**區段中使用。

刪除報告

若要刪除報告：

1. 開啟KUMA網頁介面，選擇**報告→已產生的報告**。
2. 在已產生的報告清單中，選擇一份報告。
3. 點按表格上方的**刪除**按鈕。
   確認視窗隨即開啟。
4. 點擊**刪除**按鈕。
   所選報告隨即刪除。

事件和事件分類

本節提供有關事件和事件分類、Kaspersky Next XDR Expert 元件中發生的事件類型，以及管理頻繁事件封鎖的資訊。

關於 Kaspersky Next XDR Expert 中的事件

Kaspersky Next XDR Expert 可讓您接收管理伺服器和安裝在受管理裝置上的 Kaspersky 應用程式運作期間所發生事件的相關資訊。事件資訊儲存在管理伺服器資料庫。

事件類型

Kaspersky Next XDR Expert 有以下幾種類型的通知：

- 一般事件。這些事件會發生在所有受管理的 Kaspersky 應用程式中。一般事件指的像是病毒爆發。一般事件已嚴格定義語法與語意。例如，一般事件會用於報告和儀表板。
- 受管理的 Kaspersky 應用程式特定的事件。每個 Kaspersky 應用程式都擁有自己的事件集。

事件來源

您可以在應用程式政策的**事件組態**頁簽中檢視可以由應用程式生產的事件的完整清單。對於管理伺服器，您還可以在管理伺服器屬性中檢視事件清單。

事件可以由以下應用程式產生：

- Kaspersky Next XDR Expert 元件：
  - 管理伺服器
  - 網路代理
- 受管卡巴斯基應用程式

  有關卡巴斯基受管應用程式產生的事件的詳細資訊，請參閱相應應用程式的文件。

事件重要性等級

每個事件都有自己的重要等級。取決於發生的條件，一個事件可以被分配不同的重要等級。四個事件重要等級如下：

- *緊急事件*指示發生了可能導致資料遺失、作業系統異常或嚴重錯誤的嚴重問題。
- *功能失效*指示在應用程式操作中或過程執行中發生了嚴重問題、錯誤或功能異常。
- *警告*是不緊急的事件，但是也指示了今後可能發生的潛在問題。如果在事件發生後應用程式可以被還原而不遺失資料或功能，則這些事件是警告等級。
- *資訊*事件用於提示成功完成操作、應用程式的正常功能或完成了某過程。

每個事件都有指定的儲存期限，在此期間，您可以在 Kaspersky Next XDR Expert 中檢視或修改該事件。一些事件預設下不儲存在管理伺服器資料庫，因為它們的儲存期限是零。僅可以在管理伺服器資料庫中儲存至少一天的事件可以被匯出到外部系統。

Kaspersky Next XDR Expert 元件事件

每個 Kaspersky Next XDR Expert 元件都有自己的一組事件類型。本節列出了管理伺服器和網路代理中會發生的事件類型。Kaspersky 應用程式中發生的事件類型不在此區域列出。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型描述的資料結構

對於每個事件類型，它的顯示名稱、識別碼（ID）、字母碼、描述和預設儲存期限被提供。

- **事件類型顯示名稱**。當您設定事件以及事件發生時，此文字會顯示在 Kaspersky Next XDR Expert 中。
- **事件類型 ID**。該數碼在您使用協力廠商工具分析事件時使用。
- **事件類型**（字母碼）。當您使用 Kaspersky Next XDR Expert 資料庫提供的公用檢視來瀏覽及處理事件，以及將事件匯出至 SIEM 系統時，會使用此代碼。
- **敘述**。該文字包含事件發生的情況以及此種情況下您可以做的事。
- **預設儲存期限**。這是事件儲存在管理伺服器資料庫的天數，顯示在管理伺服器事件清單中。該時間段之後，事件被刪除。如果事件儲存期限值是 0，此類事件被偵測但不顯示在管理伺服器事件清單。如果您設定了儲存此類事件到作業系統事件記錄，您可以在那裡找到它們。

  您可以變更事件的儲存期限：設定事件的儲存期限。

管理伺服器事件

該部分包含管理伺服器相關事件資訊。

管理伺服器緊急事件

下表顯示嚴重程度為**緊急**的管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器緊急事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
行動裝置的管理伺服器憑證已過期	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	當行動裝置和 UEFI 裝置的管理伺服器憑證過期時，會發生此類事件。 您需要更新過期的憑證。	180 天
稽核：匯出到 SIEM 失敗	5130	KLAUD_EV_SIEM_EXPORT_ERROR	當匯出事件到 SIEM 系統因 SIEM 系統連線錯誤而失敗時，會發生此類型的事件。	180 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
裝置已不受管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理裝置在網路中可見，但一定時間未連線到管理伺服器，則該類型的事件發生。 找到什麼封鎖了裝置上網路代理的正常功能。可能的原因包括網路問題和從裝置移除網路代理。	180 天
裝置狀態為「緊急」	4113	KLSRV_HOST_STATUS_CRITICAL	當受管理裝置被分配*緊急*狀態時，該類型的事件發生。您可設定將裝置狀態變更為緊急的條件。	180 天
產品授權即將到期	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	當接近商業授權到期日時，就會發生此類事件。 Open Single Management Platform每天會檢查一次產品授權是否接近到期日。此類事件會在產品授權到期日期前30天、15天、5天和1天發布。無法變更此天數。如果管理伺服器在產品授權到期日期前的指定日期關閉，則事件將在第二天發布。 正式產品授權到期後，Kaspersky Next XDR Expert 僅提供基本功能。 您可以透過以下方式回應事件： • 請確定已將備用產品授權金鑰新增至管理伺服器。 • 如果您使用訂購方案，請確保續訂該方案。無限制訂購如果已經預付給服務提供商了，則會在到期日自動續約。	180 天
已超過產品授權數量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Next XDR Expert 每天檢查一次是否超過產品授權數量限制。 當管理伺服器檢測到安裝在用戶端設備上的卡巴斯基應用程式某些授權限制即將被超過，且目前單一授權所涵蓋的使用授權單元數量超過該授權總單元總數的110%時，就會發生此類事件。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 Kaspersky Next XDR Expert 決定超過產品授權數量限制時產生事件的規則。	180 天
受限功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	當 Kaspersky Next XDR Expert 開始僅以基本功能運作，不提供弱點和修補程式管理及行動裝置管理功能時，就會發生此類事件。 以下是事件發生的原因和正確回應： • 產品授權期限已到期。提供產品授權，以使用 Kaspersky Next XDR Expert 的完整功能模式（將有效啟動碼或金鑰檔案新增至管理伺服器）。 • 管理伺服器管理比產品授權限制更多的裝置。從管理伺服器的管理群組移動裝置到其他管理伺服器的管理群組（如果其他管理伺服器的產品授權限制允許）。	180 天
MDM 憑證已到期	4132	KLSRV_CERTIFICATE_EXPIRED	當行動裝置上的用戶端憑證過期時，就會發生此類事件。	180 天
金鑰檔案已新增到拒絕清單	4124	KLSRV_LICENSE_BLACKLISTED	當 Kaspersky 已新增您使用的啟動碼或金鑰檔案到拒絕清單時，會發生該類型的事件。 聯絡技術支援獲得更多詳情。	180 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
卡巴斯基應用程式模組更新已撤銷	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	當卡巴斯基專家撤銷更新時（例如，以較新版本取代這些更新），就會發生此類事件。對於此類更新，狀態為*已撤銷*。此事件涉及 Kaspersky Next XDR Expert 修補程式，與受管理的 Kaspersky 應用程式模組無關。事件提供無縫更新未被安裝的原因。	180 天
病毒爆發	• 26（對於檔案威脅防護） • 27（對於郵件威脅防護） • 28（對於防火牆）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	

管理伺服器功能失效事件

下表顯示了重要性等級為**功能失效**的管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
將更新複製到指定資料夾失敗	4123	KLSRV_UPD_REPL_FAIL	當軟體更新被複製到附加分享資料夾時，該類型的事件發生。 您可以透過以下方式回應事件： • 檢查用於獲取資料夾存取的使用者帳戶是否具有寫權限。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網際網路連線，因為它可能是事件原因。遵照指示更新資料庫和軟體模組。	180 天
輪詢雲端區段失敗	4143	KLSRV_KLCLOUD_SCAN_ERROR	當管理伺服器無法在雲端環境中輪詢網路區段時，將發生此類事件。讀取事件敘述中的詳細資訊，並據此做出回應。	未儲存
其中一個已授權應用程式群組已超過最大安裝數量	4126	KLSRV_INVLICPROD_EXCEDED	管理伺服器定期產生該類型的事件（每小時）。如果您在 Kaspersky Next XDR Expert 中管理第三方應用程式的產品授權金鑰，且安裝數量已超過第三方應用程式的產品授權金鑰所設定的限制，就會發生此類事件。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。從未使用協力廠商應用程式的裝置上移除該應用程式。 • 為更多裝置使用協力廠商產品授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。這是一組由滿足您所設標準的協力廠商應用程式組成的授權應用程式群組。	180 天
沒有剩餘硬碟空間	4107	KLSRV_DISK_FULL	當安裝管理伺服器的裝置磁碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	180 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
管理伺服器資料庫空間不足	4110	KLSRV_DATABASE_FULL	當管理伺服器資料庫沒有剩餘空間時，該類型的事件發生。 當管理伺服器的資料庫達到其容量，以及當不可能再往資料庫記錄時，管理伺服器不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應： • 限制儲存在管理伺服器資料庫的事件數量。 • 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security 政策設定。 在 DBMS 選項處檢視資訊。	180 天
執行時錯誤	4125	KLSRV_RUNTIME_ERROR	由於未知問題，該類型的事件發生。 多數情況下，這些是 DBMS 問題、網路問題和其他軟體和硬體問題。 事件詳情可以在事件描述中找到。	180 天
共用資料夾無法使用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理伺服器共用資料夾不可用，則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查管理伺服器（共用資料夾所在位置）是否已開啟並可用。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網路連線。	180 天
管理伺服器資料庫無法使用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理伺服器資料庫不可用則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查安裝了 DBMS 的遠端伺服器是否可用。 • 檢視 DBMS 記錄以發現管理伺服器資料庫不可用的原因。	180 天

管理伺服器警告事件

下表顯示具有**警告**嚴重等級的網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器警告事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
行動裝置的管理伺服器憑證即將過期	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	當行動裝置和 UEFI 裝置的管理伺服器憑證過期時，會發生此類事件。 您需要更新過期的憑證。	90 天
APN 憑證即將到期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	當 APNs 憑證剩餘時間不足 14 天時，就會發生此類事件。 當 APNs 憑證到期時，您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。 建議您在到期日之前安排續訂 APNs 憑證。	未儲存
APN 憑證已到期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	當 APNs 憑證過期時，會發生此類事件。 您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。	未儲存

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
稽核：SIEM 伺服器連線測試失敗	5120	KLAUD_EV_SIEM_TEST_FAILED	當 SIEM 伺服器自動連線測試失敗時，會發生此類型的事件。	90 天
憑證已刪除	4134	KLSRV_CERTIFICATE_REMOVED	當管理員為行動裝置管理移除任何類型的憑證（一般、郵件、VPN）時，會發生此類事件。 移除憑證後，透過此憑證連線的行動裝置將無法連線到管理伺服器。 在調查與行動裝置管理相關的故障時，此事件可能會有所幫助。	90 天
憑證已被請求	4133	KLSRV_CERTIFICATE_REQUESTED	當無法自動重新發佈行動裝置管理憑證時，將發生此類事件。 以下可能是事件的原因和適當的回應： • 已針對憑證的以下內容啟動自動重新發佈：已停用**如果可能，自動重新發佈憑證**選項。這可能是由於建立憑證期間發生的錯誤。可能需要手動重新發佈憑證。 • 如果您使用與公開金鑰基礎架構的整合，則可能是由於缺少適用於與 PKI 整合和發佈憑證之帳戶的 SAM-Account-Name 屬性。檢視帳戶屬性。	90 天
裝置名稱衝突	4102	KLSRV_EVENT_HOSTS_CONFLICT	當管理伺服器將兩個或更多受管理裝置視為單一裝置時，會發生此類事件。 當複製的硬碟用在受管理裝置上進行軟體佈署，並且沒有將網路代理切換到參考裝置上的專用磁碟複製模式時，通常會發生這種情況。 為避免此問題，請在複製該裝置硬碟之前將網路代理切換到參考裝置上的磁碟複製模式。	90 天
連到主管理伺服器的連線已中斷	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	當與主要管理伺服器的連線中斷時，會發生此類事件。 在安裝了主要管理伺服器的裝置上讀取作業系統記錄，並據此做出回應。	90 天
連到從屬管理伺服器的連線已中斷	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	當與次要管理伺服器的連線中斷時，會發生此類事件。 在安裝了次要管理伺服器的裝置上讀取作業系統記錄，並據此做出回應。	90 天
裝置在網路上已長時間沒有活動	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	當受管理裝置顯示閒置狀態時，有時會發生該類型的事件。 最常在停用受管理裝置時發生。 您可以透過以下方式回應事件： • 要從受管理裝置清單中手動刪除裝置。 使用OSMP主控台指定在多久之後會產生**裝置在網路上已長時間沒有活動**事件的時間間隔。 • 使用OSMP主控台指定在多久之後裝置會自動從群組中移除。	90 天
裝置狀態為「警告」	4114	KLSRV_HOST_STATUS_WARNING	當受管理裝置被分配*警告*狀態時，該類型的事件發生。您可設定將裝置狀態變更為*警告*的條件。	90 天
下載檔案到裝置失敗	4165	KLSRV_FILE_DOWNLOAD_FAILED	此類事件會在以下情況發生： • 您嘗試將檔案下載到企業容器中，但尚未建立企業容器。 • 裝置空間不足。 • 無法從伺服器下載檔案資訊。 • 無法從伺服器下載檔案內容。 • 無法在裝置上建立資料夾。 • 個人裝置上缺少檔案存取權限。 • 企業容器中缺少檔案存取權限。	90 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
傳送 FCM 訊息到 FCM 伺服器失敗	4140	KLSRV_GCM_GENERAL_ERROR	使用 Google Firebase Cloud Messaging HTTP 通訊協定時，由於管理伺服器端發生意外錯誤，因此會發生此類事件。 讀取事件敘述中的詳細資訊，並據此做出回應。 如果您自己找不到問題的解決方案，建議您與卡巴斯基技術支援聯絡。	90 天
傳送 FCM 訊息到行動裝置失敗	4138	KLSRV_GCM_DEVICE_ERROR	當配置行動裝置管理使用 Google Firebase Cloud Messaging (FCM) 連線到具有 Android 作業系統的受管理行動裝置並且 FCM 伺服器無法處理從管理伺服器收到的某些要求時，會發生此類事件。這意味著某些受管理行動裝置將不會收到推送通知。 讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。如需從 FCM 伺服器接收到的 HTTP 程式碼以及相關錯誤的詳細資訊，請參閱 Google Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。	90 天
已偵測到頻繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	當管理伺服器在受管理裝置上偵測到頻繁發生的事件時，就會發生這種類型的事件。有關詳細資訊，請參閱以下部分：阻止頻繁事件。	90 天
硬碟磁碟機幾乎已滿	4105	KLSRV_NO_SPACE_ON_VOLUMES	當安裝管理伺服器的裝置硬碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	90 天
傳送 FCM 訊息到 FCM 伺服器時發生 HTTP 錯誤	4139	KLSRV_GCM_HTTP_ERROR	當配置行動裝置管理使用 Google Firebase Cloud Messaging (FCM) 連線到具有 Android 作業系統的受管理行動裝置並且 FCM 伺服器透過 200 (OK) 以外的 HTTP 程式碼還原管理伺服器的要求時，會發生此類事件。 以下可能是事件的原因和適當的回應： • FCM 伺服器端出現問題。讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。如需從 FCM 伺服器接收到的 HTTP 程式碼以及相關錯誤的詳細資訊，請參閱 Google Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。 • 代理伺服器端的問題（如果使用代理伺服器）。讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。	90 天
已超過產品授權數量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Next XDR Expert 每天檢查一次是否超過產品授權數量限制。 當管理伺服器檢測到安裝在用戶端設備上的卡巴斯基應用程式超過某些授權限制，且單一授權所涵蓋的當前使用授權單元數量超過該授權所涵蓋單元總數的 100%-110%時，會發生此類事件。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 Kaspersky Next XDR Expert 決定超過產品授權數量限制時產生事件的規則。	90 天
已授權應用程式群組之一的安裝即將達到限制	4128	KLSRV_INVLICPROD_EXPIRED_SOON	當已授權應用程式群組中包含的協力廠商應用程式的產品授權金鑰之一即將過期時，就會發生此類事件。結果，其中一個群組的安裝限制將被減少。 您可以透過以下方式回應事件： • 如果某些受管理裝置上未使用協力廠商應用程式，請從這些裝置上刪除該應用程式。 • 如果您預計協力廠商應用程式的安裝數量將在不久的將來超過允許的最大值，請考慮預先獲取更多裝置的協力廠商授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。	90 天
已註冊卡巴斯基應用程式模組的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	當管理伺服器為需要批准安裝的受管理裝置上安裝的 Kaspersky 軟體註冊新更新時，將發生此類事件。 使用卡巴斯基安全管理中心網頁主控台核准或拒絕更新。	90 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
管理伺服器資料庫空間不足	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理伺服器資料庫受限制則該類型的事件發生。如果您不糾正情況，管理伺服器資料庫就將達到其容量且管理伺服器將不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應。 • 不限制儲存在管理伺服器資料庫的事件數量 • 降低儲存在管理伺服器資料庫的事件數量 在 DBMS 選項處檢視資訊。	90 天
超過資料庫中的事件數量限制，刪除事件開始	4145	KLSRV_EVP_DB_TRUNCATING	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後開始時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存
超過資料庫中的事件數量限制，事件已被刪除	4146	KLSRV_EVP_DB_TRUNCATED	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後完成時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更允許儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存

管理伺服器資訊事件

下表顯示了重要性等級為**資訊**的管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
行動裝置的管理伺服器憑證正在更新中	6127	KLSRV_EV_SRV_CERT_RENEWED	當管理伺服器憑證已續約時會發生此事件。	30 天
稽核：指令已傳送到裝置	4170	KLAUD_EV_COMMAND_SENT	當使用者向行動裝置傳送指令時，會發生此類事件。	30 天
稽核：連到管理伺服器的連線已終止	4151	KLAUD_EV_SERVERDISCONNECT		30 天
稽核：到管理伺服器的連線已建立	4147	KLAUD_EV_SERVERCONNECT	當使用者透過OSMP主控台連接到管理伺服器時，會發生此類事件。這些事件包括安裝OSMP主控台伺服器的裝置的IP位址。	30 天
稽核：加密金鑰已匯入/匯出	5100	KLAUD_EV_DPEKEYSEXPORT	例如，遷移期間會發生該事件。	30 天
稽核：群組設定已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	當安全群組已被編輯時，該類型事件發生。	30 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
稽核：物件已修改	4148	KLAUD_EV_OBJECTMODIFY	此事件追蹤以下物件的變更： • 管理群組 • 安全群組 • 使用者 • 套件 • 工作 • 政策 • 伺服器 • 虛擬伺服器	30 天
稽核：物件內容已修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	此事件追蹤以下屬性的變更： • 使用者 • 產品授權 • 伺服器 • 虛擬伺服器	30 天
稽核：物件狀態已修改	4150	KLAUD_EV_TASK_STATE_CHANGED	例如，當工作因錯誤而失敗時會發生此事件。	30 天
稽核（SIEM 伺服器連線測試成功）	5110	KLAUD_EV_SIEM_TEST_SUCCESS	當 SIEM 伺服器連線測試成功時，該類型事件發生。	30 天
稽核：使用者權限已修改	4153	KLAUD_EV_OBJECTACLMODIFIED	當使用者權限被修改時會發生該事件。	30 天
連到主管理伺服器的連線已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 天
連到從屬管理伺服器的連線已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	有關詳細資訊，請參閱以下文章：建立管理伺服器階層架構：新增從屬管理伺服器。	30 天
資料庫已更新	4144	KLSRV_UPD_BASES_UPDATED	當 將更新下載至管理伺服器儲存區工作完成資料庫更新時，就會發生此類事件。	30 天
裝置已被自動新增到群組	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	當根據行動裝置規則將裝置分配到群組時，會發生此類事件。	30 天
根據規則自動移動裝置	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	當已使用裝置移動規則將裝置移動到管理群組時，會發生此類事件。	30 天
裝置已從群組中刪除：長時間在網路中不活動	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	當裝置因無活動而自動從群組中刪除時，該類型事件發生。	30 天
此行動裝置上的 FCM 實例 ID 已被變更	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	當裝置上的 Firebase Cloud Messaging 權杖變更時，該類型事件發生。 有關 FCM 權杖輪換的資訊，請參閱 Firebase 服務文件。	30 天
檔案已上傳到管理伺服器	4162	KLSRV_FILE_UPLOADED	如果管理員已將檔案上傳至 **資產管理** → **Mobile** → **Apps & files** → **Files**清單，就會發生此類事件。	30 天
檔案被從管理伺服器中刪除	4163	KLSRV_FILE_REMOVED	如果管理員已從**資產管理** → **Mobile** → **Apps & files** → **Files**清單中刪除檔案，就會發生此類事件。	30 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
檔案已下載到裝置	4164	KLSRV_FILE_DOWNLOADED	此類事件會在以下情況發生： • 管理員已從網頁主控台的 **資產管理 → Mobile → Apps & files → Files**清單將檔案下載到管理員工作站。 • **資產管理 → Mobile → Apps & files → Files** 清單中的檔案已下載到安裝 Kaspersky Endpoint Security for Android 的裝置。	30 天
下載檔案到裝置失敗	4165	KLSRV_FILE_DOWNLOAD_FAILED	此類事件會在以下情況發生： • 管理員嘗試從網頁主控台的 **資產管理 → Mobile → Apps & files → Files**清單將檔案下載到管理員工作站時發生錯誤。 • 將檔案從**資產管理 → Mobile → Apps & files → Files**清單下載到安裝 Kaspersky Endpoint Security for Android 的裝置時發生錯誤。	30 天
找到了要傳送至 Kaspersky 以分析的檔案	4131	KLSRV_APS_FILE_APPEARED		30 天
已授權應用程式群組之一的安裝即將超過限制（已經使用 90% 以上）	4127	KLSRV_INVLICPROD_FILLED	當已授權應用程式群組中包含的協力廠商應用程式的安裝數量達到產品授權金鑰屬性中指定之最大允許值的 90% 時，將發生此類事件。 您可以透過以下方式回應事件： • 如果某些受管理裝置上未使用協力廠商應用程式，請從這些裝置上刪除該應用程式。 • 如果您預計協力廠商應用程式的安裝數量將在不久的將來超過允許的最大值，請考慮預先獲取更多裝置的協力廠商授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。	30 天
已偵測到新裝置	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	當發現新的連網裝置時，就會發生此類事件。	30 天
產品授權金鑰的 90% 已經使用	4097	KLSRV_EV_LICENSE_CHECK_90	當管理伺服器檢測到安裝在用戶端設備上的卡巴斯基應用程式某些授權限制即將被超過，且目前單一授權所涵蓋的使用授權單元數量超過該授權總單元總數的90%時，就會發生此類事件。 即使超出許可限制，用戶端裝置也會受到防護。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 Kaspersky Next XDR Expert 決定超過產品授權數量限制時產生事件的規則。	30 天
已為行動裝置創建預留管理伺服器憑證	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	當管理伺服器憑證已建立時會發生此事件。	30 天
更新被成功複製至指定的資料夾	4122	KLSRV_UPD_REPL_OK	當**將更新下載至管理伺服器儲存區**工作完成將檔案複製到指定資料夾時，便會發生此類事件。	30 天

僅當對行動裝置和UEFI裝置的管理伺服器憑證執行了對應操作時，管理伺服器才會自動發布並在管理主控台中顯示**備用憑證已建立**與**憑證續約**事件。

網路代理事件

該部分包含網路代理相關事件資訊。

網路代理警告事件

下表顯示具有**警告**嚴重等級的網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理警告事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
KSN 代理已啟動。檢查 KSN 可用性失敗	7718	KSNPROXY_STARTED_CON_CHK_FAILED	當已設定的 KSN 代理連線的連線測試失敗時，該類型事件發生。	30 天
發生了安全問題	549	GNRL_EV_APP_INCIDENT_OCCURED	當在裝置上發現事件時，該類型事件發生。例如，當裝置磁碟空間不足時，就會發生該類型事件。	30 天
Sudoers 檔案與參考值不匹配	7724	KLNAG_EV_SUDOER_DIFFERENT	當 sudoers 檔案與參考檔案不符時，就會發生此類事件。	30 天
協力廠商軟體更新已延時	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	例如，當第協力廠商更新安裝的 EULA 被拒絕時，就會發生該類型事件。	30 天
協力廠商軟體更新安裝已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	下載偵錯檔案並檢查 KLRI_PATCH_RES_DESC 欄位的值以了解詳細資訊。	30 天
使用者管理：警告	7722	KLNAG_EV_USR_MNG_WRN	一般警告事件。	30 天
在安裝軟體模組更新期間返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	下載偵錯檔案並檢查 KLRI_PATCH_RES_DESC 欄位的值以了解詳細資訊。	30 天

網路代理資訊事件

下表顯示具有**資訊**嚴重等級的網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件組態**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
應用程式已安裝	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
應用程式已解除安裝	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
收到網頁伺服器 HTTPS 連接埠的憑證	—	WEB_SERVER_CERTIFICATE_RENEWED	30 天
裝置已被授權	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
已偵測到新裝置	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
裝置已被刪除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
軟體模組更新安裝已啟動	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
KSN 代理已啟動。KSN 可用性檢查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天
已安裝監控的應用程式	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已解除安裝監控的應用程式	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已新增裝置	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
根憑證已安裝	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 天

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
根憑證已移除	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 天
Sudoers 檔案已被成功還原到參考值	7725	KLNAG_EV_SUDOER_RESTORED	30 天
已安裝協力廠商應用程式	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
協力廠商軟體更新已成功安裝	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
協力廠商軟體更新安裝已開始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
軟體模組更新已成功安裝	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
使用者管理：資訊	7721	KLNAG_EV_USR_MNG_INF	30 天
網頁伺服器在主機上啟動	—	WEB_SERVER_STARTED	30 天
網頁伺服器在主機上停止	—	WEB_SERVER_STOPPED	30 天
Windows 桌面共用：應用程式已啟動	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 桌面共用：檔案已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 桌面共用：檔案已讀取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 桌面共用：已啟動	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 桌面共用：已停止	7716	KLUSRLOG_EV_WDS_END	30 天

使用事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

- 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
- 依時間—**最近事件**
- 依類型—**使用者請求**和**稽核事件**

您可以在OSMP主控台介面中，根據可用設定建立並檢視使用者定義的事件選取，以進行配置。

事件選取可OSMP主控台中使用，路徑為**監控—>事件分類**。

預設下，事件分類包含 7 天內的資訊。

Kaspersky Next XDR Expert 提供一組預設的事件選取項目：

- 不同重要等級的事件：
  - **緊急事件**
  - **功能失效**
  - **警告**
  - **資訊訊息**
- **使用者請求**（受管理應用程式事件）

- **最近事件**（上周）
- **稽核事件**。

在卡巴斯基Next XDR Expert中，與服務操作相關的稽核事件會顯示在您的OSMP主控台中。這些事件的發生條件是由 Kaspersky 專家操作設定。這些事件包括以下內容：登入管理伺服器；管理伺服器端口變更；管理伺服器資料庫備份；使用者帳號的建立、修改和刪除。

您也可以建立和配置附加使用者定義分類。在使用者定義分類中，您可以根據裝置內容（裝置名稱、IP 範圍和管理群組）、根據事件類型和嚴重等級、根據應用程式和元件名稱、以及根據時間間隔來篩選事件。也可以包含工作結果到搜尋範圍。您也可以單一搜尋欄位，可以輸入一個詞或幾個詞。所有內容（例如事件名稱、描述、元件名稱）中包含任意所輸入詞的事件被顯示。

對於預先定義和使用者定義的分類，您可以限制顯示事件的數量或者要搜尋的記錄的數量。這兩個選項都會影響 Kaspersky Next XDR Expert 顯示事件所需的時間。資料庫越大，過程越耗時。

您可以執行以下操作：

- 編輯事件分類的內容
- 產生事件分類
- 檢視事件分類的詳細資訊
- 刪除事件分類
- 從管理伺服器資料庫中刪除事件

建立事件分類

要建立事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控 → 事件分類**。
2. 點擊**新增**。
3. 在開啟的**新事件分類**視窗，指定新事件分類的設定。在視窗中重複此操作。
4. 按一下**儲存**以儲存變更。

   確認視窗隨即開啟。
5. 若要檢視事件分類結果，請持續選取**轉到分類結果**核取方塊。
6. 點擊**儲存**以確認建立事件分類。

若您持續選取**轉到分類結果**核取方塊，會顯示事件分類結果。否則，新事件分類出現在事件分類清單。

編輯事件分類

要編輯事件分類：

1. 在主功能表中，轉至 **監控 → 事件分類**。
2. 選取您要編輯的事件分類旁邊的核取方塊。
3. 點擊**內容**按鈕。
   事件分類設定視窗開啟。
4. 編輯事件分類內容。

   > 對於預先定義的事件分類，您盡可編輯以下頁籤的內容：**一般**（分類名稱除外）、**時間**以及**存取權限**。

   對於使用者定義分類，您可以編輯所有內容。
5. 按一下**儲存**以儲存變更。

編輯的事件分類顯示在清單。

檢視事件分類清單

要檢視事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控 → 事件分類**。
2. 選取您要啟動的事件分類旁邊的核取方塊。
3. 執行以下操作之一：
   - 如果您要在事件分類結果中配置排序，做以下：
     a. 點擊**重新設定排序並啟動**按鈕。
     b. 在顯示的 **重新設定事件分類排序** 視窗中指定排序設定。
     c. 請點擊選項的名稱。
   - 或者，若您要在管理伺服器上排序好事件後檢視事件清單，請點擊選項名稱。

事件分類結果被顯示。

匯出事件分類

Open Single Management Platform允許您將事件分類及其設定儲存到KLO檔案。您可以使用此 KLO 檔案匯入儲存的事件分類到 卡巴斯基安全管理中心 Windows 和 卡巴斯基安全管理中心 Linux。

請注意，您只能匯出使用者定義的事件分類。Open Single Management Platform預設集合中的事件分類（預定義選擇）無法儲存到檔案中。

要匯出事件分類，請執行以下操作：

1. 在主功能表中，轉至**監控 → 事件分類**。
2. 選取您要匯出的事件分類旁邊的核取方塊。

   您不能同時匯出多個事件分類。如果您選擇了多個分類，**匯出**按鈕將被停用。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存為**視窗中，指定事件分類檔案名稱和路徑，然後點擊**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，事件分類檔案會自動儲存在**下載**資料夾中。

匯入事件分類

Open Single Management Platform允許您從KLO檔案匯入事件分類。KLO 檔案包含匯出事件分類及其設定。

要匯入事件分類，請執行以下操作：

1. 在主功能表中，轉至**監控 → 事件分類**。
2. 點擊**匯入**按鈕，然後選擇要匯入的事件分類檔案。
3. 在開啟的視窗中，指定 KLO 檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個事件分類檔案。

   事件分類處理開始。

此時會顯示匯入結果通知。如果事件分類匯入成功，您可以點擊**檢視匯入詳細資訊**連接來檢視事件分類屬性。

匯入成功後，事件分類會顯示在分類清單中。事件分類的設定也會被匯入。

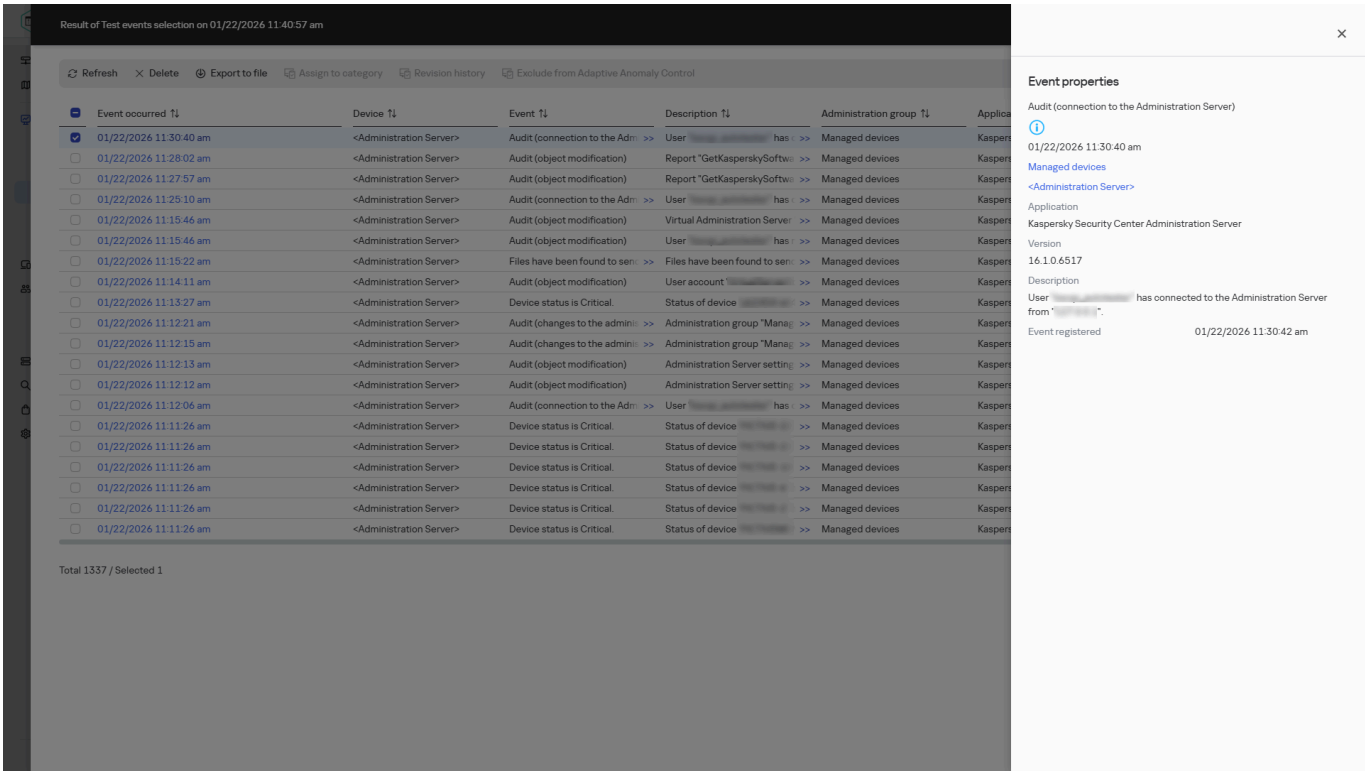
如果新匯入事件分類的名稱與現有事件分類的名稱相同，則匯入分類的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

檢視事件詳細資料區域

要檢視事件詳情：

1. 啟動事件分類。
2. 點擊所需事件的時間。

   事件內容視窗開啟。



"事件內容"視窗

3. 在顯示的視窗中，您可以做以下：
   - 檢視關於所選事件的資訊
   - 轉到發生事件的裝置
   - 轉到包含發生事件的裝置的管理群組
   - 對於工作相關事件，轉到工作內容

匯出事件到檔案

Open Single Management Platform可讓您將事件分類中的事件儲存為TXT檔案。

要匯出事件到檔案：

1. 啟動事件分類。
2. 選取所需事件旁邊的核取方塊。
   您也可以選擇多個事件或整個事件分類。
3. 點擊**匯出至檔案**按鈕。

所選事件被匯出到 TXT 檔案。

從事件檢視物件歷程

從建立或修改支援修訂管理的物件的事件，您可以切換到物件的修訂歷程。

要從事件檢視物件歷程：

1. 啟動事件分類。
2. 選取所需事件旁邊的核取方塊。
3. 點擊**變更歷史**按鈕。

物件修訂歷程被開啟。

刪除事件

要從事件分類中刪除事件：

1. 啟動事件分類。
2. 選擇事件：
   - 若要刪除一個或多個事件，請選取其旁邊的核取方塊。
   - 若要刪除目前頁面上的所有事件，請選取事件清單上方的核取方塊，然後按一下**全部選取目前頁面**選項。
   - 若要刪除選定區域中的所有事件，請選取事件清單上方的核取方塊，然後按一下**全選**選項。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**刪除**按鈕。

若要從裝置事件清單中刪除事件：

1. 開啟裝置清單。
   - 對於受管理裝置：**資產管理→資產（裝置）**。
   - 對於未指派的裝置：**資產管理→未指派的裝置**。
2. 在裝置清單中，按一下所需裝置名稱的連結，然後轉至**事件**標籤。
3. 選擇事件：
   - 若要刪除一個或多個事件，請選取其旁邊的核取方塊。
   - 若要刪除目前頁面上的所有事件，請選取事件清單上方的核取方塊，然後按一下**全部選取目前頁面**選項。
   - 若要刪除選定區域中的所有事件，請選取事件清單上方的核取方塊，然後按一下**全選**選項。
4. 按一下**刪除**，然後確認操作。
5. 在開啟的視窗中，點擊**刪除**按鈕。

   所選事件被刪除且無法還原。

刪除事件分類

您僅可以刪除使用者定義的事件分類。預定義事件分類無法被刪除。

要刪除一個或幾個事件分類：

1. 在主功能表中，轉至 **監控 → 事件分類**。
2. 選取您要刪除的事件分類旁邊的核取方塊。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**。

   事件分類被刪除。

設定事件儲存期限

Kaspersky Next XDR Expert 可讓您接收管理伺服器和安裝在受管理裝置上的 Kaspersky 應用程式運作期間所發生事件的相關資訊。事件資訊儲存在管理伺服器資料庫。您可能需要比預設值將一些事件儲存較長或較短的時間。您可以變更事件儲存期限的預設設定。

若您有意在管理伺服器資料庫中儲存部分事件，您可在管理伺服器政策和 Kaspersky 應用程式政策或管理伺服器內容中停用適當設定（僅限管理伺服器事件）。這將降低資料庫中的事件類型數量。

事件的儲存期限越長，資料庫達到最大值速度越快。然而，較長期的事件可讓您執行較長時間的監控與回報工作。

要為管理伺服器中的事件設定儲存期限：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 點擊所需政策的名稱。

   您可以選擇受管理卡巴斯基應用程式、網路代理或管理伺服器的政策。對於管理伺服器，您也可以點擊管理伺服器名稱來設定事件的儲存期限。
3. 選擇**事件組態**標籤。

   與**緊急**區段相關的事件類型清單隨即顯示。如果需要，您可以移動到**功能失效**、**警告**或**資訊**部分。
4. 在右側面板中的事件類型清單中，點擊您要變更其儲存期限的事件的連結。

   在開啟的視窗的**事件註冊**區段，會啟用**儲存在管理伺服器資料庫中（天）**切換開關。
5. 在該開關按鈕下面的編輯方塊中，輸入儲存事件的天數。
6. 若您要在管理伺服器資料庫儲存事件，請停用**儲存在管理伺服器資料庫中（天）**選項。

   若您在管理伺服器內容視窗中設定管理伺服器事件，以及若事件設定在管理伺服器政策中鎖定，您無法重新定義事件的儲存期限值。
7. 按一下**確定** ，然後在右側窗格關閉後，按一下**儲存**按鈕。

   政策內容視窗隨即關閉。

從現在開始，當管理伺服器接收並儲存所選類型的事件時，它們將具有變更的儲存期限。管理伺服器不會變更以前接收到的事件的儲存期限。

封鎖頻發事件

本節提供有關管理頻繁事件封鎖和移除對頻繁事件封鎖的資訊。

關於封鎖頻發事件

安裝在單個或多個受管理裝置上的受管理應用程式（例如，Kaspersky Endpoint Security for Linux）可以將許多相同類型的事件傳送到管理伺服器。接收頻繁的事件可能會使管理伺服器資料庫超載並覆寫其他事件。當所有接收到的事件數超過資料庫的指定限制時，管理伺服器將開始封鎖最頻繁的事件。

管理伺服器會封鎖自動接收頻發事件。您不能自己封鎖頻發事件，也不能選擇要封鎖的事件。

如果您想了解某個事件是否被封鎖，您可檢視通知清單或檢視該事件是否存在於**封鎖頻繁事件**的管理伺服器屬性區段。在封鎖的事件中，您可以進行以下操作：

- 如果要封鎖覆寫資料庫，則可以繼續封鎖接收此類事件。
- 例如，如果要查找將頻發事件傳送到管理伺服器的原因，則可以取消封鎖頻發事件並繼續接收此類事件。
- 如果要繼續接收頻發事件直到再次被封鎖，可以從封鎖頻發事件中刪除。

管理頻發事件封鎖

管理伺服器封鎖自動接收頻繁事件，但是您可以取消封鎖並繼續接收頻繁事件。您還可以封鎖接收以前取消封鎖的頻繁事件。

若要管理頻發的事件封鎖：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**封鎖頻繁事件**區段。
3. 在**封鎖頻繁事件**區段：
   - 如果要取消封鎖接收頻繁事件，請執行以下操作：
     a. 選取您要封鎖的頻繁事件並點擊**排除**按鈕。
     b. 按一下**儲存**按鈕。
   - 如果要封鎖接收頻繁事件：
     a. 選取您要封鎖的頻繁事件並點擊**封鎖**按鈕。
     b. 按一下**儲存**按鈕。

管理伺服器會接收取消封鎖的頻繁事件，並且不會接收已封鎖的頻繁事件。

移除對頻發事件的封鎖

您可以刪除對頻繁事件的封鎖並開始接收它們，直到管理伺服器再次封鎖這些頻繁事件為止。

要移除對頻繁事件的封鎖：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**封鎖頻繁事件**區段。
3. 在**封鎖頻繁事件**區段，選擇要為其移除封鎖的頻繁事件類型。
4. 點擊**移除封鎖**按鈕。

頻繁事件將從頻繁事件清單中移除。管理伺服器將接收此類型的事件。

在管理伺服器上的事件處理和儲存

應用程式和受管理裝置操作期間發生的事件的有關資訊儲存在管理伺服器資料庫中。每個事件都歸屬於特定類型和安全等級（*緊急事件*、*功能失效*、*警告*或*資訊*）。基於事件發生的條件，程式可以分配不同的安全等級到相同類型的事件。

您可以在管理伺服器內容視窗的**事件配置**區域檢視分配給事件的類型和安全等級。在**事件配置**區域，您也可以設定管理伺服器對每個事件的處理：

- 在管理伺服器以及裝置作業系統和管理伺服器事件記錄中註冊事件。
- 通知管理員事件的方法（例如，SMS 或者郵件訊息）。

在管理伺服器內容視窗的**事件儲存區**區域，您可以透過限制事件記錄數和儲存期限來編輯管理伺服器資料庫的事件儲存設定。當您指定事件最大數時，應用程式計算用於指定數目的儲存空間的大概大小。您可以使用該大概計算來評估您在磁碟上是否具有足夠空間以避免資料庫溢出。管理伺服器資料庫的預設容量是 400,000 個事件。最大建議的資料庫容量是 45,000,000 個事件。

應用程式每 10 分鐘檢查一次資料庫。如果事件數達到指定的最大值加 10,000，應用程式將刪除最舊的事件，以便僅保留指定的最大事件數。

若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入作業係統記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。預設情況下，事件佇列的上限為 20,000 個事件。您可以透過編輯 KLEVP_MAX_POSTPONED_CNT 標誌的值來自訂佇列上限。

回溯掃瞄

在正常模式下，相關器僅即時處理來自收集器的事件。如果您需要偵錯關聯規則或分析資料，可以使用**回溯掃描**將關聯規則套用至歷史事件。

若要測試關聯規則，無需即時重播事件。您可以在**回溯掃描**模式下執行關聯規則，以處理包含目標事件的現有事件。

您可以使用搜尋查詢來定義要進行回溯掃描的事件清單，以及指定搜尋期間和要搜尋事件的儲存體。您可以設定工作，以便在事件回溯掃描期間產生警示並套用回應規則。

若要執行回溯掃描：

1. 在解決方案網頁介面的**監控 → 搜尋威脅**區段中，建立所需的事件分類：
   - 選擇儲存體。

     執行回溯掃描之前，請確保已選擇正確的叢集和空間。

- 使用建構函式或搜尋查詢設定搜尋運算式。

  執行回溯掃描之前，請確保已在 SQL 查詢欄位中指定正確的運算式。

- 根據需要設定期間。

  執行回溯掃描之前，請確保已在期間欄位中選擇正確的期間。

2. 在 ··· 下拉清單中，選擇**回溯掃描**。
   回溯掃描視窗開啟。

3. 在**關聯器**下拉清單中，選擇要為選定的事件提供關聯器。

   執行回溯掃描之前，請檢查 SQL 查詢找到的事件數量。此資訊顯示在**顯示時間線→總計**下方。如果SQL查詢中未指定**LIMIT** ，則會將該期間內的所有事件傳送至關聯器，從而延長工作完成時間。如果設定了相對期間（例如，*now-1h*），則在回溯掃描開始時可能會產生新事件；這些事件也會傳送到關聯器。如果關聯器安裝在主租用戶（Main、RootTenant）以外的租用戶中，則它只能接收其自身租用戶的事件。

4. 在**關聯規則**下拉清單中，選擇處理事件時必須使用的關聯規則。如果未在此步驟中選擇任何規則，則將套用所有關聯規則執行掃描。

5. 在**EPS 上限**欄位中，指定回溯掃描要使用的最大 EPS。指定的值會設定執行回溯掃描時的最大負載。預設設定為 0，表示不會對回溯掃描套用 EPS 限制。

   不允許出現負的EPS值。

6. 如果希望在處理事件時執行回應，請開啟**執行回應**切換開關。

7. 如果您希望在事件處理期間產生警示，請開啟**建立警示**切換開關。

8. 按一下**建立工作**按鈕。

回溯掃描工作隨即建立，並顯示在**工作管理員**區段中。

若要檢視掃描結果，請在 KUMA 網頁介面的**工作管理員**區段中，按一下您建立的工作，然後在下拉式清單中選取**前往事件頁面**。

回溯掃描結果僅顯示產生的關聯事件。
在回溯掃描結果中，期間的開始時間顯示為<工作建立的日期和時間>，期間的結束時間顯示為<工作建立的日期和時間 + 一小時>（如果自工作建立以來尚未經過一小時，則顯示目前時間）。
如果回溯掃描結果中沒有事件，則表示傳送至關聯器的 SQL 選取結果中的事件未觸發關聯器。

系統會開啟新的瀏覽器頁籤，其中包含在回溯掃描期間處理的事件，以及在事件處理期間建立的彙總事件和關聯事件。回溯掃描產生的關聯事件會有額外的 ReplayID 欄位，用於儲存回溯掃描的唯一 ID。分析員可以從工作的快顯表單中重新啟動回溯掃描。新的關聯事件將具有不同的ReplayID。

根據您的瀏覽器設定，系統可能會提示您確認開啟回溯掃描結果頁籤。有關更多詳細資訊，請參閱您使用的瀏覽器的說明文件。

回溯掃描過程中處理的事件不會使用來自CyberTrace或 Kaspersky Threat Intelligence Portal 的資料進行擴充。

回溯掃描期間會更新活動清單。

無法根據包含算術運算式或僅包含彙總欄位的 SQL 查詢執行回溯掃描。只有在查詢處理完成後，才能對使用分組 SQL 查詢取得的事件群組執行回溯掃描。為此，請先執行具有資料分組的 SQL 查詢並取得事件群組清單，然後對其中一個群組執行回溯掃描。

