kaspersky

Kaspersky Anti Targeted Attack Platform

© 2026 AO Kaspersky Lab

目錄

Kaspersky Anti Targeted Attack Platform 說明
關於 Kaspersky Anti Targeted Attack Platform
新增功能
已修復問題
使用 Kaspersky Threat Intelligence Portal
分發套件
硬體和軟體需求
Kaspersky Endpoint Security for Windows 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性
Kaspersky Endpoint Security for Linux 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性
Kaspersky Endpoint Security for Mac 與 Kaspersky Anti Targeted Attack Platform 版本的相容性
KUMA 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性
XDR 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性
KPSN 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性
Kaspersky Anti Targeted Attack Platform 與 VK 雲端的相容性
限制
一般限制
將 Central Node 作為叢集部署
Sensor 限制
Sandbox 限制
在虛擬化平台上部署應用程式
在分佈式解決方案和多組織用戶模式下使用應用程式
與 Kaspersky Endpoint Security for Windows 的相容性有限
與 Kaspersky Endpoint Security for Linux 的相容性有限
與 Kaspersky Endpoint Security for Mac 的相容性有限
XDR 相容性限制
透過 ICAP 與代理伺服器整合
資料提供
應用程式的服務資料
Central Node 和 Sensor 元件的資料
Sensor 元件的流量資料
偵測中的資料
事件中的資料
報告中的資料
儲存和隔離區中物件的資料
Sandbox 元件資料
應用程式元件之間傳輸的資料
應用程式偵錯檔案中包含的資料
Kaspersky Endpoint Security for Windows 資料
Kaspersky Endpoint Security for Linux 資料
Kaspersky Endpoint Security for Mac 資料
應用程式產品授權
關於最終使用者產品授權協議
關於產品授權憑證

- 關於產品授權
- 關於產品授權金鑰
- 關於金鑰檔案
- 關於啟動碼
- 關於訂購
- 新增產品授權金鑰
- 替代產品授權金鑰
- 刪除產品授權金鑰
- 在 Central Node 的 Web 介面中檢視有關新增的產品授權金鑰的資訊
- 在 Central Node 的 Web 介面中檢視最終使用者產品授權協議的文字
- 在 Central Node 的 Web 介面中檢視隱私權政策文字
- 檢視應用程式中使用的協力廠商代碼的資訊
- 在 Sandbox 的 Web 介面中檢視最終使用者產品授權協議的文字
- 檢視 Endpoint Agent 元件的最終使用者產品授權協議文字
- 基於產品授權的應用程式模式

應用程式架構
- Sensor 元件
- Central Node 元件
- Sandbox 元件
- Endpoint Agent 元件

應用程式的工作原理

分佈式解決方案和多租戶
- 分佈式解決方案及多租戶模式過渡方案
- 修改分佈式解決方案和多租戶模式的應用程式設定
- 將 PCN 角色分配給一台伺服器
- 將 SCN 角色指派給一台伺服器
- 處理 SCN 到 PCN 的連線請求
- 檢視有關租戶、PCN 和 SCN 伺服器的資訊
- 將租戶新增至 PCN 伺服器
- 從 PCN 伺服器刪除租戶
- 在 PCN 伺服器上重新命名租戶
- 還原 SCN 到 PCN 的連線
- 斷開 SCN 與 PCN 的連線
- 修改斷開 SCN 與 PCN 連線的應用程式設定

規模調整指南
- 部署和安裝應用程式元件的常見方案
  - 雙伺服器部署方案
  - 三伺服器部署方案
  - 四台或以上伺服器部署方案
  - 使用 Sandbox 元件部署 KEDR 功能的方案
  - 在沒有 Sandbox 元件的情況下部署 KEDR 功能的方案
- 大小計算器
  - Sensor 元件的計算
  - 使用 KATA 功能時對 Central Node 元件的計算
  - 使用 KEDR 功能時對 Central Node 元件的計算
  - 使用 KATA 和 KEDR 功能時對 Central Node 元件的計算
  - 使用 KATA 和 NDR 功能時對 Central Node 元件的計算

使用 KATA 和 NDR 功能時對 Central Node 元件的計算
配置與外部系統整合時 Central Node 元件的計算
與 Kaspersky Secure Mail Gateway 整合時 Central Node 元件的計算
使用 ICAP 功能時對 Central Node 元件的計算
分佈式解決方案和多租戶模式下 Central Node 元件的計算
作為叢集部署的 Central Node 元件的計算
解決方案小規模配置的計算
計算事件資料庫和儲存空間的大小，以配置應用程式延伸參數
Sandbox 元件計算
安裝和執行應用程式的初始配置
準備安裝應用程式元件
準備 IT 基礎架構以安裝應用程式元件
為透過 POP3 與用於接收訊息的郵件伺服器整合準備 IT 基礎架構
為透過 SMTP 與郵件伺服器整合準備 IT 基礎架構
準備虛擬機以安裝 Sandbox 元件
準備包含 Central Node、Sensor 和 Sandbox 元件的安裝磁碟映像
安裝和設定應用程式元件的步驟
安裝 Sandbox 元件
步驟 1：檢視最終使用者產品授權協議和隱私權政策
步驟 2：選擇安裝 Sandbox 元件的磁碟
步驟 3：設定 Sandbox 管理員密碼的最小密碼長度
步驟 4：建立 Sandbox 管理員帳戶
步驟 5：設定管理網路介面
步驟 6：指派主機名稱並新增DNS伺服器位址
步驟 7：設定靜態網路路由
將帶有嵌入式 Sensor 的 Central Node 元件部署為叢集
部署儲存伺服器
步驟 1：檢視最終使用者產品授權協議和隱私權政策
步驟 2：選擇伺服器角色
步驟 3：選取部署模式
步驟 4：與 Kaspersky Endpoint Security for Linux 的相容性有限
步驟 5：選擇伺服器定址的網路遮罩
步驟 6：選擇用於定址應用程式元件的網路遮罩
步驟 7：選擇叢集網路介面
步驟 8：選擇外部網路介面
步驟 9：若要選擇用於取得網路介面 IP 位址的方法
步驟 10：建立管理員帳戶並在叢集中驗證伺服器
建立管理員帳戶
驗證叢集中的伺服器
步驟 11：新增 DNS 伺服器位址
步驟 12：配置與 NTP 伺服器的時間同步
步驟 13：選擇用於 Ceph 儲存的磁碟
部署處理伺服器
步驟 1：檢視最終使用者產品授權協議和隱私權政策
步驟 2：選擇伺服器角色
步驟 3：與 Kaspersky Endpoint Security for Linux 的相容性有限
步驟 4：選取叢集伺服器定址的網路遮罩

步驟 5：選擇用於定址應用程式元件的網路遮罩
步驟 6：選擇叢集網路介面
步驟 7：選擇外部網路介面
步驟 8：選擇取得網路介面 IP 位址的方法
步驟 9：驗證叢集中的伺服器
步驟 10：選擇 NDR 功能的在地化語言並配置從 SPAN 連接埠接收鏡像流量
選擇 NDR 功能的本地化語言
配置從 SPAN 連接埠接收映像流量
清除儲存伺服器上的硬碟
在伺服器上安裝帶有嵌入式 Sensor 的 Central Node 元件
步驟 1：檢視最終使用者產品授權協議和隱私權政策
步驟 2：選擇伺服器角色
步驟 3：與 Kaspersky Endpoint Security for Linux 的相容性有限
步驟 4：分配用於 Targeted Attack Analyzer 元件資料庫的磁碟
步驟 5：選擇伺服器定址的網路遮罩
步驟 6：為應用程式元件的定址選擇網路遮罩
步驟 7：選擇外部網路介面
步驟 8：若要選擇用於取得網路介面 IP 位址的方法
步驟 9：建立管理員帳戶
步驟 10：選擇 NDR 功能的本地化語言
步驟 11：新增 DNS 伺服器位址
步驟 12：配置與 NTP 伺服器的時間同步
在獨立伺服器上安裝 Sensor 元件
步驟 1：檢視最終使用者產品授權協議和隱私權政策
步驟 2：選擇伺服器角色
步驟 3：選擇安裝元件的磁碟
步驟 4：為伺服器定址選擇網路遮罩
步驟 5：為應用程式元件的定址選擇網路遮罩
步驟 6：選擇外部網路介面
步驟 7：選擇取得網路介面 IP 位址的方法
步驟 8：建立管理員帳戶
步驟 9：新增 DNS 伺服器位址
步驟 10：配置與 NTP 伺服器的時間同步
最佳化 Sensor 元件的網路介面設定
連線和配置 Sensor 元件的外部儲存
配置應用程式的大小設定
配置防火牆規則
裝有 Kaspersky Anti Targeted Attack Platform 元件的電腦使用的連接埠
叢集配置中 Kaspersky Anti Targeted Attack Platform 服務使用的連接埠
作為伺服器部署的 Central Node 的服務使用的連接埠
在獨立伺服器上安裝 Sensor 元件的配置中，服務使用的連接埠
網路流量分析服務之間的通訊連接埠
在 iptables 中管理 MTU 設定
配置 Endpoint Agent 元件與 KEDR 功能塊的整合
配置與 Kaspersky Endpoint Security 的受信任連線
下載 Central Node 伺服器的 TLS 憑證
在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中為 Central Node 伺服器產生 TLS 憑證

使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面為 Central Node 伺服器上傳您自己的 TLS 憑證
在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中啟用 Endpoint Agent 元件的 TLS 憑證驗證
在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中產生 Endpoint Agent 元件的 TLS 憑證並下載加密容器
使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面上您自己的 Endpoint Agent 元件的 TLS 憑證
在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中檢視 Endpoint Agent 元件的 TLS 憑證表
在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中篩選和搜尋 Endpoint Agent 元件的 TLS 憑證
在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中刪除 Endpoint Agent 元件的 TLS 憑證
設定從 Kaspersky Agent 到 Sensor 伺服器的流量重新導向
配置Endpoint Agent 元件與 NDR 功能塊的整合
準備從 Endpoint Agent 元件接收資料的場景
Integration Server 表
新增 Integration Server
為 Integration Server 的用戶端建立通訊封包
啟用或停用 Integration Server
編輯 Integration Server 設定
刪除 Integration Server
與郵件感應器的整合
應用程式使用入門
使用管理員帳戶開始使用應用程式 Web 介面
應用程式管理員功能表使用入門
在技術支援模式下開始使用應用程式
管理應用程式管理員和使用者的帳戶
建立用於應用程式 Web 介面的管理員帳戶
建立用於應用程式 Web 介面的使用者帳戶
配置使用者帳戶表顯示
檢視使用者帳戶表
篩選使用者帳戶
清除帳戶篩選器
變更使用者帳戶對 PCN 和 SCN 資料的存取權限
啟用或停用使用者帳戶
修改使用者帳戶的密碼
變更您的帳戶密碼
使用網域帳戶進行身分驗證
建立 keytab 檔案
配置與 Active Directory 的整合
停用與 Active Directory 的整合
參與卡巴斯基安全網路並使用卡巴斯基私有安全網路
檢視 KSN 聲明並配置參與 KSN
配置使用 KPSN
配置與 KPSN 本機信譽資料庫的連線
配置要儲存到 KPSN 本機信譽資料庫的資訊
KSN 參與度和 KPSN 使用量下降
透過 Web 介面管理 Sandbox 元件
更新 Sandbox 元件資料庫
手動更新資料庫
選擇資料庫更新來源
使用卡巴斯基更新實用程式更新元件資料庫

- 使用卡巴斯基更新實用程式下載更新套件
- 啟用和停用更新資料庫的代理伺服器
- 配置資料庫更新的代理伺服器連線設定

配置 Sandbox 和 Central Node 元件間的連線

- 在 Sandbox Web 介面處理來自 Central Node 伺服器的連線請求

配置 Sandbox 元件網路介面

- 配置 DNS 設定
- 設定管理網路介面的設定
- 配置用於對已處理物件進行 Internet 存取的網路介面的設定
- 新增、變更和移除靜態網路路由

Sandbox 身分驗證政策

- 終止不活動的 Sandbox 工作階段
- 關於 Sandbox 身分驗證嘗試失敗的通知

設定 Sandbox 系統的日期和時間

準備虛擬機以供使用

管理 Sandbox 儲存中的作業系統和應用程式映像

- 檢視 Sandbox 儲存中的作業系統和應用程式映像表
- 將作業系統和應用程式映像上傳到儲存
- 啟動 Sandbox 儲存中的作業系統和應用程式映像
- 從 Sandbox 儲存中刪除作業系統和應用程式映像

管理虛擬機範本

- 建立虛擬機範本
- 檢視範本表
- 開啟或關閉範本
- 編輯範本
- 配置作業系統和軟體
  - 緩解 Spectre 和 Meltdown 弱點
  - 解除安裝 Windows Defender
- 匯出範本
- 匯入範本
- 刪除範本

管理虛擬機

- 建立虛擬機
  - 在“虛擬機”部分建立虛擬機
  - 在範本表中建立虛擬機
  - 在範本視圖中建立虛擬機
  - 使用命令列建立和安裝虛擬機器
- 檢視自預設虛擬機器表
- 檢視自訂虛擬機表
- 安裝虛擬機
- 刪除虛擬機
- 下載偵錯符號

設定同時運作的虛擬機的最大數量

變更自訂虛擬機器的產品授權金鑰數量

匯出 Sandbox 設定

匯入 Sandbox 設定

重新啟動 Sandbox 伺服器

關閉 Sandbox 伺服器電源
變更 Sandbox 管理員帳戶密碼
對於管理員：應用程式 Web 介面使用入門
Kaspersky Anti Targeted Attack Platform 介面
監控應用程式的效能
關於小工具和佈局
在"儀表板"部分選擇要管理的租戶和伺服器
新增小工具到目前佈局
在目前佈局中移動小工具
變更 NDR 小工具中資訊的顯示
從目前佈局移除小工具
儲存佈局為 PDF
配置小工具中的資料顯示週期
監控傳入資料的接收與處理
監控由應用程式模組和元件對資料進行處理的佇列
監控 Sandbox 元件對資料的處理
檢視應用程式模組和元件的工作狀況
管理 Central Node 或 Sensor 伺服器資訊
檢視有關 Central Node 或 Sensor 伺服器的資訊
檢視網路介面資訊
識別與網路介面關聯的乙太網路連接埠
使用應用程式 Web 介面管理 Central Node、PCN 或 SCN 伺服器
配置伺服器上的日期和時間
產生或上傳伺服器的 TLS 憑證
下載伺服器的 TLS 憑證
伺服器的 FQDN 設定
配置 DNS 設定
設定網路介面的設定
設定預設網路路由
設定代理伺服器連線設定
設定郵件伺服器連線
管理流量節省設定
管理儲存流量傾印檔案的設定
管理 Sensor 元件
將 Sandbox 元件連線到 Central Node
使用通訊封包連線 Sensor 元件
透過網路自動新增和連線 Sensor 元件
刪除 Sensor 元件
編輯獨立於 Central Node 安裝的 Sensor 設定
準備編輯獨立於 Central Node 安裝的 Sensor 設定
管理 Sensor 伺服器的憑證
在 Sensor 伺服器的管理員功能表中為 Sensor 伺服器產生 TLS 憑證
在 Sensor 伺服器的管理員功能表中上傳您自己的 TLS 憑證
將 Sensor 伺服器的 TLS 憑證下載到您的電腦
變更伺服器名稱

管理監控點
新增監控點
重新命名監控點
啟用監控點
停用監控點
正在刪除監控點
配置掃描檔案的最大大小
配置 HTTP 封包主體傾印
配置透過 SMTP 與郵件伺服器整合
配置透過 ICAP 與代理伺服器整合
啟用和停用透過 ICAP 與代理伺服器整合
啟用或停用 ICAP 流量即時掃描
配置 ICAP 流量即時掃描
配置通知頁面的顯示
配置 SPAN 連接埠映像流量的記錄
選擇用於從 SPAN 連接埠接收映像流量的網路協定
配置 SPAN 連接埠映像流量的記錄
配置透過 POP3 與郵件伺服器整合
身分驗證政策
首次身分驗證成功後強制變更密碼
強制定期變更密碼
終止非活動工作階段
關於身分驗證嘗試失敗的通知
管理叢集
檢視叢集的伺服器表
將伺服器新增至叢集
增加儲存伺服器上的磁碟空間
重新啟動叢集中的伺服器
停用伺服器
從叢集中刪除伺服器
啟動和關閉叢集
有關 Central Node 和 Sensor 伺服器允許的最大CPU 和 RAM 負載的通知
配置 Central Node 和 Sensor 伺服器允許的最大CPU 和 RAM 負載
設定 SNMP 協定連線
Kaspersky Anti Targeted Attack Platform 的 MIB 物件描述
管理 Endpoint Agent 主機資訊
在“Endpoint Agent”部分中選擇要管理的租戶
檢視獨立 Central Node 伺服器上具有 Endpoint Agent 元件的主機表
檢視有關主機的資訊
依主機名稱篩選並搜尋具有 Endpoint Agent 元件的主機
根據已與網路隔離的 Endpoint Agent 元件篩選和搜尋主機
按 PCN 和 SCN 伺服器名稱篩選並搜尋具有 Endpoint Agent 元件的主機
依電腦 IP 位址篩選並搜尋具有 Endpoint Agent 元件的主機
依電腦上的作業系統版本篩選並搜尋具有 Endpoint Agent 元件的主機
依元件版本篩選並搜尋具有 Endpoint Agent 元件的主機
依活動篩選並搜尋具有 Endpoint Agent 元件的主機
為具有 Endpoint Agent 元件的主機快速建立篩選器

為具有 Endpoint Agent 元件的主機重設篩選器
配置 Endpoint Agent 元件的活動指示器
刪除具有 Endpoint Agent 元件的主機
自動刪除不活動的主機
配置與 Sandbox 元件的整合
檢視具有 Sandbox 元件的伺服器表
使用 Sandbox 元件建立連線到伺服器的請求
啟用和停用與 Sandbox 元件的連線
刪除與 Sandbox 元件的連線
選擇掃描 Sandbox 中的物件時要使用的作業系統
從 Endpoint Agent 主機手動傳送檔案以供 Sandbox 掃描
啟用和停用從 Endpoint Agent 主機手動傳送檔案以供 Sandbox 掃描
配置與外部系統的整合
檢視外部系統表
處理來自外部系統的請求
從允許整合的清單中移除外部系統
配置處理來自郵件感應器的流量的優先順序
配置與 Kaspersky Managed Detection and Response 的整合
啟用 MDR 整合
停用 MDR 整合
替換 MDR 設定檔
配置與 SIEM 系統的整合
啟用和停用事件資訊記錄到遠端日誌
配置 SIEM 系統整合的主要設定
上傳 TLS 憑證
啟用和停用與 SIEM 系統的連線的 TLS 加密
有關偵測的 syslog 郵件的內容和屬性
管理連線器
受管理和不受管理的連線器
將事件、應用程式訊息和稽核記錄傳送到第三方系統
透過 Cisco 交換機連線器自動控制裝置的網路存取
新增連線器
檢視連線器表
啟用或停用連線器
編輯連線器設定
為連線器建立新的通訊封包
正在刪除連線器
新增和刪除連線器類型
檢視連線器類型表
新增連線器類型
刪除連線器類型
管理遠端連線的帳戶憑據 Secret
新增 Secret
檢視 Secret 表
連線到遠端裝置時防止 Secret 洩漏
編輯 Secret 的設定
刪除 Secret

更新應用程式資料庫
選擇資料庫更新來源
手動更新資料庫
使用卡巴斯基更新實用程式更新應用程式資料庫
使用卡巴斯基更新實用程式下載更新套件
更新使用 API 連線到 Central Node 的憑證
與工具整合以解包加密的 SSL/TLS 流量
對於安全人员：應用程式 Web 介面使用入門
Kaspersky Anti Targeted Attack Platform 介面
選擇要在應用程式的 Web 介面中管理的租戶
監控應用程式的效能
關於小工具和佈局
新增小工具到目前佈局
在目前佈局中移動小工具
變更 NDR 小工具中資訊的顯示
從目前佈局移除小工具
儲存佈局為 PDF
配置小工具中的資料顯示週期
配置小工具顯示縮放
"警示"類型小工具管理基礎知識
事件小工具中的資訊
事件小工具中的資訊
檢視應用程式模組和元件的工作狀況
管理技術
啟用或停用技術
配置裝置活動偵測模式
管理技術繼承
檢視警示表
配置警示表顯示
篩選、排序和搜尋警示
按 VIP 身分篩選警示
按時間篩選並搜尋警示
按重要性等級篩選警示
按偵測到的物件的類別篩選和搜尋警示
按取得的資訊篩選和搜尋警示
按來源位址篩選和搜尋警示
按目的位址篩選並搜尋警示
按伺服器名稱篩選並搜尋警示
按技術名稱篩選並搜尋警示
依使用者處理狀態篩選和搜尋警示
按分配了警示的使用者的名稱篩選和搜尋警示
對表中的警示進行排序
快速建立警示篩選器
儲存篩選器
重置警示篩選器

警示處理建議
AM 警示處理建議
TAA 警示處理建議
SB 警示處理建議
IOC 警示處理建議
YARA 警示處理建議
IDS 警示處理建議
處理 NDR:IDS 和 AA 警示的建議
檢視警示
檢視警示詳細資訊
有關任何類型警示的一般資訊
物件資訊部分中的資訊
“警示詳情”部分的資訊
“有關使用 NDR 技術進行掃描的資訊”部分中的資訊
掃描結果部分的資訊
IDS 規則部分中的資訊
URL 部分的資訊
“偵測相關裝置的 IP 位址”部分的資訊
網路事件部分的資訊
Sandbox 掃描結果
IOC 掃描結果
主機部分中的資訊
“變更日誌”部分中的資訊
傳送警示資料
檢視警示關係
在警示上執行的使用者操作
將警示分配給特定使用者
標記單個警示處理的完成
標記警示處理的完成
修改 VIP 警示的狀態
為警示新增註釋
監控網路流量事件
NDR 事件分數和嚴重程度
NDR 事件註冊技術
NDR 事件狀態
已註冊 NDR 事件表
配置已註冊事件表
檢視嵌套在聚合事件內的事件
檢視 NDR 事件的詳細資訊
變更 NDR 事件的狀態
新增標記
將 NDR 事件複製到文字編輯器
下載事件流量
建立用於將事件匯出至網路共用的目錄
事件資料庫威脅追蹤
在建構器模式下搜尋事件
在原始碼模式下搜尋事件

- 轉換產生器查詢以在原始碼模式下搜尋事件
- 事件搜尋條件
- 運算子
- 將表中的事件進行排序
- 變更事件搜尋條件
- 搜尋“偵測”和“偵測處理結果”類型的事件
- 使用 IOC 或 YAML 檔案中指定的條件搜尋事件
- 根據事件搜尋條件建立 TAA (IOA) 規則

事件資訊

- 事件處理建議
  - 遵循建議隔離主機
  - 遵循建議防止檔案運行
  - 遵循建議建立工作
- 有關事件樹中事件的資訊
  - 檢視事件樹中的父處理程序資訊
  - 檢視事件樹中有關父處理程序發起的事件的資訊
  - 檢視事件樹中的主機資訊
- 檢視事件表
- 配置事件表顯示
- 檢視有關事件的資訊
- 有關“處理程序已啟動”事件的資訊
- 有關“處理程序已終止”事件的資訊
- 有關“模組已載入”事件的資訊
- 有關“遠端連線”事件的資訊
- “防護規則”事件資訊
- 有關“文件被封鎖”事件的資訊
- 有關“檔案已修改”事件的資訊
- 有關“系統事件日誌”事件的資訊
- 有關“登錄檔變更”事件的資訊
- 有關“連接埠被偵聽”事件的資訊
- 有關“驅動程式已載入”事件的資訊
- 有關“DNS”事件的資訊
- 有關“LDAP”事件的資訊
- 有關“命名管道”事件的資訊
- 有關“WMI”事件的資訊
- 有關“偵測”事件的資訊
- 有關“偵測處理結果”事件的資訊
- 有關“被解釋檔案運行”事件的資訊
- 有關“AMSI 掃描”事件的資訊
- 有關“在主控台進行互動式命令輸入”事件的資訊
- 有關“代碼注入”事件的資訊
- 有關“處理程序存取”事件的資訊
- 關於“USB 裝置”事件的資訊

根據 Kaspersky TAA (IOA) 規則進行事件鏈掃描

- 啟用或停用根據 Kaspersky TAA (IOA) 規則進行事件鏈掃描
- 檢視由 Kaspersky TAA (IOA) 規則標記的事件

管理資產
- 檢視裝置表
- 檢視裝置資訊
- 自動新增和更新裝置
- 手動新增裝置
  - 使用裝置表時新增裝置
  - 在管理拓撲圖時新增裝置
  - 根據網路互動圖上的未知裝置節點新增裝置
  - 根據拓樸圖上非管理交換器新增裝置
- 自動分配裝置狀態
- 根據條件自動對裝置進行分組
  - 根據條件自動將裝置分組，從群組樹的根開始
  - 自動將裝置分組到選定的裝置群組中
- 手動將裝置分組
  - 將裝置新增至群組中
  - 將多個裝置新增至一個群組
  - 從群組中刪除裝置
  - 從群組中刪除多個裝置
- 將帶有元件和群組的伺服器移至網路互動圖上的其他群組
- 裝置群組樹
- 手動編輯裝置群組樹
  - 新增群組
  - 重新命名群組
  - 刪除群組
  - 移動群組
  - 搜尋群組
  - 更新樹
- 新增和刪除裝置標籤
  - 為單個裝置新增標籤
  - 為多個裝置新增標籤
  - 從單個裝置上刪除標籤
  - 清除多個裝置的標籤清單
- 回應
- 監控裝置上的使用者
- 監控裝置上的檔案執行狀況
- 主動裝置輪詢作業
  - 新增主動輪詢作業
  - 編輯主動輪詢作業
  - 檢視主動輪詢作業表
  - 啟動和停止主動輪詢作業
  - 檢視有關主動輪詢作業運行的一般資訊
  - 檢視有關主動輪詢作業執行的報告
  - 刪除主動輪詢作業

配置位址空間
- 關於位址空間規則
- 關於位址空間子網
- 新增位址空間

為資產管理建立子網路清單
新增子網路
編輯子網路設定
刪除子網路
檢視所選子網路中具有 IP 位址的裝置的資訊
變更位址空間
刪除位址空間
使用網路互動圖
網路互動圖上的節點
網路互動圖上的裝置群組
網路互動圖上的連結
檢視物件詳細資訊
改變網路互動圖的比例
定位網路互動圖
固定和取消固定節點和群組
手動重新排列節點和群組
自動排列節點和群組
在網路互動圖上搜尋節點
篩選網路互動圖上的物件
節點和連結的全面篩選
使用時間尺度上的時間段進行過濾
按已註冊事件篩選
節點過濾
按裝置狀態篩選節點
按裝置安全狀態篩選節點
按裝置類別篩選節點
啟用和停用與過濾節點關聯的節點的顯示
篩選連結
按緊急性分數過濾連接
按通訊協定篩選連接
按 OSI 模型層篩選連接
重置篩選條件
儲存和載入網路互動圖顯示設定
新增視圖，同時儲存目前網路互動圖顯示設定
在儲存目前網路互動圖顯示設定的同時更新視圖
重新命名網路互動圖視圖
刪除網路互動圖視圖
在網路互動圖上套用已儲存的視圖設定
監控網路工作階段
網路工作階段表
檢視網路工作階段詳細資訊
下載網路工作階段流量
搜尋網路封包
預先配置網路封包搜尋規則
Kaspersky Anti Targeted Attack Platform 偵測到的協定

監控風險
關於弱點類別中的風險
持續風險管理流程的實施方案
檢視風險表
檢視風險資訊
手動變更風險狀態
使用裝置表時檢視風險詳細資訊
配置 NDR 事件類型
檢視事件類型表
編輯系統事件類型的設定
配置自動儲存系統事件類型的流量
配置透過連線器轉送事件
Kaspersky Anti Targeted Attack Platform 中的常見替換變數
NDR 事件註冊技術
Kaspersky Anti Targeted Attack Platform 中的系統事件類型
入侵偵測技術的系統事件類型
資產管理技術的系統事件類型
外部系統技術的系統事件類型
端點防護平台技術的系統事件類型
配置風險類型
檢視風險類型表
變更風險類型的基本分數
管理儲存風險的設定
管理 Endpoint Agent 主機資訊
配置具有 Endpoint Agent 元件的主機表的顯示
配置具有 Endpoint Agent 元件的主機表的顯示
檢視有關主機的資訊
依主機名稱篩選並搜尋具有 Endpoint Agent 元件的主機
根據已與網路隔離的 Endpoint Agent 元件篩選和搜尋主機
按 PCN 和 SCN 伺服器名稱篩選並搜尋具有 Endpoint Agent 元件的主機
依電腦 IP 位址篩選並搜尋具有 Endpoint Agent 元件的主機
依電腦上的作業系統版本篩選並搜尋具有 Endpoint Agent 元件的主機
依元件版本篩選並搜尋具有 Endpoint Agent 元件的主機
依活動篩選並搜尋具有 Endpoint Agent 元件的主機
為具有 Endpoint Agent 元件的主機快速建立篩選器
為具有 Endpoint Agent 元件的主機重設篩選器
刪除具有 Endpoint Agent 元件的主機
限制來自 Endpoint Agent 的遙測
使用 Endpoint Agent 元件對主機進行網路隔離
建立一個網路隔離規則
新增網路隔離規則中的排除項
刪除網路隔離規則
與網路隔離相關的限制
根據 Kaspersky TAA (IOA) 規則自動從 Kaspersky Endpoint Agent 主機傳送檔案以供 Sandbox 元件掃描
啟用並停用從具有 Endpoint Agent 元件的主機自動傳送檔案以供 Sandbox 元件掃描

選擇掃描 Sandbox 中的物件時要使用的作業系統
檢視具有 Sandbox 元件的伺服器表
選擇掃描 Sandbox 中的物件時要使用的作業系統
管理工作
檢視工作表
檢視有關工作的資訊
建立獲取檔案工作
建立取證收集工作
建立登錄機碼檢索工作
建立 NTFS 中繼檔檢索工作
建立處理程序記憶體傾印檢索工作
建立磁碟映像檢索工作
將檔案從 RAW 轉換為 EWF 格式
建立 RAM 傾印檢索工作
建立處理程序終止工作
建立工作以使用 YARA 規則掃描主機
建立服務管理工作
建立應用程式執行工作
建立檔案刪除工作
建立檔案隔離工作
建立隔離檔案還原工作
建立工作副本
刪除工作
依建立時間篩選工作
按類型篩選工作
按名稱篩選工作
按檔案名稱和路徑篩選工作
依描述篩選工作
按伺服器名稱篩選工作
根據建立工作的使用者的名稱篩選工作
按處理狀態篩選工作
清除工作篩選器
管理政策（阻止規則）
檢視阻止規則表
配置阻止規則表顯示
檢視防止規則
建立阻止規則
匯入阻止規則
啟用和停用阻止規則
啟用和停用預設
刪除阻止規則
按名稱篩選阻止規則
按類型篩選阻止規則
按檔案雜湊篩選阻止規則
按伺服器名稱篩選阻止規則
清除阻止規則篩選器

管理使用者定義的規則
使用入侵指標 (IOC) 和攻擊指標 (IOA) 進行威脅搜索
管理使用者定義的 TAA (IOA) 規則
檢視 TAA（IOA）規則表
根據事件搜尋條件建立 TAA (IOA) 規則
匯入 TAA (IOA) 規則
檢視自訂 TAA (IOA) 規則詳細資訊
搜尋其中觸發了 TAA (IOA) 規則的警示和事件
篩選與搜尋 TAA (IOA) 規則
重置 TAA (IOA) 規則篩選器
啟用和停用 TAA (IOA) 規則
修改 TAA (IOA) 規則
刪除 TAA (IOA) 規則
管理使用者定義的 IOC 規則
檢視 IOC 檔案表
檢視有關 IOC 檔案的資訊
上傳 IOC 檔案
下載 IOC 檔案到電腦
掃描主機時啟用和停用 IOC 檔案的自動使用
刪除 IOC 檔案
在 IOC 掃描結果中搜尋警示
使用 IOC 檔案搜尋事件
篩選並搜尋 IOC 檔案
清除 IOC 檔案篩選器
配置 IOC 掃描排程
管理使用者定義的入侵偵測規則
檢視入侵偵測規則表
配置入侵偵測規則表的顯示
其他入侵偵測方法
啟用和停用入侵偵測規則集
載入和替換使用者定義的入侵偵測規則集
刪除使用者定義的入侵偵測規則集
管理使用者定義的 YARA 規則
檢視 YARA 規則表
配置 YARA 規則表顯示
匯入 YARA 規則
檢視 YARA 規則詳細資訊
篩選並搜尋 YARA 規則
清除 YARA 規則篩選器
啟用和停用 YARA 規則
刪除 YARA 規則
管理儲存和隔離區中的物件
檢視放入儲存空間的物件表
使用 Web 介面檢視有關手動放置在儲存中的物件的資訊
檢視有關透過獲取檔案工作放置在儲存中的物件的資訊
檢視有關透過獲取資料工作放置在儲存中的物件的資訊
從儲存下載物件

將物件上傳到儲存
傳送儲存中的物件進行掃描
刪除儲存中的物件
按物件類型篩選儲存中的物件
按物件描述篩選儲存中的物件
根據掃描結果篩選儲存中的物件
根據 Central Node、PCN 或 SCN 伺服器的名稱篩選儲存中的物件
按物件來源篩選儲存中的物件
根據物件放置在儲存中的時間篩選物件
清除儲存物件篩選器
檢視在具有 Kaspersky Endpoint Agent 元件的電腦上被隔離的物件表
檢視被隔離物件的資訊
從隔離中還原物件
取得 Kaspersky Anti Targeted Attack Platform 伺服器上被隔離物件的副本
從表格中移除隔離物件的資訊
按物件類型篩選有關隔離物件的資訊
按物件描述篩選有關隔離物件的資訊
按主機名稱篩選有關隔離物件的資訊
按時間篩選有關隔離物件的資訊
重置有關隔離物件資訊的篩選器
管理報告
管理常見報告
檢視範本和報告的表格
建立範本
根據範本建立報告
檢視報告
將報告下載到本機
編輯範本
按名稱篩選範本
根據建立範本的使用者的名稱篩選範本
按建立時間篩選範本
清除範本篩選器
刪除範本
按建立時間篩選報告
按名稱篩選報告
以具有 Central Node 元件的伺服器名稱篩選報告
根據建立報告的使用者的名稱篩選報告
清除報告篩選器
刪除報告
管理 NDR 報告
檢視 NDR 報告範本表
檢視 NDR 報告範本詳細資訊
檢視 NDR 報告表
根據範本手動產生 NDR 報告
複製 NDR 報告範本
編輯 NDR 報告範本
將 NDR 報告匯出到檔案

- 刪除 NDR 報告範本
- 刪除 NDR 報告
- 取消 NDR 報告產生
- 管理儲存報告檔案的設定

管理將 VIP 身分指派給警示的規則
- 檢視 VIP 身分分配規則表
- 建立 VIP 身分分配規則
- 刪除 VIP 身分分配規則
- 修改 VIP 身分分配規則
- 匯入 VIP 身分分配規則清單
- 匯出從掃描中排除的資料清單
- 按 VIP 身分指派規則類型篩選和搜尋
- 按 VIP 身分規則的值篩選和搜尋
- 按 VIP 身分分配規則描述篩選和搜尋
- 清除 VIP 身分分配規則篩選器

管理 NDR 事件的允許規則
- 檢視允許規則表格
- 使用空白設定或範本中的設定建立允許規則
- 從已註冊事件建立允許規則
- 複製允許規則
- 編輯允許規則的設定
- 啟用或停用允許規則
- 刪除允許規則

管理掃描排除項目清單
- 檢視從掃描中排除的資料表
- 新增掃描排除規則
- 刪除掃描排除規則
- 編輯新增到掃描排除項目的規則
- 匯出從掃描中排除的資料清單
- 依條件篩選掃描排除項目清單中的規則
- 按值搜尋掃描排除項目清單中的規則
- 重設掃描排除項目清單中的規則篩選器

管理入侵偵測規則排除項目
- 檢視新增至排除項目的入侵偵測規則表
- 將入侵偵測規則新增至排除項目
- 編輯新增至排除項目的入侵偵測規則的描述
- 從排除項目中刪除入侵偵測規則

管理 TAA 排除項目
- 檢視新增至排除項目的 TAA (IOA) 規則表
- 將 TAA (IOA) 規則新增到排除項目
- 檢視新增至排除項目的 TAA (IOA) 規則
- 從排除項目中刪除 TAA (IOA) 規則

管理 ICAP 排除項目
- 檢視 ICAP 排除表
- 將規則新增至 ICAP 排除項目
- 從 ICAP 排除項目中刪除規則
- 編輯或停用 ICAP 排除項目清單中的規則

- 按條件篩選 ICAP 排除項目清單中的規則
- 按值篩選 ICAP 排除項目清單中的規則
- 按狀態篩選 ICAP 排除項目清單中的規則
- 清除 ICAP 排除項目清單中的規則篩選條件
- 管理 SPAN 連接埠的映像流量
- 建立存檔的密碼清單
- 管理 Central Node 或 Sensor 伺服器資訊
- 檢視伺服器設定
- 檢視具有 Sandbox 元件的伺服器表
- 檢視用於掃描 Sandbox 中物件的作業系統集的設定
- 檢視外部系統表

管理使用者定義的 Sandbox 規則

- 檢視使用者定義的 Sandbox 規則表
- 配置 Sandbox 規則表顯示
- 篩選並搜尋 Sandbox 規則
- 清除 Sandbox 規則篩選器
- 檢視使用者定義的 Sandbox 規則資訊
- 建立使用者定義的檔案掃描 Sandbox 規則
- 建立使用者定義的 URL 掃描 Sandbox 規則
- 複製使用者定義的 Sandbox 規則
- 匯入使用者定義的檔案掃描 Sandbox 規則
- 編輯使用者定義的 Sandbox 規則
- 啟用或停用使用者定義 Sandbox 規則
- 匯出使用者定義的檔案掃描 Sandbox 規則
- 刪除使用者定義的 Sandbox 規則
- 檔案類別的副檔名清單

為 GosSOPKA 準備資料

- 執行用於準備 GosSOPKA 資料的實用程式

傳送通知

- 檢視傳送通知的規則表
- 建立傳送有關偵測的通知的規則
- 建立用於傳送有關應用程式元件操作的通知的規則
- 啟用和停用傳送通知的規則
- 修改傳送通知的規則
- 刪除傳送通知的規則
- 依規則類型篩選和搜尋通知轉送規則
- 根據通知主旨篩選和搜尋通知轉發規則
- 按電子郵件信箱篩選並搜尋通知轉送規則
- 根據狀態篩選和搜尋通知轉送規則
- 清除通知轉送規則篩選器

管理日誌

- 管理應用程式使用者活動日誌
  - 啟用和停用在活動日誌中記錄訊息
  - 下載活動日誌檔案
  - 應用程式使用者活動日誌中的記錄

管理 NDR 使用者活動日誌
管理日誌儲存設定
啟用和停用使用者活動稽核
檢視使用者活動稽核項目
設定追蹤日誌的最大儲存空間限制
設定追蹤日誌的最大儲存空間限制
Sensor 使用者活動日誌。
Sensor 元件管理員功能表中使用者操作的記錄
Sandbox 日誌
下載 Sandbox 系統日誌
下載 Sandbox 使用者活動日誌
應用程式使用者活動日誌中的記錄
下載 Kaspersky Anti Targeted Attack Platform 日誌
檢視應用程式訊息
配置 Kaspersky Anti Targeted Attack Platform 系統日誌和警示的保留期
檢視已傳送至 Kaspersky Anti Targeted Attack Platform 進行掃描的檔案的資訊
管理 Kaspersky Endpoint Security for Windows
管理 Kaspersky Endpoint Security for Linux
管理 Kaspersky Endpoint Security for Mac
備份和還原資料
備份和還原 Central Node 伺服器的資料
備份和還原作為叢集部署的 Central Node 伺服器的資料
分佈式解決方案和多租戶模式下 Central Node 伺服器的資料備份與還原
匯出資料的內容
建立備份副本時套用的限制
從備份副本還原應用程式後還原嵌入式 Sensor
升級 Kaspersky Anti Targeted Attack Platform
升級伺服器上安裝的 Central Node
清理 Central Node 伺服器磁碟
升級作為叢集安裝的 Central Node
將 Central Node 從版本 7.1 升級到版本 7.1.1 或 7.1.2
將 Central Node 從版本 7.1.1 或 7.1.2 升級至版本 7.1.3
將 Central Node 從版本 7.1.3 升級至版本 7.1.7
升級安裝在獨立伺服器上的 Sensor
還原連線到 Sensor 元件的外部儲存上的資料
升級 Kaspersky Anti Targeted Attack Platform 時保留的資訊內容與數量
在管理員選單中管理應用程式元件
Central Node 管理員選單
Sensor 管理員選單
Sandbox 管理員選單
使用 KATA 和KEDR API
將外部系統與 Kaspersky Anti Targeted Attack Platform 整合
用於掃描外部系統物件的 API
請求掃描物件
請求掃描結果
請求刪除掃描結果
請求顯示物件掃描限制

外部系統可用於接收應用程式警示資訊的 API
請求顯示警示資訊
傳輸資料的範圍
有關偵測到的物件的資料
有關偵測到的威脅的資料
有關偵測到的物件的環境資料
外部系統可用於接收應用程式事件資訊的 API
查詢事件資訊的請求
用於篩選事件的查詢語言
用於篩選事件的欄位
用於管理威脅回應操作的 API
請求取得具有 Endpoint Agent 元件的主機清單
請求有關網路隔離以及具有 Kaspersky Endpoint Agent 元件的主機是否存在阻止規則的資訊
主機網路隔離管理
請求啟用網路隔離
請求停用網路隔離
請求將排除項目新增至網路隔離規則
管理防護規則
請求建立阻止規則
請求刪除阻止規則
管理應用程式運行工作
請求獲取有關工作的資訊
請求建立工作
請求刪除工作
使用 NDR API
確保使用 Kaspersky Anti Targeted Attack Platform API 時的安全性
建立並使用 Kaspersky Anti Targeted Attack Platform API 的連線器
有關應用程式的資訊來源
聯絡技術支援服務
如何獲得技術支援
透過 Kaspersky CompanyAccount 獲得技術支援
術語表
Central Node
CSRF 攻擊
Endpoint Agent 元件
ICAP 用戶端
ICAP 資料
IOA
IOC
IOC 檔案
Kaspersky Anti Targeted Attack Platform
Kaspersky Secure Mail Gateway
Kaspersky Threat Intelligence Portal
KATA
KEDR
Kerberos 身分驗證
Keytab 檔案

KPSN 的本機信譽資料庫
MIB（管理資訊庫）
MITRE 技術
NTP 伺服器
OpenIOC
Sandbox
Sensor
SIEM 系統
SPAN
Syslog
TAA (IOA) 規則
TLS 加密
VIP 身分
YARA
YARA 規則
中間人攻擊
偵測
備用資料流
傾印
入侵偵測系統
最終使用者產品授權協議
分佈式解決方案
卡巴斯基安全網路（KSN）
卡巴斯基私有安全網路
多租戶
後門程式
惡意 Web 位址
惡意軟體防護引擎
新一代威脅
映像流量
服務主要名稱（SPN）
租戶
簽章
網路釣魚 URL 位址
警示
追蹤
通訊頻道頻寬
進階持續性威脅（APT）
針對性攻擊
針對性攻擊分析器
零時差弱點
零時差攻擊
有關協力廠商代碼的資訊
商標聲明

Kaspersky Anti Targeted Attack Platform 說明

新功能

- Kaspersky Anti Targeted Attack Platform 的新增功能 硬體和軟體需求
  - 硬體和軟體需求
  - Kaspersky Anti Targeted Attack Platform 與 Kaspersky Endpoint Security for Windows 的相容性、Linux 和 Mac

產品授權

- 授權 Kaspersky Anti Targeted Attack Platform

使用入門

- 分佈式解決方案和多租戶
- 調整 Kaspersky Anti Targeted Attack Platform 大小
- Kaspersky Anti Targeted Attack Platform 的安裝與初始配置
- 配置 Kaspersky Anti Targeted Attack Platform 與 Kaspersky Endpoint Agent 元件的整合 開始使用 Kaspersky Anti Targeted Attack Platform Web 介面
  - 應用程式 Web 介面入門 — 適用於管理員
  - 應用程式 Web 介面入門 — 適用於安全員 附加功能

- 透過 Web 介面管理 Sandbox 元件
- 透過 API 與外部系統互動 更新
  - 更新先前版本的 Kaspersky Anti Targeted Attack Platform

聯絡技術支援服務

- 如何獲得技術支援

關於 Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform（以下簡稱“該應用程式”）是一個設計用來防護企業 IT 基礎架構和及時偵測諸如*零時差攻擊*、*針對性攻擊*，以及被稱為*進階持續性威脅*（以下也稱為“*APT*”）的複雜針對性攻擊等威脅的解決方案。該解決方案是為企業使用者開發的。

Kaspersky Anti Targeted Attack Platform 包含三個功能模組：

- Kaspersky Anti Targeted Attack Platform（以下也稱為“KATA”），為企業 IT 基礎架構提供邊界安全。
- Kaspersky Endpoint Detection and Response（以下也稱為“KEDR”），為組織的區域網路提供防護。
- 網路偵測與回應（以下也稱為“NDR”），為企業 LAN 提供防護。

此解決方案可以透過以下方式接收和處理資料：

- 整合到區域網路中，接收和處理映像的 *SPAN、ERSPAN 和 RSPAN 流量*，並從 HTTP、HTTP2、FTP、SMTP、DNS、SMB 和 NFS 協定中提取物件和中繼資料。
- 透過 ICAP 協定連線到代理伺服器，接收和處理HTTP 流量、HTTP2 流量和 FTP 流量以及 HTTPS 流量（如果管理員在代理伺服器上配置了 SSL 憑證更換）的資料。
- 透過 POP3 (S) 和 SMTP 協定連線到郵件伺服器，接收和處理電子郵件訊息的副本。
- 與 Kaspersky Secure Mail Gateway 和 Kaspersky Security for Linux 郵件伺服器整合，接收並處理電子郵件的副本。
- 使用 Kaspersky SD-WAN 應用程式接收並處理從遠端位置取得的網路流量副本。此功能提高了偵測和監控網路活動的靈活性，使您能夠分析來自網路不同點的流量並採取適當的措施以確保網路安全。

  有關 Kaspersky Secure Mail Gateway、Kaspersky Security for Linux Mail Server 和 Kaspersky SD-WAN 的詳情，請參閱這些應用程式的檔案。
- 與 Kaspersky Endpoint Security 整合，並從企業 IT 基礎架構中運行 Microsoft® Windows®、Linux® 和 Mac® 作業系統的單台電腦接收資料（*事件*）。這些應用程式將持續監控在這些電腦上執行的處理程序、活動的網路連線和被修改的檔案。
- 使用 REST API 介面與外部系統整合並掃描這些系統上的檔案。

此解決方案使用以下威脅情報手段：

- 卡巴斯基安全網路（也稱為“KSN”）雲端服務的基礎架構，提供對卡巴斯基線上知識庫的存取，其中包含有關檔案、Web 資源和軟體信譽的資訊。使用來自卡巴斯基安全網路的資料可確保卡巴斯基應用程式能夠更快地回應威脅，提高某些防護元件的效能，並降低誤報的可能性。
- 與卡巴斯基私人安全網路 (KPSN) 整合，以存取卡巴斯基安全網路的信譽資料庫以及其他統計資料，而無需將資料從使用者電腦傳送到卡巴斯基安全網路。
- 與被稱為 Kaspersky Threat Intelligence Portal 的卡巴斯基資訊系統整合，該系統包含並顯示有關檔案和 URL 信譽的資訊。

- IOC（入侵指標）。Kaspersky Anti Targeted Attack Platform 使用符合 OpenIOC 標準的 IOC 檔案，該標準是描述入侵指標的開放標準。IOC 檔案包含一組與事件指標進行比較的指標。如果比較的指標匹配，應用程式將該事件視為警示。

- IOA（攻擊指標）。Kaspersky Anti Targeted Attack Platform 掃描應用程式的事件資料庫，並標記與 TAA (IOA) 規則描述的行為相符的事件或事件鏈。

此解決方案可以偵測企業 IT 基礎架構內發生的以下事件：

- 檔案已下載，或試圖將檔案下載到企業 LAN 電腦。

- 檔案已傳送至企業 LAN 上的使用者的電子郵件信箱。

- 網站連結在企業 LAN 電腦上開啟。

- 偵測到在企業 LAN 電腦的 IP 位址或網域名稱上有網路活動發生。

- 在企業 LAN 電腦上的處理程序已啟動。

應用程式可以透過以下方式向使用者提供其運行結果和威脅情報：

- 顯示在 Central Node、主 Central Node（以下簡稱"PCN"）或從屬 Central Node（以下簡稱"SCN"）伺服器的 Web 介面中完成的工作結果。

- 透過 syslog 協定向組織中已使用的 SIEM 系統發布警示。

- 透過 REST API 與外部系統整合，並根據需要將解決方案產生的警示資訊傳送到外部系統。

- 在卡巴斯基私人安全網路的本機信譽資料庫中發布有關 Sandbox 元件警示的資訊。

具有**資深安全員**或**安全官**角色的使用者可以在應用程式中執行以下操作：

- 監控解決方案的元件。

- 檢視偵測到的針對性攻擊和入侵企業 IT 基礎架構的跡象表，篩選和搜尋警示，檢視和管理每個警示，遵循建議進行評估和調查事件。

- 檢視企業 IT 基礎架構的電腦和伺服器上發生的事件表，搜尋威脅，篩選、檢視和管理每個事件，遵循建議進行評估和調查事件。

- 在安裝有 Kaspersky Endpoint Security 的電腦上執行工作：執行應用程式和停止處理程序、下載和刪除檔案、在安裝有 Kaspersky Endpoint Security 的電腦上隔離物件、將檔案副本放置在 Kaspersky Anti Targeted Attack Platform 的儲存中，從隔離區還原檔案區。

- 在安裝有 Kaspersky Endpoint Security 的選定電腦上，設定政策以防止執行他們認為不安全的檔案和處理程序。

- 將安裝有 Kaspersky Endpoint Security 的單台電腦與網路隔離。

- 管理TAA（IOA）規則以進行事件分類和分析。

- 管理使用者定義的目標攻擊分析器 TAA (IOA)、YARA、Sandbox 和入侵偵測規則：上傳應用程式用於檢查事件和建立警示的規則。

- 使用 OpenIOC 相容檔案（IOC 檔案）在具有 Endpoint Agent 元件的主機上和警示資料庫中搜尋目標攻擊、受感染和可能受感染物件的跡象。

- 從掃描中排除卡巴斯基定義的 TAA (IOA) 規則和 IDS 規則。
- 管理隔離區中的物件和儲存中物件的副本。
- 管理有關應用程式效能和警示的報告。
- 配置將有關應用程式遇到的警示和問題的通知傳送到使用者的電子郵件信箱。
- 管理 VIP 警示清單和從掃描中排除的資料清單，並填充 KPSN 的本機信譽資料庫。
- 儲存和下載原始網路流量的副本，以便在外部系統中進行分析。

具有**安全稽核員**角色的使用者可以在應用程式中執行以下操作：

- 監控解決方案的元件。
- 檢視偵測到的針對性攻擊和入侵企業 IT 基礎架構的跡象表，篩選和搜尋警示，以及檢視每個警示的資料。
- 檢視企業 IT 基礎架構的電腦和伺服器上發生的事件表，搜尋威脅，篩選並檢視每個事件。
- 檢視具有 Endpoint Agent 元件的主機清單以及所選主機的資訊。
- 檢視使用者定義的目標攻擊分析器 TAA (IOA)、YARA、Sandbox 和入侵偵測規則。
- 檢視卡巴斯基專家定義的掃描排除 TAA (IOA) 規則和 IDS 規則。
- 檢視有關應用程式效能和警示的報告。
- 檢視 VIP 警示清單以及被從掃描中排除的資料清單。
- 檢視在應用程式 Web 介面中進行的所有設定。
- 儲存和下載原始網路流量的副本，以便在外部系統中進行分析。

具有**管理員**角色的使用者可以在應用程式中執行以下操作：

- 編輯應用程式設定。
- 配置分佈式解決方案和多租戶模式的伺服器。
- 設定應用程式與其他應用程式和系統的整合。
- 管理 TLS 憑證並在 Central Node 伺服器和 Sandbox 伺服器之間、Kaspersky Anti Targeted Attack Platform 伺服器和 Endpoint Agent 元件之間以及與外部系統之間建立信任連線。
- 管理應用程式使用者的帳戶。
- 監控應用程式健康狀況。

新增功能

Kaspersky Anti Targeted Attack Platform 7.1.7 引入了以下變更：

1. 從 HTTP/2 流量中提取物件時發生的錯誤已修復。
2. 與 KPSN 4.0 整合時發生的錯誤已修復。
3. 在“**威脅搜尋**”區段顯示選定期間的資訊時發生的錯誤已修復。
4. 在從警示卡中搜尋與警示相關的所有事件時發生的資料顯示錯誤已修復。
5. 修復了 ICAP 整合錯誤並提高了穩定性。

Kaspersky Anti Targeted Attack Platform 7.1.3 引入了以下變更：

1. 修正了升級 Kaspersky Anti Targeted Attack Platform 時出現的錯誤。
2. 修復了備份和還原資料時發生的錯誤。
3. 修復了顯示“**威脅搜尋**”區段中的資訊時發生的錯誤
4. 修復了傳送 AA（總結警示）通知時發生的錯誤。

Kaspersky Anti Targeted Attack Platform 7.1.1 和 7.1.2 引入了以下變更：

1. 修復了作業系統弱點。
2. 修正了升級Kaspersky Anti Targeted Attack Platform時出現的錯誤。
3. 修復了註冊網路流量事件和相應警示時出現的錯誤。
4. 如果掃描包含多個 URL 的電子郵件訊息時產生警示，則警示包含每個 URL 的資訊。
5. 修復了下載 GosSOPKA 系統的資料時發生的錯誤。

Kaspersky Anti Targeted Attack Platform 7.1 引入了以下變更：

1. Kaspersky Anti Targeted Attack Platform 的效能得到提升
2. 改進了即時 ICAP 流量掃描：
   - 提高了請求處理速度。
   - 改進了統計資料收集。
   - 最佳化了與卡巴斯基安全網路 (KSN) 的互動。
   - 在 POST 請求 (REQMOD) 中新增了檔案掃描。
   - 新增了物件掃描請求的重複資料刪除。

- 標準即時 ICAP 流量掃描進行了以下變更：
  - 在掃描檔案時，其下載速度會降低。如果無法在指定時間內掃描檔案，則下載將以正常速度繼續。

    此功能實施後，您將無法再設定**掃描檔案**和**檔案已過期**通知頁面。
  - 多媒體檔案不包含在掃描範圍內。
- 對進階即時 ICAP 流量掃描進行了以下變更：
  - 為了最佳化工作負載，應用程式可能會暫時從進階ICAP 流量掃描模式切換到標準掃描模式。發生這種情況時，應用程式 Web 介面的**控制板**上會顯示有關切換到標準掃描模式的警告。

3. 改進了管理使用者定義的入侵偵測規則的介面。
4. 現在，您可以使用儲存區域網路 (SAN) 系統作為磁碟機，用於儲存安裝在伺服器上的 Central Node 元件的資料。
5. 現在，您可以使用ERSPAN（封裝遠端SPAN）技術接收映像流量。為此，Central Node或Sensor伺服器必須充當透過通用路由封裝(GRE)協定建立的隧道的端點。

   要在元件之間傳遞 ERSPAN 流量，您需要在 iptables 中管理 MTU 設定，將 MTU 大小設為 1900。
6. 新事件類型：**USB 裝置**。
7. 現在，您可以在威脅搜尋區段中搜尋事件時選擇**過去 7 天**時段。
8. 管理身分驗證政策的新方法：
   - 在 Central Node 或 Sandbox 元件的 Web 介面或管理主控台中追蹤失敗的身分驗證嘗試。
   - 在指定時間後，終止非活動使用者工作階段，適用於 Central Node、Sensor 或 Sandbox 元件的 Web 介面或管理主控台。
9. 將卡巴斯基的入侵偵測規則新增至排除項目時，您可以指定您希望其套用的條件。例如，您可以僅將排除項目套用到選定的主機。
10. 現在您可以將有關網路流量警示和事件（NDR 事件）的資訊上傳到 GosSOPKA 系統。
11. 日誌記錄功能已擴充：
    - Sandbox 元件的新活動日誌記錄有關使用者在 Web 介面和元件管理員選單中的操作的資訊。
    - Sensor 元件的新活動日誌記錄有關使用者在元件管理員選單中的操作的資訊。
    - 應用程式使用者活動日誌中記錄的事件清單已擴展。
    - 現在您可以配置 Central Node 元件資料庫中日誌和警示資料的保留期限，以及 Sensor 和 Sandbox 日誌的保留期限。
12. 現在，您可以限制來自 Endpoint Agent 元件的遙測量（與 KEDR 功能整合時）。

13. 應用程式的 Web 介面進行了以下變更：

- 新的本地化語言，繁體中文。
- “**執行應用程式**”工作已重新命名為“**執行應用程式**”。

14. 不再提供對 Sensor 元件的 Web 介面的存取。

Kaspersky Endpoint Security 12.9 for Windows 中的變更

您可以在 Kaspersky Endpoint Security for Windows 線上說明 中檢視 Kaspersky Endpoint Security 12.9 for Windows 中的變更清單。

Kaspersky Endpoint Security 12.2 for Linux 中的變更

您可以在Kaspersky Endpoint Security for Linux 線上說明 中檢視 Kaspersky Endpoint Security 12.2 for Linux 中的變更清單。

Kaspersky Endpoint Security 12.1 for Mac 中的變更

您可以在Kaspersky Endpoint Security for Mac 線上說明 中檢視 Kaspersky Endpoint Security 12.1 for Mac 的變更清單。

已修復問題

下表列出了在 Kaspersky Anti Targeted Attack Platform 目前版本中發現並已透過更新修復的問題資訊。

更新發布日期	更新修訂號	問題首次出現的應用程式版本	問題描述				
7.04.2026	7.1.7	7.1.3	[9403837] 修復了在"伺服器"欄位中輸入最後一個八位元組中有一個數字的 IP 位址時，"儲存"按鈕在代理連線設定中不可用的問題。				
		7.1.1	[9047903] 修正了 Kaspersky Secure Mail Gateway 的 Web 介面中顯示錯誤訊息而不是 Kaspersky Anti Targeted Attack Platform 中的物件掃描結果的問題。 [9458080] 在 SCN 到 PCN 的連線設定中新增了对 PCN IP 位址的檢查。 [9159104] 修復了某些連結的事件無法在警示卡的搜尋結果中顯示的問題。 [9109119] 修復了處理透過 HTTP2 協定接收的檔案時在"**控制板**"部分中顯示的"*檔案被 Sensor 丟棄*"錯誤。	7.1	[8971563] 修復了按日期過濾時，指定時間段內建立的事件無法顯示在搜尋結果中的問題。 [9169778] 修復了在具有嵌入式 Sensor 的 Central Node 上啟用映像 SPAN 流量接收時"**控制板**"部分中的"*使用 IDS 技術的 SPAN 流量掃描工作不正常*。"錯誤。		
						7.0	[8705844] 修復了如果電子郵件來自 Kaspersky Secure Mail Gateway 且電子郵件本文中包含 URL 位址，則因逾時而被排除在掃描範圍之外的問題。

使用 Kaspersky Threat Intelligence Portal

有關您認為可疑的檔案的其他資訊，您可以訪問卡巴斯基應用程式 Kaspersky Threat Intelligence 門戶網站，該網站分析每個檔案的惡意代碼，並顯示檔案信譽的相關資訊。

Kaspersky Threat Intelligence 應用程式的存取權限付費提供。應用程式網站上的授權要求將應用程式存取憑證安裝在您電腦上的憑證儲存中。另外，您必須擁有用於存取應用程式的使用者名稱和密碼。

有關 Kaspersky Threat Intelligence Portal 的更多詳細資訊，請造訪卡巴斯基網站。

分發套件

Kaspersky Anti Targeted Attack Platform 分發套件包含以下檔案：

- 磁碟映像（帶有 iso 副檔名的檔案），其中包括 Ubuntu® Server 22.04 作業系統以及 Sensor、Central Node 和 Sandbox 元件的安裝檔。
- Sensor、Central Node 元件的壓縮檔案（.tar.gz 檔案），用於基於 Astra Linux Special Edition 1.8.1 建立 iso 映像。
- 用於基於 Astra Linux Special Edition 1.8.1 建立 iso 映像的 Sandbox 元件的壓縮檔案（.tar.gz 檔案）。

- Sandbox 元件在其中執行檔案的作業系統的磁碟映像（.iso 檔案）。
- 用於基於 Astra Linux Special Edition 1.8.1 建立 iso 映像的實用程式（.tar 檔案）。
- 為 GosSOPKA 準備資料的實用程式 (gossopka_alert_exporter.tar.gz)。
- 基於 Ubuntu 作業系統的 Central Node 和 Sensor 元件的更新套件。
- 基於 Astra Linux 作業系統的 Central Node 和 Sensor 元件的更新套件。
- 關於 Kaspersky Anti Targeted Attack Platform 中使用的協力廠商代碼的資訊檔案。

硬體和軟體需求

安裝 Kaspersky Anti Targeted Attack Platform 的虛擬平台的軟體需求

您可以在以下虛擬平台上部署應用程式元件：

- Central Node 和 Sensor：
  - VMware ESXi™ 6.7.0 或 7.0
  - KVM
  - “Brest” 3.3 虛擬化軟體
  - “RED Virtualization” 7.3
  - zVirt Node 4.2
  - Nutanix Acropolis 作業係統 (Nutanix AOS) 7.3.1.2 和 Acropolis Hypervisor (AHV) 10.3.1.2
- Sandbox：
  - VMware ESXi™ 6.7.0 或 7.0
  - “Brest” 3.3 虛擬化軟體
  - “RED Virtualization” 7.3
  - zVirt Node 4.2

若要在 VMware ESXI 虛擬平台上部署應用程式，必須安裝 Hypervisor 的目前更新套件。

如果您想在 VMware ESXI Hypervisor 中的 Astra Linux 作業系統上部署應用程式，則需要確保您使用的伺服器硬體與 Astra Linux 作業系統相容。如需支援的伺服器硬體完整清單，請參閱 Astra Linux 開發者網站。

如需 Central Node、Sensor 和 Sandbox 的硬體需求，請參閱 規模調整指南。

在虛擬化平台上部署應用程式時，可能會有限制。我們建議在安裝應用程式之前先了解這些內容。

安裝 Endpoint Agent 元件的硬體和軟體需求

Endpoint Agent 元件的硬體和軟體需求反映了充當 Endpoint Agent 元件之應用程式的硬體和軟體需求，並於這些應用程式的說明文件中加以說明：

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

> 從此版本開始，Kaspersky Anti Targeted Attack Platform 不再支援與 Kaspersky Endpoint Agent 應用程式整合。

如果您將 Kaspersky Endpoint Agent 與先前版本的 KATA 一起使用，則需要將 Kaspersky Endpoint Agent 替換為 Kaspersky Endpoint Security for Windows。您可以在下列模式下使用 Kaspersky Endpoint Security for Windows：

- EDR 代理

  如果您之前使用過未與 EPP 應用程式整合的Kaspersky Endpoint Agent，我們建議您使用此模式。

- Light Agent

  如果您之前使用過 Kaspersky Endpoint Agent 與 Kaspersky Security for Virtualization Light Agent 的整合，我們建議您使用此模式。

有關 Kaspersky Endpoint Security for Windows 模式的更多資訊，請參閱 Kaspersky Endpoint Security for Windows 線上說明的"*應用程式的模式：標準、EDR 代理、Light Agent*"部分。

使用 Kaspersky Anti Targeted Attack Platform Web 介面的硬體和軟體需求

必須在電腦上安裝以下瀏覽器之一，才能使用 Web 介面設定和管理該應用程式：

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

使用 Web 介面的最低螢幕解析度：1366x768。

透過 ICAP 配置整合時的代理伺服器軟體要求

透過 ICAP 配置代理伺服器整合時，我們建議使用以下應用程式作為代理伺服器：

- Ideco NGFW 版本 14（內部版本 14.13.4）
- Squid 版本 5.9
- User Gate

Kaspersky Endpoint Security for Windows 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

您可以使用 Kaspersky Endpoint Security 作為 Endpoint Agent 元件。

下表列出了有關 Kaspersky Endpoint Security 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性資訊。

Kaspersky Endpoint Security for Windows 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

Kaspersky Endpoint Security 版本	相容 KATA 4.0	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
Kaspersky Endpoint Security 12.1、12.2	否	是	是	是	是	否	有限制	有限制
Kaspersky Endpoint Security 12.3、12.4	否	是	是	是	是	是	有限制	有限制
Kaspersky Endpoint Security 12.5、12.6	否	否	是	是	是	是	有限制	有限制
Kaspersky Endpoint Security 12.7	否	否	有限制	有限制	有限制	有限制	是	有限制
Kaspersky Endpoint Security 12.8、12.9	否	否	有限制	有限制	有限制	有限制	有限制	是
Kaspersky Endpoint Security 12.10、12.11	否	否	是	是	是	是	是	是

有關 Kaspersky Endpoint Security 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性限制的更多資訊，請參閱*Kaspersky Endpoint Security for Windows 版本與 Kaspersky Anti Targeted Attack Platform 版本的有限相容性*一節。

從版本 12.8 開始，Kaspersky Endpoint Security for Windows 可用作 Kaspersky Security for Virtualization 應用程式的 Light Agent for Windows 元件。有關整合的更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

Kaspersky Endpoint Security for Linux 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

您可以使用 Kaspersky Endpoint Security 作為 Endpoint Agent 元件。

下表列出了有關 Kaspersky Endpoint Security 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性資訊。

Kaspersky Endpoint Security for Linux 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

Kaspersky Endpoint Security 版本	相容 KATA 4.0	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
Kaspersky Endpoint Security 11.4	否	否	否	有限制	有限制	有限制	有限制	有限制
Kaspersky Endpoint Security 12	否	否	有限制	有限制	有限制	有限制	有限制	有限制
Kaspersky Endpoint Security 12.1	否	否	否	有限制	有限制	有限制	有限制	有限制
Kaspersky Endpoint Security 12.2、12.3	否	否	否	否	有限制	有限制	有限制	有限制

有關 Kaspersky Endpoint Security 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性限制的更多資訊，請參閱*Kaspersky Endpoint Security for Linux 版本與 Kaspersky Anti Targeted Attack Platform 版本的有限相容性*部分。

從版本 12 開始，Kaspersky Endpoint Security for Linux 可用作 Kaspersky Security for Virtualization 的 Light Agent for Linux 元件。當使用 Kaspersky Endpoint Security for Linux 作為 Light Agent for Linux 元件時，Kaspersky Endpoint Security for Linux 仍然與 Kaspersky Anti Targeted Attack Platform 整合。

有關整合的更多資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

Kaspersky Endpoint Security for Mac 與 Kaspersky Anti Targeted Attack Platform 版本的相容性

您可以使用 Kaspersky Endpoint Security for Mac 作為 Endpoint Agent 元件。

下表列出了有關 Kaspersky Endpoint Security for Mac 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性資訊。

Kaspersky Endpoint Security for Mac 與 Kaspersky Anti Targeted Attack Platform 版本的相容性

Kaspersky Endpoint Security 版本	相容 KATA 4.0	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
Kaspersky Endpoint Security 12、12.1、12.2	否	否	否	否	有限制	有限制	有限制	有限制

有關 Kaspersky Endpoint Security 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性限制的更多資訊，請參閱*Kaspersky Endpoint Security for Mac 版本與 Kaspersky Anti Targeted Attack Platform 版本的有限相容性*部分。

KUMA 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

您可以使用 KUMA 作為 SIEM 系統。

下表列出了 KUMA 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性資訊。

KUMA 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

KUMA 版本	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
KUMA 2.0	是	是	否	否	否	否	否
KUMA 2.1	否	是	是	是	否	否	否
KUMA 3.0.2	否	否	否	是	是	否	否
KUMA 3.0.3	否	否	否	是	是	否	否
KUMA 3.2	否	否	否	是	是	否	是
KUMA 3.3	否	否	否	否	否	是	否
KUMA 3.4	否	否	否	否	否	是	是

XDR 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

您可以使用 XDR 作為 SIEM 系統。

下表列出了有關 XDR 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性資訊。

XDR 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

XDR 版本	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
XDR 1.0	否	否	是	否	否	否	否
XDR 1.1	否	否	否	是	是	否	否
XDR 1.2	否	否	否	否	否	是	否
XDR 1.3	否	否	否	否	否	是	有限制

KPSN 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

您可以使用卡巴斯基私人安全網路 (KPSN) 而不是卡巴斯基安全網路 (KSN)，以避免將組織的資料傳送到公司 LAN 之外。

下表列出了 KPSN 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性資訊。

KPSN 版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性

KPSN 版本	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
KPSN 3.3	是	是	是	是	是	否	否
KPSN 3.4	否	否	否	是	是	是	是

KPSN 版本	相容 KATA 4.1	相容 KATA 5.0	相容 KATA 5.1	相容 KATA 6.0	相容 KATA 6.1	相容 KATA 7.0	相容 KATA 7.1
KPSN 3.5	否	否	否	是	是	是	是
KPSN 4.0	否	否	否	否	是	是	是

Kaspersky Anti Targeted Attack Platform 與 VK 雲端的相容性

您可以在VK Cloud 中建立的虛擬機上部署 Kaspersky Anti Targeted Attack Platform，設定如下：一個Central Node 元件（採用單一角色），並有一個或多個 KSMG 郵件 Sensor及數個沙盒與其連線。

在 VK Cloud 公有雲中建立的虛擬機上部署 Kaspersky Anti Targeted Attack Platform 時，適用以下限制：

- Central Node 必須以單一角色安裝在伺服器上。
- 僅支援基於 Astra Linux 的應用程式的認證版本。
- 支援安裝 KATA 或 KATA+NDR 授權金鑰。
- 僅支援接收及處理來自安裝在 VK Cloud 外部的 KSMG 的郵件之相關場景。其他場景不受支援。

為了使Sandbox 元件正常運作，必須滿足以下要求：

- 必須為虛擬機啟用嵌套虛擬化。
- 必須正確配置網路介面設定，以便為正在被處理的物件提供 Internet 存取。

  > 僅當可存取網際網路的網路介面配置正確時，才能啟用 Windows 映像。

- 用於對已處理物件進行 Internet 存取的網路介面必須與組織的本機網路隔離。
- 處理物件用於存取 Internet 的網路介面必須連線到與控制介面所連線的子網路不同的子網路。
- 我們建議使用外部防火牆規則，限制用於讓處理中物件存取網際網路的網路介面上的傳入連線。

限制

Kaspersky Anti Targeted Attack Platform 的已知限制

Kaspersky Anti Targeted Attack Platform 7.1.3 和 7.1.7 具有以下已知限制：

1. 將應用程式升級至 7.1.3 或 7.1.7 版本時，入侵偵測規則不會自動遷移。您需要手動新增自訂入侵偵測規則。

2. 還原資料後，自訂 YARA 和 IOC 規則會被還原到非功能狀態。

   我們建議您下載無效的規則，在 Web 介面中刪除該規則，然後重新上傳已儲存的規則。

3. 在分佈式解決方案和多組織用戶模式下還原資料後，AM 技術建立的新警示可能不會顯示在警示表中。您可以檢查該限制是否適用於您，並在必要時採取措施修復它。有關詳細資訊，請參閱"*分佈式解決方案和多租戶模式下 Central Node 伺服器的資料備份與還原*"部分。