通知和裝置狀態

本節包含有關如何檢視通知、配置通知傳遞、使用裝置狀態和啟用變更裝置狀態的資訊。

使用通知

通知會警示您關於事件的資訊，並協助您透過執行建議動作或您認為適當的動作加速回應這些事件。

根據選取的通知方法，有以下類型的通知可用：

- 螢幕通知
- 透過簡訊通知
- 透過電子郵件通知
- 透過可執行檔或指令碼通知

螢幕通知

螢幕通知提醒您按照重要等級分組的事件（*緊急*、*警告*和*資訊*）。

螢幕通知可以有兩種狀態之一：

- *已檢視*。您已對通知執行建議操作，或您已手動為通知分配該狀態。
- *未檢視*。您未對通知執行建議操作，或您未手動為通知分配該狀態。

預設下，通知清單包含*未檢視*狀態的通知。

您可以透過檢視螢幕通知和即時回應它們來監控您的組織網路。

透過電子郵件、SMS 和可執行檔或指令碼通知

Kaspersky Next XDR Expert 可透過傳送您認為重要之任何事件的通知，監控您組織的網路。對任意事件，您可以配置透過電子郵件、SMS 或執行可執行檔或指令碼進行通知。

在透過電子郵件或 SMS 接收通知時，您可以決定您對事件的回應。該回應應該是最適合您組織網路的。透過執行可執行檔或指令碼，您預定義對事件的回應。您也可以認為執行可執行檔或指令碼是對事件的首選回應。可執行檔執行後，您可以採取其他步驟回應事件。

檢視螢幕通知

您可以透過三種方式在螢幕上檢視通知：

- 在**監控** 中 → **通知**區段。這裡，您可以檢視預定義類別的通知。
- 您可以開啟單獨的視窗。此種情況下，您可以標記通知為已檢視。
- 在 **監控** 上的**所選嚴重等級的通知**小工具中 → **控制板**區段。在部件中，您可以僅檢視處在*嚴重*和*警告*重要性等級的事件通知。

您可以執行操作，例如，您可以回應事件。

要檢視預定義類別的通知：

1. 在主功能表中，轉至 **監控 → 通知**。

   在左窗格中選取**所有通知**類別，右窗格會顯示所有通知。

2. 在左側面板，選取類別之一：

   - **佈署**
   - **裝置**
   - **防護**
   - **更新**

     此通知包含有關可供下載的卡巴斯基應用程式、已下載的病毒資料庫更新，以及網路代理更新後需要重新啟動之裝置（若有）的通知。
   - **弱點利用防禦**
   - **管理伺服器**。

     這僅包括與管理伺服器相關的事件。

- **有用連結**。

  這包括卡巴斯基資源的連結，例如卡巴斯基技術支援、卡巴斯基論壇、金鑰續約頁面或 Kaspersky IT 百科全書。

所選類別的通知清單被顯示。清單包含以下：

- 與通知主題相關的圖示：佈署（ ）、防護（ ）、更新（ ）、裝置管理（ ）、弱點利用防禦（ ）、管理伺服器（ ）。
- 通知重要性等級。以下重要等級通知會顯示：**緊急通知**（ ），**警告通知**（ ），**資訊通知**。清單中的通知按重要性等級分組。
- **通知**。這包含通知敘述。
- **動作**。這包含建議您執行的快速操作連結。例如，透過按一下該連結，您可以轉到儲存區並安裝安全應用程式到裝置，或檢視裝置清單或事件清單。您為通知執行建議操作之後，該通知被分配*已檢視*狀態。
- **狀態註冊時間**。這包含從通知被註冊到管理伺服器到現在為止過去的天數或小時數。

要按照重要性等級在單獨的視窗中檢視螢幕通知：

1. 在OSMP主控台的右上角，按一下旗幟圖示（ ）。

   如果旗幟圖示具有紅點，表示有未檢視的通知。

   列出通知的視窗被開啟。依預設會選取**所有通知**頁籤，通知會根據重要等級分組：*Critical*、*Warning*和*Info*。

2. 選取 **系統**標籤。

   嚴重（ ）和*警告*（ ）重要性等級通知清單被顯示。通知清單包含以下：

   - 顏色標記。嚴重通知標記為紅色。警告通知標記為黃色。
   - 指出通知主題的圖示：佈署（ ）、防護（ ）、更新（ ）、裝置管理（ ）、弱點利用防禦（ ）、管理伺服器（ ）。
   - 通知敘述。
   - 複選標記圖示。旗幟圖示是灰色的，如果通知被分配了*未檢視*狀態。當您選取灰色旗幟圖示並分配*已檢視*狀態到通知時，圖示變更顏色到白色。
   - 建議操作的連結。您對通知執行建議操作之後，該通知會變成*已檢視*狀態。
   - 從通知被註冊到管理伺服器到現在為止過去的天數。

3. 選取 **更多**標籤。

   *資訊*重要性等級通知清單被顯示。

   清單的組織會與**系統**頁籤上的清單相同（請參閱以上說明）。僅有的不同是沒有顏色標記。

您可以透過註冊在管理伺服器上的日期間隔來過濾通知。使用**顯示篩選器**核取方塊來管理篩選條件。

要在部件上檢視螢幕通知：

1. 在**控制板**區段上，選取**新增或還原小部件**。
2. 在開啟的視窗中，點擊**其他**類別，選取**所選嚴重等級的通知**小工具，接著點擊新增。

   小工具現在會顯示在**控制板**頁籤上。預設下，*嚴重*重要性等級的通知顯示在部件。

   您可以按一下部件上的**設定**按鈕並變更部件設定以檢視*警告*重要性等級的通知。或者，您可以新增其他部件：**所選嚴重等級的通知**，帶有*警告*重要性等級。

   部件上的通知清單由尺寸限制並包含兩個通知。這兩個通知是關於最近事件的。

部件上的通知清單包含以下：

- 與通知主題相關的圖示：佈署（）、防護（）、更新（）、裝置管理（）、弱點利用防禦（）、管理伺服器（）。
- 通知敘述和建議操作的連結。您對通知執行建議操作之後，該通知會變成*已檢視*狀態。
- 從通知被註冊到管理伺服器到現在為止過去的天數或小時數。
- 到其他通知的連結。點擊此連結後，系統會將您轉移至**監控**區段中**通知**區段的通知檢視畫面。

關於裝置狀態

Kaspersky Next XDR Expert 會為每個受管理裝置指派一個狀態。特定狀態會根據是否符合使用者定義的條件而指派。在某些情況下，Kaspersky Next XDR Expert 會在為裝置指派狀態時，將裝置在網路上的可見性旗標納入考量（請參閱下表）。如果 Kaspersky Next XDR Expert 在兩小時內未於網路上找到裝置，該裝置的可見性旗標會設為*不可見*。

這些狀態如下：

- *緊急*或*緊急/可見*
- *警告*或*警告/可見*
- *正常*或*正常/可見*

下表列出在指派給裝置的*緊急*或*警告*狀態時必須符合的預設條件，其中包含所有可能的值。

分配狀態到裝置的條件

條件	條件敘述	可用值
安全應用程式未安裝	網路代理已安裝到裝置，但是安全應用程式未安裝。	• 開關按鈕被開啟。 • 開關按鈕被關閉。
偵測到太多病毒	一些病毒被病毒偵測工作在裝置上發現，例如，惡意軟體掃描工作，且發現的病毒數量超過指定值。	大於 0。
即時保護等級不符合管理員設定的等級	裝置在網路中可見，但即時防護等級與管理員在裝置狀態條件中設定的等級不同。	• 已停止。 • 暫停。 • 執行中。
惡意軟體掃描已長時間未執行	裝置在網路中可見且安全應用程式已安裝到裝置，但*惡意軟體掃描*工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於 1 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於 1 天。

條件	條件敘述	可用值
偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。
自重新啟動以來需要的時間	裝置在網路上可見，但應用程式要求重新啟動的時間已超過指定時間間隔。	多於 0 分鐘。
重新啟動的原因	裝置在網路上可見，但應用程式因所選原因之一需要重新啟動裝置。	• 未知原因 • 應用程式在重新啟動前不會執行 • 需要重新啟動以完成更新；應用程式正在執行 • 需要重新啟動以啟動更新 • 需要重新啟動以完成掃描或解毒 • 需要重新啟動以完成遠端安裝/移除 • 即將完成磁碟的資料加密
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到軟體弱點	裝置在網路中可見且網路代理已安裝到裝置，但*弱點掃描和所需更新*工作在裝置應用程式中偵測到指定嚴重等級的弱點。	• 嚴重 • 高。 • 中等。 • 如果弱點無法被修補則略過。 • 如果為安裝分配了更新則略過。
產品授權已到期	裝置在網路中可見，但產品授權已過期。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
產品授權即將到期	裝置在網路中可見，但裝置上的產品授權即將在指定天數內過期。	少於 0 天。
Windows Update 更新檢查已長時間未執行	裝置在網路中可見，但*尋找弱點和所需更新*工作未在指定時間段內未執行。	多於 1 天。
無效的加密狀態	網路代理已安裝到裝置，但裝置加密結果等於指定值。	• 由於使用者拒絕未遵從政策（僅對外部裝置）。 • 由於錯誤未遵從政策。 • 套用政策時需要重新啟動。 • 未指定加密政策。 • 不支援。 • 當套用政策時。
行動裝置設定與政策不同	行動裝置設定不同於 Kaspersky Endpoint Security for Android 政策中指定的設定。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到未處理的安全問題	裝置上發現了一些未處理的安全問題。安全問題可以透過安裝在使用者端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB。
裝置已不受管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。 在這種情況下，安全應用程式的狀態為*stopped*或*failure*，不同於下列狀態：*starting*、*running*或*suspended*。	多於 0 分鐘。
安全應用程式沒有執行	裝置在網路中可見且安全應用程式已安裝到裝置，但其未在執行。	• 開關按鈕被關閉。 • 開關按鈕被開啟。

Kaspersky Next XDR Expert 可讓您設定在符合指定條件時，自動切換管理群組中裝置的狀態。當滿足指定條件時，用戶端裝置會被分配以下狀態之一：*緊急*或*警告*。當不滿足指定條件時，用戶端裝置會被分配*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，預設情況下，若**資料庫已過期**條件的值為**多於 3 天**，則用戶端裝置會被指派*警告*狀態；若值為**多於 7 天**，則會被指派*緊急*狀態。

當 Kaspersky Next XDR Expert 為裝置指派狀態時，對於某些條件（請參閱上表中的「條件說明」欄），會將可見性標記納入考量。例如，若受管理裝置因符合資料庫已過期條件而被指派*緊急*狀態，之後能見度標記也已針對該裝置設定，則裝置會被指派*正常*狀態。

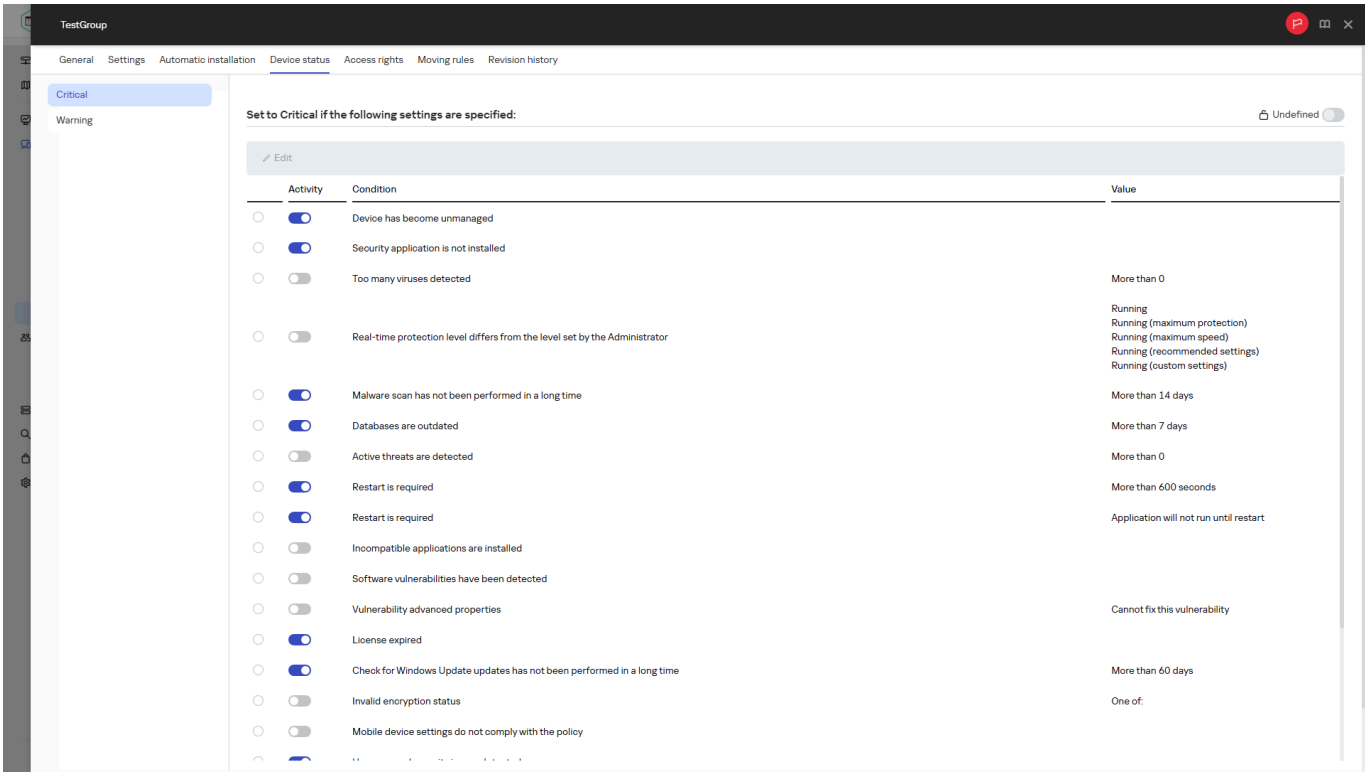
設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 透過以下方式之一，前往要變更切換裝置狀態的管理群組內容：
   - 點擊管理群組的名稱。
   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。

   管理群組內容視窗將開啟。
3. 在屬性視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**緊急**。
5. 在右方窗格中的**如果指定了以下設定，則設定為「緊急」**區段，啟用將裝置切換為*緊急*狀態的條件。



然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。
10. 按一下**儲存**以儲存變更。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**警告**。
5. 在右方窗格中的**如果指定了以下設定則設定為「警告」**區段，啟用將裝置切換為*警告*狀態的條件。

然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。
10. 按一下**儲存**以儲存變更。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

配置通知傳送

您可以配置 Kaspersky Next XDR Expert 中發生之事件的通知。根據選取的通知方法，有以下類型的通知可用：

- 電子郵件—當事件發生時，Kaspersky Next XDR Expert 會將通知傳送至指定的電子郵件地址。
- 簡訊—當事件發生時，Kaspersky Next XDR Expert 會將通知傳送至指定的電話號碼。
- 可執行檔—當事件發生時，可執行文件會在管理伺服器上運行。

若要配置 Kaspersky Next XDR Expert 中發生之事件的通知傳送：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 點擊**通知**區段，並在右窗格選取您需要之通知方法的頁籤：

   - **電子郵件**

     電子郵件標籤允許您透過電子郵件配置事件通知。

     在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

     - IPv4 或 IPv6 位址
     - SMTP 伺服器的 DNS 名稱

     在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

     如果您啟用**使用 DNS MX 尋找**選項，您可以將 IP 位址的多個 MX 記錄用於 SMTP 伺服器的相同 DNS 名稱。相同 DNS 名稱可能有幾個 MX 記錄，具有不同的接收電子郵件的優先次序。管理伺服器嘗試按 MX 記錄優先次序向 SMTP 伺服器傳送電子郵件通知。

     > 如果您啟用**使用 DNS MX 尋找**選項並且不啟用 TLS 設定的使用，我們建議您使用伺服器裝置上的 DNSSEC 設定作為傳送電子郵件通知的額外防護措施。

     如果啟用**使用 ESMTP 身分驗證**選項，則可以在**使用者名稱**和 **密碼**欄位中指定 ESMTP 身分驗證設定。預設情況下，該選項被停用，ESMTP 身分驗證設定不可用。

     您可以用 SMTP 伺服器指定連線的 TLS 設定：

     - **不使用 TLS**

     如果您想停用電子郵件訊息加密，您可以選取此選項。

     - **如果受 SMTP 伺服器支援則使用 TLS**

     如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

     - **始終使用 TLS，檢查伺服器憑證是否有效**

     如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

     > 我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

如果您選取**始終使用 TLS，檢查伺服器憑證是否有效**值，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

您可以透過點擊**指定憑證**連結指定 TLS 連線的憑證：

- 瀏覽 SMTP 伺服器憑證檔案：

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。Kaspersky Next XDR Expert 會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果 SMTP 伺服器的憑證並非從受信任的憑證頒發機構取得，Kaspersky Next XDR Expert 將無法連線到 SMTP 伺服器。

- 瀏覽用戶端憑證檔案：

您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

- X-509 憑證：

您必須指定一個帶有憑證的檔案和一個帶有私密金鑰的檔案。這兩個檔案彼此獨立。檔案的載入順序並不重要。當同時載入兩個檔案時，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

- pkcs12容器：

您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

點擊**傳送測試訊息**按鈕允許您檢查是否正確配置了通知：應用程式傳送測試通知到您指定的郵件信箱。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。

在 **主旨** 欄位中，使用 替代參數輸入電子郵件主旨，例如：`[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`。偵測到威脅時的主旨行範例：`[KSC-SAMARA-1] [Critical] Threat detected`。您可以置此欄位為空。

在**主旨範本**下拉清單中，選取您主旨的範本。選取的範本判定的變數會自動放在**主旨**欄位。您可以選取幾個郵件範本構建郵件主旨。

在**寄件者電子郵件信箱：如果未指定此設定，則將使用收件者信箱。 警告：我們不建議您使用虛構的電子郵件信箱**欄位中，指定寄件者的電子郵件位址。如果您將該欄位置空，收件者信箱被使用。不建議使用虛假郵件信箱。

通知訊息欄位包含事件發生時應用程式傳送的事件資訊標準文字。該文字包含替代參數，例如事件名稱、裝置名稱和網域名稱。您可以透過新增其他帶有更新事件詳情的替代參數編輯訊息文字。

欄位值範例

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

Sender 字串為選用項目。例如，如果您有多個管理伺服器，可以指定通知來源的管理伺服器名稱：Sender - KSC-SAMARA-1。

通知文字的顯示範例：

```
Sender - KSC-SAMARA-1

Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access: root; Object type: File; File owner: user; Detection certainty: Sure; File: /home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

> 如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%”。

點擊**設定通知限制數**連結允許您指定應用程式在指定時間段可以傳送的最大通知數量。

- **SMS**

SMS 頁籤可讓您設定將各種事件的 SMS 通知傳到手機。SMS 訊息透過郵件閘道傳送。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

如果啟用**使用 ESMTP 身分驗證**選項，則可以在**使用者名稱**和 **密碼**欄位中指定 ESMTP 身分驗證設定。預設情況下，該選項被停用，ESMTP 身分驗證設定不可用。

您可以用 SMTP 伺服器指定連線的 TLS 設定：

- **不使用 TLS**

如果您想停用電子郵件訊息加密，您可以選取此選項。

- **如果受 SMTP 伺服器支援則使用 TLS**

如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

- **始終使用 TLS，檢查伺服器憑證是否有效**

如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

如果您選取**始終使用 TLS，檢查伺服器憑證是否有效**值，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

您可以按一下**指定憑證**連結，指定 SMTP 伺服器憑證檔案。您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。Kaspersky Next XDR Expert 會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果 SMTP 伺服器的憑證並非從受信任的憑證頒發機構取得，Kaspersky Next XDR Expert 將無法連線到 SMTP 伺服器。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。通知將被傳送到指定郵件信箱關聯的電話號碼。

在**主旨**欄位，指定電子郵件主旨。

在**主旨範本**下拉清單中，選取您主旨的範本。以已選取範本為依據的變數會放在**主旨**欄位。您可以選取幾個郵件範本構建郵件主旨。

在**寄件者電子郵件信箱：如果未指定此設定，則將使用收件者信箱。 警告：我們不建議您使用虛構的電子郵件信箱**欄位中，指定寄件者的電子郵件位址。如果您將該欄位置空，收件者信箱被使用。不建議使用虛假郵件信箱。

在**SMS 接收者電話號碼**欄位中，指定短信通知接收人的手機號碼。

通知訊息欄位中會包含事件發生時應用程式傳送的事件資訊標準文字。該文字可以包含替代參數，例如事件名稱、裝置名稱和網域名稱。

如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%”。

點擊**傳送測試訊息**檢查是否正確配置了通知：應用程式傳送測試通知到您指定的收件者。

點擊**設定通知限制數**連結指定應用程式在指定時段內可以傳送的最大通知數量。

- **要執行的可執行檔**

可執行檔必須包含您希望管理員接收之事件的環境變數。

在**當事件發生時要在管理伺服器上執行的可執行檔**欄位中，指定要執行的資料夾與檔案名稱。

欄位值範例：

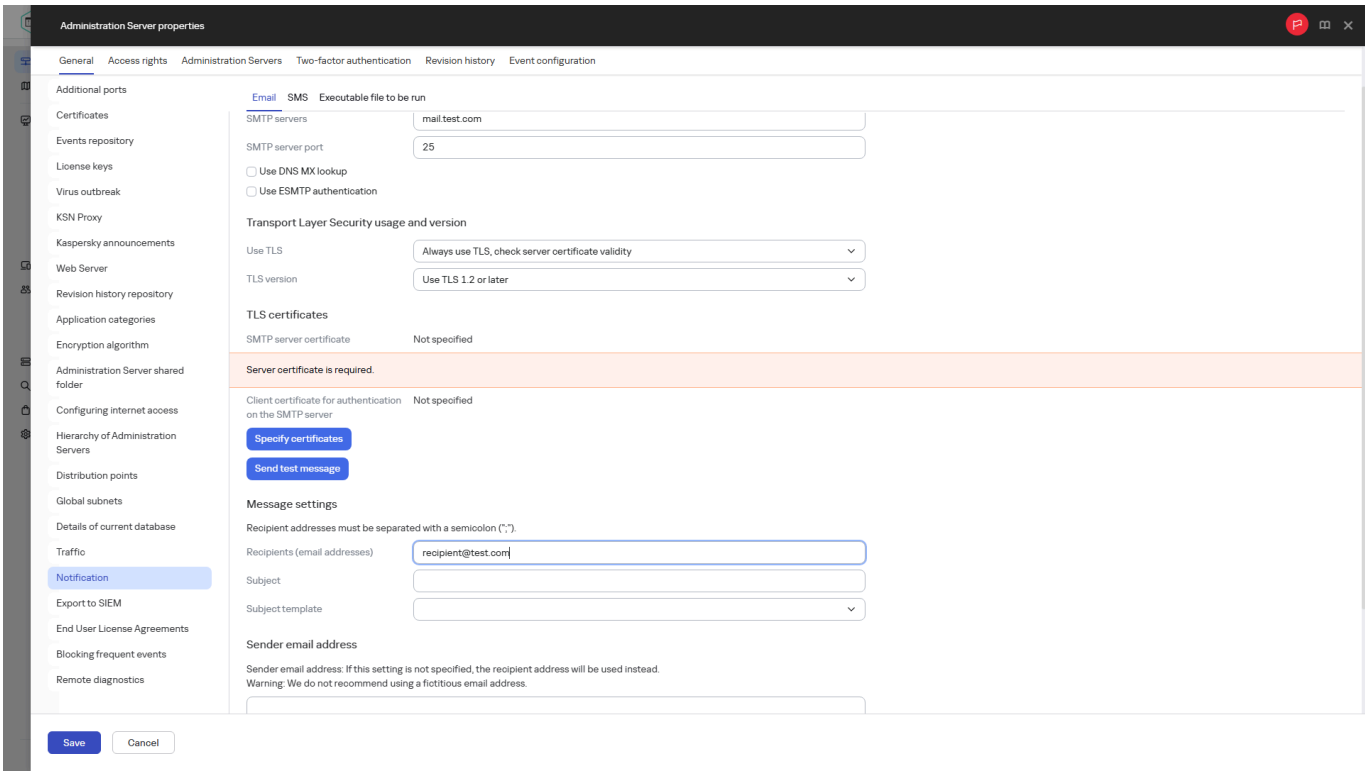
```
/opt/scripts/notifications.sh
```

必須預先準備檔案，並指定代表訊息中所傳送事件資訊的替代參數。資料夾和檔案必須位於管理伺服器上。

測試或偵錯指令碼範例：

```
#!/usr/bin/env bash
touch /tmp/ksc_notification.txt
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

點擊**設定通知限制數**連結允許您指定應用程式在指定時間段可以傳送的最大通知數量。



選取通知方法

3. 在標籤上，定義通知設定。

4. 點擊**儲存**以儲存變更並關閉管理伺服器屬性視窗。

已儲存的通知傳送設定會套用至 Kaspersky Next XDR Expert 中發生的所有事件。

您可在管理伺服器設定、政策設定或應用程式設定的**事件組態**區域覆寫特定事件的通知交付設定。

測試通知

為了檢查事件通知是否可以傳送,程式將在用戶端裝置上使用 Eicar 試病毒偵"測通知。

要驗證事件通知的傳送，請執行以下操作：

1. 停止用戶端裝置上的即時檔案系統防護工作，將 EICAR 測試病毒複製到用戶端裝置。現在，重新啟用檔案系統的即時防護。

2. 為管理群組中的用戶端裝置或指定裝置執行掃描工作，包括帶有 EICAR 測試病毒的裝置。

   如果掃描工作設定正確，會偵測到測試病毒。如果通知設定正確，您將收到偵測到病毒的通知。

要開啟測試病毒偵測記錄：

1. 在主功能表中，轉至 **監控 → 事件分類**。
2. 點擊**最近事件**分類名稱。

   在開啟的視窗中，將顯示有關測試病毒的通知。

EICAR 測試病毒不包含任何危害您裝置的代碼。不過，多數廠商的安全應用程式都將該檔案視為病毒。您可以從 EICAR 官方網站 下載該測試病毒。

用於描述事件的參數和環境變數

設定 Kaspersky Next XDR Expert 事件通知時，您可以使用參數和環境變數來描述事件（請參閱下表）。

如果您選擇執行可執行檔作為通知方法，請在撰寫檔案時使用變數。

如果您想透過電子郵件或 SMS 傳送事件通知，在相應的頁籤上設定通知時，也可以在**主旨**和**通知訊息**欄位中指定變數。

用於描述事件的參數和環境變數

替換參數（用於通知）	環境變數（用於指令碼）	環境變數說明
%SEVERITY%	$SEVERITY	事件嚴重等級。可能的值： • **資訊** • **警告** • **錯誤** • **緊急**
%COMPUTER%	$COMPUTER	發生事件的裝置的名稱。 裝置名稱的最大長度為 256 個字元。
%DOMAIN%	$DOMAIN	發生事件的裝置的網域名稱。
%EVENT%	$EVENT	事件類型的名稱。 事件類型名稱的最大長度為 50 個字元。
%DESCR%	$DESCR	事件敘述。 敘述的最大長度為 1000 個字元。
%RISE_TIME%	$RISE_TIME	事件建立時間。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	工作名稱。 工作名稱的最大長度為 100 個字元。
%KL_PRODUCT%	$KL_PRODUCT	應用程式名稱。
%KL_VERSION%	$KL_VERSION	應用程式版本號。
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	事件嚴重性編號。可能的值： • 1—**資訊** • 2—**警告** • 3—**錯誤** • 4—**緊急**
%HOST_IP%	$HOST_IP	發生事件的裝置的 IP 位址。
%HOST_CONN_IP%	$HOST_CONN_IP	發生事件的裝置的連線 IP。

監控事件來源

本章節提供監控事件來源的資訊。

來源狀態

在KUMA中，您可以監控收集器接收的資料來源的狀態。一台伺服器上可以有多個事件來源，並且一個收集器可以接收來自多個來源的資料。

您可以使用下列欄位集之一來設定事件來源的自動識別：

- 自訂欄位集。您可以按所需順序指定1到9個欄位。TenantID無需單獨指定，系統會自動確定。
- **套用預設對應**—DeviceProduct、DeviceHostName、DeviceAddress、DeviceProcessName。欄位順序無法變更。

  如果事件中的以下欄位不為空，則表示已識別來源：DeviceProduct 字段、DeviceAddress和/或DeviceHostname欄位以及TenantID欄位（您無需指定TenantID欄位，它會自動確定）。DeviceProcessName欄位可以為空。如果DeviceProcessName欄位不為空，且填寫了其他必填欄位，則會識別出新的來源。

  根據非空事件欄位識別事件來源

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID（自動確定）	
+	+			+	來源1已識別
+		+		+	來源2已識別
+	+	+		+	來源3已識別
+	+		+	+	來源4已識別
+		+	+	+	來源5已識別
+	+	+	+	+	來源6已識別
	+	+		+	未識別來源
	+		+	+	未識別來源
		+	+	+	未識別來源
+			+	+	未識別來源

整個安裝僅套用一個欄位集。升級到新的KUMA版本時，將套用預設欄位集。只有具有主管理員角色的使用者才能設定用於識別事件來源的欄位集。儲存對欄位集的變更後，先前識別的事件來源將從KUMA主控台和資料庫中刪除。您可以根據需要還原為使用欄位集來確定預設事件來源。為了使編輯的設定生效，並使KUMA能夠根據新設定開始識別事件來源，您必須重新啟動收集器。

若要識別事件來源：

1. 在主功能表中，轉至**監控 → 來源狀態**。
2. 這將開啟**來源狀態**視窗；在此視窗中，按一下**設定**按鈕。
3. 這將開啟**事件來源偵測設定**視窗；在此視窗中，在**來源偵測的分組欄位**下拉清單中，選擇要用來識別事件來源的事件欄位。

您可以按所需順序指定1到9個欄位。在自訂組態中，KUMA會識別填入了TenantID欄位的來源（您無需單獨指定此欄位，它會自動確定），並且至少填入了一個**用於識別來源的相同欄位**中的欄位。對於數字字段，0被視為空值。如果選擇單一數字欄位來識別來源，且此數字欄位的值為0，則不會偵測到來源。

儲存修改後的欄位集後，將建立一個稽核事件，並從KUMA主控台和資料庫中刪除所有先前識別的來源；指派的政策將會停用。

4. 如果要返回用於識別預設事件來源的欄位列表，請按一下**套用預設對應**。預設欄位順序無法變更。如果以錯誤的順序手動指定欄位，則會顯示錯誤，並且儲存設定按鈕將不可用。正確的預設欄位序列是DeviceProduct、DeviceHostName、DeviceAddress、DeviceProcessName。使用預設事件集識別事件來源的最低組態：DeviceProduct欄位、DeviceAddress和/或DeviceHostName欄位以及TenantID欄位中的非空值（TenantID自動確定）。

5. 按一下**儲存**按鈕。

6. 重新啟動收集器以套用變更，並開始透過指定的欄位清單識別事件來源。

來源識別隨即設定。

若要檢視與事件來源關聯的事件：

1. 在主功能表中，轉至**監控 → 來源狀態**。

這將打開**來源狀態**視窗。

2. 在**事件來源**頁籤上，從清單中選擇事件來源。在**名稱**欄中，從所選事件來源的下拉式清單選擇**過去 <number> 天的事件**。

KUMA會讓您轉至**事件**部分，您可以在其中檢視過去5分鐘內所選來源的事件清單。事件來源識別設定中設定的欄位值會自動在查詢中指定。如有必要，您可以在**事件**部分變更查詢中的時間段，然後再次按一下**執行查詢**以檢視指定時間段的查詢資料。

限制

1. 在設定了預設欄位的組態中，只有當原始事件包含DeviceProduct欄位以及DeviceAddress和/或DeviceHostName欄位時，KUMA才會註冊事件來源。

如果原始事件不包含DeviceProduct欄位以及DeviceAddress和/或DeviceHostName欄位，您可以：

- 在標準化器中設定擴充功能：在標準化器的**擴充功能**頁籤上，選擇**事件**資料類型，指定**來源欄位**設定，對於**目標欄位** ，選擇DeviceProduct + DeviceAddress和/或Deviceost，然後按一下確定。

- 使用擴充規則：選擇**事件**資料來源類型，指定**來源欄位**設定，並在**目標欄位**中選擇DeviceProduct + DeviceAddress和/或DeviceHostName，然後按一下**建立**。建立的擴充規則必須在事件擴充步驟中連結到收集器。

KUMA將執行擴充操作並註冊事件來源。

2. 如果KUMA接收的事件與辨別來源的欄位值相同，則在滿足下列條件的情況下，KUMA會註冊不同的來源：

- 必填欄位的值相同，但為事件確定了不同的租用戶。

- 必填欄位的值相同，但其中一個事件指定了可選的DeviceProcessName欄位。

- 必填欄位的值相同，但這些欄位中的資料大小寫不同。

如果您希望KUMA在同一來源下記錄此類事件，則可以在標準化器中進一步設定欄位。

來源清單在收集器中生成，在KUMA Core中合併，並顯示在程式網頁介面的事件來源清單**頁籤上的來源狀態**下。資料每分鐘更新一次。

傳入事件的速率和數量是受觀察系統狀態的重要指標。您可以設定監控政策，以便自動追蹤變更，並在指標達到特定邊界值時自動建立通知。監控政策顯示在KUMA主控台的**監控**頁籤上的**監控和報告** → 來源狀態下。

觸發監控政策時，將建立監控事件並包含有關事件來源的資料。

事件來源清單

事件來源顯示在**監控** → **來源狀態** → **事件來源**下的表格中。一頁最多可顯示250個來源。您可以透過點選相關參數的列標題並選擇**升序**或**降序**來對表格進行排序。

您可以使用**搜尋**欄位搜尋事件來源。搜尋使用規則運算式（RE2）執行。您也可以透過點選相關列的標頭並選擇要顯示的值，按**狀態**或**監控政策**列過濾表格。

如有必要，您可以設定更新表中資料的間隔。可用更新的週期：**1分鐘**、**5分鐘**、**15分鐘**、**30分鐘**、**1小時**。預設值為**無重新整理**。您可能需要設定更新週期以追蹤對來源清單所做的變更。

檢視事件來源資訊

在**事件來源**頁籤上，事件來源資訊顯示在以下直欄中：

- **狀態**— 事件來源的狀態：
  - 綠色 — 事件接收符合已指派監控政策的限制。
  - 紅色 — 傳入事件的頻率或數量超出了至少一個已指派監控政策中定義的範圍。
  - 灰色 — 監控政策尚未指派給事件來源。

  如果狀態為紅色，則表示產生了監控類型的事件。監控事件在擁有事件來源的租用戶中產生，並傳送到主租用戶的儲存體（儲存體必須已部署在主租用戶中）。如果您有權存取事件來源的租用戶，但無法存取主租用戶，您仍可在主租用戶的儲存體中搜尋監控事件；系統將顯示您可用的租用戶的監控事件。您也可以設定要傳送到任意電子郵件地址的通知。

  表格可以依狀態篩選。

- **名稱**—事件來源的名稱。此名稱是根據事件來源識別設定中設定的欄位值自動產生的。

  您可以將滑鼠懸停在事件來源表中的事件來源名稱上並點選鉛筆圖示來重新命名事件來源。名稱最多可包含128個Unicode字元。

- **主機名稱或IP位址**—如果在事件來源識別設定中指定了DeviceHostName或DeviceAddress欄位，則為事件來源主機的名稱或IP位址。

- **監控政策**—指派給事件來源的監控政策清單。

  如果要按已套用的監控政策篩選事件來源列表，請點選此列的名稱，然後選擇一個或多個監控政策。如有必要，您可以使用**搜尋**欄位在清單中尋找政策。

您可以透過點選事件來源所在行來檢視指派給該事件來源的所有監控政策的資訊。這將開啟一個窗口，顯示監控政策的設定以及每個政策對應的來源狀態。如果為該來源指派了多個監控政策，則此視窗中來源表格中的紅色狀態可讓您識別觸發的政策。您還可以查看哪些政策已啟用、哪些政策已停用，以及已停用的政策何時將再次啟用。

- **串流**—從事件源接收事件的頻率。如果僅向該來源指派了byCount類型的**監控政策**或不同類型的監控政策，則此值顯示為事件數。如果僅向該來源指派了byEPS類型的**監控政策**或未指派任何政策，則此值顯示為每秒事件數。

- **租用戶**—擁有從事件來源接收的事件的租用戶。

管理事件來源

您可以透過選取表格第一列中的核取方塊來選擇一個或多個事件來源。您可以透過選取第一列標題中的核取方塊並選擇**全選**或**在頁面中全選**來一次選擇多個事件來源以執行群組操作。**在頁面中全選**選項僅適用於清單中顯示的事件來源：如果清單中僅顯示1500個來源中的500個，則下載、啟用或停用政策或刪除事件來源的群組操作僅適用於選定的500個來源。如果要對表中的所有來源執行操作，請選擇**全選**。

如果您選擇事件來源，以下按鈕可用：

- **啟用政策**按鈕啟用事件來源的監控政策。您必須在顯示的視窗中選擇政策才能套用它們。

- 您可以使用**停用政策**來停用事件來源的監控政策。停用政策時，您必須選擇政策的停用時間：暫時或永久。

- **更新政策**按鈕會套用為事件來源啟用的監控政策，或變更已指派的監控政策。政策更新後，工作管理器中會啟動一項工作。

  變更指派給事件來源的監控政策後，此按鈕將變為可用。

- 您可以點選**移除**按鈕從表格中移除事件來源。此來源的統計資訊也將被移除。如果收集器繼續從該來源接收資料，則該事件來源將重新出現在表中，但其舊的統計資料將不予考慮。

  如果您想要刪除所有事件來源，但距離上次刷新表已過一段時間，在此期間新增的事件來源可能不會顯示在表中，但無論如何都會被刪除。

  如果您刪除了超過100,000個套用了篩選或搜尋的事件來源，則只會刪除前100,000個事件來源。您可以再次選擇所有已篩選的事件來源並刪除它們，然後重複此操作，直到刪除所有要刪除的事件來源。如果超過100,000個事件來源未套用任何篩選或搜索，您可以透過使用**全選**按鈕選擇來源來刪除它們。

- 您可以點選**CSV**將所選事件來源的資料下載到CSV檔案。

  僅在監控政策已指派至事件來源時，才會下載 `Stream` 欄位；在此情況下，下載的檔案中會指定取自該政策的測量單位。若未指派任何政策，`Stream` 欄位為空屬於預期行為。

- 您可以點選**圖表**按鈕繪製所選事件來源過去七天的傳入事件圖表。您最多可以選擇五個事件來源。
  。

將事件來源資訊下載到CSV檔案

您可以將有關一個或多個事件來源以及套用至它們的監控政策的資訊下載到UTF-8編碼的CSV檔案中。如果將多個監控政策套用至一個來源，則在該來源的檔案中，每個監控政策及其參數都會從新行開始。對於套用於來源的每個監控政策，下列參數將會匯出至檔案：**狀態**、**名稱**、**監控政策**、**下限**、**上限**、**串流**、**租用戶**。

若要將事件來源資訊下載到CSV檔案：

1. 在主功能表中，轉到**監控 → 來源狀態 → 事件來源**，透過選擇相關來源旁邊第一直欄中的核取方塊，在表格中選擇一個或多個事件來源。

   在表格的左下角，您可以找到所選來源的數量以及表格中的來源總數。您最多可以選擇150,000個事件來源。

   您可以透過點擊第一列標題中的核取方塊並選擇以下選項之一來選擇多個事件來源：

   - **全選**以選擇表格所有頁面上的所有事件來源。如果您已使用搜尋功能篩選來源，這將選擇所有符合搜尋查詢的來源。
   - **在頁面中全選**以選擇目前顯示頁面上的所有事件來源。如果您已使用搜尋功能篩選來源，這將選擇目前顯示頁面上所有符合搜尋查詢的來源。

2. 點選表格上方的**CSV**按鈕。

   > 根據瀏覽器視窗的大小，**CSV**按鈕可能位於附加功能表中，您可以透過點選具有三個點的圖示⋮來開啟該選單。

   工作管理器中會建立一個新事件來源匯出工作。

3. 轉到**工作管理器**部分並找到已建立的工作。

   文檔準備就緒後，工作的**狀態**列將顯示**已完成**狀態。

4. 按一下工作類型名稱，然後從下拉清單中選擇**下載**。

包含事件來源資訊的CSV檔案將根據您的瀏覽器設定下載。預設檔名為event-source-list.csv。

檢視傳入事件的動態

您可以檢查過去七天從來源接收的事件的動態，同時考慮所應用的監控政策，使用以下方式之一：

- 檢視單一事件來源的圖表。
- 根據多個（最多五個）來源的圖表繪製圖表。

若要檢視單一事件來源的圖表，請轉至**監控 → 來源狀態 → 事件來源**，然後按一下相關事件來源行中的箭頭圖示 **›** 。傳入事件的圖表顯示在來源行下方。

圖表中的資料顯示如下：

- 資料顯示的是接收事件的日期。最長週期為七天。

  圖表左上角顯示天數，右上角顯示資料顯示週期。您可以點選**<number>天的事件**按鈕前往**事件**部分，檢視所選來源的事件清單。

- X軸表示天數，Y軸表示事件頻率（EPS）。
- 這些行分別表示過去七天內每15分鐘的平均、最大和最小事件數。

  如果要檢視特定時間的事件數，請將滑鼠停留在圖表上的某個點上。系統會顯示一個工具提示，其中包含特定日期和時間的平均、最大和最小事件數。

您也可以基於多個事件來源的圖表繪製傳入事件圖表，例如，如果您需要比較同一類型的事件來源的活動，這些事件來源的行為應該相似，但實際上卻不同。

若要基於多個事件來源的圖形繪製圖表：

1. 在主功能表中，轉至**監控 → 來源狀態 → 事件來源**，然後透過選擇相關源旁邊第一直欄中的核取方塊，在表格中選擇一個或多個事件來源。

   您最多可以同時為5個事件來源繪製圖表。

2. 點擊表格上方的**圖表**按鈕。

   > 根據瀏覽器視窗的大小，**圖表**按鈕可能位於附加功能表中，您可以透過點選帶有三個點的圖示⋮來開啟該功能表。

   顯示的**圖表**窗格包含所有選定來源的傳入事件圖表，以及一個表格，該表格顯示每個來源的當前事件數、最大事件數和平均事件數（基於圖表中的資料計算）。您可以比較所選來源的資料如何隨著時間的推移相互關聯。

   圖表中的資料顯示如下：

   - 資料顯示的是接收事件的日期。最長週期為七天。

     圖表右上角顯示資料顯示週期。

   - X軸表示天數，Y軸表示事件頻率（EPS）。

   - 圖表中的線條表示過去七天中，每15分鐘間隔來自所選事件源的平均傳入事件數量。

   您可以將滑鼠游標停留在圖表上，以檢視每個來源在特定時間的平均事件數。

3. 如有必要，請清除圖表下方表格中您想要隱藏的事件來源旁邊的核取方塊。

4. 如果要顯示圖表的詳盡資訊，請點選雙箭頭 ↙↗ 圖示以全螢幕模式開啟面板並放大圖表。

監控政策

傳入事件的速率和數量是系統狀態的重要指標。例如，您可以偵測到事件過多、過少或根本沒有事件的情況。監控政策旨在偵測此類情況。在政策中，您可以指定下限閾值、可選的上限閾值以及事件計數方式：按頻率或按總數。

政策必須套用至事件來源。您可以將一個或多個監控政策套用至一個來源。套用政策後，您可以在**事件來源清單**頁籤上監控來源的狀態。

用於監控事件來源的政策顯示在**監控 → 來源狀態 → 監控政策**下的表格中。您可以透過點選相關設定的列標題來對表格進行排序。政策清單的最大大小沒有限制。

在**來源**欄位中，您可以按一下**顯示**按鈕以查看套用了該政策的所有事件來源。點擊此按鈕後，您將進入**事件來源**頁籤，來源表格將依所選政策進行篩選。

監控政策的演算法

監控政策依照下列演算法套用至事件來源：

1. 事件流在收集器處進行計數。
2. KUMA Core伺服器每15秒從收集器獲取一次有關串流的資訊。
3. 取得的資料儲存在KUMA Core伺服器上的Victoria Metrics時間序列資料庫中，KUMA Core伺服器上的資料儲存深度為15天。
4. 事件來源的清點每分鐘進行一次。
5. 每個事件來源的串流將根據以下規則單獨計數：
   - 如果事件來源套用了監控政策，則顯示的最大事件數將根據目前套用的監控政策在政策指定的時間間隔內計算。

     根據政策類型，事件串流的數量將依事件數（對於**byCount**政策類型）或按每秒事件數（EPS，對於**byEPS**政策類型）進行計數。您可以在**事件來源**頁籤的串流直欄中找尋已套用政策的串流計數方式。
   - 如果事件來源未套用任何監控政策，則事件串流的數量對應於最後一個值。
6. 應用程式每分鐘檢查一次是否存在必須套用於事件來源或根據監控政策規劃停止的監控政策。
7. 事件串流每分鐘會依據政策的限制條件進行檢查。

如果來自來源的事件流超過監控政策中指定的閾值，則有關此資訊將以以下方式記錄：

- 有關觸發監控政策的通知將會傳送到政策中指定的電子郵件地址。對於每個政策，您也可以配置通知範本。
- 已產生類型為 `5(Type=5)` 的串流監控資訊事件。該事件各個欄位的描述如下表所示。

監控事件的欄位

事件欄位名稱	欄位值
ID	事件的唯一ID。
時間戳	事件時間
類型	稽核事件的類型。對於稽核事件，該值為 `5`（監控）。
名稱	監控政策的名稱。
DeviceProduct	`KUMA`
DeviceCustomString1	通知中 `value` 欄位的值。顯示觸發該通知的指標數值。

產生的監控事件將傳送至下列資源：

- 主租用戶的所有儲存體
- 主租用戶的所有關聯器
- 事件來源所在租用戶的所有關聯器

新增監控政策

若要新增監控政策：

1. 在主功能表中，轉到**監控 → 來源狀態 → 監控政策**，然後按一下**新增政策**，並在顯示的視窗中設定監控政策：

2. 在**政策名稱**欄位中，輸入您要建立的政策的唯一名稱。此名稱必須包含1到128個Unicode字元。

   我們建議選擇一個反映監控政策的設定排程的名稱。

3. 在**租用戶**下拉清單中，選取要擁有該政策的租用戶。您選擇的租用戶決定了監控政策可以涵蓋的特定事件來源。

4. 在**類型**欄位中，選擇下列監控政策類型之一：

   - **依計數**— 按一定時間段內的事件數統計。
   - **by EPS**—按特定時間內每秒事件數（EPS）統計。系統會計算整個時間段的平均值。您也可以追蹤特定時間段內的峰值。

5. 在**計數間隔**欄位中，指定監控政策必須考慮監控來源資料的時間段。您可以使用右側的下拉清單選擇一個值（以分鐘、小時或天為單位）。最大值為14天。

6. 如果您選擇了**by EPS**政策類型，請在**控制間隔（分鐘）**欄位中指定控制時間間隔（以分鐘為單位），在此時間間隔內，事件數量必須超過閾值才能觸發監控政策：

   - 如果在此週期內，所有檢查（每分鐘執行一次）發現串流超過閾值，則觸發監控政策。
   - 如果在此週期內，其中一項檢查（每分鐘執行一次）發現串流在閾值範圍內，則不會觸發監控政策，並且檢查結果計數將被重設。

   如果您未指定測量頻率，則在發現串流超過閾值後立即觸發監控政策。

7. 在**下限**和**上限**欄位中，定義表示正常行為的邊界。超出這些邊界的偏差將觸發監控政策、建立警示並轉發通知。

   下限設定為必填項。

8. 在**評估間隔**欄位中，指定在將政策套用至事件來源時，VMalert服務會向VictoriaMetrics查詢政策資料的頻率。您可以使用右側的下拉清單選擇一個值（以分鐘、小時或天為單位）。預設間隔是 5 分鐘。

   指定評估間隔時，請留意政策排程。例如，如果您將政策設定為每隔幾個小時套用一次，我們不建議設定較短的間隔，這會導致VictoriaMetrics負載過重。

9. 如有必要，在**傳送通知**欄位中，指定必須向其發送有關啟動KUMA監控政策的通知的電子郵件地址。若要新增位址，請在欄位中輸入該位址，然後按**Enter**或按一下**新增**。您可以指定多個電子郵件地址。

   若要轉送通知，必須設定與SMTP伺服器的連線。

10. 在**通知範本**下拉清單中，選擇要用於通知的範本。如有必要，請點選**新建**按鈕開始建立新的通知範本。

    預設情況下，選擇基本通知範本。您可以重置模板選擇並透過點選X圖示切換到基本模板。

11. 在**排程**部分中，配置您希望將監控政策套用至事件來源的頻率。預設情況下，每週每天從00:00到23:59套用該政策。若要設定監控政策計劃，請執行以下操作：

- 如果您希望在每週的特定日期套用監控政策：

  a. 啟用**按每週日期設定排程**切換開關。

  b. 在**每週日期**下拉清單中，選擇您希望將政策套用至來源的日期。

  如果要清除選擇，請點選X圖示。

  c. 在**時間**欄位中，指定政策的開始和結束時間，精確到分鐘。

  政策適用間隔包含其界限；例如，如果結束時間設定為23:59，則政策將一直套用至23:59:59.999。預設間隔為00:00至23:59。開始時間必須早於結束時間。

  d. 若要新增其他週期，請點選**新增期間**按鈕，然後重複步驟b和c。

  您可以新增任意數量的週期。

- 如果您想要每週在特定日曆日期套用監控政策：

  a. 請啟用**按每週日期設定排程**切換開關。

  b. 點選**每月日期**字段，並使用日曆選擇要將政策套用至來源的日期。您可以選擇多日或單日的週期。時段的開始日期必須早於結束日期。

  日期配置時沒有年份值，因此政策將在每年的指定日期套用，直到您刪除此週期為止。如果要清除選擇，請點選X圖示。

  c. 在**時間**欄位中，指定政策的開始和結束時間，精確到分鐘。

  政策適用間隔包含其界限；例如，如果結束時間設定為23:59，則政策將一直套用至23:59:59.999。預設間隔為00:00至23:59。開始時間必須早於結束時間。

  d. 若要新增其他週期，請點選**新增期間**按鈕，然後重複步驟b和c。

  您可以新增任意數量的時間段。

如果您同時按每週幾和每月日期套用了排程，則首先套用每月日期政策。

12. 按一下**新增**。

這將新增監控政策。

編輯監控政策

監控 → 來源狀態 → 監控政策部分顯示已新增的監控政策及其您在建立政策時指定的設定。您可以按一下某個政策以顯示包含其所有設定的側邊欄。如有必要，您可以在此側邊欄中編輯政策設定。

如果將監控政策套用至事件來源，且要編輯某些政策設置，則可能需要更新該政策以套用變更。KUMA會每30分鐘檢查一次是否有任何監控政策需要更新，如果需要，它會自動執行工作來更新這些監控政策。您也可以透過按一下表格頂部的**更新政策**按鈕手動執行更新工作。一項工作會更新所有需要更新的政策。

只有當某些監控政策需要更新時，**更新政策**按鈕才會變成活動狀態。政策是否需要更新的資訊顯示在**政策更新狀態**中的監控政策表中，狀態如下：

- 如果編輯了以下監控政策設定之一，但變更尚未套用於事件來源，則**需要更新**：
  - **政策名稱**
  - **類型**
  - **下限**
  - **上限**
  - **計數間隔**
  - **控制間隔**
  - **評估間隔**
- 在以下任何情況下都**已更新**：
  - 編輯政策後，啟動了應用程式政策的工作，並將變更套用至事件來源。
  - 您編輯了以下政策設定之一，這不需要啟動更新工作：
    - **傳送通知**
    - **通知範本**
    - **排程**

    在這種情況下，編輯的政策設定會在一分鐘後套用至事件來源。**通知範本**設定的變更會立即套用。
  - 修改後的監控政策不會套用至事件來源。

上次將政策套用至事件來源的日期和時間顯示在**上次套用的政策**列中。

> 在政策更新工作運作時，所有使用者都無法使用**更新政策**按鈕。如果其他使用者編輯了需要更新的政策設定，則只有在您重新整理頁面或編輯政策或事件來源後，**更新政策**按鈕才會變成活動狀態。

套用監控政策

若要將監控政策套用至事件來源：

1. 在主功能表中，轉至**監控 → 來源狀態 → 事件來源**，然後透過選擇相關源旁邊第一直欄中的核取方塊，在表格中選擇一個或多個事件來源。您可以透過點選第一列標題中的核取方塊並選擇以下選項之一來選擇多個事件來源：

   - **全選**以選擇表格所有頁面上的所有事件來源。如果您已使用搜尋功能篩選來源，這將選擇所有符合搜尋查詢的來源。
   - **在頁面中全選**以選擇目前顯示頁面上的所有事件來源。如果您已使用搜尋功能篩選來源，這將選擇目前顯示頁面上所有符合搜尋查詢的來源。

   在表格的左下角，您可以找到所選來源的數量以及表格中的來源總數。

   選擇要套用監控政策的事件來源後，工具列上的**啟用政策**按鈕將變成可用。

2. 按一下**套用政策**。

3. 這將開啟**套用政策**視窗；在該視窗中，選擇一個或多個要套用至所選事件來源的監控政策。此表僅列出您可以指派給所選來源的監控政策：屬於相同租用戶或共用租用戶（如果您有權存取）的政策。如果所選事件來源不存在共用政策，且您無權存取共用租用戶，則政策表為空。

   若要選擇所有可用的政策，您可以選取第一列標頭中的核取方塊。您也可以按政策名稱進行上下文搜索，或透過按一下要按其排序的列標題並選擇**升序**或**降序**來對政策進行排序。

   > **來源**、**排程**、**政策更新狀態**和**上次套用的政策**欄位不支援搜尋和排序。

4. 點選**套用**。

5. 在來源表中，按一下**更新政策**以將變更套用至事件來源。

   監控政策將套用至選定的事件來源；這些來源的狀態將變為綠色。套用至來源的政策名稱將顯示在**監控政策**欄位中。同時也會顯示一則訊息，指示已套用政策的來源數量。如果某個事件來源觸發了監控政策，則該來源的新狀態將在您手動重新整理頁面後顯示，或頁面會自動重新整理。我們建議配置自動資料刷新周期，以追蹤來源清單中的變化。

如果您選擇了超過100,000個事件來源並對其套用了一個或多個政策，則這些政策將僅套用於尚未套用這些政策的前100,000個來源。如果您需要將政策套用至其餘來源，可以執行下列其中一項操作：

- 再次選擇所有來源並對其套用政策。
- 依任意參數篩選來源表，使表顯示的來源少於100,000個，然後將政策套用至這些來源。

重複此操作，直到將政策套用至您需要的所有來源。

停用監控政策

若要停用事件來源的監控政策：

1. 在主功能表中，轉至**監控 → 來源狀態 → 事件來源**，然後透過選擇相關源旁邊第一直欄中的核取方塊，在表格中選擇一個或多個事件來源。

   在表格的左下角，您可以找到所選來源的數量以及表格中的來源總數。在清單中選擇要套用監控政策的事件來源後，工具列上將顯示**停用政策**按鈕。

   您可以透過點選第一列標題中的核取方塊並選擇以下選項之一來選擇多個事件來源：

   - **全選**以選擇表格所有頁面上的所有事件來源。如果您已使用搜尋功能篩選來源，這將選擇所有符合搜尋查詢的來源。
   - **在頁面中全選**以選擇目前顯示頁面上的所有事件來源。如果您已使用搜尋功能篩選來源，這將選擇目前顯示頁面上所有符合搜尋查詢的來源。

2. 點選**禁用政策**。

3. 這將開啟**停用政策**視窗；在該視窗中，選擇要為所選事件來源停用的一個或多個監控政策。此表列出了套用至至少一個所選事件來源的所有監控政策。

   若要選擇所有可用的政策，您可以選取第一列標頭中的核取方塊。您也可以使用上下文搜尋或對政策進行排序，方法是按一下要按其對表格進行排序的列標題，然後選擇**升序**或**降序**。

   來源、**排程**、**政策更新狀態**和**上次套用的政策**欄位不支援搜尋和排序。

4. 在政策表上方的設定部分中，執行下列其中一項操作：

   - 如果您想暫停政策，請選擇**在指定時間內**，並指定時間（以分鐘、小時或天為單位），之後所選政策將重新套用至事件源。最大值：
     - 天數：30
     - 小時：743
     - 分鐘：44579
   - 如果要永久停用事件來源的選定政策，請選擇**直到手動啟用**。

   預設選擇**在指定時間內**，值設定為**5分鐘**。

5. 點選**停用**。

6. 在來源表中，按一下**更新政策**以將變更套用至事件來源。

   監控政策將針對選定的事件來源在指定時間內停用或暫停。表中這些來源的狀態將會變更為灰色。將顯示一則訊息，指示已停用政策的來源數。

如果選擇了100,000多個事件來源並為它們停用了一個或多個政策，則僅對套用了這些政策的前100,000個來源停用這些政策。如果您需要停用剩餘來源的政策，可以執行以下操作之一：

- 再次選擇所有來源並停用這些政策。
- 依任意參數篩選來源表，使表格顯示的來源少於100,000個，然後停用這些來源的政策。

重複此操作，直到所有需要的來源的政策已停用。

基於現有政策新增的監控政策

若要根據現有政策建立新的監控政策：

1. 在主功能表中，轉到**監控 → 來源狀態 → 監控政策**，然後選擇要基於新政策的監控政策。

   如有必要，您可以使用**搜尋**欄位在清單中尋找監控政策。搜尋將在以下列中執行：**名稱**、**租用戶**、**類型**、**排程**（日期和時間的名稱）。

2. 按一下**複製政策**。

3. 這將打開**新增政策**窗口，您可以在其中編輯政策設定。

   預設情況下，`- copy` 會附加至新政策的名稱。其餘設定與正在複製的政策相同。

4. 按一下**新增**按鈕以建立新政策。

監控政策是基於現有政策建立的。

刪除監控政策

若要刪除政策，請執行以下操作：

1. 在主功能表中，轉至**監控 → 來源狀態 → 監控政策**，然後選擇要刪除的一個或多個監控政策。

   如有必要，您可以使用**搜尋**欄位在清單中尋找監控政策。搜尋將在以下列中執行：**名稱**、**租用戶**、**類型**、**排程**（日期和時間的名稱）。

2. 按一下**刪除政策**並確認操作。

這將刪除選定的監控政策。

您無法刪除預先定義的監控政策或已指派給資料來源的政策。

卡巴斯基公告

本節說明如何使用、設定和停用卡巴斯基公告。

關於卡巴斯基公告

卡巴斯基公告區段（**監控 → 卡巴斯基公告**）會提供與您的 Open Single Management Platform 版本及受管理裝置上所安裝之受管理應用程式相關的資訊，讓您隨時掌握最新消息。Open Single Management Platform會透過刪除過時的公告並新增資訊來定期更新此部分中的資訊。

Open Single Management Platform僅顯示與目前連線的管理伺服器和安裝在該管理伺服器的受管理裝置上卡巴斯基應用程式的相關公告。對於任何類型的管理伺服器（主要、次要或虛擬），公告會單獨顯示。

管理伺服器必須具有網際網路連線才能接收卡巴斯基公告。

公告包括以下類型的資訊：

- 與安全相關的公告

  與安全相關的公告旨在使網路中安裝的卡巴斯基應用程式保持最新狀態並具有完整功能。公告可能包括有關卡巴斯基應用程式的重要更新、已發現弱點的修復以及解決卡巴斯基應用程式中其他問題的方法資訊。預設情況下啟用與安全相關的公告。如果您不想接收卡巴斯基公告，則可以停用此功能。

  為了向您顯示與您的網路防護配置相對應的資訊，Open Single Management Platform將資料傳送到卡巴斯基雲端伺服器，並僅接收與網路中安裝的卡巴斯基應用程式相關的公告。可以傳送到伺服器的資料集在您安裝管理伺服器時接受的最終使用者產品授權協議中有說明。

- 行銷公告

  行銷公告包括有關卡巴斯基應用程式的特別優惠、廣告和卡巴斯基新聞的資訊。預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到此類公告。您可以透過停用 KSN 停用行銷公告。

  為了僅向您顯示可能有助於防護網路裝置和日常工作的相關資訊，Open Single Management Platform會將資料傳送到卡巴斯基雲端伺服器並接收相應的公告。可傳送到伺服器的資料集在 KSN聲明的“已處理資料”區段中有說明。

根據重要性，新資訊分為以下幾類：

1. 重要資訊
2. 警告
3. 資訊

當卡巴斯基公告區段中出現新資訊時，OSMP主控台會顯示一個與公告的重要性等級相對應的通知標籤。您可以在“卡巴斯基公告”部分中點擊標籤以查看此公告。

如果您不想接收卡巴斯基公告，則可以停用此功能。

停用卡巴斯基公告

卡巴斯基公告部分（**監控 → 卡巴斯基公告**）透過提供與您的Open Single Management Platform和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。如果您不想接收卡巴斯基公告，則可以停用此功能。

卡巴斯基公告包括兩種類型的資訊：與安全相關的公告和行銷公告。

停用與安全性有關的公告：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**卡巴斯基公告**部分。

3. 將切換按鈕切換到**已停用相關安全公告**位置。

4. 點擊**儲存**按鈕。

   卡巴斯基的公告已停用。

預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到行銷公告。您可以透過停用 KSN 來停用此類公告。

停用 KSN 可能會影響使用 KSN 服務的受管理卡巴斯基應用程式。此類應用程式可能無法再與卡巴斯基通訊，以傳送或接收信譽資料、遙測資料或統計資料。

Cloud Discovery

Kaspersky Next XDR Expert 可讓您監控執行 Windows 的受管理裝置使用雲端服務的情況，並封鎖對您視為不需要之雲端服務的存取。Cloud Discovery 會追蹤使用者嘗試透過瀏覽器和桌面應用程式對這些服務進行的存取活動。它還會追蹤使用者嘗試透過未加密連線（例如，使用 HTTP 通訊協定）對雲端服務進行的存取活動。此功能可協助您偵測並制止"影子 IT"使用雲端服務。

僅當您已使用 Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 授權啟用 Kaspersky Next XDR Expert 時，才能使用封鎖功能。

僅當您使用 Kaspersky Endpoint Security 11.2 for Windows 或以上版本時，封鎖功能才可使用。該安全應用程式的更早版本僅能讓您監控雲端服務的使用情況。

您可以啟用 Cloud Discovery 功能，然後選取要啟用該功能的安全政策或設定檔。您也可以分別在每個安全政策或設定檔中啟用或停用該功能。對於您不想讓使用者存取的雲端服務，您可以封鎖對這些雲端服務進行的存取活動。

為了能夠封鎖對不需要的雲端服務進行的存取活動，請確保滿足以下先決條件：

- 使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本。該安全應用程式的更早版本僅能讓您監控雲端服務的使用情況。
- 您已購買 Kaspersky NEXT 產品授權，其層級允許您封鎖對不需要的雲端服務進行的存取活動。詳情請參閱 Kaspersky Next 說明。

Cloud Discovery 小工具和 Cloud Discovery 報告會顯示與嘗試存取雲端服務時成功與遭封鎖的活動有關的資訊。該小工具還會顯示每項雲端服務的風險等級。Kaspersky Next XDR Expert 會從僅受已啟用此功能之安全設定檔保護的所有受管理裝置取得雲端服務使用情況資訊。

使用小工具啟用 Cloud Discovery

Cloud Discovery 功能可讓您向所有受安全政策（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況資訊。僅能對 Kaspersky Endpoint Security for Windows 政策啟用或停用 Cloud Discovery。

有兩種方式啟用 Cloud Discovery 功能：

- 透過使用 Cloud Discovery 小工具。
- 在 Kaspersky Endpoint Security for Windows 政策內容中完成。

  有關如何在 Kaspersky Endpoint Security for Windows 政策內容中啟用 Cloud Discovery 功能的詳細信息，請參閱 Kaspersky Endpoint Security for Windows 幫助的 Cloud Discovery 部分。

請注意，只能在 Kaspersky Endpoint Security for Windows 政策參數中停用 Cloud Discovery 功能。

要能夠啟用 Cloud Discovery，您必須在**一般功能：基本功能**功能區域中具有**寫入**權限。

要使用 Cloud Discovery 小工具啟用 Cloud Discovery 功能：

1. 開啟 Kaspersky Next XDR Expert。
2. 在主功能表中，轉至 **監控 → 控制板**。
3. 在 **Cloud Discovery** 小工具上，點擊**啟用**按鈕。

   如果您安裝了 Kaspersky Endpoint Security for Windows 版本 12.4，請在 Kaspersky Endpoint Security for Windows 政策屬性中啟用 Cloud Discovery 功能。如需取得詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 說明的 Cloud Discovery 區域。

   如果您擁有早於 12.4 版本的 Kaspersky Endpoint Security for Windows，請將 Kaspersky Endpoint Security for Windows 外掛程式更新至版本 12.5。

4. 在開啟的**啟用 Cloud Discovery** 視窗中，選取要啟用該功能的安全政策，然後點擊**啟用**按鈕。

   以下政策設定將自動啟用：**將指令碼注入 Web 流量以與網頁互動**、 **Web 工作階段監控**和**加密連線掃描**。

Cloud Discovery 功能已啟用，且小工具已新增至儀表板中。

在儀表板中新增 Cloud Discovery 小工具

您可以在儀表板中新增 **Cloud Discovery** 小工具，以監控受管理裝置上使用雲端服務的情況。

若要在儀表板中新增 Cloud Discovery 小工具，您必須在**一般功能：基本功能**功能區域中具有 **寫入** 權限。

若要在儀表板中新增 Cloud Discovery 小工具：

1. 開啟 Kaspersky Next XDR Expert。
2. 在主功能表中，轉至 **監控 → 控制板**。
3. 點擊**新增或還原小部件**按鈕。
4. 在可用小工具清單中，點擊**其他** 類別旁邊的箭頭圖示 (>)。
5. 選取 **Cloud Discovery** 小工具，然後點擊**新增**按鈕。

   如果 Cloud Discovery 功能已停用，請依照使用小工具啟用 Cloud Discovery 部分中的說明進行操作。

所選的小工具即會新增到儀表板的尾端。

檢視雲端服務使用情況資訊

您可以檢視 **Cloud Discovery** 小工具，其中會顯示與嘗試對雲端服務進行的存取活動有關的資訊。該小工具還會顯示每項雲端服務的風險等級。Kaspersky Next XDR Expert 只會從受已啟用此功能的安全設定檔保護之所有受管理裝置，取得雲端服務使用情況的相關資訊。

在檢視之前，請確定：

- Cloud Discovery 小工具已新增至儀表板中。
- Cloud Discovery 功能已啟用。
- 您在**一般功能：基本功能**功能區域中具有**讀取**權限。

若要檢視 Cloud Discovery 小工具：

1. 開啟 Kaspersky Next XDR Expert。
2. 在主功能表中，轉至 **監控 → 控制板**。

   Cloud Discovery 小工具會顯示在儀表板中。
3. 在 **Cloud Discovery** 小工具的左側，選取雲端服務類別。

   小工具右側的表格會顯示所選類別中，最多五項最常為使用者所嘗試存取的服務。所謂的嘗試，同時包括了成功和遭封鎖的嘗試。
4. 在小工具的右側，選取特定服務。

   下方的表格會顯示最多十台最常嘗試存取該服務的裝置。在此表中，您可以產生兩種類型的報告：成功存取嘗試的報告和被阻止存取嘗試的報告。

   此外，在此表中您可以阻止特定裝置對雲端服務的存取。

小工具即會顯示所請求的資訊。

在顯示的小工具中，您可以執行以下操作：

- 前往**監控** → **報告**區段以檢視 Cloud Discovery 報告。
- 封鎖或允許存取所選的雲端服務。

只有在您使用 Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 許可證啟動 Kaspersky Next XDR Expert 時，才能使用封鎖功能。只有在您使用 Kaspersky Endpoint Security 11.2 for Windows 或更新版本時，才能使用封鎖功能。
舊版安全應用程式僅允許您監控雲端服務的使用情況。

雲端服務的風險等級

對於每項雲端服務，Cloud Discovery 會向您顯示風險等級。風險等級可幫助您判斷哪些服務不符合組織安全要求。例如，您可以在決定是否封鎖對特定服務的存取活動時，將風險等級納入考慮。

風險等級是一項估計的指數，並未指出任何與雲端服務品質或服務製造商有關的資訊。風險等級純粹為來自 Kaspersky 專家的建議。

在 Cloud Discovery 小工具以及列出所有受監控雲端服務的清單中，會顯示雲端服務的風險等級。

封鎖對不需要的雲端服務進行的存取活動

對於您不想讓使用者存取的雲端服務，您可以封鎖對這些雲端服務進行的存取活動。您也可以允許對先前封鎖的雲端服務進行存取。

您在決定是否封鎖對特定服務進行的存取活動時，除了其他眾多考量，還可以將風險等級納入考慮。

您可以在安全政策或設定檔中封鎖或允許對雲端服務進行的存取活動。

有兩種方法封鎖對不需要的雲端服務進行的存取活動：

- 透過使用 Cloud Discovery 小工具啟用。

  在這種情況下，您可以逐一封鎖對服務的存取。

- 在 Kaspersky Endpoint Security for Windows 政策內容中完成。

  在這種情況下，您可以逐一封鎖對服務的存取，或一次性封鎖整個類別。

  有關如何在 Kaspersky Endpoint Security for Windows 政策內容中啟用 Cloud Discovery 功能的詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 幫助的 Cloud Discovery 部分。

要封鎖或允許透過小工具對雲端服務的存取：

1. 開啟 Cloud Discovery 小工具，然後選取所需的雲端服務。
2. 在**使用服務的前 10 台裝置**中，找到要用於封鎖或允許該服務的安全政策或設定檔。

3. 在所需行的**政策或設定檔中的存取狀態**欄位中，執行以下任一操作：

   - 若要封鎖服務，請在下拉清單中選取**已封鎖**。
   - 若要允許服務，請在下拉清單中選取**允許**。

4. 點擊**儲存**按鈕。

安全政策或設定檔即會封鎖或允許對所選服務進行的存取活動。

匯出到 SIEM 系統的事件

本節將介紹如何配置匯出事件到 SIEM 系統。

設定事件匯出到 SIEM 系統

Kaspersky Next XDR Expert 可讓您透過下列其中一種方法設定將事件匯出至 SIEM 系統：匯出至任何使用 Syslog 格式的 SIEM 系統；匯出至使用 LEEF 和 CEF 格式的 Kaspersky SIEM、QRadar、Splunk、ArcSight SIEM 系統；或直接從卡巴斯基安全管理中心資料庫將事件匯出至 SIEM 系統。完成此情境後，管理伺服器會自動將事件傳送到 SIEM 系統。

先決條件

開始在 Kaspersky Next XDR Expert 中設定事件匯出之前：

- 深入了解事件匯出的方法。
- 確保您有系統設定值。

您可以按任何順序執行此情境的步驟。

將事件匯出到 SIEM 系統的過程包括以下步驟：

- **設定 SIEM 系統以接收來自 Kaspersky Next XDR Expert 的事件**

  說明：配置在 SIEM 系統中的事件匯出

- **選取要匯出到 SIEM 系統的事件**

  標記要匯出到 SIEM 系統的事件。首先，標記發生在所有受管理的卡巴斯基應用程式中的一般事件。然後，您可以標記特定受管理的卡巴斯基應用程式的事件。

- **配置匯出事件到 SIEM 系統**

您可以使用下列方法之一匯出事件：

- 使用 TCP、UDP 或 TLS over TCP 通訊協定。
- 直接從卡巴斯基安全管理中心資料庫匯出事件。卡巴斯基安全管理中心資料庫包含一組公用檢視；您可以在 klakdb.chm 文件中找到這些公用檢視的說明。

結果

如果您選取了要匯出的事件，配置事件匯出到 SIEM 系統後，您可以檢視匯出結果。

先決條件

在 Kaspersky Next XDR Expert 中設定事件自動匯出時，您必須指定 SIEM 系統的部分設定。建議您事先檢查這些設定，以便準備設定 Kaspersky Next XDR Expert。

要成功配置自動傳送事件到 SIEM 系統，您必須知道以下設定：

- **SIEM 系統伺服器位址**

  安裝了目前使用的 SIEM 系統的伺服器的 IP 位址。在您的 SIEM 系統設定中檢查此值。

- **SIEM 系統伺服器連接埠**

  用於在 Kaspersky Next XDR Expert 與您的 SIEM 系統伺服器之間建立連線的連接埠號碼。您必須在 Kaspersky Next XDR Expert 設定以及 SIEM 系統的接收器設定中指定此值。

- **協定**

  用於將訊息從 Kaspersky Next XDR Expert 傳送到您的 SIEM 系統的協定。您必須在 Kaspersky Next XDR Expert 設定以及 SIEM 系統的接收器設定中指定此值。

關於事件匯出

Kaspersky Next XDR Expert 可讓您接收管理伺服器和安裝在受管理裝置上的 Kaspersky 應用程式運作期間所發生之事件的相關資訊。事件資訊儲存在管理伺服器資料庫。

您可以將事件匯出用在處理組織和技術級別的安全問題的中心系統中，提供安全監控服務，以及從不同解決方案合併資訊。即是提供對網路硬體和應用程式生成的安全警告的即時分析的 SIEM 系統，或者安全操作中心 (SOCs)。

這些系統可以從許多來源接收資料，包括網路、安全、伺服器、資料庫和應用程式。SIEM 系統也提供功能以集成監控的資料，以便說明您避免遺失關鍵事件。而且，系統執行相關事件和警告的自動分析以通知管理員安全問題。警告可以透過儀表板實現，或可以透過協力廠商管道傳送，例如郵件。

將事件從 Kaspersky Next XDR Expert 匯出至外部 SIEM 系統的程序涉及兩方：事件傳送者 Kaspersky Next XDR Expert，以及事件接收者 SIEM 系統。若要成功匯出事件，您必須在 SIEM 系統和 Kaspersky Next XDR Expert 中進行設定。您可以先設定任意一端。您可以先在 Kaspersky Next XDR Expert 中設定事件傳送，再設定由 SIEM 系統接收事件，反之亦然。

從 Kaspersky Next XDR Expert 傳送事件的方法

將事件從 Kaspersky Next XDR Expert 傳送至外部系統有三種方法：

- 透過 Syslog 協定傳送事件到任意 SIEM 系統

  使用 Syslog 協定，您可以轉發發生在 Kaspersky EDR Expert 管理伺服器上和受管理裝置上安裝的卡巴斯基應用程式中的任意事件。Syslog 協定是標準訊息記錄協定。您可以用它匯出事件到任何 SIEM 系統。

  為此，您需要標記要轉送到 SIEM 系統的事件。您可以在OSMP主控台中標記事件。只有標記的事件才會被轉送到 SIEM 系統。如果您沒有標記任何內容，則不會轉送任何事件。

- 透過 CEF 和 LEEF 協定將事件傳送到 Kaspersky SIEM、QRadar、Splunk 和 ArcSight 系統

  您可使用 CEF 和 LEEF 協定匯出一般事件。當透過 CEF 和 LEEF 協定匯出事件時，您不必能夠選取指定事件以匯出。相反，所有一般事件都被匯出。若要將Open Single Management Platform事件轉換為CEF和LEEF格式的事件，您需要使用siem_conversion_rules.xml檔案。此檔案包含 Kaspersky Next XDR Expert 事件屬性清單，以及 CEF 和 LEEF 格式事件的對應屬性。此外，siem_conversion_rules.xml 檔案包含用於產生與事件對應的訊息的規則。此檔案隨附於 Kaspersky Next XDR Expert 發佈套件中。

  不同於 Syslog 協定，CEF 和 LEEF 協定不通用。CEF 和 LEEF 是為相應的 SIEM 系統（Kaspersky SIEM、QRadar、Splunk 和 ArcSight）所設計。因此，當您選取透過這些協定匯出事件時，您使用 SIEM 系統所需解析器。

- 直接從 Kaspersky Next XDR Expert 資料庫傳送至任何 SIEM 系統

  以該方法匯出事件可以用於透過使用 SQL 查詢直接從資料庫公共視圖接收事件。查詢結果被儲存到 XML 檔案，可以用於外部系統的輸入資料。僅僅公共視圖中的事件可以被直接從資料庫中匯出。

透過 SIEM 系統接收事件

SIEM 系統必須接收並正確解析從 Kaspersky Next XDR Expert 接收的事件。若要這麼做，您必須正確設定 SIEM 系統。設定取決於特定的 SIEM 系統。然而，有一些設定所有 SIEM 系統的通用步驟，例如設定接收器和解析器。

配置在 SIEM 系統中的事件匯出

將事件從 Kaspersky Next XDR Expert 匯出至外部 SIEM 系統的程序涉及兩方：事件傳送者 Kaspersky Next XDR Expert，以及事件接收者 SIEM 系統。您必須在 SIEM 系統和 Kaspersky Next XDR Expert 中設定事件匯出。

您在 SIEM 系統中指定的設定取決於您使用的系統。通常，對於所有 SIEM 系統，您必須設定接收器和訊息解析器（可選）以解析接收的事件。

設定接收器

若要接收 Kaspersky Next XDR Expert 傳送的事件，您必須在 SIEM 系統中設定接收器。通常，必須在 SIEM 系統指定以下設定：

- **匯出協定**

  訊息傳輸協定，可以是 UDP、TCP 或基於 TCP 的 TLS。此協定必須與您在 Kaspersky Next XDR Expert 中指定的協定相同。

- **連接埠**

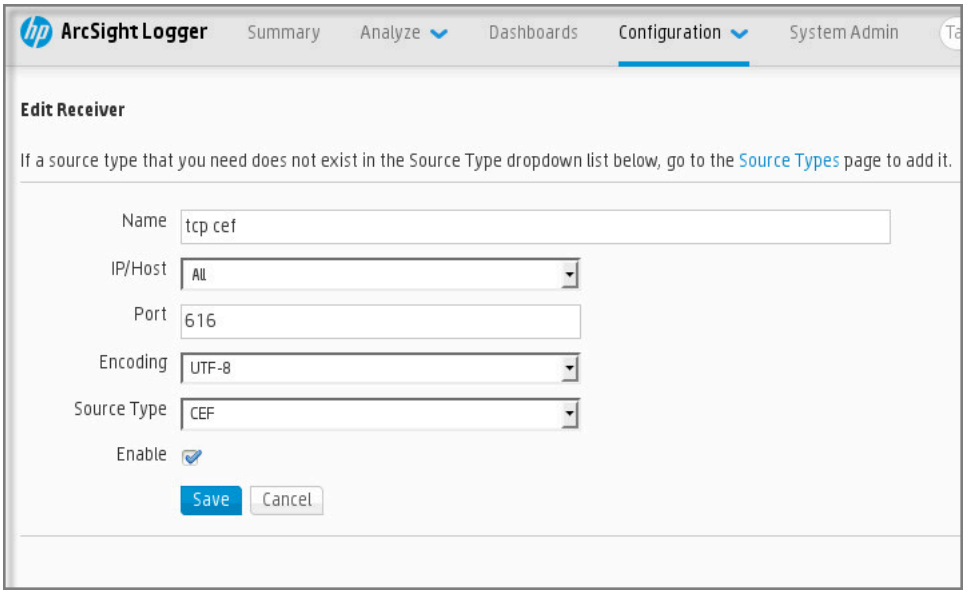
  指定用於連線至 Kaspersky Next XDR Expert 的連接埠號碼。此連接埠必須與您在 Kaspersky Next XDR Expert 中設定與 SIEM 系統的整合時所指定的連接埠相同。

- **日期格式**

  指定Syslog、CEF或LEEF格式。

依據所使用的 SIEM 系統，您可能需要指定一些附加接收器設定。

下圖顯示 ArcSight 的接收器設定截圖。



ArcSight 的接收器設定

訊息解析器

匯出的事件作為訊息被傳遞到 SIEM 系統。接著，系統會將解析器套用至這些訊息，以確保 SIEM 系統可使用事件資訊。訊息解析器是 SIEM 系統的一部分，用於將訊息內容分割為事件代碼、嚴重程度、描述和參數等欄位。這可讓 SIEM 系統處理從 Kaspersky Next XDR Expert 接收的事件，以便將其儲存在 SIEM 系統資料庫中。

標記事件，將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。

- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

對於政策變更事件，您只能啟用或停用將所有此類事件匯出到 SIEM 系統。

關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。

- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出

如果您要匯出發生在特定受管理裝置上安裝的個別受管理應用程式中的事件，標記要在應用程式政策中匯出的時間。在這種情況下，標記的事件將從注冊範圍內的所有裝置中匯出。

若要為特定受管理應用程式標記要匯出的事件：

1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 點擊您要爲其標記事件的應用程式的政策。

   政策設定視窗隨即開啟。
3. 轉到**事件組態**部分。
4. 選取您要匯出到 SIEM 系統的事件旁邊的核取方塊。
5. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**按鈕。

   您還可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。
6. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。
7. 點擊**儲存**按鈕。

受管理應用程式中的標記事件已準備好匯出到 SIEM 系統。

您可以為特定受管理裝置標記要匯出到 SIEM 系統的事件。如果先前匯出的事件在應用程式的政策中標記過，您將不能為受管理的裝置重新定義標記的事件。

若要為受管理裝置標記要匯出的事件：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
   受管理裝置清單隨即顯示。
2. 點擊所需裝置名稱在受管理裝置清單中的連結。
   所選裝置的屬性視窗隨即顯示。
3. 轉到**應用程式**區域。
4. 點擊所需應用程式名稱在應用程式清單中的連結。
5. 轉到**事件組態**部分。
6. 選取您要匯出到 SIEM 系統的事件旁邊的核取方塊。
7. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**按鈕。

   您還可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

8. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。

從現在開始，如果配置了匯出到 SIEM 系統，管理伺服器會將標記的事件發送到 SIEM 系統。

標記一般事件，將其以 Syslog 格式匯出

您可以使用 Syslog 格式標記管理伺服器將匯出到 SIEM 系統的一般事件。

標記一般事件以匯出到 SIEM 系統：

1. 在主功能表中，執行以下操作之一：
   - 按一下管理伺服器名稱。
   - 轉到 **資產管理 → 政策**，然後單擊某個政策的連接。
2. 在開啟的視窗中，請前往**事件組態**頁籤。
3. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**。

   您還可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

4. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。

從現在開始，如果配置了匯出到 SIEM 系統，管理伺服器會將標記的事件發送到 SIEM 系統。

關於使用 Syslog 格式匯出事件

您可以使用 Syslog 格式匯出管理伺服器和受管理裝置上安裝的其他 Kaspersky 應用程式中發生的事件到 SIEM 系統。

Syslog 是訊息記錄協定的標準。它允許分離生成訊息的軟體、儲存訊息的系統和報告和分析訊息的軟體。每個訊息都帶有裝置代碼標籤，指示生成訊息的軟體類型，並被分配嚴重等級。

Syslog 格式由 Request for Comments (RFC) 文件定義，該文件由 Internet Engineering Task Force（網際網路標準）發佈。RFC 5424 標準用於將事件從 Kaspersky Next XDR Expert 匯出至外部系統。

在 Kaspersky Next XDR Expert 中，您可以設定使用 Syslog 格式將事件匯出至外部系統。

匯出過程包含兩個步驟：

1. 啟用自動事件匯出。在此步驟中，Kaspersky Next XDR Expert 會設定為將事件傳送至 SIEM 系統。啟用自動匯出後，Kaspersky Next XDR Expert 會立即開始傳送事件。

2. 選取事件以匯出到外部系統。在該步驟，您可以選取匯出哪些事件到 SIEM 系統。

使用 CEF 和 LEEF 格式匯出事件

您可使用 CEF 和 LEEF 格式，將一般事件、政策變更事件以及由 Kaspersky 應用程式傳輸至管理伺服器的事件匯出至 SIEM 系統。匯出事件集是預定義的，您無法選取要匯出的事件。在將事件傳送至 SIEM 系統（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，必須使用 siem_conversion_rules.xml 檔案中指定的規則，將 Open Single Management Platform 事件解譯為 CEF 和 LEEF 格式的事件。

基於使用的 SIEM 系統選取匯出格式。下表顯示了 SIEM 系統和對應的匯出格式。

匯出事件到 SIEM 系統的格式

SIEM 系統	匯出格式
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- LEEF（日誌事件延伸格式）是 IBM Security QRadar SIEM 專用的事件格式。QRadar 可以接收、識別及處理透過 LEEF 通訊協定傳輸的事件。LEEF 事件必須使用 UTF-8 字元編碼。您可以在 IBM Knowledge Center 檢視 LEEF 協定的詳情。

- CEF（通用事件格式）—開放式日誌管理標準，涉及來自不同的網路裝置和應用程式的安全資訊的協同工作。CEF 允許您使用通用日誌格式，因此資料可以被簡易整合以用企業管理系統分析。CEF 事件必須使用 UTF-8 字元編碼。

自動匯出是指 Kaspersky Next XDR Expert 將一般事件傳送至 SIEM 系統。事件自動匯出在您啟用後立即開始。該部分詳細解釋了如何啟用自動事件匯出。

將事件轉換為 CEF 或 LEEF 格式

在將事件傳送到 SIEM 系統（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 檔案中指定的規則，將 Open Single Management Platform 事件解譯為 CEF 和 LEEF 格式的事件。此檔案包含在Open Single Management Platform分發包中。

siem_conversion_rules.xml 檔案包含將事件轉換為 CEF 和 LEEF 格式的預先定義容器解釋規則。如果想使用額外的事件解釋規則，您可以手動將它們新增至檔案。

siem_conversion_rules.xml檔案包含以下區段：

- `<product name="SP_QRADAR" vendor="IBM">`

  此區段包含用於產生LEEF格式事件的規則，這些事件可以匯出到QRadar SIEM系統。

- `<product name="SP_ARCSIGHT" vendor="HP">`。

  此區段包含用於產生CEF格式事件的規則，這些事件可以匯出到ArcSight或Splunk SIEM系統。

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`。

  此區段包含用於產生CEF格式事件的規則，這些事件可以匯出到KUMA。

每個區段都有 `<common>` 子區段，其中包含 Open Single Management Platform 事件屬性以及 LEEF 格式事件的對應屬性。這些通用屬性用於所有可以匯出的事件類型。

此外，每個區段都有 `<event>` 子區段。每個 `<event>` 子區段都包含額外屬性，這些屬性會新增至 `<common>` 區段中列出的屬性。

您可以手動將新的事件產生規則新增至 siem_conversion_rules.xml 檔案。

若要新增新的事件產生規則：

1. 將新的 `<event>` 子區段新增至 `<product name="SP_QRADAR" vendor="IBM">`、`<product name="SP_QRADAR" vendor="IBM">` 或 `<product name="Kaspersky SIEM" vendor="Kaspersky">` 區段，然後視需要指定額外的事件屬性。

2. 如果事件僅由通用屬性組成，`<event>` 子區段將為空。

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
```

```
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Open Single Management Platform event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

配置 Kaspersky Next XDR Expert 以將事件匯出到 SIEM 系統

若要將事件匯出至 SIEM 系統，您必須在 Kaspersky Next XDR Expert 中設定匯出程序。

在將事件傳送至 SIEM 系統（Kaspersky SIEM、QRadar、ArcSight 或 Splunk）之前，必須使用 siem_conversion_rules.xml 檔案中指定的規則，將 Kaspersky Next XDR Expert 事件轉換為 CEF 和 LEEF 格式的事件。

若要在OSMP主控台中設定匯出至SIEM系統：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽，選擇**匯出至 SIEM**區域。

3. 點擊**設定**連結。

   匯出設定區域將開啟。

4. 在**匯出設定**區域中指定設定：

   - **SIEM 系統伺服器位址**

     安裝了目前使用的 SIEM 系統的伺服器的 IP 位址。在您的 SIEM 系統設定中檢查此值。

   - **SIEM 系統連接埠**

     用於在 Kaspersky Next XDR Expert 與您的 SIEM 系統伺服器之間建立連線的連接埠號碼。您必須在 Kaspersky Next XDR Expert 設定以及 SIEM 系統的接收器設定中指定此值。

- **協定**

  選取該協定用於傳輸訊息到 SIEM 系統。您可以選取TCP、UDP或TLS over TCP通訊協定。

  如果您透過 TCP 通訊協定選取 TLS，則可以指定以下 TLS 設定：

  - **伺服器身分驗證**

    在**伺服器身分驗證**欄位，您可以選擇**受信任的憑證**或者 **SHA 指紋**值：

    - **受信任的憑證**。您可以從受信任的憑證頒發機構 (CA) 接收完整的憑證鏈（包含根憑證），並將該檔案上傳到Open Single Management Platform。Open Single Management Platform會檢查SIEM系統伺服器的憑證鏈是否也由受信任的CA簽署。

      要新增受信任的憑證，請點擊**瀏覽 CA 憑證檔案**按鈕，然後上傳憑證。

    - **SHA 指紋**。您可以在Open Single Management Platform中指定SIEM系統完整憑證鏈（包含根憑證）的SHA1指紋。要新增 SHA1 指紋，請在**指紋**欄位中輸入它，然後點擊**新增**按鈕。

    透過使用**新增用戶端身分驗證**設定，您可以產生憑證來驗證Open Single Management Platform。因此，您將使用Open Single Management Platform的自簽憑證。在此情況下，您可以同時使用受信任的憑證和 SHA 指紋來驗證 SIEM 系統伺服器。

  - **新增主旨名稱/主旨別名**

    主體名稱是接收憑證的網域。如果SIEM系統伺服器的網域與SIEM系統伺服器憑證的主體名稱不符，Open Single Management Platform將無法連線到SIEM系統伺服器。但是，如果憑證中的名稱已變更，則 SIEM 系統伺服器可以變更其網域名稱。在此情況下，您可以在 **新增主旨名稱/主旨別名**欄位中指定主體名稱。如果任何指定的主體名稱與SIEM系統憑證的主體名稱比對，Open Single Management Platform將驗證SIEM系統伺服器憑證。

  - **新增用戶端身分驗證**

    對於用戶端身分驗證，您可以插入您的憑證或在Open Single Management Platform中產生它。

    - **插入憑證**。您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

      - **X.509 憑證 PEM**。在 **包含憑證的檔案** 欄位中上傳憑證檔案，並在 **包含金鑰的檔案** 欄位中上傳私密金鑰檔案。這兩個檔案彼此獨立。檔案的載入順序並不重要。當兩個檔案都上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

      - **X.509 憑證 PKCS12**。上傳包含憑證及其私密金鑰的單個檔案到**包含憑證的檔案**欄位。當兩個檔案都上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

    - **產生金鑰**。您可以在Open Single Management Platform中產生自簽憑證。結果，Open Single Management Platform儲存自簽憑證，您可以將憑證的公共部分或SHA1指紋傳遞給SIEM系統。

- **日期格式**

  您可以根據 SIEM 系統的要求，選擇 Kaspersky SIEM、IBM QRadar SIEM、ArcSight、Splunk 或系統日誌格式。

  如果選擇系統日誌資料格式，則必須指定**最大訊息大小（位元組）**

  指定 SIEM 系統訊息的最大大小。每個事件被一條訊息轉發。如果訊息的精確長度超過指定值，訊息被截斷且資料可能遺失。預設大小是 2048 位元組。如果您在“**Protocol**”欄位中選取了系統日誌格式，則可使用該欄位。

5. 如果需要，您可以從管理伺服器資料庫中匯出封存事件，並設定開始匯出封存事件的開始日期：

   a. 點擊**設定匯出開始日期**連接。

   b. 在開啟的部分中，在**啟動匯出日期自**欄位中指定開始日期。

   c. 點擊**確定**。

6. 啟用**匯出事件至 SIEM**選項。

7. 若要將政策變更事件傳送至SIEM，請啟用**將政策變更的擴充事件匯出至 SIEM**選項。針對每項已變更的政策設定，都會向SIEM傳送一個單獨事件。

8. 若要檢查 SIEM 系統連線是否已配置，請點擊**偵測連線**按鈕。

   與 SIEM 系統伺服器的連線已建立，測試事件已傳送。連線狀態即會顯示。

9. 點擊**儲存**按鈕。

匯出到 SIEM 系統已配置。從現在開始，如果您已在 SIEM 系統中配置事件接收，管理伺服器會將標記的事件或政策變更事件匯出到 SIEM 系統。如果設定匯出的開始日期，管理伺服器也會匯出儲存在管理伺服器資料庫中從指定日期開始的標記事件。

監控政策與政策設定檔變更

政策設定變更時，會產生政策變更事件，您可以接著匯出至 SIEM 系統，以監控政策變更並產生警示。政策變更事件只能透過 SIEM 系統存取。

政策變更事件產生後不會儲存在管理伺服器資料庫中，且無法在 OSMP Console 的 **監控 → 事件分類** 區段中檢視。您也無法在 **事件組態** 索引標籤上指定這些事件的通知設定和儲存設定。

建立政策時，會針對每個政策設定產生政策變更事件。變更政策時，會針對政策中每個已變更的設定產生政策變更事件。刪除政策時，會產生一個事件。例如，建立卡巴斯基安全管理中心政策會產生約 1000 個事件，而建立 Kaspersky Endpoint Security 政策會產生超過 7000 個事件。

產生政策變更事件的條件

在下列情況下會建立政策變更事件：

- 以下應用程式的政策遭到建立、修改或刪除：
  - 卡巴斯基安全管理中心網路代理
  - 卡巴斯基安全管理中心管理伺服器
  - Kaspersky Endpoint Security for Windows 14.1
  - Kaspersky Endpoint Security for Linux 12.5
  - Kaspersky Endpoint Security for Linux 12.4
  - Kaspersky Endpoint Security for Mac 12.2.1。

- 管理伺服器內容中的 **將政策變更的擴充事件匯出至 SIEM** 選項已啟用。
- 政策可透過 OSMP 主控台手動修改。

在下列情況下不會建立政策變更事件：

- 修改一般政策設定。
- 修改從父政策繼承的政策設定。
- 透過 卡巴斯基安全管理中心 OpenAPI 修改政策設定。
- 直接在應用程式中修改卡巴斯基應用程式設定。