4. Kaspersky Anti Targeted Attack Platform 能夠處理網路事件並立即產生對應的 IDS 警示，每日最多可產生 100 萬個警示。如果超過此閾值，應用程式會延遲產生警示：需要 1 小時才能趕上 10 萬個警示的延遲。

5. 為了讓 Central Node、Sensor、PCN 和 SCN 之間的連線正常運作，必須將安裝了元件的伺服器放置在同一子網路中。不支援網路位址轉換 (NAT)。此限制不適用於 Endpoint Agent 元件，這些元件可以位於與 Central Node 子網路分離的子網路中。

Kaspersky Anti Targeted Attack Platform 7.1.1 和 7.1.2 具有以下已知限制：

1. 不支援依賴系統監控 (Sysmon) 和 Windows 事件日誌以外的資料來源的 Sigma 規則。

2. 不支援相關 Sigma 規則。

3. 作為與 NDR 功能塊整合的一部分，最多 2000 個 Endpoint Agent 元件可以連線到單個 Central Node 元件。

4. 在根據掃描 Web 流量副本的結果建立的檔案警示中，如果使用者在具有基本身分驗證的代理伺服器上進行身分驗證，"**使用者名稱**"欄位為空。

5. 如果 Central Node 伺服器上的日期比目前日期晚 30 天以上，Kaspersky Anti Targeted Attack Platform 將無法運作。我們建議確保在要安裝應用程式元件的伺服器上設定目前日期。

6. 在卡巴斯基安全網路中檢查檔案的信譽時，有關受信任簽章的供應商的資訊不會記錄在日誌中。

7. Kaspersky Anti Targeted Attack Platform 可正確處理透過虛擬介面接收的 ERSPAN 流量，速率高達 2 Gbps。ERSPAN 流量速率較高會導致資料遺失。

8. Kaspersky Anti Targeted Attack Platform 能夠處理網路事件並立即產生對應的 IDS 警示，每日最多可產生 100 萬個警示。如果超過此閾值，應用程式會延遲產生警示：需要 1 小時才能趕上 10 萬個警示的延遲。

9. 為了讓 Central Node、Sensor、PCN 和 SCN 之間的連線正常運作，必須將安裝了元件的伺服器放置在同一子網路中。不支援網路位址轉換 (NAT)。此限制不適用於 Endpoint Agent 元件，這些元件可以位於與 Central Node 子網路分離的子網路中。

Kaspersky Anti Targeted Attack Platform 7.1 有以下已知限制：

1. 不支援依賴系統監控 (Sysmon) 和 Windows 事件日誌以外的資料來源的 Sigma 規則。

2. 不支援相關 Sigma 規則。

3. 作為與 NDR 功能塊整合的一部分，最多 2000 個 Endpoint Agent 元件可以連線到單個 Central Node 元件。

4. 在根據掃描 Web 流量副本的結果建立的檔案警示中，如果使用者在具有基本身分驗證的代理伺服器上進行身分驗證，"**使用者名稱**"欄位為空。

5. 如果 Central Node 伺服器上的日期比目前日期晚 30 天以上，Kaspersky Anti Targeted Attack Platform 將無法運作。我們建議確保在要安裝應用程式元件的伺服器上設定目前日期。

6. Central Node 和 Sensor 伺服器以及 PCN 和 SCN 之間的連線的每個套件的有效載荷大小（最大傳輸單元，MTU）的值為 1500。如果您知道您的 ISP 限制了解決方案元件之間的連結上的 MTU，則需要設定 MTU，以使其大小不超過您的 ISP 允許的值。

7. 在卡巴斯基安全網路中檢查檔案的信譽時，有關受信任簽章的供應商的資訊不會記錄在日誌中。

8. Kaspersky Anti Targeted Attack Platform 可正確處理透過虛擬介面接收的 ERSPAN 流量，速率高達 2 Gbps。ERSPAN 流量速率較高會導致資料遺失。

9. 如果為Targeted Attack Analyzer 元件資料庫指派了 2 TB 或更大的磁碟，則升級伺服器上安裝的 Central Node 可能會失敗，出現"升級工作"(MoveVolumesDataTask)"完成但有錯誤"的錯誤。

   解決"升級工作"(MoveVolumesDataTask)"完成但有錯誤"錯誤

   1. 透過 SSH 或終端登入要執行升級的 Central Node 伺服器的管理主控台。

   2. 在 /data/upgrade 目錄中，建立wa.sh 檔案，內容如下：

      set -e

      rsync -ah /data/storage/volumes/clickhouse/ /data/volumes/clickhouse/

      rm -rf /data/storage/volumes/clickhouse/

      docker volume rm -f kata_product_edr_synchronizer_storage_1 kata_product_agent_server_storage_1 \

      kata_product_ksn_proxy_storage_1 kata_product_prometheus_volume_1 kata_product_nta_database_storage_1 \

      kata_product_postfix_storage_1 kata_product_response_actions_processor_volume_1 kata_product_siem_proxy_storage_1 \

      kata_product_updater_storage_1 kata_product_zookeeper_data_volume_1 kata_product_clickhouse_storage_1

      sed -i 's/"current_task_index":[[:space:]]*25/"current_task_index": 26/' /data/upgrade/upgrade_config.json

      ./run_kata_upgrade.py

   3. 透過執行以下命令使指令碼可執行：

      ```
      chmod +x wa.sh
      ```

   4. 透過執行以下命令來運行指令碼：

      ```
      ./wa.sh
      ```

   升級過程將恢復。

10. 為了使安裝在 Astra Linux 伺服器上的 Central Node 元件正常工作，與應用程式 7.0.3 版本相比，需要更多可用的磁碟空間。如果 Central Node 伺服器上沒有足夠的可用空間，則升級失敗。但應用程式仍可運行。

    您可以釋放磁碟空間。有關詳細資訊，請參閱"*升級伺服器上安裝的 Central Node*"部分。

11. 為了讓 Central Node、Sensor、PCN 和 SCN 之間的連線正常運作，必須將安裝了元件的伺服器放置在同一子網路中。不支援網路位址轉換 (NAT)。此限制不適用於 Endpoint Agent 元件，這些元件可以位於與 Central Node 子網路分離的子網路中。

Kaspersky Endpoint Security 12.9 for Windows 的限制

您可以在 Kaspersky Endpoint Agent for Windows 線上說明 中檢視 Kaspersky Endpoint Agent 12.9 for Windows 的限制清單。

Kaspersky Endpoint Security 12.2 for Linux 的限制

您可以在 Kaspersky Endpoint Security for Linux 發行備註 中檢視 Kaspersky Endpoint Security 12.2 for Linux 中的限制清單。

Kaspersky Endpoint Security 12.1 for Mac 的限制

您可以在 Kaspersky Endpoint Agent for Windows 線上說明 中檢視 Kaspersky Endpoint Agent 12.1 for Mac 的限制清單。

一般限制

為確保 Kaspersky Anti Targeted Attack Platform 正常運行，必須滿足以下要求：

1. Central Node 和 Sensor 伺服器以及 PCN 和 SCN 之間的連線的每個套件的有效載荷大小（最大傳輸單元，MTU）的值為 1500。如果您知道您的 ISP 限制了解決方案元件之間的連結上的 MTU，則需要設定 MTU，以使其大小不超過您的 ISP 允許的值。

2. 不支援在命令列上變更 Central Node 伺服器的名稱。

3. 如果您想在虛擬機上安裝Endpoint Agent 元件，我們強烈建議不要透過複製包含 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的參考映像來建立此虛擬機。複製映像時，虛擬機的唯一 ID 會保持不變，這會導致 Kaspersky Anti Targeted Attack Platform 隨後將多部虛擬機識別為同一部裝置。這會使屬於KEDR 功能單元的功能無法正常運作，例如事件資料庫威脅搜尋或網路隔離。您可以在虛擬機部署完成後，在虛擬機上安裝 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux，以解決此限制。

將 Central Node 作為叢集部署

將 Central Node 元件部署為叢集時，存在以下限制：

1. 一個叢集必須至少包含 4 台伺服器：2 台儲存伺服器和 2 台處理伺服器。您可以根據 規模調整指南 擴展叢集，以增加可處理的流量或已連線電腦的數量。

2. 該叢集具有高可用性，但效能不高。在叢集中新增比規模調整指南中建議的數量多的工作伺服器並不會無限增加可接收的遙測量或可處理的流量。

3. 如果叢集中的某些伺服器發生故障，則只有至少有兩台 Docker swarm 中具有管理員角色的伺服器正常運作，才能還原叢集的功能。

4. 我們建議將具有相同硬體配置的伺服器新增至叢集中。否則，無法保證性能按比例提高。

5. 在叢集中新增額外伺服器不會加快處理掃描佇列中已有的物件。

6. 如果託管應用程式的伺服器發生故障，應用程式的 Web 介面可能會暫時無法使用。

7. 如果處理伺服器發生故障，您可能會遺失 ICAP、POP3 和 SMTP 流量資料以及等待處理的電子郵件副本以及與其關聯的偵測。

8. 如果處理伺服器設定為從 SPAN 連接埠接收鏡像流量，則當此伺服器發生故障時，不會處理 SPAN 流量。

9. Sensor 元件只能連線到叢集中的一個處理伺服器。此伺服器必須**設定為從 SPAN 連接埠接收鏡像流量**。

   您可以在安裝元件時啟用接收鏡像流量。如果您在安裝階段停用了流量接收：

   若要開啟從 SPAN 連接埠接收映像流量：

   1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。

   2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任一工作伺服器的管理主控台。

   3. 執行以下指令：

      ```
      kata-enable-span
      ```

      將啟用從 SPAN 連接埠接收映像流量。

10. 如果其中一台叢集伺服器發生故障，或該伺服器與已連線到 KEDR 功能的 Endpoint Agent 元件之間的連線暫時遺失，事件資料庫中的資料可能會暫時無法同步。

11. 如果叢集伺服器的配置被變更，來自具有連線到 KEDR 功能的 Endpoint Agent 元件的電腦的流量和事件的處理可能會暫時減慢。

12. 將 Kaspersky Anti Targeted Attack Platform 安裝為叢集或更新叢集配置時，嵌入式 Sensor 可能無法啟動。

在這種情況下，我們建議執行以下操作：

- 如果 Sensor 未連線，您必須在應用程式的 Web 介面中將其移除，然後在技術支援模式中執行**啟動 Sensor 的一系列指令**。

  1. `kata-sensor-tool reset`
  2. `kata-sensor-tool reset-core`
  3. `kata-sensor-tool init-embedded-sensor`

- 如果 Sensor 未執行，您需要在技術支援模式中執行一系列指令以**啟動 Sensor**。

  1. `kata-sensor-tool reset`
  2. `kata-sensor-tool reset-core`
  3. `kata-sensor-tool init-embedded-sensor`

過一段時間後，Sensor 會出現在 Web 介面中。

13. 在 zVirt Node、“RED 虛擬化”、KVM、VMware ESXi 虛擬平台上不支援作為叢集安裝 Kaspersky Anti Targeted Attack Platform。

Sensor 限制

Sensor 元件具有以下限制：

1. 只有安裝在獨立伺服器上的 Sensor 元件才能用來以最大10 Gbps 的速度捕捉網路流量。
2. 以 10 Gbps 的最大速度擷取FTP 流量可能會導致嚴重遺失。
3. 只能在技術支援模式下才能配置在具有 Sensor 元件的獨立伺服器上進行即時 ICAP 流量掃描。

Sandbox 限制

Sandbox 元件具有以下限制：

1. 以下作業系統版本支援自訂映像：
   - Windows 7
   - Windows 8.1 64 位元
   - Windows 10 64 位元（最高版本 1909）
2. 自訂作業系統映像完全支援以下在地化語言：俄語、英語、中文（簡體）、阿拉伯語、西班牙語（墨西哥）。

3. 不提供用於啟動作業系統和軟體的產品授權金鑰。

4. 如果 Sandbox 伺服器上未安裝 Central Node 伺服器上作業系統集合中所選擇的某些作業系統，Kaspersky Anti Targeted Attack Platform 不會將物件傳送至 Sandbox 元件進行掃描。如果具有 Sandbox 元件的多個伺服器連線到具有 Central Node 元件的伺服器，則應用程式會將物件傳送到其安裝的作業系統與 Central Node 上所選集相符的伺服器。

在虛擬化平台上部署應用程式

zVirt Node、“RED 虛擬化”、KVM、VMware ESXi

zVirt Node、“RED 虛擬化”、KVM 或 VMware ESXi 虛擬化平台不支援應用程式的高可用性部署（Central Node 叢集）。

“Brest”、“zVirt Node”、“RED Virtualization”

如果要在“Brest”虛擬平台、zVirt Node 或“RED 虛擬化”上使用 Sandbox 元件，則還必須額外配置使用該元件掃描物件的時間，以提高偵測機率。若要進行配置，請聯絡技術支援。

Nutanix

如果您使用 Nutanix 叢集，且打算在此平台上以叢集配置使用 Central Node，則 Central Node 叢集的所有伺服器都必須部署在 Nutanix 叢集的同一部主機上。這是確保封包通過內部虛擬交換機正確路由所必需的。

在分佈式解決方案和多組織用戶模式下使用應用程式

當應用程式在分佈式解決方案和多組織用戶模式下使用時，適用以下限制：

1. 在 PCN 伺服器上，**資產** → **裝置**索引標籤僅顯示已連線到該 PCN 伺服器的主機。

2. 只能在 PCN 伺服器上變更使用者帳戶密碼。

3. 斷開 SCN 與 PCN 的連線是不可逆的，不支援將 SCN 後續連線到任何 PCN 伺服器。

與 Kaspersky Endpoint Security for Windows 的相容性有限

Kaspersky Endpoint Security for Windows 版本與 Kaspersky Anti Targeted Attack Platform 版本有限的相容性

- Kaspersky Endpoint Security 12.1–12.6 與 Kaspersky Anti Targeted Attack Platform 7.0 的整合。

  Kaspersky Endpoint Security 傳送的資料範圍有限：

  - 不會傳輸有關以下事件的資訊：**DNS**、**代碼注入**、**命名管道**、**WMI**、**LDAP**。
  - 對於"**檔案修改時間**"事件，不會處理有關以下子類型的資訊：**檔案讀取**、**已建立硬連接**、**符號連接已建立**。
  - 對於"**登錄檔已修改**"事件，不會處理有關以下子類型的資訊：**登錄機碼已重命名**、**登錄機碼已儲存**。
  - "**模組已載入**"和"**到遠端主機的連線**"事件的新欄位不可用。

- Kaspersky Endpoint Security 12.1–12.6 與 Kaspersky Anti Targeted Attack Platform 7.1 的整合。

  Kaspersky Endpoint Security 傳送的資料範圍有限：

  - 不會傳輸有關以下事件的資訊：**命名管道**、**WMI**、**LDAP**、**DNS**、**代碼注入**、**USB 裝置**。
  - 對於"**檔案修改時間**"事件，不會處理有關以下子類型的資訊：**檔案讀取**、**已建立硬連接**、**符號連接已建立**。
  - 對於"**登錄檔已修改**"事件，不會處理有關以下子類型的資訊：**登錄機碼已重命名**、**登錄機碼已儲存**。
  - "**模組已載入**"和"**到遠端主機的連線**"事件的新欄位不可用。

- Kaspersky Endpoint Security 12.7 與 Kaspersky Anti Targeted Attack Platform 5.0–6.1 的整合。

  這些 Kaspersky Anti Targeted Attack Platform 版本的伺服器可以從 Kaspersky Endpoint Security 應用程式接收有限範圍的資料：

  - 不會處理有關以下事件的資訊：**命名管道**、**WMI**、**LDAP**、**DNS**、**代碼注入**。
  - 對於"**檔案修改時間**"事件，不會處理有關以下子類型的資訊：**檔案讀取**、**已建立硬連接**、**符號連接已建立**。
  - 對於"**登錄檔已修改**"事件，不會處理有關以下子類型的資訊：**登錄機碼已重命名**、**登錄機碼已儲存**。
  - "**模組已載入**"和"**到遠端主機的連線**"事件的新欄位不可用。

- Kaspersky Endpoint Security 12.7 與 Kaspersky Anti Targeted Attack Platform 7.1 的整合。

  Kaspersky Endpoint Security 傳送的資料量是有限的：有關"**USB 裝置**"事件的資訊未被處理。

- Kaspersky Endpoint Security 12.8–12.9 與 Kaspersky Anti Targeted Attack Platform 5.0–6.1 的整合。

這些 Kaspersky Anti Targeted Attack Platform 版本的伺服器可以從 Kaspersky Endpoint Security 應用程式接收有限範圍的資料：

- 不會處理有關以下事件的資訊：**命名管道**、**WMI**、**LDAP**、**DNS**、**代碼注入**、**USB 裝置**。
- 對於"**檔案修改時間**"事件，不會處理有關以下子類型的資訊：**檔案讀取**、**已建立硬連接**、**符號連接已建立**。
- 對於"**登錄檔已修改**"事件，不會處理有關以下子類型的資訊：**登錄機碼已重命名**、**登錄機碼已儲存**。
- "**模組已載入**"和"**到遠端主機的連線**"事件的新欄位不可用。

- Kaspersky Endpoint Security 12.8–12.9 與 Kaspersky Anti Targeted Attack Platform 7.0 的整合。
  此版本的 Kaspersky Anti Targeted Attack Platform 伺服器不處理"**USB 裝置**"事件的資料。

與 Kaspersky Endpoint Security for Linux 的相容性有限

Kaspersky Endpoint Security for Linux 版本與 Kaspersky Anti Targeted Attack Platform 版本有限的相容性

- Kaspersky Endpoint Security 11.4 與 Kaspersky Anti Targeted Attack Platform 5.1、6.1 的整合。
  Kaspersky Endpoint Security 傳送的資料範圍有限：
  - 不支援建立網路隔離規則。
  - 不支援建立防護規則。
  - 使用 IOC 檔案搜尋電腦上的入侵指標不受支援。
  - 僅傳輸以下類型的事件：**處理程序已啟動**、**檔案已變更**、**系統事件日誌**、**偵測**、**偵測處理結果**。
  - 僅可使用以下工作：**獲取檔案**、**執行應用程式**。
- Kaspersky Endpoint Security 12、12.1 與 Kaspersky Anti Targeted Attack Platform 5.1 的整合。
  Kaspersky Endpoint Security 傳送的資料範圍有限：
  - 不支援建立阻止規則。
  - 僅傳輸以下類型的事件：**處理程序已啟動**、**檔案已變更**、**系統事件日誌**、**偵測**、**偵測處理結果**。
  - 僅可使用以下工作：**獲取檔案**、**執行應用程式**、**刪除檔案**、**殺死處理程序**。
- Kaspersky Endpoint Security 12、12.1 與 Kaspersky Anti Targeted Attack Platform 6.0–7.1 的整合。
  Kaspersky Endpoint Security 傳送的資料範圍有限：
  - 僅傳輸以下類型的事件：**處理程序已終止**、**阻止的應用程式（阻止規則）**、**檔案已封鎖**。
  - 僅可使用以下工作：**獲取檔案**、**執行應用程式**、**刪除檔案**、**殺死處理程序**。

- Kaspersky Endpoint Security 12.2、12.3 與 Kaspersky Anti Targeted Attack Platform 6.0、6.1 的整合。
  Kaspersky Endpoint Security 傳送的資料範圍有限：
  - 僅傳輸以下類型的事件：**處理程序已終止**、**阻止的應用程式（阻止規則）**、**檔案已封鎖**。
  - 僅可使用以下工作：**獲取檔案**、**執行應用程式**、**刪除檔案**、**殺死處理程序**、**隔離檔案**、**從隔離區還原檔案**。
- Kaspersky Endpoint Security 12.2、12.3 與 Kaspersky Anti Targeted Attack Platform 7.0–7.1 的整合。
  Kaspersky Endpoint Security 傳送的資料範圍有限：
  - 僅傳輸以下類型的事件：**處理程序已終止**、**阻止的應用程式（阻止規則）**、**檔案已封鎖**、**代碼注入**、**DNS**。
  - 僅可使用以下工作：**獲取檔案**、**執行應用程式**、**刪除檔案**、**殺死處理程序**、**隔離檔案**、**從隔離區還原檔案**。

與 Kaspersky Endpoint Security for Mac 的相容性有限

Kaspersky Endpoint Security for Mac 版本與 Kaspersky Anti Targeted Attack Platform 版本有限的相容性

- Kaspersky Endpoint Security 12、12.1、12.2 與 Kaspersky Anti Targeted Attack Platform 6.0–7.1 的整合。
  Kaspersky Endpoint Security 傳送的資料範圍有限：
  - 不支援建立網路隔離規則。
  - 不支援建立防護規則。
  - 使用 IOC 檔案搜尋電腦上的入侵指標不受支援。
  - 僅傳輸以下類型的事件：**處理程序已啟動**、**處理程序已終止**、**檔案已變更**、**偵測**、**偵測處理結果**。
  - 僅可使用以下工作：**獲取檔案**、**執行應用程式**。

XDR 相容性限制

XDR 版本與 Kaspersky Anti Targeted Attack Platform 版本的有限相容性

Kaspersky Anti Targeted Attack Platform 7.1 與 XDR 1.3 整合時傳輸的資料範圍受到限制：資產資料無法傳輸。

透過 ICAP 與代理伺服器整合

透過 ICAP 與代理伺服器整合時，存在以下限制：

1. 無法配置 ICAP 與 SQUID 服務版本 5.9 或更低版本的整合。
2. 透過代理伺服器同時連線到應用程式的數量不得超過 20000 個。推薦值為 1000。

資料提供

運行 Kaspersky Anti Targeted Attack Platform 的某些元件需要卡巴斯基方的資料處理。未經 Kaspersky Anti Targeted Attack Platform 管理員的同意，元件不會傳送資料。

您可以檢視資料清單及其使用條款，以及在您的組織與卡巴斯基之間的以下協議中同意資料處理：

- 在最終使用者產品授權協議裡（例如，安裝應用程式期間）。

  根據最終使用者產品授權協議條款，您同意自動向卡巴斯基傳送在資料提供下的最終使用者產品授權協議中列出的資訊。最終使用者產品授權協議包含在應用程式分發套件中。

- 在 KSN 聲明裡（例如，安裝應用程式期間或安裝後的管理員功能表中）。

  當您參與卡巴斯基安全網路時，Kaspersky Anti Targeted Attack Platform 運行獲得的資訊會自動傳送至卡巴斯基。傳輸資料清單在 KSN 聲明中指定。Kaspersky Anti Targeted Attack Platform 使用者自主決定是否參與 KSN。KSN 聲明包含在應用程式分發套件中。

  在傳送到卡巴斯基之前，KSN 統計資料累積在託管Kaspersky Anti Targeted Attack Platform 元件的伺服器的快取中。

卡巴斯基將按照法律和卡巴斯基適用規則規定的方式防護接收到的任何資訊。資料透過加密的通訊頻道傳送。

在使用卡巴斯基私有安全網路時，卡巴斯基不會傳送關於 Kaspersky Anti Targeted Attack Platform 運作的資訊。然而，KSN 統計資料在託管Kaspersky Anti Targeted Attack Platform 元件的伺服器上的快取中的累積程度與使用卡巴斯基安全網路時的程度相同。如果具有卡巴斯基私有安全網路的伺服器位於您的組織之外，那麼累積的 KSN 統計資料可能會傳輸到超出您的組織的範圍。

卡巴斯基私有安全網路的管理員必須親自確保此資料的安全性。

應用程式的服務資料

Kaspersky Anti Targeted Attack Platform 資源不提供限制安裝 Central Node 元件的伺服器和作業系統使用者權限的功能。建議管理員根據自己的判斷使用任何系統資源來控制如何允許安裝了應用程式的伺服器和作業系統的使用者存取其他使用者的個人資料。

Kaspersky Anti Targeted Attack Platform 的服務資料資訊如下表所示。

資料類型	儲存地點和期限
• 關於使用者帳戶的資料。 • Central Node 元件的資料。 • 有關租戶的資料。 • 有關連線到安裝了 Endpoint Agent 元件的 Central Node 元件的電腦的資訊。 • 有關預設和防護規則的資料。 • 有關使用 Endpoint Agent 元件指派給電腦的工作的資訊。 • 自訂小工具佈局資料。 • 有關使用者定義的 TAA (IOA) 規則資訊。 • 有關使用者定義的 IDS 規則資訊。 • 有關使用者定義的 IOC 規則資訊。 • 有關網路隔離規則的資料。 • 有關掃描排除項目的資料。 • 關於報告和報告範本的資訊。 • 有關 Endpoint Agent 元件憑證的資訊。	如果伺服器上安裝了 Central Node 元件，則資料將無限期地儲存在託管 Central Node 元件的伺服器上的 `/data` 目錄中。當 Central Node 元件安裝在叢集上時，資料將無限期地儲存在儲存伺服器上。

資料類型	儲存地點和期限
有關 MDR、KSN、KPSN 整合的資訊。	此資訊無限期地儲存在 Central Node 伺服器的 `/data` 目錄中。
有關應用程式的產品授權金鑰或啟動碼的資訊。	
Endpoint Agent 設定。	
用於傳送通知的郵件伺服器的設定： • 伺服器的 IP 位址和連接埠。 • 憑證的指紋。 • 伺服器上授權的使用者的登入名稱和密碼雜湊。 • 用作解密金鑰的 Secret 的名稱。 • 是否正在使用加密。	
目前伺服器的名稱。	
連線到目前伺服器的伺服器位址以及用於與這些伺服器相互認證的憑證資訊。	
連線器設定： • 連線器節點的位址。 • 連線器與之互動的協力廠商系統的伺服器位址。	
有關 Secret 和 Central Node 使用者的使用者帳戶資訊的資訊。	
監控點位址。	
有關 ICAP 排除項目的資訊。	

資料類型	儲存地點和期限
Sensor 與 ICAP 整合的設定： • 狀態（啟用或停用）。 • 最大連線數。 • REQMOD 模式下的連線位址。 • RESPMOD 模式下的連線位址。 • ICAP 請求標頭，其中包含透過代理伺服器接收此請求時傳出 HTTP 請求的用戶端的 IP 位址。 • ICAP 請求標頭，其中包含透過代理伺服器接收此請求時傳出 HTTP 請求的用戶端的連接埠。 • 使用者名稱。 • ICAP 請求標頭，其中包含透過代理伺服器接收此請求時傳出 HTTP 請求的用戶端的使用者名稱。 • 是否使用了 base64 解碼。 • 操作模式。 • 掃描逾時。 • 偵測重要性。 • 檔案被封鎖時回傳給使用者的頁面。 • URL 被封鎖時傳回給使用者的頁面。 • 監聽的接口。	
用於將使用者定義的入侵偵測規則傳送到 KSN 的設定。	
有關 Kerberos 認證中使用的 Keytab 檔案的狀態和名稱的資訊。	
有關 KSMG 電子郵件掃描優先順序的資訊。	
CPU 與 RAM 負載通知設定： • CPU、硬碟和 RAM 使用率閾值。 • 統計更新間隔。	
有關用於 Sensor 和 Central Node 相互認證的憑證的資訊。	
Sensor 與 POP3 整合的設定： • POP3 伺服器的 IP 位址和連接埠。 • POP3 伺服器上授權的使用者的登入名稱和密碼雜湊。 • 用作解密金鑰的 Secret 的名稱。 • 憑證驗證政策。 • 用戶端憑證。	

資料類型	儲存地點和期限
代理伺服器設定： • 代理伺服器的 IP 位址和連接埠。 • 代理伺服器上授權的使用者的登入名稱和密碼雜湊。 • 用作解密金鑰的 Secret 的名稱。 • 代理伺服器的狀態。	
儲存伺服器設定： • 儲存大小。 • 儲存期限。	
Sandbox 伺服器的設定： • 伺服器的 IP 位址和名稱。 • 伺服器的狀態。 • 憑證的指紋。	
Sandbox 設定： • 虛擬機映像清單。 • Sandbox 同步狀態。	
安全設定： • 密碼變更和重置期限。 • 認證計數器失敗。 • 最大使用者不活動時間。 • **控制板**由於使用者不活動而處於鎖定狀態。	
Sensor 伺服器的設定：可以傳送以進行掃描的檔案的最大大小。	
SIEM 設定： • 本機和遠端更新和操作日誌的狀態。 • TLS 加密狀態。 • SIEM 伺服器位址和連接埠。 • 正在使用的網路協定。 • 向 SIEM 傳送資料的主機的 ID。 • TLS 加密憑證。	
Sensor 與 SMTP 整合的設定： • 用於相互身份認證的憑證。 • 網域名稱和子網域名稱。 • SMTP 用戶端網路和子網路。 • TLS 安全級別。 • 請求用戶端 TLS 憑證的狀態。 • SMTP 狀態。	
SNMP 連線設定： • 登入名。 • 密碼雜湊。 • 用作解密金鑰的 Secret 的名稱。 • 協定版本。 • SNMP 狀態。	

資料類型	儲存地點和期限
Sensor 與 SPAN 整合的設定： • 監聽的接口。 • 保存 HTTP 標頭的狀態。 • SPAN 狀態。 • 用戶端憑證。	
SPAN 連接埠映像流量的儲存設定： • 儲存狀態和大小。 • 正在使用的目錄。 • 最大檔案數。	
威脅搜尋設定： • 是否使用 TAA 規則掃描事件鏈。 • 正在使用的資料模型的版本。	
時區設定。	
更新設定： • 更新伺服器類型。 • 更新伺服器的自訂 URL。	此資訊無限期地儲存在 Central Node 伺服器的 `/data` 目錄中。
系統事件日誌	作業系統日誌檔案無限期地儲存在託管 Central Node 元件的伺服器上的 `/var/log` 目錄中。
包含應用程式操作資訊的日誌。	如果元件安裝在伺服器上，則日誌檔案將無限期地儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件安裝在叢集上時，資料將無限期地儲存在儲存伺服器上。
檔案掃描佇列。	如果元件安裝在伺服器上，檔案將儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件後安裝在叢集上時，資料將儲存在儲存伺服器上。資料將保留直至掃描完成。
從具有 Endpoint Agent 元件的電腦接收的檔案。	如果元件安裝在伺服器上，檔案將儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件後安裝在叢集上時，資料將儲存在儲存伺服器上。當磁碟空間已滿時，資料將被輪換。
包含YARA 和 IDS 規則（使用者定義的和來自卡巴斯基的）的檔案。	如果元件安裝在伺服器上，檔案將無限期地儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件安裝在叢集上時，資料將無限期地儲存在儲存伺服器上。
包含傳送到外部系統的偵測資料的檔案。	如果元件安裝在伺服器上，檔案將無限期地儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件安裝在叢集上時，資料將無限期地儲存在儲存伺服器上。
Sandbox 元件的工件。	如果元件安裝在伺服器上，檔案將儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件後安裝在叢集上時，資料將儲存在儲存伺服器上。當磁碟空間已滿時，資料將被輪換。
Sandbox 元件為其建立了偵測的檔案。	如果元件安裝在伺服器上，檔案將儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件後安裝在叢集上時，資料將儲存在儲存伺服器上。當磁碟空間已滿時，資料將被輪換。
用於驗證應用程式元件的憑證檔案。	檔案將無限期地儲存在託管 Central Node、PCN、SCN、Sensor 元件的伺服器或具有 Endpoint Agent 元件的電腦上的/data 目錄中。
在應用程式元件之間傳輸的加密金鑰。	檔案將無限期地儲存在託管 Central Node、PCN、SCN、Sensor 元件的伺服器或具有 Endpoint Agent 元件的電腦上的/data 目錄中。

資料類型	儲存地點和期限
SPAN 連接埠的映像流量副本。	檔案儲存在具有 Sensor 元件的伺服器上安裝的記憶體中。當磁碟空間已滿時，資料將被刪除。

資料類型	儲存地點和期限
ICAP 排除項目篩選器。	如果元件安裝在伺服器上，檔案將無限期地儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件安裝在叢集上時，資料將無限期地儲存在儲存伺服器上。
• 有關網路工作階段的資訊。 • 裝置資訊。 • 與 Endpoint Agent 元件整合時的遙測。 • 網路流量事件。 • 使用者帳戶資料。 • 有關可執行檔的資訊。 • 與已註冊事件相關的流量傾印。 • 與網路工作階段相關的流量傾印。	資料儲存在 Central Node 伺服器的/data/storage/volumes/nta_database 目錄中。當磁碟空間被填滿時，資料將被輪換。
• 使用者帳戶 ID。 • 使用者帳戶名稱。 • 使用者的網域名稱。 • 使用者帳戶角色。 • 使用者帳戶狀態。 • 使用者帳戶上次變更密碼的日期和時間。	如果元件安裝在伺服器上，檔案將無限期地儲存在託管 Central Node 元件的伺服器上的/data 目錄中。當 Central Node 元件安裝在叢集上時，資料將無限期地儲存在儲存伺服器上。
虛擬機配置資訊： • 託管 Sandbox 元件的伺服器的 IP 位址 • 虛擬機清單	

資料類型	儲存地點和期限
關於使用者帳戶的資料： • 使用者帳戶 ID。 • 使用者帳戶名稱。 • 授權使用者的電腦的名稱。	資料儲存在 Central Node 伺服器的/data/storage/volumes/nta_database 目錄中。當磁碟空間被填滿時，資料將被輪換。
網路工作階段資訊： • 網路通訊參與者的姓名。 • 網路通訊參與者的 IP 和 MAC 位址。	
有關在應用程式中註冊的裝置的資訊： • 裝置名稱。 • 裝置的 IP 和 MAC 位址。	
作為 NDR 功能的一部分與 Endpoint Agent 元件整合時儲存的資料： • 具有 Endpoint Agent 元件的電腦的 IP 和 MAC 位址。 • 具有 Endpoint Agent 元件的電腦的名稱。 • 在具有 Endpoint Agent 元件的電腦上註冊的使用者帳戶的名稱。 • 電腦正在運作的作業系統。 • 使用者代理。	
網路流量事件的資訊：裝置的 IP 和 MAC 位址。	
有關作為 NDR 功能的一部分連線的 Endpoint Agent 電腦上的可執行檔的資訊： • 檔案名稱。 • 檔案路徑。 • 檔案版本。 • 檔案的 MD5 雜湊和 SHA256 雜湊。	
與記錄的網路工作階段和事件相關的流量傾印資料： • 網路通訊參與者的姓名。 • 網路通訊參與者的 IP 和 MAC 位址。 • 裝置名稱。 • 裝置的 IP 和 MAC 位址。 • 使用者帳戶名稱。 • 使用者帳戶 ID。 • 電腦正在運作的作業系統。 • 使用者代理。 • 可執行檔的名稱。 • 可執行檔路徑。 • 可執行檔的版本。 • 可執行檔的 MD5 雜湊和 SHA256 雜湊。	
與 NDR 功能相關的使用者活動的稽核日誌。	

Central Node 和 Sensor 元件的資料

本節包含有關儲存在具有 Central Node 元件的伺服器上以及具有 Sensor 元件的伺服器上的使用者資料的以下資訊：

- 儲存資料的內容
- 儲存位置
- 儲存期限
- 使用者存取資料

Sensor 元件的流量資料

Sensor 元件的流量資料儲存在具有 Sensor 元件的伺服器上，或者如果 Sensor 和 Central Node 安裝在同一台伺服器上或部署為叢集，則儲存在帶有 Sensor 和 Central Node 元件的伺服器上。

流量資料被記錄並儲存在按順序建立的檔案中。如果出現以下情況，應用程式將停止在一個檔案中記錄資料並開始在下一個檔案中記錄資料：

- 已達到最大檔案大小（您可以設定此設定）
- 配置的時間間隔已過（您可以設定此設定）
- 流量節省服務或整個 Kaspersky Anti Targeted Attack Platform 應用程式被重新啟動

隨著流量資料累積，Kaspersky Anti Targeted Attack Platform 會篩選資料並僅保留以下資訊：

- 與使用針對性攻擊分析器技術掃描後產生的警示相關的資訊
- PCAP 檔案，其中：
  - 來源或目的 IP 位址與偵測中的 IP 位址相符。
  - 流量資料屬於偵測時間後 15 分鐘內的時間段。

篩選後的流量資料將被移至單獨部分。其餘流量資料（不符合篩選條件）將被刪除。

篩選後的流量資料被儲存在依序建立的檔案中。如果出現以下情況，應用程式將停止在一個檔案中記錄資料並開始在下一個檔案中記錄資料：

- 已達到最大檔案大小
- 設定的時間間隔已過

儲存的資料流量涵蓋過去 24 小時。較舊的資料被刪除。

偵測中的資料

Kaspersky Anti Targeted Attack Platform 資源不提供限制安裝 Central Node 元件的伺服器和作業系統使用者權限的功能。建議管理員根據自己的判斷使用任何系統資源來控制如何允許安裝了應用程式的伺服器和作業系統的使用者存取其他使用者的個人資料。

下表列出了建立偵測時可能儲存的資料的相關資訊。

資料類型	儲存地點和期限
所有偵測的以下資料儲存在伺服器上： • 偵測建立日期和時間。 • 偵測修改的日期和時間。 • 偵測到的物件的類別。 • 偵測到的檔案的名稱。 • 偵測到的檔案的類型。 • 偵測到的物件的來源。 • 偵測到的 URL。 • 偵測到的檔案的 MD5 雜湊和 SHA256 雜湊。 • 與偵測相關的警示詳細資訊中新增了使用者評論。 • 建立偵測所依據的 TAA (IOA) 規則的 ID。 • 產生偵測的電腦的 IP 位址和名稱。 • 在其上產生偵測的電腦的 ID。 • 使用者代理。 • 與偵測相關的警示被分配到的使用者帳戶。 • 檔案清單。 • 警示重要性取決於根據卡巴斯基的經驗此警示對電腦或企業區域網路可能造成的安全影響。 • 進行偵測的技術。 • 與偵測相關的警示的狀態。 • 與偵測相關的警示被指派的使用者的姓名。 • 事件 ID（使用 NDR 功能時）。 • 裝置 ID（使用 NDR 功能時）。	如果 Central Node 安裝在伺服器上，偵測資訊會儲存在 Central Node 伺服器的 /data 目錄中。如果 Central Node 作為叢集安裝，則偵測資訊會儲存在 ceph 儲存中。 當單項掃描技術產生的偵測記錄數量達到 1000000 條時，資料就會輪替。
當與偵測相關的警示被修改時，以下資訊將儲存在伺服器上： • 修改警示的使用者帳戶。 • 向其分配了警示的使用者帳戶。 • 警示修改的日期和時間。 • 警示狀態。 • 使用者評論。	
如果偵測是由掃描檔案建立的，則下列資訊可能儲存在伺服器上： • 偵測到的檔案的完整名稱。 • 偵測到的檔案的 MD5 雜湊和 SHA256 雜湊。 • 偵測到的檔案的大小。 • 有關檔案簽章的資訊。	
如果偵測是由掃描 FTP 流量建立的，則下列資訊可能儲存在伺服器上： • FTP 請求的 URI。	
如果偵測是由掃描 HTTP 流量建立的，則下列資訊可能儲存在伺服器上： • HTTP 請求的 URI。 • 請求來源的 URI。 • 使用者代理。 • 有關代理伺服器的資訊。	
如果偵測是由於入侵偵測技術的掃描而建立的，則以下資訊可能儲存在伺服器上： • 傳送資料的電腦的名稱。 • 接收資料的電腦的名稱。 • 傳送資料的電腦的 IP 位址。 • 接收資料的電腦的 IP 位址。 • 傳輸的資料。 • 資料傳輸時間。 • 從包含流量、使用者代理和方法的檔案中提取的 URL。 • 包含偵測發生處的流量的檔案。 • 基於 IDS 資料庫的物件類別。 • 用於產生偵測的自訂 IDS 規則的名稱。 • HTTP 請求主體。 • 偵測到的物件的清單。	

資料類型	儲存地點和期限
如果偵測是由於 URL 信譽技術掃描而建立的，則下列資訊可能儲存在伺服器上： • 傳送資料的電腦的名稱。 • 接收資料的電腦的名稱。 • 傳送資料的電腦的 IP 位址。 • 接收資料的電腦的 IP 位址。 • 傳輸資源的 URI。 • 有關代理伺服器的資訊。 • 電子郵件的唯一 ID。 • 郵件寄件者和收件者的電子郵件信箱（包括副本收件者和郵件的密件副本）。 • 電子郵件主旨。 • Kaspersky Anti Targeted Attack Platform 接收到郵件的日期和時間，精確到秒。 • 偵測到的物件的清單。 • 網路連線時間。 • 網路連線的 URL。 • 使用者代理。	
如果偵測是由掃描 HTTP 流量建立的，則下列資訊可能儲存在伺服器上： • 用於產生偵測的應用程式資料庫的版本。 • 偵測到的物件的類別。 • 偵測到的物件名稱。 • 偵測到的物件的 MD5 雜湊。 • 偵測到的物件的資訊。	
如果偵測是由於惡意軟體防護技術的掃描而建立的，則以下資訊可能儲存在伺服器上： • 用於產生警示的 Kaspersky Anti Targeted Attack Platform 元件的資料庫版本。 • 偵測到的物件的類別。 • 偵測到的物件的清單。 • 偵測到的物件的 MD5 雜湊。 • 有關偵測的其他資訊。	
如果偵測是因為 DNS 活動偵測建立的，則下列資訊可能儲存在伺服器上： • DNS 查詢資料。 • DNS 伺服器對查詢的回應內容。 • 查詢的主機清單。	
如果根據使用者定義的 IOC 或TAA (IOA) 規則進行掃描後建立偵測，則下列資訊可能會儲存在伺服器上： • 掃描完成的日期和時間。 • 產生偵測的電腦的 ID。 • TAA (IOA) 規則的名稱。 • IOC 檔案的名稱。 • 偵測到的物件的資訊。 • 具有 Endpoint Agent 元件的主機清單。	
如果使用 YARA 規則建立了偵測，則可以在伺服器上儲存以下資訊： • 用於產生偵測的 YARA 規則的版本。 • 偵測到的物件的類別。 • 偵測到的物件的名稱。 • 偵測到的物件的 MD5 雜湊。 • 偵測到物件的日期和時間。 • 有關警示的其他資訊。	

資料類型	儲存地點和期限
如果偵測是由掃描檔案建立的，則下列資訊可能儲存在伺服器上： • 郵件寄件者和收件者的電子郵件信箱（包括郵件副本和密件副本收件者）。 • 電子郵件主旨。 • Kaspersky Anti Targeted Attack Platform 接收到郵件的日期和時間，精確到秒。 • 郵件的所有服務標題（如果它們出現在郵件中）。	如果 Central Node 安裝在伺服器上，偵測資訊會儲存在 Central Node 伺服器的 /data 目錄中。如果 Central Node 作為叢集安裝，則偵測資訊會儲存在 ceph 儲存中。 資料將無限期儲存。
如果偵測是由重新掃描建立的，則下列資訊可能儲存在伺服器上： • 檔案名稱。	

事件中的資料

事件可能包含使用者資料。如果伺服器上安裝了 Central Node，則發生的事件的資訊將儲存在 `/data` 目錄中。如果 Central Node 作為叢集安裝，則資訊儲存在 ceph 儲存中。

當磁碟變滿時，資料會輪換。

Kaspersky Anti Targeted Attack Platform 資源不提供限制安裝 Central Node 元件的伺服器和作業系統使用者權限的功能。建議管理員根據自己的判斷使用任何系統資源來控制如何允許安裝了應用程式的伺服器和作業系統的使用者存取其他使用者的個人資料。

事件資料可以包含與以下內容相關的資訊：

- 發生事件的電腦的名稱。
- 具有 Endpoint Agent 元件的電腦的唯一 ID。
- 發生事件的使用者帳戶的名稱。
- 使用者所屬群組的名稱。
- 事件類型。
- 事件時間。
- 有關為其記錄事件的檔案的資訊：名稱、路徑、完整名稱。
- 檔案的 MD5 雜湊和 SHA256 雜湊。
- 檔案建立時間。
- 檔案修改時間。
- 檔案存取權限。
- 處理程序的環境變數。
- 命令列參數。

- 輸入到命令列中的命令文字。
- 介面卡的本機 IP 位址。
- 本機連接埠。
- 遠端主機名稱。
- 遠端主機 IP 位址。
- 遠端主機連接埠。
- 造訪過的網站的 URL 和 IP 位址，以及來自這些網站的連結。
- 網路連線協定。
- HTTP 請求方法。
- HTTP 請求標頭。
- 有關 Windows 登錄檔變數的資訊：變數的路徑、變數名稱、變數值。
- 傳送用於 AMSI 掃描的指令碼或二進位檔案的內容。
- 有關 Windows 日誌中事件的資訊：事件類型、事件類型 ID、事件 ID、記錄事件的使用者帳戶、來自 Windows 事件日誌的 XML 格式的事件完整文字。

報告中的資料

如果伺服器上安裝了 Central Node 元件，則報告資料將無限期地儲存在 `/data` 目錄中。如果 Central Node 作為叢集安裝，則資訊將無限期地儲存在 ceph 儲存中。

Kaspersky Anti Targeted Attack Platform 資源不提供限制安裝 Central Node 元件的伺服器和作業系統使用者權限的功能。建議管理員根據自己的判斷使用任何系統資源來控制如何允許安裝了應用程式的伺服器和作業系統的使用者存取其他使用者的個人資料。

報告可能包含以下資訊：

- 報告建立日期。
- 報告中涉及的時間段。
- 產生報告的使用者帳戶的 ID。
- 報告狀態。
- 產生報告的中 Central Node 元件。
- 報告文字為 HTML 代碼。
- 報告描述。

- 產生報告的範本的名稱。
- 租戶 ID。

如果使用 NDR 功能，報告可能包含以下資訊：

- 產生報告的範本的名稱。
- 報告建立日期。
- 產生報告的使用者帳戶的 ID。
- 報告文字為 HTML 代碼。

儲存和隔離區中物件的資料

如果伺服器上安裝了 Central Node 元件，則儲存區和隔離區中物件的相關資料將無限期地儲存在/data 目錄中。如果 Central Node 作為叢集安裝，則資訊將無限期地儲存在 ceph 儲存中。

Kaspersky Anti Targeted Attack Platform 資源不提供限制安裝 Central Node 元件的伺服器和作業系統使用者權限的功能。建議管理員根據自己的判斷使用任何系統資源來控制如何允許安裝了應用程式的伺服器和作業系統的使用者存取其他使用者的個人資料。

備份區和隔離區中的物件資料可能包含以下資訊：

- 物件的名稱。
- 具有 Endpoint Agent 元件的電腦上的物件路徑。
- 檔案的 MD5 雜湊和 SHA256 雜湊。
- 檔案大小。
- 隔離物件的使用者的 ID。
- 將物件置於儲存中的使用者的 ID。
- 儲存隔離物件的電腦的 IP 位址。
- 儲存隔離物件的電腦的名稱。
- 儲存中儲存隔離物件的電腦的唯一 ID。
- 產生偵測所依據的 TAA (IOA) 規則的 ID。
- 偵測到的物件的類別。
- 使用應用程式的單個模組和技術掃描的物件的結果。
- 檔案下載時間。

- 被掃描檔案及其來源的中繼資料。
- 儲存中物件的結果狀態。

Sandbox 元件資料

對於處理時間，Central Node 元件傳送的檔案主體以開放形式儲存在託管 Sandbox 元件的伺服器上。在處理過程中，伺服器管理員可以在技術支援模式下存取傳送的檔案。已掃描檔案將定時被特殊指令碼刪除。預設狀態下每 60 分鐘一次。

下表中提供了有關使用 Sandbox 元件儲存在伺服器上的資料的資訊。

儲存在具有 Sandbox 元件的伺服器上的資料

資料範圍	儲存位置	儲存期限	存取資料
掃描的檔案	`/var/opt/kaspersky/sandbox/library/`	在 Central Node 元件收到掃描結果後或直到自動刪除時，但儲存時間不超過 24 小時。	使用者存取權限由管理員使用 定義。
檔案掃描結果	• `/var/opt/kaspersky/sandbox/library/` • `/tmp/`	在 Central Node 元件收到掃描結果後或直到自動刪除時，但儲存時間不超過 24 小時。	使用者存取權限由管理員使用 定義。
工作設定	• `/var/opt/kaspersky/sandbox/library/` • Sandbox 元件資料庫	在 Central Node 元件收到掃描結果後或直到自動刪除時，但儲存在目錄 `/var/opt/kaspersky/sandbox/library/` 中的時間不超過 24 小時。 在 Sandbox 元件資料庫中最多儲存 90 天。	使用者對 `/var/opt/kaspersky/sand` 目錄的存取權限由管理員使用 定義。 資料庫中的使用者身分驗證需 啟動資料庫程序的使用者和具 使用者授予對資料庫檔案的存 僅透過加密的 IPSec 通道提供
偵錯檔案	`/var/log/kaspersky/sandbox/`	最多 21 天。	使用者存取權限由管理員使用 定義。 只有授權使用者才能對偵錯檔 有關偵錯檔案操作的資訊儲存 件日誌中。
更新來源設定	`/var/opt/kaspersky/apt-updater`	直至被修改或刪除。	使用者存取權限由管理員使用 定義。
最短密碼長度設定	`/var/opt/kaspersky/apt-config-ram-common/validator.conf`	直至被修改或刪除。	使用者存取權限由管理員使用 定義。
虛擬機	`/vm`	直至被修改或刪除。	使用者存取權限由管理員使用 定義。
下載 iso 格式的作業系統和應用程式映像	`/var/opt/kaspersky/sandbox/custom_images/iso`	直至被修改或刪除。	使用者存取權限由管理員使用 定義。

應用程式元件之間傳輸的資料

Central Node 和 Endpoint Agent 元件

用作 Endpoint Agent 元件的應用程式向 Central Node 元件傳送以下內容：工作完成報告、安裝了這些應用程式的電腦上發生的事件和警示的資訊、有關終端工作階段的資訊。

如果沒有與 Central Node 元件的連線，所有待定資訊將會累積起來，直到被傳送至 Central Node 元件，或直到被用作 Endpoint Agent 的應用程式被從電腦移除為止，但不會超過 21 天。

所有事件的一般資訊

如果使用者電腦上發生事件，則應用程式會向事件資料庫傳送以下資料：

- 事件類型。
- 事件時間。
- 事件 ID。
- 事件架構的版本。
- 事件被 Central Node 伺服器處理的時間。
- 為其產生事件的使用者帳戶。
- 發生事件的主機的名稱。
- 主機的 IP 位址。
- 主機上安裝的作業系統類型。
- 作業係統系列。
- 作業係統名稱。
- 作業係統版本。
- Endpoint Agent 角色中使用的應用程式用於連線 Central Node 或 Sensor 伺服器的網路介面卡的 IP 位址。
- 充當 Endpoint Agent 元件角色的應用程式的版本。
- KBD 資料庫最後更新的日期。

- SW 資料庫最後更新的日期。
- 索引日期。
- 根據 TAA (IOA) 規則標記事件時，將傳輸以下資訊：
  - 觸發的攻擊指標的 ID。
  - 觸發的攻擊指標的決定。
  - 觸發的攻擊指標的來源。
  - 觸發的攻擊指標的版本。
  - MITRE 技術代碼。
  - MITRE 戰術代碼。
  - 警示重要性取決於根據卡巴斯基的經驗此警示對電腦或企業區域網路可能造成的安全影響。
  - 偵測的置信度（取決於規則引起誤報的可能性）：

Central Node 和 Kaspersky Endpoint Security for Windows

如果使用者電腦上發生事件，則應用程式會向事件資料庫傳送以下資料：

1. 檔案修改事件。
   - 有關建立檔案的處理程序的資訊：處理程序檔案名稱、處理程序檔案的 MD5 雜湊和 SHA256 雜湊。
   - 有關建立或修改的檔案的資訊：名稱、路徑、完整名稱、類型、MD5 雜湊、SHA256 雜湊、建立日期、修改日期、屬性、屬性修改日期、大小、區域 ID、檔案的應用程式名稱、供應商、頒發數位憑證的組織名稱、描述、數位簽章驗證結果、數位簽章的時間、原始名稱、修改前的名稱、修改前的路徑、修改前的完整名稱。
   - 有關建立連結的檔案的資訊：MD5 雜湊、SHA256 雜湊、建立日期、修改日期、屬性、屬性修改日期、大小、類型、區域 ID、檔案的應用程式名稱、原始名稱、頒發數位憑證的組織名稱、描述、簽章的主旨、數位簽章驗證結果、數位簽章的時間、連結檔案的完整名稱。
2. 登錄檔監控事件。
   - 有關修改了登錄檔的處理程序的資訊：處理程序ID、處理程序檔案名稱、處理程序檔案的 MD5 雜湊和 SHA256 雜湊。
   - 登錄機碼路徑。
   - 登錄檔值名稱。
   - 登錄檔值資料。
   - 登錄檔值類型。

- 以前的登錄機碼路徑。
- 以前的登錄檔值資料。
- 以前的登錄檔值類型。
- 登錄檔操作的類型。
- 儲存登錄機碼的檔案的路徑。

3. 驅動程式載入事件。

- 檔案名稱。
- 原始檔案名稱。
- 檔案路徑。
- 檔案完整名稱。
- 檔案的 MD5 雜湊和 SHA256 雜湊。
- 檔案大小。
- 檔案建立和修改日期。
- 檔案屬性修改日期。
- 檔案大小。
- 檔案類型。
- 檔案屬性。
- 檔案區域 ID。
- 檔案供應商。
- 檔案描述。
- 核發數位憑證的組織名稱。
- 簽章主旨。
- 數位簽章驗證結果。
- 數位簽章的時間。
- 從其檢索檔案的 URL。
- 從中檢索檔案的訊息的中繼資料。

4. 監聽埠開放事件。

- 有關開放監聽連接埠的處理程序的詳細資訊：處理程序檔案名稱和處理程序檔案的 MD5 雜湊和 SHA256 雜湊。
- 連接埠號。
- 介面卡 IP 位址。
- 運行狀態。

5. 遠端連線事件。

- 本機的資訊：IP 位址、連接埠號。
- 有關遠端電腦的資訊：IP 位址、連接埠號、FQDN。
- 有關連線的 TLS 加密的資訊：協定版本、SNI、加密的 SNI、憑證檔案的 MD5 雜湊、憑證檔案的 SHA1 雜湊、憑證授權人名稱、憑證序號、憑證驗證結果、憑證到期日、Ja3、Ja3s、Ja3 的 MD5 雜湊、Ja3s 的 MD5 雜湊類型、套接字類型。
- LANA 號碼。
- HTTP 方法。
- 所跟蹤的 URL。
- 處理程序狀態。
- 連線方向。

6. DNS 尋找事件。

- DNS 伺服器的 IPv4 位址。
- 正在執行的 DNS 查詢的二進位遮罩。
- DNS 回應錯誤代碼。
- DNS 查詢類型 ID。
- 要解析 DNS 記錄的網域名稱。
- DNS 回應的日期。

7. LDAP 事件。

- 搜尋範圍。
- 搜尋查詢篩選器。
- 查詢中指定為要傳回的屬性。
- 要搜尋的 LDAP容器的路徑。

8. 處理程序啟動事件。

   有關父處理程序和祖處理程序、載入器處理程序、建立者處理程序、正在運行的處理程序的檔案的資訊：名稱、路徑、完整名稱、MD5 雜湊、SHA256 雜湊、建立日期和時間、修改日期和時間、屬性、屬性修改日期和時間、大小、區域 ID、供應商、頒發數位憑證的組織名稱、描述、原始名稱、數位簽章主旨、數位簽章驗證結果、數位簽章的日期和時間、檔案版本、登入類型、登入工作階段 ID、使用者帳戶類型、使用者名稱、使用者帳戶 ID、登入電腦的 IP 位址、完整性等級、處理程序 ID、目前目錄。

9. 處理程序停止事件。

   - 有關處理程序的檔案的資訊：檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊、檔案大小以及處理程序結束時間。
   - 處理程序的唯一 ID。
   - 處理程序啟動選項。
   - 有關父處理程序的資訊：檔案路徑、UniquePID、MD5 和 SHA256 雜湊、命令列選項。

10. 處理程序存取事件。

    - 操作類型。
    - 處理程序存取權限。
    - 呼叫堆疊。
    - 有關接收方處理程序的檔案以及複製句柄的處理程序的檔案的資訊：名稱、路徑、完整路徑、MD5 和 SHA256 雜湊、建立日期和時間、修改日期和時間、屬性修改日期和時間、大小、唯一 ID、系統 ID、命令列選項、從中擷取檔案的網址、從中擷取檔案的訊息的中繼資料。

11. 模組載入事件。

    - 有關載入模組的檔案的詳細資訊：UniquePID、檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊以及檔案大小。
    - DLL 名稱。
    - DLL 的路徑。
    - DLL 完整名稱。
    - DLL 的 MD5 雜湊或 SHA256 雜湊。
    - DLL 大小。
    - DLL 屬性。
    - DLL 區域 ID。
    - DLL 應用程式名稱。
    - 原始 DLL 名稱。
    - DLL 建立和修改日期。

- 頒發 DLL 數位憑證的組織名稱。
- DLL 數位簽章驗證結果。
- DLL 數位簽章日期。
- 替換 DLL 的路徑。
- DLL 檔案類型。
- 從其檢索檔案的 URL。
- 從中檢索檔案的訊息的中繼資料。
- .NET 組合語言名稱。
- .NET 組合語言標誌。
- .NET 模組標誌。

12. 處理程序啟動阻止事件。

- 有關嘗試運行的檔案的詳細資訊：檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊、檔案大小以及檔案建立和修改日期。
- 命令列參數。

13. 檔案啟動阻止事件。

- 有關正在開啟的檔案的資訊：檔案名稱、檔案路徑、完整檔案名稱、MD5 雜湊、SHA256 雜湊、觸發封鎖的總和檢查碼類型（MD5 為0，SHA256 為!=0，不用於搜尋）、下載執行檔的網站 URL、附加下載的檔案的訊息的中繼資料。
- 有關可執行檔案的詳細資訊：檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊、檔案大小以及檔案建立和修改日期。
- 有關父處理程序的詳細資訊：檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊以及 UniquePID。

14. 命名管道開啟並連線的事件。

- 建立或連線到命名管道的程序的檔案名稱。
- 管道操作類型。

15. 威脅偵測事件和偵測處理結果。

- 偵測到的物件的名稱。
- 偵測到的物件的 MD5 雜湊。
- 偵測到的物件的 SHA256 雜湊。
- 偵測物件的類型。

- 掃描結果。
- 應用程式資料庫中記錄的 ID。
- 用於產生偵測的應用程式資料庫的版本。
- 物件處理模式。
- 偵測到的物件的類別（例如，病毒的名稱）。
- 協議。
- 本機的 IPv4 或 IPv6 位址。
- 本機連接埠號。
- 遠端電腦的 IPv4 或 IPv6 位址。
- 遠端連接埠號。
- 從其檢索檔案的 URL。
- 寄件者的電子郵件信箱（如果檔案是從電子郵件中取得的）。
- 檔案載入器的完整名稱、MD5 雜湊、SHA256 雜湊。
- 處理程序的唯一 ID。
- Windows工作管理員中顯示的處理程序 PID。
- 處理程序啟動命令列。
- 處理物件時出錯的原因。
- 使用 AMSI 掃描的指令碼內容和類型。

16. USB 裝置操作事件：

- 裝置操作類型。
- 已連線裝置的類型。
- 已連線裝置的 ID。
- 已連線裝置的名稱。
- 已連線裝置的路徑。
- 已連線裝置是否為系統碟。

17. WMI 服務啟動事件。

- 操作類型。
- WMI 服務的遠端啟動標誌。

- 啟動 WMI 服務的電腦的名稱。
- 啟動 WMI 服務的使用者的名稱。
- WMI 命名空間。
- 事件消費者篩選器名稱。
- 建立的事件消費者的名稱。
- 事件消費者原始碼。

18. AMSI 掃描事件。

- 使用 AMSI 掃描的指令碼內容。
- 傳送掃描的指令碼的內容類型。
- 傳送掃描的指令碼的名稱。
- 指令碼檔案的 MD5 雜湊。
- 指令碼檔案的 SHA256 雜湊。

19. 代碼注入事件。

- 有關接收方程序的資訊：應用程式名稱、應用程式完整名稱、應用程式路徑、檔案的 MD5 雜湊值、檔案的 SHA256 雜湊值、下載檔案的 URL、附加下載的檔案的訊息的中繼資料、應用程式的唯一 ID、應用程式的系統 ID、命令列、處理程序 DLL 的名稱、處理程序 DLL 的路徑、處理程序在位址空間中的位址。
- 注入方法。
- 修改的處理程序的命令列。
- 系統調用參數。
- 攔截注入相關函數時的 API 呼叫堆疊。

20. 解釋檔案運行事件。

    有關解釋檔案的資訊：名稱、路徑、完整名稱、MD5、SHA256、檔案建立日期和時間、檔案修改日期和時間、大小、類型、屬性、屬性修改日期和時間、原始名稱、描述、區域 ID、頒發數位憑證的組織名稱、數位簽章驗證的結果、數位簽章的日期和時間、數位簽章的主旨、獲取檔案的 URL、附加下載的檔案的訊息的中繼資訊。

21. 作業系統日誌中的事件。

- 事件時間、發生事件的主機和使用者帳戶名稱。
- 事件 ID。
- 通道/日誌名稱。
- 日誌中的事件 ID。
- 提供者名稱。

- 認證事件子類型。
- 網域名稱。
- 遠端 IP 位址。

- 事件標題欄位：ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer。

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

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

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

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

Central Node 和 Kaspersky Endpoint Security for Linux

如果使用者電腦上發生事件，則應用程式會向事件資料庫傳送以下資料：

1. 檔案修改事件。

   - 有關建立檔案的處理程序的資訊：處理程序檔案名稱、處理程序檔案的 MD5 雜湊和 SHA256 雜湊。
   - 有關建立或修改的檔案的資訊：名稱、路徑、完整名稱、類型、MD5 雜湊、SHA256 雜湊、建立日期、修改日期、屬性、屬性修改日期、大小、區域 ID、檔案的應用程式名稱、供應商、頒發數位憑證的組織名稱、描述、數位簽章驗證結果、數位簽章的時間、原始名稱、修改前的名稱、修改前的路徑、修改前的完整名稱。
   - 有關建立連結的檔案的資訊：MD5 雜湊、SHA256 雜湊、建立日期、修改日期、屬性、屬性修改日期、大小、類型、區域 ID、檔案的應用程式名稱、原始名稱、頒發數位憑證的組織名稱、描述、簽章的主旨、數位簽章驗證結果、數位簽章的時間、連結檔案的完整名稱。
   - 檔案類型。
   - 所有者 ID。
   - 所有者群組 ID。
   - 所有者使用者名稱。
   - 所有者群組名稱。
   - 從其檢索檔案的 URL。
   - 從中檢索檔案的訊息的中繼資料。
   - 請求的存取標誌。
   - 重啟後檔案刪除的指示。
   - 檔案存取標誌。

2. 作業系統日誌中的事件。

   - 事件時間。
   - 事件類型。
   - 活動名稱。

- 操作結果。
- 有關父處理程序的資訊：檔案路徑、處理程序檔案的 UniquePID、MD5 或 SHA256 雜湊、用於啟動處理程序的命令。

3. 處理程序啟動事件。

   有關父處理程序和祖處理程序、載入器處理程序、建立者處理程序、正在運行的處理程序的檔案的資訊：名稱、路徑、完整名稱、MD5 雜湊、SHA256 雜湊、建立日期和時間、修改日期和時間、屬性、屬性修改日期和時間、大小、區域 ID、供應商、頒發數位憑證的組織名稱、描述、原始名稱、數位簽章主旨、數位簽章驗證結果、數位簽章的日期和時間、檔案版本、登入類型、登入工作階段 ID、使用者帳戶類型、使用者名稱、使用者帳戶 ID、登入電腦的 IP 位址、完整性等級、處理程序ID、目前目錄、擁有者 ID、擁有者群組 ID、擁有者使用者名稱、擁有者群組名稱、真實使用者名稱、真實群組名稱、有效群組名稱、有效使用者名稱、檔案存取權限標誌、下載檔案的 URL、取得檔案的訊息的中繼資料、流程環境變數、命令列選項、處理程序類型。

4. 處理程序停止事件。

   - 有關處理程序的檔案的資訊：檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊、檔案大小以及處理程序結束時間。
   - UniquePID。
   - 處理程序啟動選項。
   - 有關父處理程序的資訊：檔案路徑、處理程序檔案的 UniquePID、MD5 或 SHA256 雜湊值、處理程序啟動選項。

5. 偵測事件及其處理結果。

   - 掃描結果。
   - 偵測到的物件的名稱。
   - 應用程式資料庫中記錄的 ID。
   - 用於產生偵測的應用程式資料庫的發佈時間。
   - 物件處理模式。
   - 偵測到的物件的類別（例如，病毒的名稱）。
   - 偵測到的物件的 MD5 雜湊。
   - 偵測到的物件的 SHA256 雜湊。
   - 處理程序的唯一 ID。
   - 處理程序的 PID。
   - 處理程序啟動命令列。
   - 處理物件時出錯的原因。

6. DNS 尋找事件。

- DNS 伺服器的 IPv4 位址。
- 正在執行的 DNS 查詢的二進位遮罩。
- DNS 回應錯誤代碼。
- DNS 查詢類型 ID。
- 要解析 DNS 記錄的網域名稱。
- DNS 回應的日期。

7. 代碼注入事件。

- 有關接收方程序的資訊：應用程式名稱、應用程式完整名稱、應用程式路徑、檔案的 MD5 雜湊值、檔案的 SHA256 雜湊值、下載檔案的 URL、附加下載的檔案的訊息的中繼資料、應用程式的唯一 ID、應用程式的系統 ID、命令列、處理程序 DLL 的名稱、處理程序 DLL 的路徑、處理程序在位址空間中的位址。
- 注入方法。
- 修改的處理程序的命令列。
- 系統調用參數。
- 攔截注入相關函數時的 API 呼叫堆疊。

Central Node 和 Kaspersky Endpoint Security for Mac

如果使用者電腦上發生事件，則應用程式會向事件資料庫傳送以下資料：

1. 檔案建立事件。

- 有關建立檔案的處理程序的資訊：處理程序檔案名稱、處理程序檔案的 MD5 雜湊和 SHA256 雜湊。
- 檔案名稱。
- 檔案路徑。
- 檔案完整名稱。
- 檔案類型。
- 檔案的 MD5 雜湊和 SHA256 雜湊。
- 檔案建立和修改日期。
- 檔案大小。

2. 處理程序啟動事件。

   有關父處理程序和祖處理程序、載入器處理程序、建立者處理程序、正在運行的處理程序的檔案的資訊：名稱、路徑、完整名稱、MD5 雜湊、SHA256 雜湊、建立日期和時間、修改日期和時間、屬性、屬性修改日期和時間、大小、區域 ID、供應商、頒發數位憑證的組織名稱、描述、原始名稱、數位簽章主旨、數位簽章驗證結果、數位簽章的日期和時間、檔案版本、登入類型、登入工作階段 ID、使用者帳戶類型、使用者名稱、使用者帳戶 ID、登入電腦的 IP 位址、完整性等級、處理程序ID、目前目錄、擁有者 ID、擁有者群組 ID、擁有者使用者名稱、擁有者群組名稱、真實使用者名稱、真實群組名稱、有效群組名稱、有效使用者名稱、檔案存取權限標誌、下載檔案的 URL、取得檔案的訊息的中繼資料、流程環境變數、命令列選項、處理程序類型。

3. 處理程序停止事件。

   - 有關處理程序的檔案的資訊：檔案名稱、檔案路徑、檔案完整名稱、檔案的 MD5 雜湊和 SHA256 雜湊、檔案大小以及處理程序結束時間。
   - UniquePID。
   - 處理程序啟動選項。
   - 有關父處理程序的資訊：檔案路徑、處理程序檔案的 UniquePID、MD5 或 SHA256 雜湊值、處理程序啟動選項。

4. 威脅偵測事件和偵測處理結果。

   - 掃描結果。
   - 偵測到的物件的名稱。
   - 應用程式資料庫中記錄的 ID。
   - 用於產生偵測的應用程式資料庫的發佈時間。
   - 物件處理模式。
   - 偵測到的物件的類別（例如，病毒的名稱）。
   - 偵測到的物件的 MD5 雜湊。
   - 偵測到的物件的 SHA256 雜湊。
   - 處理程序的唯一 ID。
   - 處理程序的 PID。
   - 處理程序啟動命令列。
   - 處理物件時出錯的原因。

Central Node 和 Sandbox

Central Node 元件傳送檔案給Sandbox 元件以及從網路和郵件流量擷取的 URL。在傳送前，檔案不會做任何形式的改變。Sandbox 元件將掃描結果傳送至 Central Node 元件。

Central Node 和 Sensor

該應用程式可以在 Central Node 和 Sensor 元件之間傳輸以下資料：

- 檔案和電子郵件。
- 入侵偵測系統和 URL信譽技術產生的警示資料。
- 產品授權資訊。
- 被從掃描中排除的資料清單。
- 如果配置了代理伺服器整合，則作為 Endpoint Agent 元件的應用程式的資料。
- 如果已配置從 Central Node 元件接收資料庫更新，則為應用程式資料庫。

具有 PCN 和 SCN 角色的伺服器

如果應用程式在分佈式解決方案模式下執行，則在 PCN 和連線的 SCN 之間傳輸以下相關資料：

- 警示。
- 事件。
- 工作資料。
- 政策資料。
- 使用 IOC、TAA (IOA)、IDS、YARA 使用者規則進行的掃描。
- 儲存中的檔案資料。
- 關於使用者帳戶的資料。
- 關於產品授權。
- 具有 Endpoint Agent 元件的電腦清單。
- 放在儲存中的物件。
- 在具有 Endpoint Agent 元件的電腦上被隔離的物件。
- 附加到警示的檔案。
- IOC 和 YARA 檔案。

應用程式偵錯檔案中包含的資料

Kaspersky Anti Targeted Attack Platform 資源不提供限制安裝 Central Node 元件的伺服器和作業系統使用者權限的功能。建議管理員根據自己的判斷使用任何系統資源來控制如何允許安裝了應用程式的伺服器和作業系統的使用者存取其他使用者的個人資料。

偵錯檔案可包括使用者的任何個人資料或組織的機密資料。檔案無限期地儲存在 `/var/log/kaspersky` 目錄中。

Kaspersky Endpoint Security for Windows 資料

有關 Kaspersky Endpoint Security 傳輸的資料的詳細資訊，請參閱應用程式的線上說明：

- 根據最終使用者產品授權協議提供資料。
- 使用卡巴斯基安全網路時提供資料。
- 遵守歐洲聯盟法律 (GDPR)。
- 使用“偵測與回應” → “Kaspersky Anti Targeted Attack Platform (EDR)”解決方案時的提供資料。