政策變更事件欄位

下表顯示一組政策變更事件欄位。這些欄位的表示方式取決於輸出事件格式（例如 Syslog、CEF 或 LEEF）。如需確切的欄位名稱和事件範本，請參閱 siem_conversion_rules.xml 檔案。事件參數僅提供英文版。

事件欄位	資料類型	描述
EventType	字串	事件類型。可針對特定事件類型建立關聯規則。 可能值："Policy created", "Policy modified", "Policy deleted"。
srvName	字串	管理伺服器名稱。
eventTime	日期時間	事件的日期與時間 (UTC)。
eventGroupID	整數	修改事件群組的 ID。
objectID	整數	物件的內部 ID。
objectName	字串	政策顯示名稱。
objectGroup	字串	包含該政策的管理群組完整路徑和名稱。
user	字串	進行修改的使用者名稱。
operation	字串	參數修改類型。 可能值："Added"、"Removed"、"Changed"。
path	字串	參數路徑。包含末端參數父節點的路徑。路徑是根據政策區段和子區段的名稱建立。此路徑結構與網路代理政策設定、一般政策設定及比較政策修訂中所述的路徑結構相同。
parameter	字串	末端參數名稱。
oldValue	字串	末端參數的舊值。
newValue	字串	末端參數的新值。

直接從資料庫匯出事件

您可以直接從 Kaspersky Next XDR Expert 資料庫擷取事件，而不必使用 Kaspersky Next XDR Expert 介面。您可以直接查詢公共視圖並接收事件資料，或基於現有公共視圖建立您自己的視圖並定位它們以獲取您需要的資料。

公共視圖

為方便您使用，Kaspersky Next XDR Expert 資料庫提供了一組公共視圖。您可以在 klakdb.chm 文件中找到這些公共視圖的敘述。

v_akpub_ev_event 公共視圖包含一組展示資料庫中事件參數的欄位集。在 klakdb.chm 文件中，您也可以找到與其他 Kaspersky Next XDR Expert 實體（例如裝置、應用程式或使用者）對應的公共視圖資訊。您可以在您的查詢中使用該資訊。

該部分包含了使用 klsql2 實用程式執行 SQL 查詢的說明以及查詢例子。

要建立 SQL 查詢或資料庫視圖，您也可以使用其他程式以操作資料庫。如需瞭解如何檢視 Kaspersky Next XDR Expert 資料庫的連線參數（例如實例名稱和資料庫名稱），請參閱對應章節。

使用 klsql2 實用程式執行 SQL 查詢

本文旨在說明如何使用 klsql2 公用程式，以及如何使用該公用程式執行 SQL 查詢。請使用已安裝之 Kaspersky Next XDR Expert 版本中隨附的 klsql2 公用程式版本。

要使用 klsql2 公用程式：

1. 轉至安裝管理伺服器的目錄。預設安裝路徑為/opt/kaspersky/ksc64/sbin。
2. 在此目錄中，建立一個副檔名為 .sql 的空白檔案。
3. 在任意文字編輯器中開啟建立的 .sql 檔案。
4. 在 .sql 檔案中，輸入所需的 SQL 查詢，然後儲存該檔案。
5. 在安裝有管理伺服器的裝置上，在命令列，輸入以下指令以從 .sql 檔案執行 SQL 查詢並儲存結果到 result.xml 檔案：

   ```
   sudo ./klsql2 -i src.sql -u <使用者名稱> -p <密碼> -o result.xml
   ```

   其中 <使用者名稱> 和 <密碼> 是有權存取資料庫的使用者帳戶的憑證。
6. 如果需要，輸入有權存取資料庫的使用者帳戶的登入名稱和密碼。
7. 開啟新建立的 result.xml 檔案以檢視 SQL 查詢結果。

您可以編輯 .sql 檔案並建立到公共視圖的任意 SQL 查詢。然後，從命令列，執行您的查詢並儲存結果到檔案。

klsql2 實用程式中的 SQL 查詢例子

該部分顯示 SQL 查詢的例子，透過 klsql2 實用程式執行。

以下例子闡述了對過去七天發生在裝置上的事件的獲取，並依據事件發生時間顯示事件。首先顯示最近的事件。

PostgreSQL 的例子：

```
SELECT
  /* 事件識別器 */
  "e"."nId",

  /* 事件發生的時間 */
  "e"."tmRiseTime",

  /* 事件類型的內部名稱 */
  "e"."strEventType",

  /* 事件的顯示名稱 */
  "e"."wstrEventTypeDisplayName",

  /* 事件的顯示描述 */
  "e"."wstrDescription",

  /* 事件的顯示描述 */
  "e"."wstrGroupName",

  /* 發生事件的裝置的顯示名稱 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 發生事件的裝置的 IP 位址 */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 或 MariaDB 的例子：

```
SELECT

  /* 事件識別碼 */
  `e`.`nId`,

  /* 事件發生的時間 */
  `e`.`tmRiseTime`,

  /* 事件類型的內部名稱 */
  `e`.`strEventType`,

  /* 事件的顯示名稱 */
  `e`.`wstrEventTypeDisplayName`,

  /* 事件的顯示描述 */
  `e`.`wstrDescription`,

  /* 裝置群組名稱 */
  `e`.`wstrGroupName`,

  /* 發生事件的裝置的顯示名稱 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 發生事件的裝置的 IP 位址 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

檢視 Kaspersky Next XDR Expert 資料庫名稱

如果您想要透過 MySQL 或 MariaDB 資料庫管理工具存取 Kaspersky Next XDR Expert 資料庫，則必須知道資料庫名稱，才能從 SQL 指令碼編輯器連線至該資料庫。

若要檢視 Kaspersky Next XDR Expert 資料庫名稱：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選擇**目前資料庫詳細資訊**區域。

   資料庫名稱在**資料庫名稱**欄位中指定。使用資料庫名稱在您的 SQL 查詢中定位資料庫。

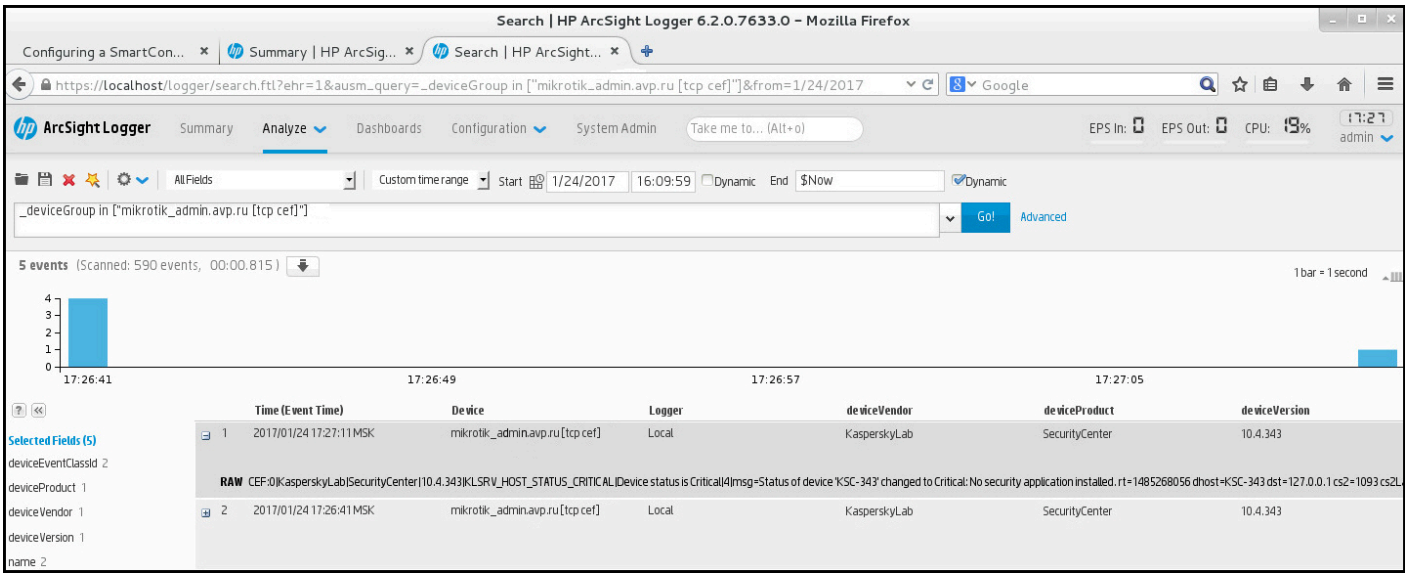
檢視匯出結果

您可以控制事件匯出過程的成功完成。為此，檢查帶有匯出事件的郵件是否被您的 SIEM 系統接收。

如果您的 SIEM 系統能夠接收並正確剖析 Kaspersky Next XDR Expert 傳送的事件，表示雙方的設定皆已正確完成。否則，請將您在 Kaspersky Next XDR Expert 中指定的設定與 SIEM 系統中的設定進行核對。

下圖顯示匯出到 ArcSight 的事件。例如，第一個事件是緊急的管理伺服器事件：「*Device status is Critical*」。

匯出事件在您 SIEM 系統中的顯示隨您使用的 SIEM 系統而不同。



例子事件

將事件從OSMP收集器傳送到外部SIEM系統收集器

若要設定向外部SIEM系統的收集器傳送事件，必須符合下列條件：

1. 您必須使用具有「主管理員」權限的使用者帳戶登入 OSMP 主控台。
2. 在OSMP中，必須將**[OOTB]Kaspersky EDR**收集器安裝在Kubernetes叢集內。
3. KUMA中必須安裝具有以下元件的收集器：
   - 啟用TLS且使用\n分隔符號的**TCP**類型連接器。
   - 不帶對映且包含原始事件的**json**類型規範化器。
   - **儲存體**類型的目標。
4. 必須有安裝了curl和openssl公用工具的Unix終端。

設定將事件從OSMP收集器匯出到外部SIEM系統的收集器涉及以下步驟：

1. **取得用於將事件傳送至 [OOTB]Kaspersky EDR收集器的憑證和金鑰**

   1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
   2. 點選**根租用戶**，然後轉至**設定→憑證**子區段。
   3. 選取TLS憑證旁的核取方塊，然後按一下**匯出**。
   4. 這將打開一個視窗；在該視窗中，輸入密碼並點擊**匯出**按鈕。

      憑證將以PFX格式下載到您的預設下載目錄。
   5. 執行以下命令，擷取下載的憑證，取得cert.pem檔案和key.pem檔案：

      ```
      openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out cert.pem && \
      openssl pkcs12 -in certificate.pfx -nocerts -nodes -out key.pem
      ```

      輸入並重新輸入匯出PFX憑證時指定的密碼。

   取得用於向收集器發送事件的cert.pem憑證和key.pem金鑰。

2. **建立並設定用於將事件匯出到外部SIEM系統的TCP目標**

   1. 在主應用程式視窗中，轉至**監控→資源和服務→活動服務**區段。
   2. 選擇**[OOTB]Kaspersky EDR**收集器。
   3. 在顯示的收集器編輯視窗中，選擇**路由**頁籤，然後按一下**新增**按鈕。
   4. 建立目標：

      a. 在**基本設定**頁籤上，在**類型**下拉清單中，選擇**tcp**。

      b. 在**URL**欄位中，指定要建立連線的URL。例如：<KUMA收集器主機名稱>:<KUMA收集器連接埠>。

c. 轉至**進階設定**頁籤。

d. 在**TLS模式**下拉清單中，選擇**啟用**。

e. 在**分隔符號**下拉清單中，選取**\n**。

f. 按一下**儲存**按鈕。

5. 選擇**設定驗證**頁籤，然後按一下**儲存並重新啟動服務**按鈕。

6. 關閉收集器編輯視窗。

用於將事件匯出到外部SIEM系統的啟用TLS模式的TCP目標隨即設定。

3 取得[OOTB]Kaspersky EDR收集器的連接器閘道URL

1. 在**監控→資源與服務→活動服務**部分，以滑鼠右鍵按一下**[OOTB]Kaspersky EDR**收集器，然後在快顯表單中選擇**部署**。

2. 這將開啟一個視窗；在該視窗中，複製**連接器閘道URL**設定的值。

4 向[OOTB]Kaspersky EDR收集器發送測試事件

1. 在您的終端中執行以下命令：

```
curl -w "%{http_code}\n" -X POST \
--cert cert.pem \
--key key.pem \
-H "Content-Type: application/json" \
--data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \
https://<Connector gateway URL> -k
```

2. 將 `<Connector gateway URL>` 取代為您先前複製的 **連接器閘道 URL** 設定值。

範例

```
curl -w "%{http_code}\n" -X POST \
--cert cert.pem \
--key key.pem \
-H "Content-Type: application/json" \
--data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \
https://in.mbpeo8s3rqnmjqt8z56cysb9w.kuma.xdr-name.kuma.avp.ru:443 -k
```

您可以在終端看到回應代碼200。該事件已傳送至外部SIEM系統的收集器。

5 檢查事件是否已到達外部SIEM系統

1. 使用具有主管理員權限的使用者帳戶登入 KUMA Web 介面。

2. 轉至**事件**區段。

3. 在**KL_HostOsFamily**欄位中找尋值為**Test_send_to_external_SIEM_collector**的事件。

Raw欄位的範例內容


```
{
  "ID":"fca85cda-f760-48a8-8060-382bbaf7af14",
  "Timestamp":1776534533425,
  "TenantID":"d22648f7-bd98-4f55-a7ca-90b51f4d3fae",
  "ServiceID":"efd93e7c-1f8c-4035-bc76-a6efdd72197f",
  "ServiceName":"[OOTB] Kaspersky EDR",
  "Priority":0,
  "SpaceID":"",
  "DeviceTimeZone":"+03:00",
  "EndTime":1776534533425,
  "DeviceReceiptTime":1776534533425,
  "Type":1,
  "Extra":{
    "Product":"EDR"
  },
  "S":{
    "KL_HostOsFamily":"Test_send_to_external_SIEM_collector",
    "KL_Product":"EDR"
```


該事件已到達外部SIEM系統的收集器。

管理物件修訂

該區域包含了物件修訂管理的資訊。Kaspersky Next XDR Expert 可讓您追蹤物件的修改。您每次儲存變更到物件時，*修訂被建立*。每個修訂都有一個數字。

支援修訂管理的應用程式物件包括：

- 管理伺服器內容
- 政策
- 工作
- 管理群組
- 使用者帳戶
- 安裝套件

您可以對物件修訂採取以下操作：

- 檢視已選取的修訂（僅適用於政策）
- 將對物件所做的變更回溯到選取的修訂
- 將修訂儲存為 JSON 檔案（僅適用於政策）

在支援修訂管理的任何物件的內容視窗中，**變更歷史**區域會顯示含有以下詳情的物件修訂清單：

- **修訂** — 物件修訂版本。
- **時間** — 物件修改的日期和時間。
- **使用者** — 修改物件的使用者的名稱。

- **使用者裝置 IP 位址** — 從中修改物件之裝置的 IP 位址。
- **網頁主控台 IP 位址**—用於修改物件的OSMP主控台的IP位址。
- **動作** — 對物件執行的操作。
- **描述** — 與物件設定變更相關的修訂敘述。

  預設下，物件修訂敘述為空。若要為某次修訂新增說明，請選取該修訂，然後點擊**編輯描述**按鈕。在開啟的視窗中，輸入修訂敘述的部分文字。

檢視並儲存政策修訂

Open Single Management Platform可讓您檢視在特定時間段內對政策進行了哪些修改，並將這些修改的相關資訊儲存在檔案中。

如果對應的管理 Web 外掛程式支援此功能，則可以檢視和儲存政策修訂。
這些選項適用於管理伺服器、網路代理、Kaspersky Endpoint Security for Windows（自 Web 外掛程式 14.0 版起）、Kaspersky Endpoint Security for Linux（自 Web 外掛程式 12.4 版起），以及 Kaspersky Endpoint Security for Mac（自 Web 外掛程式 12.2.1 修補程式 A 版起）的政策。

檢視政策修訂：

1. 在主功能表中，前往**資產管理 → 政策**。
2. 按一下要檢視修訂的政策，然後前往**變更歷史**區域。
3. 在政策修訂清單中，按一下要檢視的修訂編號。

   如果修訂大小超過10MB，您將無法使用OSMP主控台檢視它。系統將提示您將已選取的修訂儲存到 JSON 檔案。

   如果修訂大小未超過 10 MB，則會顯示 HTML 格式的報告，其中包含已選取政策修訂的設定。由於報告會顯示在彈出視窗中，請確保您的瀏覽器允許彈出視窗。

對於 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Mac 的政策，報告將不包含政策設定檔資訊。

若要將政策修訂儲存到 JSON 檔案，

在政策修訂清單中，選取要儲存的修訂，然後點擊**儲存到檔案**。

修訂將儲存到 JSON 檔案。

如有必要，您可以比較政策修訂版本。

比較政策版本

您可以將政策的歷史版本與其目前版本進行比較，比較清單中選定的不同版本，或將一個政策的版本與另一個政策的版本進行比較。此選項適用於管理伺服器、網路代理程式、Kaspersky Endpoint Security for Windows（14.0及更高版本的網頁外掛程式）和 Kaspersky Endpoint Security for Mac （12.2.1 Patch A及更高版本的網頁外掛程式）。

若要比較政策版本：

1. 在主功能表中，轉至**資產管理→政策**。
2. 按一下要比較其版本的政策。
   政策設定視窗隨即開啟。
3. 前往**變更歷史**頁籤，然後選取要比較的版本旁的核取方塊。
4. 在工具列中，按一下**比較**按鈕，然後從下拉清單中選擇以下選項之一：
   - **與目前版本比較**，如果您想將在步驟3中選擇的版本與相同政策的上次儲存版本進行比較。
   - **與選定版本比較**，若要比較步驟3中選取的兩個版本。

     核取方塊的選擇順序不會影響比較結果。預設情況下，會將所選版本的較早版本與最新版本進行比較。例如，若選取版本5和版本1旁邊的核取方塊，則會將版本1與版本5進行比較。報告將包含版本1中相對於版本5新增、刪除或變更的設定資訊。

   - **與其他政策版本比較**，若要比較兩個不同政策的版本。
     在開啟的右側窗格中，執行以下操作：
     a. 在**應用程式名稱**欄位中，選擇要比較的政策：網路代理程式或管理伺服器。
     b. 在**政策名稱**欄位中，指定要與步驟3中所選的政策版本進行比較的政策名稱。
        政策版本清單隨即顯示。
     c. 選取所需的版本，然後點擊**比較**按鈕。

版本比較報告將以HTML格式顯示在瀏覽器的新頁籤中。

如果比較結果超過10MB，則會顯示對應的對話方塊。您可以點擊**儲存到檔案**按鈕將報告儲存為檔案，或取消操作。

報告將以OSMP主控台的介面語言顯示。您可以透過點擊該部分旁邊的向下箭頭圖示（ ）來展開報告的某些部分，或者透過點擊向上箭頭（ ）圖示來摺疊該部分。

報告包含以下資訊：

- 卡巴斯基標誌。
- 報告名稱。
- 報告建立時間和日期。
- 政策名稱、管理伺服器和管理群組，其中包括比較版本的政策。
- **另存為HTML**按鈕。點擊此按鈕，報告將儲存到您的電腦。
- **摘要**部分顯示有關比較版本的常規資訊：政策名稱、版本號、版本儲存的時間和日期、儲存版本的使用者以及版本描述

  對於繼承的政策，不顯示使用者。

- 比較版本之間的差異。差異顯示在以下部分：
  - **新增的設定**
  - **刪除的設定**
  - **變更設定**
  - **僅適用於物件 1 的設定**（如果您比較了兩個不同政策的修訂版本）
  - **僅適用於物件 2 的設定**（如果您比較了兩個不同政策的修訂版本）

  如果某個部分沒有資料，則不會顯示該部分。

對於 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Mac 的政策，版本比較報告將不包含政策設定檔資訊。

回溯物件到先前修訂

如果必要，您可以回溯對物件所做的變更。例如，您可能必須轉換政策設定到特定日期的狀態。

要回溯對物件所做的變更：

1. 在物件的內容視窗中，開啟**變更歷史**頁籤。
2. 在物件修訂清單中，選取您必須復原的修訂。

3. 點擊**回溯**按鈕。

4. 點擊**確定**以確認操作。

該物件被回溯到所選修訂。物件修訂清單顯示所做的操作記錄。修訂敘述顯示了您轉換物件所到的修訂號的資訊。

復原操作僅適用於政策和工作物件。

物件刪除

本節提供有關刪除物件的資訊。

您可以刪除物件，包括以下：

- 政策
- 工作
- 安裝套件
- 虛擬管理伺服器
- 使用者
- 安全群組
- 管理群組

要刪除物件：

1. 開啟OSMP主控台的所需部分，然後選取物件。

2. 在工具列上，點擊**刪除**按鈕。

3. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

所選物件被刪除。

當您刪除物件時，其資訊保留在資料庫。已刪除物件的資訊的儲存期與物件修訂的儲存期一致（建議期限是 90 天）。只有當您在權限的**已刪除物件**區域有**修改**權限時才可變更儲存期。

關於刪除用戶端裝置

當您從管理群組中刪除受管理裝置時，應用程式會將裝置移至未分配的裝置群組。然後選取您需要執行測試更新安裝的裝置刪除裝置後，已安裝的卡巴斯基應用程式——網路代理和任何安全應用程式，例如 Kaspersky Endpoint Security ——將保留在裝置上。

卡巴斯基Next XDR Expert根據以下規則處理「未分配裝置」群組中的裝置：

- 如果您配置了裝置移動規則，並且裝置符合移動規則的條件，則該裝置會被根據規則自動移動到管理群組。
- 裝置會被儲存在未分配的裝置群組中，並被根據裝置保留規則自動從群組中刪除。

  裝置保留規則不會影響具有一個或多個使用完整磁碟加密進行加密的磁碟機的裝置。此類裝置不會被自動刪除——您只能手動刪除它們。如果您需要刪除帶有加密磁碟機的裝置，請先解密磁碟機，然後再刪除該裝置。

  > 當您刪除帶有加密磁碟機的裝置時，解密磁碟機所需的資料也會被刪除。如果您在刪除此類裝置（不論是從**未指派的裝置**或**受管理裝置**群組）時開啟的確認視窗中選取**我了解風險並希望刪除所選裝置**核取方塊，則表示您已知悉後續會有資料被刪除。

  想解密磁碟機，必須滿足以下條件：

  - 裝置被重新連線到管理伺服器以還原解密磁碟機所需的資料。
  - 裝置使用者記得解密密碼。
  - 用於加密磁碟機的安全應用程式（例如 Kaspersky Endpoint Security for Windows）仍安裝在裝置上。

  如果磁碟機由 Kaspersky Disk Encryption 技術加密，您還可以嘗試使用 FDERT Restore Utility 還原資料.

> 在 VDI 中，如果您的裝置有加密磁碟機，則刪除該裝置後，加密磁碟機上的資訊也會被刪除。

當您從未分配的裝置群組中手動刪除裝置時，應用程式會從清單中刪除該裝置。刪除裝置後，已安裝的卡巴斯基應用程式（如果有）將保留在裝置上。然後，如果裝置仍然可以被管理伺服器看到，且您已經配置了定期的網路輪詢，卡巴斯基Next XDR Expert會在網路輪詢過程中發現該裝置，並將其重新添加回「未分配裝置」群組。因此，最好僅當裝置對管理伺服器不可見時再手動刪除該裝置。

從隔離區和檔案備份下載和刪除檔案

本章節提供有關如何從OSMP主控台的隔離區和檔案備份中下載和刪除檔案的資訊。

從隔離區和檔案備份區下載檔案

僅當滿足以下兩個條件之一時，您才能從隔離和備份區下載檔案：裝置設定中啟用了**不斷開與管理伺服器的連線**選項，或者正在使用連線閘道。否該下載將無法完成。

要將隔離區或檔案備份中的檔案備份儲存到硬碟磁碟機，請執行以下操作：

1. 執行以下操作之一：

   - 如果要從隔離區儲存檔案副本，請在主功能表中，轉到**操作→ 儲存區 → 隔離**。
   - 如果要從備份儲存檔案副本，請在主功能表中，轉到**操作→ 儲存區 → 檔案備份**。

2. 在開啟的視窗中，選擇要下載的檔案，然後點擊**下載**。

   下載開始。

如果您從**隔離**部分執行了該操作，則會將放置在用戶端裝置隔離目錄中的檔案副本下載到您的電腦。檔案保存在受密碼保護的ZIP封存檔案中。密碼如下：infected。

關於從隔離區、檔案備份區或主動威脅儲存路中刪除物件

當安裝在用戶端裝置上的卡巴斯基安全應用程式將物件放入**隔離**、**檔案備份**或**活動威脅**部分時，它們會將有關新增物件的資訊傳送到Open Single Management Platform的隔離區、備份區或活動威脅儲存體。開啟其中一個部分時，您可以刪除所需的物件。

對於**檔案備份**或**活動威脅**部分，從清單中選擇一個物件，然後按一下**刪除**按鈕。

對於**隔離**，您可以進行以下操作之一：

- 選取要刪除的物件名稱旁的核取方塊，然後在工具列中按一下**刪除**按鈕。
- 點擊要刪除的物件名稱，然後在開啟的詳細資料視窗的工具列中點擊**刪除**按鈕。

  在這種情況下，物件將被刪除，螢幕上會顯示相應的通知，詳細資料視窗會關閉。

Open Single Management Platform會從清單中移除所選物件，或從儲存庫中刪除所選物件。要執行的操作由將選定物件放置到存放庫的卡巴斯基應用程式定義。卡巴斯基應用程式在"**項目新增者**"欄位中指定。

有關要執行的操作的詳細資訊，請參閱卡巴斯基應用程式的文件。

上傳檔案以進行掃描

您可以上傳文件，然後立即或稍後進行掃描。Kaspersky Next XDR Expert使用反惡意軟體引擎和YARA技術進行掃描，並將檔案傳送到沙盒。

若要上傳文件進行掃描：

1. 在主功能表中，前往 **操作 → 儲存區 → 檔案**。
2. 點擊**上傳**。

   文件檔案視窗隨即打開。

3. 選擇要與該檔案關聯的租用戶。

4. 如果您希望檔案上傳完成後立即進行掃描，請確保**上傳後掃描**切換按鈕已開啟。您可以關閉此切換按鈕，稍後再掃描檔案。

5. 您可以透過拖放或點擊**上傳檔案**來上傳檔案。您可以上傳多個檔案。

6. 點擊**上傳**。

Kaspersky Next XDR Expert隨即開始上傳檔案。上傳完成後，如果**上傳後掃描**切換按鈕處於開啟狀態，Kaspersky Next XDR Expert將開始掃描。

手動掃描檔案儲存庫中的檔案

如果檔案尚未掃描或您想重新掃描該檔案，您可以手動開啟掃描。Kaspersky Next XDR Expert使用反惡意軟體引擎和YARA技術進行掃描，並將檔案傳送到沙盒。

若要掃描檔案儲存庫中的檔案：

1. 在主功能表中，前往 **操作 → 儲存區 → 檔案**。

2. 在清單中選擇一個或多個檔案。

3. 點選清單上方的**掃描**按鈕。

Kaspersky Next XDR Expert隨即開始掃描選定的檔案。您可以在**掃描狀態**直欄中找到掃描狀態。

檢視掃描狀態和掃描結果

若要檢視檔案掃描的狀態和結果：

1. 在主功能表中，轉至**操作 → 儲存區 → 檔案**。

   檔案清單中的**掃描狀態**欄位包含有關掃描狀態和結果的基本資訊：

   - **未掃描**

     檔案尚未掃描。

   - **正在掃描**

     正在掃描檔案。

   - **未偵測到**

     檔案已掃描，未偵測到威脅。

   - **偵測日期**

     已掃描文件，偵測到一些威脅。

2. 要了解更多詳細信息，請單擊要了解更多信息的檔案名稱。

   在打開的視窗中，您可以找到有關該檔案的信息，包括檔案掃描的詳細結果。

Kaspersky Next XDR Expert元件的運行診斷

本章節介紹如何取得Kaspersky Next XDR Expert元件的診斷資訊。

取得Kaspersky Next XDR Expert元件的日誌檔案

KDT可讓您取得包含Kaspersky Next XDR Expert元件和Kubernetes叢集的診斷資訊的日誌文件，以便您自行或在卡巴斯基技術支援的協助下解決問題。

Kaspersky Next XDR Expert根據下列範本產生日誌檔案名稱：pod_name.container_name.log。其中，pod_name是Kubernetes pod名稱，container_name是Kubernetes容器名稱。

要取得Kaspersky Next XDR Expert元件和管理網頁外掛程式的日誌檔案，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt logs get <flags>
```

其中 `<flags>` 為命令參數，可用於設定日誌記錄結果。

您可以指定以下日誌記錄參數：

- `--app` < 元件清單 > — 取得所列Kaspersky Next XDR Expert元件的日誌。
  例如，如果要取得管理伺服器最近一小時的日誌，請執行以下命令：
  `./kdt logs get --app ksc`
  Kaspersky Next XDR Expert可用元件清單
  `account`
  `action-registry`
  `agent-server-responser`
  `agentserver`
  `aggregator`
  `asset-account`
  `asset-manager`
  `backup-operator`
  `collector`
  `comment`

component

configuration

core

correlator

credentials

db-operator

decision-point

detects-processor

enricher

file-registry

gateway

gateway-operator

grafana

graph

hierman

iamoperator

istio-cni

istiod

kata-proxy

ksb-facade

ksc

ksc-info

ksc-tenant-binder

kscadapter

kubernetes-event-exporter

kube-state-metrics

kuma-operator

kuma-proxy

licensing-policy

local-path-provisioner

longhorn

loki

metallb

metrics

nats

ncircc

openbao

openbao-agent-injector

openbao-csi-provider

openbao-legacy-vault-csi-provider

operator

orchestra

osmp-scanner-facade

playbook-matcher

playbook-statistics

plugin-admin-agent

plugin-admin-server

plugin-agent-server

plugin-asset-management

plugin-enterprise

plugin-irp

plugin-kata

plugin-kes-linux

plugin-kesw

plugin-kuma

plugin-osmp-scanner

plugin-public-api-token-settings

plugin-spp

plugin-tenant-manager

plugin-tenant-roles

prevention-rules

prometheus-node-exporter

prometheus-redis-exporter

promtail

proxy

public-api

redis

reputation

response-manager

responser

rights

sandbox-scan-api

scan-rules-manager

scheduler

seaweedfs

secrets-store-csi-driver

ssh-remote-executor

storage

tenant-registry

tokenhub

tracker

transformer

unsealer

updater

updater-facade

victoria-metrics-operator

vmagent

vmalert

vmsingle

vtproxy

ztunnel

- `--auto-dest-dir` — 取得記錄並將其儲存至目前目錄下自動建立的 kdt-default-logs-<目前日期和時間> 目錄。若未指定記錄期間，則會取得過去一小時的診斷資訊。

  例如，如果您要取得管理伺服器和KUMA過去一小時的日誌，然後將這些日誌儲存到自動建立的目錄中，請執行以下命令：

  ```
  ./kdt logs get --app ksc,core --auto-dest-dir
  ```

- `-d, --destination <` 檔案路徑 `>` — 取得記錄並將其儲存至指定檔案。

- `-D, --destination-dir <` 目錄路徑 `>` — 取得記錄並儲存至必須事先建立的指定目錄。若 <directory_path> 為空，記錄會儲存至標準輸出資料流（stdout）。若未指定記錄期間，則會取得過去一小時的診斷資訊。

- `--to-archive` — 取得記錄並將其儲存至 kdt-default-logs-<目前日期和時間>.tar.gz 壓縮檔案。建立的封存檔案將儲存至目前目錄。若未指定日誌記錄期間，則會取得過去一小時的診斷資訊。

- `--last=<` 小時 `>h` — 取得截至目前為止，指定小時數內的記錄。

  例如，如果您想要取得過去三個小時的日誌存檔，請執行以下命令：

  ```
  ./kdt logs get --to-archive --last=3h
  ```

- `--start=<` 日期與時間 `>` — 取得從指定日期與時間（Unix 時間戳記格式）開始至目前時間為止，或至 `--end` 參數所指定日期與時間為止的記錄。

  例如，如果您要從過去的命令2024/03/26 10:00:00到現在的日誌，然後將它們儲存到目前目錄中建立的kdt-default-logs-<current_date_and_time>目錄中，請執行下列命令：

  ```
  ./kdt logs get --auto-dest-dir --start=1711447200
  ```

- `--end=<` 日期與時間 `>` — 取得從 `--start` 參數所指定日期與時間開始，至 `--end` 參數所指定日期與時間為止的記錄（Unix 時間戳記格式）。若未指定 `--start` 參數，將取得 `--end` 參數所指定日期與時間前一小時的記錄。

  例如，如果您要將10分鐘（從2024/03/26 10:0020到6:0020 10:10:00）的日誌儲存到日誌目錄，請執行下列命令：