Kaspersky Endpoint Security for Linux 資料

有關 Kaspersky Endpoint Security 傳輸的資料的詳細資訊，請參閱應用程式的線上說明。

Kaspersky Endpoint Security for Mac 資料

有關 Kaspersky Endpoint Security 傳輸的資料的詳細資訊，請參閱應用程式的線上說明。

應用程式產品授權

本節介紹 Kaspersky Anti Targeted Attack Platform 授權的主要方面。

關於最終使用者產品授權協議

*最終使用者產品授權協議 (EULA)*是使用者與 AO Kaspersky Lab 之間的綁定協議，其規定了使用者使用該應用程式的條款。

在開始使用應用程式之前，請仔細閱讀最終使用者產品授權協議的條款。

您可以透過以下方式檢視最終使用者產品授權協議(EULA) 的條款：

- 安裝 Kaspersky Anti Targeted Attack Platform 的過程中。
- 透過閱讀名稱為/EULA/License.<language>的文字。
  此檔案包含在應用程式分發套件中。
- 在應用程式 Web 介面的**設定**部分中，於**產品授權**子部分點擊**產品授權協議**按鈕。
- 在 Sandbox 元件的 Web 介面中，於ⓘ功能表中點擊**最終使用者產品授權協議**連結。

在安裝應用程式時確認您同意最終使用者產品授權協議，即表示您接受最終使用者產品授權協議(EULA) 的條款。如果您不接受最終使用者產品授權協議的條款，則必須中止應用程式安裝並且不得使用該應用程式。

關於產品授權憑證

*產品授權憑證*是隨金鑰檔案或啟動碼提供的文件。

產品授權憑證包含以下產品授權資訊：

- 產品授權 ID 或訂單號碼。
- 產品授權持有人的詳細資料。
- 有關可以使用產品授權啟動的應用程式的資訊。
- 產品授權裝置（可根據產品授權使用該應用程式的裝置）數量限制。
- 產品授權開始日期。
- 產品授權到期日期或產品授權有效期。
- 產品授權類型。

關於產品授權

*產品授權*是根據最終使用者產品授權協議(EULA) 的條款和條件授予的使用 Kaspersky Anti Targeted Attack Platform 的有限時間權利。

服務範圍和應用程式使用條款取決於用於啟動該應用程式的產品授權的類型。

Kaspersky Anti Targeted Attack Platform 提供以下幾種產品授權類型：

- NFR（不得轉售）是固定期限內的免費產品授權，旨在讓使用者熟悉應用程式並執行測試部署。
- 正式版 — 購買應用程式時提供的付費產品授權。

產品授權到期後，應用程式將繼續工作，但功能有限。您必須購買正式版產品授權或續約正式版產品授權才能使用該應用程式的所有功能。

我們建議您最遲在產品授權到期日之前續約產品授權，以免中斷您的裝置對電腦安全威脅的防護。

更新功能（包括病毒防護簽章更新和代碼庫更新）可能無法在美國境內使用。

在目前版本的 Kaspersky Anti Targeted Attack Platform 中，應用程式的可用功能也取決於新增的產品授權金鑰的類型。

關於產品授權金鑰

*產品授權金鑰*是根據最終使用者產品授權協議來啟動並使用應用程式的一串序列。產品授權金鑰由卡巴斯基產生。

您可以透過套用*金鑰檔案*或輸入*啟動碼*來為應用程式新增產品授權金鑰。將產品授權金鑰新增到應用程式後，它將作為唯一的字母數字序列顯示在應用程式介面中。

卡巴斯基可以阻止違反最終使用者產品授權協議的產品授權金鑰。如果產品授權金鑰已被封鎖，您必須新增不同的產品授權金鑰才能使用該應用程式。

在目前版本的 Kaspersky Anti Targeted Attack Platform 中，應用程式的可用功能取決於新增的產品授權金鑰的類型：

- **KATA+NDR 和 KEDR 產品授權金鑰**。應用程式的完整功能。
- **KEDR 產品授權金鑰**。接收和處理來自網路流量和郵件流量的資料有限制。
- **KATA+NDR 產品授權金鑰**。Web 介面部分**威脅搜尋**、**工作**、**阻止**、**自訂規則**、**儲存**和**資產**的功能受限。
- **KATA 產品授權金鑰**。Web 介面的**威脅搜尋**、**工作**、**阻止**、**自訂規則**、**儲存**、**資產**部分的功能受到限制，**SPAN 流量處理**部分中的儲存和下載網路流量功能受到限制。

關於金鑰檔案

*金鑰檔案*是您從卡巴斯基接收的帶有.key 副檔名的檔案。金鑰檔案旨在透過新增產品授權金鑰來啟動應用程式。

金鑰檔案將會傳送至您在購買 Kaspersky Anti Targeted Attack Platform 或訂購具有 NFR 產品授權類型的 Kaspersky Anti Targeted Attack Platform 後指定的電子郵件地址。

您無需連線到卡巴斯基啟動伺服器即可透過金鑰檔案啟動應用程式。

如果您不小心刪除了金鑰檔案您可以將其還原。您可能需要金鑰檔案才能註冊 Kaspersky CompanyAccount。

若要還原金鑰檔案，您必須執行下列操作之一：

- 聯絡您購買產品授權的供應商。
- 在卡巴斯基網站上使用您的啟動碼取得金鑰檔案。

關於啟動碼

*啟動碼*是二十個拉丁字元和數字的唯一序列。您輸入啟動碼來新增啟動 Kaspersky Anti Targeted Attack Platform 的產品授權金鑰。啟動碼將會傳送至您在購買 Kaspersky Anti Targeted Attack Platform 或訂購具有 NFR 產品授權類型的 Kaspersky Anti Targeted Attack Platform 後指定的電子郵件地址。

要使用啟動碼啟動應用程式，您需要存取網際網路以連線到卡巴斯基啟動伺服器。

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

關於訂購

*Kaspersky Anti Targeted Attack Platform 訂購*是在所選參數（訂購到期日期、受防護裝置數量）下使用解決方案的訂單。

訂購是有限制的（例如一年）。若要在有限訂購到期後繼續使用 Kaspersky Anti Targeted Attack Platform，您必須續約訂購。如果沒有續約，Kaspersky Anti Targeted Attack Platform 將繼續以有限功能模式運作。

若要在訂購下使用 Kaspersky Anti Targeted Attack Platform，您必須輸入啟動碼。應用啟動碼後，將新增一個產品授權金鑰，該金鑰決定了在訂購下使用該應用程式的產品授權。有關產品授權金鑰的資訊顯示在 Central Node 伺服器的 Web 介面上。

透過訂購購買的啟動碼不能用於啟動 Kaspersky Anti Targeted Attack Platform 的先前版本。

新增產品授權金鑰

在分佈式解決方案模式下，只能在 PCN 伺服器上替代金鑰。

您可以透過以下方式之一將產品授權金鑰新增至 Kaspersky Anti Targeted Attack Platform：

- 輸入啟動碼。
- 上傳金鑰檔案。

若要使用啟動碼將產品授權金鑰新增至 Kaspersky Anti Targeted Attack Platform：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**產品授權**子部分。
2. 在您想要啟動的以下功能塊部分，點擊**輸入啟動碼**：KATA/NDR 或 KEDR。
   這將開啟啟動視窗。
3. 在該欄位中，輸入傳送到您提供的電子郵件信箱的啟動碼。
4. 仔細閱讀卡巴斯基安全網路聲明並選擇以下選項之一：
   - **我同意參與 KSN**，如果您接受 KSN 聲明的條款並希望參與 KSN。
   - **我不同意參與 KSN**，如果您不接受 KSN 聲明的條款並且不想參與 KSN。

     如果您不同意聲明條款，將不會啟用卡巴斯基安全網路。
5. 點擊**套用**。

產品授權金鑰被新增到應用程式中。

若要使用金鑰檔案將產品授權金鑰新增至 Kaspersky Anti Targeted Attack Platform：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**產品授權**子部分。
2. 在您想要啟動的以下功能塊部分，點擊**上傳金鑰檔案**：KATA/NDR 或 KEDR。
   這將開啟啟動視窗。
3. 點擊**上傳**。
   這將開啟檔案選擇視窗。
4. 選擇要下載的金鑰檔案，然後點擊**開啟**按鈕。
   這將關閉檔案選擇視窗。

5. 仔細閱讀卡巴斯基安全網路聲明並選擇以下選項之一：

- **我同意參與 KSN**，如果您接受 KSN 聲明的條款並希望參與 KSN。
- **我不同意參與 KSN**，如果您不接受 KSN 聲明的條款並且不想參與 KSN。

> 如果您不同意聲明條款，將不會啟用卡巴斯基安全網路。

6. 點擊**套用**。

產品授權金鑰被新增到應用程式中。

替代產品授權金鑰

> 在分佈式解決方案模式下，只能在 PCN 伺服器上替代金鑰。

您可以透過以下方式之一將 Kaspersky Anti Targeted Attack Platform 的產品授權金鑰替換為不同的產品授權金鑰：

- 用啟動碼替代。
- 用金鑰檔案替代。

透過輸入啟動碼來替代 Kaspersky Anti Targeted Attack Platform 的目前產品授權金鑰：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**產品授權**子部分。
2. 在您想要啟動的以下功能塊部分，點擊**替代**：KATA/NDR 或 KEDR。在顯示的下拉清單中，選擇**使用啟動碼替代**。

   這將開啟產品授權金鑰替代視窗。
3. 在該欄位中，輸入傳送到您提供的電子郵件信箱的啟動碼。
4. 仔細閱讀卡巴斯基安全網路聲明並選擇以下選項之一：

   - **我同意參與 KSN**，如果您接受 KSN 聲明的條款並希望參與 KSN。
   - **我不同意參與 KSN**，如果您不接受 KSN 聲明的條款並且不想參與 KSN。

   > 如果您不同意聲明條款，將不會啟用卡巴斯基安全網路。

5. 點擊**套用**。

產品授權金鑰已替代。

若要使用金鑰檔案將產品授權金鑰新增至 Kaspersky Anti Targeted Attack Platform：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**產品授權**子部分。
2. 在您想要啟動的以下功能塊部分，點擊**替代**：KATA/NDR 或 KEDR。在顯示的下拉清單中，選擇**使用金鑰檔案替代**。

   這將開啟產品授權金鑰替代視窗。
3. 點擊**上傳**。

   這將開啟檔案選擇視窗。
4. 選擇要下載的金鑰檔案，然後點擊**開啟**按鈕。

   這將關閉檔案選擇視窗。
5. 仔細閱讀卡巴斯基安全網路聲明並選擇以下選項之一：
   - **我同意參與 KSN**，如果您接受 KSN 聲明的條款並希望參與 KSN。
   - **我不同意參與 KSN**，如果您不接受 KSN 聲明的條款並且不想參與 KSN。

     如果您不同意聲明條款，將不會啟用卡巴斯基安全網路。
6. 點擊**套用**。

產品授權金鑰已替代。

刪除產品授權金鑰

在分佈式解決方案模式下，只能在 PCN 伺服器上移除產品授權金鑰。

您可以刪除已新增至 Kaspersky Anti Targeted Attack Platform 的產品授權金鑰。刪除產品授權金鑰後，應用程式將進入受限功能模式。

若要移除產品授權金鑰：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**產品授權**子部分。
2. 在您要刪除其產品授權金鑰的以下功能區塊部分中，點擊**刪除**：KATA/NDR 或 KEDR。

   這將開啟產品授權金鑰刪除確認視窗。
3. 點擊**是**。

   金鑰移除確認視窗關閉。

產品授權金鑰已刪除。

在 Central Node 的 Web 介面中檢視有關新增的產品授權金鑰的資訊

在分佈式解決方案和多組織用戶模式下，您可以在管理員或應用程式 Web 介面使用者的帳戶下，在 PCN 伺服器和所有連線的 SCN 的 Web 介面中檢視有關產品授權和新增的金鑰的資訊。

要檢視有關新增的產品授權金鑰的資訊，

在 Central Node 伺服器的 Web 介面中，選擇**設定**部分，**產品授權**子部分。

Web 介面將顯示有關 KATA/NDR 產品授權金鑰的以下資訊：

- **序號**。
- **功能集合**。
- **啟動日期**。
- **到期日期**。
- **剩餘天數**。

Web 介面將顯示有關 KEDR 產品授權金鑰的以下資訊：

- **序號**。
- **啟動日期**。
- **到期日期**。
- **剩餘天數**。

在產品授權到期的 30 天內，**控制板**部分顯示有關續約產品授權的通知。對於所有使用者，無論其角色如何，該通知都將顯示在具有 Central Node 元件的所有伺服器上（在分佈式解決方案和多租戶模式下— 在 PCN 和所有連線的 SCN 上）。

在 Central Node 的 Web 介面中檢視最終使用者產品授權協議的文字

在分佈式解決方案和多組織用戶模式下，您可以在本機管理員、管理員或應用程式 Web 介面使用者帳戶下的 PCN 伺服器和所有已連線的 SCN 的 Web 介面中檢視最終使用者產品授權協議的文字。

若要檢視最終使用者產品授權協議的文字，請在託管 Central Node 元件的伺服器的 Web 介面中執行以下步驟：

1. 選擇**設定**部分的**產品授權**子部分。
2. 點擊工作區右上角的**產品授權協議**按鈕。

3. 在開啟的視窗中，仔細閱讀最終使用者產品授權協議的文字。

4. 完成後，點擊**關閉**按鈕。

在 Central Node 的 Web 介面中檢視隱私權政策文字

在分佈式解決方案和多組織用戶模式下，您可以在本機管理員、管理員或應用程式 Web 介面使用者帳戶下的 PCN 伺服器和所有已連線 SCN 的 Web 介面中檢視隱私權政策文字。

若要檢視隱私權政策的文字，請在託管 Central Node 元件的伺服器的 Web 介面中執行下列步驟：

1. 選擇**設定**部分的**產品授權**子部分。

2. 點擊工作區右上角的**隱私權政策**按鈕。

3. 在開啟的視窗中，仔細閱讀隱私權政策的文字。

4. 完成後，點擊**關閉**按鈕。

檢視應用程式中使用的協力廠商代碼的資訊

在分佈式解決方案和多租戶模式下，您可以在本機管理員、管理員或應用程式 Web 使用者帳戶下的 PCN 伺服器和所有連線的 SCN 的 Web 介面中檢視 Kaspersky Anti Targeted Attack Platform 中使用的協力廠商代碼的資訊。

若要檢視有關協力廠商代碼的資訊，請在託管 Central Node 元件的伺服器的 Web 介面中執行以下步驟：

1. 選擇**設定**部分的**產品授權**子部分。

2. 點擊工作區右上角的**協力廠商代碼**按鈕。

3. 在開啟的視窗中，檢視協力廠商代碼的資訊。

4. 完成後，點擊**關閉**按鈕。

在 Sandbox 的 Web 介面中檢視最終使用者產品授權協議的文字

要在 Sandbox Web 介面中檢視最終使用者產品授權協議的文字：

1. 使用您在安裝 Sandbox 元件期間指定的帳戶憑證登入 Sandbox Web 介面。

2. 點擊應用程式 Web 介面視窗底部帶有您的使用者名稱的連結。

3. 在開啟的清單中，選擇**關於**。

4. 這將開啟一個視窗；在該視窗中，點擊**最終使用者產品授權協議**連接。

5. 仔細閱讀最終使用者產品授權協議文字。

6. 完成後，點擊×按鈕。

檢視 Endpoint Agent 元件的最終使用者產品授權協議文字

您可以檢視被用作 Endpoint Agent 元件的應用程式的最終使用者產品授權協議文字。有關如何檢視最終使用者產品授權協議文字的詳細資訊，請參閱相關應用程式的線上說明。

關於 Kaspersky Endpoint Security for Windows 最終使用者產品授權協議

關於 Kaspersky Endpoint Security for Linux 最終使用者產品授權協議

關於 Kaspersky Endpoint Security for Mac 最終使用者產品授權協議

基於產品授權的應用程式模式

Kaspersky Anti Targeted Attack Platform 依據新增的產品授權金鑰提供不同的操作模式。

未授權

安裝應用程式並啟動 Web 介面後，應用程式將在此模式下執行，直到您新增產品授權金鑰。

未授權模式具有以下限制：

- 應用程式資料庫未更新。
- 沒有與卡巴斯基安全網路知識庫的連線。
- 接收和處理來自網路流量和郵件流量的資料有限制。
- Web 介面部分**威脅搜尋**、**工作**、**阻止**、**自訂規則**、**儲存**和**資產**的功能受限。

商業的

若要切換至商業模式，您必須替代產品授權金鑰或為商業產品授權新增新的產品授權金鑰。

在此模式下，應用程式：

- 更新資料庫。
- 連線到卡巴斯基安全網路知識庫。

Kaspersky Anti Targeted Attack Platform 目前版本中未授權模式的其他限制的刪除取決於所新增的產品授權金鑰的類型：

- **KATA+NDR 和 KEDR 產品授權金鑰**。應用程式的完整功能。
- **KEDR 產品授權金鑰**。接收和處理來自網路流量和郵件流量的資料有限制。
- **KATA+NDR 產品授權金鑰**。Web 介面部分**威脅搜尋**、**工作**、**阻止**、**自訂規則**、**儲存**和**資產**的功能受限。
- **KATA 產品授權金鑰**。Web 介面的**威脅搜尋**、**工作**、**阻止**、**自訂規則**、**儲存**、**資產**部分的功能受到限制，**SPAN 流量處理**部分中的儲存和下載網路流量功能受到限制。

應用程式架構

應用程式包含以下主要元件：

- *Sensor*。接收和掃描資料，在 Endpoint Agent 和 Central Node 之間交換資料時，也可以用作代理伺服器。
- *Central Node*。接收和掃描資料、分析物件的行為，並將分析結果發佈到應用程式的 Web 介面上。
- *Sandbox*。啟動作業系統的虛擬映像。在這些作業系統中啟動檔案並追蹤每個作業系統中檔案的行為，以偵測惡意活動以及針對企業 IT 基礎架構的針對性攻擊的跡象。
- *Endpoint Agent*。安裝在組織 IT 基礎架構中的工作站和伺服器上。持續監控在這些電腦上執行的處理程序、活動的網路連線和被修改的檔案。

Sensor 元件

此元件可以與 Central Node（嵌入式 Sensor）部署在同一台伺服器上，也可以部署在獨立的伺服器上。

Kaspersky Anti Targeted Attack Platform 的以下模組在每一台 Sensor 伺服器上執行：

- *Sensor*。從網路和郵件流量接收資料，並將資料傳送到具有 Central Node 元件的伺服器進行處理。
- *入侵偵測系統*（以下也稱為 *IDS*）。掃描 Internet 流量是否有入侵企業 IT 基礎架構的跡象。
- *KSN*。代表 Kaspersky Anti Targeted Attack Platform 檢查在卡巴斯基安全網路知識庫中的檔案和 URL 位址的信譽，並提供有關網站類別的資訊（例如，惡意網站、釣魚網站）。

  卡巴斯基安全網路（以下也稱為 *"KSN"*）是一個線上服務的基礎架構，提供對卡巴斯基線上知識庫的存取，該知識庫中包含了有關檔案信譽、網站資源和軟體的資訊。使用來自卡巴斯基安全網路的資料可確保卡巴斯基應用程式能夠更快地回應威脅，提高某些防護元件的效能，並降低誤報的可能性。

  如果您不想參與 KSN，可以使用*卡巴斯基私人安全網路*（以下也稱為 *KPSN*）。KPSN 是一個允許使用者存取卡巴斯基安全網路的信譽資料庫和其他統計資料，而不從他們自己的電腦實際傳送資料到卡巴斯基安全網路的解決方案。

- *URL 信譽*。偵測惡意和釣魚 URL 位址，以及過去駭客在針對性攻擊和入侵企業 IT 基礎架構時使用的 URL 位址。

Sensor 也可用作來自 Endpoint Agent 元件之傳出連線的代理伺服器。

Central Node 元件

此元件可部署在一台伺服器上或部署為一個高可用性叢集，該叢集含 2 個角色：儲存伺服器和處理伺服器。

高可用性透過儲存伺服器之間的資料複製和計算資源冗餘來實現：如果一台伺服器發生故障，其功能將由另一台具有相同角色的伺服器執行。同時，Kaspersky Anti Targeted Attack Platform 繼續工作。

叢集中僅允許一台伺服器發生故障。如果多台伺服器發生故障，叢集將無法運作。

以下應用程式模組、核心和技術在具有 Central Node 元件的每個伺服器或叢集上運行：

- *惡意軟體防護引擎*（以下也稱為*AM*或*AM 引擎*）。使用防毒資料庫掃描檔案和物件以尋找企業 IT 基礎架構中的病毒和其他威脅。
- *移動攻擊分析器*（也稱為*MAA*）。使用機器學習技術掃描雲端基礎架構中 APK 格式的可執行檔。掃描的結果是，Kaspersky Anti Targeted Attack Platform 會收到有關偵測到的威脅或不存在威脅的資訊。
- *YARA*。使用由 Kaspersky Anti Targeted Attack Platform 使用者建立的 YARA 規則資料庫掃描檔案和物件，以發現對企業 IT 基礎架構的針對性攻擊的跡象。
- *針對性攻擊分析器*（以下也稱為*TAA*或*TA 分析器*）。使用 TAA (IOA) 規則分析並監控公司 LAN 電腦上安裝的軟體的網路活動。搜尋 Kaspersky Anti Targeted Attack Platform 的使用者應注意的網路活動的跡象，以及對企業 IT 基礎架構的針對性攻擊的跡象。
- *KSN*。代表 Kaspersky Anti Targeted Attack Platform 檢查在卡巴斯基安全網路知識庫中的檔案和 URL 位址的信譽，並提供有關網站類別的資訊（例如，惡意網站、釣魚網站）。

Sandbox 元件

託管 Sandbox 元件的伺服器運行具有作業系統映像的虛擬機。

Sandbox 元件在這些作業系統中啟動物件，並分析物件的行為以偵測惡意活動以及對企業 IT 基礎架構的針對性攻擊的跡象。

檔案掃描中涉及的特殊注意事項

在 Sandbox 中掃描檔案時，有以下特殊注意事項：

- Sandbox 元件每天能在佇列中掃描的最大物件數量為 20000。達到上限時，應用程式會刪除排隊等待掃描時間最久物件的 10%，並用排隊等待掃描的新物件替代它們。被刪除的物件儲存在應用程式中，狀態為 NOT_SCANNED。
- 從一個壓縮檔案傳送的物件總數不得超過 20 個。
- 將掃描嵌套等級低至 3 級（包括 3 級）的檔案。

Endpoint Agent 元件

軟體元件。

對於 KEDR 功能，可以用以下應用程式來表示：

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

對於 NDR 功能，可以用以下應用程式來表示：

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

應用程式安裝在組織 IT 基礎架構中的工作站和伺服器（以下也稱為“電腦”）上。在這些電腦上，應用程式將持續監控處理程序、活動網路連線和正在修改的檔案，並將該監控資料傳送到 Central Node 伺服器。

用於安裝應用程式的電腦必須滿足硬體和軟體要求。

應用程式的工作原理

Kaspersky Anti Targeted Attack Platform 應用程式包括三個功能塊：

- Kaspersky Anti Targeted Attack（以下也稱為“KATA”），它偵測企業 IT 基礎架構邊界上的威脅。
- Kaspersky Endpoint Detection and Response（以下也稱為“KEDR”），為組織的區域網路提供防護。
- Network Detection and Response（以下也稱為“NDR”），為企業 LAN 提供防護。

您可以使用應用程式的全部功能（KATA + NDR 金鑰和 KEDR 金鑰）或部分功能（僅 KATA/KATA + NDR 金鑰或僅 KEDR 金鑰）。

Kaspersky Anti Targeted Attack 的工作原理

Kaspersky Anti Targeted Attack 包括以下主要元件：

- Sensor。
- Central Node。
- Sandbox。

Sensor、Central Node 和 Sandbox 互動操作如下：

- Sensor 元件接收映像的 SPAN、ERSPAN、RSPAN 流量、HTTP、FTP、SMTP 和 DNS 協定的物件和中繼資料、HTTP 和 FTP 流量資料以及 HTTPS 流量資料（如果管理員已在代理伺服器上設定 SSL 憑證替代）、電子郵件的副本，並對獲取的資料執行以下操作：
  - 使用入侵偵測系統技術（以下也稱為 IDS）掃描Internet 流量以尋找對企業 IT 基礎架構的入侵跡象。

    IDS 技術可以識別和偵測 80 個協定（特別是 TCP/IP 模型的 53 個應用層協定）中的網路活動，從而偵測可疑流量和網路攻擊。支援的協定包括 TCP、UDP、FTP、TFTP、SSH、SMTP、SMB、CIF、SSL、HTTP、HTTP/2、HTTPS、TLS、ICMPv4、ICMPv6、IPv4、IPv6、IRC、LDAP、NFS、DNS、RDP、DERPC、MS-RPC、Socket 等。
  - 根據卡巴斯基安全網路資料庫（以下也稱為“KSN”）或卡巴斯基私人安全網路（以下也稱為“KPSN”）檢查檔案和 URL 的信譽。
  - 傳送要由 Central Node 元件掃描的物件和檔案。

  您也可以使用*郵件感應器*作為 Sensor 元件，它是安裝了 Kaspersky Secure Mail Gateway (KSMG) 或 Kaspersky Security for Linux Mail Server (KLMS) 的伺服器或虛擬機。

- Central Node 元件使用防毒資料庫、Kaspersky Anti Targeted Attack 使用者建立的 YARA 規則資料庫掃描檔案和物件，並在必要時傳送要由 Sandbox 元件掃描的檔案和物件。

- Sandbox 元件分析虛擬作業系統中物件的行為，以偵測惡意活動和對企業 IT 基礎架構的有針對性的攻擊跡象，並將掃描結果傳送至 Central Node 伺服器。

如果偵測到任何威脅，Central Node 伺服器會在警示資料庫中記錄相關資訊。您可以應用程式 Web 介面的**警示**部分或透過產生警示報告來檢視警示表。

警示資訊也可以發佈到組織中使用的 SIEM 系統以及外部系統。有關 Sandbox 元件警示的資訊可以發佈在卡巴斯基私人安全網路的本機信譽資料庫中。

Network Detection and Response 的工作原理

Network Detection and Response 包括以下元件：

- Sensor。

- Central Node。

- 連線到 NDR 功能單元的 Endpoint Agent。

  此元件可由下列任一應用程式代表：Kaspersky Endpoint Agent for Windows、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux。

- Sandbox。

  可選元件。

使用此功能單元時，Sensor、Central Node 和Sandbox 元件之間的互動方式與使用 Kaspersky Anti Targeted Attack 功能單元時相同。您可以在本部分內容前面找到此類互動的詳細描述。

Endpoint Agent 和 Central Node 元件互操作下：

作為 Endpoint Agent 元件的應用程式之一，安裝在組織 IT 基礎架構中的獨立電腦上，並接收已安裝該元件的裝置的下列資訊：

- 由於 EPP 技術觸發而記錄在事件資料庫中的有關 NDR 事件的資訊（工作站和伺服器防護事件）。

- 裝置資訊（例如，作業系統版本、型號或供應商資訊）。

- 有關網路互動圖上裝置連線的資訊。

- 有關用於建立裝置間連線的協定的資訊。

Kaspersky Endpoint Detection and Response 的工作原理

Kaspersky Endpoint Detection and Response 包括以下元件：

- Central Node。
- Endpoint Agent。

  此元件可由下列任一應用程式代表：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。
- Sandbox。

  可選元件。

> Sensor 元件可用作 Kaspersky Endpoint Agent 傳出連線的代理伺服器。

Endpoint Agent 和 Central Node 元件互操作下：

代表 Endpoint Agent 元件的應用程式之一安裝在企業 IT 基礎架構內的單個電腦上，持續監視處理程序、開放的網路連線和正在修改的檔案。監控資料被傳送到 Central Node 伺服器。事件根據這些資料產生。

- Kaspersky Endpoint Security for Windows 會將以下事件的資料傳送至 Central Node 伺服器：**處理程序已啟動**、**處理程序已終止**、**模組已載入**、**到遠端主機的連線**、**阻止的應用程式（阻止規則）**、**檔案已封鎖**、**檔案已變更**、**系統事件日誌**、**登錄檔已修改**、**監聽的連接埠**、**驅動程式已載入**、**處理程序：解釋檔案執行**、**處理程序：主控台互動式輸入**、**偵測**、**偵測處理結果**、**AMSI 掃描**、**DNS**、**代碼注入**、**命名管道**、**WMI**、**LDAP**。
- Kaspersky Endpoint Security for Linux 會將以下事件的資料傳送至 Central Node 伺服器：**處理程序已啟動**、**處理程序已終止**、**阻止的應用程式（阻止規則）**、**檔案已封鎖**、**檔案已變更**、**系統事件日誌**、**偵測**、**偵測處理結果**、**代碼注入**、**DNS**。
- Kaspersky Endpoint Security for Mac 將以下事件的資料傳輸到 Central Node 伺服器：**處理程序已啟動**、**處理程序已終止**、**檔案已變更**、**偵測**、**偵測處理結果**。

> NDR 功能的 Endpoint Agent 單獨連線，並且不會將觀察資訊傳送到 Central Node 伺服器。

到達 Central Node 伺服器的事件由 TAA (IOA) 規則標記。由於此標記，可以為需要使用者註意的事件產生警示。如果您有 Sandbox 元件，您也可以自動從 Endpoint Agent 主機傳送檔案，以便 Sandbox 元件根據 Kaspersky TAA (IOA) 規則進行掃描。

當 Central Node 伺服器與 Kaspersky Endpoint Security for Windows 整合時，您可以執行下列操作來對偵測到的威脅做出反應：

- 在 Kaspersky Endpoint Agent 主機上執行下列工作來管理檔案和應用程式：**殺死處理程序**、**進行取證**、**啟動 YARA 掃描**、**執行應用程式**、**獲取檔案**、**刪除檔案**、**隔離檔案**、**從隔離區還原檔案**、**管理服務**、**獲取磁碟鏡像**、**獲取記憶體傾印**。
- 配置政策以封鎖檔案和處理程序在選定主機上執行。
- 將單個主機與網路隔離。
- 使用 TAA (IOA) 規則對事件進行分類和分析。

- 使用 OpenIOC 相容檔案（IOC 檔案）來搜尋主機上和警示資料庫中的針對性攻擊、受感染和可能受感染物件的跡象。

- 使用 API 執行威脅回應操作。

當 Central Node 伺服器與 Kaspersky Endpoint Security 11.4 for Linux 和 Kaspersky Endpoint Security for Mac 整合時，您可以執行下列操作來回應偵測到的威脅：

- 透過運行**獲取檔案**、**執行應用程式**工作管理檔案和應用程式。

- 使用 TAA (IOA) 規則對事件進行分類和分析。

- 使用 API 執行下列威脅回應操作：管理應用程式執行工作。

當 Central Node 伺服器與 Kaspersky Endpoint Security 12 for Linux 整合時，您可以執行下列操作來對偵測到的威脅做出反應：

- 透過運行**獲取檔案**、**執行應用程式**、**刪除檔案**、**殺死處理程序**工作管理檔案和應用程式。

- 將單個主機與網路隔離。

- 使用 OpenIOC 相容檔案（IOC 檔案）來搜尋主機上和警示資料庫中的針對性攻擊、受感染和可能受感染物件的跡象。

- 使用 API 執行下列威脅回應操作：主機網路隔離管理、管理應用程式執行工作。

當 Central Node 伺服器與 Kaspersky Endpoint Security 12.2 for Linux 整合時，您可以執行下列操作來對偵測到的威脅做出反應：

- 透過執行以下工作管理檔案和應用程式：**獲取檔案**、**執行應用程式**、**刪除檔案**、**殺死處理程序**、**隔離檔案**、**從隔離區還原檔案**。

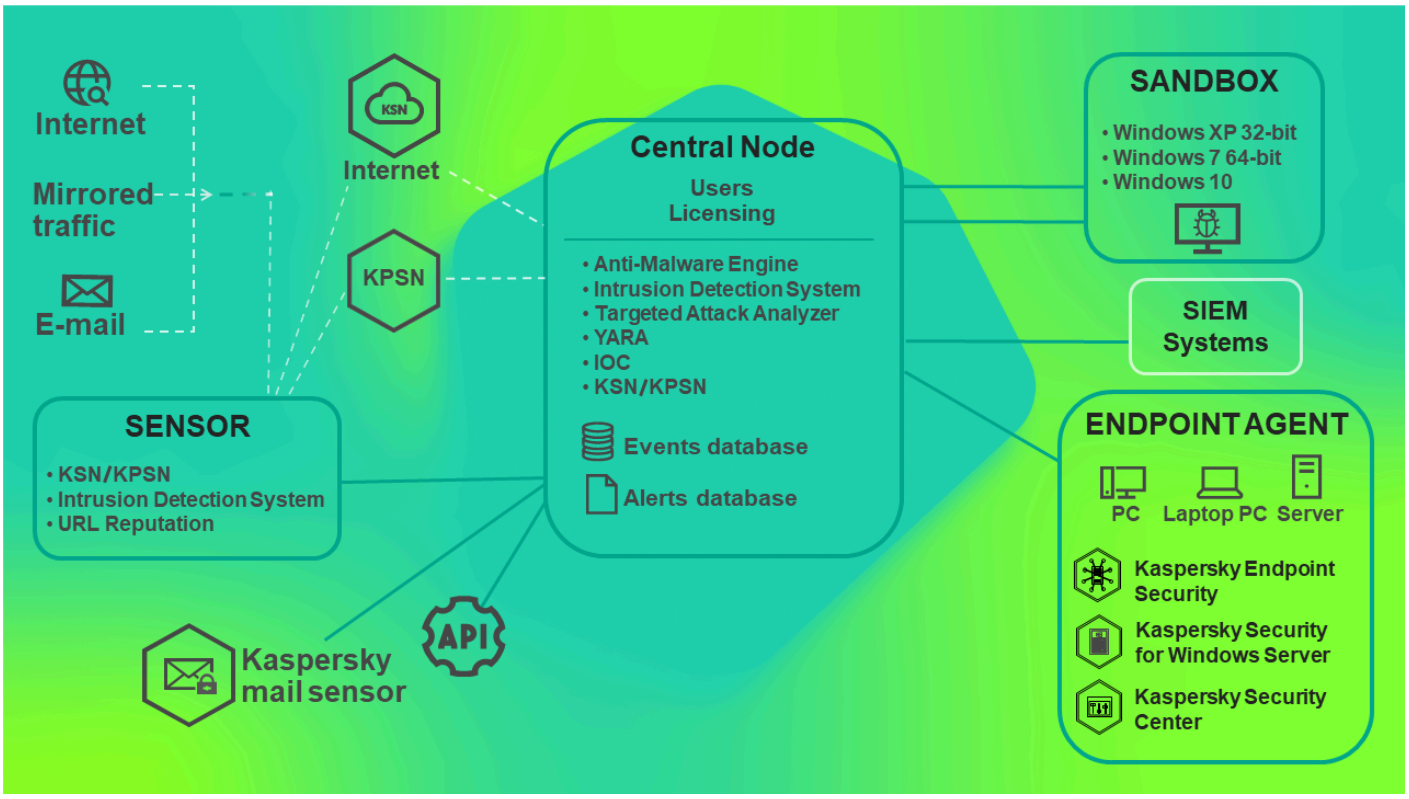
- 配置政策以封鎖檔案和處理程序在選定主機上執行。

- 將單個主機與網路隔離。

- 使用 OpenIOC 相容檔案（IOC 檔案）來搜尋主機上和警示資料庫中的針對性攻擊、受感染和可能受感染物件的跡象。

- 使用 API 執行下列威脅回應操作：主機網路隔離管理、管理應用程式執行工作、管理阻止規則。

Kaspersky Anti Targeted Attack Platform 的工作原理如下圖所示。

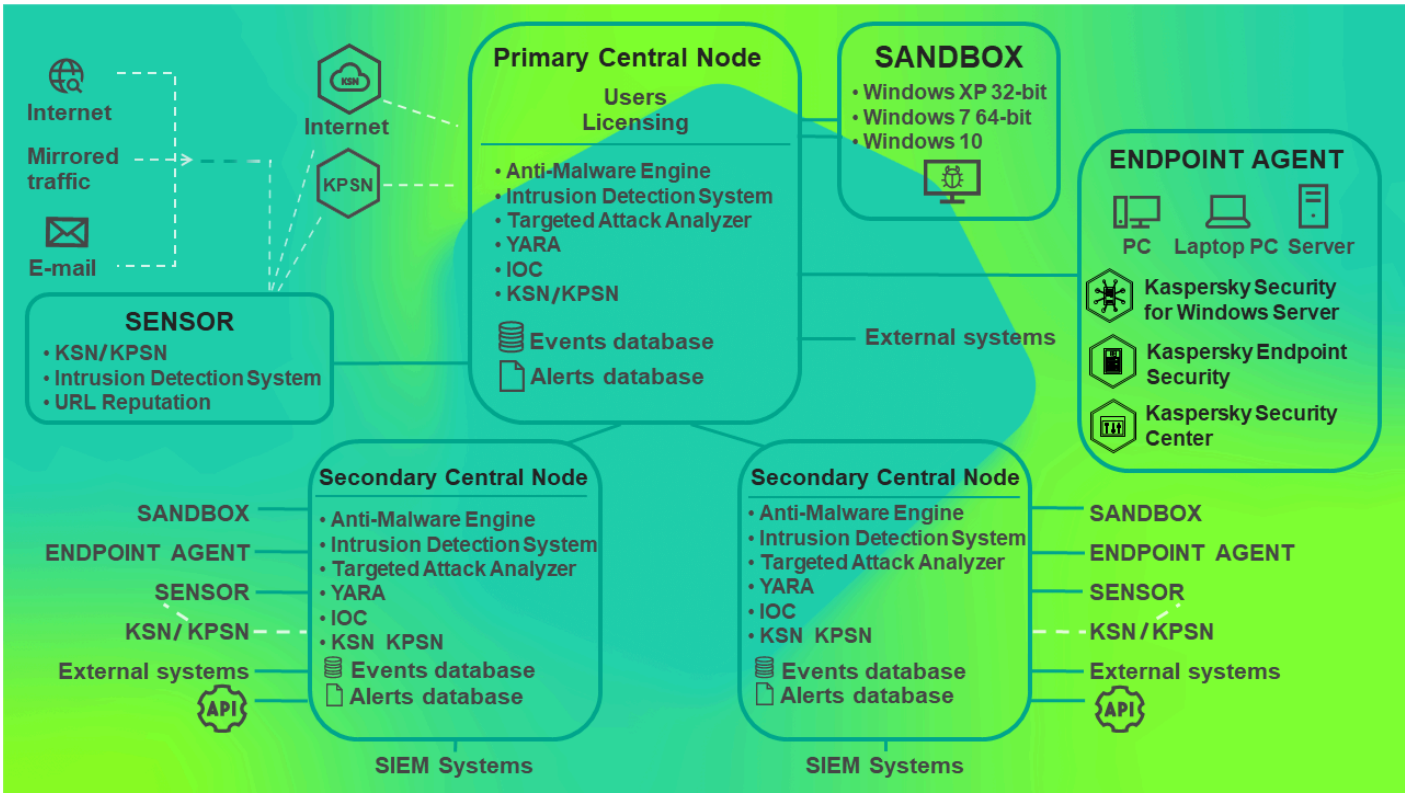


Kaspersky Anti Targeted Attack Platform 的工作原理

您可以單獨配置每個 Central Node 元件的設定，也可以在分佈式解決方案模式下集中管理多個元件。

分佈式解決方案是指 Central Node 伺服器的兩層架構。此結構將主控制伺服器（稱為“主 Central Node (PCN)”）和輔助伺服器（稱為“從屬 Central Node (SCN)”）分開。

分佈式解決方案模式下 Kaspersky Anti Targeted Attack Platform 的工作原理如下圖所示。



分佈式解決方案模式下 Kaspersky Anti Targeted Attack Platform 的工作原理

分佈式解決方案和多租戶

您可以單獨配置每個 Central Node 元件的設定，也可以在分佈式解決方案模式下集中管理多個元件。

分佈式解決方案是指安裝有 Central Node 元件的伺服器的兩層架構。該結構將主控制伺服器（稱為“*主要 Central Node（PCN）*”）和輔助伺服器（稱為“*次要 Central Node（SCN）*”）分開。伺服器的互動要求將 SCN 連線到 PCN。

如果您已將 Central Node 元件部署為叢集，則整個叢集將扮演 PCN 或 SCN 的角色。

PCN 和 SCN 使用與單獨管理的 Central Node 元件相同的技術來掃描檔案和物件。

分佈式解決方案允許對應用程式的以下功能區進行集中式管理：

- 使用者。
- 警示。
- 威脅搜尋。
- 工作。
- 阻止。
- 自訂規則。
- 儲存。
- Endpoint Agent，包括主機的網路隔離。
- 報告。

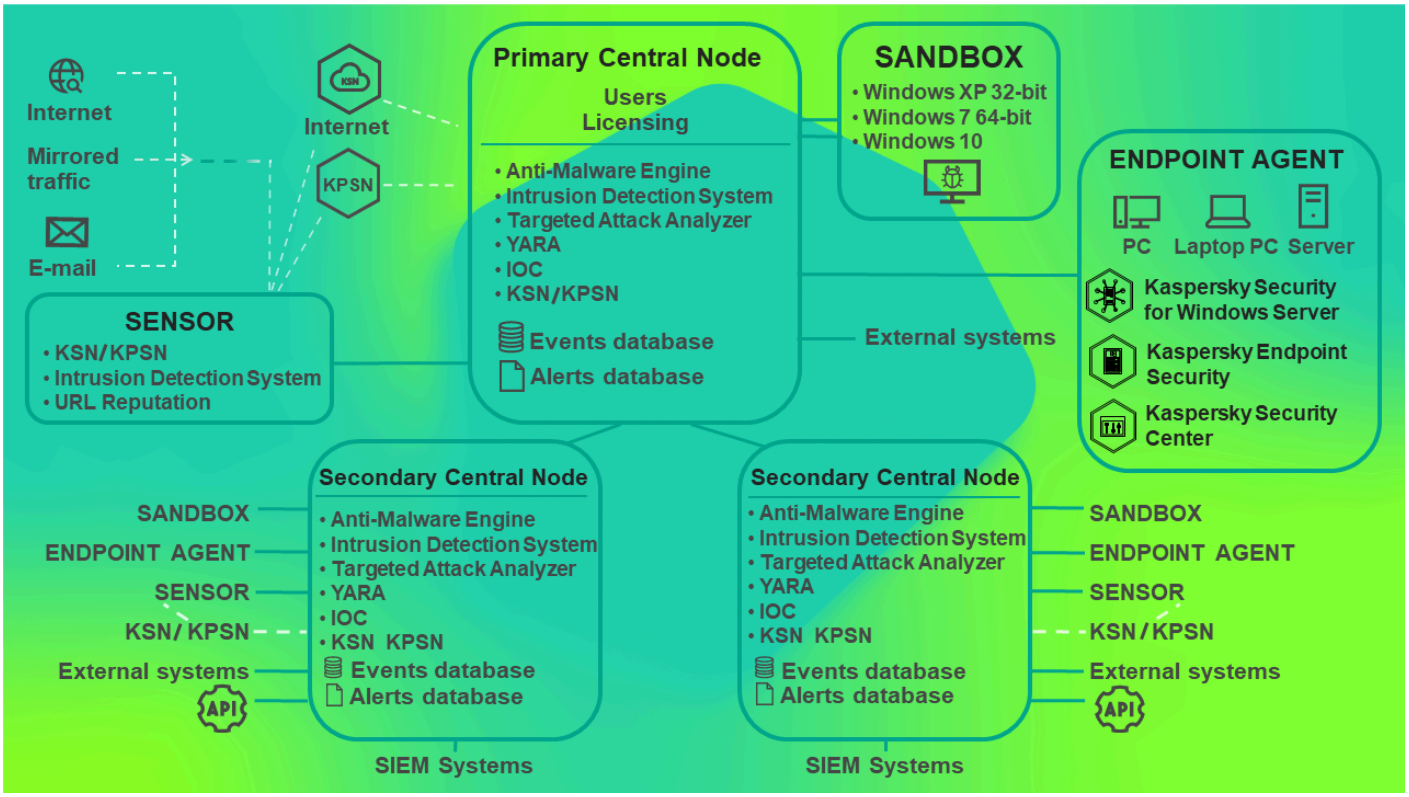
如果您支援多個組織或同一組織的多個分支機構，則可以在多租戶模式下使用該應用程式。

多組織用戶模式可讓您使用該應用程式同時防護多個組織或同一組織的多個分公司（以下也稱為“租用戶”）的基礎架構。您可以在每個租戶的一個或多個 Central Node 上安裝 Kaspersky Anti Targeted Attack Platform。每個租戶都可以獨立於其他租戶管理應用程式。服務提供者可以管理多個租戶的資料。

您要組織成階層的 Central Node 元件必須以相同的作業系統（Ubuntu 或 Astra Linux）為基礎。元件版本必須相同。

對於每個使用者帳戶，同時進行的應用程式管理工作階段的數量限制在一個 IP 位址。如果使用相同的使用者名稱從不同的 IP 位址登入應用程式，則先前的工作階段將終止。

如果您使用分佈式解決方案和多租戶模式，則對每個 PCN 和 SCN 伺服器分別實施限制。



分佈式解決方案模式下的應用程式運行

您可以在以下情況下使用分佈式解決方案和多租戶模式：

- 為了防護一個租戶的 10000 台以上主機
- 用於對租戶不同業務部門的應用程式進行集中管理
- 用於集中管理多個租戶的伺服器上的應用程式
- 用於以最大 10 Gbps 速率處理網路流量，如果您的網路封包含多個 10 Gbps 網段並且您想要處理這些網段中的流量

當應用程式切換到分佈式解決方案和多租戶模式時，所有先前新增的產品授權金鑰都將從具有 SCN 角色的伺服器中刪除。每個連線的 SCN 接收到來自 PCN 的一個金鑰。如果應用程式的完整功能用於 PCN（KATA 和 KEDR 金鑰），而部分功能用於 SCN（僅 KATA 金鑰或僅 KEDR 金鑰），則可能會因資料量增加而超出 SCN 伺服器負載限制。如果部分應用程式功能用於 PCN（僅 KATA 金鑰或僅 KEDR 金鑰），而完整功能用於 SCN（KATA 和 KEDR 金鑰），則應用程式功能部分不可用。

產品授權金鑰只能在 PCN 上管理。

您可以使用下列方案以分佈式解決方案和多租戶模式部署應用程式：

- 在新的伺服器上安裝 Central Node 元件並將 PCN 和 SCN 角色指派給那些伺服器。
- 將 PCN 和 SCN 角色指派給已經安裝了 Central Node 元件的伺服器。

  在這種情況下，您必須將 Central Node 元件更新到 7.1.1 版。

在您將安裝了 Central Node 元件的伺服器切換為分佈式解決方案模式之前，您應該在運行模式變更之後檢視將被應用到系統的變更。將 PCN 角色分配給一台伺服器是不可逆轉的。

分佈式解決方案及多租戶模式過渡方案

將應用程式切換到分佈式解決方案和多租戶模式涉及以下步驟：

1. **為要用作 PCN 的 Central Node 伺服器指派 DNS 名稱**

   如果先前已指派 DNS 名稱，請確保正確指定名稱。

2. **將 PCN 角色分配給一台伺服器**

3. **在 PCN 伺服器上建立應用程式管理員帳戶**

   您將使用此帳戶將 SCN 伺服器連線到 PCN。如果為 Kaspersky Anti Targeted Attack Platform 配置了 Active Directory 整合，您必須在建立帳戶時選擇**KATA 使用者帳戶**身分驗證類型。

4. **將 SCN 角色分配給伺服器並向 PCN 傳送連線請求**

5. **處理 SCN 到 PCN 的連線請求**

切換到分佈式解決方案和多租戶模式後，應用程式可能需要一些時間來配置元件。在此情況下，SCN 的 Web 介面不會顯示應用程式選單，而在 PCN Web 介面的**控制板**區段中，會顯示錯誤：*資料已超過 5 分鐘未傳送到 SCN*。。配置元件所需的時間取決於累積的資料量；平均需要 20 到 30 分鐘。

修改分佈式解決方案和多租戶模式的應用程式設定

分佈式解決方案模式的應用程式設定修改列在下表中。

切換到分佈式解決方案和多租戶模式時修改應用程式設定

功能區域	PCN	SCN
使用者	分配給它們的使用者和角色將被保留。此外，PCN 使用者被授予存取權限，以使用 PCN 和所有連線的 SCN。	除部署 Central Node 時建立的使用者外，將刪除所有的使用者。 之後，SCN 從 PCN 請求使用者清單，並使用該清單建立具有相同參數的本機使用者： • 名稱 • 密碼 • 角色 • 狀態 無權存取 SCN 的使用者不會顯示在使用者清單中。
警示	PCN 上的警示表會記錄所有在已連線的 SCN 上註冊的所有警示。 警示卡中的資料不會複製到 PCN。在 PCN 上檢視有關警示的資訊時，會從 SCN 請求資料。	使用者名稱不再顯示在現有的警示資訊中。使用者資料將從警示操作記錄中刪除。
網路流量事件	沒有變化。	沒有變化。
控制板	在**警示**索引標籤上，您現在可以選擇必須在小工具中顯示資訊的 SCN。 在**系統健康**索引標籤上，現在顯示 PCN 與已連線 SCN 的連線狀態。	在**系統健康**索引標籤上，現在顯示與 PCN 的連線狀態。

功能區域	PCN	SCN
工作	在將分配 PCN 角色指派給 Central Node 伺服器之前在 Central Node 伺服器上建立的工作，以及在切換到分佈式解決方案模式後在 PCN 上建立的工作，適用於所有連線的 SCN。 在 SCN 上建立的工作也會顯示在工作清單中。PCN 上無法變更這些工作的設定。	顯示在 PCN 上建立的工作，以及在此 SCN 上建立的工作。 在 PCN 上建立的工作設定無法變更。
報告	保留在切換到分佈式解決方案模式之前建立的範本和報告。 **伺服器**列被新增到報告表中，其中包含警示所屬的 SCN 的資訊。 切換到分佈式解決方案模式後，僅顯示在 PCN 上建立的報告。	保留在切換到分佈式解決方案模式之前建立的範本和報告。 如果 PCN 具有相同 ID (guid) 的使用者，則保留有關建立報告的使用者的資訊。在其他情況下，使用者資訊將被刪除。 切換到分佈式解決方案模式後，僅顯示在 SCN 上建立的報告。
阻止	在將 PCN 角色指派給 Central Node 伺服器之前在 Central Node 伺服器上建立的政策，以及在切換到分佈式解決方案模式後在 PCN 上建立的政策，適用於所有連線的 SCN。 在 SCN 上建立的政策也會顯示在政策清單中。PCN 上無法變更這些政策的設定。 自動建立防護規則的預設變得不可用，新規則未建立。先前自動建立的規則適用於所有連線的 SCN。	將顯示在 PCN 上建立的政策，以及在此 SCN 上建立的政策。 在 PCN 上建立的政策設定無法變更。 自動建立防護規則的預設變得不可用，新規則未建立。先前自動建立的規則僅適用於此 SCN。
儲存	保留在切換到分佈式解決方案模式之前儲存在 PCN 上的所有檔案和中繼資料。在**Central Node**列中顯示 PCN 的名稱。 PCN 也保留所有連線的 SCN 的儲存內容。	保留在切換到分佈式解決方案模式之前儲存在 SCN 上的所有檔案和中繼資料。
TAA 排除項目	沒有變化。	沒有變化。
VIP 狀態	沒有變化。	沒有變化。
通知規則	沒有變化。	沒有變化。
與郵件感應器的整合	沒有變化。	沒有變化。
威脅搜尋	在資料庫中的威脅搜尋期間，PCN 會向所有連線的 SCN 傳送請求。搜尋查詢處理完畢後，會顯示所選租用戶的 PCN 和 SCN 事件清單。	沒有變化。
自訂規則 - TAA	在被指派 PCN 角色之前在 Central Node 伺服器上新增的 TAA (IOA) 規則將僅被套用至 PCN 伺服器。伺服器取得 PCN 角色後新增的規則也適用於 SCN。	在 PCN 上新增的 TAA (IOA) 規則，以及在切換到分佈式解決方案模式之前和之後在此 SCN 上新增的 TAA (IOA) 規則都會顯示。
自訂規則 - 入侵偵測	沒有變化。	沒有變化。
自訂規則 - IOC	透過在 Central Node 伺服器獲得 PCN 角色之前在其上新增的 IOC 檔案來搜尋危害指標僅在該 PCN 伺服器上執行。透過在 Central Node 伺服器取得 PCN 角色之後在其上新增的 IOC 檔案來搜尋入侵指標也會在 SCN 上執行。	在 PCN 上新增的 IOC 檔案，以及在切換到分佈式解決方案模式之前和之後在此 SCN 上新增的 IOC 檔案都會顯示。
自訂規則 - YARA	在被指派 PCN 角色之前在 Central Node 伺服器上新增的 YARA 規則將只被套用於 PCN。伺服器取得 PCN 角色後新增的規則也適用於 SCN。	在 PCN 上新增的 YARA 規則，以及在切換到分佈式解決方案模式之前和之後在此 SCN 上新增的 YARA 規則都會顯示。
資產	沒有變化。	沒有變化。
網路地圖	沒有變化。	沒有變化。
風險和異常	沒有變化。	沒有變化。
應用程式備份	應用程式的備份僅在未連線 SCN 的 PCN 上可用。 若要在 PCN 上備份應用程式，請中斷所有 SCN 與 PCN 的連線。	在 SCN 上備份應用程式不可用。 要在 SCN 上備份應用程式，請將該伺服器切換到獨立伺服器模式，從而中斷該伺服器與 PCN 的連線。

將 PCN 角色分配給一台伺服器

將 PCN 角色分配給一台伺服器是不可逆轉的。將伺服器角色變更為 PCN 後，您將無法將該伺服器的角色變更為 SCN 或獨立伺服器。若要變更該伺服器的角色，您必須重新安裝應用程式。

要將 PCN 角色指派給伺服器：

1. 利用管理員帳戶登入應用程式 Web 介面。
   您需要登入要對其指派 PCN 角色的伺服器的 Web 介面。
2. 選擇**操作模式**部分。
3. 點擊**分佈式解決方案**。
4. 在**伺服器角色**下拉清單中，選擇**主要 Central Node**。
5. 在**租戶名稱**欄位中，輸入該 Central Node 伺服器所屬的租用戶名稱。
6. 點擊**分配 PCN 角色**。
   這將開啟操作確認視窗。

   確認操作後，再次登入應用程式 Web 介面。

7. 點擊**是**。

伺服器被指派 PCN 角色和租戶名稱。

使用管理員憑據登入應用程式 Web 介面後，應用程式 Web 介面的**操作模式**部分顯示以下資訊：

- **目前模式** – 分佈式解決方案。
- **伺服器角色** – 主要 Central Node。
- **憑證指紋** – 建立與 SCN 連線時，需要伺服器的憑證指紋才能進行身分驗證。
- **租戶** – 有關此伺服器和連線的 SCN 伺服器所屬租用戶的資訊：
  - **IP** – 此伺服器的主要 Central Node和 SCN 伺服器的 IP 位址（連線後）。
  - **伺服器** –該伺服器的名稱和 SCN 伺服器的名稱（連線後）。
    該名稱與安裝有應用程式的主機名稱無關。您可以變更它。
  - **憑證指紋** – 此伺服器的空白值和 SCN 伺服器的憑證指紋（連線後）。
  - **狀態** – SCN 伺服器的連線狀態（連線後）以及連線到租用戶的伺服器數量。
- **伺服器等待授權**表包含有關連線的 SCN 的資訊。

將 SCN 角色指派給一台伺服器

要將 SCN 角色指派給伺服器：

1. 利用管理員帳戶登入應用程式 Web 介面。

   您需要登入要對其指派SCN 角色的伺服器的 Web 介面。

2. 在應用程式 Web 介面視窗中選擇“**操作模式**”區域。

3. 點擊**分佈式解決方案**。

4. 在**伺服器角色**下拉清單中，選擇**次要 Central Node**。

5. 在“**伺服器名稱 (FQDN)**”欄位中，輸入要為其指派 SCN 角色的伺服器的 FQDN。

6. 在**PCN IP**欄位中，輸入您希望連線 SCN 並具有 PCN 角色的伺服器 IP 位址。

7. 點擊**獲取憑證指紋**。

   具有 PCN 角色的伺服器的憑證指紋顯示在工作區。

8. 聯絡 PCN 管理員，並將您接收的憑證指紋與 PCN 上**操作模式**部分的**憑證指紋**欄位中顯示的指紋進行比較。

9. 如果 SCN 和 PCN 上的憑證指紋匹配，則在“**使用者名稱**”和“**密碼**”欄位中，輸入在 PCN 上建立的用於連線 SCN 的管理員帳戶的使用者名稱和密碼。

10. 點擊“**傳送連線請求**”。

    這將開啟一個確認視窗。

11. 點擊**是**。

SCN 角色被指派給伺服器。

處理 SCN 到 PCN 的連線請求

要處理 SCN 到 PCN 的連線請求：

1. 登入要用來處理來自其他伺服器的連線請求的 PCN 伺服器的 Web 介面。

2. 在應用程式 Web 介面視窗中選擇“**操作模式**”區域。

   工作區將顯示**伺服器等待授權**表。

3. 聯絡傳送連線請求的 SCN 管理員並驗證**伺服器等待授權**表中的憑證指紋。它必須與**操作模式**部分中**來自請求的憑證指紋**欄位內 SCN 上顯示的指紋相符。

4. 如果 PCN 和 SCN 上的指紋相符，執行如下之一：

- 如果您想拒絕來自 SCN 的連線請求，請點擊“**拒絕**”。
- 如果想要接受來自 SCN 的連線請求：

  a. 點擊**接受**。

  b. 這將開啟**接受連線請求**視窗。

  c. 在**租戶**清單中，選擇要對其指派此 SCN 伺服器的租用戶。此清單包括先前新增的租用戶。

  d. 點擊**接受**。

> 如果憑證指紋不相符，則不建議接受連線要求。確保您輸入的資料正確。

在 SCN 伺服器連線到 PCN 期間，**操作模式**視窗中的所有按鈕將被鎖定。連線完成後，按鈕解鎖。

如果拒絕連線請求，SCN 將繼續作為獨立的 Central Node 伺服器運作。

檢視有關租戶、PCN 和 SCN 伺服器的資訊

在 PCN 伺服器的 Web 介面中，您可以檢視有關該伺服器以及與其連線的所有 SCN 伺服器的資訊。

檢視多租戶模式下 PCN 和 SCN 伺服器的資訊：

1. 利用管理員帳戶登入應用程式 Web 介面。
   您需要登入PCN 伺服器的 Web 介面。
2. 在應用程式 Web 介面視窗中選擇“**操作模式**”區域。

工作區將顯示有關伺服器的以下資訊：

- **目前模式** – 分佈式解決方案。
- **伺服器角色** – 主要 Central Node。
- **憑證指紋** – PCN 伺服器的憑證指紋。
- **租戶** – 有關伺服器所屬租用戶的資訊，以及連線到 PCN 的所有 SCN 伺服器的資訊。
  - **IP** – PCN 伺服器的主要 Central Node和連線到 PCN 的 SCN 伺服器的 IP 位址。
  - **伺服器** – 伺服器名稱以及連線到 PCN 的 SCN 伺服器的名稱。
    該名稱與安裝有應用程式的主機名稱無關。你可以變更它。
  - **憑證指紋** – PCN 伺服器的空白值和等待連線到 PCN 的 SCN 伺服器的憑證指紋。
  - **狀態** – SCN 伺服器的連線狀態以及連線到租用戶的伺服器數量。

- **伺服器等待授權**表格包含以下資訊：
  - **IP** – SCN 伺服器的 IP 位址或網域名稱。
  - **伺服器**是應用程式 Web 介面中顯示的 SCN 伺服器名稱。
    該名稱與安裝有應用程式的主機名稱無關。您可以變更它。
  - **憑證指紋** – 與連線請求一起傳送到 PCN 的 SCN 伺服器的憑證指紋。
  - **狀態** – SCN 到 PCN 連線的狀態。

將租戶新增至 PCN 伺服器

若要在 PCN 伺服器Web 介面中新增租戶：

1. 利用管理員帳戶登入應用程式 Web 介面。
   您必須登入要為其新增租戶的 PCN 伺服器的 Web 介面。
2. 在應用程式 Web 介面視窗中選擇“**操作模式**”區域。
3. 在**租戶**工作區右側，點擊**新增**。
4. 在**名稱**欄位中，輸入您要新增的租戶的名稱。
5. 點擊**新增**。

租戶已新增並顯示在清單中。

從 PCN 伺服器刪除租戶

若要在 PCN 伺服器Web 介面中刪除租戶：

1. 利用管理員帳戶登入應用程式 Web 介面。
   您必須登入要為其刪除租戶的 PCN 伺服器的 Web 介面。
2. 在應用程式 Web 介面視窗中選擇“**操作模式**”區域。
3. 在**租戶**工作區中，選擇要刪除的租用戶。
4. 點擊**刪除**。
   這將開啟操作確認視窗。

該操作不可逆轉。該租戶的所有全域物件以及報告和報告範本都會遺失。

5. 點擊**是**。

租戶被刪除。

在 PCN 伺服器上重新命名租戶

若要在 PCN 伺服器的 Web 介面中重新命名租戶：

1. 利用管理員帳戶登入應用程式 Web 介面。

   您必須登入要為其重新命名租戶的 PCN 伺服器的 Web 介面。

2. 在應用程式 Web 介面視窗中選擇"**操作模式**"區域。

3. 在**租戶**清單中，點擊您要重新命名的租用戶旁邊的 ✎。

   這將開啟一個視窗，您可以在其中重命名租戶。

4. 在**名稱**欄位中，輸入租用戶的新名稱。

5. 點擊**儲存**。

租戶被重命名。

還原 SCN 到 PCN 的連線

可能發生的情況是，SCN 與 PCN 長時間（超過一天）失去連線，導致用於連線的權杖過期。在這種情況下，在"**控制板**"部分，將顯示"*PCN 權杖已過期。登入 SCN 並還原 PCN 連線。*"訊息。

若要還原SCN 到 PCN 的連線：

1. 利用管理員帳戶登入應用程式 Web 介面。

   您需要登入需要重新連線到 PCN 的特定 SCN 的 Web 介面。

2. 在應用程式 Web 介面視窗中選擇"**操作模式**"區域。

3. 點擊"**登入**"連結開啟PCN 伺服器上的授權視窗。

4. 輸入 SCN 先前連線到的 PCN 伺服器 IP 位址，以及在 PCN 上為 SCN 連線建立的管理員帳戶的使用者名稱和密碼。

5. 點擊"**登入**"。

一段時間後，SCN 重新連線到 PCN，並且"*PCN 權杖已過期。登入 SCN 並還原 PCN 連線。*"訊息不再顯示在"**控制板**"部分。

斷開 SCN 與 PCN 的連線

如果要中斷 SCN 與PCN 的連線，請注意以下特殊事項：

- 從7.0 版本開始，SCN 伺服器無法重新連線到任何PCN 伺服器。
- 如果您想將伺服器重新連線為 SCN，則需要在此伺服器上重新安裝 Central Node 元件。
- 斷開 SCN 與 PCN 的連線會變更應用程式設定。

Kaspersky Anti Targeted Attack Platform 的管理員負責保密 PCN、SCN 和 Central Node 伺服器上的資料。如果您打算將 SCN 伺服器從一個租戶移至另一個租戶，則必須在使用 Kaspersky Anti Targeted Attack Platform 後刪除伺服器上剩餘的所有資料，並重新安裝 Kaspersky Anti Targeted Attack Platform，然後再將伺服器移交給其他租戶。

要斷開 SCN 與 PCN 之間的連線：

1. 登入要使用管理員帳戶從其斷開連線 SCN 的 PCN 伺服器的 Web 介面。
2. 在應用程式 Web 介面視窗中選擇"**操作模式**"區域。
3. 在伺服器清單中，選擇您要斷開連線的 SCN。
4. 點擊**斷開連線**。
   這將開啟操作確認視窗。
5. 點擊**是**。

SCN 與 PCN 斷開連線並繼續作為獨立的 Central Node 伺服器工作。

修改斷開 SCN 與 PCN 連線的應用程式設定

下表列出了 SCN 與 PCN 斷開連線後應用程式設定的修改。

SCN 與 PCN 斷開連線後應用程式設定的修改

功能區域	PCN	SCN
使用者	斷開連線的 SCN 不會從應用程式使用者權限的伺服器清單中刪除。 有關對已斷開連線的 SCN 具有權限的使用者帳戶變更的資訊不會傳送至 SCN。	從 PCN 收到的使用者帳戶不會被刪除。 您可以再次建立新使用者帳戶，以及停用和變更現有使用者帳戶的密碼。
警示	已刪除已斷線的 SCN 上的警示資訊。	保留操作歷史記錄和所有警示資訊。
工作	在已斷開連線的 SCN 上建立的工作將會被刪除。	在 PCN 上建立的工作將被刪除。 保留有關在 SCN 上建立工作的使用者的資訊。
報告	先前建立的有關已斷開連線的 SCN 的所有報告都將保留，並且可以保留此伺服器篩選報告清單的功能。	範本和報告不會被修改。
阻止	在已斷開連線的 SCN 上建立的政策將被刪除。	在 PCN 上建立的政策將被刪除。 保留有關在 SCN 上建立政策的使用者的資訊。

功能區域	PCN	SCN
儲存	從儲存中刪除與斷開連線的 SCN 相關的所有物件。	儲存中的所有物件都將保留。 指向該工作的連結將停止處理有關作為 PCN 上建立的工作的一部分而接收的物件的資訊。
TAA 排除項目	沒有變化。	沒有變化。
VIP 狀態	沒有變化。	沒有變化。
通知規則	沒有變化。	沒有變化。
與郵件感應器的整合	沒有變化。	沒有變化。
威脅搜尋	處理完搜尋查詢後，不會顯示與已中斷連線的 CN 相關的事件。	沒有變化。
自訂規則 - TAA 和IOC	斷開連線的 SCN 的 IOC 和 TAA（IOA）規則被刪除。	PCN 上建立的 IOC 和 TAA（IOA）規則被刪除。
應用程式備份	應用程式的備份保持不可用。	備份應用程式變為可用。

規模調整指南

要在應用程式的不同操作條件下獲得並保持最佳效能，必須考慮聯網裝置的數量，網路拓撲以及所需的應用程式功能集合。

選擇最佳應用程式配置包括以下步驟：

1. **選擇通用部署方案**
2. **使用大小計算器計算硬體需求**

部署和安裝應用程式元件的常見方案

部署和安裝應用程式元件的方案取決於應用程式伺服器上的計劃載入。

您可以安裝一個或多個 Central Node 元件。您可以安裝一個或多個 Central Node 元件。如果您安裝了多個 Central Node 元件，您可以彼此獨立地使用它們或將它們組合起來用於分佈式解決方案模式下的集中管理。

部署方案選擇取決於所使用的應用程式功能。本手冊中列出的所有方案也適用於在虛擬平台上部署應用程式。

完整功能（KATA、NDR 和 KEDR）

使用 KATA、NDR 和 KEDR 功能時，您可以掃描企業區域網路電腦上的網路流量、郵件流量和資料。

如果組織內使用超過 5000 台具有 Endpoint Agent 元件的主機，則不建議使用 Central Node 元件來處理流量。

> 您可以將 Sensor 元件用作代理伺服器，以便將連線到 KEDR 功能單元的 Endpoint Agent 連線到Central Node。一個 Sensor 元件支援連線最多 1000 台具有 Endpoint Agent 元件的主機。

使用 KATA、NDR 和 KEDR 功能時，選擇部署方案的條件如下表所示。選擇演算法如下：

1. 在表格的每一行中，選擇包含與IT 基礎結構對應的條件值的儲存格。

   如果一行中包含兩個具有相同值的儲存格，則必須選取左側的儲存格。

2. 選擇有標記儲存格的最右側列。

使用 KATA、NDR 和 KEDR 功能時選擇部署方案

條件	雙伺服器方案	三伺服器方案	四台或以上伺服器方案	分佈式解決方案
無法在同一裝置上接收網路流量和郵件流量。	否	是	是	是
Endpoint Agent 主機數量	否	從 5000 到 10000	從 5000 到 10000	10000 以上
通訊頻道頻寬	1 Gbps	1 到 2 Gbps	2 Gbps 以上	2 Gbps 以上

條件	雙伺服器方案	三伺服器方案	四台或以上伺服器方案	分佈式解決方案
需要分析流量的遠端基礎架構的數量。	否	一個	兩個或以上	兩個或以上
一個 Sandbox 元件的容量不足以在可接受的時間範圍內分析所有物件。	否	否	是	是

在分佈式解決方案模式下，每個應用程式元件必須滿足大小計算器中指定的硬體要求。

處理網路流量、郵件流量和 Web 流量（KATA 和 NDR）

如果組織不需要處理企業區域網路電腦上的資料，建議使用 KATA 和 NDR 功能。如果是這種情況，則僅處理網路流量和郵件流量。

使用 KATA 功能時選擇部署方案的條件如下表所示。選擇演算法如下：

1. 在表格的每一行中，選擇包含與IT 基礎結構對應的條件值的儲存格。
   如果一行中包含兩個具有相同值的儲存格，則必須選取左側的儲存格。
2. 選擇有標記儲存格的最右側列。

使用 KATA 功能時選擇部署方案

條件	雙伺服器方案	三伺服器方案	四台或以上伺服器方案
無法在同一裝置上接收網路流量和郵件流量。	否	是	是
通訊頻道頻寬	1 Gbps	1 到 2 Gbps	2 Gbps 以上
需要分析流量的遠端基礎架構的數量。	否	一個	兩個或以上
一個 Sandbox 元件的容量不足以在可接受的時間範圍內分析所有物件。	否	否	是

處理來自企業區域網路電腦 (KEDR) 的資料

如果組織不需要處理流量，建議使用 KEDR 功能。如果是這種情況，則僅處理企業區域網路電腦上的資料。

取決於組織中是否存在第三方 Sandbox 解決方案，您可以使用下列部署方案之一：

- 沒有 Sandbox 元件
- 使用 Sandbox 元件

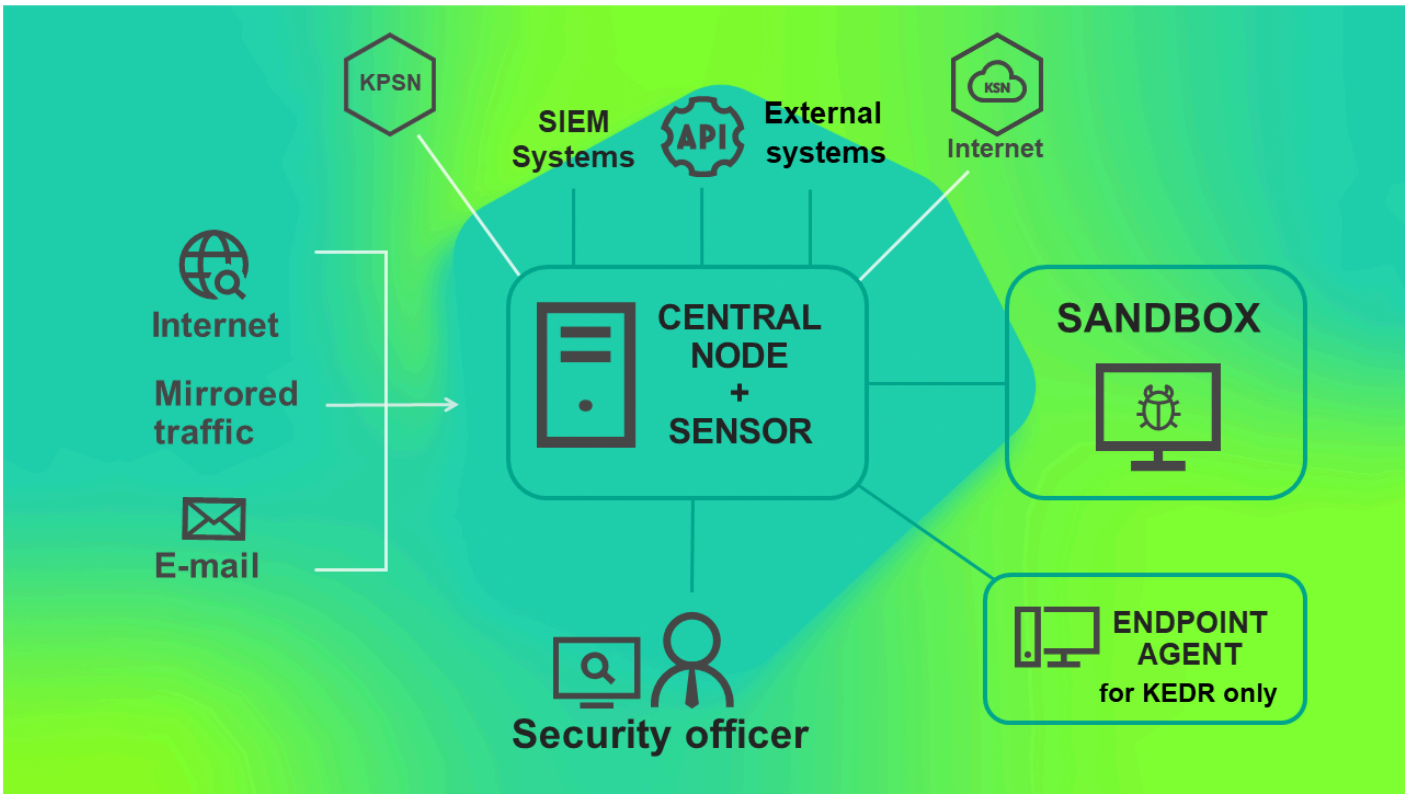
雙伺服器部署方案

使用 KATA 和 KEDR 功能時，可以在企業區域網路電腦上安裝 Endpoint Agent 元件。使用 KATA 功能時，Endpoint Agent 元件不會被安裝。

使用此部署方案時，Central Node 和 Sensor 元件將安裝在相同伺服器或叢集上。此伺服器或叢集可接收流量，執行流量的初始分析並對提取的檔案進行更深入的分析。根據掃描結果，元件偵測到對組織的 IT 基礎架構進行針對性攻擊的跡象。

Sandbox 元件安裝在另一台伺服器上。

部署在兩台伺服器上的應用程式運行方案如下圖所示。



部署在兩台伺服器上的應用程式運行方案

三伺服器部署方案

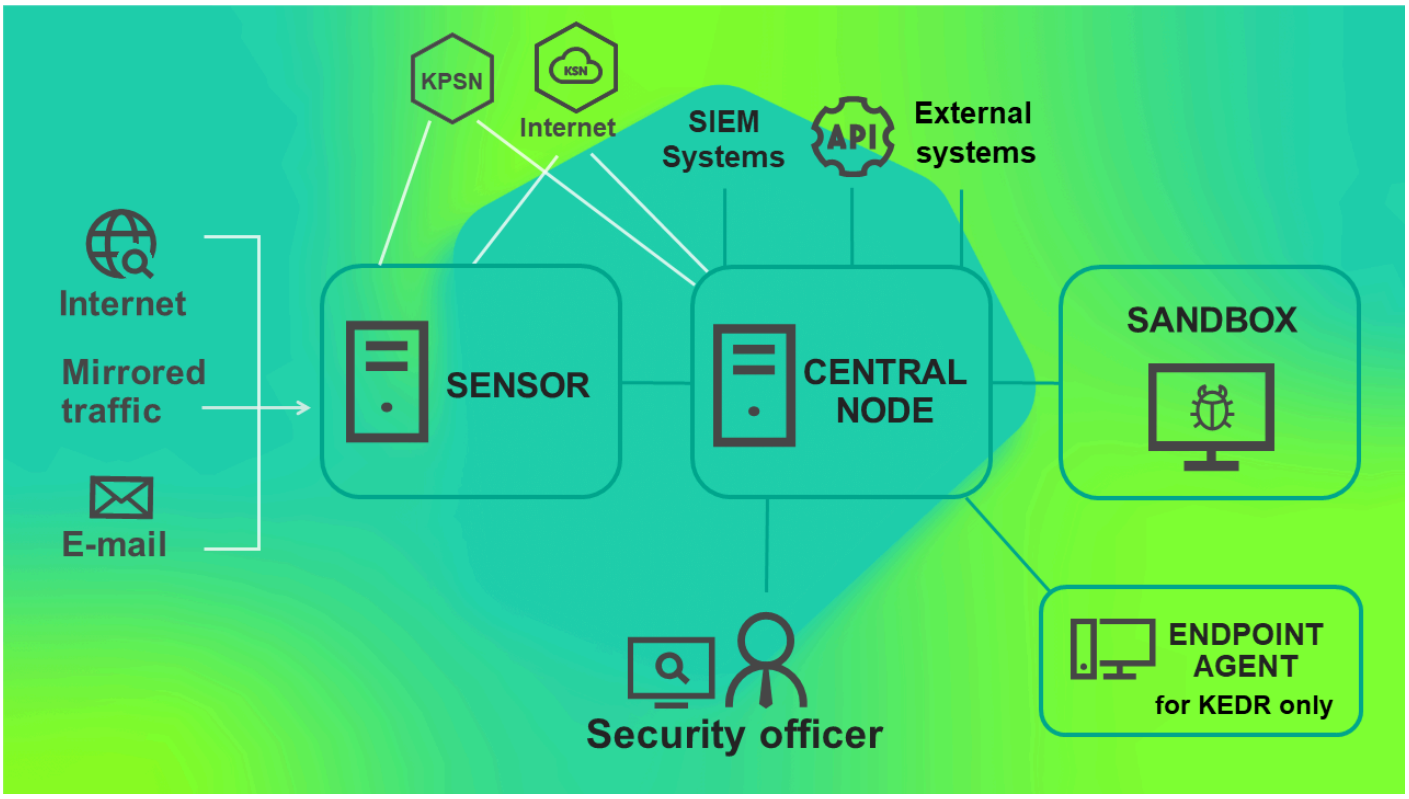
使用 KATA 和 KEDR 功能時，可以在企業區域網路電腦上安裝 Endpoint Agent 元件。使用 KATA 功能時，Endpoint Agent 元件不會被安裝。

使用此部署方案時，Sensor、Central Node 和 Sandbox 元件會安裝在不同的伺服器上。Central Node 元件也可以部署為叢集。Sensor 可接收流量，執行初始分析，提取檔案並將它們轉送到 Central Node 元件以進行更深入的分析。

使用此部署方案，Central Node 元件可以接收流量並對主基礎架構中的資料執行初始分析。在這種情況下，您可以將 Sensor 元件安裝在需要分析其流量的遠端基礎架構的伺服器上。如果主基礎設施中的連結頻寬超過 2 Gbps，我們建議在主基礎設施中安裝 Sensor。

Central Node 和 Sensor 元件之間交換的流量最多佔 Sensor 元件接收的流量的 20%。

部署在三台伺服器上的應用程式運行方案如下圖所示。



部署在三台伺服器上的應用程式運行方案

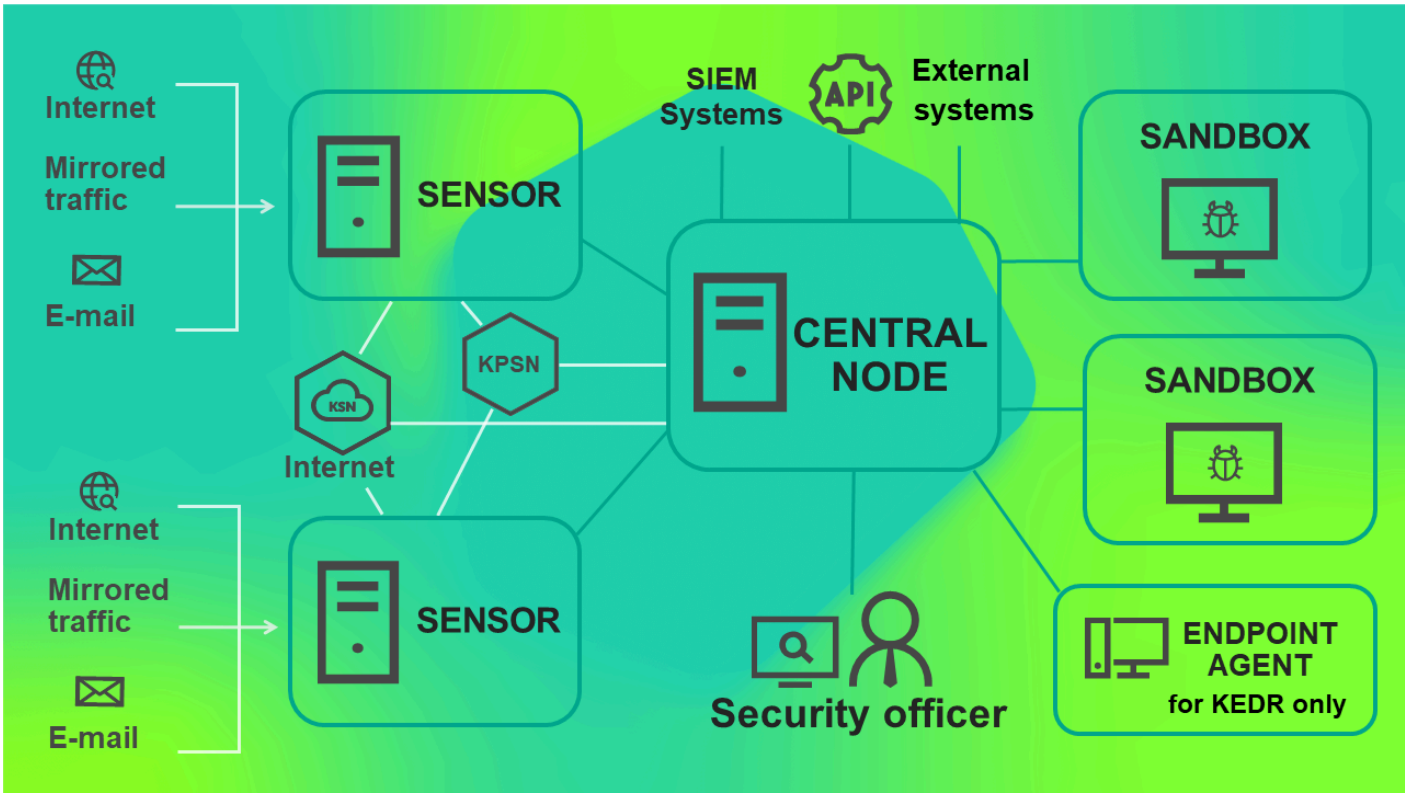
四台或以上伺服器部署方案

使用 KATA 和 KEDR 功能時，可以在企業區域網路電腦上安裝 Endpoint Agent 元件。使用 KATA 功能時，Endpoint Agent 元件不會被安裝。

如果存在大量流量，則可以在不同伺服器上安裝多個 Sensor 元件或多個 Sandbox 元件。建議在大型組織中部署此方案。

您也可以使用一個 Sandbox 元件連線到多個 Central Node 元件。

部署在四台或更多伺服器上的應用程式操作原理圖如下圖所示。

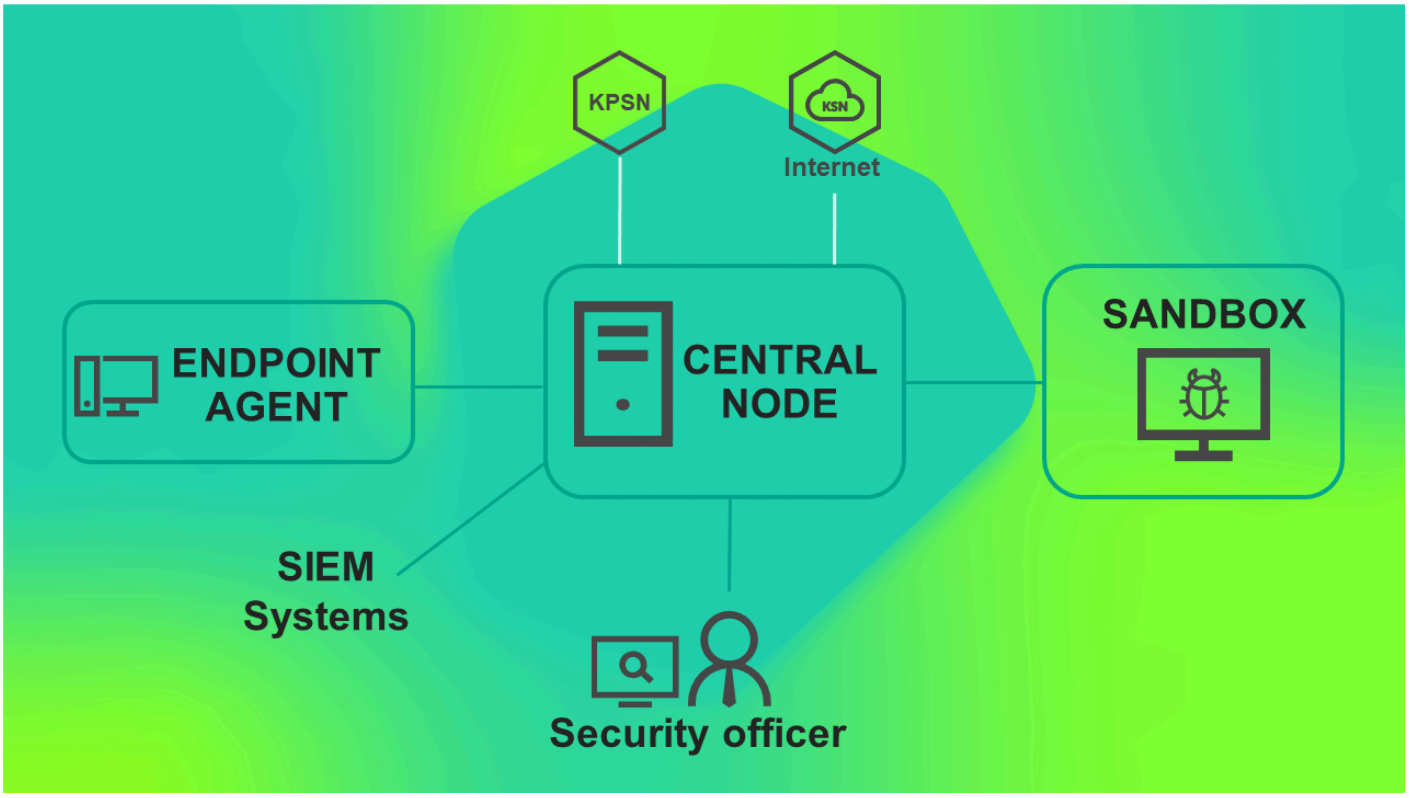


部署在四台及以上伺服器上的應用程式運行方案

使用 Sandbox 元件部署 KEDR 功能的方案

如果使用此部署方案，您需要將 Central Node 元件與 Sensor 元件分開安裝。

使用 Sandbox 元件部署 KEDR 功能時的應用程式運作方案如下圖所示。



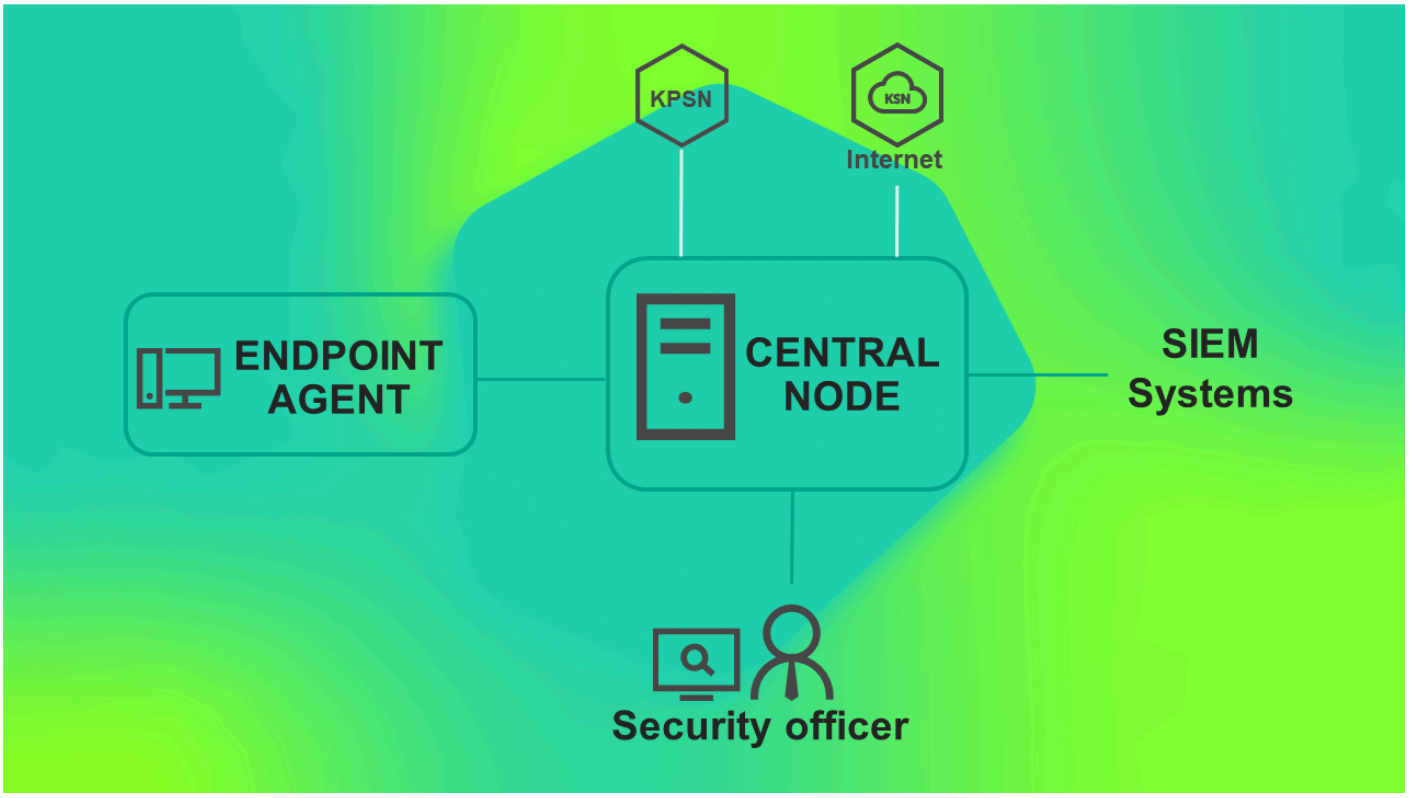
使用 Sandbox 元件部署 KEDR 功能時的應用程式運行方案

在沒有 Sandbox 元件的情況下部署 KEDR 功能的方案

您無需安裝 Sandbox 元件，只需使用 Central Node 元件來管理 Endpoint Agent 元件和資料分析。

如果使用此部署方案，您需要將 Central Node 元件與 Sensor 元件分開安裝。

不使用 Sandbox 元件部署 KEDR 功能時的應用程式運作方案如下圖所示。



不使用 Sandbox 元件部署 KEDR 功能時的應用程式運作方案

大小計算器

選擇最適合 IT 基礎架構的部署方案後，必須計算用於安裝應用程式元件的伺服器硬體需求。

7.1 Central Node 伺服器的硬體需求與元件先前版本的硬體需求不同。我們強烈建議確保伺服器配置符合以下章節所述的要求：使用 KATA 功能時 Central Node 元件的計算、使用 KEDR 功能時 Central Node 元件的計算、使用 KATA 和 KEDR 功能時 Central Node 元件的計算、使用 KATA 和 NDR 功能時 Central Node 元件的計算、使用 KATA、KEDR 和 NDR 功能時 Central Node 元件的計算。

如果需要，您可以在為應用程式 5.1 版本設計的硬體上使用應用程式 7.1.7 版本。

在這種情況下，適用以下限制：

- 您只能使用 5.1 版本中提供的應用程式功能。如果您想使用應用程式其他版本的功能，Central Node 伺服器的硬體必須滿足這些版本的說明中列出的硬體要求。

  您可以在 Kaspersky Anti Targeted Attack Platform 6.0–8.0 對應版本說明的*新功能*章節中找到新功能清單。

- 應用程式必須部署在 Ubuntu Server 作業系統上。

- 您只能使用 KATA 和/或 KEDR 產品授權金鑰。

- 只有當 Central Node 伺服器的 CPU 支援 BMI2、AVX 和 AVX2 指令集時，才可以將應用程式從 5.1 版本升級到 7.1.7 版本。如果不支援這些指令集，您可以從分發套件安裝 7.1 版本應用程式，然後將其升級到 7.1.7 版本。

  升級必須從版本 5.1 開始依序進行：5.1 → 6.0、6.0 → 6.0.2、6.0.2 → 6.1、6.1 → 7.0.3、7.0.3 → 7.1.1、7.1.1 → 7.1.3、7.1.3 → 7.1.7。

Sensor 元件的計算

在計算 Sensor 元件的硬體需求時，請考慮可處理的最大流量為 10 Gbps。此最大流量可以在獨立伺服器上安裝的一個 Sensor 上處理，也可以在連線到一個 Central Node 的獨立伺服器上安裝的多個 Sensor 上進行處理。連線到一個 Central Node 的所有 Sensor 的總流量不得超過 10 Gbps。

如果網路中包含多個 10 Gbps 網段，且您需要處理這些網段的流量，則必須採用分散式解決方案模式。

您可以在 Endpoint Agent 工作站和 Central Node 之間交換資料期間，將託管 Sensor 的伺服器用作代理伺服器（與 KEDR 功能整合時），以簡化網路規則的配置。例如，如果帶有 Endpoint Agent 的工作站位於網路的單獨段中，則只需配置 Central Node 和 Sensor 伺服器之間的連線即可。

當使用 Sensor 作為代理伺服器在 Endpoint Agent 元件和 Central Node 元件之間進行通訊時，請考慮以下限制：

- 最多 15000 台具有 Endpoint Agent 元件的工作站可以連線到單個 Central Node 元件。
- Sensor 伺服器和 Central Node 之間允許的最大封包遺失率為 10%，封包延遲最多為 100 毫秒。

Central Node 和 Sensor 伺服器之間的連結所需的頻寬取決於必須處理的流量，計算如下：

`典型負載時 10% 的 SPAN 連接埠流量或峰值負載時 20% 的 SPAN 連接埠流量 + 電子郵件流量 + ICAP 流量 + Central Node 和 Endpoint Agent 之間的連結要求`

Sensor 伺服器的硬體需求

Sensor 元件可以與組織的 IT 基礎架構整合，如下所示：

- 從 SPAN 連接埠接收來自網路裝置的鏡像流量。
- 透過 POP3 協定連線到郵件伺服器。
- 透過 SMTP 協定連線到郵件伺服器。
- 透過 ICAP 協定從代理伺服器接收流量。
- 從 Endpoint Agent 元件接收資料。

下表列出了 Sensor 伺服器的硬體需求。

Sensor 元件在負載高達 1000 Mbit/s 的虛擬平台上進行了測試；但是，虛擬平台支援更大的負載。如果您想在虛擬平台上部署 Sensor 元件，並計劃處理高達 1000 Mbps 的流量，則可以使用下表計算 Sensor 伺服器的硬體需求。如果您計劃處理更多流量，請聯絡您的客戶經理以取得硬體需求的計算。

Sensor 伺服器的硬體需求取決於使用 KATA 和KEDR 功能時從 SPAN 連接埠處理的流量

Endpoint Agent 元件的數量（與 KEDR 功能整合）	處理的流量 (Mbps)	最小 RAM (GB)	最小邏輯核心數
10000	100	20	6
15000	500	24	10

Endpoint Agent 元件的數量（與 KEDR 功能整合）	處理的流量 (Mbps)	最小 RAM (GB)	最小邏輯核心數
15000	1000	32	14
15000	2000	48	20
15000	4000	56	30
15000	7000	128	44
15000	10000	160	60

Sensor 伺服器的硬體需求取決於使用 KATA 和NDR 功能時從 SPAN 連接埠處理的流量

處理的流量 (Mbps)	最小 RAM (GB)	最小邏輯核心數	儲存映像流量傾印時的最小邏輯核心數
100	28	6	8
500	32	12	14
1000	40	16	18
2000	64	24	26
4000	80	36	40
7000	160	52	56
10000	192	72	76

如果 Sensor 用作伺服器，用於從最多 2000 台具有 Endpoint Agent 元件的主機進行 NDR 遙測，則需要另外 2 個邏輯核心和 4 GB 的額外 RAM。

CPU 必須支援 BMI2、AVX 和AVX2 指令集合。

如果您只想處理電子郵件，而不處理來自 SPAN 連接埠的映像流量，我們建議使用安裝在與 Central Node 相同的伺服器上的 Sensor。

如果一個 Sensor 伺服器透過多種協定處理流量，則若要計算伺服器硬件，您必須考慮到郵件伺服器或郵件感應器整合需要停用 SMTP 流量處理。

Sensor 伺服器上的磁碟空間需求

建議使用 RAID 1 磁碟陣列。磁碟總空間必須至少為 600 GB。

儲存來自 SPAN 連接埠的映像流量傾印時的 Sensor 硬體需求

如果要儲存來自 SPAN 連接埠的映像流量傾印，則Sensor 伺服器的下列硬體需求會更高：

- 以 RAID 陣列或 DAS 池的形式安裝單獨的磁碟儲存，其最大頻寬使用以下公式計算：
  <磁碟儲存頻寬> = 3 * <記錄流量的最大吞吐量>
- 磁碟儲存的容量取決於預期的儲存時間和儲存的最大流量吞吐量，並考慮到篩選器。根據粗略計算，要儲存 7 天最大吞吐量為 10 Gbps 的記錄流量，需要 750 TiB 的磁碟儲存空間。

使用 KATA 功能時對 Central Node 元件的計算

本節介紹使用 KATA 功能時實體和虛擬 Central Node 伺服器的軟體和硬體需求。

Central Node 實體伺服器的硬體需求

Central Node 實體伺服器的硬體需求取決於以下條件：

- 處理的流量

  與未加密流量（來自 SPAN 連接埠的標準流量）相比，Kaspersky Anti Targeted Attack Platform 對已解密的 SSL/TLS 流量的處理負載增加了 5 倍。在此情況下，要確定用於計算伺服器負載的已處理流量，請使用下列公式：

  <解密流量> = 5 * <未加密流量>

  ICAP 伺服器上處理的流量會根據"使用 ICAP 功能時對 Central Node 元件的計算"部分中的表格進行計算。

- 每秒處理的電子郵件數。

如果處理的流量大於 1 Gbps，則必須在獨立伺服器上安裝 Central Node 和 Sensor 元件。

下表列出了 Central Node 伺服器的硬體需求。

Central Node 實體伺服器的硬體需求

每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）			
					ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量
2	500	沒有處理	72	24	100	1000	2	4
2	1000	沒有處理	88	32	100	1000	2	4
5	沒有處理	2000	64	32	100	1000	2	2
20	沒有處理	4000	80	56	100	1000	3	2
20	沒有處理	7000	112	92	200	1500	4	2
20	沒有處理	10,000	128	128	200	1500	4	2

Kaspersky Anti Targeted Attack Platform 不支援軟體 RAID 陣列的操作。

Central Node 虛擬伺服器的硬體需求

在 VMware ESXi 虛擬平台上安裝此元件時，需要將最小邏輯核心數（Central Node 實體伺服器硬體需求表中指定的數值）增加 10%。

如果您想在“Brest”、“RED Virtualization”、KVM 或 zVirt Node 虛擬平台上安裝 Central Node 元件，則需要將最小邏輯核心數增加 40%。如果您想在 Hypervisor 作業系統層級緩解 Spectre 或 Meltdown 類型的漏洞，則需要額外將最小邏輯核心數量增加 1.5 倍。

虛擬伺服器的其他硬體需求與實體伺服器的要求類似。

Central Node 已在負載最高達到 1000 Mbps（含）的虛擬平台上經過測試。

Central Node 虛擬伺服器的軟體需求

在虛擬磁碟設定中，必須選擇 Thick Provision Eager Zeroed 類型。

為了避免在虛擬平台上部署應用程式時可能出現的效能下降，您需要執行以下操作：

- 將延遲敏感度設定為“高”。

  如果您的 Hypervisor 不支援高延遲敏感性，您可以使用其他虛擬機優先權機制，例如 CPU Affinity 或資源預留。

- 保留所有記憶體。
- 保留所有 CPU。

Central Node 伺服器的其他需求

Central Node 實體伺服器的其他硬體需求請參閱以下部分：設定與外部系統整合時 Central Node 元件的運算、使用 ICAP 功能時 Central Node 元件的計算、分散式解決方案和多租戶模式下 Central Node 元件的計算、部署為叢集的 Central Node 元件的計算。

使用 KEDR 功能時對 Central Node 元件的計算

本節介紹使用 KEDR 功能時實體和虛擬 Central Node 伺服器的軟體和硬體需求。

Central Node 實體伺服器的硬體需求

託管 Central Node 的實體伺服器硬體需求取決於安裝 Endpoint Agent 元件的主機數量。

Endpoint Agent 元件可安裝在工作站、終端伺服器、檔案伺服器或網路附加儲存 (NAS) 上。

若要確定具有 Endpoint Agent 元件的有效主機數量來計算伺服器負載，可以使用下列公式：

```
K = A+2*B+3*C+20*D
```

其中

- “K”是具有 Endpoint Agent 元件的主機的最大數量。
- “A”是運行安裝了 Endpoint Agent 元件的 Windows 作業系統的終端伺服器的工作站和使用者數量。
- “B”是運行安裝了 Endpoint Agent 元件的 Linux 作業系統的終端伺服器的工作站和使用者數量。
- “C”是執行 macOS 作業系統並安裝了 Endpoint Agent 元件的終端伺服器的工作站和使用者數量。
- “D”是伺服器數量。

以下“說明”部分提供了有關代表 Endpoint Agent 元件的應用程式版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性的資訊：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

下表列出了 Central Node 伺服器的硬體需求。

Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統 (RAID 10)	
			ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	96	24	100	1000	2	4	300	300
2000	128	32	100	1000	2	4	700	700
5000	160	48	100	1200	2	4	1000	900
10000	224	60	100	1200	2	4	1500	1200
5000	160	52	100	1200	2	4	1000	900
10000	224	90	100	1500	2	4	1500	**200**
15000	288	104	100	1500	2	4	1500	1600
15000	320	140	200	2000	2	4	1500	1600
15000	336	176	200	2000	2	4	1500	1600

如果要使用 2.1 GHz 處理器，Central Node 的硬體必須符合下表中的規格。

使用 2.1 GHz CPU 時對 Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	最小 RAM (GB)	2.1 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
			ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	64	18	100	250	1	4	300	300
3000	96	24	100	500	1	4	700	750
5000	112	28	100	500	1	4	1000	900
10000	160	52	100	500	1	4	1500	1200
15000	224	72	100	750	1	4	1500	1600

如有必要，您可以透過限制來自 Endpoint Agent的事件資料（遙測）的數量來降低 Central Node 的負載。Central Node 伺服器的硬體需求如下表所示。

遙測受限的 Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統 (RAID 10)	
			ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	64	10	100	250	1	4	300	250
3000	80	14	100	500	1	4	500	500
5000	96	16	100	500	1	4	700	600
10000	144	24	100	500	1	4	1000	800
15000	192	32	100	500	1	4	1500	1000

下表列出了使用事件鏈掃描功能時 Central Node 實體伺服器的硬體需求。

啟用事件鏈掃描功能的 Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	最小 RAM (GB)	2.1 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
			ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	64	12	100	250	1	4	300	300
3000	96	16	100	500	1	4	700	750
5000	112	20	100	500	1	4	1000	900
10000	160	34	100	500	1	4	1500	1200
15000	224	48	100	750	1	4	1500	1600
20000*	256	64	150	75	1	4	2000	2000

* 我們建議使用 SSD 磁碟機。

Kaspersky Anti Targeted Attack Platform 不支援軟體 RAID 陣列的操作。

Central Node 虛擬伺服器的硬體需求

以下值適用於將安裝在執行 Windows 作業系統的工作站和終端伺服器上的 10000 個 Endpoint Agent 連線到 Central Node 的情況。

在 VMware ESXi 虛擬平台上安裝此元件時，需要將最小邏輯核心數（Central Node 實體伺服器硬體需求表中指定的數值）增加 10%。

如果您想在“Brest”、“RED 虛擬化”、KVM、zVirt Node 或 Nutanix Acropolis Operating System 虛擬平台上安裝 Central Node 元件，則需要將最小邏輯核心數增加 30%。如果您想在 Hypervisor 作業系統層級緩解 Spectre 或 Meltdown 類型的漏洞，則需要在 30% 的基礎上將最小邏輯核心數量再增加 1.5 倍。

虛擬伺服器的其他硬體需求與實體伺服器的要求類似。

Central Node 虛擬伺服器的軟體需求

在虛擬磁碟設定中，必須選擇 Thick Provision Eager Zeroed 類型。

為了避免在虛擬平台上部署應用程式時可能出現的效能下降，您需要執行以下操作：

- 將延遲敏感度設定為“高”。

  如果您的 Hypervisor 不支援高延遲敏感性，您可以使用其他虛擬機優先權機制，例如 CPU Affinity 或資源預留。

- 保留所有記憶體。

- 保留所有 CPU。

Central Node 伺服器上第二個磁碟子系統的容量需求

第二個磁碟子系統的總最小有效儲存容量使用以下公式計算：

E = 1,5 * (P+T+S+N)

其中

- “E”是第二個磁碟子系統的總最小有效大小。

- P 是持久性儲存容量，可使用下列公式計算：

  30 MB * <具有 Endpoint Agent 元件的主機的有效數量> * <儲存天數>

  永久儲存容量不得超過 20 TB。

- T 是暫時儲存容量，使用下列公式計算：

  27 MB * <具有 Endpoint Agent 元件的主機的有效數量>

  如果您已啟用事件鏈掃描，則暫存量使用下列公式計算：

  40 MB * <具有 Endpoint Agent 元件的主機的有效數量>

- S 是系統檔案的大小，為 150 GB。

該公式可用於粗略估計所需的磁碟空間。實際儲存的資料量取決於組織的流量概況，並且可能與計算結果不同。

根據持久儲存的大小，需要額外的 RAM:

- 對於 10–15 TB 的儲存，請在上表*列出*的最小RAM 基礎上增加 16 GB。

- 對於 15–20 TB 的儲存，請在上表*列出*的最小RAM 基礎上增加 32 GB。

通信頻道要求

您必須確保 Central Node 伺服器與每個網段之間有足夠的通訊頻道頻寬，具體取決於網段中Endpoint Agent 主機數量。下表列出了頻寬需求，取決於 Endpoint Agent 主機數量。

通訊頻道頻寬取決於 Endpoint Agent 主機的數量

Endpoint Agent 的最大有效數量	為 Endpoint Agent 保留的通訊頻道所需頻寬(Mbps)
10	1
50	2
100	3
1000	20
10000	200

Central Node 伺服器的其他需求

Central Node 實體伺服器的其他硬體需求請參閱以下部分：設定與外部系統整合時 Central Node 元件的運算、使用 ICAP 功能時 Central Node 元件的計算、分散式解決方案和多租戶模式下 Central Node 元件的計算、部署為叢集的 Central Node 元件的計算。

使用 KATA 和 KEDR 功能時對 Central Node 元件的計算

本節介紹使用 KATA 和 KEDR 功能時，實體和虛擬 Central Node 伺服器的軟體和硬體需求。

Central Node 實體伺服器的硬體需求

Central Node 實體伺服器的硬體需求取決於以下條件：

- 處理的流量

  與未加密流量（來自 SPAN 連接埠的標準流量）相比，Kaspersky Anti Targeted Attack Platform 對已解密的 SSL/TLS 流量的處理負載增加了 5 倍。在此情況下，要確定用於計算伺服器負載的已處理流量，請使用下列公式：

  <解密流量> = 5 * <未加密流量>

  ICAP 伺服器上處理的流量會根據“使用 ICAP 功能時對 Central Node 元件的計算”部分中的表格進行計算。

- 每秒處理的電子郵件數

- Endpoint Agent 主機數量

  Endpoint Agent 元件可安裝在工作站、終端伺服器、檔案伺服器或網路附加儲存 (NAS) 上。

  以下“說明”部分提供了有關代表 Endpoint Agent 元件的應用程式版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性的資訊：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

若要確定具有 Endpoint Agent 元件的有效主機數量來計算伺服器負載，可以使用下列公式：

```
K = A+2*B+3*C+20*D
```

其中

- “K”是具有 Endpoint Agent 元件的主機的最大數量。
- “A”是運行安裝了 Endpoint Agent 元件的 Windows 作業系統的終端伺服器的工作站和使用者數量。
- “B”是運行安裝了 Endpoint Agent 元件的 Linux 作業系統的終端伺服器的工作站和使用者數量。
- “C”是執行 macOS 作業系統並安裝了 Endpoint Agent 元件的終端伺服器的工作站和使用者數量。
- “D”是伺服器數量。

如果處理的流量大於 1 Gbps，則必須在獨立伺服器上安裝 Central Node 和 Sensor 元件。

下表列出了 Central Node 伺服器的硬體需求。

Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
						ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	1	200	沒有處理	96	24	100	1000	2	4	300	300
2000	2	500	沒有處理	128	32	100	1000	2	4	700	700
5000	1	1000	沒有處理	160	48	100	1200	2	4	1000	900
10000	2	1000	沒有處理	224	60	100	1200	2	4	1500	1200
5000	5	沒有處理	2000	160	52	100	1200	2	4	1000	900
10000	20	沒有處理	4000	224	90	100	1500	2	4	1500	1200
15000	20	沒有處理	4000	288	104	100	1500	2	4	1500	1600
15000	20	沒有處理	7000	320	140	200	2000	2	4	1500	1600
15000	20	沒有處理	10000	336	176	200	2000	2	4	1500	1600

下表列出了使用事件鏈掃描功能時 Central Node 實體伺服器的硬體需求。

啟用事件鏈掃描功能的 Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
						ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	1	200	沒有處理	144	24	100	1000	1.9	4	300	300
2000	2	500	沒有處理	160	32	100	1000	2	4	700	700
5000	1	1000	沒有處理	192	48	100	1000	2	4	1000	900
10000	2	1000	沒有處理	240	64	100	1000	2	4	1500	1200
5000	5	沒有處理	2000	192	60	100	1000	1.9	4	1000	900
10000	20	沒有處理	4000	256	100	100	1000	1.9	4	1500	1200

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
						ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
15000	20	沒有處理	4000	304	112	100	1000	1.9	4	1500	1600
15000	20	沒有處理	7000	320	148	100	1000	1.9	4	1500	1600
15000	20	沒有處理	10000	336	184	100	1000	1.9	4	1500	1600

Central Node 虛擬伺服器的硬體需求

> 以下值適用於將安裝在執行 Windows 作業系統的工作站和終端伺服器上的 10000 個 Endpoint Agent 連線到 Central Node 的情況。

在 VMware ESXi 虛擬平台上安裝此元件時，需要將最小邏輯核心數（Central Node 實體伺服器硬體需求表中指定的數值）增加 10%。

如果您想在“Brest”、“RED 虛擬化”、KVM、zVirt Node 或 Nutanix Acropolis Operating System 虛擬平台上安裝 Central Node 元件，則需要將最小邏輯核心數增加 30%。如果您想在 Hypervisor 作業系統層級緩解 Spectre 或 Meltdown 類型的漏洞，則需要在 30% 的基礎上將最小邏輯核心數量再增加 1.5 倍。

虛擬伺服器的其他硬體需求與實體伺服器的要求類似。

Central Node 虛擬伺服器的軟體需求

在虛擬磁碟設定中，必須選擇 Thick Provision Eager Zeroed 類型。

為了避免在虛擬平台上部署應用程式時可能出現的效能下降，您需要執行以下操作：

- 將延遲敏感度設定為“高”。

  如果您的 Hypervisor 不支援高延遲敏感性，您可以使用其他虛擬機優先權機制，例如 CPU Affinity 或資源預留。

- 保留所有記憶體。
- 保留所有 CPU。

Central Node 伺服器上第二個磁碟子系統的容量需求

第二個磁碟子系統的總最小有效儲存容量使用以下公式計算：

E = 1,5 * (P+T+S+N)

其中

- “E”是第二個磁碟子系統的總最小有效大小。
- P 是持久性儲存容量，可使用下列公式計算：
  30 MB * <具有 Endpoint Agent 元件的主機的有效數量> * <儲存天數>
  永久儲存容量不得超過 20 TB。
- T 是暫時儲存容量，使用下列公式計算：
  27 MB * <具有 Endpoint Agent 元件的主機的有效數量>
- 如果您已啟用事件鏈掃描，則暫存量使用下列公式計算：
  40 MB * <具有 Endpoint Agent 元件的主機的有效數量>
- S 是系統檔案的大小，為 150 GB。

該公式可用於粗略估計所需的磁碟空間。實際儲存的資料量取決於組織的流量概況，並且可能與計算結果不同。

根據持久儲存的大小，需要額外的 RAM:

- 對於 10–15 TB 的儲存，請在上表*列出*的最小RAM 基礎上增加 16 GB。
- 對於 15–20 TB 的儲存，請在上表*列出*的最小RAM 基礎上增加 32 GB。

通信頻道要求

您必須確保 Central Node 伺服器與每個網段之間有足夠的通訊頻道頻寬，具體取決於網段中Endpoint Agent 主機數量。下表列出了頻寬需求，取決於 Endpoint Agent 主機數量。

通訊頻道頻寬取決於 Endpoint Agent 主機的數量

Endpoint Agent 的最大有效數量	為 Endpoint Agent 保留的通訊頻道所需頻寬(Mbps)
10	1
50	2
100	3
1000	20
10000	200

Central Node 伺服器的其他需求

Central Node 實體伺服器的其他硬體需求請參閱以下部分：設定與外部系統整合時 Central Node 元件的運算、使用 ICAP 功能時 Central Node 元件的計算、分散式解決方案和多租戶模式下 Central Node 元件的計算、部署為叢集的 Central Node 元件的計算。

使用 KATA 和 NDR 功能時對 Central Node 元件的計算

本節介紹使用 KATA 和 NDR 功能時，實體和虛擬 Central Node 伺服器的軟體和硬體需求。

Central Node 實體伺服器的硬體需求

Central Node 實體伺服器的硬體需求取決於以下條件：

- 處理的流量

  與未加密流量（來自 SPAN 連接埠的標準流量）相比，Kaspersky Anti Targeted Attack Platform 對已解密的 SSL/TLS 流量的處理負載增加了 5 倍。在此情況下，要確定用於計算伺服器負載的已處理流量，請使用下列公式：

  <解密流量> = 5 * <未加密流量>

  ICAP 伺服器上處理的流量會根據"使用 ICAP 功能時對 Central Node 元件的計算"部分中的表格進行計算。

- 每秒處理的電子郵件數。

如果處理的流量大於 1 Gbps，則必須在獨立伺服器上安裝 Central Node 和 Sensor 元件。

下表列出了 Central Node 伺服器的硬體需求。

Central Node 實體伺服器的硬體需求

每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）			
					ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量
2	500	沒有處理	96	38	100	1000	2	4
2	1000	沒有處理	112	48	200	2000	2	4
5	沒有處理	2000	96	44	200	2000	3	4
20	沒有處理	4000	112	72	200	2000	3	4
20	沒有處理	7000	144	104	300	2500	4	4
20	沒有處理	10,000	160	140	300	2500	4	4

Kaspersky Anti Targeted Attack Platform 不支援軟體 RAID 陣列的操作。

如果要連接最多 1000 個 Endpoint Agent NDR，則 Central Node 伺服器的硬體需求與上表列出的類似。當連接超過 1000 個 Endpoint Agent NDR 時，您需要額外的 4 GB RAM 和 3 個邏輯核心。

在 VMware ESXi 虛擬平台上安裝此元件時，需要將最小邏輯核心數（Central Node 實體伺服器硬體需求表中指定的數值）增加 10%。

虛擬伺服器的其他硬體需求與實體伺服器的要求類似。

Central Node 虛擬伺服器的軟體需求

在虛擬磁碟設定中，必須選擇 Thick Provision Eager Zeroed 類型。

為了避免在虛擬平台上部署應用程式時可能出現的效能下降，您需要執行以下操作：

- 將延遲敏感度設定為“高”。

  如果您的 Hypervisor 不支援高延遲敏感性，您可以使用其他虛擬機優先權機制，例如 CPU Affinity 或資源預留。

- 保留所有記憶體。

- 保留所有 CPU。

Central Node 伺服器的其他需求

Central Node 實體伺服器的其他硬體需求請參閱以下部分：設定與外部系統整合時 Central Node 元件的運算、使用 ICAP 功能時 Central Node 元件的計算、分散式解決方案和多租戶模式下 Central Node 元件的計算、部署為叢集的 Central Node 元件的計算。

使用 KATA 和 NDR 功能時對 Central Node 元件的計算

本節介紹使用 KATA、KEDR 和 NDR 功能時，實體和虛擬 Central Node 伺服器的軟體和硬體需求。

Central Node 實體伺服器的硬體需求

Central Node 實體伺服器的硬體需求取決於以下條件：

- 處理的流量

  與未加密流量（來自 SPAN 連接埠的標準流量）相比，Kaspersky Anti Targeted Attack Platform 對已解密的 SSL/TLS 流量的處理負載增加了 5 倍。在此情況下，要確定用於計算伺服器負載的已處理流量，請使用下列公式：

  <解密流量> = 5 * <未加密流量>

  ICAP 伺服器上處理的流量會根據“使用 ICAP 功能時對 Central Node 元件的計算”部分中的表格進行計算。

- 每秒處理的電子郵件數

- Endpoint Agent 主機數量

  Endpoint Agent 元件可安裝在工作站、終端伺服器、檔案伺服器或網路附加儲存 (NAS) 上。

  以下“說明”部分提供了有關代表 Endpoint Agent 元件的應用程式版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性的資訊：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

若要確定具有 Endpoint Agent 元件的有效主機數量來計算伺服器負載，可以使用下列公式：

```
K = A+2*B+3*C+20*D
```

其中

- “K”是具有 Endpoint Agent 元件的主機的最大數量。
- “A”是運行安裝了 Endpoint Agent 元件的 Windows 作業系統的終端伺服器的工作站和使用者數量。
- “B”是運行安裝了 Endpoint Agent 元件的 Linux 作業系統的終端伺服器的工作站和使用者數量。
- “C”是執行 macOS 作業系統並安裝了 Endpoint Agent 元件的終端伺服器的工作站和使用者數量。
- “D”是伺服器數量。

如果處理的流量大於 1 Gbps，則必須在獨立伺服器上安裝 Central Node 和 Sensor 元件。

下表列出了 Central Node 伺服器的硬體需求。

連線最多 1000 個 Endpoint Agent NDR 元件時Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
						ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	1	200	沒有處理	160	36	100	1000	1.9	4	300	500
2000	2	500	沒有處理	160	48	100	1000	2	4	700	900
5000	1	1000	沒有處理	224	72	100	1000	2	4	1000	1200
10000	2	1000	沒有處理	256	80	100	1000	2	4	1500	1400
5000	5	沒有處理	2000	192	72	100	1000	1.9	4	1000	1000
10000	20	沒有處理	4000	256	104	100	1000	1.9	4	1500	1300
15000	20	沒有處理	4000	320	120	100	1000	1.9	4	1500	1700
15000	20	沒有處理	7000	352	160	100	1000	1.9	4	1500	1700
15000	20	沒有處理	10000	384	192	100	1000	1.9	4	1500	1700

連線最多 2000 個 Endpoint Agent NDR 元件時Central Node 實體伺服器的硬體需求

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
						ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
1000	1	200	沒有處理	160	40	100	1000	1.9	4	300	500
2000	2	500	沒有處理	160	52	100	1000	2	4	700	900
5000	1	1000	沒有處理	224	72	100	1000	2	4	1000	1200
10000	2	1000	沒有處理	288	88	100	1000	2	4	1500	1400
5000	5	沒有處理	2000	192	72	100	1000	1.9	4	1000	1000
10000	20	沒有處理	4000	256	112	100	1000	1.9	4	1500	1300
15000	20	沒有處理	4000	320	128	100	1000	1.9	4	1500	1700

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	嵌入式 Sensor 上的最大 SPAN 流量 (Mbps)	獨立 Sensor 上的最大 SPAN 流量 (Mbps)	最小 RAM (GB)	3 GHz 時的最小邏輯核心數	第一個磁碟子系統（RAID 1 或 RAID 10）				第二個磁碟子系統（有快取和電池的 RAID 10 或硬體 RAID 5）	
						ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）	磁碟陣列大小 (TB)	陣列中的磁碟數量	ROPS（每秒讀取操作數）	WOPS（每秒寫入操作數）
15000	20	沒有處理	7000	352	160	100	1000	1.9	4	1500	1700
15000	20	沒有處理	10000	384	192	100	1000	1.9	4	1500	1700

Kaspersky Anti Targeted Attack Platform 不支援軟體 RAID 陣列的操作。

Central Node 虛擬伺服器的硬體需求

以下值適用於將安裝在執行 Windows 作業系統的工作站和終端伺服器上的 10000 個 Endpoint Agent 連線到 Central Node 的情況。

在 VMware ESXi 虛擬平台上安裝此元件時，需要將最小邏輯核心數（Central Node 實體伺服器硬體需求表中指定的數值）增加 10%。

虛擬伺服器的其他硬體需求與實體伺服器的要求類似。

Central Node 虛擬伺服器的軟體需求

在虛擬磁碟設定中，必須選擇 Thick Provision Eager Zeroed 類型。

為了避免在虛擬平台上部署應用程式時可能出現的效能下降，您需要執行以下操作：

- 將延遲敏感度設定為“高”。

  如果您的 Hypervisor 不支援高延遲敏感性，您可以使用其他虛擬機優先權機制，例如 CPU Affinity 或資源預留。

- 保留所有記憶體。
- 保留所有 CPU。

Central Node 伺服器上第二個磁碟子系統的容量需求

第二個磁碟子系統的總最小有效儲存容量使用以下公式計算：

E = 1,5 * (P+T+S+N)

其中

- “E”是第二個磁碟子系統的總最小有效大小。
- P 是持久性儲存容量，可使用下列公式計算：

  30 MB * <具有 Endpoint Agent 元件的主機的有效數量> * <儲存天數>

  永久儲存容量不得超過 20 TB。
- T 是暫時儲存容量，使用下列公式計算：

  27 MB * <具有 Endpoint Agent 元件的主機的有效數量>
- S 是系統檔案的大小，為 150 GB。
- N 是 NDR 儲存容量，使用以下公式計算：

  (<連線到 NDR 功能塊的 Endpoint Agent 元件數量> * 0.02 GB + <來自 SPAN 連接埠的流量 (Gbps)> * 10 GB) * <您要儲存多少天 NDR 資料, = 7>。

根據持久儲存的大小，需要額外的 RAM:

- 對於 10–15 TB 的儲存，請在上表列出的最小RAM 基礎上增加 16 GB。
- 對於 15–20 TB 的儲存，請在上表列出的最小RAM 基礎上增加 32 GB。

該公式可用於粗略估計所需的磁碟空間。實際儲存的資料量取決於組織的流量概況，並且可能與計算結果不同。

通信頻道要求

您必須確保 Central Node 伺服器與每個網段之間有足夠的通訊頻道頻寬，具體取決於網段中Endpoint Agent 主機數量。下表列出了頻寬需求，取決於 Endpoint Agent 主機數量。

通訊頻道頻寬取決於 Endpoint Agent 主機的數量

Endpoint Agent 的最大有效數量	為 Endpoint Agent 保留的通訊頻道所需頻寬(Mbps)
10	1
50	2
100	3
1000	20
10000	200

Central Node 伺服器的其他需求

Central Node 實體伺服器的其他硬體需求請參閱以下部分：設定與外部系統整合時 Central Node 元件的運算、使用 ICAP 功能時 Central Node 元件的計算、分散式解決方案和多租戶模式下 Central Node 元件的計算、部署為叢集的 Central Node 元件的計算。

配置與外部系統整合時 Central Node 元件的計算

如果您已配置使用 REST API 掃描內部系統物件的整合，則需要提高“使用 KATA 功能時 Central Node 元件的計算”、“KEDR”、“KATA 和 KEDR”、“ KATA 和 NDR”、“KATA、KEDR 和 NDR”章節中所述的 Central Node 實體伺服器的硬體需求。其他硬體需求如下表所示。

與外部系統整合的 Central Node 實體伺服器的硬體需求

每秒處理的最大物件數	其他邏輯核心數	附加 Sandbox 伺服器的數量
8	2	1
16	4	2
24	7	3

如果您配置了整合以使用 REST API 將事件傳送到外部系統，則必須提高對 Central Node 伺服器的硬體需求，增加 1 個邏輯核心和 6 GB RAM。

與 Kaspersky Secure Mail Gateway 整合時 Central Node 元件的計算

下表列出了使用 KATA 功能和與 Kaspersky Secure Mail Gateway 2.1.1 整合時 Central Node 實體伺服器的硬體需求。

使用 KATA 功能和與 Kaspersky Secure Mail Gateway 2.1.1 整合時 Central Node 實體伺服器的硬體需求

每秒的最大電子郵件數	SPAN 連接埠的最大流量 (Mbps)	磁碟			
		最小 RAM (GB)	最小邏輯核心數	邏輯核心時脈頻率	WOPS（每秒寫入操作數）
1	10000	36	4	1.15	200
2	10000	36	4	1.15	200
5	10000	36	6	1.15	200
10	10000	36	10	1.15	200
20	10000	36	12	1.5	200
30	10000	36	16	2.7	200
50	10000	36	20	2.7	200
100	10000	36	40	2.7	200

使用 ICAP 功能時對 Central Node 元件的計算

下表中的**AV_rps**值代表每秒傳送用於病毒防護掃描的檔案數。

平均而言，每秒 1 Mbps 的流量會建立兩個病毒防護掃描作業。ICAP 請求總數不得超過每秒 5000 個。

Central Node 實體伺服器的配置

低：AV_rps 最高 65；75 Mbps	
最小邏輯核心數	16

最小 RAM	64 GB
第一個磁碟子系統 (RAID 10)	4 個磁碟機，每個 1200 GB
中：AV_rps 最高 250；0.3 Gbps	
最小邏輯核心數	32
最小 RAM	80 GB
第一個磁碟子系統 (RAID 10)	4 個磁碟機，每個 1200 GB
高：AV_rps 最高 750；1 Gbps	
最小邏輯核心數	72
最小 RAM	96 GB
第一個磁碟子系統 (RAID 10)	4 個磁碟機，每個 1200 GB

分佈式解決方案和多租戶模式下 Central Node 元件的計算

您最多可以將 150 台 SCN 連線到一台 PCN。

如果要將最多 10 個 SCN 連線到一個 PCN，PCN 伺服器上的最小 RAM 量和最小邏輯內核數必須比未處於分佈式解決方案模式的 Central Node 伺服器上的 RAM 量和邏輯內核數高 20%。SCN 上的負載可以在 Central Node 伺服器的硬體需求中指定的限制範圍內變更。

當將 11 到 150 個 SCN 連線到一個 PCN 時，必須滿足以下條件：

- 最多可有 5000 個 Endpoint Agent（最大有效數量）連線到一個 SCN 伺服器。
- PCN 伺服器的硬體配置需符合以下要求：
  - <Central Node 伺服器硬體要求中列出的最小邏輯核心數> + 10。
  - <Central Node 伺服器硬體要求中列出的最小 RAM> + 32。
  - <Central Node 伺服器硬體需求中列出的 ROPS> + 1500。
  - <Central Node 伺服器硬體需求中列出的 WOPS> + 3000。

如果您只想將 PCN 用於 SCN 管理，而不打算將其連線到外部資料來源（例如 Endpoint Agent 或外部系統），則 PCN 實體伺服器可以採用下列配置：

- CPU：
  - 時脈頻率：2.5 GHz。
  - 執行緒數：20。
  - 核心數量：10。
- RAM：80 千兆位元組 (GB)。
- 2 個 SSD (寫入密集型 (WI))。

以下部分提供了 Central Node 元件的計算：

- *使用 KATA 功能時對 Central Node 元件的計算*。
- *使用 KEDR 功能時對 Central Node 元件的計算*。
- *使用 KATA 和 KEDR 功能時對 Central Node 元件的計算*。
- *使用 KATA 和 NDR 功能時對 Central Node 元件的計算*。
- *使用 KATA、KEDR 和 NDR 功能時對 Central Node 元件的計算*。

PCN 和 SCN 伺服器之間通訊頻道的最低要求

分佈式解決方案模式下 PCN 和 SCN 伺服器之間通訊通道的最低要求如下表所示。

PCN 和 SCN 伺服器之間通訊頻道的最低要求

Endpoint Agent 的最大有效數量	每秒的最大電子郵件數	SPAN 連接埠的最大流量 (Mbps)	所需通訊頻道頻寬 (Mbps)
5000	5	2000	20
10000	20	4000	30

作為叢集部署的 Central Node 元件的計算

一個叢集必須至少包含 4 台伺服器：2 台儲存伺服器和 2 台處理伺服器。如果您有多達 15000 個已連線的 Endpoint Agent 元件，則至少需要 2 台處理伺服器。如果您有 15000 到 30000 個已連線的 Endpoint Agent 元件，則至少需要 3 台處理伺服器。儲存伺服器的數量取決於儲存資料所需的磁碟空間大小。

每台叢集伺服器必須有兩個網路介面卡來設定叢集和外部子網路。叢集子網路的速率必須高達 10 Gbps。

叢集子網路也必須滿足以下要求：

- 叢集子網路必須僅包含叢集伺服器和網路交換機。
- 叢集子網路必須被隔離。
- 叢集伺服器必須全部位於同一 L1 或 L2 網段中。為此，您可以將叢集中的所有伺服器連線到單個網路交換機或使用軟體隧道。例如，L2TPv3 或覆寫傳輸虛擬化 (OTV)。
- “網路延遲”值必須符合“個位數延遲”要求，即該值必須小於 10 毫秒。

下表列出了使用 KEDR 功能時叢集實體伺服器的硬體需求。

使用 KEDR 功能時處理伺服器的硬體需求

最小 RAM (GB)	最小邏輯核心數	RAID 磁碟陣列類型	RAID 磁碟陣列中的磁碟數	單硬碟容量 (GB)
256	48	RAID 1	2	1200

最小 RAM (GB)	最小邏輯核心數	第一個磁碟子系統			第二個磁碟子系統	
		RAID 磁碟陣列類型	RAID 磁碟陣列中的磁碟數	單硬碟容量 (GB)	磁碟數量	單硬碟容量 (GB)
128	16	RAID 1	2	1200	至少 6	至少 1200

我們建議兩個磁碟子系統使用相同大小的磁碟。對於第二個磁碟子系統，您必須使用未組合成RAID 陣列的磁碟。

磁碟子系統的效能需求與"*使用 KEDR 功能時具有 Central Node 元件的伺服器的硬體需求*"部分中指定的要求相同。

解決方案小規模配置的計算

本節介紹具有 50 到 750 個已連線 Endpoint Agent 的 Central Node 伺服器的硬體和軟體需求。

要在 KVM 虛擬平台上部署應用程式，需要使用 QEMU 8.0.2 安裝基於 Debian GNU/Linux 12 作業系統的 KVM Hypervisor。

VMware ESXi 虛擬平台的軟體需求在*硬體和軟體需求*部分提供。

在虛擬平台上部署 Central Node 時，您必須記住以下限制：

- KVM：
  - 該應用程式只能使用 Ubuntu 安裝檔案進行安裝。
  - 只能安裝應用程式的非高可用性版本。
  - 僅可使用嵌入式 Sensor。
  - 您只能連線部署在實體伺服器上的 KVM 虛擬化平台以外或另一個受支援的虛擬化平台上的 Sandbox 元件。
  - 對於虛擬基礎架構中部署的每個 Central Node 伺服器，必須使用單獨的網路介面來接收映像 SPAN 流量。
  - 外部系統無法使用 API 取得警示資訊和應用程式事件。
  - 不保證支援雲端解決方案中使用的 KVM 虛擬化。
  - 在虛擬機設定中，CPU 設定中的 **Type**參數必須設定為 **host** 值，網路介面卡設定中**的 model**參數必須設定為**VMware vmxnet3**值。
- VMware ESXi：
  - 只能安裝應用程式的非高可用性版本。
  - 僅可使用嵌入式 Sensor。
  - 對於虛擬基礎架構中部署的每個 Central Node 伺服器，必須使用單獨的網路介面來接收映像 SPAN 流量。

下表列出了根據所使用的功能對 Central Node 伺服器的硬體需求。

使用 KEDR 功能時對 Central Node 伺服器的硬體需求

Endpoint Agent 的最大有效數量	每分鐘的最大電子郵件數	來自具有 Central Node 元件的伺服器上的 SPAN 連接埠的最大流量 (Mbps)	3 GHz 時的最小邏輯核心數	最小 RAM (GB)
50	0	0	4	31
100	0	0	4	31
150	0	0	6	31*/32
250	0	0	6	31/32
500	0	0	8	31/34
750	0	0	10	31/38

* 斜線前的值表示安裝 Central Node 元件所需的 RAM 數量。安裝後，必須將 RAM 數量增加到斜線後的值。

使用 KATA 和 KEDR 功能時對 Central Node 伺服器的硬體需求

Endpoint Agent 的最大有效數量	每分鐘的最大電子郵件數	來自具有 Central Node 元件的伺服器上的 SPAN 連接埠的最大流量 (Mbps)	3 GHz 時的最小邏輯核心數	最小 RAM (GB)
100	1	20	6	31*/32
250	5	50	6	31/32
500	30	100	12	31/40
750	30	100	12	31/46

* 斜線前的值表示安裝 Central Node 元件所需的 RAM 數量。安裝後，必須將 RAM 數量增加到斜線後的值。

若要確定具有 Endpoint Agent 元件的有效主機數量來計算伺服器負載，可以使用下列公式：

```
K = A+2*B+3*C+20*D
```

其中

- “K”是具有 Endpoint Agent 元件的主機的最大數量。
- “A”是運行安裝了 Endpoint Agent 元件的 Windows 作業系統的終端伺服器的工作站和使用者數量。
- “B”是運行安裝了 Endpoint Agent 元件的 Linux 作業系統的終端伺服器的工作站和使用者數量。
- “C”是執行 macOS 作業系統並安裝了 Endpoint Agent 元件的終端伺服器的工作站和使用者數量。
- “D”是伺服器數量。

以下“說明”部分提供了有關代表 Endpoint Agent 元件的應用程式版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性的資訊：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

計算事件資料庫和儲存空間的大小，以配置應用程式延伸參數

如果在伺服器上安裝了 Central Node（不是作為高可用性叢集），則在配置大小調整參數時，必須使用以下公式計算“**事件資料庫，GB**”和“**儲存，GB**”參數的磁碟空間：

A = F - R，GB。

其中

- A 是事件資料庫和儲存所使用的空間。
- F 是安裝 Central Node 元件的硬碟的大小。
- R 是第二個磁碟子系統上根據連線的具有 Endpoint Agent 元件的主機數量保留的可用空間量(GB)；此參數取自下表。

  Endpoint Agent 元件可安裝在工作站、終端伺服器、檔案伺服器或網路附加儲存 (NAS) 上。

  若要確定具有 Endpoint Agent 元件的有效主機數量來計算伺服器負載，可以使用下列公式：

  ```
  K = A+2*B+3*C+20*D
  ```

  其中

  - "K"是具有 Endpoint Agent 元件的主機的最大數量。
  - "A"是運行安裝了 Endpoint Agent 元件的 Windows 作業系統的終端伺服器的工作站和使用者數量。
  - "B"是運行安裝了 Endpoint Agent 元件的 Linux 作業系統的終端伺服器的工作站和使用者數量。
  - "C"是執行 macOS 作業系統並安裝了 Endpoint Agent 元件的終端伺服器的工作站和使用者數量。
  - "D"是伺服器數量。

  以下"說明"部分提供了有關代表 Endpoint Agent 元件的應用程式版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性的資訊：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

如果連線到 Central Node 的 Endpoint Agent 元件數量介於列出的值之間，請在計算中使用較大的數字。

根據 Endpoint Agent 元件數量預留的可用空間量

Endpoint Agent 的最大有效數量	預留的可用空間量 (GB)
1000	1000
3000	1200
5000	1400
10000	1900
15000	2400

Sandbox 元件計算

具有 Sandbox 元件的伺服器的硬體需求取決於已處理流量的類型和數量以及允許的物件掃描時間。

預設情況下，允許的物件掃描時間為 1 小時。為了縮短這一時間，您需要使用更強大的伺服器或具有 Sandbox 元件的多台伺服器。

建議如下計算 Sandbox 元件的配置：

1. 在一台伺服器上安裝 Central Node 和 Sensor 元件，在另一台伺服器上安裝 Sandbox 元件，以便對應用程式進行試運行。

   為了獲得足夠的統計資料，應用程式必須處理該組織的流量一週。

2. 透過執行以下命令來執行資料記錄指令碼：

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

   `--output-dir <目錄路徑>`

   當指令碼完成執行後，*collect.tar.gz* 壓縮檔案將被移至指定目錄。

3. 將此壓縮檔案轉發給卡巴斯基工作人員進行分析。

> 如果同時啟動多個虛擬機，則會增加從佇列處理物件的速度。

AMD 處理器不支援 Sandbox 元件。

託管 Sandbox 元件的伺服器的硬體需求

使用作業系統預設映像時，具有 Sandbox 元件的伺服器數量的計算如下表所示。

使用作業系統預設映像時 Sandbox 元件的硬體需求

每秒的最大電子郵件數	SPAN 連接埠的最大流量 (Mbps)	具有 Endpoint Agent 元件的最大電腦數量	具有 Sandbox 元件的實體伺服器的數量	
			使用所有映像時	僅使用兩個 Linux 映像時
1	200	1000	1	1
2	500	3000	1	1
1	1000	5000	1	1
5	2000	5000	1	1
20	4000	10000	2	1
20	7000	15000	4	2
20	10000	15000	5	2

如果要在 VMware ESXi 虛擬機上安裝 Sandbox 元件，則需要 5 倍的虛擬伺服器才能獲得與實體伺服器相同的效能。在 Brest、“RED Virtualization”或“zVirt Node”虛擬平台上安裝 Sandbox 元件時，需要 13 倍的伺服器。考慮到需要配置物件掃描持續時間，給出了伺服器數量的估計值。

如果您對 Sandbox 伺服器使用自訂映像，則可能需要額外的容量。要計算使用自訂作業系統映像時所需的實體 Sandbox 伺服器數量，可以使用下列公式：

`<根據使用者定義的 Sandbox 規則每小時需要處理的檔案數量> * <自訂作業系統映像數量> / 1000`

若要計算使用自訂作業系統映像時所需的帶有 Sandbox 元件的 VMware ESXi 虛擬機的數量，您可以使用下列公式：

`<根據使用者定義的 Sandbox 規則每小時需要處理的檔案數量> * <自訂作業系統映像數量> / 200`

在“Brest”或 zVirt Node 虛擬化平台上安裝Sandbox 元件時，可以使用下列公式計算使用自訂作業系統映像時所需的虛擬機數量：

具有 `Sandbox` 元件的實體伺服器的數量> `* 5 * 2.6`

在 RED 虛擬化平台上安裝 Sandbox 元件時，可以使用以下公式計算使用自訂作業系統映像時所需的虛擬機數量：

<具有 `Sandbox` 元件的實體伺服器的數量> `* 5 * 2.5`

有關具有 Sandbox 元件的實體伺服器數量，請參閱上面的*使用預設作業系統映像時 Sandbox 元件的硬體需求表*。

列出了具有以下配置的伺服器的 Sandbox 伺服器數量的估計值：

- 在實體伺服器上安裝 Sandbox 元件時：
  - 2 個 CPU：2.6 GHz 或更高頻率的 Intel® Xeon® 8 Core™ (HT)
  - 80 GB RAM
  - 2 個 HDD，每個 300 GB，組合成 RAID 1 陣列

  在此配置的實體伺服器上安裝 Sandbox 元件時，您需要設定同時執行的虛擬機數量限制為 48。

- 在虛擬機上安裝 Sandbox 元件時：
  - Intel Xeon 15 Core (HT) CPU，主頻為 2.1 GHz 或更高

    在“Brest”、zVirt Node 或 RED 虛擬化平台上安裝Sandbox 元件時，我們建議使用 Ice Lake 一代或更高版本的 Intel 處理器。
  - 32 GB RAM。
  - 300 GB HDD。

    在虛擬機上：

    1. 嵌套虛擬化已啟用。
    2. 啟用高延遲敏感度設定（僅當在 VMware ESXi 虛擬機上安裝時）。
    3. 整個 RAM 被保留。
    4. 整個 CPU 頻率被保留。

  在此配置的虛擬機器上安裝 Sandbox 元件時，您需要將同時執行的虛擬機數量限制設定為 12 個。

  如果您打算使用自訂作業系統映像，我們建議將磁碟空間增加到 600 GB 或更多。

安裝和執行應用程式的初始配置

本節包含 Kaspersky Anti Targeted Attack Platform 的安裝和初始設定說明。

元件存在許多限制。我們建議在安裝應用程式之前先了解這些內容。

準備安裝應用程式元件

本節提供有關如何為安裝 Kaspersky Anti Targeted Attack Platform 元件準備企業 IT 基礎架構的資訊。

準備 IT 基礎架構以安裝應用程式元件

本節介紹安裝應用程式之前必須配置的連接埠。為了應用程式元件在安裝後能夠正確運行，您必須配置防火牆規則。

在安裝應用程式前，請準備企業 IT 基礎架構以安裝 Kaspersky Anti Targeted Attack Platform 元件：

1. 確保伺服器、要使用應用程式 Web 介面的電腦以及要安裝“Endpoint Agent”元件的電腦均符合硬體和軟體要求。
2. 為了防護網路免受被分析物件的攻擊，拒絕管理網路介面和用於處理物件的網際網路存取的網路介面存取 Sandbox 伺服器的本機網路。
3. 請依照下表準備企業 IT 基礎架構：