  ```
  ./kdt logs get -D ./logs/ start=1711447200 --end=1711447800
  ```

若要檢視可用的日誌記錄參數，您可以執行以下其中一項命令：

- `./kdt logs get -h`
- `./kdt logs get --help`

檢視OSMP指標

Kaspersky Next XDR Expert的可觀察元件允許您檢視OSMP指標，透過儀表板監控每個元件的狀態，檢視Kubernetes叢集的資料儲存系統（Longhorn）的指標，並在Kubernetes叢集節點效能指標超過正常值時透過電子郵件通知使用者。

您可以使用可觀測元件監控指標，以便進一步分析其元件的可操作性和效能。

您可以使用下列可用方法之一檢視OSMP指標：

- 透過使用Grafana儀表板
- 透過使用您自己的監控工具

若要使用Grafana儀表板檢視OSMP指標：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   `<monitoring_host>` 是主機名稱，`<smp_domain>` 是網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。

2. 輸入組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。

或者，您可以在**控制板**部分檢視OSMP指標：

1. 在主功能表中，轉至**監控**部分。→ **控制板**，然後選取 **偵測與回應** 索引標籤。
2. 點按省略號（ ⋮ ）圖示。
3. 按一下「轉至OSMP指標」按鈕。

Grafana介面隨即顯示。您可以檢視每個Kaspersky Next XDR Expert元件的診斷資訊，檢視Kubernetes叢集資料儲存系統 (Longhorn) 的指標，並設定有關Kubernetes叢集運行狀況事件的電子郵件通知。

若要使用您自己的監控工具檢視OSMP指標：

1. 設定您的監控工具以從Kaspersky Next XDR Expert API取得指標。
2. 前往 API 位址 `<api_host>.<smp_domain>/api/read-api` 以取得指標。

   `<api_host>` 是主機名稱，`<smp_domain>` 是網域名稱。這些參數構成提供Kaspersky Next XDR Expert API存取權限的服務的FQDN。這些參數是在部署Kaspersky Next XDR Expert時在組態檔中設定的。

取得OpenMetrics格式的OSMP指標。

如果要檢視有關KUMA Core、儲存體、收集器和關聯器效能的資訊，則必須檢視KUMA指標。

監控Kaspersky Next XDR Expert元件的狀態

儀表板以圖形方式顯示每個Kaspersky Next XDR Expert元件的狀態。

例如，您可以查看以下元件參數：

- CPU請求使用情況和限制
- CPU和RAM請求使用情況
- 容器的CPU和RAM使用情況
- 容器分配的元件資源
- 網路效能指標：
  - 頻寬
  - 資料包速率（接收到的資料包數量）
  - 丟包數（遺失的資料包數量）
  - 錯誤數（網路錯誤數量）

若要在儀表板檢視診斷資訊：

1. 前往`<monitoring_host>.<smp_domain>` URL。

   `<monitoring_host>` 是主機名稱，`<smp_domain>` 是網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。例如：`monitoring.smp.local`。

2. 輸入您在組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。
3. 在功能表中，轉到**主頁→儀表板→Kubernetes/視圖/Pods**。
4. 在**namespace**下拉列表中，選擇要檢視診斷資訊的元件。
5. 您也可以指定其他參數來自訂儀表板視圖。

包含所選Kaspersky Next XDR Expert元件診斷資訊的儀表板隨即顯示。

設定有關Kubernetes叢集運行狀況事件的電子郵件通知

Kaspersky Next XDR Expert的可觀測元件可讓您在Kubernetes叢集節點效能指標超出正常值時透過電子郵件通知使用者。電子郵件通知是基於Grafana中的電子郵件通知規則產生。這些規則定義了通知訊息、收件者以及發送電子郵件警示的條件。

您可以在Grafana中查看可用電子郵件通知規則的清單。規則可以是預先定義的，也可以是自訂的。預定義規則由Kaspersky Next XDR Expert提供，無法變更。自訂規則可以建立、修改或刪除。

用於產生電子郵件通知的預定義規則

Kaspersky Next XDR Expert包含以下預定義規則，用於產生有關Kubernetes叢集運行狀況事件的電子郵件通知。您無法刪除或編輯這些規則。

用於產生電子郵件通知的預定義規則

指標	嚴重等級	通知訊息
CPU使用率過高	警告	節點<node_name>上的CPU使用率已超過警告閾值。這可能表示CPU負載過高或CPU資源不足。
	嚴重	節點<node_name>的CPU使用率極高。這可能導致CPU降頻、Pod調度問題以及叢集元件效能下降。
磁碟I/O使用率過高	警告	節點<node_name>上的磁碟裝置<disk_name>的I/O負載過高。應用程式可能會開始出現延遲。
	緊急	節點<node_name>上的磁碟裝置<disk_name>已過載。這可能會嚴重降低有狀態應用程式的效能。
磁碟延遲過高	警告	節點<node_name>上的儲存裝置<disk_name>的讀取/寫入延遲已超過警告閾值。
	緊急	節點<node_name>上的儲存裝置<disk_name>的I/O延遲極高。
磁碟使用率（檔案系統）過高	警告	節點<node_name>上的檔案系統<mountpoint_name>的使用率過高。接近上限可能會影響日誌記錄、Pod調度或kubelet穩定性。
	緊急	節點<node_name>上的檔案系統<mountpoint_name>幾乎已滿。這可能會導致寫入錯誤、服務故障和節點不穩定。
記憶體使用率過高	警告	節點<node_name>上的記憶體使用率已超過警告閾值。工作負載可能面臨記憶體不足問題。
	緊急	節點<node_name>的記憶體即將耗盡。這可能會觸發OOMKill或Pod驅逐。必須立即採取措施以防止工作負載故障。

若要查看用於產生電子郵件通知的預設規則：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   `<monitoring_host>` 是主機名稱，`<smp_domain>` 是網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。例如：`monitoring.smp.local`。

2. 輸入您在組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。

3. 在功能表中，轉至**首頁→警示→警示規則**。

   在**警示規則**部分中，將顯示用於產生電子郵件通知的預先定義規則清單。

用於產生電子郵件通知的自訂規則

您可以建立自己的規則來產生有關Kubernetes叢集運行狀況事件的電子郵件通知。

如果未在組態檔中指定 SMTP 伺服器連線參數，則不會傳送電子郵件通知：`grafana_smtp_host`、`grafana_smtp_user`、`grafana_smtp_password`、`grafana_smtp_bundle`、`grafana_smtp_skip_verify`、`grafana_smtp_from_address`、`grafana_smtp_from_name`、`grafana_smtp_ehlo_identity`、`grafana_starttls_policy`、`grafana_smtp_enable_tracing`。如果您在部署Kaspersky Next XDR Expert之前未在組態檔中指定這些參數，您可以稍後新增。

若要建立用於產生電子郵件通知的自訂規則：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   `<monitoring_host>` 是主機名稱，`<smp_domain>` 是網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。例如：`monitoring.smp.local`。

2. 輸入您在組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。

3. 在功能表中，轉至**首頁→警示→警示規則**。

4. 在**警示規則**部分中，按一下**新增警示規則**，然後指定新電子郵件通知規則的參數。

5. 指定規則參數後，按一下**儲存規則並退出**。

自訂規則隨即建立。您也可以建立資料夾並將建立的規則放在其中。

若要從儀表板建立用於產生電子郵件通知的自訂規則：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

2. 輸入您在組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。

3. 在功能表中，轉到**主頁→儀表板**。

4. 在儀表板清單中，按一下包含要用於警示的效能指標的儀表板名稱。

   儀表板隨即打開。

5. 按一下儀表板所需窗格上的**選單**圖示（⋮），然後在右鍵功能表中選擇**更多... → 新警示規則**。

6. 在**新警示規則**窗格中，指定新電子郵件通知規則的參數。

7. 按一下**儲存規則並退出**。

儀表板中的自訂規則隨即建立。

若要編輯或刪除用於產生電子郵件通知的自訂規則：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

2. 輸入您在組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。

3. 在功能表中，轉至**首頁→警示→警示規則**。

4. 在**警示規則**部分中，找到所需的規則，然後執行下列其中一項操作：

   - 若要編輯規則，請按一下鉛筆按鈕，然後變更規則參數。
   - 若要刪除該規則，請按一下**更多**，然後按一下**刪除**。

自訂規則隨即更改或刪除。

管理Kubernetes叢集運行狀況事件的電子郵件通知收件者

Kaspersky Next XDR Expert允許您指定、編輯和刪除通知收件者電子郵件地址。

如果未在組態檔中指定 SMTP 伺服器連線參數，則不會傳送電子郵件通知：`grafana_smtp_host`、`grafana_smtp_user`、`grafana_smtp_password`、`grafana_smtp_bundle`、`grafana_smtp_skip_verify`、`grafana_smtp_from_address`、`grafana_smtp_from_name`、`grafana_smtp_ehlo_identity`、`grafana_starttls_policy`、`grafana_smtp_enable_tracing`。如果您在部署Kaspersky Next XDR Expert之前未在組態檔中指定這些參數，您可以稍後新增。

若要新增通知收件者電子郵件地址：

1. 前往 `<monitoring_host>.<smp_domain>` URL。

   `<monitoring_host>` 是主機名稱，`<smp_domain>` 是網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。例如：`monitoring.smp.local`。

2. 輸入您在組態檔中指定的 Grafana 憑證（`grafana_admin_user` 和 `grafana_admin_password` 參數）。

3. 在選單中，轉至**首頁→警示→聯繫點**。

4. 在**聯絡點**工作區中，按一下**新增聯絡點**，然後指定下列收件者參數：

   - **名稱** - 收件者或收件者群組的名稱。必填欄位。
   - **整合**– 整合類型。使用電子郵件接收郵件通知。
   - **地址** - 一個或多個收件者電子郵件地址。地址之間可以使用逗號、換行符號 (`\n`) 或分號分隔。
   - **單封郵件** - 可選擇發送一封電子郵件給所有收件者。可能的參數值：
     - **已啟用** - 所有收件者將收到一封電子郵件通知。
     - **已停用** - 每個收件者都會收到單獨的電子郵件通知。
   - **訊息**– 電子郵件正文。您可以使用範本，也可以點選**編輯訊息**設定自訂文字。
   - **主題**– 電子郵件主題。您可以使用範本，也可以點選**編輯主題**設定自訂文字。
   - **通知設定**– 一般通知設定。
   - **停用已解決訊息** - 停用在問題或警示解決時發送訊息。
   - **測試** - 發送測試通知。允許檢查設定是否正確。
   - **複製** - 建立聯絡點組態的副本。可以快速建立類似的聯絡點。
   - **刪除** - 刪除目前的聯絡點組態。

5. 點選**儲存聯絡點**。

若要編輯或刪除通知收件者電子郵件地址：

1. 前往 `<monitoring_host>.<smp_domain>` URL。
2. 輸入您在組態檔中指定的 Grafana 憑證（ `grafana_admin_user` 和 `grafana_admin_password` 參數）。
3. 在選單中，轉至**首頁→警示→聯繫點**。
4. 在**聯絡點**工作區中，找到所需的聯絡點，然後執行下列其中一項操作：
   - 若要編輯規則，請按一下鉛筆按鈕，然後變更規則參數。
   - 若要刪除該規則，請按一下**更多**，然後按一下**刪除**。

聯絡點隨即更改或刪除。

無需重新安裝Kaspersky Next XDR Expert即可將SMTP伺服器連線參數新增到組態檔中

若要無需重新安裝Kaspersky Next XDR Expert即可將SMTP伺服器連線參數新增到組態檔中：

1. 在管理員主機上，匯出目前的組態檔。
2. 在匯出的組態檔中，於 `parameters` 區段新增並指定下列參數：`grafana_smtp_host`、`grafana_smtp_user`、`grafana_smtp_password`、`grafana_smtp_bundle`、`grafana_smtp_skip_verify`、`grafana_smtp_from_address`、`grafana_smtp_from_name`、`grafana_smtp_ehlo_identity`、`grafana_starttls_policy`、`grafana_smtp_enable_tracing`。
3. 使用下列命令套用參數變更：

   ```
   ./kdt apply -i '< full_path_to_updated_configuration_file >'
   ```

SMTP伺服器連線參數隨即新增至組態檔中。

檢視Longhorn指標

Kaspersky Next XDR Expert包含一個儀表板，用於顯示叢集資料儲存系統 (Longhorn) 的關鍵指標。Longhorn儀表板能夠監控資料儲存體的運作狀況和效能。

依預設，儀表板會顯示過去三小時的資料。您可以變更此時段。儀表板每15秒重新整理一次。

若要檢視Longhorn儀表板：

1. 前往 `<monitoring_host>.<smp_domain>`。

   `<monitoring_host>` 代表主機名稱，`<smp_domain>` 代表網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。
2. 輸入您在 組態檔中指定的 Grafana 認證（ `grafana_admin_user` 和 `grafana_admin_password` ）。
3. 在選單中，前往 **首頁 → 儀表板 → Longhorn 儀表板**。

儀表板儀表板隨即顯示。

Longhorn儀表板指標描述如下。

節點

- **節點數**— 系統中的節點總數。
- **可排程節點**— 可用於分發磁碟區副本的節點數量。
- **已停用節點**— 使用者停用的節點。
- **故障節點**— 無回應、離線或無法使用的節點。

磁碟區

- **已掛載磁碟區**— 目前掛載到節點的磁碟區。
- **已斷開連線的磁碟區**— 未連線到節點的磁碟區。
- **已降級磁碟區**— 副本數量不足的磁碟區。
- **故障磁碟區**— 沒有正常運作副本的磁碟區。

容量

- **節點容量**— 每個節點上的總儲存容量。
- **磁碟容量**— 每個磁碟的儲存容量。
- **磁碟區容量**— 每個磁碟區的容量。

資源使用率

- **節點儲存使用率/容量**— 每個節點上的儲存容量百分比。
- **磁碟空間使用率**— 每個磁碟的容量百分比。
- **每個節點的磁碟區數量**— 每個節點上掛載的磁碟區數量。
- **卷大小/容量**— 目前卷/最大卷比率。
- **磁碟區寫入吞吐量**— 系統每秒寫入的資料量（bps）。
- **磁碟區讀取吞吐量**— 系統每秒讀取的資料量（bps）。
- **磁碟區寫入IOPS**— 寫入輸入/輸出操作次數（IOPS）。
- **磁碟區讀取IOPS**— 讀取輸入/輸出操作次數（IOPS）。
- **磁碟區寫入延遲時間**— 完成一次寫入操作所需的時間（ns）。
- **磁碟區讀取延遲時間**— 完成一次讀取操作所需的時間（ns）。
- **節點CPU使用率/容量**— 每個節點的CPU使用率百分比。
- **節點記憶體使用率/容量**— 每個節點的記憶體利用率百分比。

- **Longhorn管理器CPU使用率**— Longhorn管理器的CPU負載（milliCPU）。
- **Longhorn管理器記憶體使用率**— Longhorn管理器的記憶體負載。
- **實例管理器CPU使用率**— Longhorn實例的CPU負載（milliCPU）。
- **實例記憶體使用率**— Longhorn實例使用的記憶體。

磁碟使用率

磁碟使用率窗格上的指標顯示磁碟讀取和寫入所花費的時間百分比。這些指標基於以下指標：

- `longhorn_volume_read_iops`
- `longhorn_volume_read_latency_seconds`
- `longhorn_volume_write_iops`
- `longhorn_volume_write_latency_seconds`

查看EDR儀表板和指標

Kaspersky Next XDR Expert包含EDR儀表板，用於顯示負責處理從端點代理程式取得的物件的解決方案元件的關鍵指標。監控這些指標有助於確保組件平穩安全地運行，從而採取主動措施來預防潛在問題。

以下儀表板可用：

- EDR代理程式伺服器
- EDR KSB
- EDR KSN代理
- EDR沙盒
- EDR掃描程式

若要檢視EDR儀表板：

1. 前往 `<monitoring_host>.<smp_domain>`。

   `<monitoring_host>` 代表主機名稱，`<smp_domain>` 代表網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。

2. 輸入您在 組態檔中指定的 Grafana 認證（ `grafana_admin_user` 和 `grafana_admin_password` ）。
3. 在功能表中，轉到**主頁→儀表板**。
4. 在標籤篩選下拉清單（**按標籤篩選**）中，選擇**edr**標籤。

   可用EDR儀表板隨即顯示。

5. 點選您想要檢視的儀表板名稱。

選定的儀表板隨即開啟。

每個EDR儀表板中可用的小工具和指標描述如下。

EDR代理程式伺服器

預設情況下，儀表板顯示最近2天的資料。您可以點擊頁面頂部的**最近2天**並選擇其他期間來更改期間。

EDR代理伺服器小工具與指標

小工具名稱	指標名稱	描述
工作數	xdr_agentserver_tasks_total	從事件回應平台收到的工作總數。
設定	xdr_agentserver_settings_total	從事件回應平台收到的組態總數。
活動工作數	xdr_agentserver_tasks_active	執行中的工作總數。
活動設定	xdr_agentserver_settings_active	執行中的組態應用程式總數。
工作錯誤	xdr_agentserver_tasks_errors_total	完成工作時出錯的工作總數。
設定錯誤	xdr_agentserver_settings_errors_total	組態應用程式錯誤總數。
物件儲存體	xdr_agentserver_objectstorage_upload_errors_total	物件儲存體中的檔案上傳錯誤總數。
物件儲存體	xdr_agentserver_objectstorage_download_errors_total	物件儲存體中的檔案下載錯誤總數。
代理程式資訊更新數	xdr_agentserver_agentinfo_updates_total	端點代理程式資訊更新並傳送到資產管理器的總次數。
資產解決錯誤	xdr_agentserver_assets_resolve_errors_total	在OSMP和端點代理之間對映識別符號時的錯誤總數。
資產	xdr_agentserver_assets_resolve_total	解決總數。
代理程式伺服器速率超限	xdr_agentserver_rate_limit_exceeded_total	速率超限的案例總數。
代理程式授權數	xdr_agentserver_agent_auth_total	端點代理程式驗證嘗試總數。
代理程式授權數	xdr_agentserver_agent_auth_errors_total	端點代理程式驗證錯誤總數。
Vtproxy會話	xdr_agentserver_vtproxy_sessions_total	建立的會話總數。
Vtproxy驗證錯誤數	xdr_agentserver_vtproxy_auth_errors_total	會話驗證錯誤總數。
Vtproxy驗證成功數	xdr_agentserver_vtproxy_successful_auths_total	會話認證成功總數。
Vtproxy活動感測器會話數	xdr_agentserver_vtproxy_sensor_session_active	感測器的活動會話數。
Vtproxy活動會話數	xdr_agentserver_vtproxy_sessions_active	活動會話的數量。
Vtproxy會話持續時間	xdr_agentserver_vtproxy_session_duration_seconds	會話持續時間（秒）。
Vtproxy傳輸位元組數	xdr_agentserver_vtproxy_bytes_transferred_total	傳輸的位元組總數。

EDR KSB

預設情況下，儀表板顯示最近2天的資料。您可以點擊頁面頂部的**最近2天**並選擇其他期間來更改期間。

EDR KSB小工具與指標

小工具名稱	指標名稱	描述
多工作	xdr_ksb_multitasks_total	掃描工作總數。
活動多工作	xdr_ksb_multitasks_active	活動掃描工作數。
重複多工作	xdr_ksb_multitask_duplicates_total	重複掃描工作數。

小工具名稱	指標名稱	描述
重複多工作檔案	xdr_ksb_multitask_file_duplicates_total	掃描工作中的重複檔案數。
多工作檔案大小	xdr_ksb_multitask_files_size_bytes_total	多工作檔案的大小（以位元組為單位）。
代理城市驗證失敗數	xdr_ksb_agent_auth_failures_total	端點代理程式驗證失敗的數量。
速率超限數	xdr_ksb_rate_limit_exceeded_total	速率超限的案例總數。

EDR KSN代理

預設情況下，儀表板顯示最近6小時的資料。您可以透過點擊頁面頂部的**最近6小時**並選擇其他期間來更改期間。

ED KSN代理小工具與指標

小工具名稱	指標名稱	描述
統計資訊訊息	xdr_scanner_ksnproxyfacade_stats_messages_total	統計資訊訊息的總數。
整合模式變更數	xdr_scanner_ksnproxyfacade_integration_mode_changes_total	整合類型變更總數。
KSN代理啟動數	xdr_scanner_ksnproxysupervisor_ksnproxy_starts_total	KSN代理啟動總數。
KSN代理啟動錯誤數	xdr_scanner_ksnproxysupervisor_ksnproxy_start_errors_total	KSN代理啟動錯誤總數。
KSN可用性	xdr_scanner_ksnproxy_ksn_proxy_ksn_available	KSN可用性。
KSN心跳失敗請求數	xdr_scanner_ksnproxy_ksn_proxy_ksn_heartbeat_failed_requests_total	失敗心跳請求總數。
KSN心跳請求數	xdr_scanner_ksnproxy_ksn_proxy_ksn_heartbeat_requests_total	心跳請求的總數

EDR沙盒

預設情況下，儀表板顯示最近6小時的資料。您可以透過點擊頁面頂部的**最近6小時**並選擇其他期間來更改期間。

若要檢視特定沙盒的指標，請在頂部的**沙盒**選單中選擇其IP位址。

EDR沙盒的小工具與指標

小工具名稱	指標名稱	描述
開始時間 正常運行時間	xdr_scanner_sb_process_start_time_seconds	沙盒進程啟動的時間及其正常執行時間，以秒為單位。
沙盒上次運行狀況檢查 沙盒運行狀況檢查錯誤數	xdr_scanner_sb_health_check_errors_current	上次運行狀況檢查的時間以及目前偵測到的錯誤數量。
沙盒資料庫年齡	xdr_scanner_sb_health_bases_age_seconds	沙盒中病毒資料庫的年齡，以秒為單位
CPU	xdr_scanner_sb_process_cpu_seconds_total	使用的CPU核心數量
記憶體：使用情況	xdr_scanner_sb_go_memstats_sys_bytes	系統請求的記憶體使用量（位元組）。
記憶體：使用情況	xdr_scanner_sb_go_memstats_heap_inuse_bytes	正在使用的堆積記憶體，以位元組為單位。
記憶體：使用情況	xdr_scanner_sb_go_memstats_stack_inuse_bytes	堆疊記憶體使用量（以位元組為單位）。
記憶體：使用情況	xdr_scanner_sb_process_resident_memory_bytes	駐留記憶體（RSS）使用量（以位元組為單位）。
磁碟讀寫	xdr_scanner_sb_node_disk_read_bytes_total	從磁碟讀取的位元組總數。
磁碟讀寫	xdr_scanner_sb_node_disk_written_bytes_total	寫入磁碟的位元組總數。
網路使用情況	xdr_scanner_sb_process_network_receive_bytes_total	入站流量。

小工具名稱	指標名稱	描述
網路使用情況	xdr_scanner_sb_process_network_transmit_bytes_total	出站流量。
惡意軟體通道可用性	xdr_scanner_sbscanapi_sb_malware_channel_availability	特定沙盒的惡意軟體通道可用性。
沙盒映像狀態	xdr_scanner_sb_vm_images_status	沙盒中虛擬機器的當前狀態，指示作業系統是否已安裝。
沙盒映像版本狀態	xdr_scanner_sb_vm_image_version_status	虛擬機器上使用的映像版本的狀態，指示每個版本是否正確。

EDR掃描程式

預設情況下，儀表板顯示最近2天的資料。您可以點擊頁面頂部的**最近2天**並選擇其他期間來更改期間。

在頂部的**掃描引擎**選單中，選擇掃描引擎以查看其指標：

- **AM**：反惡意軟體引擎指標
- **YARA**：YARA指標
- **SB** ：沙盒指標

EDR掃描程式的小工具與指標

小工具名稱	指標名稱	敘述
上次資料庫更新時間	xdr_scanner_updater_updater_bases_age	更新程式資料庫的年齡。
上次資料庫更新時間	xdr_scanner_updater_updater_retranslation_age	更新程式重譯的年齡。
上次資料庫更新時間	xdr_scanner_internalscanner_am_bases_age	惡意軟體引擎的病毒資料庫的年齡。
上次資料庫更新時間	xdr_scanner_sb_health_bases_age_seconds	自上次沙盒中病毒資料庫更新以來經過的時間（以秒為單位）。
AM掃描引擎完成 SB掃描引擎完成 YARA掃描引擎完成	xdr_scanner_internalscanner_scan_engine_complete_total	每個掃描引擎和物件掃描結果的已完成掃描工作數量。
掃描運行狀況	xdr_scanner_internalscanner_total_scans	掃描的數量。
掃描運行狀況	xdr_scanner_internalscanner_failed_scans	失敗掃描的數量。
惡意軟體掃描工作數	xdr_scanner_internalscanner_am_queue_len	惡意軟體引擎佇列中的作業數。
惡意軟體掃描工作數	xdr_scanner_internalscanner_am_queue_total_items	所有反惡意軟體引擎佇列中的工作總數。
惡意軟體掃描工作數	xdr_scanner_internalscanner_am_queue_failed_items_total	反惡意軟體引擎佇列中失敗工作的總數。
反惡意軟體引擎佇列大小	xdr_scanner_internalscanner_am_queue_size	反惡意軟體引擎佇列所使用的檔案系統大小。
反惡意軟體引擎佇列大小	xdr_scanner_internalscanner_am_storage_size_limit	反惡意軟體引擎佇列允許的最大大小。
沙盒掃描工作	xdr_scanner_internalscanner_sb_wait_queue_len	OSMP掃描程式中沙盒佇列中的作業數。
沙盒掃描工作	xdr_scanner_internalscanner_sb_queue_total_items	所有沙盒佇列中的工作總數。
沙盒掃描工作	xdr_scanner_internalscanner_sb_queue_failed_items_total	沙盒佇列中失敗工作的總數。
沙盒掃描工作	xdr_scanner_internalscanner_sb_queue_len	沙盒佇列中的工作數量。
沙盒佇列大小	xdr_scanner_internalscanner_sb_queue_size	沙盒佇列中資料（樣本）的近似大小。
沙盒佇列大小	xdr_scanner_internalscanner_sb_storage_size_limit	沙盒佇列允許的最大大小。
平均沙盒掃描時間	xdr_scanner_sbscanapi_sb_scan_time_total	沙盒掃描總時間。
沙盒平均掃描時間	xdr_scanner_sbscanapi_sb_scan_count_total	沙盒上的總掃描次數。

小工具名稱	指標名稱	敘述
YARA掃描工作	xdr_scanner_internalscanner_yr_queue_len	YARA佇列中的作業數。
YARA佇列大小	xdr_scanner_internalscanner_yr_queue_size	YARA佇列所使用的檔案系統大小。
YARA佇列大小	xdr_scanner_internalscanner_yr_storage_size_limit	最大YARA佇列大小。
YARA掃描工作	xdr_scanner_internalscanner_yr_queue_total_items	所有YARA佇列中的工作總數。
YARA掃描工作	xdr_scanner_internalscanner_yr_queue_failed_items_total	YARA佇列中失敗工作的總數。
上次資料庫更新時間	xdr_scanner_internalscanner_am_bases_age	惡意軟體引擎的病毒資料庫的年齡。

檢視Node Exporter完整版的儀表板

Node Exporter完整版儀表板顯示叢集節點效能的關鍵指標。

若要檢視Node Exporter完整版儀表板：

1. 前往 `<monitoring_host>.<smp_domain>`。

   `<monitoring_host>` 代表主機名稱，`<smp_domain>` 代表網域名稱。這些參數構成了Kaspersky Next XDR Expert服務的FQDN，並在部署Kaspersky Next XDR Expert時於組態檔中設定。

2. 輸入您在 組態檔中指定的 Grafana 認證（ `grafana_admin_user` 和 `grafana_admin_password` ）。

3. 在功能表中，轉到**主頁→儀表板**。

4. 按一下**Node Exporter完整版**。

   儀表板隨即打開。

預設情況下，儀表板顯示最近24小時的資料。您可以透過點擊頁面頂部的**最近24小時**並選擇其他期間來更改期間。

儀表板中可用的窗格如下表所示。

Node Exporter完整版窗格

窗格	描述
CPU/記憶體/磁碟快速概覽	快速概覽關鍵資源：CPU負載、記憶體使用量和磁碟使用量。
壓力	壓力失速資訊 (PSI)：CPU、記憶體和輸入/輸出。顯示系統負載情況。
CPU繁忙情況	處理器忙於計算的時間百分比（使用者時間 + 系統時間）。
系統負載情況	1分鐘、5分鐘和15分鐘的平均係統負載（平均負載）。
RAM使用量	已使用RAM，包括緩衝區和快取。
交換空間使用率	使用的交換空間。
根檔案系統使用量	根檔案系統 (/) 上已使用的空間。
CPU核心數	節點上的核心數（vCPU）。
正常運行時間	自上次系統啟動以來經過的時間。
根檔案系統總大小	根檔案系統的總大小。
RAM總容量	RAM總量。
交換空間總容量	可用交換記憶體總量。
CPU/記憶體/網路/磁碟概覽	關鍵CPU、記憶體、網路和磁碟指標的概覽。
CPU概覽	基本CPU負載窗格，包含使用者/系統/閒置/iowait。

窗格	描述
記憶體：概覽	主RAM和交換空間使用指標。
網路流量：概覽	按介面統計的總網路流量（入站/出站）。
磁碟空間使用量概覽	磁碟空間使用情況和分割區情況。
CPU	詳細的CPU使用率指標（百分比，依核心分組）。
記憶體：堆疊記憶體	記憶體層使用圖（已使用、快取、緩衝區、可用）。
網路流量	按介面統計的網路總流量（位元組/秒）。
磁碟空間使用量	按分割區統計的詳盡磁碟空間使用量。
磁碟IOPS	每秒輸入/輸出的數量（每秒輸入/輸出數）。
輸入/輸出使用率：讀寫	磁碟上的資料讀寫速度（位元組/秒）。
輸入/輸出使用率	儲存裝置使用率，即磁碟忙於輸入/輸出的時間百分比。
CPU在來賓（虛擬機器）上花費的時間（秒）	CPU在來賓虛擬機器上運行的時間（來賓時間）。
記憶體：活動/非活動	活動記憶體分頁和非活動記憶體分頁（已使用和潛在可回收）。
記憶體：提交情況	分配給進程的記憶體量（包括超額提交）。
記憶體：活動/非活動詳情	活動和非活動分頁的詳情，包括匿名/檔案。
記憶體回寫頁和髒頁數	等待寫入磁碟的分頁數量（髒頁、回寫頁）。
記憶體：共享和對映	共享和對應的記憶體。
記憶體：Slab	分配給核心物件（Slab，可回收/不可回收）的記憶體。
記憶體：Vmalloc	核心虛擬記憶體分配情況。
記憶體：跳出率	跳出頁的數量（很少見，適用於舊硬體）。
記憶體：匿名	匿名記憶體（不支援檔案）。
記憶體：核心/CPU	核心和CPU結構使用的記憶體。
記憶體：巨頁計數器	已使用的巨頁數量。
記憶體巨頁大小	巨頁的大小和狀態。
記憶體：直接對映	實體記憶體的直接對映（DirectMap）。
記憶體：不可驅逐和鎖定	RAM中鎖定的記憶體（記憶體鎖定、不可驅逐）。
記憶體：NFS	NFS子系統的記憶體使用情況。
記憶體：Meminfo	proc/meminfo的摘要資訊。
記憶體：分頁輸入/輸出數	載入/卸載到記憶體中的分頁數。
記憶體：分頁交換輸入/輸出數	在RAM和交換空間之間移動的分頁數。
記憶體：分頁錯誤數	分頁錯誤（次要錯誤/主要錯誤）的數量。
OOM Killer	由於記憶體不足而導致系統終止進程的事件數。
記憶體：Vmstat	擴充虛擬記憶體統計資訊（/proc/vmstat）。
時間同步漂移	系統時間和同步來源之間的差異。
時間PLL調整	時間調整參數（PLL、偏移量）。
時間同步狀態	時間同步狀態（例如，chrony/ntpd）。
時間其他指標	其他與時間相關的指標（偏移量、抖動）。
系統時間同步	節點上的整體時間同步狀態。
進程狀態	依狀態（運行、睡眠、殭屍）統計的進程統計資訊。
進程狀態直方圖	進程狀態直方圖。
進程分支數	建立進程（分支）的數量。
記憶體：進程	進程記憶體的使用情況。

窗格	描述
PID數量和限制	系統中目前和最大PID數量。
進程調度統計資訊：執行/等待	按下"運行"和"等待"狀態進行進程分佈。
線程數和限制	線程數和系統限制。
上下文切換/中斷	上下文切換和硬體中斷。
系統負載	1分鐘、5分鐘和15分鐘的平均負載（負載平均值）。
CPU頻率調節	當前CPU頻率和調節（調速器，最小值/最大值）。
壓力失速資訊	CPU、記憶體和輸入/輸出壓力 - 顯示工作延遲。
中斷詳情	中斷類型的詳細分類。
每個CPU執行的排程時間片	每個核心執行的時間片數量。
熵	可用熵（隨機數產生品質）。
CPU在使用者和系統上下文中所花費的時間	使用者模式和系統模式下的CPU總時間。
檔案描述符數	開啟的文件描述符數量。
硬體溫度監控	系統元件（CPU、磁碟、感測器）的溫度。
節流閥冷卻裝置	冷卻系統狀態和節流情況。
電源	電源資料（電壓、電流、電池）。
Systemd套接字	活動的systemd套接字。
Systemd單元狀態	systemd單元的狀態（活動、失敗、非活動）。
磁碟輸入/輸出操作完成數	已完成的輸入/輸出操作數。
磁碟讀寫資料	讀取/寫入的資料量。
磁碟平均等待時間	輸入/輸出平均等待時間。
佇列平均長度	輸入/輸出佇列平均長度。
合併的磁碟讀寫數	合併的讀取/寫入操作次數。
輸入/輸出時間	輸入/輸出操作所花費的時間。
瞬時佇列大小	目前輸入/輸出的佇列長度。
已完成/已合併的磁碟IOPS丟棄數	已完成/合併的丟棄（TRIM）操作數。
可用檔案系統空間	檔案系統上的可用空間。
免費檔案節點	空閒inode的數量。
檔案描述符數	檔案描述符數量。
檔案節點大小	inode表大小。
檔案系統：唯讀/錯誤狀態	檔案系統狀態（錯誤、唯讀掛載）。
網路流量：資料包	各介面接收/發送資料包的數量。
網路流量：錯誤數	傳輸和接收錯誤數。
網路流量：丟包率	丟包數。
網路流量：壓縮	壓縮的流量。
網路流量：組播	多播的流量。
網路流量：Fifo	接口上的FIFO錯誤。
網路流量：幀	幀錯誤數。
網路流量：載波	鏈路級錯誤數（載波）。
網路流量：衝突	網路衝突。
NF Conntrack	追蹤的網路連線數（conntrack）。
ARP條目數	ARP表（條目數）。

窗格	描述
MTU	最大資料包大小。
速率	網路介面速率（比特/秒）。
佇列長度	介面資料套件佇列長度。
Softnet資料包	Softnet資料包處理（核心）。
Softnet超出配額	因軟體網路溢出而丟包數。
網路運作狀態	目前介面狀態（開啟/關閉）。
Sockstat TCP / UDP / FRAG / RAW	TCP、UDP和其他協定套接字的統計資料。
記憶體：Sockstat大小/使用情況	按套接字統計的記憶體使用情況和活動套接字數。
Netstat IP：輸入/輸出位元組數	傳入/傳出的IP資料包數量（以位元組為單位）。
Netstat IP：轉發	IP轉送狀態。
ICMP輸入/輸出/錯誤	ICMP資料包和錯誤統計資訊。
UDP輸入/輸出/錯誤	UDP資料包和錯誤統計資訊。
TCP：輸入/輸出/錯誤	TCP流量和錯誤。
TCP：連線數	依狀態統計的活動TCP連線數。
TCP：SynCookie/直接轉換/狀態	SYN cookie保護、TCP狀態直接轉換和TCP統計資訊。
Node Exporter抓取時間/抓取	Node Exporter的效能，重點在於抓取持續時間和目標狀態。

服務監控

您可以使用以下功能來監控除冷儲存和代理程式之外的所有服務的狀態：

- 檢視VictoriaMetrics警示

  具有主管理員角色的使用者可以設定 KUMA 服務的閾值，如果超過指定的閾值，則會發生以下變更：

  - KUMA會記錄一則稽核事件：VictoriaMetrics警示已註冊為服務。
  - KUMA 會向主管理員傳送通知電子郵件。
  - 服務會在**活動服務**部分以黃色狀態顯示。將滑鼠懸停在狀態圖示上，即可顯示錯誤訊息。

    可能的服務狀態

    - 綠色表示該服務正在運行，並且可以從Core伺服器存取。
    - 紅色表示服務未運行或無法從Core伺服器存取。
    - 黃色是適用於除代理程式之外所有服務的狀態。黃色狀態表示服務正在運行，但服務日誌中存在錯誤，或者VictoriaMetrics發出了針對該服務的警示。您可以將滑鼠懸停在**活動服務**部分中服務的狀態上，查看錯誤訊息。
    - 紫色是適用於正在執行的服務的狀態，這些服務在資料庫中的組態檔已更改，但沒有其他錯誤。如果服務的組態檔不正確且有錯誤（例如來自Victoria Metrics的錯誤），則服務狀態為黃色。
    - 灰色表示，如果已刪除的租用戶中存在仍在執行的服務，則該服務在「活動服務」頁面上將顯示為灰色狀態。當您刪除租戶時，灰色狀態的服務會被保留，以便您可以複製ID並刪除伺服器上的服務。只有「主管理員」可以刪除灰色狀態的服務。刪除租用戶後，該租用戶的服務將分配給主租用戶。

- 如果使用者擁有具備指標存取權限的角色，則可檢視 VictoriaMetrics 指標。

以下範例展示如何監控服務狀態。

1. 如果收集器服務在**活動服務**部分中顯示為黃色狀態，並且您看到**資料擴充錯誤數增加**的訊息，您可以：

   - 轉至**監控→指標→**<服務類型>**→**<服務名稱>**→資料擴充→錯誤數**部分，找到狀態為黃色的服務，找出哪個資料擴充導致錯誤，並檢視圖表以找出問題何時開始以及它是如何演變的。

   - 資料擴充錯誤的可能原因是DNS伺服器不可用或CyberTrace資料擴充錯誤，因此您可以檢查DNS伺服器或CyberTrace連線設定。

2. 如果收集器服務在**活動服務**部分中顯示為黃色狀態，並且您看到**輸出事件遺失數增加**訊息，您可以：

   - 轉至**監控→指標→**<服務類型>**→**<服務名稱>**→輸入/輸出→輸出事件遺失數**部分，找到狀態為黃色的服務並檢視圖表，以瞭解問題是什麼時候開始的，以及它是如何演變的。

   - 資料擴充錯誤的可能原因是緩衝區溢位或目標不可用，因此您可以檢查目標的可用性和連線情況，或找出緩衝區容量超出限制的原因。

設定服務監控

若要設定服務監控：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在「其他」下，按一下**服務監控**。

   這將開啟**服務監控**視窗。

3. 指定服務的監控參數值。

   服務監控不適用於冷儲存。

   如果您指定的值無效（不符合範圍或格式），則該值將重設為先前設定的值。

4. 按一下**儲存**。

   儲存參數後，KUMA會記錄一個稽核事件：服務的監控閾值已變更。

KUMA會根據指定的參數監控服務的狀態。

在**活動服務**部分，您可以按狀態篩選服務，或在搜尋欄位中輸入錯誤文字中的某個字詞，例如“QPS”或“緩衝區”，然後按「回車鍵」。這將顯示存在錯誤的服務清單。請勿在搜尋欄位中使用特殊字元「"」、「}」、「{」。這會導致搜尋結果錯誤。

停用服務監控

若要停用服務監控：

1. 在主應用程式視窗中，轉至**設定→KUMA→開啟 KUMA 設定**部分。

   這將開啟KUMA設定視窗。

2. 在「其他」下，按一下**服務監控**。

   這將開啟**服務監控**視窗。

3. 若要僅針對收集器停用服務監控，請在**服務監控。閾值設定**設定視窗中，在**收集器**下選中**停用連接器錯誤**核取方塊。

   這將僅停用對收集器**連接器錯誤數**指標的分析。

4. 若要停用所有服務的監控，請在**服務監控。閾值設定**設定中，選擇**停用**核取方塊。

KUMA服務監控將會停用，服務不會顯示黃色狀態。

檢視KUMA指標

為了監控其元件、事件串流和關聯上下文的效能，KUMA會收集並儲存大量參數。VictoriaMetrics時間序列資料庫用於收集、儲存和分析這些參數。收集到的指標透過Grafana進行視覺化。您可以在 **監控 → 指標** 區段找到用於將各種 KUMA 元件的關鍵效能參數視覺化的儀表板。
KUMA Core 服務會自動設定 VictoriaMetrics 和 Grafana，使用者無需進行任何操作。

或者，您可以在**控制板**部分檢視KUMA指標：

1. 在主功能表中，轉至**監控**部分。→ **控制板**，然後選取 **偵測與回應** 索引標籤。

2. 點按省略號（ ⋮ ）圖示。

3. 按一下**轉至KUMA指標**按鈕。

收集到的指標使用Grafana解決方案進行視覺化。「kuma-core」服務的RPM套件會產生Grafana配置，並建立一個單獨的儀表板來視覺化每個服務的指標。**指標**部分的圖表大約會延遲1.5分鐘顯示。

有關指標的完整信息，請參閱OSMP主控台的**指標**部分。選取此區段會開啟安裝 KUMA Core 時部署的 Grafana 入口網站，且該入口網站會自動更新。如果**「指標」**部分顯示core: <port number>，則表示KUMA部署在高可用性配置中，且指標是從**安裝Core**的主機接收的。在其他配置中，將顯示KUMA接收指標的主機名稱。

若要確定Core在哪個主機上運作，請在其中一個控制器的終端機中執行下列命令：

```
k0s kubectl get pod -n kuma -o wide
```

收集器指標

指標名稱	敘述
IO - 與服務輸入和輸出相關的指標。	
處理EPS數	每秒處理的事件數。
輸出EPS數	每秒傳送到目的地的事件數。
輸出延遲時間	傳送事件資料包並接收來自目的地的回應時所需的毫秒數。顯示中位數。
輸出錯誤數	事件資料包傳送到目的地時每秒發生的錯誤數量。網路錯誤和寫入目標磁碟緩衝區的錯誤會單獨顯示。
輸出事件遺失數	每秒遺失的事件數。事件可能會因網路錯誤或寫入目標磁碟緩衝區的錯誤而遺失。如果目標回應錯誤代碼（例如，在出現無效請求的情況下），事件也會遺失。
輸出磁碟緩衝區大小	與目的地關聯的收集器的磁碟緩衝區大小（以位元組為單位）。如果顯示零值，則表示收集器的磁碟緩衝區中沒有放置事件包，服務運作正常。

指標名稱	敘述
寫入網路BPS數	每秒接收到網路的位元組數量。
連接器錯誤數量	連接器日誌中的錯誤數量。

規範化 - 與規範化器相關的指標。	
原始事件和規範化事件大小	原始事件的大小和規範化事件的大小。顯示中位數。
錯誤	每秒規範化錯誤的數量。

過濾——與過濾器相關的指標。	
EPS	每秒與過濾條件匹配並發送進行處理的事件數量。只有當使用者已將過濾器新增至收集器服務配置時，收集器才會處理符合過濾條件的事件。

聚合 - 與聚合規則相關的指標。	
EPS數	聚合規則每秒接收和產生的事件數量。此指標有助於確定聚合規則的有效性。
儲存桶	聚合規則中的儲存桶數量。

富集分析 - 與富集規則相關的指標。	
快取RPS數	每秒向本機快取發出的請求數。
來源RPS數	每秒向富集來源（如字典）發送的請求數。
來源延遲時間	向富集來源發送請求並從其接收回應所經過的毫秒數。顯示中位數。
佇列大小	富集分析請求佇列的大小。此指標有助於尋找瓶頸富集規則。
錯誤數	向富集來源發送請求時每秒出現的錯誤數量。

關聯器指標

指標名稱	敘述
IO - 與服務輸入和輸出相關的指標。	
處理EPS數	每秒處理的事件數。
輸出EPS數	每秒傳送到目的地的事件數。
輸出延遲時間	傳送事件資料包並接收來自目的地的回應時所需的毫秒數。顯示中位數。

指標名稱	敘述
輸出錯誤數	事件資料包傳送到目的地時每秒發生的錯誤數量。網路錯誤和寫入目標磁碟緩衝區的錯誤會單獨顯示。
輸出事件遺失數	每秒遺失的事件數。事件可能會因網路錯誤或寫入目標磁碟緩衝區的錯誤而遺失。如果目標回應錯誤代碼（例如，在出現無效請求的情況下），事件也會遺失。
輸出磁碟緩衝區大小	與目的地關聯的收集器的磁碟緩衝區大小（以位元組為單位）。如果顯示零值，則表示收集器的磁碟緩衝區中沒有放置事件包，服務運作正常。

關聯分析 - 與關聯規則相關的指標。	
EPS數	關聯規則每秒產生的關聯事件數量。
儲存桶數	標準型別關聯規則中的儲存桶數量。
速率限制器觸發次數	關聯規則超過每秒速率限制的次數。
活動清單OPS數	每秒傳送到活動清單的操作請求數以及操作本身。
活動清單記錄數量	活動清單中的記錄數量。
磁碟上活動清單大小	磁碟上活動清單的大小（以位元組為單位）。

富集分析 - 與富集規則相關的指標。	
快取RPS數	每秒向本機快取發出的請求數。
來源RPS數	每秒向富集來源（如字典）發送的請求數。
來源延遲時間	向富集來源發送請求並從其接收回應所經過的毫秒數。顯示中位數。
佇列大小	富集分析請求佇列的大小。此指標有助於尋找瓶頸富集規則。
錯誤數	向富集來源發送請求時每秒出現的錯誤數量。

回應分析 - 與回應規則相關的指標。	
RPS數	每秒啟動回應規則的次數。

儲存指標

指標名稱	描述
ClickHouse/常規 - 與ClickHouse叢集的常規設定相關的指標。	
活動查詢數	傳送到ClickHouse叢集的活動查詢數。每個ClickHouse實例都會顯示此指標。
QPS數	每秒傳送到ClickHouse叢集的查詢數。
失敗QPS數	每秒發送到ClickHouse叢集的查詢失敗次數。
記憶體分配容量	分配給ClickHouse程序的RAM容量（以GB為單位）。

ClickHouse/插入—與向ClickHouse實例插入事件相關的指標。	
插入EPS數	每秒插入ClickHouse實例的事件數。
插入QPS數	每秒傳送至ClickHouse叢集的ClickHouse實例插入查詢數。 如果**插入QPS**指標顯示查詢佇列不斷增長且該指標大於1，我們建議您同時查看**批次大小**指標值，以便在儲存服務配置的設定中調整儲存緩衝設定。 範例： **插入QPS**指標大於1，等於8。 **批量大小**指標為1.2GB（以位元組為單位）。 在這種情況下，您可以將**插入QPS**乘以**批次大小來計算緩衝區大小**： 8*1.2=9.6GB。 將結果值9.6四捨五入，並在儲存服務配置的**進階設定**頁籤中將其指定為位元組數（例如，10000000000位元組），作為進階設定設定。同時，將**緩衝區刷新間隔**指定為2秒。增加緩衝區大小和緩衝區刷新間隔有助於緩解查詢佇列的壓力。 通常，**插入QPS**指標應小於1。
插入QPS失敗數	每秒傳送到ClickHouse叢集的失敗ClickHouse實例插入查詢數。
插入QPS延遲數	每秒傳送到ClickHouse叢集的延遲ClickHouse實例插入查詢數。由於超出活動合併的軟體限制，查詢被ClickHouse節點延遲。
插入QPS拒絕數	每秒傳送到ClickHouse叢集的被拒絕的ClickHouse實例插入查詢數。由於超出活動合併的硬限制，查詢被ClickHouse節點拒絕。
活動合併數	活動合併的數量。
分發佇列數	由於ClickHouse實例不可用而無法插入到其中的事件臨時檔案的ClickHouseClickHouse中的事件選擇相關的指標。無法透過搜尋找到這些事件。

ClickHouse/選取—與ClickHouse實例中的事件選擇相關的指標。	
選取QPS數	每秒傳送到ClickHouse叢集的ClickHouse實例事件分類查詢的數量。
選取QPS失敗數	每秒傳送到ClickHouse叢集的失敗的ClickHouse實例事件分類查詢的數量。

ClickHouse/複製—與ClickHouse節點副本相關的指標。	
活躍的Zookeeper連線數	Zookeeper叢集節點的活動連線數。正常運作時，此數量應等於Zookeeper叢集中的節點數。
只讀副本數	ClickHouse節點的只讀副本數。正常運作時， ClickHouse節點的只讀副本數不得存在。
活躍的複製獲取數	資料複製期間從ClickHouse節點下載資料的活動進程數。
活動複製發送數	資料複製期間向ClickHouse節點發送ClickHouse的活動進程數。
活動複製一致性檢查數	資料複製期間對ClickHouse節點副本進行主動資料一致性檢查的次數。

ClickHouse/網路—與ClickHouse業績網路相關的指標。	
活動HTTP連接數	ClickHouse業績HTTP伺服器的活動連線數。

活動TCP連線數	ClickHouse叢集TCP伺服器的活動連線數。
活動伺服器間連接數	ClickHouse節點之間的活動服務連線數。

核心指標

指標名稱	描述
Raft分析 - 與讀取和更新Core狀態相關的指標。	
查找RPS數	每秒發送到Core的查找過程請求數以及過程本身。
查找延遲時間	運作查找過程和過程本身所花費的毫秒數。顯示查找過程的第99個百分位數的時間。1%的查找過程可能需要更長時間才能運作。
建議RPS數	每秒發送到Core的Raft（SQLite）建議過程請求數以及過程本身。
建議延遲時間	執行Raft（SQLite）建議流程和流程本身所花費的毫秒數。顯示建議過程的第99個百分位數的時間。1%的建議過程可能需要更長時間才能運作。
資料探勘 - 與資料收集和分析相關的指標	
執行規則數	用於執行資料收集和分析請求的正在運作的調度程序數。
佇列規則數	用於執行佇列的資料收集和分析請求的調度程序數。
執行錯誤數	運作資料收集和分析調度程序時發生的錯誤數。
執行延遲時間	調度程序執行請求所需的時間。
工作分析 - 與監控KUMA Core上工作運作相關的指標	
活動工作數	單位時間內運作的工作數。
工作執行延遲時間	工作運作的持續時間（秒）。
錯誤	運作工作時的錯誤數。

API分析 - 與API請求相關的指標。	
RPS數	每秒向Core發出的API請求數。
延遲時間	處理Core的單一API請求所花費的毫秒數。顯示中位數。
錯誤	向Core發送API請求時每秒發生的錯誤數。

通知提要—與使用者活動相關的指標。	
訂閱數	透過SSE連接到Core以即時接收伺服器訊息的用戶端數量。此數字通常等於使用KUMA網頁介面的用戶端數量。
錯誤	向用戶發送通知時每秒發生的錯誤數。

調度程序 - 與Core工作相關的指標。	
活動數	重複的活動系統工作數。使用者建立的工作將被忽略。
延遲時間	運作工作所花費的毫秒數。顯示中位數。
錯誤	執行工作時每秒發生的錯誤數。

KUMA代理程式指標

指標名稱	敘述
IO - 與服務輸入和輸出相關的指標。	
處理EPS數	每秒處理的事件數。
輸出EPS數	每秒傳送到目的地的事件數。
輸出延遲時間	傳送事件資料包並接收來自目的地的回應時所需的毫秒數。顯示中位數。
輸出錯誤數	事件資料包傳送到目的地時每秒發生的錯誤數量。網路錯誤和寫入目標磁碟緩衝區的錯誤會單獨顯示。
輸出事件遺失數	每秒遺失的事件數。事件可能會因網路錯誤或寫入目標磁碟緩衝區的錯誤而遺失。如果目標回應錯誤代碼（例如，在出現無效請求的情況下），事件也會遺失。
輸出磁碟緩衝區大小	與目的地關聯的收集器的磁碟緩衝區大小（以位元組為單位）。如果顯示零值，則表示收集器的磁碟緩衝區中沒有放置事件包，服務運作正常。
寫入網路BPS數	每秒接收到網路的位元組數量。

事件路由器指標

指標名稱	敘述
IO - 與服務輸入和輸出相關的指標。	
處理EPS數	每秒處理的事件數。
輸出EPS數	每秒傳送到目的地的事件數。
輸出延遲時間	傳送事件資料包並接收來自目的地的回應時所需的毫秒數。顯示中位數。
輸出錯誤數	事件資料包傳送到目的地時每秒發生的錯誤數量。網路錯誤和寫入目標磁碟緩衝區的錯誤會單獨顯示。
輸出事件遺失數	每秒遺失的事件數。事件可能會因網路錯誤或寫入目標磁碟緩衝區的錯誤而遺失。如果目標回應錯誤代碼（例如，在出現無效請求的情況下），事件也會遺失。
輸出磁碟緩衝區大小	與目的地關聯的收集器的磁碟緩衝區大小（以位元組為單位）。如果顯示零值，則表示收集器的磁碟緩衝區中沒有放置事件包，服務運作正常。
寫入網路BPS數	每秒接收到網路的位元組數量。
連接器錯誤數量	連接器日誌中的錯誤數量。

所有服務通用的一般指標

指標名稱	描述
進程分析—一般進程指標。	
記憶體數	RAM使用量（RSS）（以兆位元組為單位）。
磁碟BPS數	每秒從磁碟讀取或寫入磁碟的位元組數。
網路BPS數	每秒透過網路接收/傳輸的位元組數。
網路封包遺失數	每秒遺失的網路封包數。
GC延遲時間	執行 GO 記憶體回收週期所花費的時間（以毫秒為單位）。顯示中位數。
Goroutines數	活動goroutine的數量。此數字與作業系統的執行緒數不同。

作業系統分析 — 與作業系統相關的指標。	
負載	平均負載。
處理器	CPU負載百分比。
記憶體	RAM使用率（RSS）。
磁碟	磁碟空間使用率。

指標儲存週期

KUMA操作資料預設保存3個月。此儲存週期可以變更。

若要變更KUMA指標的儲存週期：

1. 登入安裝KUMA Core的伺服器的作業系統。
2. 在檔案 /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service 的 ExecStart 參數中，編輯 `--retentionPeriod=<metrics storage period, in months>` 旗標，插入所需的儲存週期。例如，`--retentionPeriod=4` 表示指標將儲存 4 個月。
3. 依序執行以下命令重新啟動KUMA：

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-victoria-metrics`

   指標的儲存週期已變更。

KUMA指標警示觸發條件

如果某服務的 KUMA 指標值超過 KUMA 的 **服務監控** 區段中所設定之對應參數的閾值，VictoriaMetrics 會傳送警示，且該服務的狀態中會顯示錯誤訊息。

VictoriaMetrics的警示接收時間間隔如下：

- VictoriaMetrics 每 15 秒從 KUMA 服務取得一次資訊。
- VictoriaMetrics每分鐘更新一次KUMA服務的警示；
- KUMA Core 服務每 15 秒從 VictoriaMetrics 取得一次資訊。

因此，服務狀態更新的總延遲小於2-3分鐘。

如果您停用了接收來自VictoriaMetrics的警示，某些KUMA服務的狀態可能仍會顯示為黃色。這可能在以下情況中發生：

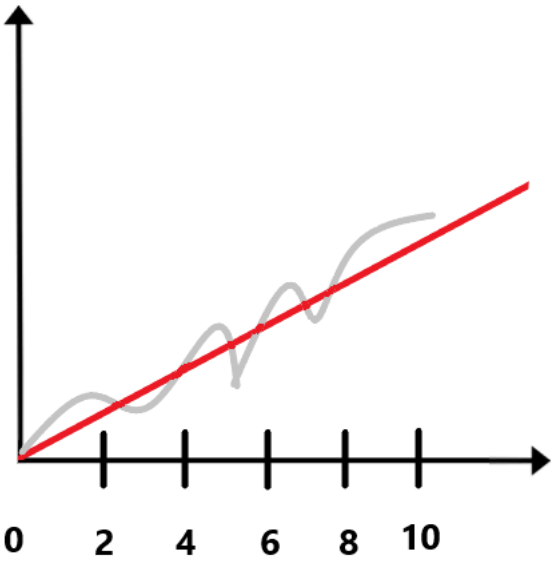
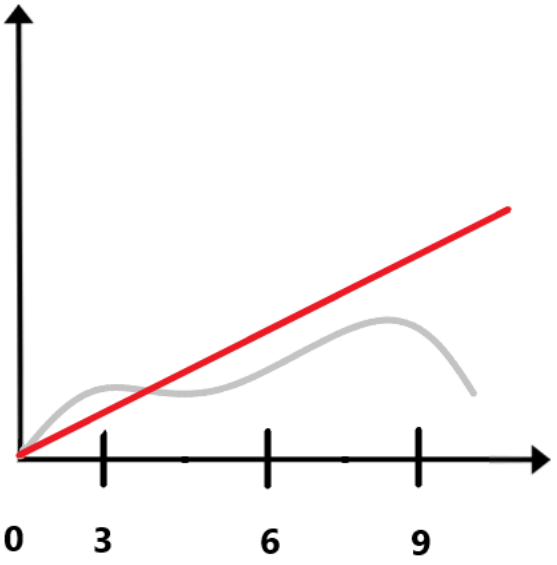
- 對於儲存服務：
  - 如果收到ClickHouse API 請求的/status參數中的警示
  - 如果儲存服務的冷儲存未受到監控
- 對於收集器服務：如果收到API請求的/status參數中的警示。
- 對於關聯器服務：如果存在需要進階回應模組的回應規則，但該模組不在目前產品授權的涵蓋範圍內，或涵蓋該模組的產品授權已過期。

下表提供了當收到VictoriaMetrics警示時，服務狀態中可能出現的錯誤訊息，以及這些錯誤訊息是基於哪些指標和參數，並說明其依據方式。如需可用於建立VictoriaMetrics警示的KUMA指標詳細資訊，請參閱檢視KUMA指標。

例如，如果某服務的**活動服務**表格顯示黃色狀態和`High distribution queue`錯誤訊息（下表中的「錯誤訊息」欄），您可以在**擴充**小工具的**分發佇列**指標（下表中的「KUMA指標」欄）中檢視資訊。

KUMA服務錯誤訊息描述

錯誤訊息	可設定的警示參數	KUMA指標	描述
`QPS threshold reached`	**QPS時間間隔/窗口（分鐘）** **QPS閾值**	Clickhouse / 一般 → 失敗的QPS	如果「失敗的QPS」指標在**QPS時間間隔/窗口（分鐘）**參數指定的持續時間內超過指定的**QPS閾值**，則會顯示錯誤訊息。 例如，如果VictoriaMetrics向服務發出的 100 個請求中有25個失敗，且**QPS閾值**為0.2，則警示計算如下： (25 / 100) * 100 > 0.2 * 100 25% > 20% 由於失敗請求的百分比大於指定的閾值，因此會為該服務顯示錯誤訊息。
`Failed Insert QPS threshold reached`	**失敗的插入QPS計算時間間隔/窗口（分鐘）** **插入QPS閾值**	Clickhouse / 插入 → 失敗的插入QPS	如果「失敗的插入QPS」指標在**失敗的插入QPS 計算時間間隔/窗口（分鐘）**參數指定的時間內超過指定的**失敗的插入QPS閾值**，則會顯示錯誤訊息。 例如，如果VictoriaMetrics向服務發出的100個請求中有25個失敗，且**失敗的插入 QPS閾值**為0.2，則警示計算如下： (25 / 100) * 100 > 0.2 * 100 25% > 20% 由於失敗請求的百分比大於指定的閾值，因此會為該服務顯示錯誤訊息。
`High distribution queue`	**分發佇列閾值** **分發佇列計算時間間隔/窗口（分鐘）**	Clickhouse / 插入 → 分發佇列	如果「分發佇列」指標在**分發佇列計算時間間隔/視窗（分鐘）**參數指定的時間段內超過指定的**分發佇列閾值**，則會顯示錯誤訊息。
`Low disk space`	**磁碟可用空間閾值**	作業系統 → 磁碟	如果「磁碟」指標值指示的可用磁碟空間量（以百分比表示）小於**可用磁碟空間閾值**參數中指定的值，則會顯示錯誤訊息。 例如，如果安裝KUMA的分割區佔用了所有磁碟空間，則會顯示錯誤訊息。

錯誤訊息	可設定的警示參數	KUMA指標	描述
`Low disk partition space`	**分割區可用空間閾值**	作業系統 → 磁碟	如果KUMA使用的磁碟分割區上的可用空間量（以百分比表示）小於**分割區可用空間閾值**參數中指定的值，則會顯示錯誤訊息。 例如，在以下情況下會顯示錯誤訊息： • 如果KUMA安裝在高可用性組態中，則磁碟將作為磁碟區掛載。 • 如果磁碟掛載在/opt下。
`Output Event Loss increasing`	**輸出事件遺失數**	輸入/輸出 → 輸出事件遺失數	如果「輸出事件遺失數」指標連續一分鐘增加，則會顯示錯誤訊息。您可以使用**輸出事件遺失數**參數啟用或停用顯示此錯誤訊息。
`Disk buffer size increasing`	**磁碟緩衝區增加時間間隔/窗口（分鐘）**	輸入/輸出 → 輸出磁碟緩衝區大小	如果「輸出磁碟緩衝區大小」指標在**磁碟緩衝區增加時間間隔/窗口（分鐘）**參數指定的取樣間隔下單調遞增10分鐘，則會顯示錯誤訊息。 例如，如果**將磁碟緩衝區增加時間間隔/窗口（分鐘）**設定為2分鐘，則當磁碟緩衝區大小以2分鐘的取樣間隔單調遞增10分鐘時，將顯示錯誤訊息（請參閱下圖）。 
`High enrichment queue`	**不斷增長的資料擴充佇列時間間隔/窗口（分鐘）**	資料擴充 → 佇列數	如果「佇列」指標在**不斷增長的資料擴充佇列時間間隔/窗口（分鐘）**參數指定的取樣間隔下單調遞增10分鐘，則會顯示錯誤訊息。 例如，如果**不斷增長的資料擴充佇列時間間隔/窗口（分鐘）**的值為3，則當資料擴充佇列每10分鐘單調遞增，取樣間隔為3分鐘時，將顯示錯誤訊息。 在下圖所示的例子中，沒有顯示錯誤訊息，因為在第九分鐘，指標值下降了，而不是單調遞增。 

錯誤訊息	可設定的警示參數	KUMA指標	描述
`Enrichment errors increasing`	**資料擴充錯誤數**	資料擴充 → 錯誤數	如果「錯誤數」指標在一分鐘內持續增加，則會顯示錯誤訊息。您可以使用**資料擴充錯誤數**參數啟用或停用顯示此錯誤訊息。
`Connector log errors increasing`	**停用連接器錯誤**	輸入/輸出 → 連接器錯誤數	如果 VictoriaMetrics 在一分鐘內連續兩次輪詢「連接器錯誤數」指標，且該指標持續增加，則會顯示錯誤訊息。您可以使用**停用連接器錯誤**參數啟用或停用顯示此錯誤訊息。

儲存有關Kaspersky Next XDR Expert元件的診斷資訊

有關 Kaspersky Next XDR Expert 元件的診斷資訊儲存於 Kubernetes 叢集的工作節點上。用於儲存此資訊所需的磁碟空間容量，會在部署 Kaspersky Next XDR Expert前於設定檔中指定（ `loki_size` 參數）。

若要檢查用於儲存Kaspersky Next XDR Expert元件的診斷資訊的磁碟空間，

在KDT公用程式所在的管理員主機上，執行以下命令：