Kaspersky Anti Targeted Attack Platform 元件之間互動的連接埠

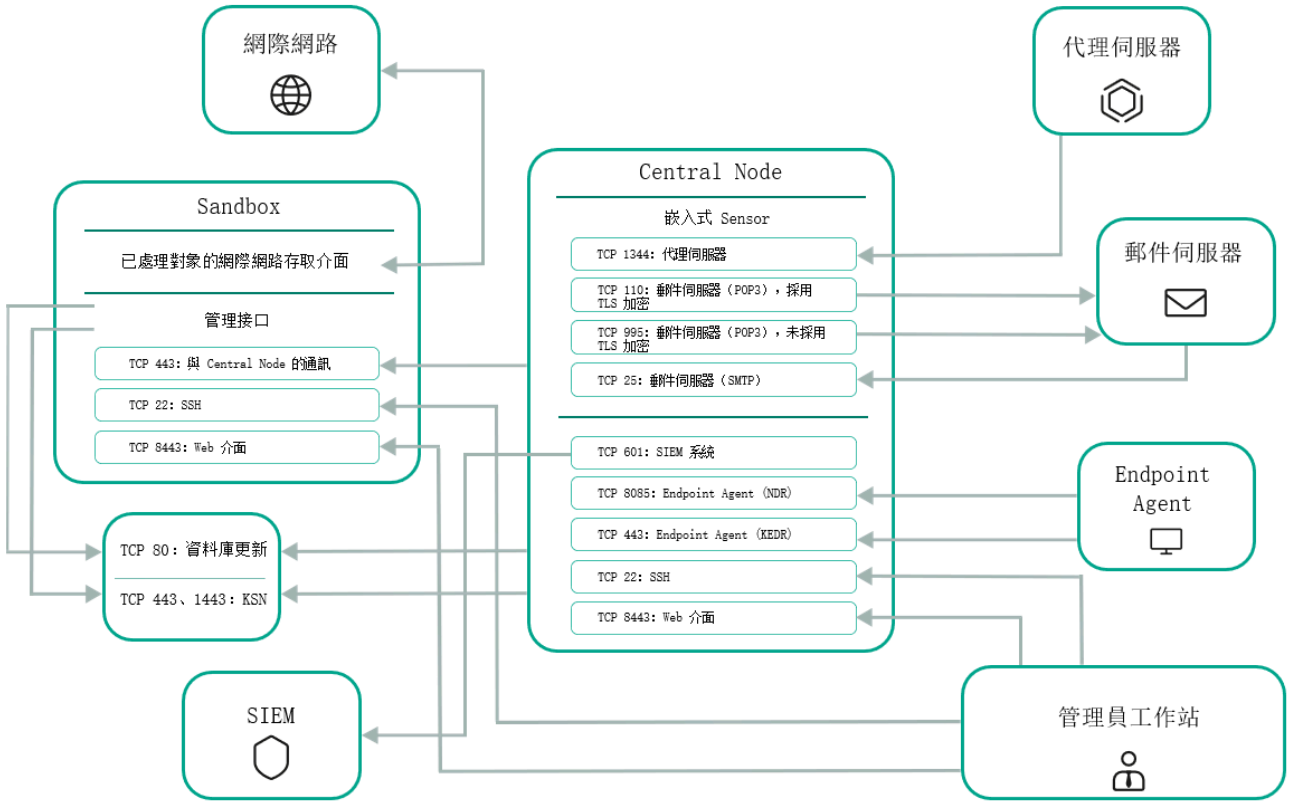
來源	方向	連接埠或協定	敘述
Central Node	傳入	TCP 22	透過 SSH 連線到伺服器
		TCP 443	從 Endpoint Agent (KEDR) 接收資料
		TCP 8085	從 Endpoint Agent (NDR) 接收資料
		TCP 8443	存取應用程式的 Web 介面
		TCP 7423、8443、9081、13520	與 Sensor 伺服器的通信
		UDP 53	
	傳出	TCP 80 TCP 443 TCP 1443	與 KSN 伺服器和卡巴斯基更新伺服器的通信
		TCP 443	將物件傳送到 Sandbox 進行掃描
		TCP 601	向 SIEM 系統傳送訊息
		TCP 9443	與 Sensor 伺服器的通信
		UDP 53	
	傳入和傳出	ESP	用於透過基於 IPSec 協定的安全鏈路在 Central Node 和 Sensor 之間進行互動

來源	方向	連接埠或協定	敘述
Sensor	傳入	TCP 22	透過 SSH 連線到伺服器
		TCP 1344	從代理伺服器接收流量
		TCP 25	從郵件伺服器接收 SMTP 流量
		TCP 443	當 Sensor 用作代理伺服器，用於在具有 Endpoint Agent 的工作站和 Central Node 之間進行通訊時
		TCP 8085	從 Endpoint Agent (NDR) 接收資料
		TCP 9444	存取元件的 Web 介面。該連接埠預設是關閉的。
		TCP 9443	與 Central Node 伺服器的通信
		UDP 53	
	傳出	TCP 80 TCP 443	與 KSN 伺服器和卡巴斯基更新伺服器的通信
		TCP 995	與郵件伺服器整合以實現安全連線
		TCP 110	與郵件伺服器整合以輔助不安全的連線
		TCP 7423、8443、9081、13520	與 Central Node 伺服器的通信
		UDP 53	
	傳入和傳出	ESP	用於透過基於 IPSec 協定的安全鏈路在 Central Node 和 Sensor 之間進行互動
Sandbox	傳入（管理 介面）	TCP 22	透過 SSH 連線到伺服器
		TCP 443	與 Central Node 互動
		TCP 8443	存取應用程式的 Web 介面
	傳出（管理接口）	TCP 80 TCP 443	與卡巴斯基更新伺服器通訊
	傳出和對應的傳入（所處理物件的存取介面）	任何	存取網際網路以分析已處理物件的網路行為。 拒絕存取企業區域網路以防護網路免受被分析物件的攻擊。
SCN（使用分佈式解模式時）	傳出	TCP 8443、8444	用於透過基於 IPSec 協定的安全鏈路在 SCN 和 PCN 之間進行互動
	傳入和傳出	TCP 443、53、11000:11006、UDP 53 ESP	
PCN（使用分佈式解決方案模式時）	傳入	TCP 8443、8444	
	傳入和傳出	TCP 443、53、11000:11006、UDP 53 ESP	

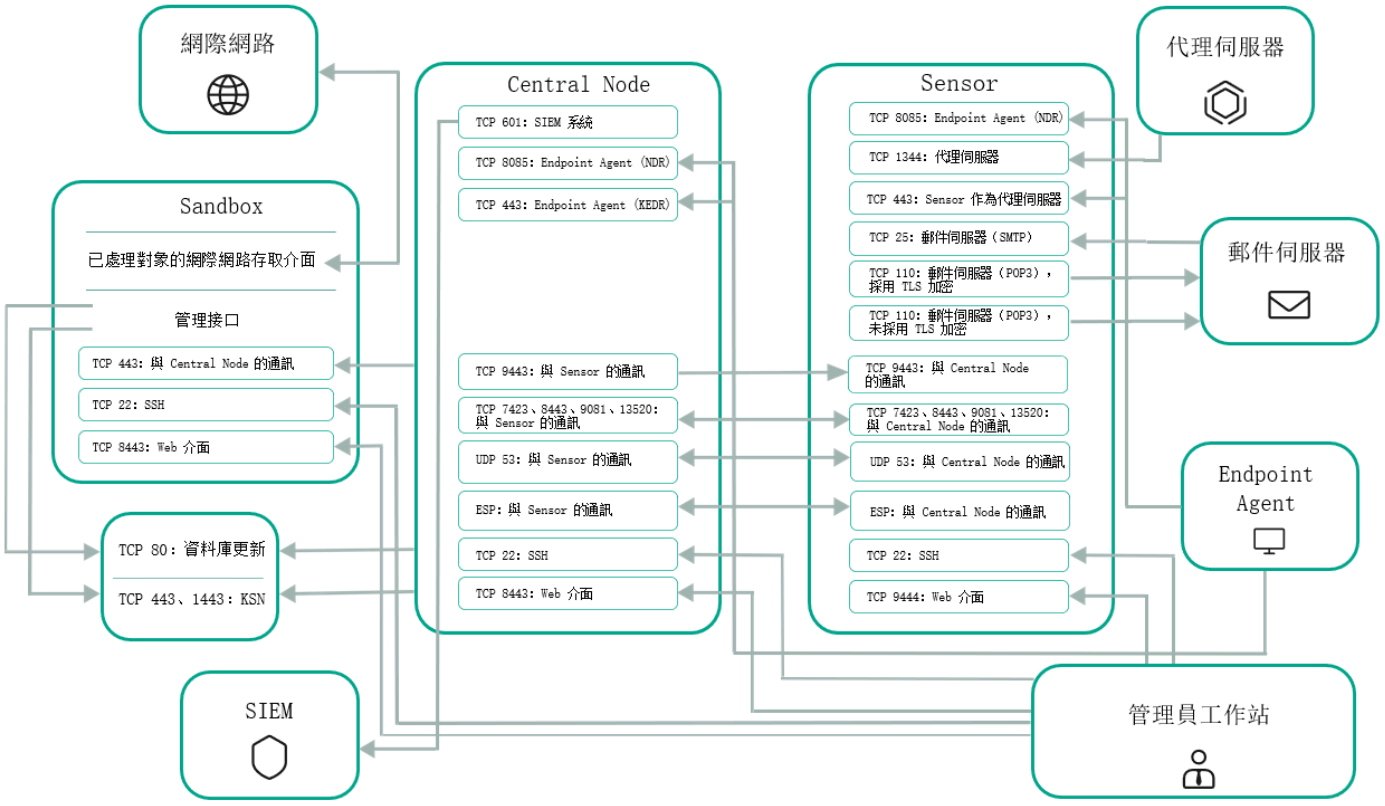
如果在 VMware ESXi™ 虛擬環境中安裝僅接收映像流量的其他網路介面，請使用 E1000 網路介面卡或停用 VMXNET3 網路介面卡上的 LRO（大量接收減負）選項。

為了讓 Central Node、Sensor、PCN 和 SCN 之間的連線正常運作，必須將安裝了元件的伺服器放置在同一子網路中。不支援網路位址轉換 (NAT)。此限制不適用於 Endpoint Agent 元件，這些元件可以位於與 Central Node 子網路分離的子網路中。

下圖展示了應用程式元件與應用程式所依賴的系統之間的網路通訊圖。圖中的箭頭表示連結的方向：每個箭頭從發起連線的物件指向回應的物件。



應用程式元件與應用程式所依賴的系統之間的網路通訊圖。用嵌入式 Sensor 部署的 Central Node



應用程式元件與應用程式所依賴的系統之間的網路通訊圖。部署在與 Central Node 不同的伺服器上的 Sensor

為透過 POP3 與用於接收訊息的郵件伺服器整合準備 IT 基礎架構

如果使用 Microsoft Exchange 郵件伺服器作為您的郵件伺服器，且電子郵件寄件者配置了閱讀回執通知要求，則必須停用閱讀回執通知。否則，閱讀回執通知將從您配置用於 Kaspersky Anti Targeted Attack Platform 接收郵件的電子郵件信箱傳送出去。您也必須停用自動處理會議要求，以防止佔用 Kaspersky Anti Targeted Attack Platform 接收郵件的信箱。

若要停用傳送來自 Kaspersky Anti Targeted Attack Platform 接收郵件的電子郵件信箱的閱讀回執通知：

1. 在 Microsoft Exchange 伺服器上，檢查通知是否已啟用。為此，請執行以下命令：

   `Get-MailboxMessageConfiguration -Identity<Kaspersky Anti Targeted Attack Platform 接收郵件的电子邮件信箱> | fl`

2. 如果通知已啟用，請執行以下命令：

   `Set-MailboxMessageConfiguration -Identity<Kaspersky Anti Targeted Attack Platform 接收郵件的电子邮件信箱> -ReadReceiptResponse NeverSend`

這將停用來自 Kaspersky Anti Targeted Attack Platform 接收郵件的電子郵件信箱的閱讀回執通知。

若要停用自動處理會議請求：

1. 在 Microsoft Exchange 伺服器上，檢查通知是否已啟用。為此，請執行以下命令：

   `Get-CalendarProcessing -Identity<Kaspersky Anti Targeted Attack Platform 接收郵件的电子邮件信箱> | fl`

2. 如果自動處理會議請求已啟用，請執行下列命令：

   `Set-CalendarProcessing -Identity<Kaspersky Anti Targeted Attack Platform 接收郵件的电子邮件信箱> -AutomateProcessing:None`

這將停用自動處理會議請求。

為透過 SMTP 與郵件伺服器整合準備 IT 基礎架構

若要為透過 SMTP 協定整合Kaspersky Anti Targeted Attack Platform 與郵件伺服器而準備企業 IT 基礎架構：

1. 在外部郵件伺服器上設定規則，以便將要傳送的用於 Kaspersky Anti Targeted Attack Platform 掃描的郵件副本轉送至 Kaspersky Anti Targeted Attack Platform 指定的位址中。

2. 指定將電子郵件轉送至 Sensor 伺服器的路由。

   建議指定一個靜態路由 — Sensor 伺服器的 IP 位址。

3. 配置組織的防火牆以允許從正在轉送電子郵件資訊副本的郵件伺服器到 Sensor 伺服器連接埠 25 的傳入連線。

您也可以透過 SMTP 協定提高 Kaspersky Anti Targeted Attack Platform 與郵件伺服器整合的安全性。

若要透過 SMTP 協定提高 Kaspersky Anti Targeted Attack Platform 與郵件伺服器整合的安全性。

1. 在為 Kaspersky Anti Targeted Attack Platform 轉送電子郵件的郵件伺服器端，設定 Kaspersky Anti Targeted Attack Platform 伺服器的認證。

2. 在為 Kaspersky Anti Targeted Attack Platform 轉送電子郵件的郵件伺服器上配置強制加密流量。

3. 在 Kaspersky Anti Targeted Attack Platform 端，配置為 Kaspersky Anti Targeted Attack Platform 轉送電子郵件的郵件伺服器的認證。

準備虛擬機以安裝 Sandbox 元件

準備虛擬機以安裝 Sandbox 元件：

1. 執行 VMware ESXi hypervisor。

2. 開啟虛擬機管理主控台。

3. 在要安裝 Sandbox 元件的虛擬機右鍵功能表中，選擇**編輯設定**。

   這將開啟虛擬機屬性視窗。

4. 在**虛擬硬體**索引標籤上，展開**CPU**設定群組並勾選**向來賓作業系統公開硬體輔助虛擬化**核取方塊。

5. 在**虛擬機選項**索引標籤上的**延遲敏感度**下拉清單中，選擇**高**。

6. 點擊**確定**。

虛擬機已準備好安裝 Sandbox 元件。

準備包含 Central Node、Sensor 和 Sandbox 元件的安裝磁碟映像

在安裝應用程式之前，您需要準備好基於 Astra Linux 作業系統的安裝碟 iso 映像，其中包含 Central Node、Sensor 和 Sandbox 元件。

可用於建立 iso 映像的裝置的最低硬體需求：

- CPU：4 核，時脈頻率 2500 MHz 或更高。

- RAM：8 千兆位元組 (GB)。

- 可用磁碟空間：100 GB。

軟體要求：

- 基於最新 Linux 核心的作業系統。

- Docker 20 或更高版本

- 一個**不包含** Debian 安裝程式的 Astra Linux Special Edition 1.8.1.16 ISO 映像（映像名稱中沒有“-di”）。本部分內容將該映像稱為 `astra-installation.iso`。

> Kaspersky Anti Targeted Attack Platform 不支援其他版本的 Astra Linux 作業系統。

您可以建立以下版本的 Central Node 和 Sensor 元件的 ISO 映像：

- 7.1.1.531（已認證版本）。
- 7.1.2.532（未認證版本）。
- 7.1.3.533（未認證版本）。
- 7.1.7.537.1（未認證版本）。

執行以下說明中的命令時，請將“<元件版本號>”變數替換為您的版本號。若要建立特定版本的 ISO 映像，您必須依序執行所有步驟。

要掛載基於 Astra Linux 作業系統、包含 Central Node 和 Sensor 或 Sandbox 元件的 iso 映像：

1. 從分發套件下載以下檔案：

   a. 名為 kata-cn-distribution-<元件版本號>-x86_64_en-ru-zh.tar.gz 的 Central Node 和 Sensor 分發套件。

   b. Sandbox 分發套件，kata-sb-distribution-7.1.0.530-x86_64_en-ru-zh.tar.gz

   c. 名為 iso-builder-7.1.7.537-x86_64_en-ru-zh.tar 的用於建立 ISO 映像的檔案。

2. 建立**包含以下內容**的 iso_builder.sh 檔案。

```
#!/bin/bash
usage="建置 KATA 安裝 ISO。
用法：
$(basename "$0") [-h] source_iso distribution iso_builder_image build target_iso_name
其中：
    -h, --help        - 顯示此文字並結束
    source_iso        - 來源作業系統 ISO 檔案的絕對路徑
    distribution      - KATA 分發壓縮檔案的絕對路徑
    iso_builder_image - iso_builder docker 映像的絕對路徑
    build             - 暫存版本目錄的絕對路徑
    target_iso_name   - 產生的 ISO 檔案的絕對路徑
"
if [ "$#" -eq 0 ] || [ "$1" == "-h" ] || [ "$1" == "--help" ]
then
    echo "$usage"; exit 10;
fi
if [ "$#" -lt 5 ]
then
    echo "錯誤：參數不足。請參閱說明文字。"; exit 11;
fi
docker load -i $3
docker run -v $1:$1 -v $2:$2 -v $4:/build kaspersky/kata/deployment/iso_builder:6.0 --
source-iso-uri file://$1 --kata-distribution-uri file://$2 --target-iso-name $5
```

3. 執行以下指令：

```
mkdir /var/kata_builder
```

4. 將步驟 1 中列出的檔案和 `astra-installation.iso` 映像放入新建立的 /var/kata_builder 目錄中。

5. 執行以下指令：

- 如果您正在準備包含 Central Node 和 Sensor 元件的磁碟映像：

  ```
  sudo ./iso_builder.sh /var/kata_builder/astra-installation.iso
  /var/kata_builder/kata-cn-distribution-<元件版本號>-x86_64_en-ru-zh.tar.gz
  /var/kata_builder/iso-builder-7.1.7.537-x86_64_en-ru-zh.tar /var/kata_builder
  buildCNSensorAstra.iso
  ```

- 如果您正在準備包含 Sandbox 的磁碟映像：

  ```
  sudo ./iso_builder.sh /var/kata_builder/astra-installation.iso
  /var/kata_builder/kata-sb-distribution-7.1.0.530-x86_64_en-ru-zh.tar.gz
  /var/kata_builder/iso-builder-7.1.7.537-x86_64_en-ru-zh.tar /var/kata_builder
  buildSandboxAstra.iso
  ```

執行指令後，包含 Central Node 和 Sensor 元件的安裝磁碟映像（名為buildCNSensorAstra.iso 和 buildSandboxAstra.iso）位於/var/kata_builder 目錄中。

如果將檔案保存在不同的目錄中，可以執行以下命令：

`sudo ./iso_builder.sh <Astra Linux Special Edition 1.8.1.16` 分發套件路徑`> <`元件分發套件`> <iso-builder-7.1.7.537-x86_64_en-ru-zh.tar` 檔案路徑`> <ISO` 映像的掛載路徑（不包含指派的 `ISO` 映像名稱）`> <`指派給 `ISO` 映像的名稱`>`

安裝和設定應用程式元件的步驟

安裝和設定應用程式涉及以下步驟：

1. **安裝帶有嵌入式 Sensor 的 Central Node**

   您可以按照以下配置之一安裝帶有嵌入式 Sensor 的 Central Node 元件：

   - 叢集。
   - 伺服器。

   如果有多個 Central Node 元件，則可以在分佈式解決方案模式下使用該應用程式。

2. **在與 Central Node 不同的伺服器上安裝 Sensor**

   如果有多個 Sensor 元件，則可以在必要數量的伺服器上安裝和設定 Sensor 元件。

3. **安裝套件含 Sandbox 元件的磁碟映像**

4. **配置 Central Node 和 Sensor 元件**

5. **透過 Sandbox Web 介面設定 Sandbox 元件**

6. **安裝 Microsoft Windows 作業系統和 Sandbox 元件應用程式的磁碟映像**

7. **在公司 IT 基礎架構的電腦上安裝 Endpoint Agent 元件。**

   作為 Endpoint Agent 元件，您可以使用下列應用程式：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

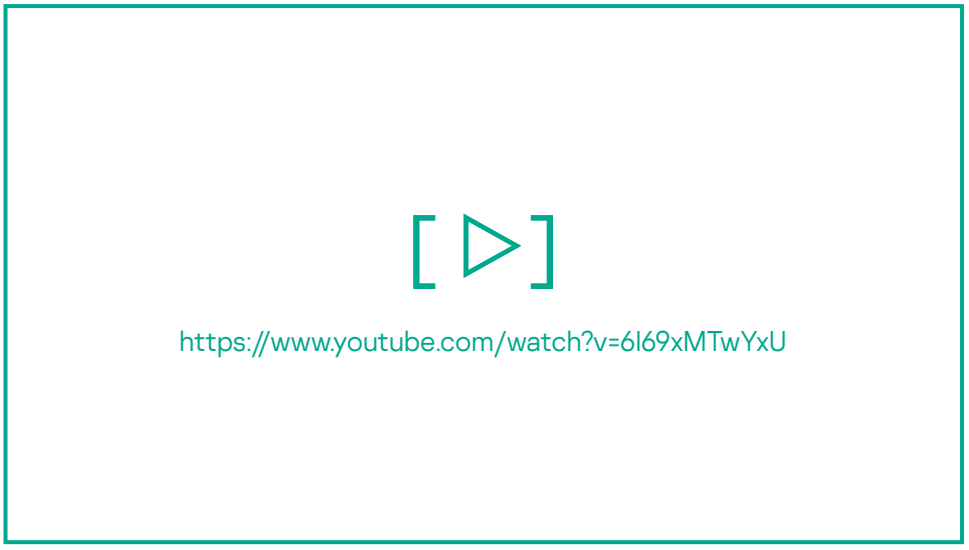
   以下“說明”部分提供了有關代表 Endpoint Agent 元件的應用程式版本與 Kaspersky Anti Targeted Attack Platform 版本的相容性的資訊：Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、Kaspersky Endpoint Security for Mac。

有關安裝 Kaspersky Endpoint Security 的詳細資訊，請參閱應用程式的線上說明：

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

如果您的主機安裝了早期版本的應用程式，您可以升級它們。

觀看在 Microsoft Windows 上部署 EDR 的視頻教程。您可以在幫助頁面（見下方）播放視頻，或點擊連結 https://youtu.be/6l69xMTwYxU?si=lQU1mWrchjvZmuQW。



在 Microsoft Windows 上部署 EDR

安裝 Sandbox 元件

本節提供安裝 Sandbox 元件的逐步說明。

要開始 Sandbox 元件的安裝：

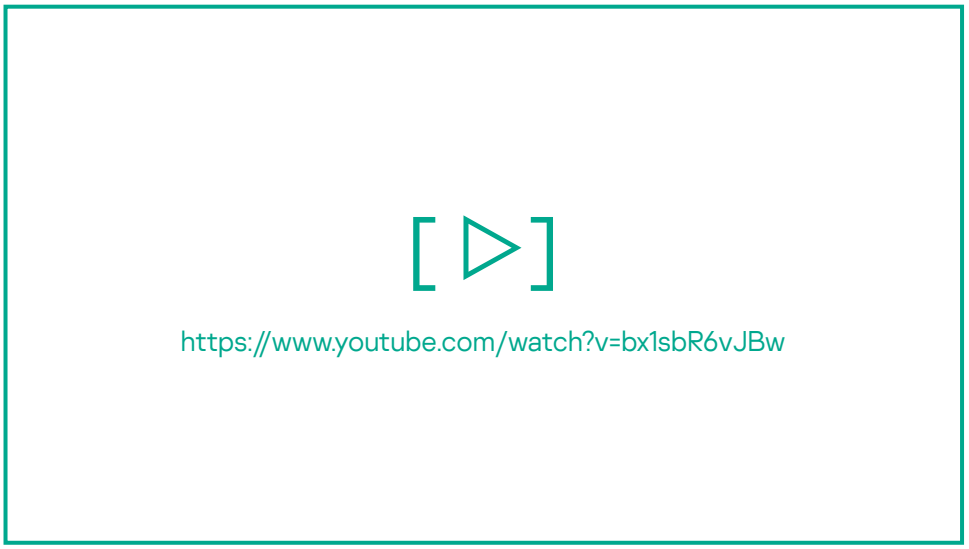
1. 運行包含 Sandbox 元件的磁碟映像。

   安裝精靈啟動。

2. 選擇**繼續**，然後按 **Enter** 鍵。

安裝元件後，您需要配置其與 Central Node 的連線。

觀看有關部署 Sandbox 元件的視頻教程。您可以在幫助頁面（見下方）播放視頻，或點擊連結 https://youtu.be/bx1sbR6vJBw?si=D1PrZ5o4vwlxaNoP。



部署 Sandbox 元件

步驟 1：檢視最終使用者產品授權協議和隱私權政策

若要繼續安裝，您必須閱讀並接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件（以下分別稱為"最終使用者產品授權協議"和"隱私權政策"）。只有當您接受最終使用者產品授權協議和隱私權政策的條款後，安裝才能繼續進行。

要在安裝基於 Ubuntu Server 作業系統的 Sandbox 元件時接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇用於檢視最終使用者產品授權協議和隱私政策的語言，然後按 **Enter**。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

   這將開啟顯示最終使用者產品授權協議文字的視窗。

2. 請閱讀最終使用者產品授權協議。

3. 如果您接受最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。

   這將開啟一個顯示隱私權政策文字的視窗。

4. 請仔細閱讀隱私權政策。

5. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

要在安裝基於 Astra Linux 作業系統的 Sandbox 元件時接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇檢視 Astra Linux 作業系統的最終使用者產品授權協議、最終使用者產品授權協議和隱私政策的語言，然後按下 **Enter** 鍵。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

   這將開啟一個視窗，其中包含 Astra Linux 最終使用者產品授權協議的文字。

2. 閱讀 Astra Linux 作業系統的最終使用者產品授權協議。

3. 如果您接受 Astra Linux 作業系統的最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個視窗，其中包含 AO Kaspersky Lab 最終使用者產品授權協議的文字。

4. 請閱讀最終使用者產品授權協議。

5. 如果您接受最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個顯示隱私權政策文字的視窗。

6. 請仔細閱讀隱私權政策。

7. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

步驟 2：選擇安裝 Sandbox 元件的磁碟

選擇用於安裝 Sandbox 元件的實體磁碟。

所選磁碟機上的所有資料都將被刪除。

如果可用磁碟空間少於 150 GB，安裝將完成並出現錯誤。

若要選擇用於安裝元件的磁碟：

1. 選擇建議的磁碟機之一來安裝程式，然後按 **Enter** 鍵。
   系統將顯示一個確認視窗，要求您確認刪除磁碟上的所有資料，並隨後在此磁碟上安裝元件。

2. 選擇**安裝**並按 **Enter** 鍵，以確認刪除磁碟上的所有資料並將元件安裝到此磁碟上。

   安裝過程中裝置將重啟。

   安裝精靈將繼續執行下一步。

步驟 3：設定 Sandbox 管理員密碼的最小密碼長度

要設定 Sandbox 元件的管理員密碼的最小長度：

1. 在**最小密碼長度**欄位中，輸入密碼長度（至少 8 個字元）。
   建議密碼長度為 12 個或更多字元。

2. 選擇**確定**，然後按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

步驟 4：建立 Sandbox 管理員帳戶

建立一個管理員帳戶，用於在 Sandbox Web 介面、管理員功能表以及具有 Sandbox 元件的伺服器的管理主控台中工作。

要建立 Sandbox 管理員帳戶：

1. 在**新使用者名稱**欄位中，輸入管理員帳戶名稱。預設使用'admin'帳戶。
2. 在**新密碼**欄位中，輸入管理員帳戶的密碼。
   密碼必須符合以下要求：
   - 必須包含至少 8 個字元。
   - 必須包含至少三種字元：
     - 大寫字母 (A-Z)。
     - 小寫字母 (a-z)。
     - 數字。
     - 特殊字元。
   - 不能與使用者名稱完全或基本相同。
   - 不能包含連續三個或更多相同的字元。
3. 在**確認密碼**欄位中，再次輸入密碼。
4. 選擇**確定**，然後按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

步驟 5：設定管理網路介面

為確保 Sandbox 元件正常運作，必須連接至少兩個網路卡，並配置下列網路介面：

- 管理網路介面。此介面用於提供對 Sandbox 伺服器的 SSH 存取；Sandbox 伺服器也使用此介面從 Central Node 接收物件。
- 用於對已處理物件進行 Internet 存取的網路介面。由 Sandbox 處理的物件可以使用此介面嘗試在互聯網上活動，並且 Sandbox 可以分析其行為。如果阻止網際網路存取，則 Sandbox 無法分析網路上物件的行為，因此將只分析無網路存取的物件的行為。

> 用於對已處理物件進行 Internet 存取的網路介面必須與組織的本機網路隔離。

選擇您想要用作管理介面的網路介面並進行設定。

若要選擇管理網路介面並進行設定：

1. 在網路介面清單中，選擇您想要用作管理介面的網路介面。
2. 按下 **Enter**。
3. 在**位址**欄位中，輸入想要指派給此網路介面的 IP 位址。
4. 在**網路遮罩**欄位中，輸入想使用此網路介面的網路遮罩。
5. 選擇**確定**，然後按 **Enter** 鍵。
6. 選擇**繼續**，然後按 **Enter** 鍵。

   安裝精靈將繼續執行下一步。

步驟 6：指派主機名稱並新增DNS伺服器位址

分配 DNS 伺服器要使用的伺服器主機名稱並新增DNS 伺服器位址。

要分配伺服器主機名稱並新增 DNS 伺服器位址：

1. 在 **DNS 設定**視窗中，選擇**主機名稱**。
2. 在**主機名稱**欄位中，輸入伺服器的完整網域名稱。
   以 FQDN 格式指定伺服器名稱（例如：host.domain.com 或 Host.domain.subdomain.com）。
3. 選擇“**確定**”，然後按 **Enter** 鍵。
4. 在 **DNS 設定**視窗中，選擇**DNS 伺服器**。
5. 選擇**建立**，然後按 **Enter** 鍵。
   這將開啟 DNS 伺服器位址輸入視窗。
6. 在**DNS 伺服器**文字方塊中，以 IPv4 格式輸入主 DNS 伺服器的 IP 位址。
7. 選擇“**確定**”，然後按 **Enter** 鍵。
   DNS 伺服器位址輸入視窗關閉。
8. 如果要新增其他 DNS 伺服器的 IP 位址，請對要新增的每台伺服器重複這些說明中的步驟 5 到 7。
9. 新增所有 DNS 伺服器後，選擇**返回**並按 **Enter**。
10. 在**DNS 伺服器**視窗中，選擇**繼續**並按 **Enter**。

    安裝精靈將繼續執行下一步。

步驟 7：設定靜態網路路由

若要設定靜態網路路由：

1. 在“**IPv4 路由**”視窗中，選擇“**建立**”並按 **Enter**。
   這將開啟 **IPv4 靜態路由**視窗。
2. 在**位址/遮罩**欄位中，輸入要為其設定網路路由的子網路的 IP 位址和遮罩。
   如果要使用預設網路路由，請輸入 0.0.0.0/0。
3. 在**閘道**欄位中，輸入閘道的 IP 位址。
4. 選擇“**確定**”，然後按 **Enter** 鍵。
5. 如果要新增其他網路路由，請對要新增的每個網路路由重複這些說明中的步驟 1 到 5。
6. 如果您已完成新增網路路由，請點擊**繼續**。

配置可能需要一些時間。然後安裝完成。

將帶有嵌入式 Sensor 的 Central Node 元件部署為叢集

一個叢集必須至少包含 4 台伺服器：2 台儲存伺服器和 2 台處理伺服器。您可以使用規模指南來確定適合您組織的伺服器數量。

以叢集形式部署帶有嵌入式 Sensor 的 Central Node 元件包括以下步驟：

1. **部署第一台儲存伺服器**

   第一步是部署儲存伺服器。部署儲存伺服器後，您可以向叢集新增其他儲存和處理伺服器。

2. **部署處理伺服器**和**附加儲存伺服器**

   您可以按任何順序部署伺服器。

3. **配置應用程式的大小設定**

   在叢集部署的最後階段，您需要設定應用程式的擴充設定：指定計畫的 SPAN 流量、電子郵件流量、具有 Endpoint Agent 元件的主機數量以及儲存和事件資料庫的大小。

   安裝應用程式後，我們建議立即配置（啟用或停用）第一次成功身分驗證後的強制密碼變更。

如果您在實體伺服器上部署了叢集，並且想要在這些伺服器上新增更多的硬碟，或更換一些現有磁碟機，然後重新安裝叢集，則在安裝元件之前，您必須清除儲存伺服器上先前指派給 OSD (Object Storage Daemon) 的磁碟機。否則，不能保證應用程式正常運作。如果您想完全斷開磁碟機並且不再計劃將其重新連線到伺服器，則無需清除磁碟機。

部署儲存伺服器

要部署資料儲存伺服器，您需要執行具有 Central Node 和 Sensor 元件的磁碟映像。

如果執行安裝精靈步驟時發生錯誤，請聯絡技術支援。

系統磁碟的容量以及元件工作所需的 Ceph 儲存磁碟數量和容量，可以使用規模調整指南來確定。安裝元件所需的最小系統磁碟容量為 150 GB。安裝元件所需的 Ceph 儲存磁碟的最小數量為 3。每個磁碟必須至少有 30 GB 的磁碟空間。

步驟 1：檢視最終使用者產品授權協議和隱私權政策

若要繼續安裝，您必須閱讀並接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件（以下分別稱為"最終使用者產品授權協議"和"隱私權政策"）。只有當您接受最終使用者產品授權協議和隱私權政策的條款後，安裝才能繼續進行。

安裝基於 Ubuntu 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇用於檢視最終使用者產品授權協議和隱私政策的語言，然後按 **Enter**。

   這將開啟顯示最終使用者產品授權協議文字的視窗。

2. 請閱讀最終使用者產品授權協議。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受最終使用者產品授權協議，請選擇"**我接受**"並按 **Enter**。

   這將開啟一個顯示隱私權政策文字的視窗。

4. 請仔細閱讀隱私權政策。

5. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

安裝基於 Astra Linux 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇檢視 Astra Linux 作業系統的最終使用者產品授權協議、最終使用者產品授權協議和隱私政策的語言，然後按下 **Enter** 鍵。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

   這將開啟一個視窗，其中包含 Astra Linux 最終使用者產品授權協議的文字。

2. 閱讀 Astra Linux 作業系統的最終使用者產品授權協議。

3. 如果您接受 Astra Linux 作業系統的最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。

   這將開啟一個視窗，其中包含 AO Kaspersky Lab 最終使用者產品授權協議的文字。

4. 請閱讀最終使用者產品授權協議。

5. 如果您接受最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個顯示隱私權政策文字的視窗。
6. 請仔細閱讀隱私權政策。
7. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

步驟 2：選擇伺服器角色

要選擇伺服器角色：

1. 選擇**儲存**。
2. 按下**Enter**。

安裝精靈將繼續執行下一步。

步驟 3：選取部署模式

選擇部署模式：

1. 選擇以下選項之一：
   - **首個節點安裝**。
     當部署叢集中的第一台伺服器時選擇此值。
   - **向叢集新增額外節點**。
     當部署將被新增至現有叢集的伺服器時選擇此值。
2. 按下**Enter**。

安裝精靈將繼續執行下一步。

步驟 4：與 Kaspersky Endpoint Security for Linux 的相容性有限

在此步驟中，您需要選擇用於安裝元件的磁碟（系統磁碟）。可使用“篩選精靈”確定元件運作所需的系統磁碟容量。安裝元件所需的最小系統磁碟容量為 150 GB。

如果可用磁碟空間少於 150 GB，安裝將完成並出現錯誤。

若要選擇用於安裝元件的磁碟：

1. 選擇建議的磁碟機之一來安裝程式，然後按 **Enter** 鍵。
   確認視窗將顯示。

2. 選擇**是**，然後按 **ENTER**。

安裝精靈將繼續執行下一步。

步驟 5：選擇伺服器定址的網路遮罩

我們建議使用預設值。

此網路遮罩可能與組織基礎架構中使用的網路遮罩不符。

要指定伺服器定址的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇**確定**按鈕，然後按 **Enter**。
  預設值：198.18.0.0/16。

- 如果要指定不同的網路遮罩，請在**子網路**欄位中輸入您的值，選擇**確定**按鈕，然後按 **Enter**。
  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 6：選擇用於定址應用程式元件的網路遮罩

我們建議使用預設值。

應用程式元件定址的網路不得與叢集伺服器定址的網路重疊。

若要指定用於定址應用程式主要元件的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇“**確定**”按鈕，然後按 **Enter**。
  預設值：198.19.0.0/16。

- 如果要指定不同的網路遮罩，請在“**Bridge/Overlay 子網路**”欄位中輸入您的值，選擇“**確定**”按鈕，然後按 **Enter**。
  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 7：選擇叢集網路介面

叢集網路介面用於叢集伺服器之間的通訊。

若要選擇叢集網路介面：

1. 選擇包含用於內部網路的網路介面的行。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
2. 按下 **Enter**。

安裝精靈將繼續執行下一步。

步驟 8：選擇外部網路介面

外部網路介面用於透過 SSH 存取伺服器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 介面以及其他外部連線。

若要選擇外部網路介面：

1. 選擇包含用於外部網路的網路介面的行。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
2. 按下 **Enter**。

安裝精靈將繼續執行下一步。

步驟 9：若要選擇用於取得網路介面 IP 位址的方法

若要選擇用於取得網路介面 IP 位址的方法：

1. 選擇包含**配置類型：**的行，然後按 **Enter**。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
2. 在開啟的視窗中，選擇以下選項之一：
   - **dhcp**。
   - **static**。
3. 如果您選擇了**static**：
   a. 選擇包含參數的行然後按 **Enter** 鍵。
   b. 這會開啟一個視窗；在該視窗中輸入所需資訊。

   > 您需要為每個參數指定一個值。

4. 選擇**確定**。

5. 按下**Enter**。

   安裝精靈將繼續執行下一步。

步驟 10：建立管理員帳戶並在叢集中驗證伺服器

在此步驟中，您需要執行下列其中一項操作：

- 如果您要部署叢集中的第一台伺服器，請建立管理員帳戶。
- 如果您要部署其他儲存伺服器，請對叢集中的伺服器進行驗證。

建立管理員帳戶

> 僅在部署叢集中的第一台伺服器時才需要管理員帳戶。如果您正在部署額外的儲存伺服器，應用程式不會開啟提示您建立管理員帳戶的視窗，而是提示您對叢集中的伺服器進行身分驗證。

在部署叢集中的第一台伺服器時，您需要建立一個管理員帳戶。此使用者帳戶用於管理應用程式的 Web 介面、應用程式的管理員功能表以及在技術支援模式下管理應用程式。

預設情況下，管理員帳戶的使用者名稱為 *admin*。您必須輸入該使用者帳戶的密碼。

輸入管理者使用者帳戶的密碼：

1. 這將開啟一個視窗；在該視窗中，在**最小長度**欄位中輸入最小密碼長度。您必須輸入 8 或更大的值。
2. 選擇**確定**，然後按 **Enter** 鍵。
   這將開啟密碼建立視窗。
3. 這將開啟一個視窗；在該視窗的**密碼**欄位中，輸入管理員帳戶的密碼。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
4. 在**確認**欄位中，再次輸入新密碼。
5. 選擇**確定**，然後按 **Enter** 鍵。

   安裝精靈將繼續執行下一步。

驗證叢集中的伺服器

> 僅當部署額外的儲存伺服器時才需要對叢集中的伺服器進行身分驗證。如果您正在部署叢集中的第一台伺服器，應用程式會提示您建立管理員帳戶，而不是對伺服器進行身分驗證。

若要對叢集中的伺服器進行身分驗證，您需要輸入部署叢集中第一台伺服器時設定的管理員帳戶密碼。

對叢集中的伺服器進行身分驗證：

1. 在**密碼**欄位中，輸入管理員帳戶的密碼。
2. 選擇**確定**，然後按 **Enter** 鍵。
   要選擇按鈕，可以使用↑、↓、PageUp 和 PageDown 鍵。

叢集中的伺服器將得到身分驗證。安裝精靈將繼續執行下一步。

步驟 11：新增 DNS 伺服器位址

如果您正在部署叢集中的第一台伺服器，則此步驟可用。

為具有應用程式元件的伺服器的運作配置 DNS 設定。

> 請確保您已正確指定 DNS 伺服器的 IP 位址。如果指定的 IP 位址不正確，則與 NTP 伺服器的時間同步將失敗，應用程式的安裝也將中斷。

新增 DNS 伺服器位址：

1. 選擇**新增**欄位，然後按 **Enter** 鍵。
2. 以 IPv4 格式輸入 DNS 伺服器的 IP 位址。
3. 選擇"**確定**"，然後按 **Enter** 鍵。
4. 如果要新增其他 DNS 伺服器的 IP 位址，請重複這些說明中的步驟 1 至 3。
   新增所有 DNS 伺服器後，選擇**繼續**並按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

步驟 12：配置與 NTP 伺服器的時間同步

> 如果您正在部署叢集中的第一台伺服器，則此步驟可用。

配置伺服器時間與 NTP 伺服器的同步。

1. 選擇**新增**欄位，然後按 **Enter** 鍵。
2. 輸入 NTP 伺服器的 IP 位址或名稱。
3. 選擇**確定**，然後按 **Enter** 鍵。
4. 如果要新增其他 NTP 伺服器的 IP 位址或名稱，請重複這些說明中的步驟 1 至3。
5. 新增所有 NTP 伺服器後，選擇**繼續**，並按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

為了使叢集正常運行，叢集伺服器上的時間必須同步。確保您新增的 NTP 伺服器正常運作並能確保叢集伺服器之間的時間同步。

步驟 13：選擇用於 Ceph 儲存的磁碟

選擇用於 Ceph 儲存的磁碟。Ceph 儲存所需的磁碟數量和容量可以使用規模調整指南來確定。安裝元件所需的最小磁碟數為 3。在這種情況下，每個磁碟必須至少有 30 GB 的磁碟空間。

若要為 Ceph 儲存選擇磁碟：

1. 選擇包含所需磁碟機的行。

   若要選擇一行，您可以使用 ↑、↓、PageUp 和 PageDown 鍵。

2. 按下 **Enter**。

3. 如果要選擇多個磁碟機，請重複步驟 1 到 2 以選擇更多磁碟機。

4. 選擇**應用並完成**欄位並按 **Enter**。

   確認視窗將顯示。

5. 選擇**是**，然後按 **ENTER**。

配置可能需要一些時間。然後安裝完成。您可以繼續配置叢集的伺服器。

部署處理伺服器

要部署處理伺服器，您需要執行具有 Central Node 和 Sensor 元件的磁碟映像。

如果執行安裝精靈步驟時發生錯誤，請聯絡技術支援。

您可以使用“篩選精靈”來確定元件運作所需的系統磁碟容量。安裝元件所需的最小系統磁碟容量為 150 GB。

步驟 1：檢視最終使用者產品授權協議和隱私權政策

若要繼續安裝，您必須閱讀並接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件（以下分別稱為“最終使用者產品授權協議”和“隱私權政策”）。只有當您接受最終使用者產品授權協議和隱私權政策的條款後，安裝才能繼續進行。

安裝基於 Ubuntu 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇用於檢視最終使用者產品授權協議和隱私政策的語言，然後按 **Enter**。

   這將開啟顯示最終使用者產品授權協議文字的視窗。

2. 請閱讀最終使用者產品授權協議。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受最終使用者產品授權協議，請選擇“**我接受**”並按 **Enter**。

   這將開啟一個顯示隱私權政策文字的視窗。

4. 請仔細閱讀隱私權政策。

5. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

安裝基於 Astra Linux 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇檢視 Astra Linux 作業系統的最終使用者產品授權協議、最終使用者產品授權協議和隱私政策的語言，然後按下 **Enter** 鍵。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

   這將開啟一個視窗，其中包含 Astra Linux 最終使用者產品授權協議的文字。

2. 閱讀 Astra Linux 作業系統的最終使用者產品授權協議。

3. 如果您接受 Astra Linux 作業系統的最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。

   這將開啟一個視窗，其中包含 AO Kaspersky Lab 最終使用者產品授權協議的文字。

4. 請閱讀最終使用者產品授權協議。

5. 如果您接受最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。

   這將開啟一個顯示隱私權政策文字的視窗。

6. 請仔細閱讀隱私權政策。

7. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

步驟 2：選擇伺服器角色

要選擇伺服器角色：

1. 選擇“**處理**”。

   該角色還包括 Sensor 元件的安裝和配置。

2. 按下“**Enter**”。

安裝精靈將繼續執行下一步。

步驟 3：與 Kaspersky Endpoint Security for Linux 的相容性有限

在此步驟中，您需要選擇用於安裝元件的磁碟（系統磁碟）。可使用 規模調整指南 確定元件運作所需的系統磁碟容量。安裝元件所需的最小系統磁碟容量為 150 GB。

如果可用磁碟空間少於 150 GB，安裝將完成並出現錯誤。

若要選擇用於安裝元件的磁碟：

1. 選擇建議的磁碟機之一來安裝程式，然後按 **Enter** 鍵。
   確認視窗將顯示。
2. 選擇**是**，然後按 **ENTER**。

安裝精靈將繼續執行下一步。

步驟 4：選取叢集伺服器定址的網路遮罩

我們建議使用預設值。

此網路遮罩可能與組織基礎架構中使用的網路遮罩不符。

若要指定叢集伺服器定址的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇**確定**按鈕，然後按 **Enter**。
  預設值：198.18.0.0/16。
- 如果要指定不同的網路遮罩，請在**子網路**欄位中輸入您的值，選擇**確定**按鈕，然後按 **Enter**。
  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 5：選擇用於定址應用程式元件的網路遮罩

我們建議使用預設值。

應用程式元件定址的網路不得與叢集伺服器定址的網路重疊。

若要指定用於定址應用程式主要元件的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇“**確定**”按鈕，然後按 **Enter**。

  預設值：198.19.0.0/16。

- 如果要指定不同的網路遮罩，請在“**Bridge/Overlay 子網路**”欄位中輸入您的值，選擇“**確定**”按鈕，然後按 **Enter**。

  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 6：選擇叢集網路介面

叢集網路介面用於叢集伺服器之間的通訊。

若要選擇叢集網路介面：

1. 選擇包含用於內部網路的網路介面的行。

   若要選擇一行，您可以使用 ↑、↓、PageUp 和 PageDown 鍵。所選行以紅色突出顯示。

2. 按下**Enter**。

安裝精靈將繼續執行下一步。

步驟 7：選擇外部網路介面

外部網路介面用於透過 SSH 存取伺服器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 介面以及其他外部連線。

若要選擇外部網路介面：

1. 選擇包含用於外部網路的網路介面的行。

   若要選擇一行，您可以使用 ↑、↓、PageUp 和 PageDown 鍵。

2. 按下 **Enter**。

安裝精靈將繼續執行下一步。

步驟 8：選擇取得網路介面 IP 位址的方法

若要選擇用於取得網路介面 IP 位址的方法：

1. 選擇包含**配置類型：**的行，然後按 **Enter**。

   若要選擇一行，您可以使用 ↑、↓、PageUp 和 PageDown 鍵。

2. 在開啟的視窗中，選擇以下選項之一：

   - **dhcp**。
   - **static**。

3. 如果您選擇了**static**:

   a. 選擇包含參數的行然後按 **Enter** 鍵。

   b. 這會開啟一個視窗；在該視窗中輸入所需資訊。

   > 您需要為每個參數指定一個值。

4. 選擇“**確定**”。

5. 按下“**Enter**”。

安裝精靈將繼續執行下一步。

步驟 9：驗證叢集中的伺服器

若要對叢集中的伺服器進行身分驗證，您需要輸入部署叢集中第一台伺服器時設定的管理員帳戶密碼。

對叢集中的伺服器進行身分驗證：

1. 在**密碼**欄位中，輸入管理員帳戶的密碼。

2. 選擇**確定**，然後按 **Enter** 鍵。
   要選擇按鈕，可以使用↑、↓、PageUp 和 PageDown 鍵。

叢集中的伺服器將得到身分驗證。安裝精靈將繼續執行下一步。

步驟 10：選擇 NDR 功能的在地化語言並配置從 SPAN 連接埠接收鏡像流量

如果您正在部署叢集的第一個工作伺服器，則在此步驟中，您必須依照下列順序完成安裝精靈的步驟：

1. 選擇 NDR 功能的在地化語言。

2. 配置從 SPAN 連接埠接收鏡像流量。

如果您正在部署額外的工作伺服器，則可以省略NDR 在地化選擇步驟。對叢集中的伺服器進行認證後，安裝精靈將繼續執行配置從 SPAN 連接埠接收鏡像流量的步驟。

選擇 NDR 功能的本地化語言

所選語言用於顯示與 NDR 功能相關的應用程式部分。

若要選擇 NDR 功能的在地化語言：

在清單中選擇它並按 Enter。

選擇 NDR 功能的本地化語言。安裝精靈會繼續前往您設定從 SPAN 連接埠接收鏡像流量的步驟。

配置從 SPAN 連接埠接收映像流量

為了使應用程式正常運作，必須在叢集中的一台處理伺服器上啟用從 SPAN 連接埠接收映像流量。如果您實際上不需要處理來自 SPAN 連接埠的鏡像流量，請在配置大小時將 SPAN 流量指定為 0。

必須僅在叢集中的一台處理伺服器上啟用映像流量處理。

若要開啟從 SPAN 連接埠接收映像流量：

在顯示的視窗中選擇**是**，並按 **Enter** 鍵。

配置可能需要一些時間。然後安裝完成。為了使應用程式正常工作，您必須配置伺服器。

若要關閉從 SPAN 連接埠接收映像流量：

在開啟的視窗中，選擇**否**並按 **Enter** 鍵。

配置可能需要一些時間。然後安裝完成。為了使應用程式正常工作，您必須配置伺服器。

清除儲存伺服器上的硬碟

如果您已經在伺服器上部署了叢集，並且想要在這些伺服器上新增更多的硬碟，或更換一些現有磁碟機，然後重新安裝叢集，則在安裝元件之前，必須清除儲存伺服器上先前指派給 OSD (Object Storage Daemon) 的磁碟機。否則，不能保證應用程式正常運作。

若要清除活動儲存伺服器上指派給 OSD 的磁碟：

1. 透過 SSH 或終端登入要清除磁碟的伺服器的管理主控台。
2. 透過執行`sudo systemctl stop kata-osd-starter.service`停止OSD 啟動服務。
3. 透過執行`sudo docker ps --filter name=osd -q | xargs docker stop`停止OSD 容器。
4. 透過執行`sudo ceph-volume --cluster ceph lvm list | grep devices`取得 OSD 磁碟清單。
5. 使用 `sudo wipefs -af /dev/<磁碟名稱>` 指令從這些磁碟中刪除檔案系統簽章和分割區表。
   您必須對在步驟 4 中獲得的每個磁碟機執行此命令。例如：`sudo wipefs -af /dev/sda`。

6. 透過執行 `sudo ceph-volume lvm zap --destroy /dev/<磁碟名稱>`清除這些磁碟。

   您必須對在步驟 4 中獲得的每個磁碟機執行此命令。例如：`sudo ceph-volume lvm zap --destroy /dev/sda`。

OSD 守護程式被從磁碟中刪除。

如果伺服器不在活動狀態，則必須從為 OSD 指派的每個磁碟中刪除有關磁碟區群組的資訊。

若要從非活動伺服器上為 OSD 指派的每個磁碟中刪除有關磁碟區群組的資訊：

1. 使用備用作業系統啟動伺服器。

2. 使用 `sudo pvs` 指令取得為 OSD 指派的每個磁碟的群組 ID。

   此指令輸出一個表，其中 `PV` 表示實體卷，`VG` 表示邏輯組成員身分，`Fmt` 表示卷格式，`Size` 表示實體卷大小。

3. 透過執行 `sudo vgremove <卷組 ID>` 刪除相關卷組。

指派給 OSD 的磁碟上的磁碟區組資訊被刪除。

在伺服器上安裝帶有嵌入式 Sensor 的 Central Node 元件

在伺服器上安裝帶有嵌入式 Sensor 的 Central Node 元件涉及以下步驟：

1. **安裝帶有嵌入式 Sensor 的 Central Node 元件**

   要在實體伺服器上安裝元件，您要從帶有 Central Node 和 Sensor 元件的磁碟映像啟動。

   要在虛擬伺服器上安裝元件，您需要將具有 Central Node 和 Sensor 元件的磁碟映像連線到所選虛擬機並執行它。虛擬機啟動後安裝立即開始。您可以使用虛擬機的主控台管理安裝過程。

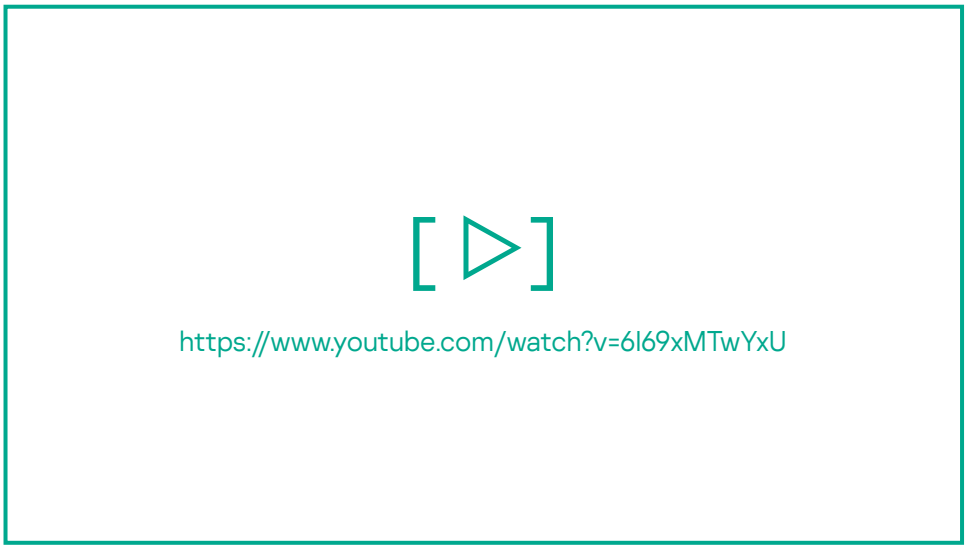
2. **配置應用程式的大小設定**

   在叢集部署的最後階段，您需要設定應用程式的擴充設定：指定計畫的 SPAN 流量、電子郵件流量、具有 Endpoint Agent 元件的主機數量以及儲存和事件資料庫的大小。

   安裝應用程式後，我們建議立即配置（啟用或停用）第一次成功身分驗證後的強制密碼變更。

如果執行安裝精靈步驟時發生錯誤，請聯絡技術支援。

觀看有關部署 Central Node 元件的視頻教程。您可以在幫助頁面（見下方）播放視頻，或點擊連結 https://youtu.be/6l69xMTwYxU?si=lQU1mWrchjvZmuQW。



部署 Central Node 元件。

步驟 1：檢視最終使用者產品授權協議和隱私權政策

若要繼續安裝，您必須閱讀並接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件（以下分別稱為"最終使用者產品授權協議"和"隱私權政策"）。只有當您接受最終使用者產品授權協議和隱私權政策的條款後，安裝才能繼續進行。

安裝基於 Ubuntu 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇用於檢視最終使用者產品授權協議和隱私政策的語言，然後按 **Enter**。

   這將開啟顯示最終使用者產品授權協議文字的視窗。

2. 請閱讀最終使用者產品授權協議。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受最終使用者產品授權協議，請選擇"**我接受**"並按 **Enter**。

   這將開啟一個顯示隱私權政策文字的視窗。

4. 請仔細閱讀隱私權政策。

5. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

安裝基於 Astra Linux 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇檢視 Astra Linux 作業系統的最終使用者產品授權協議、最終使用者產品授權協議和隱私政策的語言，然後按下 **Enter** 鍵。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

   這將開啟一個視窗，其中包含 Astra Linux 最終使用者產品授權協議的文字。

2. 閱讀 Astra Linux 作業系統的最終使用者產品授權協議。

3. 如果您接受 Astra Linux 作業系統的最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個視窗，其中包含 AO Kaspersky Lab 最終使用者產品授權協議的文字。

4. 請閱讀最終使用者產品授權協議。

5. 如果您接受最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個顯示隱私權政策文字的視窗。

6. 請仔細閱讀隱私權政策。

7. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

步驟 2：選擇伺服器角色

要選擇伺服器角色：

1. 選擇"**單個**"。
   此角色用於在同一台伺服器上安裝 Central Node 和 Sensor 元件。

2. 按下"**Enter**"。

安裝精靈將繼續執行下一步。

步驟 3：與 Kaspersky Endpoint Security for Linux 的相容性有限

在此步驟中，您需要選擇用於安裝元件的磁碟（系統磁碟）。可使用篩選精靈確定元件運作所需的系統磁碟容量。安裝元件所需的最小系統磁碟容量為 150 GB。

如果可用磁碟空間少於 150 GB，安裝將完成並出現錯誤。

SAN 儲存系統不能用作元件安裝磁碟機。

若要選擇用於安裝元件的磁碟：

1. 選擇建議的磁碟機之一來安裝程式，然後按 **Enter** 鍵。
   確認視窗將顯示。

2. 選擇**是**，然後按 **ENTER**。

安裝精靈將繼續執行下一步。

步驟 4：分配用於 Targeted Attack Analyzer 元件資料庫的磁碟

在此步驟中，您可以為針對性攻擊分析器分析元件資料庫指派實體磁碟，或拒絕為其指派實體磁碟。為了實現針對性攻擊分析器元件的最佳效能，建議您在伺服器上為元件資料庫指派至少 1 TB 的實體磁碟。

> 您只能在此步驟中為針對性攻擊分析器元件資料庫分配物理磁碟。安裝應用程式後將無法分配磁碟。

分配用於針對性攻擊分析器元件資料庫的磁碟：

1. 為針對性攻擊分析器元件資料庫選擇建議的磁碟機之一。
   如果您不需要 Targeted Attack Analyzer 元件的資料庫，請選擇**不為 TAA 指派單獨的磁碟**行。
2. 在確認視窗中，選擇**是**並按下 **Enter**。

安裝精靈將繼續執行下一步。

如果您想使用 SAN 儲存系統，請在此安裝步驟中選擇顯示為本機磁碟的 SAN 磁區作為資料庫儲存磁碟。

> 連線 SAN 的說明由其供應商提供。

步驟 5：選擇伺服器定址的網路遮罩

> 我們建議使用預設值。

> 此網路遮罩可能與組織基礎架構中使用的網路遮罩不符。

要指定伺服器定址的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇**確定**按鈕，然後按 **Enter**。
  預設值：198.18.0.0/16。
- 如果要指定不同的網路遮罩，請在**子網路**欄位中輸入您的值，選擇**確定**按鈕，然後按 **Enter**。
  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 6：為應用程式元件的定址選擇網路遮罩

我們建議使用預設值。

應用程式元件定址的網路不得與伺服器定址的網路重疊。

若要指定用於定址應用程式主要元件的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇“**確定**”按鈕，然後按 **Enter**。

  預設值：198.19.0.0/16。

- 如果要指定不同的網路遮罩，請在“**Bridge/Overlay 子網路**”欄位中輸入您的值，選擇“**確定**”按鈕，然後按 **Enter**。

  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 7：選擇外部網路介面

外部網路介面用於透過 SSH 存取伺服器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 介面以及其他外部連線。

若要選擇外部網路介面：

1. 選擇包含用於外部網路的網路介面的行。

   若要選擇一行，您可以使用 ↑、↓、PageUp 和 PageDown 鍵。

2. 按下 **Enter**。

安裝精靈將繼續執行下一步。

步驟 8：若要選擇用於取得網路介面 IP 位址的方法

若要選擇用於取得網路介面 IP 位址的方法：

1. 選擇包含**配置類型：**的行，然後按 **Enter**。

   若要選擇一行，您可以使用 ↑、↓、PageUp 和 PageDown 鍵。

2. 在開啟的視窗中，選擇以下選項之一：

   - **dhcp**。
   - **static**。

3. 如果您選擇了**static**：

   a. 選擇包含參數的行然後按 **Enter** 鍵。

   b. 這會開啟一個視窗；在該視窗中輸入所需資訊。

   > 您需要為每個參數指定一個值。

4. 選擇**確定**。

5. 按下**Enter**。

安裝精靈將繼續執行下一步。

步驟 9：建立管理員帳戶

管理員帳戶用於管理應用程式的 Web 介面，應用程式的管理員功能表，以及在技術支援模式下管理應用程式。

預設情況下，管理員帳戶的使用者名稱為 *admin*。您必須輸入該使用者帳戶的密碼。

輸入管理者使用者帳戶的密碼：

1. 這將開啟一個視窗；在該視窗中，在**最小長度**欄位中輸入最小密碼長度。您必須輸入 8 或更大的值。

2. 選擇**確定**，然後按 **Enter** 鍵。
   這將開啟密碼建立視窗。

3. 這將開啟一個視窗；在該視窗的**密碼**欄位中，輸入管理員帳戶的密碼。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。

4. 在**確認**欄位中，再次輸入新密碼。

5. 選擇**確定**，然後按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

步驟 10：選擇 NDR 功能的本地化語言

所選語言用於顯示與 NDR 功能相關的應用程式部分。

若要選擇 NDR 功能的在地化語言：

在清單中選擇它並按 Enter。

步驟 11：新增 DNS 伺服器位址

為具有應用程式元件的伺服器的運作配置 DNS 設定。

> 請確保您已正確指定 DNS 伺服器的 IP 位址。如果指定的 IP 位址不正確，則與 NTP 伺服器的時間同步將失敗，應用程式的安裝也將中斷。

新增 DNS 伺服器位址：

1. 選擇**新增**欄位，然後按 **Enter** 鍵。
2. 以 IPv4 格式輸入 DNS 伺服器的 IP 位址。
3. 選擇"**確定**"，然後按 **Enter** 鍵。
4. 如果要新增其他 DNS 伺服器的 IP 位址，請重複這些說明中的步驟 1 至 3。
5. 新增所有 DNS 伺服器後，選擇**繼續**並按 **Enter** 鍵。

   安裝精靈將繼續執行下一步。

步驟 12：配置與 NTP 伺服器的時間同步

配置伺服器時間與 NTP 伺服器的同步。

1. 選擇**新增**欄位，然後按 **Enter** 鍵。
2. 輸入 NTP 伺服器的 IP 位址或名稱。
3. 選擇**確定**，然後按 **Enter** 鍵。
4. 如果要新增其他 NTP 伺服器的 IP 位址或名稱，請重複這些說明中的步驟 1 至3。
5. 新增所有 NTP 伺服器後，選擇**繼續**，並按 **Enter** 鍵。

   安裝完成。為了使應用程式正常工作，您必須配置伺服器。

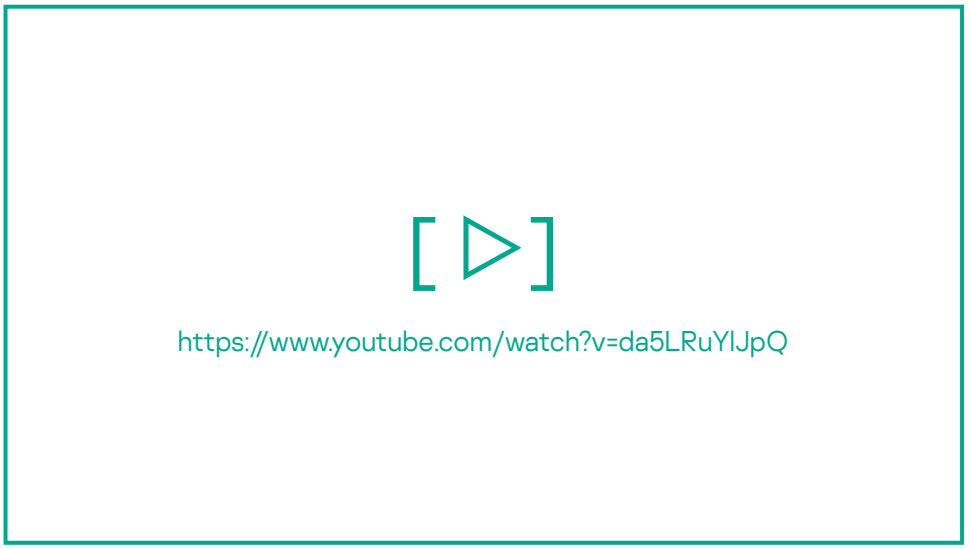
在獨立伺服器上安裝 Sensor 元件

要在實體伺服器上安裝 Sensor 元件，您需要執行包含 Central Node 和 Sensor 元件的磁碟映像。

要在虛擬伺服器上安裝 Sensor 元件，您需要將具有 Central Node 和 Sensor 元件的磁碟映像連線到所選虛擬機並執行它。虛擬機啟動後安裝立即開始。您可以使用虛擬機的主控台管理安裝過程。

安裝元件後，您需要將其連線到 Central Node。

觀看有關部署 Sensor 元件的視頻教程。您可以在幫助頁面（見下方）播放視頻，或點擊連結 https://youtu.be/da5LRuYlJpQ?si=JRSPsNRPlK-Jqcfc。



部署 Sensor 元件

步驟 1：檢視最終使用者產品授權協議和隱私權政策

若要繼續安裝，您必須閱讀並接受 AO Kaspersky Lab 的最終使用者產品授權協議和隱私權政策的條款和條件（以下分別稱為"最終使用者產品授權協議"和"隱私權政策"）。只有當您接受最終使用者產品授權協議和隱私權政策的條款後，安裝才能繼續進行。

安裝基於 Ubuntu 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇用於檢視最終使用者產品授權協議和隱私政策的語言，然後按 **Enter**。

   這將開啟顯示最終使用者產品授權協議文字的視窗。

2. 請閱讀最終使用者產品授權協議。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

3. 如果您接受最終使用者產品授權協議，請選擇"**我接受**"並按 **Enter**。

   這將開啟一個顯示隱私權政策文字的視窗。

4. 請仔細閱讀隱私權政策。

5. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

安裝基於 Astra Linux 作業系統的元件時接受最終使用者產品授權協議和隱私權政策的條款和條件：

1. 在清單中選擇檢視 Astra Linux 作業系統的最終使用者產品授權協議、最終使用者產品授權協議和隱私政策的語言，然後按下 **Enter** 鍵。

   若要向上和向下移動，您可以使用下列按鍵：↑、↓、**PageUp** 和 **PageDown**。

   這將開啟一個視窗，其中包含 Astra Linux 最終使用者產品授權協議的文字。

2. 閱讀 Astra Linux 作業系統的最終使用者產品授權協議。

3. 如果您接受 Astra Linux 作業系統的最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個視窗，其中包含 AO Kaspersky Lab 最終使用者產品授權協議的文字。

4. 請閱讀最終使用者產品授權協議。

5. 如果您接受最終使用者產品授權協議的條款和條件，請選擇**我接受**並按 **Enter**。
   這將開啟一個顯示隱私權政策文字的視窗。

6. 請仔細閱讀隱私權政策。

7. 如果您接受隱私政策的條款和條件，請選擇**我接受**並按 **Enter**。

安裝精靈將繼續執行下一步。

步驟 2：選擇伺服器角色

要選擇伺服器角色：

1. 選擇“ **Sensor**”。
   此角色用於在獨立伺服器上安裝 Sensor 元件。

2. 按下“**Enter**”。

安裝精靈將繼續執行下一步。

步驟 3：選擇安裝元件的磁碟

在此步驟中，您需要選擇用於安裝元件的磁碟（系統磁碟）。您可以使用“篩選精靈”來確定元件運作所需的系統磁碟容量。安裝元件所需的最小系統磁碟容量為 150 GB。

如果可用磁碟空間少於 150 GB，安裝將完成並出現錯誤。

若要選擇用於安裝元件的磁碟：

1. 選擇建議的磁碟機之一來安裝程式，然後按 **Enter** 鍵。
   確認視窗將顯示。

2. 選擇**是**，然後按 **ENTER**。

安裝精靈將繼續執行下一步。

步驟 4：為伺服器定址選擇網路遮罩

我們建議使用預設值。

此網路遮罩可能與組織基礎架構中使用的網路遮罩不符。

要指定伺服器定址的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇“**確定**”按鈕，然後按 **Enter**。
  預設值：198.18.0.0/16。
- 如果要指定不同的網路遮罩，請在“**子網路**”欄位中輸入您的值，選擇“**確定**”按鈕，然後按 **Enter**。
  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 5：為應用程式元件的定址選擇網路遮罩

我們建議使用預設值。

應用程式元件定址的網路不得與伺服器定址的網路重疊。

若要指定用於定址應用程式主要元件的網路遮罩：

- 如果要使用網路遮罩的預先定義值，請選擇“**確定**”按鈕，然後按 **Enter**。
  預設值：198.19.0.0/16。
- 如果要指定不同的網路遮罩，請在“**Bridge/Overlay 子網路**”欄位中輸入您的值，選擇“**確定**”按鈕，然後按 **Enter**。
  遮罩必須與範本相符：xx0.0/16。

安裝精靈將繼續執行下一步。

步驟 6：選擇外部網路介面

外部網路介面用於透過 SSH 存取伺服器、管理 Kaspersky Anti Targeted Attack Platform 的 Web 介面以及其他外部連線。

若要選擇外部網路介面：

1. 選擇包含用於外部網路的網路介面的行。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
2. 按下 **Enter**。

安裝精靈將繼續執行下一步。

步驟 7：選擇取得網路介面 IP 位址的方法

若要選擇用於取得網路介面 IP 位址的方法：

1. 選擇包含**配置類型：**的行，然後按 **Enter**。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
2. 在開啟的視窗中，選擇以下選項之一：
   - **dhcp**。
   - **static**。
3. 如果您選擇了**static**:
   a. 選擇包含參數的行然後按 **Enter** 鍵。
   b. 這會開啟一個視窗；在該視窗中輸入所需資訊。

   > 您需要為每個參數指定一個值。

4. 選擇“**確定**”。
5. 按下“**Enter**”。

安裝精靈將繼續執行下一步。

步驟 8：建立管理員帳戶

管理員帳戶用於管理應用程式的 Web 介面，應用程式的管理員功能表，以及在技術支援模式下管理應用程式。

預設情況下，管理員帳戶的使用者名稱為 *admin*。您必須輸入該使用者帳戶的密碼。

輸入管理者使用者帳戶的密碼：

1. 這將開啟一個視窗；在該視窗中，在**最小長度**欄位中輸入最小密碼長度。您必須輸入 8 或更大的值。
2. 選擇**確定**，然後按 **Enter** 鍵。
   這將開啟密碼建立視窗。

3. 這將開啟一個視窗；在該視窗的**密碼**欄位中，輸入管理員帳戶的密碼。
   若要選擇一行，您可以使用↑、↓、PageUp 和 PageDown 鍵。
4. 在**確認**欄位中，再次輸入新密碼。
5. 選擇**確定**，然後按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

步驟 9：新增 DNS 伺服器位址

為具有應用程式元件的伺服器的運作配置 DNS 設定。

> 請確保您已正確指定 DNS 伺服器的 IP 位址。如果指定的 IP 位址不正確，則與 NTP 伺服器的時間同步將失敗，應用程式的安裝也將中斷。

新增 DNS 伺服器位址：

1. 選擇**新增**欄位，然後按 **Enter** 鍵。
2. 以 IPv4 格式輸入 DNS 伺服器的 IP 位址。
3. 選擇"**確定**"，然後按 **Enter** 鍵。
4. 如果要新增其他 DNS 伺服器的 IP 位址，請重複這些說明中的步驟 1 至 3。
5. 新增所有 DNS 伺服器後，選擇**繼續**並按 **Enter** 鍵。

安裝精靈將繼續執行下一步。

步驟 10：配置與 NTP 伺服器的時間同步

配置伺服器時間與 NTP 伺服器的同步。

1. 選擇**新增**欄位，然後按 **Enter** 鍵。
2. 輸入 NTP 伺服器的 IP 位址或名稱。
3. 選擇**確定**，然後按 **Enter** 鍵。
4. 如果要新增其他 NTP 伺服器的 IP 位址或名稱，請重複這些說明中的步驟 1 至3。
5. 新增所有 NTP 伺服器後，選擇**繼續**，並按 **Enter** 鍵。