```
./kdt invoke observability --action getPvSize
```

已指派的可用磁碟空間容量（以千兆位元組為單位）隨即顯示。

您也可以在部署Kaspersky Next XDR Expert後增加用於儲存有關Kaspersky Next XDR Expert元件的診斷資訊的磁碟空間。您不能將磁碟空間容量設定為小於之前指定的量。

若要增加用於儲存有關Kaspersky Next XDR Expert元件的診斷資訊的磁碟空間，

請在KDT公用程式所在的管理員主機上執行下列命令並指定所需的可用磁碟空間（以GB為單位）（例如「50Gi」）：

```
./kdt invoke observability --action setPvSize --param
loki_size='<new_disk_space_amount>Gi'
```

分配用於儲存有關Kaspersky Next XDR Expert元件的診斷資訊的可用磁碟空間容量隨即變更。

取得追蹤檔案

KDT可讓您取得Kaspersky Next XDR Expert和OSMP元件的偵錯檔案，以便您自行或在卡巴斯基技術支援的協助下對基礎設施進行錯誤排查。

偵錯檔案以OpenTelemetry格式下載。

若要取得Kaspersky Next XDR Expert或OSMP元件的偵錯檔案：

1. 在安裝了KDT公用程式的管理員主機上，執行以下命令，並指定要儲存偵錯檔案清單的檔案路徑：

   ```
   ./kdt traces find -o <output_file_path>
   ```

   將追蹤檔案清單及其ID輸出到指定檔案。

2. 若要輸出特定的偵錯檔案，請執行以下命令並指定輸出檔案路徑和偵錯檔案ID：

```
./kdt traces get -o <output_file_path> --trace-id=<trace_ID>
```

指定的偵錯檔案已儲存。

記錄自訂操作的啟動

KDT可讓您取得特定Kaspersky Next XDR Expert元件的自訂操作啟動歷程記錄以及特定自訂操作啟動的日誌。所取得的日誌可以幫助您自行或在卡巴斯基技術支援的協助下調查Kaspersky Next XDR Expert元件的運作問題。

若要取得特定Kaspersky Next XDR Expert元件的自訂操作啟動歷程記錄，

在KDT公用程式所在的管理員主機上，執行下列命令並指定元件名稱：

```
./kdt state -H <component_name>
```

已執行的自訂操作及其ID清單隨即顯示。

若要取得自訂操作啟動日誌，

請在安裝了KDT公用程式的管理員主機上執行下列命令，然後指定元件名稱和自訂操作啟動的ID：

```
./kdt state -l <component_name> -m <custom_action_launch_ID>
```

指定自訂操作啟動的日誌隨即顯示。

多租用戶

Kaspersky Next XDR Expert支援多租用戶模式。此模式使主管理員能夠獨立地向多個用戶端提供Kaspersky Next XDR Expert功能，或將資產、應用程式設定和物件分開用於不同辦公室。每個用戶端或辦公室都與其他用戶端或辦公室隔離，被稱為租用戶。

通常，多租用戶模式適用於以下情況：

- 服務提供商擁有多個用戶端組織，並希望獨立地向每個用戶端組織提供Kaspersky Next XDR Expert功能。為此，服務提供商管理員可以為每個用戶端組織建立一個租用戶。
- 大型企業的管理員可能想要隔離辦公室或組織單位的資產、應用程式設定和對象，並獨立管理辦公室或組織單位。為此，管理員可以為每個辦公室或組織單位建立一個租用戶。

多租用戶模式具有以下功能：

- 租用戶隔離
- 跨租用戶場景

租用戶隔離

租用戶與其他租用戶隔離並獨立管理。只有擁有租用戶存取權限的使用者才能使用及管理該租用戶。除非主管理員明確授予其他租用戶的管理員相關存取權限，否則該管理員無法存取租用戶的資料、資源和資產。

對於每個租用戶，您可以定義多個物件，包括以下物件：

- 資產

  每個租用戶的資產清單都是唯一的。每個資產只能屬於一個租用戶。
- 使用者及其存取權限
- 警示和事件
- 指令劇本
- 與其他卡巴斯基應用程式、服務和協力廠商解決方案整合

跨租用戶場景

所有租用戶都排列在租用戶層級結構中。預設情況下，租用戶層級結構在層級結構的頂部包含一個預先建立的根租用戶。不能在與根租用戶相同的層級建立任何其他租戶。您可以建立一個新租用戶作為任何現有租用戶的子租用戶，包括根租用戶。租用戶層級結構可以有任意數量的巢狀層級。

租用戶層級結構用於提供跨租用戶場景，包括以下場景：

- 繼承和複製

  子租用戶從父租用戶接收以下物件：

  - 使用者及其存取權限

    存取權限由層級結構向下繼承，且不能在層級結構的較低層級撤銷。

  - 租用戶設定，包括整合設定

    租用戶設定從父租用戶複製到其子租用戶。建立子租戶後，您可以重新配置複製的設定以滿足新租戶的需求。

  > 彙總和分段規則僅會沿租用戶層級結構向下繼承一個層級。例如，在根租用戶中建立的規則會由第一層級子租用戶繼承，但不會由其子租用戶繼承。

- 產品授權

  Kaspersky Next XDR Expert的產品授權金鑰套用於連結到根租用戶的主管理伺服器層級。然後，該產品授權金鑰將自動套用於層級結構中的所有租用戶。

使用者角色

Kaspersky Next XDR Expert為您提供了一組預先定義的使用者角色。您可以透過為使用者指派使用者角色來授予使用者管理租用戶的權限。

使用者角色	使用者角色權限		
	讀取	寫入	刪除
一般管理員	✓	✓	✓
租用戶管理員	✓	✓	✓
SOC管理員	✓	✓	—
第 1 層分析師	✓	—	—
第 2 層分析師	✓	—	—
初級分析師	✓	—	—
SOC管理員	✓	—	—
核准人	✓	—	—
稽核員	✓	—	—
與子事件互動	✓	—	—

SLA管理角色可讓使用者在**事件詳情頁面**中編輯SLA指標（**分類時間**、**回應時間**、解決時間）。

租用戶和管理伺服器

您只能將實體管理伺服器綁定到租用戶。租用戶和管理伺服器之間的連結可讓您結合兩種解決方案的功能—Kaspersky Next XDR Expert和Open Single Management Platform。

應用程式介面中的租用戶篩選器

在Kaspersky Next XDR Expert介面中，您可以設定物件清單以僅顯示與您選擇的租用戶相關的物件。租用戶篩選器適用於以下物件：

- **警示**部分中的警示
- **事件**部分中的事件
- 威脅搜尋部分中的**事件**
- **常規程式**部分中的指令劇本

當您套用租用戶篩選器時，新設定將套用於您使用的主控台介面（OSMP主控台或KUMA主控台）的所有物件類型。

關於將管理伺服器連結到租用戶

您可以將管理伺服器綁定到租用戶。租用戶和管理伺服器之間的連結可讓您將管理伺服器管理的資產與租用戶關聯。

> 您不能將虛擬管理伺服器綁定到租用戶，只能綁定實體管理伺服器。

租用戶可以擁有子租用戶；因此，它們被排列成租用戶層級結構。管理伺服器可以擁有從屬管理伺服器；因此，它們被排列成伺服器層級結構。您不能將任意伺服器綁定到任意租用戶，因為這可能導致非法綁定。例如，使用者可能沒有租用戶層級結構中某個租用戶的存取權限，但同一使用者可能擁有該租用戶裝置的存取權限。如果該使用者擁有管理伺服器2的存取權限，而該伺服器是連結到租用戶的管理伺服器1的主要伺服器，則可能會發生這種情況。因此，預設情況下，該使用者繼承了管理伺服器1及其受管理裝置的存取權限。為了避免這種情況，租用戶和管理伺服器只能根據綁定規則相互綁定。

綁定有兩種類型：

- 明確綁定

  當您選擇要綁定到租用戶的管理伺服器時，會建立此綁定類型。

- 繼承綁定

  當您為具有從屬管理伺服器的管理伺服器建立明確綁定時，從屬管理伺服器將透過繼承綁定類型綁定到租用戶。因此，多個管理伺服器可以綁定到一個租用戶。

綁定規則：

- 根管理伺服器一律綁定至根租用戶。您無法解除其綁定。
- 租用戶可能沒有綁定的管理伺服器。這樣的租用戶可以有子租用戶，管理伺服器可以綁定到這些子租用戶。
- 您只能將兩個排列成層級結構的管理伺服器綁定到兩個也排列成層級結構的租用戶，並且僅當管理伺服器的層級結構與租用戶的層級結構相符時才可以。
- 管理伺服器只能明確或透過繼承的綁定類型綁定到一個租用戶。

- 當您將管理伺服器明確地綁定到租用戶時：
  - 如果管理伺服器已明確地綁定到另一個租用戶，則此綁定將自動刪除。
  - 如果管理伺服器有從屬管理伺服器，則從屬管理伺服器將透過繼承的綁定類型綁定到新租用戶，但不包括那些已明確綁定到其租用戶的管理伺服器。在此操作之前，Kaspersky Next XDR Expert會檢查所有新綁定是否合法。如果不合法，則無法建立綁定。
- 當您刪除租用戶和管理伺服器之間的明確綁定（解除管理伺服器綁定）時，管理伺服器及其所有從屬管理伺服器（如果有）將透過繼承的綁定類型自動綁定到所選管理伺服器的主管理伺服器所綁定的租用戶。如果某些從屬管理伺服器已明確綁定至其租用戶，則這些管理伺服器將保留其綁定。
- 當您在層級結構中新增的管理伺服器時，管理伺服器將透過繼承的綁定類型自動綁定到伺服器的主管理伺服器所綁定的租用戶。
- 當您從層級結構中刪除管理伺服器並且管理伺服器與租用戶有明確綁定時，此綁定將被刪除。

設定與Open Single Management Platform的整合

您可以將管理伺服器綁定到租用戶。管理伺服器和租用戶之間的連結可讓您將管理伺服器管理的資產與租用戶關聯。

您不能將虛擬管理伺服器綁定到租用戶，只能綁定實體管理伺服器。

先決條件：

- 確保您熟悉綁定規則。
- 您已經建立了要將管理伺服器綁定到的租用戶。
- 如果需要，您已經新增了要綁定到租用戶的從屬管理伺服器。

若要將管理伺服器綁定到租用戶或將其與租用戶解除綁定，您必須擁有授予租用戶和整合功能區域的**寫入**存取權限的角色。

將管理伺服器綁定到租用戶

若要將管理伺服器綁定到租用戶：

1. 在主功能表中，轉至**設定** → **租用戶**。

   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取** 存取權限的租用戶。

2. 按一下所需政策的名稱。

   租用戶內容視窗隨即開啟。

3. 在**設定**頁籤的**卡巴斯基整合**區段中，選取**KSC**。

4. 按一下**綁定管理伺服器**按鈕，然後在開啟的視窗中，選取要綁定到租用戶的管理伺服器。
   如果要在層級結構中新增伺服器或刪除現有伺服器，您可以在管理伺服器內容中進行操作。
5. 按一下**綁定**按鈕。

綁定過程可能需要一段時間。您可以在租用戶內容視窗中，於管理伺服器清單的**綁定狀態**欄追蹤此過程。

解除管理伺服器與租用戶的綁定

若要解除管理伺服器與租用戶的綁定：

1. 在主功能表中，轉至**設定 → 租用戶**。
   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取** 存取權限的租用戶。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 在**設定**頁籤中，選取要與租用戶解除綁定的管理伺服器旁的核取方塊，然後按一下**解除綁定**按鈕。

檢視和編輯租用戶

您可以使用租用戶為用戶端組織單獨提供Kaspersky Next XDR Expert功能，或為不同的辦公室分離資產、應用程式設定和物件。

若要檢視或編輯租用戶的內容：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。
2. 按一下所需政策的名稱。
   租用戶內容視窗將開啟。如果您對此租用戶只有**讀取**存取權限，則此內容將以唯讀模式開啟。如果您擁有**寫入**存取權限，您將能夠修改租用戶的內容。
3. 修改租用戶的內容，然後按一下**儲存**按鈕。
   您可以按一下**儲存並關閉**按鈕儲存變更並關閉租用戶內容視窗。

租用戶的內容被修改並儲存。

一般

一般頁籤包含有關租用戶的一般資訊。您可以修改租用戶的名稱和描述。

設定

設定頁籤包含以下部分：

- **卡巴斯基整合**

  此部分可讓您為目前租用戶配置要整合至Kaspersky Next XDR Expert中卡巴斯基應用程式的整合設定。

- **協力廠商整合**

  此部分可讓您為目前租用戶配置要整合至Kaspersky Next XDR Expert中協力廠商應用程式的整合設定。

- **偵測和回應**

  此部分可讓您配置與威脅偵測和回應相關的設定和物件：

  - 區隔規則
  - 彙總規則
  - 郵件伺服器連線
  - 資產稽核
  - 網路共用憑證
  - 電子郵件範本
  - 掃描設定
  - 資產設定
    - 歸檔資產保留期限
    - 自訂資產欄位
    - **KSC資產匯入**

      受此程式保護的所有資產已在卡巴斯基安全管理中心註冊。受卡巴斯基安全管理中心保護的資產的相關資訊可以匯入KUMA。為此，您需要提前設定應用程式之間的整合。

      KUMA從Kaspersky Security Center Network Agents匯入以下裝置信息：

      - 資產的基本資訊：名稱、位址、連線至卡巴斯基安全管理中心的時間、硬體資訊、防護狀態、防毒資料庫版本
      - 資產屬性資訊：弱點；軟體，包括作業系統；資產擁有者

若要匯入卡巴斯基卡巴斯基安全管理中心資產資訊：

1. 在主功能表中，**資產管理→資產（裝置）→偵測和響應**。
2. 按一下**匯入**，然後選擇以下操作之一：
   - 若要匯入資產基本屬性資訊，請按一下**匯入KSC資產**。
     這將開啟**匯入KSC資產**視窗。
   - 若要匯入資產其他屬性資訊，請按一下**匯入KSC資產屬性**。
     這將開啟**匯入KSC資產屬性**視窗。
3. 在下拉清單，選取要為其執行匯入的租用戶。
   在這種情況下，程式會下載所有卡巴斯基安全中心伺服器的所有資產的資訊，這些伺服器已設定為連線到所選租用戶。
   如果您要匯入所有租用戶的所有卡巴斯基安全管理中心伺服器的所有資產資訊，請選擇**所有**。
4. 點擊**匯入**按鈕。

將匯入資產資訊。

此外，在租用戶內容視窗中，您可以安排資產資訊的定期匯入或手動執行匯入。

- KICS/KATA資產匯入

- KPSN信譽評比資料庫
- 保留期
  警示和事件的保留期取決於您使用的Kaspersky Next XDR Expert產品授權。
- 事件管理

您無需配置共用租用戶的設定。

角色

角色頁籤列出了對租用戶具有存取權限的使用者。您可以更改此清單並為使用者指派使用者角色。

新增租用戶

開始前，請閱讀有關租用戶的一般資訊。

若要新增子租用戶，您必須在父租用戶或租用戶層級結構中較高層級的租用戶的**租用戶**功能區中具有**讀取**和**寫入**權限。

若要新增租用戶：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
2. 選取所需弱點旁邊的核取方塊。新租用戶將作為所選租用戶的子租用戶建立。
3. 按一下**新增**。
4. 在開啟的**新增租用戶**視窗中，輸入新租用戶的名稱。
5. 如有必要，請為新租用戶新增描述。
6. 按一下**新增**。

   新租戶會出現在租用戶清單中。

子租用戶從父租用戶繼承以下物件：

- 使用者及其存取權限
- 整合設定

建立租用戶後，您可以重新設定繼承的物件以滿足新租用戶的需求。

為租用戶中的使用者和群組指派角色

您可以將 XDR 角色指派給 Kaspersky Next XDR Expert 使用者和網域群組，為其提供租用戶中的一組存取權限。

為此，您必須在要向使用者指派角色的租用戶中擁有以下其中一種XDR角色：主管理員、 SOC管理員或租用戶管理員。

由於租用戶與其他租用戶隔離並獨立管理，因此只有向租用戶指派了存取權限的使用者才能在此租用戶內工作和進行租用戶管理。

存取權限在層次結構中向下繼承，並且不能在層次結構的較低層級撤銷。

OSMP主控台中的新內部使用者帳戶在帳戶建立後五分鐘內即可在租用戶中新增和指派角色。

使用者的權限是使用者本身權限和使用者所屬網域群組（如果有）權限的總和。當使用者直接包含在某個群組中或透過巢狀群組成員身分間接包含在群組中時，情況確實如此。例如，如果使用者是群組 A 的成員，而此群組巢狀於群組 B 中，則使用者的權限是指派給該使用者的權限以及指派給群組 A 和 B 的權限總和。這表示，如果您將權限指派給群組 B，其巢狀群組和屬於群組 B 的使用者都會繼承這些權限。

但是，如果群組為循環巢狀，則循環中的成員及其子群組不會繼承指派給其父群組的權限。

若要將角色指派給租用戶中的使用者或網域群組：

1. 在主功能表中，轉至**設定 → 租用戶**。

   螢幕上將顯示租用戶清單。

2. 按一下所需政策的名稱。
   這會開啟租用戶內容視窗。

3. 轉到**存取權限**選項卡，然後依據要指派角色的物件選擇**使用者**或**群組**。
   使用者或網域群組表隨即顯示。

4. 如果必要，如下設定表格：

   - 點擊篩選圖示（ ）， 然後在開啟的功能表中指定並套用篩選條件。
     您無法將篩選器套用至**群組角色**和**父群組角色**直欄。
   - 點擊設定圖示 ( ) 以設定直欄顯示。

5. 點擊**新增使用者**按鈕或**新增群組**按鈕，視您在步驟3中選擇的頁籤而定。

6. 在開啟的視窗中，執行以下操作之一：

   a. 如果您在步驟3中選擇了**使用者** 頁籤上的**使用者**欄位中，輸入使用者名稱或電子郵件地址。如果您在步驟3中選擇了**群組**頁籤，請在**群組**欄位中指定群組名稱。

   b. 選取要指派給使用者或網域群組的角色旁的核取方塊。
      如有必要，您可以選擇多個角色。

   c. 點擊**新增**。

   視窗將關閉，使用者或網域群組將顯示在清單中。

7. 點擊**儲存**按鈕。

使用者或網域群組將新增至租用戶並指派角色。如有必要，您可以透過按一下使用者或網域群組名稱來編輯角色，然後執行步驟6-7中所述的操作。

刪除租用戶

一次只能刪除一個租用戶。但是，如果所選租用戶有子租戶，則它們也會被刪除。與租用戶相關的常規程式將被刪除，並且與租用戶相關的警示和事件資訊將變得不可用。

在OSMP主控台中刪除租用戶時，KUMA主控台中會發生以下變更：

- 租用戶及其資源將被刪除。已刪除租用戶的資產將歸檔，並在歸檔資產的事件保留期間（TTL）到期後刪除。
- 與租用戶相關的儲存分割區將被刪除。
- 原始事件變得不可用。
- 已刪除租用戶的服務狀態變更為**灰色**。

若要刪除租用戶，您必須在選定租用戶的**租用戶**功能區中擁有**讀取**和**寫入**權限。

您無法刪除從Kaspersky Unified Monitoring and Analysis Platform遷移來的根租用戶和共用租用戶。

若要刪除租用戶：

1. 在主應用程式視窗中，轉至**設定→租用戶**區段。
   租用戶篩選器隨即開啟。該清單僅包含您至少擁有**讀取**存取權限的租用戶。
2. 選取您要刪除的規則旁邊的核取方塊。如果選定的租用戶有子租用戶，它們將自動選取且您無法取消選擇。
3. 按一下**刪除**按鈕。
4. 輸入要刪除的租用戶的名稱確認操作。如果租用戶有子租用戶，它們也會被列為要刪除的租用戶。

選定的租用戶、其子租用戶（如果有）和相關物件將被刪除。

設定電子郵件通知

您可以透過管理伺服器和外部 SMTP 伺服器，設定 Kaspersky Next XDR Expert 中所發生事件的電子郵件通知。為此，您必須設定與SMTP伺服器的連線設定。

若要設定SMTP伺服器連線：

1. 在主功能表中，轉至**設定 → 租用戶**。
   螢幕上將顯示租用戶清單。
2. 按一下所需政策的名稱。
   租用戶內容視窗隨即開啟。
3. 轉至**設定**頁籤，然後在**偵測和回應**部分中，按一下**郵件伺服器連線** 。
4. 在右側窗格中，按一下**檢視內容**按鈕。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

   > 無論租用戶綁定到哪個管理伺服器，此視窗都會顯示主管理伺服器的內容以及主管理伺服器的SMTP設定。

5. 依照設定通知傳遞中步驟2所述設定參數。

設定與SMTP伺服器的連線後，使用者將開始接收來自Kaspersky Next XDR Expert的電子郵件。

您可以建立電子郵件通知範本，在特定警示或事件觸發時傳送給使用者。這些範本也可以編輯和刪除。

建立通知範本

在Kaspersky Next XDR Expert中設定事件電子郵件通知後，您可以為這些電子郵件通知建立自訂範本。

若要編輯通知範本，您必須具有以下其中一種XDR角色：主管理員、租用戶管理員或SOC管理員。

部署Kaspersky Next XDR Expert時，您在根租用戶中擁有電子郵件通知範本。如果您建立子租用戶，它會自動從父租用戶複製設定。由於子租用戶和父租用戶的設定不相關，因此您在子租用戶設定中所做的變更不會影響父租用戶中的設定，反之亦然。

若要建立電子郵件通知範本：

1. 在主功能表中，轉至**設定** → **租用戶**。
   租用戶清單隨即顯示。
2. 按一下所需政策的名稱。
   這會開啟租用戶內容視窗。
3. 轉到**設定**頁籤，然後在**偵測和回應**部分中，按一下**電子郵件範本**。
   可以設定通知範本的事件類型表隨即顯示。
4. 如果在步驟2中選擇了根租用戶，請在**管理伺服器顯示名稱**欄位中輸入要在電子郵件中警示和事件連結中使用的位址。
5. 按一下**建立**按鈕，然後在開啟的下拉式清單中選取要為其建立電子郵件通知範本的事件類型。
6. 在開啟的**建立電子郵件範本**窗格中，指定以下設定：

   可用欄位會根據所選事件類型而有所不同。

   - 在**名稱**欄位中，指定電子郵件通知範本的名稱。
   - 若要變更電子郵件通知範本的事件類型，請在**事件類型**欄位中選擇新的事件類型。
   - 若要為選定的事件類型啟用電子郵件通知，請在**已啟用**欄位中將切換按鈕移至**狀態**位置。
     您也可以從事件類型表中啟用電子郵件通知。預設情況下，電子郵件通知是禁用的。
   - 在**主旨**欄位中，指定電子郵件通知的主題。必填欄位。
     您也可以在**主旨**欄位中使用警示欄位、事件欄位和KUMA 正規化事件欄位，例如`New incident in OSMP: {{ .InternalID }}, {{ .Name }}`。
   - 在**範本**欄位中，編寫電子郵件通知訊息。
     電子郵件通知訊息範例

     ```
     您好，<br>
     <br>
     ```

```
警示 {{ .InternalID }}{{ with escapeHTML .Rules.Names }}「{{ . }}」{{ else }}{{ end }} 已於 {{ .CreatedAt }}
註冊。<br>
<br>
警示詳細資訊：<br>
<br>
租用戶：{{ .TenantID }}<br>
警示嚴重程度：{{ .Severity }}<br>
首次發現警示時間：{{ .FirstEventTime }}<br>
最後發現警示時間：{{ .LastEventTime }}<br>
有關警示的完整資訊可在 OSMP 網頁介面中取得：{{ link_alert . }}<br>
<br>
Open Single Management Platform
```

您還可以使用警示欄位、事件欄位、KUMA規範化事件欄位和HTML標籤。

編寫範本時，您可以使用下列函式：

- `date` — 定義日期與時間格式。該函式將以毫秒為單位的時間（UNIX 時間）作為第一個參數。第二個參數可用於傳遞 RFC 標準格式的時間。時區無法變更。

  ```
  {{range .Events }}
  Service name: {{.Event.ServiceName}}
  Device host name:  {{.Event.DeviceHostName}}
  Message: {{.Event.Message}}
  {{end}}
  ```

  巢狀物件可以有自己的巢狀物件。您可以使用巢狀範圍函式存取它們。

- `limit` — 限制 `range` 函式傳回的物件數量。
- `link_alert` — 產生警示的連結，其 URL 指定於**管理伺服器顯示名稱**欄位中。
- `link_incident` — 產生事件的連結，其 URL 指定於**管理伺服器顯示名稱**欄位中。
- `link` — 以連結形式呈現，使用者在收到通知電子郵件時可開啟該連結。

- 在**收件者**欄位中，指定一個或多個用於傳送通知的電子郵件地址。
- 在**關聯規則**下拉清單中，選擇一個或多個關聯規則，電子郵件通知將根據這些規則發送。
- 在**基於嚴重等級的通知**欄位中，選擇觸發電子郵件通知的警示最低嚴重等級。嚴重等級低於指定等級的警示將不會觸發電子郵件通知。
- 在**偵測技術**下拉式清單中，選取一個或多個會觸發電子郵件通知的偵測技術。
- 如有必要，在**描述**欄位中，寫下通知範本的描述。

7. 點擊**建立**按鈕。

   建立電子郵件範本視窗隨即關閉。

8. 在租用戶內容視窗中，儲存變更。

電子郵件通知範本隨即建立並儲存。當Kaspersky Next XDR Expert中發生所選類型的事件時，範本通知將會傳送到您指定的電子郵件地址。

編輯並刪除通知範本

您可以編輯或刪除有關Kaspersky Next XDR Expert中發生的事件的電子郵件通知範本。

若要編輯或刪除通知範本，您需要具備下列其中一個 XDR 角色：主管理員、租用戶管理員或 SOC 管理員。

部署Kaspersky Next XDR Expert時，您在根租用戶中擁有電子郵件通知範本。如果您建立子租用戶，它會自動從父租用戶複製設定。由於子租用戶和父租用戶的設定不相關，因此您在子租用戶設定中所做的變更不會影響父租用戶中的設定，反之亦然。

若要編輯電子郵件通知範本：

1. 在主功能表中，轉至**設定 → 租用戶**。

   租用戶清單隨即顯示。

2. 按一下所需政策的名稱。

   這會開啟租用戶內容視窗。

3. 前往**設定**索引標籤，然後按一下**電子郵件範本**。

4. 在表格的**事件類型**欄位中，按一下要編輯的通知範本的事件類型。

5. 在開啟的**編輯電子郵件範本**視窗中，更改必要的設定。

6. 儲存您的變更。

   編輯電子郵件範本視窗隨即關閉。

7. 儲存您的變更。

   郵件通知範本隨即編輯並儲存。當Kaspersky Next XDR Expert中發生所選類型的事件時，範本通知將會傳送到您指定的電子郵件地址。

若要刪除電子郵件通知範本：

1. 在主功能表中，轉至**設定 → 租用戶**。

   租用戶清單隨即顯示。

2. 按一下所需政策的名稱。

   這會開啟租用戶內容視窗。

3. 前往**設定**索引標籤，然後按一下**電子郵件範本**。

4. 選取您要刪除的通知範本旁邊的核取方塊。

5. 點擊**刪除**按鈕。

6. 在開啟的視窗中，確認刪除操作：

郵件通知範本隨即刪除。

設定儲存用於存取共用網路資源的憑證

透過取得磁碟映像和取得記憶體轉儲回應操作取得的檔案需要大量的可用空間。因此，這些檔案被儲存到共用網路資源中。

如果使用多個共用網路資源，則必須為每個資源指定憑證。

若要執行此操作，您必須擁有下列XDR角色之一：主管理員、 SOC管理員、租用戶管理員。

若要設定存取共用網路資源的憑證：

1. 在主功能表中，轉至**設定 → 租用戶**。
螢幕上將顯示租用戶清單。

2. 按一下所需政策的名稱。
這會開啟租用戶內容視窗。

3. 轉至**設定**頁籤，然後選擇**網路共用憑證**部分。

4. 按一下**新增**按鈕。
新增憑證窗格隨即開啟。

5. 請在對應的欄位中指定用於存取共用網路資源的帳戶的登入名稱和密碼。

> 儲存設定後，密碼將無法刪除。

根據需要，可以在**描述**欄位中新增備注。

6. 按一下**儲存**按鈕。

窗格隨即關閉，設定將儲存並顯示在表格中。

根據需要，您可以透過點擊表格中指定登入的連結來編輯設定，或者透過選中表格中設定名稱旁邊的核取方塊，然後按一下**刪除**來刪除設定。

設定排定的IOC掃描

您可以在安裝了端點代理元件的裝置上設定IOC掃描的排程。如果設定了掃描排程，端點代理程式會根據IOC規則，每天在已啟用排定掃描的裝置上搜尋入侵指標。

預設情況下， IOC掃描每天執行一次。您可以變更掃描的開始時間和持續時間，或停用每日掃描。

若要設定IOC掃描排程：

1. 在主功能表中，轉至**設定** → **租用戶**。

   租用戶篩選器隨即開啟。清單僅包含您至少擁有**讀取**存取權限的租用戶。

2. 按一下所需政策的名稱。

   這會開啟租用戶內容視窗。

3. 選取**設定**頁籤。

4. 在**掃描設定**區段，選擇**IOC 掃描排程**頁籤。

5. 開啟**每日掃描**切換開關，然後指定掃描排程的設定：

   - **開始時間 (UTC)**。IOC掃描開始的時間。時間以您正在執行設定的OSMP伺服器的時區為準。

     如果端點代理程式收到新的掃描排程的時間晚於**開始時間 (UTC)**指定的時間，則下一次掃描將在第二天**開始時間 (UTC)**指定的時間啟動。

   - **最大掃描持續時間（小時）**。IOC掃描的時間限制以小時為單位。達到此限制後，端點代理程式將結束掃描進程，無論是否完成。

6. 點選**儲存**或**儲存並關閉**以儲存設定。

儲存更改後，IOC掃描的新排程隨即生效。如果掃描偵測到威脅，則會建立IOC警示。

Kaspersky Endpoint Security for Windows的限制

如果IOC規則中定義的IOC搜尋範圍包括RegistryItem資料類型，Kaspersky Endpoint Security for Windows會掃描有限的登錄檔金鑰集。

在檔案儲存庫中配置檔案的自動輪詢

透過限制**檔案**儲存庫的空間來確保檔案的自動輪換：一旦達到限制，儲存庫中最舊的檔案將被刪除。如果您沒有指定限制，在**部署Kaspersky Next XDR Expert**時為儲存庫分配的空間用完後，您將無法將新檔案上傳到檔案儲存庫。

例如，在部署程序期間，已為**檔案**儲存庫配置 20 GB 的磁碟空間。接著，您在租用戶設定中指定 10 GB 作為限制，當達到此限制時，系統將刪除**檔案**儲存庫中最舊的檔案。如果您未指定任何限制，當使用量達到 20 GB 時，您將無法將檔案上傳至**檔案**儲存庫。

若要在「檔案」儲存庫中設定檔案自動輪換功能：

1. 在主功能表中，轉至**設定** → **租用戶**。

   螢幕上將顯示租用戶清單。

2. 按一下所需政策的名稱。

   租用戶內容視窗隨即開啟。

3. 轉到**設定**頁籤，然後在**檔案輪換**部分執行下列操作：

   a. 在**自動檔案輪換**欄位中，將切換按鈕切換到**已啟用**位置。

   b. 在「最大儲存限制」欄位中，指定將從**檔案**儲存庫中刪除最舊檔案的檔案卷。
   最小值為1GB。

   c. 按一下**儲存**或**儲存並關閉**以儲存設定。

自動檔案輪換隨即啟用並設定。

聯絡技術支援

本節介紹如何獲取技術支援以及其適用條款。

如何取得技術支援

如果您在Kaspersky Next XDR Expert文件或有關Kaspersky Next XDR Expert的任何資訊來源中找不到問題的解決方案，請聯絡卡巴斯基客戶服務。技術支援專家將回答您關於Kaspersky Next XDR Expert安裝和使用的所有問題。

卡巴斯基在Kaspersky Next XDR Expert的生命週期內提供支援（請參閱應用程式支援生命週期頁面）。在聯絡技術支援之前，請先閱讀支援規則。

您可以透過以下任一方式聯絡技術支援：

- 造訪技術支援網站
- 從 Kaspersky CompanyAccount 入口網站向技術支援傳送請求

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount 是供使用 Kaspersky 應用程式的公司使用的入口網站。Kaspersky CompanyAccount 入口網站旨在透過網上請求促進使用者和卡巴斯基專家之間的互動。您可以使用 Kaspersky CompanyAccount 來追蹤網上請求的狀態，並儲存它們的歷史記錄。

您可以在 Kaspersky CompanyAccount 上的單一帳戶下註冊組織的所有員工。單一帳戶可讓您集中管理註冊員工向卡巴斯基發出的電子請求，並透過 Kaspersky CompanyAccount 管理這些員工的權限。

Kaspersky CompanyAccount 入口網站提供以下語言版本：

- 英語
- 西班牙語
- 意大利語
- 德語
- 荷蘭語
- 葡萄牙語
- 俄語

- 法語
- 日本語

如要瞭解更多有關 Kaspersky CompanyAccount 的資訊，請參閱技術支援網站。

已知問題與限制

Kaspersky Next XDR Expert具有許多限制，這些限制對於應用程式的執行並不重要：

- 10721464：停用 EDR 並將資產移至 KATA 時，該資產在資產表格的 **資產來源** 欄中仍保留「EDR」值（**資產（裝置）→ Detection and response**）。這可能導致無法執行 KATA 回應措施。
- 10079501：使用實例階層時，在卡巴斯基安全管理中心中指派的權限不會從父實例複寫到子實例。為確保正確運作，請在每個子實例上手動將所需權限指派給已複寫的使用者。
- 10112300：如果憑證信任鏈中斷，網頁介面不會顯示通知。此問題只能透過間接跡象識別，例如缺少資源繼承。當從父 OSMP 實例開啟繼承自父 OSMP 實例或原本屬於子 OSMP 實例的資源時，會顯示以下訊息：「SIEM 元件連線錯誤。」

  解決方法：取代憑證並修復實例階層。
- 10111236：在長條圖小工具中，代表接近0%的小數值的長條不會顯示在圖表上。
- 9302142：Microsoft Windows on Arm不支援**使用網路代理作為 DMZ 連線閘道**選項。
- 10011047：對於升級至版本2.1 HF2之前建立的租用戶，IOC掃描排程功能在介面中可能會顯示為已啟用，但排程IOC掃描實際上已停用。
- 10141948：在執行 Astra Linux（核心版本為 6.12.60-1-generic 或更新版本）的管理員裝置上，KDT 命令會延遲約 6 分鐘執行。作為因應措施，請以 root 使用者身分執行以下命令：

  ```
  echo "N" > /sys/module/nfs/parameters/localio_enabled
  ```
- 10042351：當您取得記憶體佔用量為3GB或以上的處理程序記憶體傾印時，回應操作會啟動但不會完成。
- 9957846：如果KICS/KATA資產在匯入到第一個租用戶後又匯入到第二個租用戶，則這些資產將從第一個租用戶中移除並移至第二個租用戶。如果設定了排程匯入，則資產可能會在租用戶之間持續移動。
- 9823258: 如果將整合至Kaspersky Next XDR Expert中的管理伺服器作為從屬管理伺服器新增至另一個整合XDR的管理伺服器，則無法**透過新增從屬管理伺服器精靈**自動上傳管理伺服器憑證。在這種情況下，您必須手動上傳輔助伺服器的憑證。
- 9495472: 如果您打算在基礎設施中使用多個租用戶，請為每個租用戶建立一個單獨的收集器。
- 9218282: Kaspersky Next XDR Expert 2.0採用了更新的事件資料模型。基於先前資料模型的常規程式可能無法如預期運作。您需要更新在Kaspersky Next XDR Expert 1.4及更早版本中建立的常規程式，以確保它們能夠與新的事件資料模型正確相容。
- 9365692: 當使用自簽名憑證時，從在Kaspersky Endpoint Security for Windows中啟用了**加密連線掃描**選項的裝置到另一個裝置的遠端終端連線將被阻止。若要允許遠端終端連線到目標裝置，請執行下列其中一項操作：
  - 在連線裝置上使用受信任憑證。
  - 將連線裝置的網址從加密連線掃描中排除。
  - 允許存取具有不受信任憑證的網域。

- 9117520: 使用不同的資料庫名稱和不同的憑證從備份還原Kaspersky Next XDR Expert時，部署會在`klnagchk -fullwait`驗證步驟停止。
- 8690777: 僅支援在Linux裝置上使用常規程式啟動協力廠商自訂指令碼。
- 8428740: 指定彙總或分段規則的觸發器時，具有相互依賴參數的函數的jq運算式被視為無效。例如：`any(.Observables[]; .Type == "ip" and .Value == "1.1.1.1")`
- 7143556: 關閉Kubernetes叢集的基礎架構伺服器然後重新啟動它們後，嘗試登入OSMP主控台會傳回錯誤。
- 7268335: 如果在受管裝置管理群組內容的**使用自訂權限**頁籤上啟用**存取權限**選項，則無法將用戶端裝置從Open Single Management Platform匯出至KUMA。
- 6704698: 即使Kaspersky Endpoint Security for Windows網頁外掛程式，包含透過Kaspersky Endpoint Security for Windows回應操作的常規程式也會在常規程式清單中顯示為可用。
- 7208621: 當您匯入*將更新下載到發佈點儲存庫*或*更新驗證*工作時，將啟用**選擇工作將被指派到的裝置**選項。這些工作不能被指派給裝置分類或特定裝置。如果將*下載更新指派到發佈點儲存庫*或將*更新驗證*工作指派到特定裝置，則工作將無法正確匯入。
- 6646913: 在調查圖表中，重新排列節點的操作不正確。
- 6962370: 將資料從卡巴斯基安全管理中心 Windows的輔助管理伺服器移轉到Kaspersky Next XDR Expert的主管理伺服器時，遷移精靈無法完成**匯入資料**步驟。如果您在從屬管理伺服器上建立全域工作（例如，*遠端解除安裝應用程式*工作），並在遷移精靈中僅將**要匯出的託管應用程式**參數設為**卡巴斯基安全管理中心管理伺服器**值，則會發生此問題。
- 6983311: 接收卡巴斯基公告不可用。
- 6810101: 儘管Kaspersky Next XDR Expert不支援行動裝置管理，但管理伺服器內容視窗包含行動裝置的設定。
- 6822204: 有關可供下載的新版網頁外掛程式的通知已停用。您可以使用卡巴斯基部署工具套件更新外掛程式。
- 6919635: 建立新租用戶後，與該租用戶相關的警示將傳送到伺服器，但不會顯示在警示表中。您可能需要重新整理網頁以更新表格資料。
- 9763104: 在管理伺服器屬性視窗中，**雙步驟驗證**頁籤顯示了**允許產生秘密金鑰的使用者**表。由於所有使用者都被允許產生秘鑰，因此該表不合理。
- 10412424: Kaspersky Next XDR Expert 從 2.1 版升級到 2.2 版後，**監控 → 資源**區段無法開啟。在瀏覽器設定中刪除 Cookie 後，該區段即可正確開啟。
- 10456232: 如果您要升級至 2.3 版，且已設定多個 OSMP 實例的階層，則子實例繼承的資源及在子實例中建立的資源可能不會顯示在父實例中。如果發生此情況，升級後請在子實例上重新儲存資源。或者，您可以將資源匯出後再匯入至同一租用戶（機密類型的資源除外）。
- 10751535: 如果您使用的是 2.3.224 之前的 Kaspersky Next XDR Expert 版本，且已設定多個 OSMP 實例的階層，則對於在子實例上建立或由子實例繼承的資源，父實例上的資源清單不會在**資源種類**欄中顯示值。

如需 OSMP 的已知問題清單，請參閱卡巴斯基安全管理中心文件。

故障解決

本節提供使用Kaspersky Next XDR Expert時可能遇到的常見問題的解決方案。

使用自簽名憑證時，遠端終端連線會被封鎖

當使用自簽名憑證時，從在Kaspersky Endpoint Security for Windows中啟用了**加密連線掃描**選項的裝置到另一個裝置的遠端終端連線將被阻止。

若要允許遠端終端連線到目標裝置，請執行下列其中一項操作：

- 在連線裝置上使用受信任憑證。
- 將連線裝置的網址從加密連線掃描中排除。
- 允許存取具有不受信任憑證的網域。

附錄

本章節提供的資訊與正文中的參考資訊相輔相成。

元件手動啟動和安裝命令

本章節包含KUMA可執行檔 /opt/kaspersky/kuma/kuma的參數，可用於手動啟動或安裝KUMA服務。當您需要查看伺服器作業系統主控台中的輸出時，這會很有用。

命令參數

命令	描述
`tools`	啟動KUMA管理工具。
`collector`	安裝、啟動或刪除收集器服務。
`core`	安裝、啟動或解除安裝核心服務。
`correlator`	安裝、啟動或刪除關聯器服務。
`agent`	安裝、啟動或刪除代理程式服務。
`help`	取得有關可用命令和參數的資訊。
`license`	取得有關產品授權的資訊。
`storage`	啟動或安裝儲存體。
`version`	取得有關程式版本的資訊。

標誌：

`-h`、`--h` 用於取得任何 kuma 命令的協助。例如，`kuma <component> --help`。

例如：

- `kuma version` 用於取得 KUMA 安裝程式的版本。
- `kuma core -h` — 用於取得 KUMA 安裝程式核心命令的協助。
- `kuma collector --core <` 收集器應取得自身設定的伺服器位址 `> --id <` 已安裝服務的 `ID> --api.port <` 連接埠 `>` 用於啟動收集器服務安裝。

KUMA檔案的完整性檢查

在 KUMA 目標主機上，若 KUMA 服務（收集器、關聯器、儲存體、事件路由器）安裝於 Kubernetes 叢集之外，則會使用位於 `/opt/kaspersky/kuma/integrity/bin/ directory` 的指令碼執行完整性驗證。此目錄包含服務專屬的完整性檢查指令碼（`check_collector.sh`、`check_correlator.sh`、`check_storage.sh`、`check_event_router.sh`），以及用於驗證 Windows 版 KUMA 代理的指令碼（`check_kuma_exe.sh`）。此外，還包含完整性檢查機制內部使用的驗證公用程式（`integrity_checker` 和 `integrity_checker.sh`）。

已在執行服務的機器上新增了完整性檢查指令碼，並將日誌記錄到dmsg：

- `manual_integrity_check.sh`—可手動對所需的 KUMA 服務執行完整性檢查（搭配旗標 `collector`、`correlator`、`storage`、`eventRouter` 使用）。
- `systemd_integrity_check.sh` — 在啟動或重新啟動 KUMA 服務時執行完整性檢查。

若要檢查元件檔案的完整性：

1. 在安裝了KUMA服務的KUMA目標主機上，執行以下命令以導覽到包含指令碼集的目錄：

   ```
   cd /opt/kaspersky/kuma/integrity/bin
   ```

2. 執行所需的指令碼（例如 `check_collector.sh`）。

   元件檔案的完整性隨即檢查。

   檢查每個組件的結果隨即以以下格式顯示：

- `Summary` 區段描述了已掃描物件的數量以及掃描狀態：完整性未確認/物件已略過/完整性已確認：
  - `Manifests` – 已處理的清單檔案數量。
  - `Files` – 執行 KUMA 完整性檢查時不使用。
  - `Directories` – 執行 KUMA 完整性檢查時不使用。
  - `Registries` – 執行 KUMA 完整性檢查時不使用。
  - `Registry values` – 執行 KUMA 完整性檢查時不使用。
- 元件完整性檢查結果：
  - `SUCCEEDED` – 完整性已確認。
  - `FAILED` – 完整性遭破壞。

完整性檢查成功後的命令輸出範例