安裝完成。

最佳化 Sensor 元件的網路介面設定

如果應用程式在處理網路流量時遇到網路封包遺失或效能問題，請按照這些說明進行操作。

若要減少網路封包遺失和從流量擷取檔案不完整的情況，請執行下列操作：

1. 指定 RSS 佇列的最大數量：
   - 如果網路上的資料傳輸速率小於 1 Gbps，請將數字設定為 1。
   - 如果網路上的資料傳輸速率大於 1 Gbps，請將數字設定為 16。

   如果您的網路介面不允許將 RSS 佇列的最大數量設為 16，請將其設定為受支援的最大數量。

2. 為網路介面配置對稱 RSS 雜湊。有關配置 RSS 雜湊的詳細資訊，請參閱網路介面卡的供應商檔案。
3. 建立**包含以下內容**的 interrupts.sh 檔案。

```
#!/usr/bin/env bash

set -e

dev=$1
min_cpu=$2
max_cpu=$3
step=$4

irs=($(cat /proc/interrupts | grep "$dev" | awk '{split($1,a,":"); print a[1]}'))

cpu=$min_cpu
for ir in ${irs[@]}; do
echo $cpu > /proc/irq/$ir/smp_affinity_list
cpu=$(((cpu + step) % max_cpu))
cat "/proc/irq/$ir/smp_affinity_list"
done
```

4. 執行以下指令：

   `sudo bash interrupts.sh <dev> <min_cpu> <max_cpu> <step>`，其中

   - `<dev>`是您想要在核心之間分配中斷的網路介面。
   - `<min_cpu>`是網路介面卡中斷分配範圍內的第一個核心。
   - `<max_cpu>`是網路介面卡中斷分配範圍內的最後一個核心。
   - `<step>`是選擇下一個分配給中斷的核心的增量。

   範例：

   ```
   sudo bash interrupts.sh ens192 2 11 1
   ```

5. 如果您使用 NVIDIA Mellanox 網路介面卡(mlx4)，請透過執行下列指令來設定 RSS 佇列數和 RSS 雜湊：

```
ethtool -L $dev rx 16
ethtool -X $dev equal 16
ethtool -X $dev hfunc xor
```

6. 如果您使用的是 Intel 網路介面卡 (i40e)，請設定 RSS 佇列數和 RSS 雜湊：

```
rmmod i40e && modprobe i40e
ifconfig $dev down
ethtool -L $dev combined 16
ethtool -K $dev rxhash on
ethtool -K $dev ntuple on
ifconfig $dev up
ethtool -X $dev hkey
6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:
5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A equal 16
ethtool -A $dev rx off
ethtool -C $dev adaptive-rx off adaptive-tx off rx-usecs 125
ethtool -G $dev rx 1024
ethtool -N $dev rx-flow-hash tcp4 sdfn
ethtool -N $dev rx-flow-hash tcp6 sdfn
ethtool -N $dev rx-flow-hash udp4 sdfn
ethtool -N $dev rx-flow-hash udp6 sdfn
```

網路介面已配置。

重新啟動應用程式後，您必須按照說明重新配置網路介面。

連線和配置 Sensor 元件的外部儲存

Kaspersky Anti Targeted Attack Platform 將從網路介面接收的流量儲存為網路流量傾印檔案。如果要確保網路流量傾印檔案的長期儲存，您可以連線並設定外部儲存。您可以使用外部儲存空間中的網路流量傾印檔案將網路流量下載為 PCAP 檔案。我們建議使用 SSD 磁碟機作為外部儲存。

配置外部儲存的步驟對於安裝在與 Central Node （嵌入式 Sensor）同一伺服器上的 Sensor 元件和安裝在獨立伺服器上的 Sensor 元件有所不同。以下是為指定的 Sensor 配置外部儲存的說明。

如果您要重新連接磁碟機並希望保留其上的資料，請跳過以下說明中的步驟 4 和 9。

在與 Central Node（嵌入式 Sensor）一起安裝的 Sensor 上，連線並配置用於網路流量傾印檔案的外部儲存。

要在與 Central Node（嵌入式 Sensor）一起安裝的 Sensor 上，連線並設定用於網路流量傾印檔案的外部儲存：

1. 連線一個您想要用作外部儲存、至少有 100 GB 的磁碟。
2. 進入技術支援模式。
3. 執行以下指令：

   ```
   sudo -i
   fdisk -l
   ```

   確保您連線的外部儲存磁碟顯示在主控台中。
4. 執行以下指令：

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<連線的磁碟名稱>
   ```

   > 如果您想要保留先前記錄在磁碟上的流量傾印，請跳過此步驟。

5. 開啟 `fstab` 檔案以在文字編輯器中進行編輯：

   ```
   nano /etc/fstab
   ```
6. 在檔案末尾新增以下行：

   ```
   /dev/<連線的磁碟名稱>/data/volumes/dumps/ ext4 defaults 0 0
   ```
7. 關閉文字編輯器。
8. 重新啟動 daemon-reload 服務：

   ```
   systemctl daemon-reload
   ```
9. 掛載磁碟：

   ```
   mount -a
   ```
10. 確保磁碟已掛載：

    ```
    df -h | grep /data/volumes/dumps
    ```
11. 執行以下指令：

    rm -r /data/volumes/dumps/*

    > 如果您想要保留先前記錄在磁碟上的流量傾印，請跳過此步驟。

12. 執行以下指令：

    ```
    chown kluser:klusers /data/volumes/dumps/
    ls -lah /data/volumes/dumps/
    lsblk
    ```

確保在**掛載點**欄中，已連線的磁碟名稱旁會顯示 **/data/volumes/dumps**。

13. 執行以下指令：

    ```
    docker service update kata_product_main_1_preprocessor_span --force
    docker ps | grep preprocessor_span
    ```

    等待主控台中出現“**Up <秒數> seconds**”狀態。

14. 執行以下指令：

    ```
    docker exec -it $(docker ps | grep preprocessor_span | awk '{print $1}') bash
    lsblk
    ```

    確保在 **MOUNTPOINTS** 欄中，已連線的磁碟名稱旁會顯示 **/mnt/kaspersky/nta/dumps**。這表示伺服器上的 /data/volumes/dumps/ 資料夾已掛載到 Docker 容器中，並被指定為 /mnt/kaspersky/nta/dumps。

15. 利用管理員帳戶登入應用程式 Web 介面。

16. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。

17. 點擊相關 Sensor 元件的卡片。

    這將開啟一個視窗，其中包含有關元件的資訊。

18. 點擊“**編輯**”。

19. 選擇“**外部儲存**”索引標籤，然後使用“**為流量傾印檔案連線外部儲存**”開關啟用外部儲存模式。

20. 在“**最大大小**”下設定儲存流量傾印檔案的空間限制。

    您可以選擇大小限制的計量單位：**MB**或**GB**。

21. 如有必要，請在“**使用 BPF 進行過濾**”部分啟用過濾功能，並輸入使用 BPF (Berkeley Packet Filter) 技術進行過濾的表達式。BPF 篩選表達式的寫入格式為 libpcap。有關語法的更多詳細資訊，請參閱“pcap-filter 手冊頁”。

22. 如有必要，在“**儲存時間限制**”部分中，對檔案的最短儲存時間進行限制，並指定相關的天數。

23. 點擊“**儲存**”。

安裝了 Sensor 和 Central Node 的伺服器上用於網路流量傾印檔案的外部儲存已連線並配置。

在安裝了 Sensor 元件的獨立伺服器上連線和設定網路流量傾印檔案的外部儲存

若要在安裝了 Sensor 元件的獨立伺服器上連線和設定網路流量傾印檔案的外部儲存：

1. 連線一個您想要用作外部儲存、至少有 100 GB 的磁碟。

2. 進入技術支援模式。

3. 執行以下指令：

    ```
    sudo -i
    fdisk -l
    ```

    確保您連線的外部儲存磁碟顯示在主控台中。

4. 執行以下指令：

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<連線的磁碟名稱>
   ```

   > 如果您想要保留先前記錄在磁碟上的流量傾印，請跳過此步驟。

5. 開啟 `fstab` 檔案以在文字編輯器中進行編輯：

   ```
   nano /etc/fstab
   ```

6. 在檔案末尾新增以下行：

   ```
   /dev/<連線的磁碟名稱>/data/volumes/dumps/ ext4 defaults 0 0
   ```

7. 關閉文字編輯器。

8. 重新啟動 daemon-reload 服務：

   ```
   systemctl daemon-reload
   ```

9. 掛載磁碟：

   ```
   mount -a
   ```

10. 確保磁碟已掛載：

    ```
    df -h | grep /data/volumes/dumps
    ```

11. 執行以下指令：

    rm -r /data/volumes/dumps/*

    > 如果您想要保留先前記錄在磁碟上的流量傾印，請跳過此步驟。

12. 執行以下指令：

    ```
    rm -r /data/volumes/dumps/*
    ```

    > 這些命令會從連線的磁碟中刪除所有資料。

13. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。

14. 點擊相關 Sensor 元件的卡片。

    這將開啟一個視窗，其中包含有關元件的資訊。

15. 點擊“**編輯**”。

16. 選擇“**外部儲存**”索引標籤，然後使用“**為流量傾印檔案連線外部儲存**”開關啟用外部儲存模式。

17. 在“**最大大小**”下設定儲存流量傾印檔案的空間限制。

    您可以選擇大小限制的計量單位：**MB**或**GB**。

18. 如有必要，請在“**使用 BPF 進行過濾**”部分啟用過濾功能，並輸入使用 BPF (Berkeley Packet Filter) 技術進行過濾的表達式。BPF 篩選表達式的寫入格式為 libpcap。有關語法的更多詳細資訊，請參閱“pcap-filter 手冊頁”。

19. 如有必要，在“**儲存時間限制**”部分中，對檔案的最短儲存時間進行限制，並指定相關的天數。

20. 點擊“**儲存**”。

安裝了 Sensor 元件的獨立伺服器上網路流量傾印檔案的外部儲存已連線並設定。

配置應用程式的大小設定

您可以變更 Central Node 元件上的運作負載。例如，您可以將額外的 Endpoint Agent 或Sensor 元件連線到該元件。為此，您需要指定計劃的 SPAN 流量、郵件流量、Endpoint Agent 元件的數量，以及儲存和事件資料庫的大小。Kaspersky Anti Targeted Attack Platform 將根據指定的設定決定 Central Node 伺服器的最佳配置。

如果 Central Node 元件被部署為叢集，則應用程式會決定叢集中所有伺服器的最佳配置。

為了使叢集正常運行，在配置大小參數後，必須在叢集的伺服器上同步時間。在配置大小參數之前，請確保為叢集中至少一台伺服器配置了與正常運作的 NTP 伺服器的整合。

您可以在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中設定 NTP 伺服器整合，或在叢集中任何伺服器上的元件管理員功能表中進行設定。如果您之前沒有配置 NTP 伺服器整合，我們建議在配置後重新啟動叢集伺服器。

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

如果您為**Endpoint Agent 數量**、**郵件流量，每秒訊息數**、**SPAN 流量，Mbps**或**儲存，GB**設定指定較小的值，物件可能會從應用程式元件的處理佇列中刪除。

配置 Central Node 伺服器：

1. 在任何允許存取 Central Node 伺服器的電腦的瀏覽器中，將具有 Central Node 元件的伺服器的 IP 位址輸入位址列中。

   如果您使用的是應用程式的高可用性版本，則可以輸入 Central Node 叢集的任何伺服器的 IP 位址或**叢集的完全限定網域名稱 (FQDN)**。

   為了確保程式 Web 介面的存取不間斷，可以在DNS 伺服器上設定輪詢調度演算法功能。為此，請登入 Central Node 叢集的第一台正常伺服器的 Web 介面。

   Kaspersky Anti Targeted Attack Platform 使用者的帳戶憑據輸入視窗開啟。

2. 輸入使用者名稱“admin”，以及在安裝應用程式期間設定的密碼。

3. 點擊**登入**。

4. 前往**伺服器配置**部分。

5. 在**Endpoint Agent 數量**欄位中，指定基礎架構的 Endpoint Agent 主機有效數量。

   有關如何計算 Endpoint Agent 元件有效數量的詳細資訊，請參閱 規模調整指南。

   如果您不使用 KEDR 產品授權金鑰，請指定0。

6. 在**郵件流量，每秒訊息數**欄位中，指定計劃每秒傳送的電子郵件數量。

   如果您不使用 KATA 或 KATA/NDR 產品授權金鑰，請指定 0。

7. 在**SPAN 流量，Mbps**欄位中，指定來自具有 Sensor 元件的伺服器上的 SPAN 連接埠的計畫流量。

   如果您不使用 KATA 或 KATA/NDR 產品授權金鑰，請指定 0。

8. 如果您在伺服器上安裝了 Central Node，則在**磁碟空間**部分中指定**事件資料庫**，**GB**和**儲存**，**GB**欄位中的值。

   有關計算事件資料庫和儲存大小的資訊，請參閱計算事件資料庫和儲存大小以設定應用程式擴充參數一節。

9. 如果您將 Central Node 安裝為叢集，則在**可用磁碟空間：**部分中，透過以下方式之一指定事件資料庫和儲存的大小：

   - 將分隔**事件資料庫**和**儲存**的滑桿向左或向右移動。

     請記住，減少事件資料庫或儲存的大小會根據輪換規則不可逆地刪除最舊的資料。擴大事件資料庫或儲存不會導致資料遺失。

   - 指定**事件資料庫**，**GB**和**儲存**，**GB**欄位中的值。

     有關計算事件資料庫和儲存大小的資訊，請參閱計算事件資料庫和儲存大小以設定應用程式擴充參數一節。

   - 如有必要，您可以透過移動右側的最後一個滑桿在磁碟上留下可用空間。

   安裝 Central Node 元件時，會自動為警示資料庫保留磁碟空間。

10. 點擊**配置**。

   如果伺服器上安裝了Central Node，Kaspersky Anti Targeted Attack Platform 會根據指定的參數決定最佳伺服器配置。如果 Central Node 作為叢集安裝，則應用程式將配置叢集的伺服器。

   套用大小設定並啟動所有必要的服務需要一些時間，因此我們建議您在完成大小配置後約 20 分鐘登入Web 介面並繼續管理應用程式。

配置防火牆規則

應用程式及其元件的正常運作需要在連線到已安裝應用程式元件的電腦的網路裝置上設定防火牆規則。

元件的作業系統已預先配置防火牆規則。我們強烈建議不要變更 iptables 規則。

裝有 Kaspersky Anti Targeted Attack Platform 元件的電腦使用的連接埠

所描述的規則適用於所有類型的主機，無論配置為何。這些規則透過 kata-firewall systemd 服務套用，僅適用於 INPUT 和DOCKER-USER 鏈。

INPUT 鏈

此鏈管理與具有 Kaspersky Anti Targeted Attack Platform 元件的電腦的所有連線。

網路規則如下表所列。

INPUT 鏈的網路規則

目標服務或協協議	連接埠	協定	sport	dport	外部網路存取
SSH	22	TCP	—	✓	✓
SMTP	25	TCP	—	✓	✓
DNS	53	TCP	—	✓	✓
HTTP	80	TCP	—	✓	✓
SNMPD	161	UDP	—	✓	✓
HTTPS	443	TCP	—	✓	✓
preprocessor_icap	1334	TCP	—	✓	✓
docker swarm	2377	TCP	✓	✓	—
etcd	2379	TCP	—	✓	✓
etcd	2380	TCP	—	✓	✓
ceph_mon	3300	TCP	—	✓	✓
VXLAN	4789	TCP/UDP	✓	✓	—
ceph_mon	6789	TCP	—	✓	✓
ceph OSD	6800:6900	TCP	—	✓	✓
docker swarm	7946	TCP/UDP	✓	✓	—
ipsec_manager	8084	TCP	✓	✓	—
pcap_manager	8085	TCP	—	✓	✓
HTTPS	8443	TCP/UDP	—	✓	✓
HTTPS	8444	TCP/UDP	—	✓	✓

目標服務或協協議	連接埠	協定	sport	dport	外部網路存取
suricata_metrics_exporter	9103	TCP	✓	✓	—
node_exporter	9141	TCP	✓	✓	—
cadvisor	9142	TCP	✓	✓	—
preprocessor_metrics_exporter	9191	TCP	✓	✓	—
pcap_manager_metrics_exporter	9192	TCP	✓	✓	—
ceph_mgr	9283	TCP	—	✓	✓
ceph_rgw	9284	TCP	—	✓	✓
NDR Sensor	9443	TCP	—	✓	✓
kafka bootstrap	11000:11006	TCP	—	✓	✓

DOCKER-USER 鏈

此鏈管理用於應用程式元件定址的網路連線。網路規則如下表所列。

DOCKER-USER 鏈的網路規則

目標服務或協協議	連接埠	協定	sport	dport
SMTP	25	TCP	—	✓
DNS	53	TCP/UDP	—	✓
HTTP	80	TCP	—	✓
HTTPS	443	TCP	—	✓
preprocessor_icap	1344	UDP	—	✓
NDR NATS (KICKS NAT)	7423	TCP	—	✓
NDR public API	8070	TCP	—	✓
deployment API	8080	TCP	✓	✓
部署管理 API	8090	TCP	✓	✓
授權服務	8091	TCP	✓	✓
HTTPS	8443	TCP	—	✓
apt collector ssl	9081	TCP	—	✓
Sensor	9443	TCP	—	✓
NDR EKA	13520	TCP	—	✓

叢集配置中 Kaspersky Anti Targeted Attack Platform 服務使用的連接埠

為了使應用程式在叢集配置中正常運作，您必須根據下表為我們的傳出連線配置網路存取。

叢集配置中 Kaspersky Anti Targeted Attack Platform 服務使用的連接埠

服務	連接埠	協定
agent_database_configurator	2379	TCP
agent_database_configurator	5432	TCP
agent_database_synchronizer	2379	TCP
agent_database_synchronizer	5432	TCP
agent_database_synchronizer	9092	TCP
agent_database_synchronizer	9100	TCP
agent_database_synchronizer	10000:10010	TCP
agent_server	1080	TCP
agent_server	2379	TCP
agent_server	5432	TCP
agent_server	8100	TCP
agent_server	9090	TCP
agent_server	9284	TCP
antiapt_database_configurator	2379	TCP
antiapt_database_configurator	5432	TCP
authorization_service	2379	TCP
authorization_service	4567	TCP
authorization_service	8090	TCP
authorization_service	8443	TCP
authorization_service	8701	TCP
authorization_service	8899	TCP
cadvisor	任何	任何
ceph_management_api	2379	TCP
ceph_management_api	3300	TCP
ceph_management_api	6789	TCP
ceph_management_api	8765	TCP
ceph_management_api	8080	TCP
ceph_management_api	9283	TCP
ceph_management_api	9284	TCP
ceph_mgr	2379	TCP
ceph_mgr	3300	TCP
ceph_mgr	6789	TCP
ceph_mgr	6800:6900	TCP
ceph_mgr	9141	TCP
ceph_mgr	9142	TCP
ceph_mgr	9283	TCP
ceph_mgr	9284	TCP
ceph_mon	2379	TCP
ceph_mon	3300	TCP
ceph_mon	6789	TCP

服務	連接埠	協定
ceph_mon	6800:6900	TCP
ceph_mon	9141	TCP
ceph_mon	9142	TCP
ceph_mon	9283	TCP
ceph_mon	9284	TCP
ceph_osd	2379	TCP
ceph_osd	3300	TCP
ceph_osd	6789	TCP
ceph_osd	6800:6900	TCP
ceph_osd	9141	TCP
ceph_osd	9142	TCP
ceph_osd	9283	TCP
ceph_osd	9284	TCP
ceph_rgw	2379	TCP
ceph_rgw	3300	TCP
ceph_rgw	6789	TCP
ceph_rgw	6800:6900	TCP
ceph_rgw	9141	TCP
ceph_rgw	9142	TCP
ceph_rgw	9283	TCP
ceph_rgw	9284	TCP
ceph_rgw_configurator	2379	TCP
ceph_rgw_configurator	3300	TCP
ceph_rgw_configurator	6789	TCP
ceph_rgw_configurator	6800:6900	TCP
ceph_rgw_configurator	9141	TCP
ceph_rgw_configurator	9142	TCP
ceph_rgw_configurator	9283	TCP
ceph_rgw_configurator	9284	TCP
clickhouse	2379	TCP
clickhouse	8123	TCP
clickhouse	9000	TCP
clickhouse_database_configurator	2379	TCP
clickhouse_database_configurator	9000	TCP
clickhouse_metrics_importer	2379	TCP
clickhouse_metrics_importer	6379	TCP
clickhouse_metrics_importer	8123	TCP
clickhouse_metrics_importer	9000	TCP
clickhouse_metrics_importer	9090	TCP
coredns	53	TCP
coredns	53	TCP

服務	連接埠	協定
coredns	2379	TCP
deployment_api	22	TCP
deployment_api	2377	TCP
deployment_api	2379	TCP
deployment_api	4567	TCP
deployment_api	8080	TCP
deployment_api	8443	TCP
deployment_api	8701	TCP
deployment_api	9141	TCP
deployment_api	9284	TCP
deployment_management_api	53	TCP
deployment_management_api	2379	TCP
deployment_management_api	4567	TCP
deployment_management_api	8091	TCP
deployment_management_api	8443	TCP
deployment_management_api	8701	TCP
deployment_management_api	8702	TCP
deployment_management_api	8765	TCP
deployment_management_api	8899	TCP
deployment_management_api	9141	TCP
dhcp_server	任何	任何
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
edr_synchronizer	514	TCP
edr_synchronizer	514	UDP
edr_synchronizer	2379	TCP
edr_synchronizer	5432	TCP
edr_synchronizer	6379	TCP
edr_synchronizer	8081	TCP
edr_synchronizer	8082	TCP
edr_synchronizer	8083	TCP
edr_synchronizer	9092	TCP
edr_synchronizer	10000:10010	TCP
edr_synchronizer	33334	TCP
elasticsearch	2379	TCP
elasticsearch	9200	TCP
elasticsearch	9300	TCP
elasticsearch_data	2379	TCP
elasticsearch_data	9200	TCP
elasticsearch_data	9300	TCP
elasticsearch_exporter	2379	TCP

服務	連接埠	協定
elasticsearch_exporter	9200	TCP
elasticsearch_exporter	9300	TCP
etcd	2379	TCP
etcd	2380	TCP
events_api	80	TCP
events_api	2379	TCP
events_api	5432	TCP
events_api	8080	TCP
events_api	8081	TCP
events_api	9092	TCP
events_api	9100	TCP
events_api	9284	TCP
events_api	10000:10010	TCP
fastsearch	2379	TCP
fastsearch	8080	TCP
fastsearch	8180	TCP
fastsearch_events_cleaner	9200	TCP
fastsearch_events_importer	2379	TCP
fastsearch_events_importer	8081	TCP
fastsearch_events_importer	9092	TCP
fastsearch_events_importer	9100	TCP
fastsearch_events_importer	9200	TCP
fastsearch_events_importer	10000:10010	TCP
hunts_database_configurator	2379	TCP
hunts_database_configurator	5432	TCP
hunts_database_synchronizer	2379	TCP
hunts_database_synchronizer	5432	TCP
hunts_database_synchronizer	9092	TCP
hunts_database_synchronizer	10000:10010	TCP
hunts_event_processor	2379	TCP
hunts_event_processor	5432	TCP
hunts_event_processor	8080	TCP
hunts_event_processor	8081	TCP
hunts_event_processor	9092	TCP
hunts_event_processor	9100	TCP
hunts_event_processor	10000:10010	TCP
hunts_statistics_api	2379	TCP
hunts_statistics_api	5432	TCP
hunts_statistics_api	8080	TCP
hunts_statistics_api	8081	TCP
hunts_statistics_api	9092	TCP

服務	連接埠	協定
hunts_statistics_api	9100	TCP
hunts_statistics_api	10000:10010	TCP
hunts_statistics_processor	2379	TCP
hunts_statistics_processor	5432	TCP
hunts_statistics_processor	8080	TCP
hunts_statistics_processor	8081	TCP
hunts_statistics_processor	9092	TCP
hunts_statistics_processor	9100	TCP
hunts_statistics_processor	9200	TCP
hunts_statistics_processor	10000:10010	TCP
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
ids_alert_syncer	514	UDP
ids_alert_syncer	2379	TCP
ids_alert_syncer	5432	TCP
ids_alert_syncer	777	TCP
ids_alert_syncer	8083	TCP
ids_alert_syncer	9092	TCP
ids_alert_syncer	9200	TCP
ids_alert_syncer	10000:10010	TCP
ids_alert_syncer	33334	TCP
ioa_update_validator	2379	TCP
ipsec_manager	80	TCP
ipsec_manager	2379	TCP
kafka	2379	TCP
kafka	2181	TCP
kafka	9092	TCP
kafka	9095	TCP
kafka	10000:10010	TCP
kafka_configurator	2181	TCP
kafka_configurator	2379	TCP
kafka_configurator	9092	TCP
kafka_configurator	10000:10010	TCP
kafka_exporter	2379	TCP
kafka_exporter	9092	TCP
kafka_exporter	9100	TCP
kafka_exporter	10000:10010	TCP
kafka_proxy	任何	任何
kata_scanner	25	TCP
kata_scanner	80	TCP
kata_scanner	514	TCP

服務	連接埠	協定
kata_scanner	514	UDP
kata_scanner	443	TCP
kata_scanner	2379	TCP
kata_scanner	5432	TCP
kata_scanner	6379	TCP
kata_scanner	7777	TCP
kata_scanner	8081	TCP
kata_scanner	8082	TCP
kata_scanner	8083	TCP
kata_scanner	9081	TCP
kata_scanner	9090	TCP
kata_scanner	9092	TCP
kata_scanner	9100	TCP
kata_scanner	9284	TCP
kata_scanner	10000:10010	TCP
kata_scanner	33334	TCP
ksb_agent_server	80	TCP
ksb_agent_server	2379	TCP
ksb_agent_server	5432	TCP
ksb_agent_server	8082	TCP
ksb_agent_server	8083	TCP
ksb_agent_server	9898	TCP
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
ksn_proxy	1:65535	TCP
ksqldb_configurator	2379	TCP
ksqldb_configurator	5432	TCP
ksqldb_configurator	8083	TCP
ksqldb_configurator	8088	TCP
ksqldb_configurator	9092	TCP
ksqldb_configurator	10000:10010	TCP
ksqldb_server	2379	TCP
ksqldb_server	5432	TCP

服務	連接埠	協定
ksqldb_server	9092	TCP
ksqldb_server	11000:11006	TCP
management_ui	2379	TCP
management_ui	8091	TCP
monitoring_grafana	3000	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
monitoring_prometheus	9283	TCP
multitenancy_management_api	2379	TCP
multitenancy_management_api	4567	TCP
multitenancy_management_api	8443	TCP
multitenancy_management_api	8701	TCP
multitenancy_management_api	8090	TCP
multitenancy_management_api	8899	TCP
nginx_exporter	2379	TCP
nginx_gateway	80	TCP
nginx_gateway	81	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	4443	TCP
nginx_gateway	4567	TCP
nginx_gateway	6379	TCP
nginx_gateway	8080	TCP
nginx_gateway	8081	TCP
nginx_gateway	8082	TCP
nginx_gateway	8083	TCP
nginx_gateway	8085	TCP
nginx_gateway	8090	TCP
nginx_gateway	8100	TCP
nginx_gateway	8443	TCP
nginx_gateway	8444	TCP
nginx_gateway	8701	TCP
nginx_gateway	8702	TCP
nginx_gateway	8899	TCP
nginx_gateway	9393	TCP

服務	連接埠	協定
nginx_gateway	9898	TCP
node_exporter	任何	任何
nta_core	25	TCP
nta_core	80	TCP
nta_core	2379	TCP
nta_core	5433	TCP
nta_core	8082	TCP
nta_core	8083	TCP
nta_core	9443	TCP
nta_database	-	-
nta_database_configurator	2379	TCP
nta_database_configurator	5432	TCP
nta_database_configurator	5432	TCP
nta_sensor_configurator	2379	TCP
nta_sensor_configurator	8084	TCP
nta_sensor_configurator	9443	TCP
nta_sensor_configurator	50051	TCP
nta_syncer	80	TCP
nta_syncer	2379	TCP
nta_syncer	5422	TCP
nta_syncer	5423	TCP
nta_syncer	7777	TCP
nta_syncer	8084	TCP
nta_syncer	9092	TCP
nta_syncer	10000:10010	TCP
nta_syncer	50051	TCP
postfix	25	TCP
postfix	2379	TCP
postgresql_exporter	2379	TCP
postgresql_exporter	5432	TCP
postgresql_exporter	9100	TCP
postgresql_server	2379	TCP
postgresql_server	5432	TCP
preprocessor	任何	任何
preprocessor_icap	80	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP

服務	連接埠	協定
preprocessor_icap	8081	TCP
preprocessor_icap	8082	TCP
preprocessor_icap	8083	TCP
preprocessor_icap	9092	TCP
preprocessor_icap	9192	TCP
preprocessor_icap	9284	TCP
preprocessor_icap	10000:10010	TCP
preprocessor_pop	110	TCP
preprocessor_pop	514	TCP
preprocessor_pop	514	UDP
preprocessor_pop	2379	TCP
preprocessor_pop	4223	TCP
preprocessor_pop	6379	TCP
preprocessor_pop	7777	TCP
preprocessor_pop	8081	TCP
preprocessor_pop	8082	TCP
preprocessor_pop	8083	TCP
preprocessor_pop	9081	TCP
preprocessor_pop	9092	TCP
preprocessor_pop	10000:10010	TCP
preprocessor_pop	1:65535	TCP
preprocessor_smtp	514	TCP
preprocessor_smtp	514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8082	TCP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	10000:10010	TCP
preprocessor_span	任何	任何
primary_database_configurator	2379	TCP
primary_database_configurator	5432	TCP
redis	2379	TCP
redis	6379	TCP
response_actions_processor	514	TCP
response_actions_processor	514	UDP
response_actions_processor	2379	TCP

服務	連接埠	協定
response_actions_processor	5432	TCP
response_actions_processor	8081	TCP
response_actions_processor	9092	TCP
response_actions_processor	9100	TCP
response_actions_processor	10000:10010	TCP
response_api	514	TCP
response_api	514	UDP
response_api	2379	TCP
response_api	5432	TCP
response_api	8080	TCP
response_api	9092	TCP
response_api	9100	TCP
response_api	10000:10010	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9283	TCP
s3rotator	9284	TCP
schema_registry	2379	TCP
schema_registry	8081	TCP
schema_registry	9092	TCP
schema_registry	10000:10010	TCP
sensor_event_processor	2379	TCP
sensor_event_processor	8080	TCP
sensor_event_processor	8081	TCP
sensor_event_processor	9092	TCP
sensor_event_processor	9100	TCP
sensor_event_processor	10000:10010	TCP
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
siem_proxy	任何	任何
snmpd	161	TCP
snmpd	2379	TCP

服務	連接埠	協定
updater	80	TCP
updater	443	TCP
updater	514	TCP
updater	514	TCP
updater	2379	TCP
updater	5432	TCP
updater	6379	TCP
updater	7777	TCP
updater	8083	TCP
updater	9100	TCP
updater	9500	TCP
updater	1:65535	TCP
updates_consistency_checker	80	TCP
updates_consistency_checker	2379	TCP
updates_consistency_checker	6379	TCP
updates_consistency_checker	8083	TCP
updates_consistency_checker	9092	TCP
updates_consistency_checker	10000:10010	TCP
web_backend	25	TCP
web_backend	80	TCP
web_backend	443	TCP
web_backend	514	TCP
web_backend	514	UDP
web_backend	1080	TCP
web_backend	2379	TCP
web_backend	5432	TCP
web_backend	6379	TCP
web_backend	7777	TCP
web_backend	8080	TCP
web_backend	8081	TCP
web_backend	8082	TCP
web_backend	8083	TCP
web_backend	8085	TCP
web_backend	8090	TCP
web_backend	8123	TCP
web_backend	8283	TCP
web_backend	8443	TCP
web_backend	8444	TCP
web_backend	8899	TCP
web_backend	9090	TCP
web_backend	9092	TCP

服務	連接埠	協定
web_backend	9284	TCP
web_backend	9500	TCP
web_backend	10000:10010	TCP
web_backend	33334	TCP
zookeeper	2181	TCP
zookeeper	2379	TCP
zookeeper	2888	TCP
zookeeper	3888	TCP
zookeeper	9092	TCP
zookeeper	10000:10010	TCP

作為伺服器部署的 Central Node 的服務使用的連接埠

為了使應用程式能夠與作為伺服器部署的 Central Node 元件正確協同工作，必須按照下表為傳出連線配置網路存取。

在 Central Node 元件作為伺服器部署的配置中，服務使用的連接埠

服務	連接埠	協定
agent_database_configurator	2379	TCP
agent_database_configurator	5432	TCP
agent_database_synchronizer	2379	TCP
agent_database_synchronizer	5432	TCP
agent_database_synchronizer	9092	TCP
agent_database_synchronizer	9100	TCP
agent_database_synchronizer	10000:10010	TCP
agent_server	1080	TCP
agent_server	2379	TCP
agent_server	5432	TCP
agent_server	8100	TCP
agent_server	9090	TCP
agent_server	9284	TCP
antiapt_database_configurator	2379	TCP
antiapt_database_configurator	5432	TCP
authorization_service	2379	TCP
authorization_service	4567	TCP
authorization_service	8090	TCP
authorization_service	8443	TCP
authorization_service	8701	TCP
authorization_service	8899	TCP
cadvisor	任何	任何
clickhouse	2379	TCP

服務	連接埠	協定
clickhouse	8123	TCP
clickhouse	9000	TCP
clickhouse_database_configurator	2379	TCP
clickhouse_database_configurator	9000	TCP
clickhouse_metrics_importer	2379	TCP
clickhouse_metrics_importer	6379	TCP
clickhouse_metrics_importer	8123	TCP
clickhouse_metrics_importer	9000	TCP
clickhouse_metrics_importer	9090	TCP
coredns	53	TCP
coredns	53	TCP
coredns	2379	TCP
deployment_api	22	TCP
deployment_api	2377	TCP
deployment_api	2379	TCP
deployment_api	4567	TCP
deployment_api	8080	TCP
deployment_api	8443	TCP
deployment_api	8701	TCP
deployment_api	9141	TCP
deployment_api	9284	TCP
deployment_management_api	53	TCP
deployment_management_api	2379	TCP
deployment_management_api	4567	TCP
deployment_management_api	8091	TCP
deployment_management_api	8443	TCP
deployment_management_api	8701	TCP
deployment_management_api	8702	TCP
deployment_management_api	8765	TCP
deployment_management_api	8899	TCP
deployment_management_api	9141	TCP
dhcp_server	任何	任何
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
edr_synchronizer	514	TCP
edr_synchronizer	514	UDP
edr_synchronizer	2379	TCP
edr_synchronizer	5432	TCP
edr_synchronizer	6379	TCP
edr_synchronizer	8081	TCP
edr_synchronizer	8082	TCP

服務	連接埠	協定
edr_synchronizer	8083	TCP
edr_synchronizer	9092	TCP
edr_synchronizer	10000:10010	TCP
edr_synchronizer	33334	TCP
elasticsearch	2379	TCP
elasticsearch	9200	TCP
elasticsearch	9300	TCP
elasticsearch_data	2379	TCP
elasticsearch_data	9200	TCP
elasticsearch_data	9300	TCP
elasticsearch_exporter	2379	TCP
elasticsearch_exporter	9200	TCP
elasticsearch_exporter	9300	TCP
etcd	2379	TCP
etcd	2380	TCP
events_api	80	TCP
events_api	2379	TCP
events_api	5432	TCP
events_api	8080	TCP
events_api	8081	TCP
events_api	9092	TCP
events_api	9100	TCP
events_api	9284	TCP
events_api	10000:10010	TCP
fastsearch	2379	TCP
fastsearch	8080	TCP
fastsearch	8180	TCP
fastsearch_events_cleaner	9200	TCP
fastsearch_events_importer	2379	TCP
fastsearch_events_importer	8081	TCP
fastsearch_events_importer	9092	TCP
fastsearch_events_importer	9100	TCP
fastsearch_events_importer	9200	TCP
fastsearch_events_importer	10000:10010	TCP
hunts_database_configurator	2379	TCP
hunts_database_configurator	5432	TCP
hunts_database_synchronizer	2379	TCP
hunts_database_synchronizer	5432	TCP
hunts_database_synchronizer	9092	TCP
hunts_database_synchronizer	10000:10010	TCP
hunts_event_processor	2379	TCP

服務	連接埠	協定
hunts_event_processor	5432	TCP
hunts_event_processor	8080	TCP
hunts_event_processor	8081	TCP
hunts_event_processor	9092	TCP
hunts_event_processor	9100	TCP
hunts_event_processor	10000:10010	TCP
hunts_statistics_api	2379	TCP
hunts_statistics_api	5432	TCP
hunts_statistics_api	8080	TCP
hunts_statistics_api	8081	TCP
hunts_statistics_api	9092	TCP
hunts_statistics_api	9100	TCP
hunts_statistics_api	10000:10010	TCP
hunts_statistics_processor	2379	TCP
hunts_statistics_processor	5432	TCP
hunts_statistics_processor	8080	TCP
hunts_statistics_processor	8081	TCP
hunts_statistics_processor	9092	TCP
hunts_statistics_processor	9100	TCP
hunts_statistics_processor	9200	TCP
hunts_statistics_processor	10000:10010	TCP
edr_synchronizer	25	TCP
edr_synchronizer	80	TCP
ids_alert_syncer	514	UDP
ids_alert_syncer	2379	TCP
ids_alert_syncer	5432	TCP
ids_alert_syncer	777	TCP
ids_alert_syncer	8083	TCP
ids_alert_syncer	9092	TCP
ids_alert_syncer	9200	TCP
ids_alert_syncer	10000:10010	TCP
ids_alert_syncer	33334	TCP
ioa_update_validator	2379	TCP
ipsec_manager	80	TCP
ipsec_manager	2379	TCP
kafka	2379	TCP
kafka	2181	TCP
kafka	9092	TCP
kafka	9095	TCP
kafka	10000:10010	TCP
kafka_configurator	2181	TCP

服務	連接埠	協定
kafka_configurator	2379	TCP
kafka_configurator	9092	TCP
kafka_configurator	10000:10010	TCP
kafka_exporter	2379	TCP
kafka_exporter	9092	TCP
kafka_exporter	9100	TCP
kafka_exporter	10000:10010	TCP
kafka_proxy	任何	任何
kata_scanner	25	TCP
kata_scanner	80	TCP
kata_scanner	514	TCP
kata_scanner	514	UDP
kata_scanner	443	TCP
kata_scanner	2379	TCP
kata_scanner	5432	TCP
kata_scanner	6379	TCP
kata_scanner	7777	TCP
kata_scanner	8081	TCP
kata_scanner	8082	TCP
kata_scanner	8083	TCP
kata_scanner	9081	TCP
kata_scanner	9090	TCP
kata_scanner	9092	TCP
kata_scanner	9100	TCP
kata_scanner	9284	TCP
kata_scanner	10000:10010	TCP
kata_scanner	33334	TCP
ksb_agent_server	80	TCP
ksb_agent_server	2379	TCP
ksb_agent_server	5432	TCP
ksb_agent_server	8082	TCP
ksb_agent_server	8083	TCP
ksb_agent_server	9898	TCP
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP

服務	連接埠	協定
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
ksn_proxy	1:65535	TCP
ksqldb_configurator	2379	TCP
ksqldb_configurator	5432	TCP
ksqldb_configurator	8083	TCP
ksqldb_configurator	8088	TCP
ksqldb_configurator	9092	TCP
ksqldb_configurator	10000:10010	TCP
ksqldb_server	2379	TCP
ksqldb_server	5432	TCP
ksqldb_server	9092	TCP
ksqldb_server	11000:11006	TCP
management_ui	2379	TCP
management_ui	8091	TCP
monitoring_grafana	3000	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
monitoring_prometheus	9283	TCP
multitenancy_management_api	2379	TCP
multitenancy_management_api	4567	TCP
multitenancy_management_api	8443	TCP
multitenancy_management_api	8701	TCP
multitenancy_management_api	8090	TCP
multitenancy_management_api	8899	TCP
nginx_exporter	2379	TCP
nginx_gateway	80	TCP
nginx_gateway	81	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	4443	TCP
nginx_gateway	4567	TCP
nginx_gateway	6379	TCP
nginx_gateway	8080	TCP
nginx_gateway	8081	TCP

服務	連接埠	協定
nginx_gateway	8082	TCP
nginx_gateway	8083	TCP
nginx_gateway	8085	TCP
nginx_gateway	8090	TCP
nginx_gateway	8100	TCP
nginx_gateway	8443	TCP
nginx_gateway	8444	TCP
nginx_gateway	8701	TCP
nginx_gateway	8702	TCP
nginx_gateway	8899	TCP
nginx_gateway	9393	TCP
nginx_gateway	9898	TCP
node_exporter	任何	任何
nta_core	25	TCP
nta_core	80	TCP
nta_core	2379	TCP
nta_core	5433	TCP
nta_core	8082	TCP
nta_core	8083	TCP
nta_core	9443	TCP
nta_database	-	-
nta_database_configurator	2379	TCP
nta_database_configurator	5432	TCP
nta_database_configurator	5432	TCP
nta_sensor_configurator	2379	TCP
nta_sensor_configurator	8084	TCP
nta_sensor_configurator	9443	TCP
nta_sensor_configurator	50051	TCP
nta_syncer	80	TCP
nta_syncer	2379	TCP
nta_syncer	5422	TCP
nta_syncer	5423	TCP
nta_syncer	7777	TCP
nta_syncer	8084	TCP
nta_syncer	9092	TCP
nta_syncer	10000:10010	TCP
nta_syncer	50051	TCP
postfix	25	TCP
postfix	2379	TCP
postgresql_exporter	2379	TCP
postgresql_exporter	5432	TCP

服務	連接埠	協定
postgresql_exporter	9100	TCP
postgresql_server	2379	TCP
postgresql_server	5432	TCP
preprocessor	任何	任何
preprocessor_icap	80	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	TCP
preprocessor_icap	8082	TCP
preprocessor_icap	8083	TCP
preprocessor_icap	9092	TCP
preprocessor_icap	9192	TCP
preprocessor_icap	9284	TCP
preprocessor_icap	10000:10010	TCP
preprocessor_pop	110	TCP
preprocessor_pop	514	TCP
preprocessor_pop	514	UDP
preprocessor_pop	2379	TCP
preprocessor_pop	4223	TCP
preprocessor_pop	6379	TCP
preprocessor_pop	7777	TCP
preprocessor_pop	8081	TCP
preprocessor_pop	8082	TCP
preprocessor_pop	8083	TCP
preprocessor_pop	9081	TCP
preprocessor_pop	9092	TCP
preprocessor_pop	10000:10010	TCP
preprocessor_pop	1:65535	TCP
preprocessor_smtp	514	TCP
preprocessor_smtp	514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8082	TCP
preprocessor_smtp	8083	TCP

服務	連接埠	協定
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	10000:10010	TCP
preprocessor_span	任何	任何
primary_database_configurator	2379	TCP
primary_database_configurator	5432	TCP
redis	2379	TCP
redis	6379	TCP
response_actions_processor	514	TCP
response_actions_processor	514	UDP
response_actions_processor	2379	TCP
response_actions_processor	5432	TCP
response_actions_processor	8081	TCP
response_actions_processor	9092	TCP
response_actions_processor	9100	TCP
response_actions_processor	10000:10010	TCP
response_api	514	TCP
response_api	514	UDP
response_api	2379	TCP
response_api	5432	TCP
response_api	8080	TCP
response_api	9092	TCP
response_api	9100	TCP
response_api	10000:10010	TCP
s3proxy	80	TCP
s3proxy	1080	TCP
s3proxy	2379	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9283	TCP
s3rotator	9284	TCP
schema_registry	2379	TCP
schema_registry	8081	TCP
schema_registry	9092	TCP
schema_registry	10000:10010	TCP
sensor_event_processor	2379	TCP
sensor_event_processor	8080	TCP
sensor_event_processor	8081	TCP
sensor_event_processor	9092	TCP
sensor_event_processor	9100	TCP

服務	連接埠	協定
sensor_event_processor	10000:10010	TCP
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
siem_proxy	任何	任何
snmpd	161	TCP
snmpd	2379	TCP
updater	80	TCP
updater	443	TCP
updater	514	TCP
updater	514	TCP
updater	2379	TCP
updater	5432	TCP
updater	6379	TCP
updater	7777	TCP
updater	8083	TCP
updater	9100	TCP
updater	9500	TCP
updater	1:65535	TCP
updates_consistency_checker	80	TCP
updates_consistency_checker	2379	TCP
updates_consistency_checker	6379	TCP
updates_consistency_checker	8083	TCP
updates_consistency_checker	9092	TCP
updates_consistency_checker	10000:10010	TCP
web_backend	25	TCP
web_backend	80	TCP
web_backend	443	TCP
web_backend	514	TCP
web_backend	514	UDP
web_backend	1080	TCP
web_backend	2379	TCP
web_backend	5432	TCP
web_backend	6379	TCP

服務	連接埠	協定
web_backend	7777	TCP
web_backend	8080	TCP
web_backend	8081	TCP
web_backend	8082	TCP
web_backend	8083	TCP
web_backend	8085	TCP
web_backend	8090	TCP
web_backend	8123	TCP
web_backend	8283	TCP
web_backend	8443	TCP
web_backend	8444	TCP
web_backend	8899	TCP
web_backend	9090	TCP
web_backend	9092	TCP
web_backend	9284	TCP
web_backend	9500	TCP
web_backend	10000:10010	TCP
web_backend	33334	TCP
zookeeper	2181	TCP
zookeeper	2379	TCP
zookeeper	2888	TCP
zookeeper	3888	TCP
zookeeper	9092	TCP
zookeeper	10000:10010	TCP

在獨立伺服器上安裝 Sensor 元件的配置中，服務使用的連接埠

為了讓應用程式在 Sensor 元件安裝在獨立伺服器上的設定下正常運作，您必須根據下表為傳出連線設定網路存取。

在獨立伺服器上安裝 Sensor 元件的配置中，服務使用的連接埠

服務	連接埠	協定
cadvisor	任何	任何
ksn_proxy	80	TCP
ksn_proxy	443	TCP
ksn_proxy	514	TCP
ksn_proxy	514	UDP
ksn_proxy	2379	TCP
ksn_proxy	7777	TCP

服務	連接埠	協定
ksn_proxy	8083	TCP
ksn_proxy	9092	TCP
ksn_proxy	9102	TCP
ksn_proxy	10000:10010	TCP
monitoring_prometheus	2379	TCP
monitoring_prometheus	9090	TCP
monitoring_prometheus	9100	TCP
monitoring_prometheus	9102	TCP
monitoring_prometheus	9141	TCP
monitoring_prometheus	9142	TCP
monitoring_prometheus	9191	TCP
monitoring_prometheus	9192	TCP
nginx_gateway	443	TCP
nginx_gateway	2379	TCP
nginx_gateway	8085	TCP
nginx_gateway	8100	TCP
nginx_gateway	8283	TCP
node_exporter	任何	TCP
preprocessor_icap	443	TCP
preprocessor_icap	1080	TCP
preprocessor_icap	1344	TCP
preprocessor_icap	1514	TCP
preprocessor_icap	1514	UDP
preprocessor_icap	2379	TCP
preprocessor_icap	4223	TCP
preprocessor_icap	6379	TCP
preprocessor_icap	7777	TCP
preprocessor_icap	8081	UDP
preprocessor_icap	8082	TCP
preprocessor_icap	8082	UDP
preprocessor_icap	8083	TCP
preprocessor_icap	8085	TCP
preprocessor_icap	9092	TCP
preprocessor_pop3	1514	TCP
preprocessor_pop3	1514	UDP
preprocessor_pop3	2379	TCP
preprocessor_pop3	4223	TCP
preprocessor_pop3	6379	TCP
preprocessor_pop3	7777	TCP
preprocessor_pop3	8081	TCP
preprocessor_pop3	8081	UDP

服務	連接埠	協定
preprocessor_pop3	8082	UDP
preprocessor_pop3	8083	TCP
preprocessor_pop3	9081	TCP
preprocessor_pop3	9092	TCP
preprocessor_pop3	11000	TCP
preprocessor_smtp	1514	TCP
preprocessor_smtp	1514	UDP
preprocessor_smtp	2379	TCP
preprocessor_smtp	4223	TCP
preprocessor_smtp	6379	TCP
preprocessor_smtp	7777	TCP
preprocessor_smtp	8081	TCP
preprocessor_smtp	8081	UDP
preprocessor_smtp	8082	UDP
preprocessor_smtp	8083	TCP
preprocessor_smtp	9081	TCP
preprocessor_smtp	9092	TCP
preprocessor_smtp	11000	TCP
preprocessor_span	任何	任何
preprocessor_span	13520	TCP
preprocessor_span	8081	UDP
preprocessor_span	8082	UDP
preprocessor_span	9081	TCP
preprocessor_span	7777	TCP
preprocessor_span	9092	TCP
preprocessor_span	8083	TCP
preprocessor_span	2379	TCP
preprocessor_span	6379	TCP
redis	2379	TCP
redis	6379	TCP
s3proxy	80	TCP
s3proxy	1080	TCP
s3proxy	2379	TCP
s3rotator	80	TCP
s3rotator	1080	TCP
s3rotator	2379	TCP
s3rotator	9284	TCP
sensor_management_api	任何	任何
services_configurator	2379	TCP
siem_proxy	80	TCP
siem_proxy	514	TCP

服務	連接埠	協定
siem_proxy	514	UDP
siem_proxy	1080	TCP
siem_proxy	1514	TCP
siem_proxy	1514	UDP
siem_proxy	2080	TCP
siem_proxy	2379	TCP
siem_proxy	9284	TCP
snmpd	161	TCP
snmpd	2379	TCP

網路流量分析服務之間的通訊連接埠

為了使應用程式正常運作，您必須確保網路流量分析服務可以透過下表列出的連接埠進行通訊。預設允許服務的入站連線。

網路流量分析服務之間的通訊連接埠

服務	連接埠	目標服務	協定
nta_database_configurator	5433	nta_database	TCP
nta_core	5433	nta_database	TCP
nta_core	2379	etcd	TCP
nta_core	80	web_backend	TCP
nta_core	9443	網際網路	TCP
nta_syncer	9092	kafka	TCP
nta_syncer	2379	etcd	TCP
nta_syncer	5432	postgresql_server	TCP
nta_syncer	5433	nta_database	TCP
nta_syncer	50051	nta_core	TCP
nta_syncer	8084	nta_core	TCP
nta_sensor_configurator	50051	nta_core	UDP
nta_sensor_configurator	9443	nta_core	TCP
preprocessor_span	13520	nta_core	TCP
preprocessor_span	8081	kata_scanner	UDP
preprocessor_span	8082	kata_scanner	UDP
preprocessor_span	9081	kata_scanner	TCP
preprocessor_span	7777	ksn_proxy	TCP
preprocessor_span	9092	kafka	TCP
preprocessor_span	8083	updater	TCP
preprocessor_span	2379	etcd	TCP
preprocessor_span	6379	redis	TCP
preprocessor_icap	9092	kafka	TCP
preprocessor_icap	7777	ksn_proxy	TCP

服務	連接埠	目標服務	協定
preprocessor_icap	8081	kata_scanner	UDP
preprocessor_icap	8082	kata_scanner	UDP
preprocessor_icap	2379	etcd	TCP
preprocessor_icap	8083	updater	TCP
preprocessor_icap	4223	preprocessor_span	TCP
preprocessor_smtp	8081	kata_scanner	UDP
preprocessor_smtp	8082	kata_scanner	UDP
preprocessor_smtp	9081	kata_scanner	TCP
preprocessor_smtp	7777	ksn_proxy	TCP
preprocessor_smtp	9092	kafka	TCP
preprocessor_smtp	8083	updater	TCP
preprocessor_smtp	2379	etcd	TCP
preprocessor_smtp	6379	redis	TCP
preprocessor_smtp	4223	preprocessor_span	TCP
preprocessor_pop3	8081	kata_scanner	UDP
preprocessor_pop3	8082	kata_scanner	UDP
preprocessor_pop3	9081	kata_scanner	TCP
preprocessor_pop3	7777	ksn_proxy	TCP
preprocessor_pop3	9092	kafka	TCP
preprocessor_pop3	8083	updater	TCP
preprocessor_pop3	2379	etcd	TCP
preprocessor_pop3	6379	redis	TCP
preprocessor_pop3	4223	preprocessor_span	TCP

在 iptables 中管理 MTU 設定

如果您知道您的 ISP 限制解決方案元件之間的連結上的 MTU 大小，您可以管理 iptables 中的 MTU 設定，以使 MTU 大小不超過指定值。例如，如果您的 ISP 將 MTU 大小限制為 1450，則您可以在 iptables 中指定 1400。

為了使配置更容易，並讓設定在解決方案元件重新啟動後仍然有效，我們建議使用 kata-firewall-persist-mtu 實用程式。當您將 Kaspersky Anti Targeted Attack Platform 升級到 7.1 版本時，此實用程式可用。

要管理 iptables 中的 MTU 設定：

1. 透過 SSH 或終端登入 Central Node 伺服器的管理主控台。

   如果 Central Node 部署為叢集，請登入 Docker swarm 中具有管理器角色的任一叢集伺服器的管理主控台。若要檢視角色，請使用 `$ docker node ls` 指令。

2. 系統提示時，請輸入管理員使用者名稱和在安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表中，選擇**技術支援模式**。

4. 按下 **Enter**。

   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**確定**並按 **ENTER**。

6. 使用以下選項執行該實用程式：

   ```
   kata-firewall-persist-mtu set --mss <MSS> --ip <IP 位址 1> --ip <IP 位址 2>
   ```

   where

   - `<MSS>` 是最大區段大小，計算方式為 MTU 大小減去 TCP 和 IP 標頭的長度。
   - `<IP 位址 1>` 和 `<IP 位址 2>` 是您要套用此設定的伺服器 IP 位址。您可以根據需要多次指定此選項，具體取決於要將該設定套用到的伺服器數量。

   幾分鐘內，該實用程式會將指定的設定保存在 iptables 中，並確保伺服器重新啟動時它們的持久性。

7. 執行以下指令：

   ```
   systemctl restart kata-firewall
   ```

已配置MTU。

kata-firewall-persist-mtu 實用程式的其他功能

該實用程式的附加功能：

- 檢視說明：

  ```
  kata-firewall-persist-mtu --help
  ```

- 檢視目前設定：

  ```
  kata-firewall-persist-mtu get
  ```

- 刪除設定（伺服器重新啟動後設定不再還原）：

  ```
  kata-firewall-persist-mtu flush
  ```

配置 Endpoint Agent 元件與 KEDR 功能塊的整合

本節包含有關配置 KEDR 功能與 Endpoint Agent 元件角色中使用的應用程式的整合的資訊。

配置與 Kaspersky Endpoint Security 的受信任連線

若要設定受信任連線，您必須在 Kaspersky Anti Targeted Attack Platform 端和 Kaspersky Endpoint Security 端執行操作。

您可以使用以下選項之一來設定信任連線：

- **配置與 Central Node 伺服器的連線，無需驗證 Kaspersky Anti Targeted Attack Platform 中 Kaspersky Endpoint Security 的 TLS 憑證。**

  Kaspersky Endpoint Security 使用 Central Node 伺服器的 TLS 憑證與 Kaspersky Anti Targeted Attack Platform 建立受信任連線。當 Kaspersky Endpoint Security 嘗試連線時，Kaspersky Anti Targeted Attack Platform 不會驗證 Kaspersky Endpoint Security 的 TLS 憑證。

  如果您使用此替代配置進行信任連線，則過程如下：

  1. 產生或在 Central Node 的 Web 介面中上傳獨立準備的 Central Node 伺服器 TLS 憑證（如果之前未建立 Central Node 的 TLS 憑證）。
  2. 下載 Central Node 伺服器的 TLS 憑證。
  3. 將安裝有 Kaspersky Endpoint Security 的電腦連線到 Central Node 伺服器：
     - 連線 Kaspersky Endpoint Security for Windows。
     - 連線 Kaspersky Endpoint Security for Linux。
     - 連線 Kaspersky Endpoint Security for Mac。

- **配置與 Central Node 伺服器的連線，並在 Kaspersky Anti Targeted Attack Platform 端驗證 Kaspersky Endpoint Security 的 TLS 憑證。**

  Kaspersky Endpoint Security 使用 Central Node 伺服器的 TLS 憑證與 Kaspersky Anti Targeted Attack Platform 建立受信任連線。額外的連線安全性在 Kaspersky Endpoint Security 中得到配置，Kaspersky Endpoint Security 的 TLS 憑證會上傳。當 Kaspersky Endpoint Security 嘗試連線時，Kaspersky Anti Targeted Attack Platform 會驗證 Kaspersky Endpoint Security 的 TLS 憑證。

  如果您使用此替代配置進行信任連線，則過程如下：

  1. 產生或在 Central Node 的 Web 介面中上傳獨立準備的 Central Node 伺服器 TLS 憑證（如果之前未建立 Central Node 的 TLS 憑證）。
  2. 下載 Central Node 伺服器的 TLS 憑證。

3. 在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中啟用 Kaspersky Endpoint Security TLS 憑證驗證。

4. 使用 Kaspersky Endpoint Security 的 TLS 憑證產生並下載加密容器，或使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面上傳獨立準備的 Kaspersky Endpoint Security TLS 憑證。

   如果您想自行準備 Kaspersky Endpoint Security 的 TLS 憑證，則必須使用您的憑證建立 PFX 加密容器。有關管理 TLS 憑證的詳細資訊，請參閱 OpenSSL 檔案。

5. 將安裝有 Kaspersky Endpoint Security 的電腦連線到 Central Node 伺服器：

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

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

下載 Central Node 伺服器的 TLS 憑證

下載伺服器的 TLS 憑證：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**憑證**子部分。
2. 在**伺服器憑證**部分，點擊**匯出**。

伺服器憑證檔案將會儲存在瀏覽器下載資料夾中。

在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中為 Central Node 伺服器產生 TLS 憑證

如果您已在使用 Central Node 伺服器 TLS 憑證，則產生新憑證會導致目前使用的憑證被刪除並替換為新產生的憑證。

在使用舊憑證的所有地方都必須輸入新憑證的資料。

如果您替代 TLS 憑證，您將需要：

- 重新授權 Central Node 上的郵件 Sensor (KSMG、KLMS)。
- 重新配置 Central Node、PCN、SCN 與 Sandbox 的連線。

- 重新配置從 Endpoint Agent 到 Sensor 的流量轉發以及與 Endpoint Agent 的受信任連線。
- 將新憑證上傳到 Active Directory（如果您正在使用 Active Directory）。

請確保刪除所有 Endpoint Agent 主機隔離規則。與隔離主機的連線將丟失，您將無法管理它們。

為 Central Node 伺服器產生 TLS 憑證：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在應用程式 Web 介面視窗中，選擇**設定**區段、**憑證**子區段。
3. 在**伺服器憑證**部分，點擊**產生**。
   這將開啟操作確認視窗。
4. 點擊**是**。

Kaspersky Anti Targeted Attack Platform 產生新的 TLS 憑證。頁面會自動重新整理。

使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面為 Central Node 伺服器上傳獨立準備的 TLS 憑證

您可以選擇自行準備 TLS 憑證並使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳。

準備上傳的 TLS 憑證檔案必須符合以下要求：

- 檔案必須包含憑證本身和用於連線的私人加密金鑰。
- 檔案必須是 PEM 格式。

  該應用程式不支援其他格式的憑證。

  如果您準備了其他格式的憑證，則必須將其轉換為 PEM 格式。
- 私鑰長度必須為 2048 位元或更長。

要獲取準備 TLS 憑證進行匯入的更多詳細資訊，請參閱 Open SSL 檔案。

如果您已在使用 Central Node 伺服器 TLS 憑證，則上傳新憑證會導致目前使用的憑證被刪除並替換為已上傳的憑證。

在使用舊憑證的所有地方都必須輸入新憑證的資料。

如果您替代 TLS 憑證，您將需要：

- 重新授權 Central Node 上的郵件 Sensor (KSMG、KLMS)。
- 重新配置 Central Node、PCN、SCN 與 Sandbox 的連線。
- 重新配置從 Endpoint Agent 到 Sensor 的流量轉發以及與 Endpoint Agent 的受信任連線。

刪除所有 Endpoint Agent 主機隔離規則。與隔離主機的連線被切斷，您無法管理它們。

若要使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳獨立準備的 TLS 憑證：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在應用程式 Web 介面視窗中，選擇**設定**區段、**憑證**子區段。
3. 在**伺服器憑證**區段中，點擊**上傳**。
   這將開啟檔案選擇視窗。
4. 選擇要下載的 TLS 憑證檔案，然後點擊**開啟**按鈕。
   這將關閉檔案選擇視窗。
   TLS 憑證已新增至 Kaspersky Anti Targeted Attack Platform。
   重新配置從 Endpoint Agent 到 Sensor 的流量轉發以及與 Endpoint Agent 的受信任連線。

請確保刪除所有 Endpoint Agent 主機隔離規則。與隔離主機的連線將丟失，您將無法管理它們。

在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中啟用 Endpoint Agent 元件的 TLS 憑證驗證

若要開啟與在 Endpoint Agent 元件角色中使用的應用程式的受信任連線，請執行下列操作：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在 Kaspersky Anti Targeted Attack Platform Web 介面視窗中，選取**設定**區段、**憑證**子區段。
3. 在**Endpoint Agent 憑證**區段中，開啟**驗證 Endpoint Agent TLS 憑證**開關。

當充當 Endpoint Agent 元件角色的應用程式嘗試連線到 Kaspersky Anti Targeted Attack Platform 時，Kaspersky Anti Targeted Attack Platform 將檢查TLS 憑證資料。

在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中產生 Endpoint Agent 元件的 TLS 憑證並下載加密容器

若要為 Kaspersky Anti Targeted Attack Platform 與在 Endpoint Agent 元件角色中使用的應用程式的連線產生和下載 TLS 憑證：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在 Kaspersky Anti Targeted Attack Platform Web 介面視窗中，選取**設定**區段、**憑證**子區段。
3. 在**Endpoint Agent 憑證**區段中，點擊**產生和匯出**。

   此時會開啟**匯出憑證**視窗。
4. 在**使用密碼防護檔案**區段中，於**密碼**和**確認密碼**欄位中輸入密碼。我們建議妥善保管此密碼以備將來使用，因為應用程式不會保存此密碼。

   加密容器必須設定密碼防護。無法將密碼為空的加密容器新增到 Kaspersky Endpoint Security 中。
5. 點擊**匯出**。

   新的 TLS 憑證將顯示在TLS 憑證表中。帶有作為 Endpoint Agent 的應用程式憑證的加密容器檔案（PFX 格式）將下載到您本機電腦上瀏覽器的下載資料夾。

有關管理 TLS 憑證的詳細資訊，請參閱 OpenSSL 檔案。

加密容器僅包含憑證檔案，但不包含私鑰檔案。Kaspersky Anti Targeted Attack Platform 不會儲存用於連線的 TLS 加密的私鑰。

使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面上傳獨立準備的 Endpoint Agent 元件的 TLS 憑證

您可以選擇自行準備 TLS 憑證並使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳。

準備上傳的 TLS 憑證檔案必須符合以下要求：

- 檔案必須包含憑證本身和用於連線的私人加密金鑰。
- 檔案必須是 PEM 格式。
- 私鑰長度必須為 2048 位元或更長。

要獲取準備 TLS 憑證進行匯入的更多詳細資訊，請參閱 Open SSL 檔案。

如果您想自行準備 Endpoint Agent 元件的 TLS 憑證，必須建立帶有您的憑證的 PFX 加密容器並將加密容器上傳到作為 Endpoint Agent 元件的應用程式。

有關管理 TLS 憑證的詳細資訊，請參閱 OpenSSL 檔案。

> 加密容器必須僅包含憑證檔案，但不包含私鑰檔案。Kaspersky Anti Targeted Attack Platform 不會儲存用於連線的 TLS 加密的私鑰。

若要使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳獨立準備的 TLS 憑證：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在 Kaspersky Anti Targeted Attack Platform Web 介面視窗中，選取**設定**區段、**憑證**子區段。
3. 在**Endpoint Agent 憑證**區段中，點擊**匯入**。
   這將開啟檔案選擇視窗。
4. 選擇要下載的 TLS 憑證檔案，然後點擊**開啟**按鈕。
   這將關閉檔案選擇視窗。

TLS 憑證已新增至 Kaspersky Anti Targeted Attack Platform。

在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中檢視 Endpoint Agent 元件的 TLS 憑證表

若要使用 Kaspersky Anti Targeted Attack Platform Web 介面檢視用於與在 Endpoint Agent 元件角色中使用的應用程式連線的 TLS 憑證清單，請執行下列操作：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在 Kaspersky Anti Targeted Attack Platform Web 介面視窗中，選取**設定**區段、**憑證**子區段。
3. **Endpoint Agent 憑證**區段會顯示 TLS 憑證清單，其中每個憑證包含以下詳細資訊：
   - **TLS 憑證** – 憑證指紋。
   - **序號** – 憑證的序號。
   - **到期** —憑證的到期日期。

在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中篩選和搜尋 Endpoint Agent 元件的 TLS 憑證

您可以依一個或兩個欄位（**TLS 憑證**和**序號**）篩選表格中顯示的 TLS 憑證，或輸入搜尋條件，依這些欄位搜尋 TLS 憑證。

若要篩選並蒐索表中的 TLS 憑證：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在 Kaspersky Anti Targeted Attack Platform Web 介面視窗中，選取**設定**區段、**憑證**子區段。
3. **Endpoint Agent 憑證**區段會顯示 TLS 憑證清單，其中每個憑證包含以下詳細資訊：
   - **TLS 憑證** – 憑證指紋。
   - **序號** – 憑證的序號。
   - **到期** – 憑證的到期日期。
4. 如果您想透過憑證指紋篩選或搜尋 TLS 憑證：
   a. 點擊**TLS 憑證**連結以開啟篩選器設定視窗。
   b. 在**TLS 憑證**文字方塊中輸入憑證指紋的幾個字元。
   c. 點擊**套用**。
5. 如果您想按序號篩選或搜尋 TLS 憑證：
   a. 點擊**序號**連結以開啟篩選器設定視窗。
   b. 在**序號**文字方塊中輸入序號的幾個字元。
   c. 點擊**套用**。

此表僅顯示與您設定的篩選條件相符的 TLS 憑證。

若要清除一個或多個篩選條件的篩選器：

點擊您想要清除其篩選條件的表列標題右側的 ⊠。

> 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選器將會被清除。

在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中刪除 Endpoint Agent 元件的 TLS 憑證

若要使用 Kaspersky Anti Targeted Attack Platform Web 介面刪除用於與在 Endpoint Agent 元件角色中使用的應用程式連線的一個或多個 TLS 憑證，請執行以下操作：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在 Kaspersky Anti Targeted Attack Platform Web 介面視窗中，選擇**設定**部分的**Endpoint Agent 憑證**子區域。
   Endpoint Agent 憑證部分顯示 TLS 憑證清單。
3. 選擇要刪除的一個或多個 TLS 憑證旁的核取方塊。
4. 點擊**刪除**。
   這將開啟操作確認視窗。
5. 點擊**是**。

選定的 TLS 憑證將會被刪除。

設定從 Kaspersky Agent 到 Sensor 伺服器的流量重新導向

您可以將 Sensor 伺服器用作代理伺服器以在 Endpoint Agent 組件和 Central Node 之間進行通訊，以減輕 Central Node 的負擔。為此，在連線充當 Endpoint Agent 元件的應用程式時，在該應用程式端，需要指定 Sensor 伺服器的 IP 位址，而不是 Central Node 伺服器的 IP 位址。Sensor 必須安裝在與 Central Node 不同的伺服器上。

配置流量重新導向時，請記住以下限制：

- Sensor 的最大傳入流量不得超過 1 Gbps。
- Central Node 和 Sensor 伺服器之間的建議通道頻寬必須是 SPAN 連接埠流量的 15%。
- Sensor 伺服器和 Central Node 之間允許的最大封包遺失率為 10%，封包延遲最多為 100 毫秒。

若要將 Sensor 用作代理伺服器，請將 Sensor 連線到 Central Node。

配置Endpoint Agent 元件與 NDR 功能塊的整合

如果您使用 NDR 功能，您可以設定 Kaspersky Anti Targeted Attack Platform 與 Kaspersky Endpoint Security 12.7 for Windows 和 Kaspersky Endpoint Security 12.2 for Linux 所代表的 Endpoint Agent 元件的整合，以接收有關安裝該元件之裝置的以下資訊：

- 由於 EPP 技術觸發而記錄在事件資料庫中的有關 NDR 事件的資訊（工作站和伺服器防護事件）。
- 裝置資訊（例如，作業系統版本、型號或供應商資訊）。
- 有關網路互動圖上裝置連線的資訊。
- 有關用於建立裝置間連線的協定的資訊。

> 您可以將最多 2000 個 Endpoint Agent 元件連線到單個 Central Node 元件。

若要整合 NDR 功能，必須使用 *KESB Advanced* 或 *KESB Total* 產品授權金鑰啟動 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux。

安裝了 Endpoint Agent 元件的電腦資料會透過*Integration Server*傳送到 Kaspersky Anti Targeted Attack Platform。任何安裝了 Kaspersky Anti Targeted Attack Platform 元件（Central Node 或 Sensor）的伺服器都可以作為 Integration Server。若要與 Endpoint Agent 整合，請在接收來自安裝 Endpoint Agent 之電腦資料的伺服器上新增 Integration Server。

託管 Endpoint Agent 的電腦透過 HTTPS 協定與 Integration Server 建立安全連線。連接由 Central Node 伺服器頒發的憑證防護。以下憑證可用於連線：

- Integration Server 憑證。每次建立連線時，Endpoint Agent 電腦都會驗證此憑證。直到憑證驗證成功後才建立連線。
- 用戶端憑證。此憑證用於對具有 Endpoint Agent 的電腦 Integration Server 用戶端進行身分驗證。同一個用戶端憑證可以被多台裝有 Endpoint Agent 的電腦使用。預設情況下，Integration Server 不會驗證用戶端憑證，但您可以啟用驗證以提高連線的安全性。

憑證和公鑰使用 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 分發給 Endpoint Agent 電腦。若要將這些資料上傳至 Kaspersky Endpoint Security，您可以使用通訊封包，必須在新增 Integration Server 後在 Kaspersky Anti Targeted Attack Platform 中建立。

> 在分佈式解決方案和多組織用戶模式下，與 NDR 功能單元的整合配置必須在要配置整合的 Central Node 伺服器上執行。

只有具有**管理員**角色的使用者才能配置來自 Endpoint Agent 元件的資料接收。具有**安全稽核員**角色的使用者可以檢視 Integration Server 清單。

準備從 Endpoint Agent 元件接收資料的場景

在分佈式解決方案和多組織用戶模式下，必須在 Central Node 伺服器上執行 Kaspersky Anti Targeted Attack Platform 端的操作，該伺服器用於從 Endpoint Agent 元件取得資料。

準備從 Endpoint Agent 元件接收資料的場景涉及以下步驟：

1. **在控制網路的電腦上安裝 Endpoint Agent 元件**

   在此步驟中，您必須在所有想要在 Kaspersky Anti Targeted Attack Platform 中接收資訊的電腦上安裝 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux（作為 Endpoint Agent 元件）。這些電腦必須與裝有 Sensor 元件的其中一台伺服器位於同一網路上。