```
================================================>
Summary( failed / skipped / succeeded ):
Manifests: 0 / 0 / 1
Files: 0 / 0 / 1
Directories: 0 / 0 / 0
Registries: 0 / 0 / 0
Registry values: 0 / 0 / 0
================================================>
SUCCEEDED
```

在輸出中，成功驗證的清單數量顯示在 succeeded 欄下方的 `Manifests` 行中。狀態 `SUCCEEDED` 表示所有已驗證的元件均與已簽署的清單相符，且未偵測到完整性違規。如果發現差異，檢查結果會報告為 `FAILED`。

使用此機制驗證安裝在Kubernetes叢集之外的KUMA服務的完整性。

您也可以檢查已安裝的Kaspersky Next XDR Expert元件的完整性。

標準化事件資料模型

本章節介紹KUMA標準化事件資料模型。KUMA關聯器處理的所有用於偵測警報的事件都必須符合此模型。

不符合此資料模型的事件必須使用收集器匯入此格式（或進行標準化）。

標準化事件資料模型

欄位名稱	資料類型	欄位大小	描
			欄位名稱反映其用途。欄位可修改。
ApplicationProtocol	字串	31 個字元	應用層協定的名稱。例如，HTTPS、SSH、Telnet。
BytesIn	數字	範圍：-9223372036854775808到9223372036854775807	已接收的位元組數。
BytesOut	數字	範圍：-9223372036854775808到9223372036854775807	已傳送的位元組數。
DestinationAddress	字串	45 個字元	將對其執行操作的資產的IPv4或IPv6位址。例如，0.0.0.0或xx
DestinationCity	字串	1023 個字元	與DestinationAddress欄位中的IP位址對應的城市。
DestinationCountry	字串	1023 個字元	與DestinationAddress欄位中的IP位址對應的國家/地區。
DestinationDnsDomain	字串	255 個字元	目標的完全限定網域的DNS部分。
DestinationHostName	字串	1023 個字元	目標的主機名稱。目標的FQDN（如果可用）。
DestinationLatitude	浮點	+/- 1.7E-308 至 1.7E+308	與DestinationAddress欄位中的IP位址對應的經度。
DestinationLongitude	浮點	+/- 1.7E-308 至 1.7E+308	與DestinationAddress欄位中的IP位址對應的緯度。
DestinationMacAddress	字串	17 個字元	目標的MAC位址。例如，aa:bb:cc:dd:ee:00
DestinationNtDomain	字串	255 個字元	目標的Windows網域。
DestinationPort	數字	範圍：-9223372036854775808到9223372036854775807	目標的連接埠號碼。
DestinationProcessID	數字	範圍：-9223372036854775808到9223372036854775807	在目標上註冊的系統進程ID。
DestinationProcessName	字串	1023 個字元	在目標上註冊的系統進程名稱。例如，sshd、telnet。
DestinationRegion	字串	1023 個字元	與DestinationAddress欄位中的IP位址對應的區域。
DestinationServiceName	字串	1023 個字元	目標端服務的名稱。例如，sshd。
DestinationTranslatedAddress	字串	45 個字元	轉換後的目標IPv4或IPv6位址。例如，0.0.0.0或xxxx:xxxx:xxxx
DestinationTranslatedPort	數字	範圍：-9223372036854775808到9223372036854775807	轉換後目標中的連接埠號碼。
DestinationUserID	字串	1023 個字元	目標的使用者ID。
DestinationUserName	字串	1023 個字元	目標的使用者名稱
DestinationUserPrivileges	字串	1023 個字元	用來辨識目標使用者權限的角色名稱。例如，使用者、訪客
DeviceAction	字串	63 個字元	事件來源所採取的動作。例如，封鎖、偵測。
DeviceAddress	字串	45 個字元	接收事件的裝置的IPv4或IPv6位址。例如，0.0.0.0或xxxx:xxxx
DeviceCity	字串	1023 個字元	與DeviceAddress欄位中的IP位址對應的城市。
DeviceCountry	字串	1023 個字元	與DeviceAddress欄位中的IP位址對應的國家/地區。

DeviceDnsDomain	字串	255 個字元	接收事件的裝置的完全限定網域名稱的DNS部分。
DeviceEventClassID	字串	1023 個字元	事件來源指派的事件類型ID。
DeviceExternalID	字串	255 個字元	事件來源指派的裝置或應用程式ID。
DeviceFacility	字串	1023 個字元	事件來源設定的設施參數值。
DeviceHostName	字串	100 個字元	接收事件的裝置的名稱。裝置的FQDN（如果可用）。
DeviceInboundinterface	字串	128 個字元	傳入連線介面的名稱。
DeviceLatitude	浮點	+/- 1.7E-308 至 1.7E+308	與DeviceAddress欄位中的IP位址對應的經度。
DeviceLongitude	浮點	+/- 1.7E-308 至 1.7E+308	與DeviceAddress欄位中的IP位址對應的緯度。
DeviceMacAddress	字串	17 個字元	接收事件的資產的MAC位址。例如，aa:bb:cc:dd:ee:00
DeviceNtDomain	字串	255 個字元	裝置的Windows網域名稱。
DeviceOutboundinterface	字串	128 個字元	傳出連線介面的名稱。
DevicePayloadID	字串	128 個字元	與原始事件關聯的有效負載的唯一ID。
DeviceProcessID	數字	範圍：-9223372036854775808到9223372036854775807	產生事件的裝置上的系統進程的ID。
DeviceProcessName	字串	1023 個字元	進程的名稱。
DeviceProduct	字串	63 個字元	產生事件的應用程式的名稱DeviceVendor、DeviceProduct和
DeviceReceiptTime	數字	範圍：-9223372036854775808到9223372036854775807	裝置接收事件的時間。
DeviceRegion	字串	1023 個字元	與DeviceAddress欄位中的IP位址對應的區域。
DeviceTimeZone	字串	255 個字元	產生事件的裝置的時區。
DeviceTranslatedAddress	字串	45 個字元	接收事件的裝置的重新轉換的IPv4或IPv6位址。例如，0.0.0.0
DeviceVendor	字串	63 個字元	事件來源的供應商名稱。DeviceVendor、DeviceProduct和D
DeviceVersion	字串	31 個字元	事件來源的應用程式版本。DeviceVendor、DeviceProduct和
EndTime	數字	範圍：-9223372036854775808到9223372036854775807	事件發生的日期和時間（時間戳記）。
EventOutcome	字串	63 個字元	操作的結果。例如，成功、失敗。
ExternalID	字串	40 個字元	可以儲存ID的欄位。
FileCreateTime	數字	範圍：-9223372036854775808到9223372036854775807	檔案建立的時間。
FileHash	字串	255 個字元	檔案的雜湊值。範例：CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C4
FileID	字串	1023 個字元	檔案的ID
FileModificationTime	數字	範圍：-9223372036854775808到9223372036854775807	檔案上次修改的時間。
FileName	字串	1023 個字元	檔案名稱，未指定檔案路徑。
FilePath	字串	1023 個字元	檔案路徑，包括檔案名稱。
FilePermission	字串	1023 個字元	檔案權限清單。
FileSize	數字	範圍：-9223372036854775808到9223372036854775807	檔案大小。
檔案類型	字串	1023 個字元	檔案類型。
訊息	字串	1023 個字元	事件的簡要描述。
名稱	字串	512 個字元	事件的名稱。

OldFileCreateTime	數字	範圍：-9223372036854775808到9223372036854775807	從事件中建立OLD檔案的時間。時間以UTC0指定。在KUMA
OldFileHash	字串	255 個字元	Old檔案的雜湊值。範例：CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C4
OldFileID	字串	1023 個字元	OLD檔案的ID。
OldFileModificationTime	數字	範圍：-9223372036854775808到9223372036854775807	OLD檔案的上次修改時間。
OldFileName	字串	1023 個字元	OLD檔案的名稱（不含檔案路徑）。
OldFilePath	字串	1023 個字元	OLD檔案的路徑，包含檔案名稱。
OldFilePermission	字串	1023 個字元	OLD檔案的權限清單。
OldFileSize	數字	範圍：-9223372036854775808到9223372036854775807	OLD檔案的大小。
OldFileType	字串	1023 個字元	OLD檔案的類型。
原因	字串	1023 個字元	有關事件原因的資訊。
RequestClientApplication	字串	1023 個字元	http請求的「user-agent」參數的值。
RequestContext	字串	2048 個字元	http請求上下文的描述。
RequestCookies	字串	1023 個字元	與http請求關聯的Cookie。
RequestMethod	字串	1023 個字元	發出http請求時所使用的方法。
RequestUrl	字串	1023 個字元	請求的URL。
嚴重等級	字串	1023 個字元	嚴重等級。這可以是原始事件的嚴重等級欄位或等級欄位。
SourceAddress	字串	45 個字元	來源的IPv4或IPv6位址。範例格式：0.0.0.0或xxxx:xxxx:xxxx:xx
SourceCity	字串	1023 個字元	與SourceAddress欄位中的IP位址對應的城市。
SourceCountry	字串	1023 個字元	與SourceAddress欄位中的IP位址對應的國家。
SourceDnsDomain	字串	255 個字元	來源的完全限定網域名稱的DNS部分。
SourceHostName	字串	1023 個字元	事件來源裝置的Windows網域。
SourceLatitude	浮點	+/- 1.7E-308 至 1.7E+308	與SourceAddress欄位中的IP位址對應的經度。
SourceLongitude	浮點	+/- 1.7E-308 至 1.7E+308	與SourceAddress欄位中的IP位址對應的緯度。
SourceMacAddress	字串	17 個字元	來源的MAC位址。格式範例：aa:bb:cc:dd:ee:00
SourceNtDomain	字串	255 個字元	來源的Windows網域名稱。
SourcePort	數字	範圍：-9223372036854775808到9223372036854775807	來源的連接埠號碼。
SourceProcessID	數字	範圍：-9223372036854775808到9223372036854775807	系統進程ID。
SourceProcessName	字串	1023 個字元	來源中系統進程的名稱。例如sshd、telnet等。
SourceRegion	字串	1023 個字元	與SourceAddress欄位中的IP地址對應的區域。
SourceServiceName	字串	1023 個字元	來源端服務的名稱。例如，sshd。
SourceTranslatedAddress	字串	15 個字元	來源轉換後的IPv4或IPv6位址。範例格式：0.0.0.0或xxxx:xxxx
SourceTranslatedPort	數字	範圍：-9223372036854775808到9223372036854775807	轉換後來源的連接埠號碼。
SourceUserID	字串	1023 個字元	來源的使用者ID。
SourceUserName	字串	1023 個字元	來源的使用者名稱。
SourceUserPrivileges	字串	1023 個字元	識別來源使用者權限的角色名稱。例如，使用者、訪客、管理

StartTime	數字	範圍：-9223372036854775808到9223372036854775807	與事件關聯的活動開始的日期和時間（時間戳記）。
戰術	字串	128 個字元	來自MITRE ATT&CK矩陣的戰術名稱。
技術	字串	128 個字元	來自MITRE ATT&CK矩陣的技術名稱。
TransportProtocol	字串	31 個字元	OSI模型的傳輸層協定名稱（TCP、UDP等）。
類型	數字	範圍：-9223372036854775808到9223372036854775807	事件類型：1 - 基本，2 - 彙總，3 - 關聯，4 - 稽核，5 - 監控，
使用者可以定義欄位的用途。欄位可修改。			
DeviceCustomDate1	數字，時間戳記	範圍：-9223372036854775808到9223372036854775807	用於對應日期和時間值（時間戳記）的欄位。時間以UTC0格區顯示。
DeviceCustomDate1Label	字串	1023 個字元	用來描述DeviceCustomDate1欄位用途的欄位。
DeviceCustomDate2	數字，時間戳記	範圍：-9223372036854775808到9223372036854775807	用於對應日期和時間值（時間戳記）的欄位。時間以UTC0格區顯示。
DeviceCustomDate2Label	字串	1023 個字元	用來描述DeviceCustomDate2欄位用途的欄位。
DeviceCustomFloatingPoint1	浮點	+/- 1.7E-308 至 1.7E+308	用於對應浮點數的欄位。
DeviceCustomFloatingPoint1Label	字串	1023 個字元	用於描述DeviceCustomFloatingPoint1欄位用途的欄位。
DeviceCustomFloatingPoint2	浮點	+/- 1.7E-308 至 1.7E+308	用於對應浮點數的欄位。
DeviceCustomFloatingPoint2Label	字串	1023 個字元	用於描述DeviceCustomFloatingPoint2欄位用途的欄位。
DeviceCustomFloatingPoint3	浮點	+/- 1.7E-308 至 1.7E+308	用於對應浮點數的欄位。
DeviceCustomFloatingPoint3Label	字串	1023 個字元	用於描述DeviceCustomFloatingPoint3欄位用途的欄位。
DeviceCustomFloatingPoint4	浮點	+/- 1.7E-308 至 1.7E+308	用於對應浮點數的欄位。
DeviceCustomFloatingPoint4Label	字串	1023 個字元	用於描述DeviceCustomFloatingPoint4欄位用途的欄位。
DeviceCustomIPv6Address1	字串	45 個字元	用於對應IPv6位址值的欄位。格式範例：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address1Label	字串	1023 個字元	用來描述DeviceCustomIPv6Address1欄位用途的欄位。
DeviceCustomIPv6Address2	字串	45 個字元	用於對應IPv6位址值的欄位。格式範例：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address2Label	字串	1023 個字元	用來描述DeviceCustomIPv6Address2欄位用途的欄位。
DeviceCustomIPv6Address3	字串	45 個字元	用於對應IPv6位址值的欄位。格式範例：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address3Label	字串	1023 個字元	用來描述DeviceCustomIPv6Address3欄位用途的欄位。
DeviceCustomIPv6Address4	字串	45 個字元	用於對應IPv6位址值的欄位。例如：y:y:y:y:y:y:y:y
DeviceCustomIPv6Address4Label	字串	1023 個字元	用於描述DeviceCustomIPv6Address4欄位用途的欄位。
DeviceCustomNumber1	數字	範圍：-9223372036854775808到9223372036854775807	用於對應整數值的欄位。
DeviceCustomNumber1Label	字串	1023 個字元	用來描述DeviceCustomNumber1欄位用途的欄位。
DeviceCustomNumber2	數字	範圍：-9223372036854775808到9223372036854775807	用於對應整數值的欄位。
DeviceCustomNumber2Label	字串	1023 個字元	用來描述DeviceCustomNumber2欄位用途的欄位。
DeviceCustomNumber3	數字	範圍：-9223372036854775808到9223372036854775807	用於對應整數值的欄位。
DeviceCustomNumber3Label	字串	1023 個字元	用來描述DeviceCustomNumber3欄位用途的欄位。
DeviceCustomString1	字串	4,000 個字元	用於對應字串值的欄位。
DeviceCustomString1Label	字串	1023 個字元	用來描述DeviceCustomString1欄位用途的欄位。

DeviceCustomString2	字串	4,000 個字元	用於對應字串值的欄位。
DeviceCustomString2Label	字串	1023 個字元	用來描述DeviceCustomString2欄位用途的欄位。
DeviceCustomString3	字串	4,000 個字元	用於對應字串值的欄位。
DeviceCustomString3Label	字串	1023 個字元	用來描述DeviceCustomString3欄位用途的欄位。
DeviceCustomString4	字串	4,000 個字元	用於對應字串值的欄位。
DeviceCustomString4Label	字串	1023 個字元	用來描述DeviceCustomString4欄位用途的欄位。
DeviceCustomString5	字串	4,000 個字元	用於對應字串值的欄位。
DeviceCustomString5Label	字串	1023 個字元	用來描述DeviceCustomString5欄位用途的欄位。
DeviceCustomString6	字串	4,000 個字元	用於對應字串值的欄位。
DeviceCustomString6Label	字串	1023 個字元	用於描述DeviceCustomString6欄位用途的欄位。
DeviceDirection	數字	範圍：-9223372036854775808到9223372036854775807	用來描述事件連線方向的欄位。「0」- 傳入連線，「1」- 傳
DeviceEventCategory	字串	1023 個字元	由向SIEM傳送事件的裝置所指派的事件類別。
FlexDate1	數字，時間戳記	範圍：-9223372036854775808到9223372036854775807	用於對應日期和時間值（時間戳記）的欄位。時間以UTC0格區顯示。
FlexDate1Label	字串	128 個字元	用來描述FlexDate1Label欄位用途的欄位。
FlexNumber1	數字	範圍：-9223372036854775808到9223372036854775807	用於對應整數值的欄位。
FlexNumber1Label	字串	128 個字元	用來描述FlexNumber1Label欄位用途的欄位。
FlexNumber2	數字	範圍：-9223372036854775808到9223372036854775807	用於對應整數值的欄位。
FlexNumber2Label	字串	128 個字元	用來描述FlexNumber2Label欄位用途的欄位。
FlexString1	字串	1023 個字元	用於對應字串值的欄位。
FlexString1Label	字串	128 個字元	用來描述FlexString1Label欄位用途的欄位。
FlexString2	字串	1023 個字元	用於對應字串值的欄位。
FlexString2Label	字串	128 個字元	用來描述FlexString2Label欄位用途的欄位。
			服務欄位。無法編輯。
AffectedAssets	巢狀[Affected]結構	-	巢狀結構，您可以從中查詢與警示相關的資產和使用者帳戶
AggregationRuleID	字串	-	彙總規則的ID。
AggregationRuleName	字串	-	處理事件的彙總規則的名稱。
BaseEventCount	數字	-	對於彙總基礎事件，這是彙總規則處理的基礎事件的數量。事件的數量。
BaseEvents	巢狀[Event]清單	-	包含基礎事件清單的巢狀結構。可以為關聯事件填寫此欄位
代碼	字串	-	在基礎事件中，這是從來源傳回的流程、函式或操作的代碼
CorrelationRuleID	字串	-	關聯規則的ID。
CorrelationRuleName	字串	-	觸發建立關聯事件的關聯規則的名稱。僅為關聯事件填寫。
DestinationAccountID	字串	-	此欄位儲存使用者ID。
DestinationAssetID	字串	-	此欄位儲存目標的資產ID。
DeviceAssetID	字串	-	此欄位儲存將事件傳送至SIEM的資產ID。

Extra	巢狀[string:string]字典	-	在原始事件的標準化過程中，此欄位可用於放置尚未對應到K 大小上限為 4 MB。
GroupedBy	字串	-	關聯規則中用於分組的欄位名稱清單。僅為關聯事件填寫。
ID	字串	-	UUID類型的唯一事件ID。對於在收集器上產生的基礎事件，ID 變。
Raw	字串	-	原始「raw」事件的非標準化文字。最大欄位大小是16,384位
ReplayID	字串	-	產生事件的逆向掃描的ID。
ServiceID	字串	-	服務實例的ID：關聯器、收集器、儲存體。
ServiceName	字串	-	KUMA管理員在建立微服務時所指派的微服務實例的名稱。
SourceAccountID	字串	-	此欄位儲存使用者ID。
SourceAssetID	字串	-	此欄位儲存事件來源的資產ID。
SpaceID	字串	-	空間的ID。
TenantID	字串	-	此欄位儲存租用戶ID。
TI	巢狀[string:string]字典	-	包含基於事件指標從外部威脅情報來源接收的字典格式的類別
TICategories	對應[String]：	-	此欄位包含基於事件中包含的指標從外部TI提供者接收的類別
時間戳記	數字	-	收集器中建立的基礎事件的時間戳。收集器建立的關聯事件的 值是基於使用者瀏覽器的時區顯示。

巢狀Affected結構

欄位	資料類型	描述
Assets	巢狀[AffectedRecord]清單	與警示關聯的資產清單和數量。
Accounts	巢狀[AffectedRecord]清單	與警示關聯的使用者帳戶清單和數量。

巢狀AffectedRecord結構

欄位	資料類型	描述
Value	字串	資產或使用者帳戶的ID。
Count	數字	資產或使用者帳戶在警示相關事件中出現的次數。

KUMA產生的欄位

KUMA產生以下無法修改的欄位：BranchID、BranchName、DestinationAccountName、DestinationAssetName、DeviceAssetName、SourceAccountName、SourceAssetName、TenantName。

設定來自KATA EDR的標準化事件資料模型

要調查資訊，事件和KATA/EDR流程的ID必須轉到標準化事件的某些欄位。若要為來自KATA/EDR的事件建立流程樹，您必須在KUMA標準化器中設定從原始事件欄位到標準化事件欄位的資料複製，如下所示：

1. 對於任何KATA/EDR事件，您必須透過複製下列欄位來設定標準化：
   - KATA/EDR 事件的 `EventType` 欄位必須複製至標準化 KUMA 事件的 `DeviceEventCategory` 欄位。
   - KATA/EDR 事件的 `HostName` 欄位必須複製至標準化 KUMA 事件的 `DeviceHostName` 欄位。
2. 對於DeviceProduct = 'KATA'的任何事件，必須根據下表設定標準化。

KATA/EDR事件欄位的標準化

KATA/EDR事件欄位	標準化事件欄位。
IOATag	DeviceCustomIPv6Address2
	IOATag
IOAImportance	DeviceCustomIPv6Address1
	IOAImportance
FilePath	FilePath
FileName	FileName
MD5	FileHash
FileSize	FileSize

3. 對於下表列出的事件，必須依據表格設定的額外功能設定。

透過複製KATA/EDR事件欄位進行額外標準化

事件	原始事件欄位	標準化事件欄位。
Process	UniqueParentPid	FlexString1
	UniquePid	FlexString2
	主機名稱	DeviceHostName
	FileName	FileName
Applock	UniquePid	FlexString2
	主機名稱	DeviceHostName
	FileName	FileName
BlockedDocument	UniquePid	FlexString2
	主機名稱	DeviceHostName
	FileName	FileName
模組	UniquePid	FlexString2
	主機名稱	DeviceHostName
	FileName	FileName
FileChange	UniquePid	FlexString2
	主機名稱	DeviceHostName
	FileName	FileName

事件	原始事件欄位	標準化事件欄位。
Driver	主機名稱	DeviceHostName
	FileName	FileName
	產品名稱	DeviceCustomString5
		產品名稱
	ProductVendor	DeviceCustomString6
		ProductVendor
Connection	UniquePid	FlexString2
	主機名稱	DeviceHostName
	URI	RequestUrl
	RemoteIP	DestinationAddress
	RemotePort	DestinationPort
PortListen	UniquePid	FlexString2
	主機名稱	DeviceHostName
	LocalIP	SourceAddress
	LocalPort	SourcePort
登錄檔	UniquePid	FlexString2
	主機名稱	DeviceHostName
	ValueName	DeviceCustomString5
		新值名稱
	KeyName	DeviceCustomString4
		新金鑰名稱
	PreviousKeyName	FlexString2
		舊密鑰名稱
	ValueData	DeviceCustomString6
		新值資料
	PreviousValueData	FlexString1
		舊值資料
	ValueType	FlexNumber1
		值類型
	PreviousValueType	FlexNumber2
		先前值類型
SystemEventLog	UniquePid	FlexString2
	主機名稱	DeviceHostName
	OperationResult	EventOutcome
	EventId	DeviceCustomNumber3
		EventId
	EventRecordId	DeviceCustomNumber2
		EventRecordId
	Channel	DeviceCustomString6
		Channel
	ProviderName	SourceUserID

事件	原始事件欄位	標準化事件欄位。
ThreatDetect	UniquePid	FlexString2
	主機名稱	DeviceHostName
	VerdictName	EventOutcome
	DetectedObjectType	OldFileType
	isSilent	FlexString1
		Is Silent
	RecordId	DeviceCustomString5
		記錄ID
	DatabaseTimestamp	DeviceCustomDate2
		資料庫時間戳記
ThreatDetectProcessingResult	UniquePid	FlexString2
	主機名稱	DeviceHostName
	ThreatStatus	DeviceCustomString5
		威脅狀態
PROCESS_INTERPRET_FILE_RUN	UniquePid	FlexString2
	主機名稱	DeviceHostName
	FileName	FileName
	InterpretedFilePath	OldFilePath
	InterpretedFileSize	OldFileSize
	InterpretedFileHash	OldFileHash
PROCESS_CONSOLE_INTERACTIVE_INPUT	UniquePid	FlexString2
	主機名稱	DeviceHostName
	InteractiveInputText	DeviceCustomString4
		命令列
AMSI掃描	UniquePid	FlexString2
	主機名稱	DeviceHostName
	ObjectContent	DeviceCustomString5
		物件內容

資產資料模型

資產的結構由包含值的欄位表示。欄位也可以包含巢狀結構。

資產欄位	值類型	描述
ID	字串	資產ID。
TenantName	字串	租用戶名稱。
DeletedAt	數字	資產刪除日期。
CreatedAt	數字	資產創建日期。
TenantID	字串	租用戶ID。
DirectCategories	巢狀字串清單	資產類別。

CategoryModels	巢狀 [Category] 結構	更改資產類別。
AffectedByIncidents	巢狀字典： [string:string TRUE/FALSE]	事件ID。
IPAddress	巢狀字串清單	資產IP位址。
FQDN	字串	資產FQDN。
Weight	數字	資產重要性。
Deleted	包含 TRUE/FALSE 值的字串	指示資產是否已從KUMA標記為刪除。
UpdatedAt	數字	資產的上次更新日期。
MACAddress	巢狀字串清單	資產MAC位址。
IPAddressInt	巢狀數字清單	數字格式的IP位址。
Owner	巢狀[OwnerInfo]結構	資產所有者資訊。
OS	巢狀[OS]結構	資產作業系統資訊。
displayName	字串	資產名稱。
APISoft	巢狀[Software]結構	資產上安裝的軟體。
APIVulns	巢狀[Vulnerability]結構	資產弱點。
KICSServerIp	字串	KICS for Networks伺服器IP位址。
KICSConnectorID	數字	KICS for Networks連接器ID。
KICSDeviceID	數字	KICS for Networks資產ID。
KICSStatus	字串	KICS for Networks資產狀態。
KICSHardware	巢狀[KICSSystemInfo]結構	從KICS for Networks接收的資產硬體資訊。
KICSSoft	巢狀[KICS系統資訊]結構	從KICS for Networks接收的資產軟體資訊。
KICSRisks	巢狀[KICSRisk]結構	從KICS for Networks接收的資產弱點資訊。
Sources	巢狀[Sources]結構	來自各種來源的資產基本資訊。
FromKSC	包含 TRUE/FALSE 值的字串	指示已從卡巴斯基安全管理中心匯入資產詳細資訊。
NAgentID	字串	接收資產資訊的卡巴斯基安全管理中心網路代理程式的ID。
KSCServerFQDN	字串	卡巴斯基安全管理中心伺服器的FQDN。
KSCInstanceID	字串	卡巴斯基安全管理中心實例ID。
KSCMasterHostname	字串	卡巴斯基安全管理中心伺服器主機名稱。
KSCGroupID	數字	卡巴斯基安全管理中心群組ID。
KSCGroupName	字串	卡巴斯基安全管理中心群組名稱
LastVisible	數字	卡巴斯基安全管理中心接收有關資產資訊的日期。
Products	巢狀字典： [string:巢狀[ProductInfo]結構]	從卡巴斯基安全管理中心接收的有關安裝在資產上的卡巴斯基應用程式的資訊。
Hardware	巢狀[Hardware]結構	從卡巴斯基安全管理中心接收的資產硬體資訊。
KSCSoft	巢狀[Software]結構	從卡巴斯基安全管理中心接收的資產軟體資訊。
KSCVulns	巢狀[弱點]結構	從卡巴斯基安全管理中心接收的資產弱點資訊。

巢狀類別結構

欄位	值類型	描述
ID	字串	類別ID。
TenantID	字串	租用戶ID。
TenantName	字串	租用戶名稱。
Parent	字串	父類別。
Path	巢狀字串清單	類別結構。
Name	字串	類別名稱。
UpdatedAt	數字	類別的上次更新。
CreatedAt	數字	類別建立日期。
Description	字串	類別描述。
Weight	數字	類別重要性。
CategorizationKind	字串	資產類別指派類型。
CategorizationAt	數字	分類日期。
CategorizationInterval	字串	類別指派間隔。

巢狀OwnerInfo結構

欄位	值類型	描述
displayName	字串	裝置擁有者的名稱。

巢狀OS結構

欄位	值類型	描述
Name	字串	作業系統的名稱。
BuildNumber	數字	作業系統的版本。

巢狀軟體結構

欄位	值類型	描述
displayName	字串	軟體名稱。
DisplayVersion	字串	軟體的版本。
Publisher	字串	軟體的發布者。

InstallDate	字串	安裝日期。
HasMSIInstaller	TRUE/FALSE 字串	指示軟體是否有MSI安裝程式。

巢狀弱點結構

欄位	值類型	描述
KasperskyID	字串	卡巴斯基所指派的弱點ID。
ProductName	字串	軟體名稱。
DescriptionURL	字串	包含弱點描述的URL。
RecommendedMajorPatch	字串	建議的更新。
RecommendedMinorPatch	字串	建議的更新。
SeverityStr	字串	弱點嚴重等級。
Severity	數字	弱點嚴重等級。
CVE	巢狀字串清單	CVE弱點ID。
ExploitExists	TRUE/FALSE 字串	指示是否存在弱點利用。
MalwareExists	TRUE/FALSE 字串	指示是否存在惡意軟體。

巢狀KICSSystemInfo結構

欄位	值類型	描述
Model	字串	裝置模型。
Version	字串	裝置版本。
Vendor	字串	供應商。

巢狀KICSRisk結構

欄位	值類型	描述
ID	數字	KICS for Networks風險的ID。
Name	字串	風險名稱。
Category	字串	風險類型。
Description	字串	風險描述。
DescriptionURL	字串	風險描述的連結。
Severity	數字	風險嚴重等級。
Cvss	數字	CVSS分數。

巢狀來源結構

欄位	值類型	描述
KSC	巢狀[SourceInfo]結構	從卡巴斯基安全管理中心接收的資產資訊。
API	巢狀[SourceInfo]結構	透過REST API接收的資產資訊。
Manual	巢狀[SourceInfo]結構	手動輸入的資產資訊。
KICS	巢狀[SourceInfo]結構	從KICS for Networks接收的資產資訊。

巢狀來源結構

欄位	值類型	描述
MACAddress	巢狀字串清單	資產MAC位址。
IPAddressInt	巢狀數字清單	數字格式的IP位址。
Owner	巢狀[OwnerInfo]結構	資產所有者資訊。
OS	巢狀[OS]結構	資產作業系統資訊。
displayName	字串	資產名稱。
IPAddress	巢狀字串清單	資產IP位址。
FQDN	字串	資產FQDN。
Weight	數字	資產重要性。
Deleted	包含 TRUE/FALSE 值的字串	指示資產是否已從KUMA標記為刪除。
UpdatedAt	數字	資產的上次更新日期。

巢狀ProductInfo結構

欄位	值類型	描述
ProductVersion	字串	軟體的版本。
ProductName	字串	軟體名稱。

巢狀硬體結構

欄位	值類型	描述
NetCards	巢狀[NetCard]結構	資產的網卡清單。
CPU	巢狀[CPU]結構	資產處理器清單。
RAM	巢狀[RAM]結構	資產RAM列表。
Disk	巢狀[Disk]結構	資產磁碟機清單。

巢狀網卡結構

欄位	值類型	描述
ID	字串	網卡ID。
MACAddresses	巢狀字串清單	網卡的MAC位址。
Name	字串	網卡名稱。
Manufacture	字串	網卡製造商。
DriverVersion	字串	驅動程式版本。

巢狀RAM結構

欄位	值類型	描述
Frequency	字串	RAM頻率。
TotalBytes	數字	RAM數量（以位元組為單位）。

巢狀CPU結構

欄位	值類型	描述
ID	字串	CPU ID。
Name	字串	CPU名稱。
CoreCount	字串	核心數量。
CoreSpeed	字串	頻率。

巢狀硬碟結構

欄位	值類型	描述
FreeBytes	數字	可用磁碟空間。
TotalBytes	數字	總磁碟空間。

使用者帳戶資料模型

可以從電子郵件範本和事件關聯期間處理使用者帳戶欄位。

欄位	值類型	描述
ID	字串	使用者帳戶ID。

ObjectGUID	字串	Active Directory屬性。Active Directory中的使用者帳戶ID。
TenantID	字串	租用戶ID。
TenantName	字串	租用戶名稱。
UpdatedAt	數字	使用者帳戶的上次更新。
Domain	字串	網域。
CN	字串	Active Directory屬性。使用者名稱。
displayName	字串	Active Directory屬性。顯示的使用者名稱。
DistinguishedName	字串	Active Directory屬性。LDAP物件名稱。
employeeID	字串	Active Directory屬性。員工ID。
Mail	字串	Active Directory屬性。使用者電子郵件信箱。
mailNickname	字串	Active Directory屬性。備用電子郵件地址。
Mobile	字串	Active Directory屬性。行動電話號碼。
ObjectSID	字串	Active Directory屬性。安全ID。
SAMAccountName	字串	Active Directory屬性。登入。
TelephoneNumber	字串	Active Directory屬性。電話號碼。
UserPrincipalName	字串	Active Directory屬性。使用者主體名稱（UPN）。
Archived	TRUE/FALSE string	確定使用者帳戶是否已過時的指標。
MemberOf	字串清單	Active Directory屬性。使用者加入的Active Directory群組。此屬性可用於相關性期間的事件搜尋。
PreliminarilyArchived	TRUE/FALSE string	確定使用者帳戶是否應指定為過時的指標。
CreatedAt	數字	使用者帳戶建立日期。
SN	字串	Active Directory屬性。使用者的姓氏。
SAMAccountType	字串	Active Directory屬性。使用者帳戶類型。
Title	字串	Active Directory屬性。使用者的職務。
Division	字串	Active Directory屬性。使用者的部門。
Department	字串	Active Directory屬性。使用者的分部。
Manager	字串	Active Directory屬性。使用者的主管。
Location	字串	Active Directory屬性。使用者的位置。
Company	字串	Active Directory屬性。使用者的公司。
StreetAddress	字串	Active Directory屬性。公司的地址。
PhysicalDeliveryOfficeName	字串	Active Directory屬性。送貨地址。
managedObjects	字串清單	Active Directory屬性。使用者控制的物件。
UserAccountControl	數字	Active Directory屬性。Active Directory帳戶類型。
WhenCreated	數字	Active Directory屬性。使用者帳戶建立日期。
WhenChanged	數字	Active Directory屬性。使用者帳戶修改日期。
AccountExpires	數字	Active Directory屬性。使用者帳戶到期日。
BadPasswordTime	數字	Active Directory屬性。上次登入嘗試失敗的日期。

稽核事件

在KUMA中完成某些與安全相關的操作時，會建立稽核事件。這些事件用於確保系統完整性。

稽核事件在KUMA Core伺服器上創建，並傳送到主租用戶的儲存體（主租用戶關聯器）。因此，必須在主租用戶中至少建立一個儲存體來儲存稽核事件。如果不存在任何儲存體，您需要建立一個。稽核事件會被傳送到稽核空間，該空間在儲存體中自動建立。

[OOTB] Kaspersky OSMP收集器會由OSMP安裝程式自動部署，以接收來自OSMP元件的稽核事件。[OOTB] Kaspersky OSMP收集器無法刪除。

若要檢視稽核事件，您需要前往**威脅搜尋**區段，並將`SELECT * FROM 'events' WHERE Type=4`新增至查詢。

執行查詢後，如果使用者角色允許查看稽核事件，則會顯示稽核事件。

事件欄位及一般資訊

每個稽核事件都包含下表所述的事件欄位。

事件欄位名稱	欄位值
`Timestamp`	事件時間
`DeviceHostName`	事件來源主機。對於稽核事件，主機名稱是安裝了kuma-core服務的主機名，因為該服務是事件來源。
`DeviceTimeZone`	託管KUMA Core伺服器的系統時間時區，格式為`+-hh:mm`。
`Type`	稽核事件的類型。`Audit` 或 `Base`。
`TenantID`	租用戶ID。
`DeviceVendor`	`"Kaspersky"`
`DeviceProduct`	`KUMA`
`EndTime`	事件建立時間。
`SpaceID`	`KUMA Audit`
`DeviceAction`	在稽核事件中捕獲的操作。

使用者已編輯欄位集設定以定義來源

事件欄位名稱	欄位值
`DeviceAction`	`settings updated`
`DeviceFacility`	`eventSourceIdentity`
`EventOutcome`	`succeeded`
`SourceUserName`	進行變更的使用者帳戶名稱。
`SourceUserID`	進行更改的使用者ID。
`DeviceCustomString5`	更新後的欄位集，使用「`|`」作為分隔符號。

密鑰檔案已新增

事件欄位名稱	欄位值
DeviceAction	license key installed
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	新增金鑰檔案的使用者ID。
SourceUserName	新增金鑰檔案的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

備用產品授權金鑰已新增

事件欄位名稱	欄位值
DeviceAction	reserve license key installed
DeviceAddress	新增備用備用產品授權金鑰的裝置的IP位址。
EventOutcome	succeeded
Message	產品授權名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserID	新增備用產品授權金鑰的使用者ID。
SourceUserName	新增備用產品授權金鑰的使用者帳戶名稱。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

備用產品授權金鑰已刪除

事件欄位名稱	欄位值
DeviceAction	reserve license key uninstalled
DeviceAddress	刪除備用產品授權金鑰的裝置的IP位址。
EventOutcome	succeeded
Message	產品授權名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。

SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserID	刪除備用產品授權金鑰的使用者ID。
SourceUserName	刪除備用產品授權金鑰的使用者帳戶名稱。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

使用啟動碼啟動的應用程式

事件欄位名稱	欄位值
DeviceAction	license activated
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	輸入啟動碼的使用者ID。
SourceUserName	輸入啟動碼的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

產品授權已續期

事件欄位名稱	欄位值
DeviceAction	license reactivated
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	新增金鑰檔案的使用者ID。
SourceUserName	新增金鑰檔案的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

無效的啟動碼

事件欄位名稱	欄位值
DeviceAction	activation code license activated
EventOutcome	failed

Message	錯誤文字。
SourceUserID	輸入啟動碼的使用者ID。
SourceUserName	輸入啟動碼的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

啟動碼已封鎖

事件欄位名稱	欄位值
DeviceAction	license blocked
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	輸入啟動碼的使用者ID。
SourceUserName	輸入啟動碼的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

啟動碼或金鑰檔案已刪除

事件欄位名稱	欄位值
DeviceAction	license uninstalled
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	刪除使用金鑰檔案的使用者ID。
SourceUserName	刪除金鑰檔案的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

EPS已超限

事件欄位名稱	欄位值
DeviceAction	license limit for EPS exceeded
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	新增金鑰檔案或輸入啟動碼的使用者ID。

SourceUserName	新增金鑰檔案或輸入啟動碼的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

產品授權已到期，寬限期已開始

事件欄位名稱	欄位值
DeviceAction	license expired
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	新增金鑰檔案或輸入啟動碼的使用者ID。
SourceUserName	新增金鑰檔案或輸入啟動碼的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

寬限期結束

事件欄位名稱	欄位值
DeviceAction	license ended
EventOutcome	succeeded
Message	產品授權名稱。
SourceUserID	新增金鑰檔案或輸入啟動碼的使用者ID。
SourceUserName	新增金鑰檔案或輸入啟動碼的使用者帳戶名稱。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

已新增過期的啟動碼或金鑰檔案

事件欄位名稱	欄位值
DeviceAction	license key installed
IP	新增金鑰檔案或輸入啟動碼的IP位址。
EventOutcome	failed
Message	錯誤文字。
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。

SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserID	新增金鑰檔案或輸入啟動碼的使用者ID。
SourceUserName	新增金鑰檔案或輸入啟動碼的使用者帳戶名稱。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

更改了用於區分事件存取權限的空間集

事件欄位名稱	欄位值
DeviceAction	• space set was created • space set was deleted • space set was updated (包括授予和撤銷存取權限)
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改設定的使用者帳戶名稱。
SourceUserID	修改設定的使用者ID。
DeviceCustomString5	空間集ID。
DeviceCustomString5Label	set ID
DeviceCustomString3	空間集名稱。
DeviceCustomString3Label	space name

服務監控閾值已更改

事件欄位名稱	欄位值
DeviceAction	settings updated
DeviceFacility	serviceAlertSettings
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改設定的使用者帳戶名稱。
SourceUserID	修改設定的使用者ID。
DeviceCustomString1	包含資料庫中記錄的閾值的JSON資料。
DeviceCustomString1Label	thresholds
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID

DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

KUMA Core設定已修改

事件欄位名稱	欄位值
DeviceAction	settings updated
DeviceFacility	coreProperties
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改設定的使用者帳戶名稱。
SourceUserID	修改設定的使用者ID。
DeviceCustomString1	包含資料庫中記錄的KUMA Core設定值的JSON。
DeviceCustomString1Label	properties

GeoIP資料庫已匯入

事件欄位名稱	欄位值
DeviceAction	new geobase imported
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	匯入資料庫的使用者帳戶名稱。
SourceUserID	匯入資料庫的使用者ID。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務已建立

事件欄位名稱	欄位值
DeviceAction	service created
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。

SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	建立該服務的使用者帳戶名稱。
SourceUserID	建立服務的使用者ID。
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務已刪除

事件欄位名稱	欄位值
DeviceAction	service deleted
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	刪除該服務之使用者的帳戶名稱。
SourceUserID	刪除服務的使用者ID。
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DestinationAddress	用於啟動服務的裝置的位址。如果服務之前從未啟動過，則該欄位將為空。
DestinationHostName	用於啟動服務的電腦的FQDN。如果服務之前從未啟動過，則該欄位將為空。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務已重新載入

事件欄位名稱	欄位值
DeviceAction	service reloaded
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。

SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	重新啟動服務之使用者的帳戶名稱。
SourceUserID	重啟服務的使用者ID。
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務已重新啟動

事件欄位名稱	欄位值
DeviceAction	service restarted
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	重新啟動服務之使用者的帳戶名稱。
SourceUserID	重啟服務的使用者ID。
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務已啟動

事件欄位名稱	欄位值
DeviceAction	service started
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。

DeviceFacility	服務類型。
DestinationAddress	啟動服務的裝置的位址。
DestinationHostName	啟動服務的裝置的FQDN。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務已配對

事件欄位名稱	欄位值
DeviceAction	service paired
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

工作狀態已變更

事件欄位名稱	欄位值
DeviceAction	service status changed
DeviceExternalID	服務ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DestinationAddress	啟動服務的裝置的位址。
DestinationHostName	啟動服務的裝置的FQDN。
DeviceCustomString1	green、yellow 或 red
DeviceCustomString1Label	new status
DeviceCustomString2	green、yellow 或 red
DeviceCustomString2Label	old status
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID

DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

分割區已被使用者刪除

事件欄位名稱	欄位值
DeviceAction	partition deleted
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	刪除分割區之使用者的帳戶名稱。
SourceUserID	刪除分割區的使用者ID。
Name	儲存名稱 | 正在移動或刪除的分割區的租用戶 | 分割區所屬空間的名稱。
DeviceCustomDate1	資料修改時間（UTC）。儲存分割區的 date 欄中顯示的日期。
DeviceCustomDate1Label	date of event
Message	deleted by user

資料分割區會在保留期限過後自動刪除

事件欄位名稱	欄位值
DeviceAction	applied retention policy by days
EventOutcome	succeeded
Name	分割區所屬空間的名稱。
DeviceCustomDate1	資料修改時間（UTC）。儲存體分割區中「日期」欄位顯示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分割區的大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件數量。
DeviceCustomNumber2Label	events
SourceServiceName	scheduler
Message	deleted partition data
DeviceEventCategory	event log 僅在刪除稽核分割區時才會顯示DeviceEventCategory 欄位。

分割區已按絕對保留期刪除

事件欄位名稱	欄位值
Name	分割區所屬空間的名稱。
Message	deleted partition data
DeviceAction	applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	資料修改時間（UTC）。儲存體分割區中「日期」欄位顯示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分割區大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件數量。
DeviceCustomNumber2Label	events
EventOutcome	succeeded

分割區已按相對保留期刪除

事件欄位名稱	欄位值
Name	分割區所屬空間的名稱。
Message	deleted partition data
DeviceAction	applied retention policy by percent
SourceServiceName	scheduler
DeviceCustomDate1	資料修改時間（UTC）。儲存體分割區中「日期」欄位顯示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分割區大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件數量。
DeviceCustomNumber2Label	events
EventOutcome	succeeded

分割區已移至冷儲存體

事件欄位名稱	欄位值
Name	分割區所屬空間的名稱。
Message	moved partition data to cold storage

DeviceAction	以下值可用： • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	資料修改時間（UTC）。儲存體分割區中「日期」欄位顯示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分割區大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件數量。
DeviceCustomNumber2Label	events
EventOutcome	succeeded
DeviceCustomString1	空間的ID。
DeviceCustomString1Label	nodeID

將分割區移到冷儲存體時發生錯誤

事件欄位名稱	欄位值
Name	分割區所屬空間的名稱。
Message	move partition data to cold storage failed: {"error":"Code: 243. DB::Exception: Move is not possible.Not enough space on 'cold_volume'. (NOT_ENOUGH_SPACE) (version 23.8.8.207)\n"}
DeviceAction	以下值可用： • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	資料修改時間（UTC）。儲存體分割區中「日期」欄位顯示的日期。
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	分割區大小。
DeviceCustomNumber1Label	size
DeviceCustomNumber2	事件數量。
DeviceCustomNumber2Label	events
EventOutcome	failed
DeviceCustomString1	空間的ID。
DeviceCustomString1Label	nodeID

活動清單清除成功或操作失敗

僅針對使用者執行的操作建立活動清單的稽核事件。使用關聯規則修改活動清單時不會產生稽核事件。**如果您需要追蹤此類更改，可以使用警示進行追蹤**。

如果活動清單是使用關聯規則修改，且規則類型為**簡單**，並定義了**輸出**和**迴圈**動作，則每次觸發規則時都會建立活動清單修改警示。

事件可以被指派 `succeeded` 或 `failed` 狀態。

由於清除活動清單的請求是透過遠端連線發出的，因此資料傳輸錯誤可能隨時發生：刪除之前和刪除之後。

這表示活動清單可能已成功清除，但事件被指派 `failed` 狀態，因為 EventOutcome 傳回的是請求的 TCP/IP 連線狀態，而非活動清單清除的成功或失敗狀態。

稽核事件「活動清單成功刪除或操作失敗」的欄位值

事件欄位名稱	欄位值
DeviceAction	active list cleared
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	用於清除活動清單的使用者登入名稱。
SourceUserID	用於清除活動清單的使用者ID。
DeviceExternalID	活動清單的服務ID已清除。
ExternalID	活動清單ID。
Name	活動列表名稱。
Message	若 EventOutcome = `failed`，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	租用戶名稱

活動清單項目變更成功或操作失敗

僅針對使用者執行的操作建立活動清單的稽核事件。使用關聯規則修改活動清單時不會產生稽核事件。**如果您需要追蹤此類更改，可以使用警示進行追蹤**。

如果活動清單是使用關聯規則修改，且規則類型為**簡單**，並定義了**輸出**和**迴圈**動作，則每次觸發規則時都會建立活動清單修改警示。

事件可以被指派 `succeeded` 或 `failed` 狀態。

由於更改活動清單項目的請求是透過遠端連線發出的，因此資料傳輸錯誤可能隨時發生：變更之前和變更之後。

這表示活動清單項目可能已成功變更，但事件卻被指派 `failed` 狀態，因為 EventOutcome 傳回的是請求的 TCP/IP 連線狀態，而不是活動清單項目變更的成功或失敗狀態。

稽核事件「活動清單項更改成功或操作失敗」的欄位值：

事件欄位名稱	欄位值
DeviceAction	active list item changed
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 `x-real-ip` 或 `x-forwarded-for` 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。

SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用於更改活動清單項目的使用者登入。
SourceUserID	用於變更活動清單項目的使用者ID。
DeviceExternalID	變更活動清單的服務ID。
ExternalID	活動清單ID。
Name	活動列表名稱。
DeviceCustomString1	鍵名。
DeviceCustomString1Label	key
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱
DeviceCustomString6Label	tenant name

活動清單項目刪除成功或操作失敗

僅針對使用者執行的操作建立活動清單的稽核事件。使用關聯規則修改活動清單時不會產生稽核事件。**如果您需要追蹤此類更改，可以使用警示進行追蹤**。

如果活動清單是使用關聯規則修改，且規則類型為**簡單**，並定義了**輸出**和**迴圈**動作，則每次觸發規則時都會建立活動清單修改警示。

事件可以被指派 succeeded 或 failed 狀態。