   > Kaspersky Anti Targeted Attack Platform 的目前版本僅在與 Kaspersky Endpoint Security for Windows 12.7 及更高版本或 Kaspersky Endpoint Security for Linux 12.2 及更高版本整合時支援接收和處理資料。

2. **為 Kaspersky Anti Targeted Attack Platform 元件新增 Integration Server**

   此階段涉及完成將 Integration Server 新增至 Endpoint Agent 元件將連線的伺服器的過程。伺服器與 Endpoint Agent 元件之間的網路互動僅可透過未用作監控點的網路介面來實現。沒有為 Integration Server 配置特定的網路介面和 IP 位址，因為電腦的任何可用網路介面和 IP 位址都可以用於與 Integration Server 的外部連線。

3. **為 Integration Server 的用戶端建立通訊封包**

   在此階段，您必須建立和下載通訊封包，應用程式在其中儲存用於將用戶端連線到 Integration Server 的憑證和金鑰。每個通訊封包都是一個包含以下資料的壓縮檔案：

   - Integration Server 憑證的公鑰。
   - Integration Server 的用戶端憑證（帶有私鑰）。如果整合式伺服器上啟用了用戶端憑證驗證，則會新增此憑證。憑證和金鑰使用建立通訊封包時指定的密碼加密。

4. **將連線 Integration Server 的資料上傳到用戶端電腦**

   我們建議使用卡巴斯基安全管理中心來執行此操作。對於 Kaspersky Anti Targeted Attack Platform Integration Server，用戶端是裝有 Endpoint Agent 元件的電腦。使用 Endpoint Agent 管理外掛程式將通訊封包中的憑證和/或金鑰上傳到卡巴斯基安全管理中心管理伺服器。然後，在卡巴斯基安全管理中心中建立政策，以便將資料上傳到 Endpoint Agent 電腦。有關管理資料和建立政策的資訊，請參閱 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的文件。

   對於每個 Integration Server，必須建立至少一條政策，其中包含要上傳到用戶端電腦的以下資料：

   - Integration Server 憑證的公鑰。
   - 用於連線 Integration Server 的 IP 位址。您可以指定 Integration Server 節點的任意可用 IP 位址。您可以在 Web 介面的"**設定**"部分、"**連線伺服器**"子部分中，在"**整合伺服器**"索引標籤上檢視 IP 位址。連線使用 8085 連接埠。
   - Integration Server 的用戶端憑證（帶有私鑰）。如果整合式伺服器上啟用了用戶端憑證驗證，則會新增此憑證。

5. **啟用 Integration Server**

   套用原則並將資料上傳至具有 Endpoint Agent 元件的電腦後，此階段即完成。在此階段，您需要啟用所有要向其傳送 EPP 應用程式資料的 Integration Server。

該場景的結果是，Kaspersky Anti Targeted Attack Platform 開始接收和處理來自 EPP 應用程式的資料。

Integration Server 表

Integration Server 表顯示在“**設定**”部分、“**連線伺服器**”子部分中的“**整合伺服器**”索引標籤上。此表顯示已在安裝了應用程式元件的伺服器上新增的 Integration Server 的資訊。

Integration Server 表包含以下資訊：

- **節點名稱**—安裝了應用程式元件的伺服器的名稱。
- **IP 位址**—Kaspersky Anti Targeted Attack Platform 元件伺服器所有網路介面上的 IP 位址清單（未為整合式伺服器設定特定網路介面和 IP 位址，因為電腦的任何可用網路介面和 IP 位址都可用於到整合式伺服器的外部連線）。
- **每秒請求數**—從用戶端到 Integration Server 的成功處理請求的平均數量。
- **狀態**—Integration Server 的目前狀態。
- **驗證用戶端憑證**—指示是否啟用或停用用戶端憑證驗證（如果停用驗證，則表格儲存格為空）。

在分佈式解決方案和多租戶模式下，此表僅顯示有關新增至您正在管理其 Web 介面的 Central Node 伺服器的整合伺服器的資訊。

新增 Integration Server

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

若要新增 Integration Server：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇應用程式 Web 介面視窗中“**設定**”部分的“**連線伺服器**”子部分。
3. 在“**整合伺服器**”索引標籤中，點擊“**新增 Endpoint Agent Integration Server**”按鈕。
4. 在“**節點**”下拉清單中，選擇要新增 Integration Server 的已安裝 Central Node 或 Sensor 元件的伺服器。

   您只能選擇尚未新增 Integration Server 的節點。
5. 如有必要，為整合伺服器的用戶端新增一個或多個憑證。為此，請點擊“**用戶端憑證（TCP 模式）**”部分中的“**建立新憑證**”按鈕。只有 TCP 模式的憑證用於與 Endpoint Agent 元件整合。

   您可以點擊包含憑證指紋的欄位右側的 × 圖示，從清單中刪除不必要的憑證。

若您建立了多個用戶端憑證，您可以在建立通訊資料套件時選擇憑證。

6. 點擊**儲存**。

Integration Server 已新增。

為 Integration Server 的用戶端建立通訊封包

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

新增 Integration Server 或變更其設定後，您需要為該伺服器的用戶端建立並下載通訊封包。

若要為 Integration Server 的用戶端建立新的通訊封包：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇應用程式 Web 介面視窗中"**設定**"部分的"**連線伺服器**"子部分。
3. 在"**整合伺服器**"索引標籤上，選擇要為其用戶端建立新的通訊封包的伺服器。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊 ⋮ 。
5. 選擇"**取得用戶端的通訊封包**"。
6. 如果為 Integration Server 啟用了用戶端憑證驗證，則會顯示"**產生新的通訊封包**"視窗。執行以下操作：
   a. 在"**連線類型**"下拉式清單中，選擇"**TCP**"。
   b. 在"**用戶端憑證**"下拉式清單中，選擇用於 Integration Server 用戶端身分驗證的憑證。
   c. 指定所選憑證的存取密碼。指定的密碼用於加密連線器通訊封包中的憑證。
   d. 點擊**建立通訊封包**。

Central Node 為所選 Integration Server 的用戶端產生新的通訊封包，然後瀏覽器儲存下載的檔案。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。

您需要將通訊封包的內容上傳到整合式伺服器用戶端電腦。您可以使用卡巴斯基安全管理中心管理伺服器原則上傳它。在卡巴斯基安全管理中心政策中，指定用於連線到 Integration Server 的 IP 位址（您可以使用所選 Integration Server 的詳細資訊區域中列出的可用 IP 位址之一）。有關建立和配置卡巴斯基安全管理中心政策的更多詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的文件。

啟用或停用 Integration Server

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

可以啟用或停用 Integration Server。預設情況下，建立後，Integration Server 被停用，因此 Kaspersky Anti Targeted Attack Platform 不會處理來自其用戶端的資料。

若要啟用或停用 Integration Server：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇應用程式 Web 介面視窗中"**設定**"部分的"**連線伺服器**"子部分。
3. 在"**整合伺服器**"索引標籤上，選擇要啟用或停用的伺服器。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊"**啟用**"或"**停用**"。

伺服器被啟用或停用。

編輯 Integration Server 設定

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

編輯整合式伺服器設定時，您可以替代 Integration Server 本身的憑證、啟用或停用用戶端憑證驗證以及變更用戶端的憑證清單。

要編輯 Integration Server 設定：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇應用程式 Web 介面視窗中"**設定**"部分的"**連線伺服器**"子部分。
3. 在**整合伺服器**索引標籤上，選擇您要編輯其用戶端設定的伺服器。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 在工具列上，點擊**編輯**按鈕。
5. 如果您想要替代 Integration Server 本身的憑證（頒發新憑證），請點擊**重新頒發憑證**。

   更換整合式伺服器憑證會導致舊憑證無效。

6. 如果您要變更用戶端的憑證清單，可以透過點擊**建立新憑證**按鈕建立另一個憑證，或透過點擊憑證指紋欄位右側的 × 圖示刪除先前新增的憑證。

> 為了成功保存設定，清單必須至少包含一個憑證。

7. 點擊**儲存**。

Integration Server 設定已修改。

如果您為 Integration Server 頒發了新憑證或產生了新的用戶端憑證，則需要再次建立並下載通訊資料套件，以將這些憑證的資訊傳播到用戶端電腦。

刪除 Integration Server

> 如果您使用分散式解決方案和多組織用戶模式，請使用要設定參數的 PCN 或 SCN 伺服器 Web 介面。

若要刪除 Integration Server：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇應用程式 Web 介面視窗中"**設定**"部分的"**連線伺服器**"子部分。
3. 在**整合伺服器**索引標籤上，選擇要刪除的伺服器。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊 ⋮ 。
5. 選擇**刪除**。
   這將開啟一個確認提示視窗。
6. 在提示視窗中，點擊**確定**。

Integration Server 被刪除。

與郵件感應器的整合

您可以設定 Kaspersky Anti Targeted Attack Platform 與*郵件感應器*的整合。郵件感應器是安裝了Kaspersky Secure Mail Gateway (KSMG) 或 Kaspersky Security for Linux Mail Server (KLMS) 的伺服器或虛擬機。

如果啟用此整合，應用程式會將電子郵件副本傳送給 Kaspersky Anti Targeted Attack Platform 進行掃描，並可根據掃描結果封鎖特定郵件。當偵測到威脅時，Kaspersky Anti Targeted Attack Platform 會建立警示。

如果您在 Kaspersky Anti Targeted Attack Platform 端設定了按郵件收件者和 MD5 總和檢查碼進行的掃描排除項目規則，則當郵件感應器處理郵件時，這些規則不會套用。

應用程式使用入門

本節包含有關如何在 Web 介面、管理員功能表以及技術支援模式下開始管理應用程式的資訊。

使用管理員帳戶開始使用應用程式 Web 介面

只有當用於管理應用程式 Web 介面的瀏覽器提供 HTTP POST 請求的 Referrer 標頭時，Kaspersky Anti Targeted Attack Platform 的 Web 介面才受防護免受 **CSRF 攻擊**並運作。確保用於使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面的瀏覽器不會修改 HTTP POST 請求的 Referrer 頭資訊。如果與 Kaspersky Anti Targeted Attack Platform 的 Web 介面的連線是透過組織的代理伺服器建立的，請確保代理伺服器不會修改 HTTP POST 請求的 Referrer 頭資訊。

跨站請求偽造（也稱為"XSRF 攻擊"）。利用 HTTP 協定的弱點攻擊網站使用者。這種攻擊使得駭客能夠打著授權使用者的幌子在易受攻擊的網站中執行操作。例如，在易受攻擊的網站中，駭客可以打著授權使用者的幌子秘密地向外部支付系統的伺服器傳送請求，以便將資金轉移到駭客的帳戶。

安裝 Kaspersky Anti Targeted Attack Platform 後，您必須管理應用程式的大小設定。

如果未配置 Kaspersky Anti Targeted Attack Platform 的大小設定，則無法登入應用程式 Web 介面。

若要使用管理員帳戶開始使用應用程式 Web 介面：

1. 在任何允許存取 Central Node 伺服器的電腦的瀏覽器中，將具有 Central Node 元件的伺服器的 IP 位址輸入位址列中。

   如果您使用的是應用程式的高可用性版本，則可以輸入 Central Node 叢集的任何伺服器的 IP 位址或**叢集的完全限定網域名稱 (FQDN)**。

   為了確保程式 Web 介面的存取不間斷，可以在DNS 伺服器上設定輪詢調度演算法功能。為此，請登入 Central Node 叢集的第一台正常伺服器的 Web 介面。

   Kaspersky Anti Targeted Attack Platform 使用者的帳戶憑據輸入視窗開啟。

2. 輸入使用者名稱"admin"以及部署 Central Node 元件時設定的密碼。

3. 點擊**登入**。

   應用程式 Web 介面的**控制板**頁面將顯示。

您可以透過管理員帳戶開始使用應用程式。

對於每個使用者帳戶，同時進行的應用程式管理工作階段的數量限制在一個 IP 位址。如果使用相同的使用者名稱從不同的 IP 位址登入應用程式，則先前的工作階段將終止。

應用程式管理員功能表使用入門

您可以在安裝應用程式元件的每台伺服器的管理主控台的管理員功能表中管理 Sensor、Central Node 和 Sandbox 元件的設定。

確保只能從您授予此類存取權限的電腦存取 Kaspersky Anti Targeted Attack Platform 管理員功能表和伺服器管理主控台。

確保您授予存取權限的電腦位於網路的安全範圍內。

您可以使用 Iptables 命令列實用程式設定從某些電腦對 Kaspersky Anti Targeted Attack Platform 管理員功能表和伺服器管理主控台的存取。有關管理 iptables 的詳細資訊，請參閱 iptables 檔案。

若要開始使用託管所需元件的伺服器管理中的元件管理員功能表：

1. 透過 SSH 協定或終端機登入您要變更其設定之伺服器的管理主控台。

   顯示應用程式元件管理員功能表。

2. 當系統提示時，請輸入管理員使用者名稱和在安裝應用程式期間設定的密碼。

   顯示應用程式元件管理員功能表。

您可以開始使用應用程式元件管理員功能表。

在技術支援模式下開始使用應用程式

技術支援模式下任何未經技術支援人員批准和/或不建議的操作都是被禁止的，並且是撤銷技術支援的理由。

您可以在技術支援模式下管理應用程式的 Sensor、Central Node 和 Sandbox 元件。

技術支援模式為 Kaspersky Anti Targeted Attack Platform 管理員提供對應用程式及其所有儲存資料（包括個人資訊）的無限存取權（根）。

在具有超級使用者帳戶權限的技術支援模式下從管理主控台使用 Kaspersky Anti Targeted Attack Platform，您可以：

- 使用設定檔管理應用程式操作設定。

  在應用程式節點間傳輸資料時，您還可以修改資料加密的設定，以及用於儲存和處理被掃描物件的設定。

在這種情況下，資料以未加密的形式傳輸。Kaspersky Anti Targeted Attack Platform 管理員必須獨立使用這些資料來確保伺服器受到防護。Kaspersky Anti Targeted Attack Platform 管理員負責修改應用程式的設定檔。

- 管理追蹤記錄設定。

偵錯檔案可能包含使用者的機密資料。此類檔案將無限期保留，並且可以由 Kaspersky Anti Targeted Attack Platform 的管理員手動刪除。偵錯檔案的路徑由 Kaspersky Anti Targeted Attack Platform 的管理員指定。

要開始在技術支援模式下使用 Sandbox、Sensor 或Central Node 元件：

1. 登入要透過 SSH 協定或終端機變更其設定的伺服器的管理主控台。
2. 系統提示時，請輸入管理員使用者名稱和在安裝元件期間指定的密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表中，選擇**技術支援模式**。
4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。
5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下**Enter**。

您可以繼續在技術支援模式下管理 Central Node、Sensor 或 Sandbox 元件。

管理應用程式管理員和使用者的帳戶

Kaspersky Anti Targeted Attack Platform 為具有下列元件的伺服器提供帳戶：

- Sensor。用於管理元件 Web 介面、管理員功能表和伺服器管理主控台（技術支援模式下）的管理員帳戶。預設使用在元件安裝期間建立的“admin”帳戶。
- Sandbox。用於管理元件 Web 介面、管理員功能表和伺服器管理主控台（技術支援模式下）的管理員帳戶。預設使用在元件安裝期間建立的“admin”帳戶。
- Central Node。以下帳戶：
  - 用於在應用程式管理員功能表和伺服器管理主控台（在技術支援模式下）中工作的管理員帳戶。預設使用在元件安裝期間建立的“admin”帳戶。
  - 應用程式 Web 介面的管理員帳戶。
  - 具有**安全稽核員**、**安全官**和**資深安全員**角色的應用程式 Web 介面使用者帳戶。

來自於每個此類帳戶的資料被儲存在託管該帳戶所屬的應用程式元件的伺服器上。

在分佈式解決方案和多組織用戶模式中，來自每個帳戶的資料都儲存在 PCN 上以及託管該帳戶所屬的應用程式元件的伺服器上。

用於在伺服器管理主控台中工作的管理員帳戶擁有無限權限來管理託管該帳戶所屬的應用程式元件的伺服器（超級使用者權限）。在此帳戶下，您可以關閉或重新啟動伺服器，或在伺服器管理主控台中修改應用程式在技術支援模式下的設定。

在伺服器（管理員）的管理主控台中工作的管理員帳戶可以無限制地存取該伺服器上的資料。用於在伺服器管理主控台中工作的管理員帳戶的密碼必須是強密碼。管理員必須採取步驟確保伺服器的安全。管理員具有存取儲存在伺服器上的資料的責任。

您可以使用具有**管理員**角色的帳戶來管理應用程式使用者帳戶，以及應用程式 Web 介面的管理員可用的應用程式設定。在分散式解決方案和多組織用戶模式下，使用者帳戶在 PCN 上進行管理。

具有**安全稽核員**角色的帳戶可以檢視管理員和安全官可用的 Web 介面的所有部分。具有**安全稽核員**角色的使用者可以檢視資料，但不能編輯該資料。

資深安全員和**安全官**角色專供組織中工作職責涉及管理 Kaspersky Anti Targeted Attack Platform 的事件、警示和工作以及管理回應操作的員工使用。使用具有這些角色的帳戶登入應用程式時，您可以看到安全官可用的應用程式 Web 介面的所有部分。具有**資深安全員**角色的使用者可以執行所有操作。對具有**安全官**角色的使用者的限制如下表所示。

具有**安全官**角色的應用程式使用者的存取限制

功能範圍/Web 介面部分	限制
控制板	VIP 組事件的小工具不可用。 無法使用小工具中的連結前往**警示**部分。
警示	如下操作不可用: • 檢視警示詳細資訊。 • 標記 VIP 群組警示處理的完成。 • 對多個警示執行操作。 • 匯出所有警示的清單。
資產：裝置	裝置分組不可用。
資產: Endpoint Agent	檢視 Endpoint Agent 工作站表的權限；檢視工作、政策和網路隔離詳細資料的限制。
網路流量事件	無法執行與 VIP 群組警示相關的事件的操作。
威脅搜尋	如下操作不可用: • 從 VIP 群組的警示中檢視與工作站相關的事件 • 根據事件搜尋條件建立 TAA (IOA) 規則
工作	無法存取。
防護規則	無法存取。
自訂規則：IOC	讀取。
自訂規則: YARA	僅能存取以匯出規則。
自訂規則：TAA	讀取。
使用者定義的 Sandbox 規則和入侵偵測規則	無法存取。
日誌	無法存取應用程式 Web 介面中的稽核日誌和使用者活動日誌。
儲存	無法存取由於工作而被放置在儲存中的物件。 完全存取使用者手動下載的物件。
隔離區	無法存取。
報告	無法存取。
設定	如下操作不可用: • 建立警示通知規則（完全存取傳送有關應用程式遇到的問題的通知的規則） • 管理 Kaspersky TAA (IOA) 規則的排除項目和掃描（讀取存取）排除項目 無法存取以下功能： • 管理 Endpoint Agent • 本機 KPSN 信譽資料庫連線設定 • 為警示指派 VIP 狀態的規則 • 允許規則 • Sandbox 連線設定 • 掃描 Sandbox 中的物件時要使用的作業系統設定 • 壓縮檔案密碼

如果您使用分佈式解決方案和多組織用戶模式，則可以允許或拒絕每個帳戶對租用戶和 SCN 伺服器的 Web 介面的存取。

建立用於應用程式 Web 介面的管理員帳戶

建立應用程式 Web 介面管理員帳戶：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。
3. 點擊**新增**。

   這將開啟**新使用者**視窗。

4. 若要啟用帳戶，請開啟**狀態**切換開關。

   預設情況下，該帳戶已啟用。

> 如果啟用了使用者帳戶，則允許使用者存取應用程式 Web 介面。如果使用者帳戶已停用，則禁止使用者存取應用程式 Web 介面。

5. 在**角色**下拉式清單中，選擇**管理員**。

6. 在**身分驗證類型**下面，選擇以下選項之一：

   - **KATA 使用者帳戶**。

     在這種情況下，若要連線到應用程式 Web 介面，使用者必須輸入建立帳戶時配置的使用者名稱和密碼。

   - **網域使用者帳戶**。

     在這種情況下，若要連線到應用程式 Web 介面，使用者不必輸入使用者名稱和密碼；使用者將透過網域帳戶進行身分驗證。

> 如果已配置與 Active Directory 的整合，則會顯示**身分驗證類型**設定群組。

7. 如果您選擇了**KATA 使用者帳戶**：

   a. 在**使用者名稱**欄位中，輸入要建立的帳戶的使用者名稱。

      使用者名稱必須符合以下要求：

      - 在使用者名稱清單中必須是唯一的（區分大小寫）。
      - 必須包含不超過 32 個字元。
      - 可以包含字母 A–Z、a–z、數字 0–9、連字號 (-) 和底線 (_)。
      - 必須以字母（AZ 或 az）開頭。

   b. 在**新密碼**欄位中，輸入將用於存取 Web 介面的使用者密碼。

      密碼必須符合以下要求：

      - 不能與使用者名稱完全或基本相同
      - 不得包含字典單字、常用字母組合或鍵盤佈局範例（例如 Qwerty 或 Passw0rd）。
      - 必須包含至少 8 個字元。
      - 必須包含至少三種字元：
        - 大寫字母 (A-Z)。
        - 小寫字母 (a-z)。
        - 數字。
        - 特殊字元。

當您輸入密碼時，應用程式會檢查您的密碼以確保其符合基本要求。點擊**新增**按鈕後將執行最終檢查。即使初步檢查顯示密碼符合要求，最終檢查也可能會拒絕該密碼，並在應用程式 Web 介面中顯示錯誤訊息。在這種情況下，您需要考慮錯誤訊息並想出一個不同的密碼。

c. 在**確認密碼**欄位中，再次輸入將要用於存取 Web 介面的使用者密碼。

8. 如果您選擇了**網域使用者帳戶**，請在**使用者名稱**欄位中輸入使用者的網域名稱。

9. 點擊**新增**。

應用程式管理員帳戶已建立。

如果您使用分佈式解決方案和多組織用戶模式，則 PCN 伺服器管理員帳戶可以存取與該伺服器關聯之所有組織的資料。

建立用於應用程式 Web 介面的使用者帳戶

您可以建立具有**資深安全員**、**安全官**和**安全稽核員**角色的使用者帳戶。

若要為應用程式 Web 介面建立使用者帳戶：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。

3. 點擊**新增**。

   這將開啟**新使用者**視窗。

4. 如有必要，請使用**狀態**切換開關以停用使用者帳戶。

   預設情況下，該帳戶已啟用。

   如果啟用了使用者帳戶，則允許使用者存取應用程式 Web 介面。如果使用者帳戶已停用，則禁止使用者存取應用程式 Web 介面。

5. 在**身分驗證類型**下面，選擇以下選項之一：

   - **KATA 使用者帳戶**。

     在這種情況下，若要連線到應用程式 Web 介面，使用者必須輸入建立帳戶時配置的使用者名稱和密碼。

   - **網域使用者帳戶**。

     在這種情況下，若要連線到應用程式 Web 介面，使用者不必輸入使用者名稱和密碼；使用者將透過網域帳戶進行身分驗證。

     如果您選擇了**網域使用者帳戶**身分驗證類型，請注意，使用者將無法使用不同的使用者帳戶登入應用程式 Web 介面。

   如果配置了 Active Directory 整合，則**KATA 使用者帳戶**和**網域使用者帳戶**欄位可用。

6. 在**角色**下拉清單中，選擇以下角色之一：

- **資深安全員。**
- **安全官**。
- **安全稽核員。**

7. 如果您選擇**KATA 使用者帳戶**：

   a. 在**使用者名稱**欄位中，輸入要建立的帳戶的使用者名稱。
   使用者名稱必須符合以下要求：

   - 在使用者名稱清單中必須是唯一的（區分大小寫）。
   - 必須包含不超過 32 個字元。
   - 可以包含字母 A–Z、a–z、數字 0–9、連字號 (-) 和底線 (_)。
   - 必須以字母（AZ 或 az）開頭。

   b. 在**新密碼**欄位中，輸入將用於存取 Web 介面的使用者密碼。
   密碼必須符合以下要求：

   - 不能與使用者名稱完全或基本相同
   - 不得包含字典單字、常用字母組合或鍵盤佈局範例（例如 Qwerty 或 Passw0rd）。
   - 必須包含至少 8 個字元。
   - 必須包含至少三種字元：
     - 大寫字母 (A-Z)。
     - 小寫字母 (a-z)。
     - 數字。
     - 特殊字元。

   當您輸入密碼時，應用程式會檢查您的密碼以確保其符合基本要求。點擊**新增**按鈕後將執行最終檢查。即使初步檢查顯示密碼符合要求，最終檢查也可能會拒絕該密碼，並在應用程式 Web 介面中顯示錯誤訊息。在這種情況下，您需要考慮錯誤訊息並想出一個不同的密碼。

   c. 在**確認密碼**欄位中，再次輸入將要用於存取 Web 介面的使用者密碼。

8. 如果您選擇了**網域使用者帳戶**，請在**使用者名稱**欄位中輸入使用者的網域名稱。

9. 如果您正在使用分佈式解決方案和多組織用戶模式，則在**存取**部分，配置存取權限：

   a. 開啟**SCN Web 介面**切換開關可讓使用者不僅存取該 PCN 伺服器的 Web 介面，還可以存取所有可用 SCN 伺服器的 Web 介面。

   b. 在**租戶**設定標題右側，選擇您要授予其 Web 介面存取權限的一個或多個租用戶的核取方塊。

      您可以使用**全選**和**全部清除**連結選擇或取消選擇所有租用戶。

10. 點擊**新增**。

使用者帳戶已建立。

配置使用者帳戶表顯示

您可以顯示或隱藏列以及變更應用程式 Web 介面使用者帳戶表中列的順序。

若要設定應用程式 Web 介面使用者帳戶表的顯示：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。

3. 在表格的標題部分，點擊 。

   這將開啟**自訂表格**視窗。

4. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。

   如果要隱藏表中的參數，請清除該核取方塊。

   > 必須選擇至少一個核取方塊。

5. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。

6. 如果要還原預設表格顯示設定，請點擊**預設**。

7. 點擊**套用**。

使用者帳戶表顯示已配置。

檢視使用者帳戶表

使用者帳戶表顯示在應用程式 Web 介面視窗的“**設定**”部分、“**使用者**”子部分。您可以按**使用者名稱**、**角色**、**租戶**和**狀態**列對表中的事件進行排序。

表包含以下資訊：

1. **使用者名稱**是建立帳戶時配置的使用者名稱。

2. **身分驗證類型**是使用者的身分驗證類型。可能值：

   - **KATA 使用者帳戶**。

     如果選擇此驗證類型，若要連線到應用程式 Web 介面，使用者必須輸入建立帳戶時設定的使用者名稱和密碼。

   - **網域使用者帳戶**。

     如果選擇此驗證類型，連線到應用程式 Web 介面時，使用者無需輸入使用者名稱和密碼；使用者透過網域帳戶進行身分驗證。

3. **角色**是分配給使用者的角色。

4. **租戶**是使用者有權存取的租用戶清單。

   此列僅在分佈式解決方案和多組織用戶模式下顯示。

5. **狀態**是帳戶的狀態。可以有以下值：

   - **已啟用**。

     如果啟用了使用者帳戶，則允許使用者存取應用程式 Web 介面。

   - **已停用**。

     如果使用者帳戶已停用，則禁止使用者存取應用程式 Web 介面。

篩選使用者帳戶

若要依所需條件篩選或搜尋使用者帳戶：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。

3. 根據篩選條件，執行以下操作：

   - **按使用者名稱**

     a. 點擊**使用者名稱**連結以開啟篩選功能表。

     b. 在下拉清單中，選擇以下篩選運算子之一：

        - **包含**

        - **不包含**

     c. 在文字方塊中，鍵入使用者名稱或使用者名稱中的字元序列。

     d. 點擊**套用**。

- **按身分驗證類型**

  a. 點擊**身分驗證類型**連結以開啟篩選功能表。

  b. 選擇要包含在篩選條件中的帳戶旁的核取方塊：

    - **KATA 使用者帳戶**。
    - **網域使用者帳戶**。

  c. 點擊**套用**。

- **按角色**

  a. 點擊**角色**連結以開啟篩選功能表。

  b. 選擇與要新增至篩選條件的角色對應的核取方塊。

    - **管理員**。
    - **資深安全員**。
    - **安全官**。
    - **安全稽核員**。

    您可以選擇多個核取方塊。

  c. 點擊**套用**。

- **按使用者有權存取的租戶名稱**

  a. 點擊**租戶**連結以開啟篩選功能表。

  b. 選擇與要新增至篩選條件的租戶相對應的核取方塊。
    您可以選擇多個核取方塊。

  c. 點擊**套用**。

- **按狀態**

  a. 點擊**狀態**展開篩選器設定清單。

  b. 選擇以下選項之一：

    - **所有**。
    - **已啟用**。
    - **已停用**。

此表顯示與配置的篩選條件相對應的帳戶。

您可以同時使用多個篩選器。

清除帳戶篩選器

若要依一個或多個篩選條件清除使用者帳戶篩選器：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。
3. 點擊您想要清除其篩選條件的使用者帳戶表列標題右側的。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   此表僅顯示與指定條件相符的使用者帳戶。

變更使用者帳戶對 PCN 和 SCN 資料的存取權限

如果您正在使用分佈式解決方案和多組織用戶模式，您可以變更具有**資深安全員**和**安全官**角色的使用者對 PCN 和 SCN 伺服器資料的存取權限以及對這些伺服器所屬租用戶的存取權限。

若要變更應用程式 Web 介面使用者帳戶的存取權限，請在 PCN 的 Web 介面中執行下列操作：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。
3. 選擇您要變更其存取權限的帳戶。

   這將開啟**編輯使用者帳戶**視窗。
4. 如果您想啟用或停用帳戶，請移動**狀態**切換開關。
5. 必要時在**存取**部分移動**SCN Web 介面**切換開關：
   - 如果您想要授權使用者除了此 PCN 伺服器的 Web 介面之外還可以存取所有可用 SCN 伺服器的 Web 介面，請將切換開關設為**已啟用**。
   - 如果您只想授權使用者存取此 PCN 伺服器的 Web 介面，請將切換開關設為**已停用**。

6. 在**租戶**設定名稱的右側，選擇或清除要為其變更伺服器 Web 介面存取權限的一個或多個租用戶的核取方塊。
   您可以使用**全選**和**全部清除**連結選擇或取消選擇所有租用戶。

7. 點擊**儲存**。

帳戶的存取權限已變更。

啟用或停用使用者帳戶

如果您正在使用分佈式解決方案和多組織用戶模式，請在 PCN 的 Web 介面中執行下列步驟。使用者帳戶狀態管理在 SCN 的 Web 介面中不可用。

若要啟用或停用使用者帳戶：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。

3. 在帳戶清單中，選擇要啟用或停用的使用者帳戶。

4. 在**狀態**列中，執行下列操作之一：

   - 如果您想啟用使用者帳戶，將使用者帳戶名稱旁的切換開關設定為“**已啟用**”。

   - 如果您想要停用使用者帳戶，將使用者帳戶名稱旁的切換開關設定為“**已停用**”。

   操作確認視窗將顯示。

5. 點擊**是**。

帳戶的狀態已修改。

管理員帳戶無法被停用。

修改使用者帳戶的密碼

僅具有**KATA 使用者帳戶**身分驗證類型的使用者可以變更其使用者帳戶的密碼。

如果您正在使用分佈式解決方案和多組織用戶模式，請在 PCN 的 Web 介面中執行下列步驟。在 SCN Web 介面，您只能變更自己帳戶的密碼。

若要修改使用者帳戶的密碼：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。在帳戶清單中，選擇要變更其密碼的使用者帳戶。

   這將開啟**編輯使用者帳戶**視窗。
3. 在**新密碼**欄位中，輸入應用程式 Web 介面的新密碼。

   密碼必須符合以下要求：

   - 不能與使用者名稱完全或基本相同
   - 不得包含字典單字、常用字母組合或鍵盤佈局範例（例如 Qwerty 或 Passw0rd）。
   - 必須包含至少 8 個字元。
   - 必須包含至少三種字元：
     - 大寫字母 (A-Z)。
     - 小寫字母 (a-z)。
     - 數字。
     - 特殊字元。

   當您輸入密碼時，應用程式會檢查您的密碼以確保其符合基本要求。點擊**新增**按鈕後將執行最終檢查。即使初步檢查顯示密碼符合要求，最終檢查也可能會拒絕該密碼，並在應用程式 Web 介面中顯示錯誤訊息。在這種情況下，您需要考慮錯誤訊息並想出一個不同的密碼。
4. 在**確認密碼**欄位中，再次輸入新密碼。
5. 點擊**儲存**。

應用程式管理員帳戶或使用者帳戶的密碼已變更。

修改您帳戶的密碼

> 僅具有**KATA 使用者帳戶**身分驗證類型的使用者可以變更其使用者帳戶的密碼。

若要修改您的使用者帳戶的密碼：

1. 利用您的帳戶登入程式 Web 介面。
2. 點擊應用程式 Web 介面視窗左下角帶有您的使用者名稱的連結。
3. 選擇**變更密碼**操作。

   這將開啟**變更密碼**視窗。

4. 在**旧密碼**欄位中，輸入應用程式 Web 介面的目前密碼。

5. 在**新密碼**欄位中，輸入應用程式 Web 介面的新密碼。
   密碼必須符合以下要求：

   - 不能與使用者名稱完全或基本相同
   - 不得包含字典單字、常用字母組合或鍵盤佈局範例（例如 Qwerty 或 Passw0rd）。
   - 必須包含至少 8 個字元。
   - 必須包含至少三種字元：
     - 大寫字母 (A-Z)。
     - 小寫字母 (a-z)。
     - 數字。
     - 特殊字元。

   當您輸入密碼時，應用程式會檢查您的密碼以確保其符合基本要求。點擊**新增**按鈕後將執行最終檢查。即使初步檢查顯示密碼符合要求，最終檢查也可能會拒絕該密碼，並在應用程式 Web 介面中顯示錯誤訊息。在這種情況下，您需要考慮錯誤訊息並想出一個不同的密碼。

6. 在**確認密碼**欄位中，再次輸入新密碼。

7. 點擊**變更密碼**。

用來存取應用程式 Web 介面的使用者帳戶密碼被變更。

使用網域帳戶進行身分驗證

如果配置了使用網域帳戶的身分驗證，則使用者無需輸入 Kaspersky Anti Targeted Attack Platform 帳戶憑據即可連線到應用程式 Web 介面。

若要啟用使用網域帳戶進行身分驗證：

1. 配置與 Active Directory 的整合。

   要設定 Active Directory 整合，您必須建立一個 keytab 檔案，其中包含要為其設定整合的 Central Node 伺服器的服務主體名稱（以下也稱為"SPN"）。

2. 選擇建立帳戶時使用者的**網域使用者帳戶**身分驗證類型。

建立 keytab 檔案

Kaspersky Anti Targeted Attack Platform 支援兩種身分驗證方法：部分使用者可以使用內部使用者帳戶進行身分驗證，而其他使用者則使用網域使用者帳戶。

如需 Kaspersky Anti Targeted Attack Platform 中網域身分驗證的詳細資訊，請參閱使用網域帳戶進行身分驗證章節。

您可以使用相同的 Active Directory 使用者帳戶，在多個 Central Node 伺服器上進行身分驗證。服務主體名稱 (SPN) 為此，您必須建立一個keytab 檔案，其中包含每個伺服器的*服務主體名稱（以下也稱為 SPN）*。建立 keytab 檔案時，必須使用屬性來產生*salt*（雜湊函數輸入修飾符）。

> 產生的 Salt 必須以任何方便的方式儲存，以便將來在 keytab 檔案中新增更多SPN。

您也可以為要為其設定 Kerberos 驗證的每個 Central Node 伺服器建立單獨的 Active Directory 使用者帳戶。

建立用於在多個 Central Node 上以相同使用者帳戶進行身分驗證的 keytab 檔案

若要建立用於在多個 Central Node 上以相同使用者帳戶進行身分驗證的 keytab 檔案：

1. 在網域控制器上的 **Active Directory 使用者和電腦**管理單元中，建立一個使用者帳戶（例如，使用 `control-user` 作為其名稱）。

   建立使用者帳戶時，您可以選取**密碼永不過期**核取方塊。這可讓您設定永不過期的帳戶密碼，避免密碼到期後發生身分驗證錯誤，因為密碼到期也會導致從密碼產生並儲存在 keytab 檔案中的加密金鑰失效。

2. 如果您要停用現有帳戶的密碼到期日，請在 **Active Directory 使用者和電腦**管理單元中執行下列操作：

   a. 開啟您建立的使用者帳戶的屬性。

   b. 在**帳戶**索引標籤上，選取**密碼永不過期**核取方塊。

3. 如果要使用 AES256-SHA1 加密演算法，請在 **Active Directory 使用者和電腦**管理單元中執行下列操作：

   a. 開啟您建立的使用者帳戶的屬性。

   b. 在**帳戶**索引標籤上，選取**此帳戶支援 Kerberos AES 256 位元加密**核取方塊。

4. 使用 ktpass 實用程式為 `control-user` 使用者建立 keytab 檔案。為此，請在命令列中執行以下命令：

   `C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 伺服器的完全限定網域名稱 (FQDN)>@<大寫的 Active Directory 網域的領域名稱> -mapuser control-user@<大寫的 Active Directory 網域的領域名稱> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <檔案路徑>\<檔案名稱>.keytab`

   該實用程式在執行命令時請求 `control-user` 密碼。

   所選伺服器的 SPN 將會被新增到建立的 keytab 檔案中。產生的鹽顯示在螢幕上：使用鹽**“<雜湊值>”**對密碼進行雜湊處理。

5. 將每個後續 Central Node 伺服器的 SPN 記錄新增到 keytab 檔案中。為此，請執行以下命令：

   `C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 伺服器的完全限定網域名稱 (FQDN)>@<大寫的 Active Directory 網域的領域名稱> -mapuser control-user@<大寫的 Active Directory 網域的領域名稱> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <先前建立的檔案路徑和名稱>.keytab -out <路徑和新名稱>.keytab -setupn -setpass -rawsalt "<在步驟 3 建立 keytab 檔案時取得之鹽的雜湊值>"`

   該實用程式在執行命令時請求 `control-user` 密碼。

keytab 檔案已建立。此檔案包含所選伺服器的所有新增的 SPN。

範例：

例如，您需要建立一個包含 3 台伺服器的 SPN 名稱的 keytab 檔案：`control-01.test.local`、`secondary-01.test.local` 和 `secondary-02.test.local`。

若要在 C:\keytabs\ 中建立包含伺服器的 SPN 的 `filename1.keytab` 檔案，請執行下列命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

假設您有 “`TEST.LOCALHTTPcontrol-01.test.local`” 作為鹽。

若要新增另一個 SPN，請執行以下命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

要新增第三個 SPN：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

這將建立一個 `filename3.keytab` 檔案，其中包含所有三個已新增的 SPN。

建立 keytab 檔案，以便在每個 Central Node 上使用個別使用者帳戶進行身分驗證

若要建立 keytab 檔案，以便在每個 Central Node 上使用個別使用者帳戶進行身分驗證：

1. 在網域控制器伺服器上的 **Active Directory 使用者和電腦**管理單元中，為每台伺服器建立單獨的使用者帳戶（例如，`control-user`、`secondary1-user`、`secondary2-user` 等）。

   建立使用者帳戶時，您可以選取**密碼永不過期**核取方塊。這可讓您設定永不過期的帳戶密碼，避免密碼到期後發生身分驗證錯誤，因為密碼到期也會導致從密碼產生並儲存在 keytab 檔案中的加密金鑰失效。

2. 如果您要停用現有帳戶的密碼到期日，請在 **Active Directory 使用者和電腦**管理單元中執行下列操作：

   a. 開啟您建立的使用者帳戶的屬性。

   b. 在**帳戶**索引標籤上，選取**密碼永不過期**核取方塊。

3. 如果要使用 AES256-SHA1 加密演算法，請在 **Active Directory 使用者和電腦**管理單元中執行下列操作：

   a. 開啟您建立的使用者帳戶的屬性。

   b. 在**帳戶**索引標籤上，選取**此帳戶支援 Kerberos AES 256 位元加密**核取方塊。

4. 使用 ktpass 實用程式為 `control-user` 使用者建立 keytab 檔案。為此，請在命令列中執行以下命令：

   `C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 伺服器的完全限定網域名稱 (FQDN)>@<大寫的 Active Directory 網域的領域名稱> -mapuser control-user@<大寫的 Active Directory 網域的領域名稱> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <檔案路徑>\<檔案名稱>.keytab`

   該實用程式在執行命令時請求 `control-user` 密碼。

   所選伺服器的 SPN 將會被新增到建立的 keytab 檔案中。

5. 將每個後續 Central Node 伺服器的 SPN 記錄新增到 keytab 檔案中。為此，請執行以下命令：

   `C:\Windows\system32\ktpass.exe -princ HTTP/<Central Node 伺服器的完全限定網域名稱 (FQDN)>@<大寫的 Active Directory 網域的領域名稱> -mapuser secondary1-user@<大寫的 Active Directory 網域的領域名稱> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <先前建立的檔案路徑和名稱>.keytab -out <路徑和新名稱>.keytab`

   該實用程式在執行命令時請求 `secondary1-user` 密碼。

keytab 檔案已建立。此檔案包含所選伺服器的所有新增的 SPN。

範例：

例如，您需要建立一個包含 3 台伺服器的 SPN 名稱的 keytab 檔案：`control-01.test.local`、`secondary-01.test.local` 和 `secondary-02.test.local`。

若要在 C:\keytabs\ 中建立包含伺服器的 SPN 的 `filename1.keytab` 檔案，請執行下列命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

若要新增另一個 SPN，請執行以下命令：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

要新增第三個 SPN：

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

這將建立一個 `filename3.keytab` 檔案，其中包含所有三個已新增的 SPN。

配置與 Active Directory 的整合

如需 Kaspersky Anti Targeted Attack Platform 中網域身分驗證的詳細資訊，請參閱使用網域帳戶進行身分驗證章節。

若要設定與 Active Directory 的整合：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。
3. 前往**Active Directory 整合**索引標籤。
4. 如果您想要啟用與 Active Directory 的整合，請選擇**整合**核取方塊。
5. 點擊**瀏覽**上傳keytab 檔案。
6. 選擇 keytab 檔案並點擊**開啟**。
   上傳檔案後，以下欄位將顯示：
   - **Keytab 檔案狀態**。可能值：
     - **檔案包含該伺服器的 SPN**表示上傳的 keytab 檔案包含該 Kaspersky Anti Targeted Attack Platform 伺服器的 SPN。
     - **該伺服器沒有 SPN**表示上傳的 keytab 檔案不包含該 Kaspersky Anti Targeted Attack Platform 伺服器的 SPN。
   - **檔案內容：**是檔案包含的 SPN 清單。
7. 點擊**套用**。

與 Active Directory 的整合已配置。

在分散式解決方案和多組織用戶模式下，PCN 伺服器上設定的 Active Directory 整合設定**不會**套用於連線到該 PCN 伺服器的 SCN 伺服器。如果要在單個SCN 伺服器上設定 Active Directory 整合，您必須在每個選定的 SCN 伺服器上完成上述步驟。

停用與 Active Directory 的整合

如需 Kaspersky Anti Targeted Attack Platform 中網域身分驗證的詳細資訊，請參閱使用網域帳戶進行身分驗證章節。

與 Active Directory 的整合被停用時，無法使用網域帳戶進行使用者驗證。

若要停用與 Active Directory 的整合：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**部分、**使用者**子部分。
3. 前往**Active Directory 整合**索引標籤。

4. 清除**整合**核取方塊。

5. 點擊**套用**。

與 Active Directory 的整合已停用。上傳的 keytab 檔案被永久刪除。

在分散式解決方案和多組織用戶模式下，PCN 伺服器上設定的 Active Directory 整合設定**不會**套用於連線到該 PCN 伺服器的 SCN 伺服器。如果要在單個SCN 伺服器上停用 Active Directory 整合，您必須在每個選定的 SCN 伺服器上完成上述步驟。

參與卡巴斯基安全網路並使用卡巴斯基私有安全網路

為了更有效地防護使用者的電腦，Kaspersky Anti Targeted Attack Platform 使用從全球使用者獲取的資料。*卡巴斯基安全網路*旨在獲取此類資料。

卡巴斯基安全網路（以下也稱為“KSN”）是一個線上服務的基礎架構，提供對卡巴斯基線上知識庫的存取，該知識庫中包含了有關檔案信譽、網站資源和軟體的資訊。使用 Kaspersky Security Network 提供的資料可確保 Kaspersky Anti Targeted Attack Platform 更快地回應尚未新增至防毒資料庫的新物件，提高某些防護元件的效能，並降低誤報的可能性。

感謝參與卡巴斯基安全網路的使用者，卡巴斯基能夠及時接收有關尚未新增到防毒資料庫的物件的類型和來源的資訊，開發抵禦它們的解決方案，並最大限度地減少錯誤警示的數量。使用者參與還可以幫助 Kaspersky Security Network 的其他使用者及時收到有關其組織的 IT 基礎架構威脅的資訊。

當您參與卡巴斯基安全網路時，Kaspersky Anti Targeted Attack Platform 會向卡巴斯基安全網路傳送有關檔案，網路資源和軟體聲譽的請求，並會收到包含有關這些物件聲譽的資料的回應。

使用者的個人資訊不會被收集、處理或儲存。有關 Kaspersky Anti Targeted Attack Platform 傳送到卡巴斯基安全網路的資料資訊，請參閱 KSN 聲明。

參與卡巴斯基安全網路是自願的。參與卡巴斯基安全網路的決定是在安裝 Kaspersky Anti Targeted Attack Platform 期間做出的，該決定可以隨時變更。

如果您不想參與 KSN，可以使用卡巴斯基私人安全網路（以下也稱為“KPSN”）。KPSN 是一個允許使用者存取卡巴斯基安全網路的信譽資料庫和其他統計資料，而不從他們自己的電腦實際傳送資料到卡巴斯基安全網路的解決方案。

如果您想購買卡巴斯基私人安全網路應用程式，請您可以聯絡您所在地區的卡巴斯基合作夥伴。

參與 KSN 是在 Central Node 伺服器上設定的，並套用於所有連線的 Sensor 伺服器。

如果您使用分散式解決方案和多組織用戶模式，則參與 KSN 是在 PCN 伺服器上設定的。設定的 KSN 參與適用於連線到 PCN 的所有 SCN 伺服器。

更新功能（包括病毒防護簽章更新和代碼庫更新）以及 KSN 功能可能無法在美國境內使用。

檢視 KSN 聲明並配置參與 KSN

要設定參與卡巴斯基安全網路：

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 選擇**設定**部分的**KSN/KPSN 和 MDR**子部分。

3. 在“**信譽資料庫**”設定的右側，點擊“**KSN**”按鈕。

4. 仔細閱讀卡巴斯基安全網路聲明並選擇以下選項之一：

   - **我同意參與 KSN**，如果您接受 KSN 聲明的條款並希望參與 KSN。
   - **我不同意參與 KSN**，如果您不接受 KSN 聲明的條款並且不想參與 KSN。

     如果您不同意聲明條款，將不會啟用卡巴斯基安全網路。

5. 點擊**套用**。

   將不會配置參與卡巴斯基安全網路。

配置使用 KPSN

要正確連線到 KPSN，您必須使用在*作為伺服器部署的 Central Node 的服務所使用的連接埠*部分中列出的 ksn_proxy 服務的連接埠。當 KPSN 整合與其他連接埠配置時，連線嘗試失敗。

要啟用 KPSN:

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 選擇**設定**部分的**KSN/KPSN 和 MDR**子部分。
3. 在**信譽資料庫**設定的右側，點擊 **KPSN** 按鈕。
4. 在**KPSN 設定檔**部分，透過點擊**瀏覽**上傳 kc_private.xms、kh_private.xms 和 ksncli_private.dat 檔案。
5. 點擊**套用**。

   將啟用 Kaspersky Private Security Network。

配置與 KPSN 本機信譽資料庫的連線

應用程式可以將有關 Sandbox 元件警示的資訊儲存到 KPSN 的本機信譽資料庫。在這種情況下，物件將被賦予*不受信任*狀態。本機信譽資料庫的資料僅適用於企業區域網路電腦。

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

配置 Kaspersky Anti Targeted Attack Platform 與本機 KPSN 信譽資料庫的連線：

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 選擇**設定**部分，**KPSN 信譽資料庫**子部分。
3. 在**主機**欄位中，指定儲存 KPSN 本機信譽資料庫的 KPSN 伺服器的 IP 位址。
4. 點擊**TLS 憑證**欄位右側的**瀏覽**。
   這將開啟檔案選擇視窗。
5. 在 KPSN 中選擇用於使用者身分驗證的憑證檔案，然後點擊**開啟**按鈕。
6. 在**TLS 加密金鑰**欄位的右側，點擊**瀏覽**。
   這將開啟檔案選擇視窗。
7. 選擇包含私有加密金鑰的檔案，然後點擊**開啟**按鈕。

與 KPSN 本機信譽資料庫的連線將會被設定。

配置要儲存到 KPSN 本機信譽資料庫的資訊

應用程式可以將 Sandbox 元件偵測到的物件的 MD5 和 SHA256 雜湊儲存在 KPSN 的本機信譽資料庫中。在這種情況下，物件將被賦予*不受信任*狀態。本機信譽資料庫的資料僅適用於企業區域網路電腦。

若要設定將 Sandbox 元件偵測到的物件儲存到 KPSN 的本機信譽資料庫：

1. 在進階安全人員帳戶下登入應用程式 Web 介面。
2. 選擇**設定**部分，**KPSN 信譽資料庫**子部分。
3. 執行以下操作之一：
   - 如果您希望應用程式將物件狀態設為*不受信任*，並將其相關資訊儲存在 KPSN 的本機信譽資料庫中，請開啟**將“不受信任”狀態分配給物件**開關。
   - 如果您不想將偵測到的物件相關資訊儲存在 KPSN 的本機信譽資料庫中，請關閉**將“不受信任”狀態分配給物件**開關。
4. 點擊**儲存**。

將資訊儲存到 KPSN 的本機信譽資料庫得到配置。

KSN 參與度和 KPSN 使用量下降

要拒絕參與卡巴斯基安全網路和使用 KPSN：

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 選擇**設定**部分的**KSN/KPSN 和 MDR**子部分。
3. 在“**信譽資料庫**”設定的右邊，點擊“**未使用**”按鈕。
4. 點擊**套用**。

   您將不參與 KSN 也不會使用 KPSN。

透過 Web 介面管理 Sandbox 元件

Sandbox Web 介面位於託管 Sandbox 元件的伺服器上。

防護Sandbox Web 介面免受**CSRF 攻擊**，並且僅當Web 介面使用者的瀏覽器提供 HTTP POST 請求的 Referrer 頭資訊時才運行。確保用於 Sandbox Web 介面的瀏覽器不會修改HTTP POST 請求的 Referrer 頭資訊。如果與Web 介面的連線是透過您組織的代理伺服器建立的，請檢查設定並確保代理伺服器不會修改 HTTP POST 請求的 Referrer 頭資訊。

跨站請求偽造（也稱為"XSRF 攻擊"）。利用 HTTP 協定的弱點攻擊網站使用者。這種攻擊使得駭客能夠打著授權使用者的幌子在易受攻擊的網站中執行操作。例如，在易受攻擊的網站中，駭客可以打著授權使用者的幌子秘密地向外部支付系統的伺服器傳送請求，以便將資金轉移到駭客的帳戶。

要開始使用 Sandbox 應用程式的 Web 介面：

1. 在允許存取具有 Sandbox 元件的伺服器的任何一台電腦的瀏覽器上，輸入具有 Sandbox 元件的伺服器的 IP 位址。

   這將開啟 Sandbox 元件管理員憑證輸入視窗。

2. 輸入您在安裝 Sandbox 元件期間指定的 Sandbox 元件管理員使用者名稱和密碼。

現在可以開始在 Sandbox Web 介面工作。

對於每個使用者帳戶，同時進行的 Sandbox 管理工作階段的數量限制在一個 IP 位址。如果使用相同的使用者名稱從不同的 IP 位址登入 Sandbox，則先前的工作階段將會終止。

如果您使用多個具有 Sandbox 元件的伺服器，請從此伺服器的 Sandbox Web 介面為每個 Sandbox 元件設定設定。

更新 Sandbox 元件資料庫

Sandbox 元件資料庫是具有記錄的檔案，透過這些記錄可以偵測已掃描物件中的惡意代碼和可疑行為的跡象。

卡巴斯基的病毒分析師每天偵測數百種新威脅，並建立記錄來識別它們，將它們加入*資料庫升級套件*（或升級套件）。升級套件由一個或多個包含記錄的檔案組成，這些記錄可用於識別自上次升級套件發布以來偵測到的威脅。我們建議您定期接收升級套件。

在產品授權有效期限內，您可以每小時自動取得一次更新包，或手動更新資料庫。

如果您已將 Kaspersky Anti Targeted Attack Platform 部署在隔離網路或網際網路頻寬有限的網路中，則可以使用卡巴斯基更新實用程式設定元件資料庫更新。如果選擇此 Central Node 作為更新來源，Sandbox 也可以從其連線的 Central Node 接收資料庫更新。

手動更新資料庫

若要開始手動更新資料庫：

1. 在 Sandbox Web 介面視窗中選擇**資料庫更新**部分。

   最後更新設定群組將顯示 Sandbox 資料庫最近一次更新的時間和狀態。

2. 點擊**啟動**。

選擇資料庫更新來源

選擇資料庫更新來源：

1. 在 Sandbox Web 介面視窗中選擇**資料庫更新**部分。

2. 在**更新來源**設定群組中，選擇想要接收升級套件的來源：

   - **卡巴斯基更新伺服器**。

     該應用程式透過 HTTP 連線到卡巴斯基更新伺服器並下載最新的資料庫。

   - **卡巴斯基更新伺服器（安全連線）**。

     該應用程式透過 HTTPS 連線到卡巴斯基更新伺服器並下載最新的資料庫。建議使用 HTTPS 進行資料庫更新。

   - **自訂伺服器**。

     應用程式連線到您的 FTP 或 HTTP 伺服器或電腦上包含應用程式資料庫的目錄，以下載最新資料庫。您也可以選擇 Sandbox 連線到的 Central Node 作為更新來源。

     HTTP 必須用於 HTTP 伺服器和 Sandbox 之間的通訊。在這種情況下不支援 HTTPS。

3. 如果您選擇了**自訂伺服器**：

   - 如果要指定 FTP 或 HTTP 伺服器作為更新來源，請在此設定下方的欄位中指定應用程式資料庫更新包目錄的完整路徑。

   - 如果您想要將 Sandbox 連線到的 Central Node 指定為更新來源，請在欄位下左鍵按一下要使用的 Central Node 伺服器的 IP 位址。此欄位以 HTTP://<Central Node IP 位址>/retranslation 格式顯示 Central Node 伺服器的位址。

4. 點擊視窗下部的**套用**。

資料庫更新來源被選取。

使用卡巴斯基更新實用程式更新元件資料庫

如果您已將 Kaspersky Anti Targeted Attack Platform 部署在隔離網路或網際網路頻寬有限的網路中，則可以使用卡巴斯基更新實用程式設定元件資料庫更新。在這種情況下，該實用程式會將更新套件下載到組織內部部署網路以外的電腦，然後將其複製到您的 FTP 或 HTTP 伺服器。Sandbox 將從此伺服器接收更新套件。

使用此實用程式設定元件資料庫更新涉及以下步驟：

1. 使用卡巴斯基更新實用程式下載更新套件。

   首先，您需要聯絡卡巴斯基技術支援，並索取該實用程式的分發套件以及您可以從中下載更新的伺服器清單。

2. 將使用卡巴斯基更新實用程式取得的更新套件上傳至您的 FTP 或 HTTP 伺服器。

3. 選取您的 FTP 或 HTTP 伺服器作為資料庫更新來源。

使用卡巴斯基更新實用程式下載更新套件

您需要聯絡卡巴斯基技術支援，並要求提供該實用程式的分發套件，以及可用來下載更新的伺服器清單。

安裝卡巴斯基更新實用程式：

1. 將包含實用程式分發套件的資料夾下載到您的電腦。

2. 運行 UpdateUtility-Gui.exe 檔案。

3. 在開啟的視窗中，點選“**應用程式**”按鈕，然後選取**7.0-7.1** 選項左側的核取方塊。

4. 點選**“確定”**和**“套用”** 。

   該實用程式已安裝。您可以依照以下步驟下載服務套件。

若要使用卡巴斯基更新實用程式下載更新套件：

1. 在實用程式的主視窗中，點擊“**設定**”按鈕，然後選擇“**下載**”。

2. 在“**更新來源**”下，選擇“**其他**”，然後輸入用於下載更新的伺服器位址。

3. 點選“**確定**”和“**套用**” 。

4. 點擊“**啟動**”。

   更新套件被下載到執行該實用程式的電腦上。檔案已準備好上傳到您的 FTP 或 HTTP 伺服器。

啟用和停用更新資料庫的代理伺服器

若要啟用或停用代理伺服器來更新 Sandbox 元件資料庫：

1. 在 Sandbox Web 介面視窗中選擇**資料庫更新**部分。
2. 在工作區中，執行下列其中一項操作：
   - 如果您想將代理伺服器用於 Sandbox 元件資料庫更新，請啟用**代理伺服器**設定群組名稱旁邊的開關。
   - 如果您不想將代理伺服器用於 Sandbox 元件資料庫更新，請停用**代理伺服器**設定群組名稱旁邊的開關。

配置資料庫更新的代理伺服器連線設定

設定代理伺服器連線以更新 Sandbox 元件資料庫：

1. 在 Sandbox Web 介面視窗中選擇**資料庫更新**部分。
2. 啟用**代理伺服器**設定群組名稱旁邊的開關。
3. 在**電子郵件信箱**欄位中，輸入代理伺服器位址。
4. 在**連接埠**欄位中，輸入代理伺服器連接埠號。
5. 在**使用者名稱**欄位中，輸入代理伺服器使用者名稱。
6. 在**密碼**欄位中，輸入密碼以取得與代理伺服器的連線。
7. 執行以下操作之一：
   - 選擇**略過本機位址的代理伺服器**核取方塊，如果您不想將代理伺服器用於您組織的內部 IP 位址。
   - 清除**略過本機位址的代理伺服器**核取方塊，如果您想使用代理伺服器，而不管您組織的 IP 位址隸屬關係如何。
8. 點擊視窗下部的**套用**。

配置 Sandbox 和 Central Node 元件間的連線

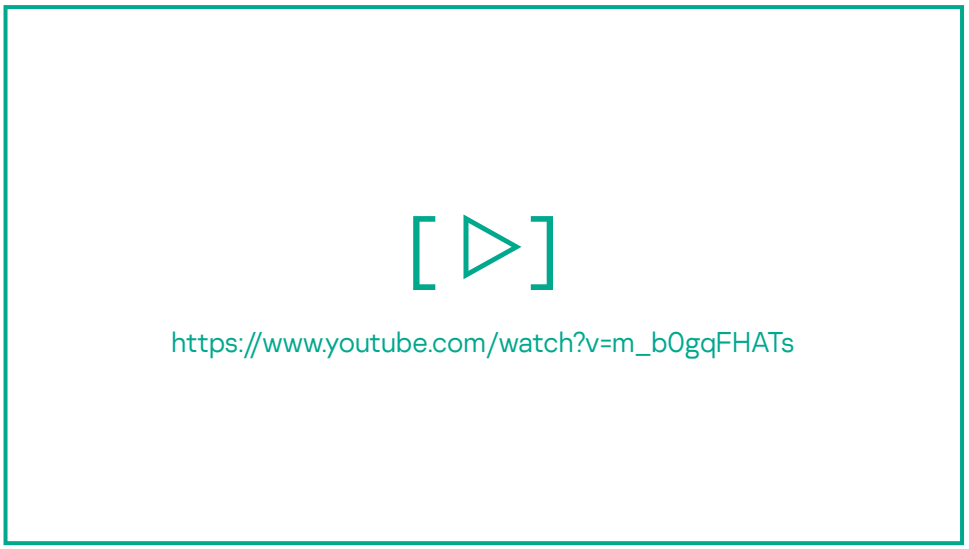
以下步驟用於設定 Sandbox 和 Central Node 元件間的連線：

1. 在應用程式 Web 介面中建立連線到 Sandbox 元件的請求。
2. Sandbox Web 介面顯示連線要求。

   您可以接受或拒絕請求。

> 配置連線後，Sandbox 伺服器需要 5 到 10 分鐘才能準備好運作。在此期間，應用程式 Web 介面的**系統健康**視窗會顯示警告：*標準配置出現問題*。當伺服器準備好運行時，警告就會消失。

觀看視頻教程，了解如何連線 Sandbox 和 Sensor 元件。您可以在幫助頁面（見下方）播放視頻，或點擊連結 https://youtu.be/m_b0gqFHATs?si=TCUGbvi0RV8JA1Kd。



連線 Sandbox 和 Sensor 元件，健康檢查

在 Sandbox Web 介面處理來自 Central Node 伺服器的連線請求

您可以在 Sandbox Web 介面中接受、拒絕或撤銷先前接受的來自 Central Node 伺服器的連線請求。

若要接受、拒絕或撤銷來自 Central Node 伺服器的連線請求：

1. 在 Sandbox Web 介面視窗中，選擇**授權**部分。

   Central Node 連線請求部分將顯示來自 Central Node 元件的連線請求清單。

   每個連線請求都包含以下資訊：

   - **IP** — Central Node 伺服器的 IP 位址。
   - **憑證指紋** — 用於在伺服器之間建立加密連線的 Central Node TLS 憑證的指紋。

- **狀態** — 連線請求的狀態。
  可能具有**待办的**或**已接受**值。

2. 確保 Central Node 憑證指紋與為 Central Node 配置的憑證指紋相符。
   您可以從**管理伺服器憑證**部分的 Central Node 伺服器管理員功能表中檢查 Central Node 憑證指紋。

3. 點擊包含來自 Central Node 元件的連線請求的行中的以下按鈕之一：

   - **接受**，如果您想接受連線請求。
   - **拒絕**，如果您想拒絕連線請求。
   - **撤銷**，如果您想撤銷先前接受的連線請求。

4. 點擊視窗下部的**套用**。

配置 Sandbox 元件網路介面

本節介紹Sandbox 元件網路介面的配置。

配置 DNS 設定

要配置 DNS：

1. 在 Sandbox Web 介面的視窗中，選擇**網路接口**部分。
2. 在**主機名稱**欄位中，輸入您要安裝 Sandbox 元件之伺服器的名稱，並採用 FQDN 格式（例如 sandbox）。
3. 在**DNS 伺服器**參數名稱的右側，點擊**新增**按鈕。
   這將會新增一個用於輸入 DNS 伺服器 IP 位址的空白欄位。
4. 以 IPv4 格式輸入主 DNS 伺服器的 IP 位址。
5. 點擊輸入欄位右側的✓按鈕。
   這將會新增一個 DNS 伺服器。
6. 如果您想新增其他 DNS 伺服器，請重複步驟 2-5。
7. 如果您想要移除先前新增的 DNS 伺服器，請點擊包含 DNS 伺服器 IP 位址的行右側的🗑按鈕。

> 您只能移除其他 DNS 伺服器。您無法移除主 DNS 伺服器。如果您新增了 2 個或更多 DNS 伺服器，那麼您可以移除它們中的任何一個，剩下的 DNS 伺服器將被用作主伺服器。

設定管理網路介面的設定

管理網路介面旨在透過 SSH 協定提供具有 Sandbox 元件的伺服器的存取權限，而Sandbox 元件也會透過此介面接收來自 Central Node 元件的物件。

您可以在 Sandbox 元件安裝期間設定管理網路介面。

您也可以從 Sandbox Web 介面設定一個管理網路介面。

若要從 Sandbox Web 介面設定一個管理網路介面：

1. 在 Sandbox Web 介面的視窗中，選擇**網路接口**部分。
2. 在**接口**下拉清單裡的**管理接口**設定群組中，選擇您要將其用作管理介面的網路介面。
3. 在**IP**欄位中，如果未指派 IP 位址，請輸入您想要指派給此網路介面的 IP 位址。
4. 在**遮罩**欄位中，輸入想要使用此網路介面的網路遮罩。
5. 點擊視窗下部的**套用**。

配置用於對已處理物件進行 Internet 存取的網路介面的設定

由 Sandbox 元件處理的物件可能會嘗試透過用於被處理物件的 Internet 存取的網路介面來嘗試在 Internet 上活動。Sandbox 元件可以對這些物件的行為進行分析。

如果封鎖網際網路存取，則 Sandbox 元件無法分析網際網路物件的行為，因此將只分析無網際網路存取物件的行為。

用於對已處理物件進行 Internet 存取的網路介面必須與組織的本機網路隔離。

如果組織的安全性原則拒絕來自本機網路使用者的電腦存取 Internet，且您已經為已處理物件配置用於存取 Internet 的 Sandbox 網路介面，則有下列情形的風險：

駭客可以將惡意應用程式附加到隨機檔案，並從本機網路使用者的電腦啟動對該檔案的 Sandbox 掃描。在透過 Sandbox 元件掃描檔案的過程中，該檔案將透過用於對已處理物件進行 Internet 存取的網路介面在本機網路以外被接管。

用於對已處理物件進行 Internet 存取的 Sandbox 網路介面不可用，這消除了此類資料傳輸的任何風險，但降低了警示品質。

若要設定用於對已處理物件進行 Internet 存取的網路介面：

1. 在 Sandbox Web 介面的視窗中，選擇**網路接口**部分。
2. 在**接口**清單的**網際網路接口**設定群組中，選擇您要將其用於對已處理物件進行網際網路存取的網路介面。

   在此網路介面清單中，您無法選擇您先前設定的管理網路介面。

3. 在**IP**欄位中，輸入您想要指派給此網路介面的 IP 位址。
4. 在**遮罩**欄位中，輸入想要使用此網路介面的網路遮罩。
5. 在**預設閘道**欄位中，輸入您想要使用此網路介面的網路的閘道位址。
6. 點擊視窗下部的**套用**。

新增、變更和移除靜態網路路由

在安裝 Sandbox 元件期間，您可以設定靜態網路路由。

您也可以從 Sandbox Web 介面新增、移除或變更靜態網路路由。

若要新增靜態網路路由：

1. 在 Sandbox Web 介面的視窗中，選擇**網路接口**部分。
2. 在**靜态路由**設定群組中，點擊**新增**按鈕。
   具有空白欄位的行將會新增到靜態網路路由清單中。
3. 在**IP**欄位中，輸入您想要為其配置靜態網路路由的伺服器的 IP 位址。
4. 在**遮罩**欄位中，輸入子網路遮罩。
5. 在**閘道**欄位中，輸入閘道的 IP 位址。
6. 從**接口**清單中，選擇一個您想要為其新增靜態網路路由的網路介面。
7. 點擊✓。
8. 點擊視窗下部的**套用**。

若要移除靜態網路路由，請執行下列操作：

1. 在 Sandbox Web 介面的視窗中，選擇**網路接口**部分。
2. 在包含您想要移除的靜態網路路由的行中的**静态路由**設定群組中，點擊🗑按鈕。
3. 點擊視窗下部的**套用**。

若要修改靜態網路路由：

1. 在 Sandbox Web 介面的視窗中，選擇**網路接口**部分。
2. 在包含您想要修改的靜態網路路由的行中的**靜态路由**設定群組中，點擊 按鈕。
   此靜態網路路由行將變為可編輯狀態。您可以變更靜態網路路由的一個或多個參數。
3. 在**IP**欄位中，變更您想要為其配置靜態路由的伺服器的 IP 位址。
4. 在**遮罩**欄位中，變更子網路遮罩。
5. 在**閘道**欄位中，變更閘道的 IP 位址。
6. 從**接口**清單中，選擇您正在編輯其網路路由的網路介面。
7. 點擊 。
8. 點擊視窗下部的**套用**。

Sandbox 身分驗證政策

您可以為 Kaspersky Anti Targeted Attack Platform 使用者設定 Sandbox 驗證政策。這些政策適用於所有具有 **KATA 使用者帳戶**帳戶類型的 Kaspersky Anti Targeted Attack Platform 使用者，無論其獲指派的角色為何。

終止非活動工作階段

如果使用者沒有執行任何操作（工作階段處於空閒狀態），我們建議終止此類工作階段。當使用者實際上已完成使用應用程式但未結束工作階段時，這可以降低未經授權存取 Kaspersky Anti Targeted Attack Platform 的風險。

關於身分驗證嘗試失敗的通知

頻繁嘗試登入 Web 介面或管理主控台失敗可能表示網路犯罪分子正在試圖透過暴力破解密碼來存取 Kaspersky Anti Targeted Attack Platform。為了防止此類未經授權的存取，我們建議啟用有關超出身分驗證嘗試失敗次數限制的通知。

終止不活動的 Sandbox 工作階段

如果使用者沒有執行任何操作（工作階段處於空閒狀態），我們建議終止此類工作階段。當使用者實際上已完成使用應用程式但未結束工作階段時，這可以降低未經授權存取 Kaspersky Anti Targeted Attack Platform 的風險。

若要啟用並配置非活動工作階段的終止：

1. 在 Sandbox Web 介面視窗中，選擇**身分驗證政策**部分。

2. 在**終止非活動工作階段**部分，指定當使用者未執行任何操作時終止使用者工作階段的時間。在**在此時間後終止非活動工作階段**欄位中輸入時間（分鐘）。

3. 點擊**套用**。

不活動的使用者工作階段將在指定時間後終止。

關於 Sandbox 身分驗證嘗試失敗的通知

頻繁嘗試登入 Web 介面或管理主控台失敗可能表示網路犯罪分子正在試圖透過暴力破解密碼來存取 Kaspersky Anti Targeted Attack Platform。為了防止此類未經授權的存取，我們建議啟用有關超出身分驗證嘗試失敗次數限制的通知。

若要啟用並設定有關失敗的身分驗證嘗試的通知：

1. 在 Sandbox Web 介面視窗中，選擇**身分驗證政策**部分。

2. 在**統計身分驗證嘗試次數**部分，將**計數嘗試次數**切換開關設定為**已啟用**。

3. 在**計數期間**欄位中，輸入要統計身分驗證失敗嘗試次數的期間。時間以分鐘為單位指定。如果使用者嘗試登入 Web 介面或管理主控台並連續失敗兩次以上，則會發生以下情況：

   - 有關使用者身分驗證嘗試失敗的記錄將寫入使用者活動日誌。

   - 如果已建立用於傳送有關過多次數身分驗證嘗試失敗的通知的規則（有關如何建立此類規則的資訊，請參閱下文），則會向通知規則中指定的位址傳送電子郵件訊息。該訊息包含有關失敗的使用者身分驗證嘗試的資訊。

   在**計數期間**欄位中，您可以指定 `0`，在這種情況下，所有失敗的身分驗證嘗試都會被計算在內，無論它們之間經過了多少時間。

4. 點擊**套用**。

系統會對失敗的身分驗證嘗試進行計數，如果超過指定的閾值（連續兩次身分驗證嘗試失敗），則會儲存有關此資訊以供審查。

若要傳送有關超出失敗的身分驗證嘗試閾值的通知，您需要在 Sensor 連線到的 Central Node 的 Web 介面中啟用和設定通知。如果 Sensor 連線到多個 Central Node，則可以設定在任意 Central Node 上傳送通知。