由於刪除活動清單項目的請求是透過遠端連線發出的，因此資料傳輸錯誤可能隨時發生：刪除之前和刪除之後。

這表示活動清單項目可能已成功刪除，但事件仍被指派 failed 狀態，因為 EventOutcome 傳回的是請求的 TCP/IP 連線狀態，而不是活動清單項目刪除成功或失敗的狀態。

稽核事件「活動清單項目成功刪除或操作失敗」的欄位值

事件欄位名稱	欄位值
DeviceAction	active list item deleted
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用於從活動清單中刪除項目的使用者登入名稱。
SourceUserID	用於從活動清單中刪除項目的使用者ID。
DeviceExternalID	活動清單的服務ID已清除。
ExternalID	活動清單ID。
Name	活動列表名稱。
DeviceCustomString1	鍵名。
DeviceCustomString1Label	key
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。

DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

活動清單匯入成功或操作失敗

僅針對使用者執行的操作建立活動清單的稽核事件。使用關聯規則修改活動清單時不會產生稽核事件。**如果您需要追蹤此類更改，可以使用警示進行追蹤**。

如果活動清單是使用關聯規則修改，且規則類型為**簡單**，並定義了**輸出**和**迴圈**動作，則每次觸發規則時都會建立活動清單修改警示。

活動清單項目透過遠端連線分部分匯入。

由於匯入是透過遠端連線執行的，因此資料傳輸錯誤可能隨時發生：資料部分匯入或全部匯入時。EventOutcome傳回連線狀態，而不是匯入狀態。

稽核事件「活動清單成功匯入或操作失敗」的欄位值：

事件欄位名稱	欄位值
DeviceAction	active list imported
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用來執行匯入的使用者登入名稱。
SourceUserID	用於執行匯入的使用者ID。
DeviceExternalID	執行匯入的服務ID。
ExternalID	活動清單ID。
Name	活動列表名稱。
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。錯誤文字可以採用 JSON 格式，例如 {"error":"line 1: header does not contain column IP!"}。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱
DeviceCustomString6Label	tenant name

活動清單已匯出

僅針對使用者執行的操作建立活動清單的稽核事件。使用關聯規則修改活動清單時不會產生稽核事件。**如果您需要追蹤此類更改，可以使用警示進行追蹤**。

如果活動清單是使用關聯規則修改，且規則類型為**簡單**，並定義了**輸出**和**迴圈**動作，則每次觸發規則時都會建立活動清單修改警示。

稽核事件「活動清單已匯出」的欄位值

事件欄位名稱	欄位值
DeviceAction	active list exported
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用來執行匯出的使用者登入名稱。
SourceUserID	用於執行匯出的使用者ID。
DeviceExternalID	執行匯出的服務ID。
ExternalID	活動清單ID。
Name	活動列表名稱。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱
DeviceCustomString6Label	tenant name

快顯表單已匯出

快顯表單的稽核事件僅針對使用者執行的操作建立。

稽核事件「快顯表單已匯出」的欄位值

事件欄位名稱	欄位值
DeviceAction	context table exported
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用來執行匯出的使用者登入名稱。
SourceUserID	用於執行匯出的使用者ID。
DeviceExternalID	執行匯出的服務ID。
ExternalID	快顯表單ID
Name	快顯表單的名稱。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

快顯表單匯入成功或操作失敗

快顯表單的稽核事件僅針對使用者執行的操作建立。

快顯表單項目透過遠端連線分部分匯入。

由於匯入是透過遠端連線執行的，因此資料傳輸錯誤可能隨時發生：資料部分匯入或全部匯入時。EventOutcome傳回連線狀態，而不是匯入狀態。

稽核事件「快顯表單匯入成功或操作失敗」的欄位值：

事件欄位名稱	欄位值
DeviceAction	context table imported
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用來執行匯入的使用者登入名稱。
SourceUserID	用於執行匯入的使用者ID。
DeviceExternalID	執行匯入的服務ID。
ExternalID	快顯表單ID
Name	快顯表單的名稱。
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

快顯表單項修改成功或操作失敗

快顯表單的稽核事件僅針對使用者執行的操作建立。

可為事件指派 succeeded 或 failed 狀態。

稽核事件「快顯表單項修改成功或操作失敗」的欄位值：

事件欄位名稱	欄位值
DeviceAction	context table item is set
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	更改快顯表單項的使用者帳戶名稱。
SourceUserID	更改快顯表單項的使用者ID。
DeviceExternalID	修改了快顯表單的服務ID。
ExternalID	快顯表單ID
Name	快顯表單的名稱。
DeviceCustomString1	記錄密鑰名稱。
DeviceCustomString1Label	key

Message	若 EventOutcome = failed，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

快顯表單項刪除成功或操作失敗

快顯表單的稽核事件僅針對使用者執行的操作建立。

可為事件指派 succeeded 或 failed 狀態。

稽核事件「快顯表單項修改成功或操作失敗」的欄位值

事件欄位名稱	欄位值
DeviceAction	context table item deleted
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	刪除快顯表單項目的使用者帳戶名稱。
SourceUserID	刪除快顯表單項的使用者ID。
DeviceExternalID	刪除快顯表單項的服務ID。
ExternalID	快顯表單ID
Name	快顯表單的名稱。
DeviceCustomString1	記錄密鑰名稱。
DeviceCustomString1Label	key
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

快顯表單刪除成功或操作失敗

快顯表單的稽核事件僅針對使用者執行的操作建立。

可為事件指派 succeeded 或 failed 狀態。

由於清除快顯表單的請求是透過遠端連線發出的，因此資料傳輸錯誤可能隨時發生：刪除之前和刪除之後。

這表示快顯表單可能已成功清除，但事件仍會取得 failed 狀態，因為 EventOutcome 傳回的是請求的 TCP/IP 連線狀態，而不是快顯表單清除成功或失敗的狀態。

稽核事件「快顯表單清除成功或操作失敗」的欄位值

事件欄位名稱	欄位值
DeviceAction	context table cleared
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	清除內容資料表的使用者帳戶名稱。
SourceUserID	清除快顯表單的使用者ID。
DeviceExternalID	清空快顯表單的服務ID。
ExternalID	快顯表單ID
Name	快顯表單的名稱。
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	租用戶名稱

資源已新增

事件欄位名稱	欄位值
DeviceAction	resource added
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用於新增資源的使用者登入名稱。
SourceUserID	用於新增資源的使用者ID。
DeviceExternalID	資源ID。
DeviceProcessName	資源名稱。
DeviceFacility	資源類型： • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	租用戶ID。

DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

資源已刪除

事件欄位名稱	欄位值
DeviceAction	resource deleted
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用於刪除資源的使用者登入名稱。
SourceUserID	用於刪除資源的使用者ID。
DeviceExternalID	資源ID。
DeviceProcessName	資源名稱。
DeviceFacility	資源類型： • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

資源已更新

事件欄位名稱	欄位值
DeviceAction	resource updated
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。

SourceUserName	用於更新資源的使用者登入名稱。
SourceUserID	用於更新資源的使用者ID。
DeviceExternalID	資源ID。
DeviceProcessName	資源名稱。
DeviceFacility	資源類型： • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

匯入資源

事件欄位名稱	欄位值
DeviceAction	import resources
EventOutcome	succeeded
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	匯入資源的使用者帳戶名稱。
SourceUserID	匯入資源的使用者ID。
DeviceCustomString5	匯入資源的租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	匯入資源的租用戶名稱。
DeviceCustomString6Label	tenant name
FileType	匯入來源：file 或 repository。
FileID	如果從儲存庫匯入資源，則需要軟體套件ID。 如果從檔案匯入資源，則為該檔案的系統ID。
ExternalID	如果從儲存庫匯入資源，則為匯入軟體套件的版本。 如果從檔案匯入資源，則值為空。

設定已更新

事件欄位名稱	欄位值
DeviceAction	settings updated
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	用於更新設定的使用者登入名稱。
SourceUserID	用於更新設定的使用者ID。
DeviceFacility	設定類型。
DeviceCustomString1	包含資料庫中記錄的閾值的JSON資料。
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

服務上的字典更新成功或操作失敗

事件欄位名稱	欄位值
DeviceAction	dictionary update succeeded
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	用於建立服務的使用者登入名稱。
SourceUserID	用於建立服務的使用者ID。
DeviceExternalID	服務ID。
ExternalID	字典ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString1	字典類型：表格、字典。
DeviceCustomString1Label	dictionary type
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。

字典項目已新增

透過API新增或更新的字典項目。

稽核事件「字典項目已新增」的欄位值：

事件欄位名稱	欄位值
DeviceAction	dictionary item added
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	新增該項目的使用者帳戶名稱。
SourceUserID	新增條目的使用者ID。
DeviceExternalID	服務ID。
ExternalID	字典ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString1	字典類型：表格、字典。
DeviceCustomString1Label	dictionary type
DeviceCustomString2	記錄金鑰。
DeviceCustomString2Label	key
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

字典項目成功刪除或操作失敗

字典項目（類型：表格、字典）已透過API刪除。

事件可以被指派 `succeeded` 或 `failed` 狀態。

稽核事件「字典項目成功刪除或操作失敗」的欄位值：

事件欄位名稱	欄位值
DeviceAction	dictionary item deleted
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	刪除字典項目的使用者帳戶名稱。
SourceUserID	刪除字典項目的使用者ID。

DeviceExternalID	刪除了字典項目的服務ID。
ExternalID	字典ID。
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceCustomString1	字典類型：表格、字典。
DeviceCustomString1Label	dictionary type
DeviceCustomString2	記錄金鑰。
DeviceCustomString2Label	key
Message	若 EventOutcome = failed，可在此處找到錯誤訊息。
DeviceCustomString5	服務租用戶ID。某些錯誤會阻止將租用戶資訊新增至事件。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

擴充事件結構欄位已建立

事件欄位名稱	欄位值
DeviceAction	extended field created
EventOutcome	succeeded
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	建立擴充事件結構欄位的使用者帳戶名稱。
SourceUserID	建立擴展事件結構欄位的使用者ID。
DeviceCustomString5	欄位的完整名稱（SA.sting_array）。

擴充事件結構欄位已編輯

事件欄位名稱	欄位值
DeviceAction	extended field edited
EventOutcome	succeeded
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	編輯擴充事件架構欄位的使用者帳戶名稱。
SourceUserID	編輯擴充事件架構欄位的使用者ID。
DeviceCustomString5	欄位的完整名稱（SA.sting_array）。

擴充事件結構欄位已匯入

事件欄位名稱	欄位值
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	匯入擴充事件架構欄位之使用者的帳戶名稱。
SourceUserID	導入擴充事件架構欄位的使用者ID。
DeviceCustomString5	欄位的完整名稱（SA.sting_array）。

包含擴充事件結果欄位的規範化器已匯入

事件欄位名稱	欄位值
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	匯入具有擴展事件結構欄位的規範化器的使用者帳戶名稱。
SourceUserID	匯入具有擴展事件結構欄位的規範化器的使用者ID。
DeviceCustomString5	欄位的完整名稱（SA.sting_array）。

擴充事件結構欄位已刪除

事件欄位名稱	欄位值
DeviceAction	extended field deleted
EventOutcome	succeeded
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	刪除擴充事件結構欄位之使用者的帳戶名稱。
SourceUserID	刪除擴充事件結構欄位的使用者ID。
DeviceCustomString5	欄位的完整名稱（SA.sting_array）。

將請求傳送至KIRA

事件欄位名稱	欄位值
DeviceAction	KIRA task
EventOutcome	succeeded/failed
SourceUserName	用於發送請求的使用者登入資訊。
SourceUserID	用於發送請求的使用者ID。
DeviceCustomString1	傳送的結果字串。
DeviceCustomString1Label	cmd
DeviceCustomString2	發送請求的事件ID。
DeviceCustomString2Label	event
DeviceCustomString3	為傳送請求而建立的工作ID。
DeviceCustomString3Label	task

KICS/KATA回應

事件欄位名稱	欄位值
DeviceAction	KICS response
DeviceAssetID	asset fqdn
DeviceFacility	manual response 或 automatic response
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	傳送請求的使用者的登入名稱。
SourceUserID	發送請求的使用者的ID。
DeviceCustomString3	回應規則名稱：Authorized、Not Authorized。
DeviceCustomString3Label	response rule name
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name
DeviceExternalID	資產ID。
SourceHostName	資產FQDN。
Name	資產名稱。
DeviceCustomString1	資產的IP位址清單。
DeviceCustomString1Label	addresses
訊息	如果 EventOutcome = failed，則會在此欄位中寫入錯誤訊息。

DeviceCustomString2	fdqn
DeviceCustomString2Label	fqdns

Kaspersky Automated Security Awareness Platform回應

事件欄位名稱	欄位值
DeviceAction	KASAP response
DeviceFacility	manual response
EventOutcome	succeeded或failed
Message	如果發生錯誤，則描述錯誤，否則該欄位為空。
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	傳送請求的使用者的登入名稱。
SourceUserID	發送請求的使用者的ID。
DeviceCustomString1	被指派課程的使用者管理員。
DeviceCustomString1Label	manager
DeviceCustomString3	有關使用者所屬群組的資訊。不適用於 failed。
DeviceCustomString3Label	manager
DeviceCustomString4	有關使用者所屬群組的資訊。
DeviceCustomString4Label	new kasap group
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name
DestinationUserID	導致回應的Active Directory使用者帳戶的ID。
DestinationUserName	帳戶名稱（sAMAccountName）。
DestinationNtDomain	會導致回應的Active Directory使用者帳戶的網域。

KEDR回應

事件欄位名稱	欄位值
DeviceAction	KEDR response
DeviceFacility	manual response 或 automatic response
EventOutcome	succeeded或failed
Message	如果發生錯誤，則描述錯誤，否則該欄位為空。
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。

SourceUserName	傳送請求的使用者的登入名稱。
SourceUserID	發送請求的使用者的ID。
SourceAssetID	導致回應的KUMA資產ID。如果回應是基於雜湊值或針對所有資產，則未指定該值。
DeviceExternalID	在KEDR中指派給KUMA的外部ID。如果只有一個外部ID，則在使用者主機上啟動時不會填寫。
DeviceCustomString1	基於事件卡中選定雜湊值的主機防護規則資產的IP/FQDN位址清單。
DeviceCustomString1Label	user defined list of ips or hostnames
DeviceCustomString2	KEDR中的感應器ID參數（UUIDv4 | 'all' | 'custom'）。
DeviceCustomString2Label	sensor id of asset in KATA/EDR
ServiceID	導致回應的服務ID。僅在自動回應的情況下填寫。
DeviceCustomString3	任務類型名稱：enable_network_isolation、disable_network_isolation、enable_prevention、disable_prevention、run_process。
DeviceCustomString3Label	kedr response kind
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

匯入MITRE ATT&CK技術與策略

事件欄位名稱	欄位值
DeviceAction	import MITRE
EventOutcome	succeeded
FileID	要匯入的檔案名稱。
SourceUserID	傳送匯入請求的使用者ID。
SourceUserName	傳送請求的使用者帳戶名稱。

指標警示已註冊服務或操作失敗

事件欄位名稱	欄位值
DeviceProcessName	服務名稱。
DeviceFacility	服務類型。
DeviceExternalID	服務ID。
DeviceCustomString6Label	tenant name
DeviceCustomString6	租用戶名稱。
DeviceCustomString5Label	tenant ID
DeviceCustomString5	租用戶ID。

DeviceCustomString2Label	可能的值： • QPS threshold reached • Failed Insert QPS threshold reached • High distribution queue • Low disk space • Low disk partition space • Output Event Loss increasing • Disk buffer size increasing • Enrichment errors increasing • High enrichment queue • Connector log errors increasing
DeviceCustomString2	created（服務建立時間）
DeviceCustomString1Label	API port.
DeviceCustomNumber1	工作持續時間（秒）。
DeviceAction	service alert
EventOutcome	succeeded或failed

Active Directory中的回應

事件欄位名稱	欄位值
DeviceAction	ad response
DeviceFacility	manual response 或 automatic response
EventOutcome	succeeded 或 failed
SourceTranslatedAddress	此欄位包含HTTP標頭x-real-ip或x-forwarded-for的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理登錄，則會有一個代理地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理登錄，則會有一個代理端的連接埠。
SourceUserName	執行回應的使用者帳戶名稱。
SourceUserID	執行回應的使用者 ID。
DeviceCustomString3	回應規則名稱：CHANGE_PASSWORD、ADD_TO_GROUP、REMOVE_FROM_GROUP、BLOCK_USER。
DeviceCustomString3Label	response rule name
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name
DestinationUserName	呼叫回應的Active Directory使用者帳戶（sAMAccountName）。
DestinationNtDomain	呼叫回應的Active Directory使用者帳戶的網域。
DestinationUserID	KUMA中的帳戶UUID。
FlexString1	有關新增或刪除使用者的群組的資訊。
FlexString1Label	group DN

備份分割區、從備份中還原、從外部安裝的KUMA匯入分割區

事件欄位名稱	欄位值
DeviceAction	backup/restore/import
EventOutcome	succeeded 或 failed
SourceUserName	執行分割區備份、從備份還原及從外部 KUMA 實例匯入分割區之使用者的使用者名稱。
SourceUserID	執行分割區備份、從備份還原及從外部 KUMA 實例匯入分割區之使用者的 ID。
DeviceExternalID	儲存服務的ID。
Name	儲存體的名稱。
FilePath	備份檔案保存的完整路徑。 要從備份中還原或匯入分割區的完整路徑。
Message	如果為 EventOutcome = failed，可在此處找到錯誤訊息。

使用KIRA將自然語言查詢轉換為SQL查詢。

事件欄位名稱	欄位值
DeviceAction	KIRA request
EventOutcome	succeeded/failed
SourceUserName	用於發送請求的使用者登入資訊。
SourceUserID	用於發送請求的使用者ID。
DeviceCustomString1	傳送的結果字串。
DeviceCustomString1Label	sql text

事件讀取嘗試

事件欄位名稱	欄位值
DeviceAction	event search
Name	讀取日誌。
EventOutcome	succeeded 或 failed
SourceUserName	發起搜尋查詢的使用者帳號名稱。
SourceUserID	進行搜尋查詢的使用者ID。
DeviceCustomString3	使用者在**事件**部分選擇的儲存空間清單。
DeviceCustomString3Label	space name
DeviceCustomString4	搜尋查詢文字。
DeviceCustomString4Label	text of the search query

搜尋請求已取消。

「訊息」欄位可能缺失。

事件欄位名稱	欄位值
DeviceAction	canceling a search query
Message	取消請求的原因。
Name	搜尋請求已取消。
DeviceCustomString5	服務租用戶ID（某些錯誤可能導致租用戶資訊缺失）。
DeviceCustomString3Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name
DeviceExternalID	儲存體ID。
EventOutcome	succeeded或failed
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	發起搜尋查詢的使用者帳號名稱。
SourceUserID	進行搜尋查詢的使用者ID。

KEDR資源已更新

事件欄位名稱	欄位值
DeviceAction	resource updated
EventOutcome	succeeded或failed
DeviceExternalID	資源ID。
DeviceProcessName	資源名稱。
DeviceFacility	資源類型。
DeviceCustomNumber2	資源版本（編號）。
DeviceCustomNumber2Label	EDR resource version
DeviceCustomString4	KUMA版本。
DeviceCustomString4Label	KUMA version
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenantID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

KEDR資源更新工作已完成

事件欄位名稱	欄位值
DeviceAction	Apply EDR resources task
Message	過時的EDR資源已更新。包含已更新EDR資源的服務已重新載入。
EventOutcome	succeeded或failed
DeviceCustomNumber1	資源收集器名稱。
DeviceCustomNumber1Label	reloaded collectors
DeviceCustomNumber3	資源關聯器名稱。
DeviceCustomNumber3Label	reloaded correlators
DeviceCustomString4	KUMA版本。
DeviceCustomString4Label	KUMA version
DeviceCustomString5	資源名稱。
DeviceCustomString5Label	imported resources

KEDR事件欄位已更新

事件欄位名稱	欄位值
DeviceAction	Apply EDR resources task
Message	新的EDR擴充欄位已套用。
EventOutcome	succeeded或failed
DeviceCustomNumber1	擴充事件欄位的版本。
DeviceCustomNumber1Label	New EDR fields version
DeviceCustomString4	KUMA版本。
DeviceCustomString4Label	KUMA version

檔案localizations.json已匯入

事件欄位名稱	欄位值
DeviceAction	Import IOA rules localizations
EventOutcome	succeeded或failed
DeviceCustomDate1	dd.mm.yyy hh:mm:ss
DeviceCustomDate1Label	Last update IoA rules localizations file content

規則已連結至收集器

事件欄位名稱	欄位值
DeviceAction	link rule to collector
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改資料的使用者名稱。
SourceUserID	修改資料的使用者ID。
ExternalID	規則連結之服務的 ID。
Name	規則連結之服務的名稱。
DeviceFacility	操作（規則已連結）。
DeviceCustomString1	規則的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	規則的名稱。
DeviceCustomString2Label	rule name
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

規則已取消與收集器的連結

事件欄位名稱	欄位值
DeviceAction	unlink rule from collector
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改資料的使用者名稱。
SourceUserID	修改資料的使用者ID。
ExternalID	已解除規則連結的服務 ID。
Name	已解除規則連結的服務名稱。
DeviceFacility	動作（規則已解除連結）。
DeviceCustomString1	規則的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	規則的名稱。

DeviceCustomString2Label	rule name
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

規則已連結至關聯器

事件欄位名稱	欄位值
DeviceAction	link rule to correlator
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改資料的使用者名稱。
SourceUserID	修改資料的使用者ID。
ExternalID	規則連結之服務的 ID。
Name	規則連結之服務的名稱。
DeviceFacility	操作（規則已連結）。
DeviceCustomString1	規則的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	規則的名稱。
DeviceCustomString2Label	rule name
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

規則已與關聯器取消連結

事件欄位名稱	欄位值
DeviceAction	unlink rule from correlator
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	修改資料的使用者名稱。
SourceUserID	修改資料的使用者ID。
ExternalID	已解除規則連結的服務 ID。

Name	已解除規則連結的服務名稱。
DeviceFacility	動作（規則已解除連結）。
DeviceCustomString1	規則的 ID。
DeviceCustomString1Label	rule ID
DeviceCustomString2	規則的名稱。
DeviceCustomString2Label	rule name
DeviceCustomString5	租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	租用戶名稱。
DeviceCustomString6Label	tenant name

從 KUMA 匯出的資源

每個匯出的資源都會產生一個獨立的稽核事件。

事件欄位名稱	欄位值
DeviceAction	export resources
EventOutcome	succeeded
SourceTranslatedAddress	此欄位包含 HTTP 標頭 x-real-ip 或 x-forwarded-for 的值。如果這些標頭不存在，則該欄位為空。
SourceAddress	使用者登入的位址。如果使用者使用代理伺服器登入，則指定代理伺服器的地址。
SourcePort	使用者登入的連接埠。如果使用者使用代理伺服器登入，則指定代理伺服器的連接埠。
SourceUserName	匯出資源的使用者名稱。
SourceUserID	匯出資源的使用者 ID。
DeviceCustomString5	資源匯出來源的租用戶ID。
DeviceCustomString5Label	tenant ID
DeviceCustomString6	匯出資源的ID。
DeviceCustomString6Label	resource ID
DeviceCustomString4	匯出資源的版本。
DeviceCustomString4Label	version

從隔離網路區段接收事件相關服務資料

事件相關的服務資訊會透過「internal」通訊協定傳輸至收集器。若要從隔離的網路區段傳輸此類資料，您可以使用安裝在該區段內的專用代理。

若要透過「internal」通訊協定將資料從代理傳輸至收集器，代理和收集器必須使用憑證相互驗證身分。您可以在代理的設定檔中建立並儲存代理憑證，然後使用此檔案在隔離區段中安裝代理。憑證資訊會以加密形式儲存在檔案中。

若要設定從隔離區段接收事件相關服務資料：

1. 建立或設定使用「internal」連接器的收集器。
2. 建立代理並設定向收集器傳輸資料：
   a. 在 KUMA 網頁介面中，於 **資源和服務** → **代理程式** 下，按一下 **建立**。
   b. 在開啟的 **建立代理程式** 視窗中，於 **基底設定** 索引標籤上，指定 **名稱** 和 **租用戶** 設定。
   c. 在 **設定資源 #{{index}}** 上，於 **連接器** 區段中，指定以下設定：
      - 在**名稱**欄位中，指定連接器的名稱。
      - 在**類型**欄位中，指定連接器類型。
      - 在**URL**欄位中，指定將安裝用於接收事件之代理的主機。
   d. 在 **設定資源 #{{index}}** 上，於 **目的地** 區段中，指定以下設定：
      - 在**名稱**欄位中，指定目的地的名稱。
      - 在**類型**欄位中，輸入將用於傳送事件的 **internal** 通訊協定。
      - 在**URL**欄位中，指定安裝了具有 **internal** 連接器之收集器的主機。
   e. 點擊**建立**。
   f. 從清單中選擇已建立的代理資源集，然後在代理內容視窗中，按一下**下載包含憑證的設定**。在顯示的視窗中，指定將用於加密憑證且也會在啟動代理時要求輸入的密碼。
      代理設定組態會根據瀏覽器的設定，以 JSON 檔案格式下載。在隔離網段中安裝代理程式時使用此檔案。

      > 您必須使用存取控制清單 (ACL) 來設定在將安裝代理程式的伺服器上存取檔案的權限。代理執行時所使用的使用者帳戶必須具有檔案讀取存取權限。

   g. 在隔離網段中安裝代理。它可以安裝到Linux和Windows裝置上。

已設定接收來自隔離網段的事件服務資料。

關聯規則

您可以按一下連結下載檔案，其中說明發行套件所包含的關聯規則。它提供了規則涵蓋的情境、使用條件以及必要的事件來源。

> 本文檔中所述的關聯規則包含在OSMP分發套件中的 SOC_package檔案中；該檔案的密碼是 SOC_package1。一次只能使用一個版本的SOC規則集：俄語或英語。

> 您可以將匯入的關聯規則新增至組織使用的關聯器。如需詳細資訊，請參閱以下主題：步驟 3。關聯。

若要將關聯規則套件匯入KUMA：

1. 在KUMA主控台的KUMA部分，轉至**設定→儲存庫更新**，然後將**更新來源**參數設定為**卡巴斯基更新伺服器**。
   您也可以設定儲存區更新。
2. 點擊**執行更新**以儲存更新設定並手動啟動*儲存區更新*工作。
3. 轉到**工作管理器**以確保*儲存區更新*工作已完成。
4. 轉至**資源**，然後按一下**匯入資源**。
5. 在**資源導入**視窗中，選擇要指派匯入資源的租用戶。
6. 在**匯入來源**下拉清單中，選擇**儲存區**，選擇SOC內容套件，然後按一下**匯入**。

   SOC內容套件中的資源被匯入到KUMA。有關匯入的更多資訊，請參閱匯入資源。

下載SOC_package.xlsx檔案所包含的關聯規則描述。

時間格式

KUMA支援以以下格式處理傳遞到事件資料模型欄位的資訊，時間戳記類型（EndTime、StartTime、DeviceCustomDate1等）：

- "May 8, 2009 5:57:51 PM",
- "oct 7, 1970",
- "oct 7, '70",
- "oct. 7, 1970",
- "oct. 7, 70",
- "Mon Jan 2 15:04:05 2006",
- "Mon Jan 2 15:04:05 MST 2006",
- "Mon Jan 02 15:04:05 -0700 2006",
- "Monday, 02-Jan-06 15:04:05 MST",
- "Mon, 02 Jan 2006 15:04:05 MST",
- "Tue, 11 Jul 2017 16:28:13 +0200 (CEST)",
- "Mon, 02 Jan 2006 15:04:05 -0700",
- "Mon 30 Sep 2018 09:09:09 PM UTC",
- "Mon Aug 10 15:44:11 UTC+0100 2015",

- "Thu, 4 Jan 2018 17:53:36 +0000",
- "Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)",
- "Sun, 3 Jan 2021 00:12:23 +0800 (GMT+08:00)",
- "2012年九月17日上午10:09",
- "2012年九月17日上午10:09 PST-08",
- "September 17, 2012, 10:10:09",
- "October 7, 1970",
- "October 7th, 1970",
- "12 Feb 2006, 19:17",
- "12 Feb 2006 19:17",
- "14 May 2019 19:11:40.164",
- "7 oct 70",
- "7 oct 1970",
- "03 February 2013",
- "1 July 2013",
- "2013-Feb-03".

dd/Mon/yyyy格式

- "06/Jan/2008:15:04:05 -0700",
- "06/Jan/2008 15:04:05 -0700".

mm/dd/yyyy格式

- "3/31/2014",
- "03/31/2014",
- "08/21/71",
- "8/1/71",
- "4/8/2014 22:05",

- "04/08/2014 22:05",
- "4/8/14 22:05",
- "04/2/2014 03:00:51",
- "8/8/1965 12:00:00 AM",
- "8/8/1965 01:00:01 PM",
- "8/8/1965 01:00 PM",
- "8/8/1965 1:00 PM",
- "8/8/1965 12:00 AM",
- "4/02/2014 03:00:51",
- "03/19/2012 10:11:59",
- "03/19/2012 10:11:59.3186369".

yyyy/mm/dd格式

- "2014/3/31",
- "2014/03/31",
- "2014/4/8 22:05",
- "2014/04/08 22:05",
- "2014/04/2 03:00:51",
- "2014/4/02 03:00:51",
- "2012/03/19 10:11:59",
- "2012/03/19 10:11:59.3186369".

yyyy:mm:dd格式

- "2014:3:31",
- "2014:03:31",
- "2014:4:8 22:05",
- "2014:04:08 22:05",

- "2014:04:2 03:00:51",
- "2014:4:02 03:00:51",
- "2012:03:19 10:11:59",
- "2012:03:19 10:11:59.3186369".

包含中文字元的格式

"2014年04月08日"

yyyy-mm-ddThh格式

- "2006-01-02T15:04:05+0000",
- "2009-08-12T22:15:09-07:00",
- "2009-08-12T22:15:09",
- "2009-08-12T22:15:09.988",
- "2009-08-12T22:15:09Z",
- "2017-07-19T03:21:51:897+0100",
- "2019-05-29T08:41-04"無秒鐘，2個字元的TZ。

yyyy-mm-dd hh:mm:ss格式

- "2014-04-26 17:24:37.3186369",
- "2012-08-03 18:31:59.257000000",
- "2014-04-26 17:24:37.123",
- "2013-04-01 22:43",
- "2013-04-01 22:43:22",
- "2014-12-16 06:20:00 UTC",
- "2014-12-16 06:20:00 GMT",
- "2014-04-26 05:24:37 PM",

- "2014-04-26 13:13:43 +0800",
- "2014-04-26 13:13:43 +0800 +08",
- "2014-04-26 13:13:44 +09:00",
- "2012-08-03 18:31:59.257000000 +0000 UTC",
- "2015-09-30 18:48:56.35272715 +0000 UTC",
- "2015-02-18 00:12:00 +0000 GMT",
- "2015-02-18 00:12:00 +0000 UTC",
- "2015-02-08 03:02:00 +0300 MSK m=+0.000000001",
- "2015-02-08 03:02:00.001 +0300 MSK m=+0.000000001",
- "2017-07-19 03:21:51+00:00",
- "2014-04-26",
- "2014-04",
- "2014",
- "2014-05-11 08:20:13,787".

yyyy-mm-dd-07:00格式

"2020-07-20+08:00"

mm.dd.yyyy格式

- "3.31.2014",
- "03.31.2014",
- "08.21.71".

yyyy.mm.dd格式

"2014.03.30"

yyyymmdd格式和類似格式

- "20140601",
- "20140722105203".

yymmdd hh:mm:yy格式

"171113 14:14:20"

Unix時間戳記格式

- "1332151919",
- "1384216367189",
- "1384216367111222",
- "13842163671112223333".

對應預定義標準化器的欄位

可透過包含預設標準化器欄位對應說明的連結下載檔案。

下載預設標準化器欄位對應說明。

詞彙表

Bootstrap

基本的執行環境，包括Kaspersky Next XDR Expert功能的Kubernetes叢集和基礎設施元件。Bootstrap包含在傳輸封存檔案中，並在Kaspersky Next XDR Expert部署期間自動安裝。

EPP應用程式

EPP應用程式安裝在終端裝置上，以提供防護並將防護狀態報告給管理伺服器，以便進行集中管理。在Kaspersky EDR Expert中，EPP應用程式包括Kaspersky Endpoint Security for Windows、 Kaspersky Endpoint Security for Linux和Kaspersky Endpoint Security for Mac。

IOA 規則

Kaspersky Next XDR Expert使用攻擊指標（IOA）。IOA規則包含系統中可疑活動的描述，這些活動可能是定向攻擊的跡象。這些規則從KUMA儲存庫下載，並由TAA（目標攻擊分析器）技術用於威脅搜尋。您可以從對應的警示詳情中開啟IOA規則詳情。此外，OSMP主控台中也預先定義了一條IOA規則。預定義的規則顯示在關聯規則表中：**監控→資源和服務→關聯規則**。如果觸發了預先定義的IOA規則，則會建立IOA警示。

IOC檔案

IOC檔案包含一組指標，這些指標將與事件的指標進行比較。如果比較的指標匹配，應用程式將該事件視為偵測並建立警示。如果掃描偵測到物件資料與多個IOC檔案完全匹配，則發出警示的可能性可能會增加。

Kaspersky Deployment Toolkit

一種公用程式，用於部署和管理Kubernetes叢集、Kaspersky Next XDR Expert元件和管理網頁外掛程式。KDT運行在管理員主機上，並透過SSH連線到目標主機。

Kubernetes叢集

一組主機，透過Kubernetes組合成一種計算資源。Kubernetes叢集用於Kaspersky Next XDR Expert元件（ KUMA服務除外）的功能。Kubernetes叢集可以包含目標主機和管理員主機。

KUMA 服務

KUMA 的主要元件，用於幫助系統管理事件。這些服務可讓您從事件來源接收事件，然後將它們轉換為公用格式，以便於找尋關聯規則、儲存體和手動分析資料。KUMA服務包括代理程式、收集器、關聯器、儲存體和事件路由器，它們安裝在Kubernetes叢集外部的主機上。

KUMA清查檔案

一個YAML格式檔案，其中包含Kubernetes叢集中未包含的KUMA服務安裝參數。KUMA清查檔案的路徑包含在KDT用於Kaspersky Next XDR Expert部署的組態檔中。

上下文

上下文是一組存取參數，用於定義使用者可以選擇與之互動的Kubernetes叢集。上下文還包括使用KDT連線到叢集的資料。

事件

資訊安全事件，在組織IT基礎設施的受監控元素上註冊。例如，事件包括登入嘗試、與資料庫的互動以及感測器資訊廣播。每個單獨的事件可能看起來毫無意義，但綜合考慮時，它們會構成網路活動的更大圖景，以幫助辨識安全威脅。

事件

一個警示容器，通常表明組織IT基礎設施中存在確認為真的問題。一個事件可能包含一個或多個警示。透過使用事件，分析師可以將多個警示作為單一問題進行調查。

事件路由器

一種KUMA 服務，可讓您接收來自收集器和關聯器的事件流，然後根據設定的篩選器將事件分發到指定的目標。

代理程式

一種KUMA服務，用於在遠端裝置上接收事件並將其轉發給KUMA收集器。

傳輸封存檔案

一種封存檔案，包含Kaspersky Next XDR Expert元件、管理網路外掛程式以及Kaspersky Next XDR Expert和KDT的終端使用者許可協議。傳輸封存檔案包含在分發套件中。

儲存體

KUMA服務，用於儲存標準化事件，以便可以從KUMA快速且連續地存取它們以提取分析資料。

分段規則

允許您根據指定條件自動將相關警示拆分為不同事件的規則。

分發套件

一種封存檔案，其中包含Kaspersky Next XDR Expert元件的傳輸封存檔案、 Kaspersky Next XDR Expert和KDT的最終使用者授權協議，以及KDT公用程式和組態檔範本以及KUMA清查檔案。

可觀察部分

與警示和事件相關的物件，例如MD5和SHA256雜湊值、IP位址、URL、網域名稱、使用者名稱或主機名稱。

回應操作

在常規程式中啟動的操作。

多租用戶

此模式使主管理員能夠獨立地向多個用戶端提供Kaspersky Next XDR Expert功能，或將資產、應用程式設定和物件分開用於不同辦公室。此外，多租戶模式可讓您從父租用戶複製和繼承租用戶設定和物件，並將Kaspersky Next XDR Expert的產品授權金鑰自動套用至層次結構中的所有租用戶。

威脅發展鏈

用於追蹤網路攻擊階段的一系列步驟。威脅發展鏈可讓您分析威脅的原因。若要建立威脅發展鏈，受管理的應用程式會透過網路代理程式將資料從裝置傳輸到管理伺服器。

常規程式

根據指定演算法（常規程式演算法）回應警示或事件的物件。常規程式可讓您自動化工作流程並減少處理警示和事件所需的時間。

常規程式演算法

一種演算法，包括一系列回應操作，有助於分析和處理警示或事件。

收集器

一種KUMA服務，接收來自事件來源的訊息，對其進行處理，然後將它們傳輸到儲存體、關聯器和/或協力廠商服務來識別警示。

標準化事件

根據KUMA標準化事件資料模型處理的事件。

登錄檔

儲存應用程式容器的基礎設施元件，用於安裝和儲存Kaspersky Next XDR Expert專家元件。

目標主機

用於部署Kaspersky Next XDR Expert的實體機器或虛擬機器。目標主機包含在Kubernetes叢集中。Kaspersky Next XDR Expert元件在這些主機上運作。

租用戶

一個邏輯實體，對應於提供Kaspersky Next XDR Expert功能的組織單位（用戶端或辦公室）。每個租用戶可以包含資產、使用者及其存取權限、事件、警示、事件、常規程式，以及與其他卡巴斯基應用程式、服務和協力廠商解決方案的整合。租用戶還定義了包含物件上的一組可用操作。

節點

部署了Kaspersky Next XDR Expert的實體機器或虛擬機器。它包含主要節點和工作線程節點。主要節點用於管理叢集、儲存元資料和分配工作負載。工作節點用於執行Kaspersky Next XDR Expert元件的工作負載。

管理員裝置

一種實體機器或虛擬機器，用於使用KDT部署和管理Kubernetes叢集和Kaspersky Next XDR Expert。KDT在管理員主機上運作。如果管理員主機未包含在Kubernetes叢集，則僅用於部署。如果管理員主機包含在叢集中，它也將充當目標主機，用於Kaspersky Next XDR Expert元件的運作。

組態檔

一個YAML格式檔案，其中包含Kaspersky Next XDR Expert部署的目標主機清單和Kaspersky Next XDR Expert元件的安裝參數集。KDT使用組態檔。

網路代理

Open Single Management Platform的一個元件，實現管理伺服器和安裝在特定網路節點（工作站或伺服器）上的卡巴斯基應用程式之間的互動。該元件是公司內所有 Microsoft® Windows® 應用程式的通用元件。對於為類 Unix OS 和 macOS 開發的 Kaspersky 應用程式，分別有不同版本的網路代理。

網路位置辨識 (NLA)

幫助作業系統辨識目前網路的 Windows 服務。NLA 可偵測網路變化並調整裝置的安全配置。

自訂操作

KDT命令可讓您執行針對Kaspersky Next XDR Expert元件的其他操作。

調查圖表

它還包含一個視覺化分析工具，用於顯示事件、警示、事件、可觀測物件和資產（裝置）之間的關係。此外，調查圖表顯示事件的詳細資訊：相應的警示、使用者、資產及其共同內容。

警示

組織IT基礎設施中的事件，被Open Single Management Platform標記為異常或可疑，並可能對組織的IT基礎設施安全構成威脅。

資產

受保護的基礎設施裝置或使用者。如果在資產上偵測到警示或事件，您可以針對該資產執行回應操作。

輕量級 Nagent（LWNGT）

用於與行動裝置上的 Kaspersky Endpoint Security 進行互動的協定。LWNGT（又稱行動協定）起到網路代理的作用，而無需在行動裝置上實際安裝網路代理。

鑑證資料

該公用程式包含一系列旨在識別、獲取和分析資料的方法和技術，這些資料可用作對裝置進行的網路攻擊或其他非法活動的數位證據。

關聯器

一種KUMA服務，用於分析標準化的事件。

關聯規則

一種KUMA資源，用於識別已處理事件的定義序列，並在識別後執行特定操作。

有關協力廠商代碼的資訊

有關第三方代碼的資訊包含在作為運算子節點的裝置上的以下檔案中：

- legal_notices_ksmp.txt;
- legal_notices_kuma.txt;
- legal_notices_kesl.txt;
- legal_notices_kesw.txt;
- legal_notices_spp.txt.

這些檔案位於執行 Kaspersky Next XDR Expert 部署之使用者的 `~/kaspersky_eula` 目錄。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

Adobe、Acrobat、Flash、PostScript、Reader、Shockwave是Adobe在美國和/或其他國家/地區的註冊商標或商標。

AMD 和 AMD64 是 Advanced Micro Devices, Inc. 的商標和註冊商標。

Amazon、Amazon EC2、Amazon Web Services、AWS 和 AWS Marketplace 是 Amazon.com, Inc. 或其附屬公司的商標。

Apache 和 Apache Cassandra 是 Apache 軟體基金會在美國和/或其他國家的註冊商標或商標。

Apple、App Store、AppleScript、Carbon、FileVault、iPhone、Mac、Mac OS、macOS、OS X、Safari、QuickTime 是 Apple Inc. 的商標。

Arm是Arm Limited（或其子公司）在美國和/或其他地方的註冊商標。

Bluetooth註冊商標和服務標誌皆為Bluetooth SIG, Inc.所有。

LTS 和 Ubuntu 是 Canonical Ltd. 的註冊商標。

Check Point NGFW為Check Point Software Technologies Ltd.或其附屬公司的商標或註冊商標。

Cisco、IOS 和 Snort 是 Cisco Systems, Inc. 和/或其關係企業在美國及其他特定國家的註冊商標或商標。

Citrix、XenServer是Cloud Software Group, Inc.和/或其子公司在美國和/或其他國家的註冊商標或商標。

Citrix、XenServer是Cloud Software Group, Inc.和/或其子公司在美國和/或其他國家的註冊商標或商標。

Cloudflare、Cloudflare 標誌和 Cloudflare Workers 是 Cloudflare, Inc. 在美國和其他司法管轄區的商標和/或註冊商標。

Grafana註冊商標和標誌是Coding Instinct AB在美國和其他國家的註冊商標/服務標誌或商標/服務標誌，並經Coding Instinct許可使用。我們與Coding Instinct或Grafana社群沒有任何關聯，也未獲得其認可或贊助。

Corel是Corel Corporation和/或其附屬公司在美國和其他特定國家/地區的註冊商標。

Dell Technologies和其他商標是Dell Inc.或其子公司的商標。

Docker和Docker標誌是Docker, Inc.在美國和/或其他國家的商標或註冊商標。Docker, Inc.和其他方可能還擁有本文所使用的其他術語的商標權。

Elasticsearch是Elasticsearch BV在美國和其他國家/地區註冊的商標。

ESET是ESET spol. s r.o.或相應ESET實體的商標或註冊商標。

F5是F5 Networks, Inc.在美國和其他某些國家的商標。

Firebird是Firebird Foundation的註冊商標。

Fortinet、FortiGate、FortiMail和FortiSOAR是Fortinet, Inc.在美國和/或其他國家的註冊商標或商標。

FreeBSD是FreeBSD foundation的註冊商標。

Google、Android、Chrome、Dalvik、Firebase、Google Chrome、Google Earth、Google Maps、Google Play和Google Public DNS是Google LLC的商標。

華為、EulerOS和華為雲是華為技術有限公司的商標。

Radmin是Famatech的註冊商標。

IBM和QRadar是International Business Machines Corporation在全球眾多司法管轄區的註冊商標。

Intel和Insider是Intel Corporation或其子公司的商標。

Node.js是Joyent, Inc.的商標。

Juniper、Juniper Networks和JUNOS是Juniper Networks, Inc.在美國和其他國家的商標或註冊商標。

Linux是Linus Torvalds在美國和其他國家/地區的註冊商標。

NetWare是Novell Inc.在美國和其他國家/地區的註冊商標。

Microsoft、Access、Active Directory、ActiveSync、ActiveX、Azure、BitLocker、Excel、Halo、Hyper-V、InfoPath、Internet Explorer、Lync、Microsoft 365、Microsoft Edge、MS-DOS、MultiPoint、Office 365、OneNote、Outlook、PowerPoint、PowerShell、Segoe、SharePoint、Skype、SQL Server、Tahoma、Visio、Win32、Windows、Windows Media、Windows Mobile、Windows Phone、Windows PowerShell、Windows Server和Windows Vista是Microsoft集團旗下公司的商標。

CVE是MITRE Corporation的註冊商標。

Mozilla和Firefox是Mozilla Foundation在美國和其他國家/地區的商標。

NetApp是NetApp, Inc.在美國和其他國家/地區的商標和註冊商標。

Netskope、Netskope標誌以及本文提及的其他Netskope產品名稱均為Netskope, Inc.和/或其子公司的商標，可能已在美國專利商標局和其他國家註冊。

NetWare是Novell Inc.在美國和其他國家/地區的註冊商標。

Novell是Novell Enterprises Inc.在美國和其他國家/地區的註冊商標。

OpenSSL是OpenSSL軟體基金會擁有的商標。

Oracle、Java和JavaScript是Oracle和/或其關係企業的註冊商標。

OpenVPN是OpenVPN, Inc.的註冊商標。

Parallels、Parallels標誌和Coherence是Parallels International GmbH的商標或註冊商標。

PROOFPOINT是Proofpoint, Inc.在美國和其他國家的商標。

Chef是Progress Software Corporation和/或其子公司或附屬公司之一在美國和/或其他國家/地區的商標或註冊商標。

Puppet 是 Puppet, Inc. 的商標或註冊商標。

Python 是 Python 軟體基金會的商標或註冊商標。

Ansible 是 Red Hat, Inc. 在美國和其他國家/地區的註冊商標。

Red Hat、Fedora和Red Hat Enterprise Linux是Red Hat Inc.或其子公司在美國和其他國家/地區的商標或註冊商標。

BlackBerry是Research In Motion Limited所有的商標，在美國和/或其他國家註冊。

Samsung是SAMSUNG在美國或其他國家的商標。

Sendmail以及其他名稱和產品名稱均為Sendmail, Inc.的商標或註冊商標。

Debian是Public Interest, Inc.公司的軟體的註冊商標。

SolarWinds、Dameware 商標為 SolarWinds Worldwide, LLC 或其附屬公司的專屬財產，在美國專利商標局註冊，可能已在其他國家/地區註冊或正在申請註冊。

Splunk是Splunk Inc.在美國和其他國家/地區的商標和註冊商標。

CommuniGate Pro名稱是Stalker Software, Inc.的商標或註冊商標。

SUSE 是 SUSE LLC 在美國和其他國家/地區的註冊商標。

Symantec是Symantec Corporation或其附屬公司在美國和其他國家的商標或註冊商標。

Symbian 是 Symbian Foundation Ltd. 所擁有的商標。

OpenAPI 是 The Linux Foundation 的商標。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商標。

Trend Micro是Trend Micro Incorporated的商標或註冊商標。

用於識別UserGate產品和服務的名稱、圖像、標誌和圖片是UserGate和/或其子公司或附屬公司的專有標誌，產品本身歸UserGate所有。

VMware、VMware vSphere和VMware Workstation是VMware, Inc.在美國和其他國家/地區的註冊商標和/或商標。

UNIX是在美國和其他國家/地區的註冊商標，透過X/Open Company Limited授權。

ClickHouse. 是 YANDEX LLC 的商標。

Zabbix 是 Zabbix SIA 的註冊商標。

MITRE公司的使用條款

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes.Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

"© 2025 The MITRE Corporation.This work is reproduced and distributed with the permission of The MITRE Corporation."

DISCLAIMERS

MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques.Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE MITRE CORPORATION, ITS BOARD OF TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.