若要啟用並設定有關超出失敗的身分驗證嘗試次數的通知：

請依照相關步驟，建立用於傳送應用程式元件運作通知的規則。建立規則時，請在“**元件**”下選取“**授權嘗試**”核取方塊。

如果在指定的時間間隔內連續發生兩次以上的使用者身分驗證嘗試，則會向通知規則中指定的電子郵件信箱傳送一條訊息，其中包含有關失敗的使用者身分驗證嘗試的資訊（請參閱**計數期間**設定）。

設定 Sandbox 系統的日期和時間

若要在託管 Sandbox 元件的伺服器上設定日期和時間：

1. 在 Sandbox Web 介面視窗中，選擇**日期和時間**。
2. 在**時區**下拉清單中，選擇相關時區。
3. 如果您希望與 NTP 伺服器的時間同步，請選擇**與 NTP 伺服器同步**。
4. 如果您希望手動設定日期和時間，請不要啟用**與 NTP 伺服器同步**參數名稱右側的開關，並執行以下操作：
   a. 在**日期**欄位中，輸入目前日期，或點擊按鈕並在日曆中選擇一個日期。
   b. 在**時間**欄位中，輸入目前時間。
5. 點擊視窗下部的**套用**。

準備虛擬機以供使用

Sandbox 使用虛擬機在各種作業系統上運行物件，以便分析物件的行為並偵測其惡意活動。

您可以安裝兩種類型的虛擬機：

- 預配置。預配置虛擬機基於分發套件中的作業系統映像（ISO 檔案）。您無法修改這些映像或其中安裝的應用程式。

  > 預設作業系統和應用程式可能需要啟動。啟動是使用您的產品授權進行的。

- 自訂。預設虛擬機是基於您選擇的作業系統。您可以在這些作業系統上安裝任何應用程式來模擬真實的工作環境。

  自訂作業系統必須按照*配置作業系統和軟體部分中的說明進行配置*。要掃描此類作業系統中的物件，您需要建立使用者定義的 Sandbox 規則。

您可以同時使用自訂和預設的作業系統映像。

> 我們強烈建議您在每台 Sandbox 伺服器上使用分發套件中的所有可用預設作業系統映像。如果僅使用分發套件中的部分映像或僅使用自訂映像，掃描物件的品質可能會降低。

基於分發套件中的作業系統映像建立預設虛擬機

基於分發套件中的作業系統映像建立虛擬機的過程包括以下步驟：

1. 匯入範本
2. 建立虛擬機
3. 安裝虛擬機

根據您自己的作業系統映像建立自訂虛擬機

基於您自己的作業系統映像建立虛擬機涉及以下步驟：

1. 將作業系統映像以及要安裝在作業系統上的應用程式上傳到 Sandbox 儲存。

   您可以跳過此步驟並在建立和編輯範本時上傳映像。

2. 建立或匯入使用者定義的範本。
3. 如果作業系統之前未配置過，則必須按照*配置作業系統和軟體*部分中的說明進行配置。配置操作在編輯範本時執行。
4. 建立虛擬機
5. 安裝虛擬機

如果您在安裝的虛擬機上遇到問題，可以參考卡巴斯基客戶服務知識庫。

> 如果作業系統或應用程式啟動出現問題，Sandbox 元件的 Web 介面會顯示錯誤訊息。如果發生這種情況，請聯絡卡巴斯基技術支援。

管理 Sandbox 儲存中的作業系統和應用程式映像

您想要在這些作業系統上安裝的作業系統和應用程式的自訂映像放置在 Sandbox 儲存中。

> 我們強烈建議使用原始 Microsoft ISO 映像。

您可以將以下自訂作業系統映像上傳到儲存空間：

- Windows XP SP3 或更高版本
- Windows 7

- Windows 8.1 64 位元
- Windows 10 64 位元（最高版本 1909）

上傳的檔案必須具有 .ISO 副檔名。

不支援上傳伺服器 Windows 作業系統或任何 Linux 作業系統的自訂映像。

如果要在範本中使用自訂作業系統映像，則必須配置這些作業系統。

檢視 Sandbox 儲存中的作業系統和應用程式映像表

要檢視 Sandbox 儲存中的作業系統和應用程式映像表：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**儲存**部分。

   Sandbox 儲存中的作業系統和應用程式映像表已顯示。

表包含以下資訊：

- **已上傳**是映像上傳時間。
- **名稱**是映像的名稱。
- **大小**是映像的大小。
- **操作**是可對映像進行的操作。可能的值：**建立 VM**、**匯出**、**刪除**。

將作業系統和應用程式映像上傳到儲存

若要將您想要在這些作業系統上安裝的作業系統和應用程式的自訂映像上傳到儲存：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**儲存**部分。
3. 點擊**上傳**。
4. 這將開啟檔案上傳視窗。
5. 選擇您想上傳到儲存的 .ISO 檔案。
6. 點擊**開啟**。

   如果要上傳多個映像，請為每個映像重複步驟 1 至 6。

   映像將被上傳到儲存並顯示在物件表中。

啟動 Sandbox 儲存中的作業系統和應用程式映像

您可以使用 Windows 7（64 位元）、Windows 10（64 位元）以及 Sandbox 元件所需應用程式的未啟動映像建立虛擬機，並在安裝虛擬機後使用您自己的產品授權代碼啟動它們。

Windows 映像和 Microsoft Office 套件可以使用 Kata_images.py 檔案啟動。若要取得該檔案，請聯絡技術支援。

正確啟動 Windows 映像和 Microsoft Office 套件需要存取 Internet。確保網際網路存取設定正確。

在**控制板**區段的啟動過程中，Central Node 會提醒您 Sandbox 發生自我診斷錯誤。成功啟動後，Sandbox 自我診斷錯誤不再顯示。啟動期間，物件不會被傳送到 Sandbox 進行掃描。

若要啟動 Windows 映像和 Microsoft Office 套件：

1. 確保具有 Windows 7（64 位元）、Windows 10（64 位元）和 Microsoft Office 套件未啟動映像的虛擬機已建立並安裝。
2. 透過 SSH 協定或終端登入 Sandbox 元件伺服器的管理主控台。
3. 當系統提示您時，請輸入在安裝應用程式期間設定的管理員使用者名稱和密碼。

   顯示 Sandbox 伺服器的管理員功能表。
4. 在應用程式管理員功能表中，選擇**技術支援模式**。
5. 按下 **Enter**。

   這將開啟技術支援模式確認視窗。
6. 選擇**是**，然後按 **ENTER**。
7. 透過執行以下命令序列啟動 Windows 映像和 Microsoft Office 套件：

   a. `cd /opt/kaspersky/sandbox/bin/`

   b. `sudo -s`

   c. `./sbimages_cli activate --vm_id Win7_x64 --component Win7 --key <Windows 7 64 位元啟動碼>`

   d. `./sbimages_cli activate --vm_id Win7_x64 --component Office2010 --key <Microsoft Office 2010 啟動碼>`

   e. `./sbimages_cli activate --vm_id Win10_x64 --component Win10 --key <Windows 10 64 位元啟動碼>`

   f. `./sbimages_cli activate --vm_id Win10_x64 --component Office2016 --key <Microsoft Office 2016 啟動碼>`

啟動碼的格式如下：XXXXX-XXXXX-XXXXX-XXXXX-XXXXX。

8. 為新增了產品授權金鑰的虛擬機建立還原點：

   ```
   ./sbimages_cli snapshot --vm_ids Win7_x64,Win10_x64
   ```

   該過程可能需要一些時間。

9. 確保應用程式 Web 介面的**控制板**區段未顯示任何有關 Sandbox 元件無法運作的警告。

Windows 映像和 Microsoft Office 套件已啟動。您必須在所有 Sandbox 伺服器上啟動 Windows 作業系統和 Microsoft Office 應用程式套件的映像。

如果您在嘗試啟動時遇到任何問題，我們建議您聯絡技術支援。

從 Sandbox 儲存中刪除作業系統和應用程式映像

若要從 Sandbox 儲存中移除作業系統或應用程式映像：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**儲存**部分。
3. 在相關映像旁的**操作**列中，點擊**刪除**。

   這將開啟操作確認視窗。

4. 點擊**是**。

映像被刪除。

管理虛擬機範本

虛擬機根據範本建立。若要建立虛擬機，您必須先為其匯入或建立範本。可以基於相同範本建立多個虛擬機。

您可以對範本執行以下操作：檢視範本表、啟用或停用範本、編輯、匯出或刪除範本。

> 如果使用此範本建立或安裝自訂虛擬機，則無法使用範本進行操作。虛擬機建立和安裝過程完成後，您可以再次使用範本進行操作。

建立虛擬機範本

若要建立虛擬機，您必須先為其建立範本。

若要為虛擬機建立範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 從**新增**下拉清單中選擇**建立範本**。
   這將開啟範本建立視窗。
4. 在**準備鏡像**步驟：
   a. 在**名稱**欄位中，輸入範本的名稱。
   b. 在**敘述**欄位中，輸入範本描述。該欄位是可選的。
   c. 在**作業系統鏡像**下拉清單中，執行下列操作之一：
      - 從可用映像清單中選擇要用於範本的作業系統映像。
        要在清單中顯示映像，您必須先將其上傳到儲存。
      - 若要上傳作業系統映像，請點擊**上傳**連結，選擇相關檔案，然後點擊**開啟**。
        上傳的檔案必須具有 ISO 副檔名。
5. 點擊**繼續**。
6. 在**自訂範本**步驟，執行下列其中一項操作：
   a. 在**掛載 ISO**下拉清單中，選擇要在作業系統中安裝的應用程式映像。
      對於要在清單中顯示的映像，請執行下列其中一項操作：
      - 將映像上傳到儲存。
      - 在**掛載 ISO**下拉清單中，點擊**上傳**連結，選擇相關檔案，然後點擊**開啟**。
        上傳的檔案必須具有 ISO 副檔名。
   b. 如果要卸載已安裝的映像，請在**掛載 ISO**下拉清單中，點擊該映像旁邊的⏏圖示。
   c. 配置作業系統和已安裝的軟體。
   d. 在**關機**下拉清單中，執行下列操作之一：
      - **關機**，如果您想關閉系統，同時儲存正在執行的應用程式的結果。
      - **關閉電源**，如果您想關閉系統而不儲存結果。

      > 如果啟用了範本，您將無法使用該範本建立虛擬機，也無法匯出該範本。如果您想繼續配置範本，請將其啟用。

虛擬機範本已建立。您可以基於它建立虛擬機。

檢視範本表

若要檢視範本表：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。

   範本表將顯示。

表包含以下資訊：

- **已建立**是範本建立時間。
- **類型**是作業系統的類型：自訂或預設。
- **名稱**是範本的名稱。
- **狀態**是範本的狀態，例如，**開機**或**應用程式的所有主要元件都將停止。若要啟動它們，請關閉叢集伺服器（如果尚未關閉），然後重新開啟它們的電源。**。
- **大小**是範本的大小。
- **作業係統**是用於範本的作業系統版本。
- **VM**是根據這個範本建立的虛擬機。
- **操作**是範本可用的操作。可以進行以下操作：**建立 VM**、**匯出**（ ）、**刪除**（ ）。
- **敘述**是建立範本時指定的描述。

開啟或關閉範本

如果範本已關閉，您可以使用範本執行下列操作：基於範本建立虛擬機、匯出或刪除它。如果範本已開啟，您可以對其進行編輯。

若要開啟或關閉範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 選擇相關範本。

4. 在**自訂範本**部分中，執行下列其中一項操作：
   - 如果您想開啟範本，請在範本管理主控台中點擊**開機**。
   - 如果您想關閉範本，請在範本中管理主控台的**關機**下拉清單中選擇選項之一：
     - **關機**，如果您想關閉系統，同時儲存正在執行的應用程式的結果。
     - **關閉電源**，如果您想關閉系統而不儲存結果。

範本已開啟或關閉。

編輯範本

編輯範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 選擇相關範本。
4. 如果範本已關閉，請點擊**開機**將其開啟。
5. 如果要在用於範本的作業系統上安裝應用程式，請從**掛載 ISO**下拉清單中選擇相關的應用程式映像。
   要在清單中顯示映像，您必須先將映像上傳到儲存空間。
6. 如果要卸載已安裝的映像，請在**掛載 ISO**下拉清單中，點擊該映像旁邊的**解除安裝**⏏圖示。
7. 配置作業系統和已安裝的軟體。

範本已編輯。

配置作業系統和軟體

準備作業系統以供使用

安裝Windows 7、8.1 或10 作業系統時，必須符合下列要求：

- 停用螢幕防護程式。
- 選擇*始終開啟*電源計劃。
- 停用自動更新。
- 停用 Windows 防火牆。

如果您使用的是Windows 7，則需要支援SHA-2 雜湊演算法。若要確保此雜湊演算法受支援，請安裝適用於 x64 系統的 Windows 7 安全更新 (KB3033929)。對於32 位元Windows 7 作業系統，也必須安裝更新 KB3033929。

> 不要安裝更新 KB4474419。此更新可能會導致虛擬機部署期間崩潰。

若要使用 Windows 7，您必須在作業系統設定中啟用 TLS 1.1 和 TLS 1.2。為此，請在 Windows 7 的**控制面板 → 網際網路選項 → 進階**區段中，選取**使用 TLS 1.1** 和**使用 TLS 1.2** 核取方塊。

使用 Windows 8.1 和10 作業系統時，必須停用快速啟動並啟用自動登入。

作業系統的當地語係化

您可以在安裝系統時選擇本地化語言，也可以安裝具有英語本地化的系統，並在該系統中額外安裝本地化套件。您可以選擇以下語言之一：俄語、英語、中文（簡體）、阿拉伯語、西班牙語（墨西哥）。如果選擇不同的本地化，物件掃描的品質會降低。

> 對於 Windows XP 作業系統，僅支援俄語和英語。

配置作業系統

安裝作業系統時：

- 確保配置了預設命令 shell。
- 啟動作業系統和其他授權軟體。

> 使用 Windows 10 作業系統時，需要緩解 Spectre 和 Meltdown 弱點並停用 Windows Defender。

您可以使用已安裝的作業系統執行以下操作：

- 為電腦分配靜態名稱。
- 建立使用者帳戶。

  > 此時，您需要設定自動登入。

- 安裝軟體。
  軟體安裝限制：
  - 一次只能將一張映像連線到一個範本。儲存範本後，您可以斷開一個映像並安裝另一個映像。
  - 支援以下版本的 Microsoft Office：Microsoft Office Professional Plus 2010 for Windows 7 和 Microsoft Office Professional Plus 2016 for Windows 10。

- 強烈建議不要安裝以下類型的軟體：
  - 將其代碼注入另一個正在運行的處理程序的軟體
  - 防護驅動程式
  - 病毒防護應用程式，包括 Windows Defender
- 無法保證偵測到依賴高度專業化軟體運作的檔案的惡意活動。

Kaspersky Anti Targeted Attack Platform 不會通知作業系統上安裝的軟體出現的問題。

緩解 Spectre 和 Meltdown 弱點

要成功安裝基於 Windows 10 作業系統的自訂虛擬機，需要緩解 Spectre 和Meltdown 弱點。

要緩解 Spectre 和 Meltdown 弱點：

1. 在來賓作業系統的命令列中，執行以下命令序列：

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 3 /f
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
   ```

2. 重啟虛擬機。

Specter 和 Meltdown 類型的弱點被緩解。

解除安裝 Windows Defender

要成功安裝基於 Windows 10 作業系統的自訂虛擬機，您必須解除安裝 Windows Defender。

所有操作必須在訪客作業系統中執行。

若要解除安裝 Windows Defender：

1. 在“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender”登錄機碼中建立一個 DWORD32 值。
2. 將下列值新增至您在步驟 1 中建立的 DWORD32 值：
   - AllowFastServiceStartup = 0.
   - ServiceKeepAlive = 0.
   - DisableAntiSpyware = 1.
3. 在“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender”登錄機碼下建立“Real-Timeer Protection Protection”鍵。

4. 在“Real-Time Protection”鍵下建立一個 DWORD32 值。

5. 將下列值新增至您在步驟 4 中建立的 DWORD32 值：

   - DisableIOAVProtection = 1.
   - DisableRealtimeMonitoring = 1.

6. 在“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender”登錄機碼下建立 Spynet 鍵。

7. 在“Spynet”鍵下建立一個 DWORD32 值。

8. 將下列值新增至您在步驟 6 中建立的 DWORD32 值：

   - DisableBlockAtFirstSeen = 1.
   - LocalSettingOverrideSpynetReporting = 1.
   - SubmitSamplesConsent = 1.

9. 使用群組原則停用 Windows Defender。為此：

   a. 按 Win+R。

   b. 這將開啟“**執行**“對話方塊；在“**開啟**”欄位中，輸入 regedit。

   c. 點擊“**確定**”。

   d. 導覽至**關閉 Microsoft Defender 病毒防護**設定：**電腦設定→管理範本→ Windows 元件→ Microsoft Defender 病毒防護→關閉 Microsoft Defender 病毒防護→編輯政策設定**。

   e. 選擇“**已停用**”。

10. 進入安全模式：

   a. 按 Win+R。

   b. 在“**執行**“對話方塊的“**開啟**”欄位中，輸入 msconfig。

   c. 點擊“**確定**”。

   d. 在顯示的視窗中，移至**“啟動”**索引標籤。

   e. 選取“**安全啟動**”核取方塊。

   f. 在**“安全啟動”**核取方塊下，選擇**“最小”**選項。

   g. 點擊“**套用**”，然後點擊“**確定**” 。

   h. 在顯示的視窗中，選擇“**重新啟動**”。

11. 重新啟動後，從登錄檔中刪除 WinDefend 鍵：

    a. 按 Win+R。

    b. 這將開啟“**執行**“對話方塊；在“**開啟**”欄位中，輸入 regedit。

    c. 點擊“**確定**”。

    d. 刪除“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”登錄機碼下的“WinDefend”鍵。

12. 停用安全模式：

    a. 按 Win+R。

    b. 在“**執行**“對話方塊的“**開啟**”欄位中，輸入 msconfig。

    c. 點擊“**確定**”。

    d. 在顯示的視窗中，移至**“啟動”**索引標籤。

    e. 取消選取“**安全啟動**”核取方塊。

    f. 點擊“**套用**”，然後點擊“**確定**” 。

    g. 在顯示的視窗中，選擇“**重新啟動**”。

    Windows Defender 被停用。

匯出範本

您可以透過以下方式之一匯出範本：

- 在範本表中。
- 檢視範本時。

> 必須關閉該範本。

要匯出範本表中的範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 在相關映像旁的**操作**列中，點擊 。

   範本已匯出。檔案下載自動開始。

檢視範本時匯出範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 選擇相關範本。
4. 在**操作**下拉式清單中，選擇**匯出**。

   檔案下載自動開始。

匯入範本

您可以匯入先前建立的範本。

若要匯入範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 在**新增**下拉清單中，選擇**匯入範本**。
4. 這將開啟檔案上傳視窗。
5. 選擇您想匯入的檔案。
6. 點擊**開啟**。

   此範本出現在範本清單中。

您可以編輯範本、根據範本建立虛擬機、匯出或刪除範本。

刪除範本

刪除範本時，所有基於該範本建立的虛擬機都將被刪除。

您可以透過以下方式之一刪除範本：

- 在範本表中。
- 檢視範本時。

必須關閉該範本。

若要刪除範本表中的範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 在相關映像旁的**操作**列中，點擊🗑。
   這將開啟操作確認視窗。
4. 點擊**是**。

範本被刪除。

檢視範本時刪除範本：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 選擇相關範本。
4. 在**操作**下拉式清單中，選擇**刪除**。
   這將開啟操作確認視窗。
5. 點擊**是**。

範本被刪除。

管理虛擬機

您可以建立、安裝或刪除已安裝的虛擬機和待安裝的虛擬機。您也可以檢視具有預設和自訂作業系統的虛擬機清單。

建立虛擬機

您可以透過以下方式之一在 Sandbox Web 介面中建立虛擬機器：

- 在**虛擬機**部分。
- 在範本表中。
- 在範本視圖中。

虛擬機範本必須關閉。建立虛擬機後，必須安裝它。

由於瀏覽器的限制，在 Sandbox Web 介面中建立虛擬機器可能會失敗。如果遇到此類限制，您可以使用命令列建立和安裝虛擬機。

建立自訂虛擬機器需要網際網路存取。

在“虛擬機”部分建立虛擬機

*在**虛擬機**部分使用預設作業系統映像建立虛擬機：*

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**虛擬機**部分。
3. 點擊**建立 VM**。
   這將開啟虛擬機建立視窗。
4. 在**範本**下拉清單中，選擇虛擬機的範本。
   如果清單中沒有合適的範本，您可以在 Sandbox Web 介面視窗中的**範本**部分匯入或建立範本。
5. 在**名稱**欄位中，鍵入虛擬機的名稱。
6. 在**敘述**欄位中，輸入虛擬機的描述。該欄位是可選的。
7. 點擊**儲存**。
8. 分發套件中的某些作業系統要求接受相關最終使用者產品授權協議的條款。閱讀最終使用者產品授權協議的文字並點擊**接受**。

具有預設作業系統映像的虛擬機已建立。

*在**虛擬機**部分使用自訂作業系統映像建立虛擬機：*

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**虛擬機**部分。
3. 點擊**建立 VM**。
   這將開啟虛擬機建立視窗。
4. 在**範本**下拉清單中，選擇虛擬機的範本。
   如果清單中沒有合適的範本，您可以在 Sandbox Web 介面視窗中的**範本**部分匯入或建立範本。
5. 在**名稱**欄位中，鍵入虛擬機的名稱。

   該名稱必須由拉丁字元組成。

6. 在**敘述**欄位中，輸入虛擬機的描述。該欄位是可選的。

7. 點擊**儲存**。

8. 如果未為建立虛擬機的伺服器設定網際網路存取，則會在**範本**視窗中顯示*無網際網路存取*錯誤訊息。要完成虛擬機建立過程，您必須下載 Debug 符號。

具有自訂作業系統映像的虛擬機被建立。

在範本表中建立虛擬機

若要使用範本表中預設的作業系統映像建立虛擬機：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。

   前往**範本**部分。

2. 在範本旁邊的**操作**列中，點擊**建立 VM**。

   這將開啟虛擬機建立視窗。

3. 在**範本**下拉清單中，選擇虛擬機的範本。

   如果清單中沒有合適的範本，您可以在 Sandbox Web 介面視窗中的**範本**部分匯入或建立範本。

4. 在**名稱**欄位中，鍵入虛擬機的名稱。

5. 在**敘述**欄位中，輸入虛擬機的描述。該欄位是可選的。

6. 點擊**儲存**。

7. 分發套件中的某些作業系統要求接受相關最終使用者產品授權協議的條款。閱讀最終使用者產品授權協議的文字並點擊**接受**。

具有預設作業系統映像的虛擬機已建立。

若要使用範本表中的自訂作業系統映像建立虛擬機：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。

   前往**範本**部分。

2. 在範本旁邊的**操作**列中，點擊**建立 VM**。

   這將開啟虛擬機建立視窗。

3. 在**範本**下拉清單中，選擇虛擬機的範本。

   如果清單中沒有合適的範本，您可以在 Sandbox Web 介面視窗中的**範本**部分匯入或建立範本。

4. 在**名稱**欄位中，鍵入虛擬機的名稱。

   該名稱必須由拉丁字元組成。

5. 在**敘述**欄位中，輸入虛擬機的描述。該欄位是可選的。

6. 點擊**儲存**。

7. 如果未為建立虛擬機的伺服器設定網際網路存取，則會在**範本**視窗中顯示*無網際網路存取*錯誤訊息。要完成虛擬機建立過程，您必須下載 Debug 符號。

具有自訂作業系統映像的虛擬機被建立。

在範本視圖中建立虛擬機

若要使用範本檢視中預設的作業系統映像建立虛擬機：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。

2. 前往**範本**部分。

3. 選擇相關範本。

4. 點擊**建立 VM**。

   這將開啟虛擬機建立視窗。

5. 在**範本**下拉清單中，選擇虛擬機的範本。

   如果清單中沒有合適的範本，您可以在 Sandbox Web 介面視窗中的**範本**部分匯入或建立範本。

6. 在**名稱**欄位中，鍵入虛擬機的名稱。

7. 在**敘述**欄位中，輸入虛擬機的描述。該欄位是可選的。

8. 點擊**儲存**。

9. 分發套件中的某些作業系統要求接受相關最終使用者產品授權協議的條款。閱讀最終使用者產品授權協議的文字並點擊**接受**。

具有預設作業系統映像的虛擬機已建立。

若要使用範本檢視中的自訂作業系統映像建立虛擬機：

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。

2. 前往**範本**部分。

3. 選擇相關範本。

4. 點擊**建立 VM**。

   這將開啟虛擬機建立視窗。

5. 在**範本**下拉清單中，選擇虛擬機的範本。

   如果清單中沒有合適的範本，您可以在 Sandbox Web 介面視窗中的**範本**部分匯入或建立範本。

6. 在**名稱**欄位中，鍵入虛擬機的名稱。

   該名稱必須由拉丁字元組成。

7. 在**敘述**欄位中，輸入虛擬機的描述。該欄位是可選的。

8. 點擊**儲存**。

9. 如果未為建立虛擬機的伺服器設定網際網路存取，則會在**範本**視窗中顯示*無網際網路存取*錯誤訊息。要完成虛擬機建立過程，您必須下載 Debug 符號。

具有自訂作業系統映像的虛擬機被建立。

使用命令列建立和安裝虛擬機器

由於瀏覽器的限制，在 Sandbox Web 介面中建立虛擬機器可能會失敗。如果您遇到此類限制，可以使用命令列建立和安裝虛擬機器。

> 建立自訂虛擬機器需要網際網路存取。

需要逐一建立虛擬機器。

若要使用命令列建立和安裝虛擬機器：

1. 透過 SSH 協定或透過終端機進入 Sandbox 伺服器的管理主控台。

2. 系統提示時，輸入在 Sandbox 安裝期間指定的管理員使用者名稱和密碼。

   顯示元件管理員選單。

3. 在元件管理員選單中，選擇“技術支援模式”。

4. 按下“**`Enter`**”。

   這將開啟技術支援模式確認視窗。

5. 確認您要在技術支援模式下管理該元件。為此，請選擇**確定**並按 **`Enter`**。

6. 檢視系統中所有可用的 ISO 映像清單：

   ```
   sb-vm-iso --list-iso
   ```

   此清單以 JSON 陣列形式顯示，其中列出了 ISO 映像的名稱。在後續說明中，`<ISO 名稱>` 變數用來取代 ISO 映像的名稱。

7. 確保 ISO 映像檔處於正常運作狀態並已準備好部署：

   ```
   sb-vm-iso --check-install <ISO 名稱>
   ```

   此指令應輸出 `'success'` 狀態。

8. 安裝虛擬機：

   ```
   sb-vm-iso --install <ISO 名稱>
   ```

   此指令需要一些時間才能完成。系統不會通知安裝成功或失敗。

9. 儲存設定：

   ```
   sb-vms --apply-all
   ```

   此指令需要一些時間才能完成。此指令應輸出 `'success'` 狀態。

10. 確保這些說明的步驟 7–9 中建立的虛擬機器顯示在虛擬機器清單中。若要檢視虛擬機器清單的說明，請參閱“檢視具有預設作業系統的虛擬機器表”和“檢視具有自訂作業系統的虛擬機器表”部分。

11. 對於要用來建立和安裝虛擬機器的每個 ISO 映像，重複這些說明的步驟 7–10。

    將建立並安裝虛擬機器。此虛擬機器的名稱會加入到虛擬機器清單中。

檢視自預設虛擬機器表

若要檢視預設虛擬機器清單，請執行下列操作：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**部分。

2. 選擇**預配置**頁簽。

   將顯示預設虛擬機器表。

表包含以下資訊：

- **名稱**是虛擬機的名稱。
- **狀態**是虛擬機的狀態，例如，**已啟用**或者**已停用**。
- **操作**是可以對虛擬機進行的操作。可以進行以下操作：**刪除**。

未安裝虛擬機部分顯示已準備好安裝但尚未安裝的虛擬機。

檢視自訂虛擬機表

若要檢視自訂虛擬機器清單，請執行下列操作：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**區段。

2. 選擇**自訂**索引標籤。

   將顯示自訂虛擬機表。

表包含以下資訊：

- **已建立**是虛擬機建立的時間。
- **名稱**是虛擬機的名稱。
- **狀態**是虛擬機的狀態，例如，**已啟用**或者**已停用**。
- **操作**是可以對虛擬機進行的操作。可以進行以下操作：**刪除**。
- **敘述**是建立虛擬機時指定的描述。

安裝虛擬機

建立虛擬機後，必須安裝它。

若要安裝具有預設作業系統映像的虛擬機：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**部分。
2. 選擇**預配置**頁簽。
3. 在**未安裝虛擬機**部分，點擊**安裝準備好的 VM**。

   所有待安裝的虛擬機均已安裝。

若要安裝具有自訂作業系統映像的虛擬機：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**區段。
2. 選擇**自訂**索引標籤。
3. 在相關虛擬機旁的**操作**列中，點擊**安裝**連接。
4. 安裝虛擬機後，在**操作**列中，點擊**啟用**連接。

   虛擬機已安裝並可供使用。

刪除虛擬機

若要刪除已安裝的虛擬機：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**部分。
2. 選擇**預配置**或者**自訂**頁簽。
3. 在相關虛擬機旁的**操作**列中，點擊**刪除**。

   虛擬機已刪除。

若要刪除具有預設作業系統映像的未安裝虛擬機：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**部分。
2. 在**未安裝虛擬機**部分，點擊**刪除所有掛起的 VM**。

   所有具有待安裝的預設作業系統映像的虛擬機都將被刪除。

若要刪除具有自訂作業系統映像的未安裝虛擬機：

1. 在 Sandbox Web 介面的視窗中，選擇**虛擬機**區段。
2. 選擇**自訂**索引標籤。
3. 在相關虛擬機旁的**操作**欄中，點擊**刪除**連結。

   具有等待安裝的自訂作業系統映像的虛擬機將被刪除。

下載偵錯符號

如果在其上安裝具有自訂映像的虛擬機的伺服器未配置 Internet 存取，則必須下載 Microsoft 偵錯符號才能正確完成虛擬機安裝。

您可以在虛擬機安裝過程中在**範本**視窗中下載偵錯符號，或在虛擬機收到虛擬機清單中的**已失敗**狀態後下載調試符號。

> 為了正確下載偵錯符號，用於虛擬機範本的作業系統必須安裝Windows 偵錯工具，且連線到網路的主機的名稱（hostname）必須僅包含拉丁字母、數字和特殊字元。

*在虛擬機安裝期間在**範本**視窗中下載偵錯符號：*

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
2. 前往**範本**部分。
3. 選擇相關範本。
4. 在包含*无網際網路存取*錯誤的視窗中，點擊**下載聲明**。

   > **下載聲明**直到虛擬機獲得**已失敗**狀態後才可用。

   壓縮檔案將下載到您的電腦上。
5. 解壓縮下載的檔案。
6. 使用 Windows PowerShell 執行 Sbsymtool.ps1。
   帶有調試符號的壓縮檔案將被下載到該檔案所在的資料夾中。
7. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。
8. 前往**範本**部分。
9. 選擇您已為其下載偵錯符號的範本。

10. 在**操作**下拉清單中，選擇**上傳符號**。

11. 這會開啟一個視窗；在該視窗中，選擇帶有偵錯符號的壓縮檔案，然後點擊**開啟**。

    調試符號被下載。虛擬機被安裝並顯示在運行自訂作業系統的虛擬機清單中。

*在虛擬機收到虛擬機清單中的**已失敗**狀態後下載調試符號：*

1. 在 Sandbox Web 介面視窗中，選擇**範本和儲存**部分。

2. 前往**範本**部分。

3. 選擇相關範本。

4. 在**操作**下拉清單中，選擇**下載聲明**。

   壓縮檔案將下載到您的電腦上。

5. 解壓縮下載的檔案。

6. 使用 Windows PowerShell 執行 Sbsymtool.ps1。

   帶有調試符號的壓縮檔案將被下載到該檔案所在的資料夾中。

7. 在**範本**視窗中，展開**操作**清單並選擇**上傳符號**。

8. 這會開啟一個視窗；在該視窗中，選擇帶有偵錯符號的壓縮檔案，然後點擊**開啟**。

   調試符號被下載。虛擬機被安裝並顯示在運行自訂作業系統的虛擬機清單中。

設定同時運作的虛擬機的最大數量

設定同時運作、且具有 Sandbox 元件在其中處理物件的作業系統的虛擬機的數量限制。我們建議使用*Sandbox 元件計算*部分中給出的值。如果要使用其他值，請確保安裝 Sandbox 的伺服器有足夠的硬體資源。

您可以使用以下公式計算同時執行的具有作業系統映像的虛擬機的數量：<邏輯核心數> * 1.5。

預設情況下，同時執行的虛擬機數量上限為 100。在為同時執行的虛擬機器設定新的限制之前，您可以按照*變更虛擬機器的產品授權金鑰數量*過程的步驟將其增加到 200。

> 同時運作的虛擬機的最大數量不能超過 200。

要設定同時運行的虛擬機的最大數量：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。

2. 在**訪客虛擬機**設定群組的**最多同時執行的 VM**欄位中，輸入同時執行的虛擬機數量。

   在預設配置下，您可以輸入 1 到 100 之間的數字。如果您之前已將自訂虛擬機的產品授權金鑰數量變更為 200，則可以輸入 1 到 200 之間的數字。

3. 點擊**儲存**。

變更自訂虛擬機器的產品授權金鑰數量

建立自訂虛擬機時，Kaspersky Anti Targeted Attack Platform 會指定該虛擬機內使用的軟體的產品授權金鑰數量。預設情況下，產品授權金鑰的數量等於同時運行的虛擬機的數量。您的產品授權必須涵蓋此數量。如有必要，您可以變更虛擬機的產品授權金鑰數量。

如果虛擬機配置的產品授權金鑰數量少於同時執行的虛擬機數量，Sandbox 伺服器的整體效能可能會下降。

不建議變更同時運行的虛擬機的指定數量。

要變更自訂虛擬機器的產品授權金鑰數量：

1. 透過 SSH 協定或透過終端機進入 Sandbox 伺服器的管理主控台。
2. 透過執行 `sb-custom-images list-vm` 指令取得伺服器清單。

   將顯示虛擬機器表，其中：

   - `id` 是虛擬機器的 ID，
   - `name` 是虛擬機的名稱。
   - `licenses` 是產品授權金鑰的數量。
3. 通过執行 `sb-custom-images licenses -id <虛拟机 ID> -ln <產品授權數量>` 命令設定所选虛拟机的產品授權金鑰數量。

產品授權金鑰的數量已變更。

若要取得指令碼的協助，請執行 `Sb-custom-images --help`指令。

匯出 Sandbox 設定

匯出 Sandbox 系統的設定：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。
2. 在**設定**設定群組中，點擊**匯出**按鈕。

   這將開啟**警告**視窗，其中包含關於匯出系統參數的警告詳情。

Sandbox 系統參數取決於安裝 Sandbox 元件的伺服器的硬體和軟體參數。Sandbox 系統匯出的參數旨在匯入至配置嚴格相同的相同伺服器或其他伺服器。任意使用儲存在其他 Sandbox 系統的參數值來還原 Sandbox 系統配置的嘗試都可能會破壞Sandbox 系統。

3. 點擊**儲存**。

將 tar.gz 檔案下載到您電腦的硬碟的資料夾中，該資料夾設定為用於使用該應用程式的瀏覽器設定中的檔案下載資料夾。檔案包含了所有 Sandbox 系統目前參數。

帶有系統參數備份副本的壓縮檔案可以包含機密資訊，例如密碼和隱私金鑰。Kaspersky Anti Targeted Attack Platform 的管理員必須自行確保此資料的安全。

匯入 Sandbox 設定

匯入 Sandbox 設定：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。

2. 在**設定**設定群組中，點擊**匯入**按鈕。

   這將開啟**警告**視窗，其中包含關於匯入系統參數的警告詳情。

   Sandbox 元件參數取決於安裝 Sandbox 的伺服器的硬體和軟體參數。Sandbox 匯出的參數旨在匯入至嚴格相同配置的相同伺服器或其他伺服器。任意使用儲存在其他 Sandbox 系統的參數設定來還原 Sandbox 系統配置的嘗試都可能會破壞Sandbox 系統。

3. 點擊**還原**。

   這將開啟檔案選擇視窗。

4. 選擇一個 Tar.gz 檔案，其中包含要下載的 Sandbox 參數，然後點擊**開啟**按鈕。

   這將關閉檔案選擇視窗。

   如果 Sandbox 參數匯入成功，Sandbox 伺服器將重新啟動。幾分鐘後，您需要重新整理瀏覽器視窗並重新登入。

帶有系統配置備份副本的壓縮檔案可以包含機密資訊，例如密碼和隱私金鑰。Kaspersky Anti Targeted Attack Platform 的管理員必須自行確保此資料的儲存安全。

重新啟動 Sandbox 伺服器

重新啟動 Sandbox 伺服器：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。
2. 在**電源**設定群組中，點擊**重新啟動**按鈕。
   這將開啟 Sandbox 伺服器重新啟動確認視窗。
3. 點擊**是**。

Sandbox 伺服器將重新啟動。幾分鐘後，您將可以登入系統。

關閉 Sandbox 伺服器電源

關閉 Sandbox 伺服器電源：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。
2. 在**電源**設定群組中，點擊**關閉電源**按鈕。
   這將開啟 Sandbox 伺服器關閉確認視窗。
3. 點擊**是**。

Sandbox 伺服器電源關閉。

變更 Sandbox 管理員帳戶密碼

變更 Sandbox 管理員帳戶密碼：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。
2. **變更密碼**設定群組將顯示您在 Sandbox 安裝期間設定的 Sandbox 管理員帳戶名稱以及修改密碼的欄位。
3. 在**目前密碼**欄位中，輸入 Sandbox 管理員帳戶的目前密碼。
4. 在**新密碼**欄位中，輸入 Sandbox 管理員帳戶的新密碼。
5. 在**確認密碼**欄位中，再次輸入 Sandbox 管理員帳戶的新密碼。
6. 點擊**變更密碼**。
   Sandbox 管理員帳戶密碼將會被變更。

對於管理員：應用程式 Web 介面使用入門

本節的目標受眾是安裝和管理 Kaspersky Anti Targeted Attack Platform 以及以分佈式解決方案和多租戶模式管理 PCN 和 SCN 伺服器和租戶的人員。

Kaspersky Anti Targeted Attack Platform 介面

該應用程式透過 Web 介面進行管理。應用程式 Web 介面的各個部分因使用者的角色不同而有所不同：管理員或高級安全官（**資深安全員**、**安全官**、**安全稽核員**）。

應用程式 Web 介面視窗包含如下內容：

- 應用程式 Web 介面視窗左側和下側的部分。
- 在應用程式 Web 介面視窗上部用於應用程式某些部分的頁簽。
- 應用程式 Web 介面視窗下側的工作區。

應用程式 Web 介面視窗的部分

管理員角色的應用程式 Web 介面包含以下幾個部分：

- **控制板**。包含 Kaspersky Anti Targeted Attack Platform 監控資料。
- **操作模式**。包含有關 PCN 和 SCN 伺服器以及分散式解決方案和多組織用戶模式中租用戶的資訊。
- **資產**。包含具有 Kaspersky Endpoint Agent 元件的線上電腦及其設定的資訊。
- **日誌**：**使用者活動**、**應用程式訊息**、**稽核**。包含有關應用程式效能的資訊以及Web 介面中使用者活動的稽核記錄。
- **設定**。包含具有 Central Node 元件的伺服器的設定。
- **Sensor 伺服器**。包含有關已連線的 Sensor 元件及其設定的資訊。
- **Sandbox 伺服器**。包含有關 Central Node 元件與 Sandbox 元件的連線的資訊。
- **外部系統**。包含有關應用程式與郵件感應器整合的資訊。
- **伺服器配置**。包含有關應用程式的尺寸參數的資訊。

應用程式 Web 介面視窗的工作區

工作區顯示了您選擇在應用程式 Web 介面視窗的各個部分和頁簽上檢視的資訊。它還包含了可用於配置資訊顯示方式的控制元素。

具有**安全稽核員**角色的使用者還可以檢視應用程式 Web 介面的這些部分。

監控應用程式的效能

您可以使用應用程式 Web 介面視窗的**控制板**部分中的小工具來監控應用程式運作。您可以新增、刪除和移動小工具，配置小工具的顯示比例，以及選擇資料顯示時段。

關於小工具和佈局

您可以使用小工具來監控應用程式運作。

*佈局*是**控制板**區段中應用程式 Web 介面視窗工作區的外觀。您可以新增、刪除和移動佈局中的小工具。

應用程式中有以下小工具：

- **管理**：
  - **Sandbox 處理時間**。顯示 Sandbox 掃描物件的平均時間。
  - **已處理**。顯示從 Sensor 和 Endpoint Agent 到 Central Node 的流量的處理狀態。
  - **佇列**。顯示有關應用程式模組和元件要掃描的物件的數量資訊。

  如果您使用分散式解決方案和多組織用戶模式，此區段會顯示您所選租用戶和伺服器的相關資訊。
- **NDR**：
  - **自訂小部件**。具有任意靜態內容的小工具。例如，您可以使用自訂小工具，在**控制板**區段中以邏輯方式分隔小工具群組。
  - **流量**。傳入流量的速率。該小工具可以顯示已安裝應用程式元件的所有節點的所有監控點的資訊，也可以顯示選定節點的監控點的資訊，或顯示單個監控點的資訊。
  - **CPU 使用率**。安裝了應用程式元件的選定節點上的 CPU 負載。
  - **記憶體使用情況**。安裝了應用程式元件的選定節點上正在使用的實體 RAM 數量。

- **NDR 健康**。有關應用程式效能目前狀態的資訊。此小工具可以顯示以下值：
  - **正常**—沒有關於效能問題的訊息，或所有效能問題已解決。
  - **非嚴重故障**—報告了非嚴重故障。該值會一直顯示，直到效能問題解決為止。
  - **操作中斷**—報告了應用程式中斷。該值會一直顯示，直到效能問題解決為止。
  - **維護模式**—應用程式正在維護模式下執行。
- **儲存**—有關安裝了應用程式元件的選定節點上的本機檔案系統中的磁碟機的資訊。在此小工具中，您可以選擇顯示以下資訊：
  - **磁碟使用情況**—處理資料讀取/寫入作業所花費的時間百分比。
  - **磁碟佔用**—磁碟空間已滿。
  - **從磁碟讀取**—從磁碟讀取資料的速率。
  - **寫入磁碟**—將資料寫入磁碟的速率。
- **流量處理延遲**。處理流量時的目前延遲，從流量到達節點的監控點開始計算。顯示所有啟用的監控點中的最大延遲。此小工具可以顯示已安裝應用程式元件的所有節點的所有監控點的資訊，以及選定節點的監控點的資訊。
- **防護功能狀態**。有關應用程式中防護功能目前狀態的一般資訊。此小工具可以顯示以下值：
  - **全部啟用**—所有用於持續使用的技術和方法都已啟用，所有建立的監控點都已啟用。
  - **並非全部啟用**—某些防護功能已停用或在學習模式下啟用，或並非所有監控點都啟用。
- **執行時間**。Kaspersky Anti Targeted Attack Platform 的運行時間。在此小工具中，您可以選擇顯示以下資訊：
  - 有效運作時間 — 自最近一次啟動到目前時刻，應用程式正常運作（無故障）的持續時間。
  - 總運行時間 — 從應用程式首次啟動到目前時刻的時間。包括應用程式正常運作期間和故障期間。
  - 自應用程式首次啟動以來 — 從應用程式首次啟動到目前時刻經過的總時間。包括正常運作期、故障期和無法運作期。

根據傳入的資訊，小工具採用各種方式來吸引註意力。例如，如果資訊需要注意（特別是，當硬體資源上的負載接近臨界負載時），包含有關應用程式和硬體資源資訊的小工具可以自動改變顏色。

小工具僅顯示動態變化的基本資訊。如果您需要檢視詳細資訊，可以從**控制板**部分導航到應用程式 Web 介面的其他部分。您可以透過點擊小工具來導航 Web 介面。

> 為了在 NDR 小工具中顯示正確的資訊，您必須配置 Central Node 和 Sensor 元件之間的日期和時間同步。

在“儀表板”部分選擇要管理的租戶和伺服器

如果您使用的是分散式解決方案和多組織用戶模式，在使用**控制板**部分之前，您必須選擇要檢視其資料的租用戶和伺服器。NDR 功能的小工具將顯示目前節點或在小工具設定中選擇的節點的資訊。

*要選擇要在“**控制板**”部分的小工具中顯示其資料的租用戶和伺服器：*

1. 在應用程式 Web 介面視窗的右上方，點擊伺服器名稱旁的箭頭。
2. 在下拉清單中，從清單中選擇租戶和伺服器。

   所選伺服器的資料將予以顯示。如果要選擇不同的租戶和伺服器，請重複選擇租戶和伺服器的步驟。

新增小工具到目前佈局

若要新增小工具到目前佈局：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 點擊**小部件**。
5. 在開啟的**管理小部件**視窗中：
   - 如果您想新增**Sandbox 處理時間**小工具，請開啟該小工具名稱旁的切換開關。
   - 如果您想要新增不同的小工具，請點擊該小工具名稱旁的 + 。
6. 關閉**管理小部件**視窗並點擊**套用**。

   所選小工具將被新增到目前佈局。

在目前佈局中移動小工具

若要在目前佈局中移動小工具：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 在佈局中選擇要移動的小工具。

5. 點擊並按住小工具的上部可將小工具拖曳到佈局中的不同位置。

6. 點擊**套用**。

目前佈局已儲存。

變更 NDR 小工具中資訊的顯示

新增 NDR 小工具後，它將根據預設設定顯示資訊。如果需要，您可以編輯顯示設定。

若要編輯 NDR 小工具顯示設定：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。

2. 在視窗的上部，點擊 ☰ 按鈕。

3. 在下拉清單中，選擇**自訂**。

4. 在要配置的 NDR 小工具的右上角，點擊⚙按鈕。

   這將開啟顯示設定視窗。

5. 管理 NDR 小工具的顯示設定。

   根據所選的 NDR 小工具，視窗可能包含以下設定：

   - **變更名稱** – 如果勾選**變更名稱**核取方塊，您可以在**小工具名稱**欄位中為小工具定義任何名稱（不同於預設名稱）。自訂小工具中沒有**變更名稱**設定。

   - **小工具名稱** – 用於輸入與預設名稱不同的小工具名稱的欄位。

   - **編輯描述** – 如果勾選**編輯描述**核取方塊，您可以在**小工具描述**欄位中為小工具提供任何描述（不同於預設描述）。自訂小工具中缺少**編輯描述**設定。

   - **小工具描述** – 用於輸入與預設名稱不同的小工具名稱的欄位。

   - **重新整理週期** – 顯示的資訊更新的時間（以秒為單位）。

   - **顯示** – 定義顯示資料的類型（適用於可讓您選擇要顯示哪些資料的小工具）。

   - **資料來源** – 安裝了應用程式元件，且小工具顯示其資訊的主機。如果選取**整個應用程式**，小工具將顯示來自所有節點的資料。

   - **根據狀態變更顏色** – 如果勾選此核取方塊，小工具的背景顏色將根據傳入資料的嚴重程度自動變更。關鍵（最大）重要等級以紅色背景表示。如果清除此核取方塊，則背景顏色已停用。

   - **定義的背景** – 定義自訂小工具的背景顏色。您可以選擇與其中一個嚴重等級（**資訊**、**警告**或**嚴重**）相對應的背景顏色，或選取**中性**以停用背景著色。

6. 點擊**套用**。

從目前佈局移除小工具

若要從目前佈局移除小工具：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 點擊要從目前佈局移除的小工具右上角的 × 圖示。
   小工具被從應用程式 Web 介面視窗的工作區移除。
5. 點擊**套用**。

小工具被從目前佈局移除。

儲存佈局為 PDF

佈局中的 NDR 小工具未儲存至 PDF。

若要儲存佈局為 PDF：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**儲存為 PDF**。
   這將開啟**另存為 PDF**視窗。
4. 在視窗下部的**佈局：**下拉清單中，選擇頁面方向。
5. 點擊**下載**。
   PDF 格式的佈局會儲存到您的電腦硬碟上的瀏覽器下載資料夾。
6. 點擊**關閉**。

配置小工具中的資料顯示週期

您可以設定在小工具中顯示資料的以下時段：

- **天**。
- **周**。
- **月份**。

對於 NDR 小工具，您可以使用以下時間段：

- **1 小時**
- **12 小時**
- **24 小時**
- **7 天**

您可以為每個單獨的 NDR 小工具配置一個資料顯示週期。

變更小工具中資訊的顯示

要配置小工具中一天的資料顯示（從早上 00:00 到晚上 11:59）：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在應用程式 Web 介面視窗右上角的資料顯示時段下拉清單中，選擇**天**。
3. 在**天**時段名稱右側的日曆中，選擇要在小工具中顯示資料的日期。

   控制板頁面上的所有小工具都會顯示選定時段的資料。

要在小工具上配置一週（週一到週日）的資料顯示：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在應用程式 Web 介面視窗右上角的資料顯示時段下拉清單中，選擇**周**。
3. 在**周**時段名稱右側的行事曆中，選擇要在小工具上顯示資料的週。

   控制板頁面上的所有小工具都會顯示選定時段的資料。

若要在小工具中顯示一個月（日曆月）的資料顯示：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在應用程式 Web 介面視窗右上角的資料顯示時段下拉清單中，選擇**月份**。
3. 在**月份**時段名稱右側的行事曆中，選擇要在小工具中顯示資料的月份。

   控制板頁面上的所有小工具都會顯示選定時段的資料。

變更小工具中資訊的顯示

若要配置 NDR 小工具中資訊的顯示：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在您要設定的 NDR 小工具的右上角，點擊代表您需要的時間間隔的按鈕。

   NDR 小工具顯示選定時間段的資訊。

監控傳入資料的接收與處理

在**已處理**小工具中，您可以存取從 Sensor 和 Endpoint Agent 到 Central Node 的資料的處理狀態，並追蹤資料處理錯誤。

若要選擇為其評估傳入資料的元件（Sensor 或 Endpoint Agent），請使用**已處理**小工具名稱右側的下拉清單。

您可以在元件名稱（Sensor 或Endpoint Agent）右側的下拉清單中選擇資料顯示類型：

- **目前負荷**—最近 5 分鐘。
- **所選期間**。在這種情況下，您也可以設定小工具中的資料顯示時段。

每個小工具的左側部分顯示小工具本身所使用的顏色的圖例。

如果選擇**目前負荷**資料顯示類型，那麼在過去 5 分鐘內的平均資料處理速率將顯示在按鍵的右側。

例如：
選擇了 **(SPAN)** 或 **(ICAP)** Sensor 類型和**目前負荷**資料顯示類型的**已處理**小工具顯示特定時間段內從 Sensor 到 Central Node 的 SPAN 和 ICAP 流量的資料處理速率。
將顯示以下資訊：

- **流量**—傳入 Central Node 伺服器的流量速率，以綠色表示 (Mbps)。

  如果流量速率低於 1 Mbps，則小工具上不會顯示有關它的資訊。

- **檔案**—檔案處理速率以灰色表示（每秒物件數）。
- **URL** —URL 處理率，以藍色表示（每秒物件數）。
- **未處理：**—由垂直紅線表示的未處理物件的數量。
  將滑鼠遊標移到小工具上時，您會看到一個彈出視窗，上面顯示了特定時段的資料處理速率。
  選擇了**(SMTP)** Sensor 類型和**目前負荷**資料顯示類型的**已處理**小工具顯示特定時間內從郵件感應器到 Central Node 伺服器的郵件流量的 SPAN 和 ICAP 流量資料處理速率。
  將顯示以下資料：
- **流量**—傳入具有 Sensor 元件的伺服器的流量速率，以綠色表示（每秒訊息數）。
- **檔案**—檔案處理速率以灰色表示（每秒物件數）。
- **URL** —URL 處理率，以藍色表示（每秒物件數）。
- **未處理：**—由垂直紅線表示的未處理物件的數量。
  將滑鼠遊標移到小工具上時，您會看到一個彈出視窗，上面顯示了特定時段的資料處理速率。
  已處理小工具選擇了**(LOAD) Endpoint Agent** Sensor 類型和**目前負荷**資料顯示類型，並顯示特定時間段內從 Endpoint Agent 元件到具有 Central Node 元件的伺服器的事件處理速率（每秒事件數）。
  將滑鼠遊標移到小工具上時，您會看到一個彈出視窗，上面顯示了特定時段的資料處理速率。

如果選擇了**所選期間**資料顯示類型，那麼在圖例的右側，您將看到至 Central Node 伺服器的傳入流量平均速率以及在選定時段內處理的物件數量。

例如：
選擇了 **(SPAN)** 或 **(ICAP)** Sensor、**所選期間**資料顯示類型以及**月份**資料顯示時段的**已處理**小工具顯示傳入 Central Node 伺服器的 SPAN 和 ICAP 流量速率，以及選定月份內從郵件流量中提取的檔案和 URL 數量。
將顯示以下資訊：

- **平均流量**—傳入具有 Central Node 元件的伺服器的流量速率，以綠色表示（每秒物件數）。
- **檔案**—提取的檔案數量，以灰色表示。
- **URL** — 提取的 URL 數量，以藍色表示。
- **未處理：**—由垂直紅線表示的未處理物件的數量。
  當您將滑鼠停留在小工具上時，會顯示一個彈出視窗，其中顯示傳入 Central Node 的流量速率和特定時間內處理的物件數量。
  選擇了**(SMTP)** Sensor、**所選期間**資料顯示類型和**月份**資料顯示時段的**已處理**小工具顯示從郵件伺服器到 Central Node 的郵件流量的資料處理速率，以及選定月份內從郵件流量中提取的檔案和 URL 的數量。
  將顯示以下資訊：
- **平均流量** — 到達 Central Node 伺服器的流量速率，以綠色表示（物件/秒）。
- **檔案**—提取的檔案數量，以灰色表示。
- **URL** — 提取的 URL 數量，以藍色表示。
- **未處理：**—由垂直紅線表示的未處理物件的數量。
  當您將滑鼠停留在小工具上時，會顯示一個彈出視窗，其中顯示傳入 Central Node 的流量速率和特定時間內處理的物件數量。

選擇了**(LOAD) Endpoint Agent** Sensor 類型、**所選期間**資料顯示類型和**月份**資料顯示時段的**已處理**小工具顯示所選月份內從 Endpoint Agent 主機傳入到 Central Node 伺服器的事件數。

將滑鼠遊標移到小工具上時，您會看到一個彈出視窗，上面顯示了特定時段的事件數。

監控由應用程式模組和元件對資料進行處理的佇列

您可以使用**佇列**小工具來評估YARA和AM Engine應用程式模組以及 Sandbox 元件的資料處理狀態，並監控未處理的資料量。

佇列中的資料傳輸以訊息數來衡量。

您可以在**佇列**小工具名稱右側的下拉清單中選擇資料顯示類型：

- **目前負荷**—最近 5 分鐘。
- **所選期間**。在這種情況下，您也可以設定小工具上的資料顯示時段。

小工具的左側部分顯示小工具中使用的顏色的圖例。

佇列小工具顯示了以下資料：

- 應用程式模組和元件處理的**訊息數量**和**資料量**：
  - **YARA**—藍色。
  - **Sandbox**—紫色。
  - **AM 引擎**—綠色。
- **未處理的** – 由垂直紅線指示的未處理資料量。

將滑鼠遊標移到小工具上時，會看到一個彈出視窗，其中顯示 **YARA** 和 **AM 引擎**應用程式模組及 **Sandbox 元件**的資料處理狀態，以及特定時段內的未處理資料量。

監控 Sandbox 元件對資料的處理

Sandbox 處理時間小工具顯示所選期間從資料傳送到一個或多個 Sandbox 元件伺服器（包括傳送先前在佇列中花費的時間）到 Sandbox 處理結果顯示在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中所經過的平均時間。

例如：
如果**月份**配置為小工具中資料顯示的周期，則**Sandbox 處理時間**小工具顯示當月每一天的橘色條。
將滑鼠遊標移到每個列上時，您會看到一個彈出視窗，顯示了在選取天內從資料傳送到一個或多個具有 Sandbox 元件的伺服器的時刻開始，直到 Sandbox 元件的資料處理結果顯示在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中的平均時間。

透過增加具有 Sandbox 元件的伺服器數量以及在這些伺服器之間分配要處理的資料，可以提高 Sandbox 元件處理資料的速率以及 Sandbox 元件的吞吐量。

檢視應用程式模組和元件的工作狀況

如果應用程式的模組或元件遇到建議管理員檢視的錯誤，則會在應用程式 Web 介面的**控制板**區段上半部顯示黃色警告框。

具有“**管理員**”或“**安全稽核員**”角色的使用者可以存取有關使用者目前管理之 Central Node、PCN 或 SCN 伺服器的工作狀況資訊。

具有“**資深安全員**”、“**安全官**”或“**安全稽核員**”角色的使用者可以存取下列工作狀況資訊：

- 如果您使用的是獨立的 Central Node 伺服器，使用者可以存取有關使用者目前管理的 Central Node 伺服器的工作狀況的資訊。
- 如果您使用分散式解決方案和多組織用戶模式，且使用者正在管理 SCN 伺服器，則使用者可以存取該 SCN 伺服器針對使用者有權存取其資料之租用戶的工作狀況資訊。
- 如果您使用分散式解決方案和多組織用戶模式，且使用者正在管理 PCN 伺服器，則使用者可以存取該 PCN 伺服器和所有連線到該伺服器的 SCN 伺服器針對使用者有權存取其資料之租用戶的工作狀況資訊。

若要詳細了解應用程式模組及元件的工作情況，

點擊**檢視詳情**開啟**系統健康**視窗。

在**系統健康**視窗中，根據應用程式模組和元件的工作狀況會顯示以下圖示之一：

- OK 如果應用程式的模組和元件正常運作。
- 如果發現建議管理員注意的問題，則會顯示帶有問題數量的圖示（例如，1）。在這種情況下，詳細的問題資訊會顯示在**系統健康**視窗的右側。

系統健康視窗包含以下部分：

- **元件健康**包含應用程式執行所在之所有伺服器上的應用程式模組和元件運作狀態、隔離區以及資料庫更新資訊。

  例如：
  如果一個或多個應用程式元件的資料庫在 24 小時內未更新，則會在安裝應用程式模組和元件的伺服器名稱旁邊顯示 ! 圖示。
  要解決該問題，請確保可以存取更新伺服器。如果您使用代理伺服器連線到更新伺服器，請確保代理伺服器沒有與 Kaspersky Anti Targeted Attack Platform 伺服器連線相關的錯誤。

- **已處理**—傳入資料接收與處理狀態。狀態根據以下條件產生：
  - 從具有 Sensor 元件的伺服器、具有郵件感應器的伺服器或虛擬機、具有 Endpoint Agent 元件的主機接收資料的狀態。
  - 有關超出物件在佇列中等待應用程式模組和元件掃描的最長允許時間的資訊。
- **與伺服器的連線**—PCN 伺服器與已連線的 SCN 伺服器之間的連線狀態（如果您使用分佈式解決方案和多組織用戶模式，則會顯示）。

如果偵測到應用程式模組或元件的效能問題，您無法自行解決這些問題，請聯絡卡巴斯基技術支援。

管理 Central Node 或 Sensor 伺服器資訊

有關具有 Central Node 或 Sensor 元件的伺服器的資訊顯示在應用程式 Web 介面視窗的“**Sensor 伺服器**”區域。

此部分顯示元件的卡片（左側）和在這些元件上偵測到的網路介面卡（每個元件的右側）。

Sensor 元件卡片上方是該 Sensor 所連線的 Central Node 元件卡片。如果 Central Node 元件部署了嵌入式 Sensor，則該 Sensor 元件的名稱將在卡片上顯示為嵌入式 Sensor。

您可以檢視元件卡和網路介面卡。

檢視有關 Central Node 或 Sensor 伺服器的資訊

若要檢視有關 Central Node 或 Sensor 元件的資訊：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。

Central Node 和 Sensor 元件的**“設定”**頁簽顯示以下資訊：

- “**狀態**”是透過圖示和文字描述指示的元件的目前狀態。
- **節點類型**表示應用程式元件：**Server**（Central Node 元件）**或 Sensor**（Sensor 元件）。
- **應用程式目前使用的磁碟空間**是應用程式檔案所佔用的磁碟空間。包括已安裝的檔案和應用程式在運行過程中建立的檔案。
- **應用程式可使用的最大磁碟空間**就是應用程式檔案可佔用的磁碟空間。包括已安裝的檔案和資料儲存規則中配置的所有空間限制的總和。該值不得超過可用磁碟空間量。
- “**磁碟佔用**”是所有檔案使用的磁碟空間。包括應用程式檔案、作業系統檔案和其他應用程式的檔案。此空間是根據包含元件檔案系統中 /var 目錄的磁碟來計算的。
- “**可用磁碟空間**”是未被檔案使用的磁碟空間。此空間是根據包含元件檔案系統中 /var 目錄的磁碟來計算的。
- “**總磁碟空間**”是包含元件檔案系統中 /var 目錄的磁碟機上的磁碟空間總量。
- “**BPF 篩選**”指示是否啟用或停用使用基於網路封包中的位址參數的 Berkeley Packet Filter (BPF) 技術進行篩選。
- **流量傾印檔案的外部儲存**指示外部儲存的連線狀態。可能顯示以下狀態：**已連線**、**未連線**。
- “**保留規則**”指示應用程式資料的大小、項目數量和儲存期限的目前值和最大值。

對於 Sensor 元件，除了“**設定**”頁簽之外，還會顯示“**外部儲存**”、“**其他**”、“**ICAP 整合**”、“**POP3 整合**”和“**SMTP 整合**”頁簽。

- “**外部儲存**”頁簽顯示有關映像 SPAN 流量的外部儲存配置的資訊。
- 在**其他**頁簽中，顯示以下資訊：
  - 掃描檔案的最大大小是元件目前能夠掃描的檔案大小的限制。
  - 傾印 HTTP 主體指示是否啟用或停用 HTTP 主體內容傾印。
- “**ICAP 整合**”頁簽顯示透過 ICAP 與代理伺服器整合的設定。

  Host欄位顯示“icap://<Sensor 連線到的 Central Node 伺服器的 IP 位址>:1344/av/<respmod or reqmod>”格式的回應修改(RESPMOD)和請求修改(REQMOD)服務的 URL。

  若要設定與 Kaspersky Anti Targeted Attack Platform 的整合，請複製相關的 URL，將Central Node 伺服器的 IP 位址取代為您要設定ICAP 整合的 Sensor 伺服器的 IP 位址，然後在您組織的代理伺服器的設定中指定產生的 URL。
- “**POP3 整合**”頁簽顯示POP3 郵件伺服器整合設定。
- “**SMTP 整合**”頁簽顯示 SMTP 郵件伺服器整合設定。

檢視網路介面資訊

應用程式 Web 介面的**Sensor 伺服器**區段中的網路介面卡顯示以下資訊：

- 網路介面名稱
- 網路介面的 MAC 位址
- 網路介面的 IP 位址
- 網路介面頻寬
- 閃爍。此連結可讓您識別與網路介面關聯的乙太網路連接埠

如果網路介面已經新增了監控點，則網路介面的卡片中將顯示該監控點的下列資訊：

- 監控點名稱。
- **技術模式**是技術繼承功能的狀態。它可以是**已啟用**或者**已停用**。

您可以檢視網路介面詳細資訊。

若要檢視網路介面詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關網路介面的卡。

   這將開啟一個視窗，其中包含有關網路介面的資訊。

網路介面卡顯示以下資訊：

- **網路介面**是作業系統中網路介面的名稱。
- **連線**是表示網路線已連線到網路介面的乙太網路連接埠的圖示：
  - — 網路線已連線。
  - — 網路已斷開連線。
    啟用乙太網路連接埠指示模式時，圖示閃爍。
  - **MAC 位址**是網路介面的 MAC 位址。
  - **IP 位址**是網路介面的 IP 位址。
    如果網路介面上發現多個 IP 位址，則詳細資料區域中最多顯示 16 個 IP 位址。

如果網路介面上已經新增了監控點，則網路介面的卡片中會顯示以下資訊：

- **狀態**是監控點目前的狀態，以圖示和文字描述表示：
  - *正常*。監測點可用。
  - *切換*。監控點運作模式正在改變。
  - *錯誤*。切換監控點操作模式時偵測到錯誤。
- **連線**是表示網路線已連線到網路介面的乙太網路連接埠的圖示：
  - — 網路線已連線。
  - — 網路已斷開連線。

  啟用乙太網路連接埠指示模式時，圖示閃爍。
- **網路介面**是作業系統中網路介面的名稱。
- **模式**是監控點目前的模式：
  - *已啟用*。
  - *已停用*。
- 在**設定**索引標籤上：
  - **技術繼承**指示是否為伺服器啟用或停用技術繼承。
  - **MAC 位址**是網路介面的 MAC 位址。
  - **IP 位址**是網路介面的 IP 位址。

識別與網路介面關聯的乙太網路連接埠

安裝應用程式元件的伺服器可以有多個乙太網路連接埠用於連線本機網路。您可以使用該應用程式為網路介面啟用閃爍模式，並找出與該介面關聯的乙太網路連接埠。在閃爍模式下，乙太網路連接埠旁的 LED 會閃爍15 秒。

如果網路介面不支援 LED 指示（例如，如果乙太網路連接埠沒有配備 LED，或網路介面是邏輯綁定介面），則嘗試啟用閃爍模式時會顯示錯誤。

若要識別與網路介面關聯的乙太網路連接埠：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 在相關網路介面的卡片上，點擊**閃爍**按鈕。

   如果網路介面支援 LED 指示，網路線連線圖示會在網路介面卡上開始閃爍。同時，電腦對應網路介面卡上乙太網路連接埠旁的 LED 開始閃爍。

當網路介面處於閃爍模式時，您無法為同一伺服器上的任何其他網路介面開啟閃爍模式。

使用應用程式 Web 介面管理 Central Node、PCN 或 SCN 伺服器

您可以使用應用程式 Web 介面利用安裝有 Central Node 元件的伺服器執行以下操作：

- 變更伺服器的 FQDN 名稱
- 配置伺服器上的日期和時間。
- 關閉並重新啟動伺服器。
- 管理伺服器的憑證
- 管理流量儲存設定
- 管理儲存流量傾印檔案的設定
- 管理伺服器的網路設定

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

配置伺服器上的日期和時間

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要配置伺服器上的日期和時間。

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**日期和時間**子部分。
2. 在**時區**下拉清單中，選擇 Central Node 伺服器實體位置的時區。
3. 在**NTP 伺服器**下，指定**最大資料包傳輸時間**設定的值，限制從 Central Node 伺服器向 NTP 伺服器傳送封包所需的最大時間。

   預設設定為 5 秒。

   > 您可以在 Central Node 的管理員選單中啟用或停用與 NTP 伺服器的同步。

4. 在**NTP 伺服器**部分：
   - 如果您要新增一個新的 NTP 伺服器：
     a. 點擊**新增**。
     b. 在開啟的欄位中，輸入 NTP 伺服器的 IP 位址或網域名稱。
     c. 點擊欄位右側的✓按鈕。
   - 如果您想要編輯 NTP 伺服器的 IP 位址或網域名稱，請點擊包含伺服器的行中的✎按鈕。
   - 如果您想要刪除一個 NTP 伺服器，請點擊包含伺服器的行中的🗑按鈕。
5. 點擊**套用**。

將配置伺服器上的日期和時間。

產生或上傳伺服器的 TLS 憑證

如果您已在使用伺服器 TLS 憑證，則產生或上傳新憑證會導致目前使用的憑證被刪除並替換為新憑證。

在使用舊憑證的所有地方都必須輸入新憑證的資料。

如果您替代 TLS 憑證，您將需要：

- 重新授權 Central Node 上的郵件 Sensor (KSMG、KLMS)。
- 重新配置 Central Node、PCN、SCN 與 Sandbox 的連線。
- 重新配置從 Endpoint Agent 到 Sensor 的流量轉發以及與 Endpoint Agent 的受信任連線。

請確保刪除所有 Endpoint Agent 主機隔離規則。與隔離主機的連線將丟失，您將無法管理它們。

您可以在 Central Node 伺服器的 Web 介面中產生新憑證或上傳您獨立建立的憑證。

為了遵守安全法規和標準，您必須將應用程式中預設安裝的 TLS 憑證替換為您自己的 TLS 憑證。

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要為 Central Node 伺服器產生 TLS 憑證：

1. 登入 Kaspersky Anti Targeted Attack Platform Web 介面時，請使用管理員憑據。
2. 在應用程式 Web 介面視窗中，選擇**設定**區段、**憑證**子區段。
3. 在**伺服器憑證**部分，點擊**產生**。
   這將開啟操作確認視窗。
4. 點擊**是**。

Kaspersky Anti Targeted Attack Platform 產生新的 TLS 憑證。頁面會自動重新整理。

與郵件感應器、Sandbox 元件和 Endpoint Agent 元件的通訊將中斷，直到重新授權。

您可以選擇自行準備 TLS 憑證並使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳。

準備上傳的 TLS 憑證檔案必須符合以下要求：

- 檔案必須包含憑證本身和用於連線的私人加密金鑰。
- 檔案必須是 PEM 格式。

  該應用程式不支援其他格式的憑證。

  如果您準備了其他格式的憑證，則必須將其轉換為 PEM 格式。
- 私鑰長度必須為 2048 位元或更長。

要獲取準備 TLS 憑證進行匯入的更多詳細資訊，請參閱 Open SSL 檔案。

在要將憑證上傳到的 PCN 或 SCN 伺服器的 Web 介面中上傳TLS 憑證。

若要使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳獨立準備的 TLS 憑證：

1. 使用管理員憑據登入 Kaspersky Anti Targeted Attack Platform Web 介面。
2. 在應用程式 Web 介面視窗中，選擇**設定**區段、**憑證**子區段。
3. 在**伺服器憑證**區段中，點擊**上傳**。
   這將開啟檔案選擇視窗。
4. 選擇要下載的 TLS 憑證檔案，然後點擊**開啟**按鈕。
   這將關閉檔案選擇視窗。

TLS 憑證已新增至 Kaspersky Anti Targeted Attack Platform。

與郵件感應器、Sandbox 元件和 Endpoint Agent 元件的通訊將中斷，直到重新授權。

下載伺服器的 TLS 憑證

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要下載伺服器的 TLS 憑證：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**憑證**子部分。
2. 在**伺服器憑證**部分，點擊**下載**。

伺服器憑證檔案將會儲存在瀏覽器下載資料夾中。

伺服器的 FQDN 設定

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

若要設定伺服器的 FQDN：

1. 在程式 Web 介面視窗中，選擇**設定**部分的**網路設定**子部分。
2. 在**伺服器名稱 (FQDN)**欄位中，輸入伺服器的完整網域名稱。
   以 FQDN 格式指定伺服器名稱（例如：`host.domain.com` 或 `host.domain.subdomain.com`）。
3. 點擊**套用**。

將分配伺服器名稱。

配置 DNS 設定

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要配置 DNS：

1. 在程式 Web 介面視窗中，選擇**設定**部分的**網路設定**子部分。
2. 在**DNS 設定**組中，在**DNS 伺服器**欄位中輸入 DNS 伺服器的 IP 位址。
3. 點擊**套用**。

   這將配置 DNS 設定。

設定網路介面的設定

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

設定網路介面：

1. 在程式 Web 介面視窗中，選擇**設定**部分的**網路設定**子部分。
2. 選擇要配置其設定的網路介面。

   這將開啟**編輯網路接口**視窗。
3. 在**狀態**設定群組中，選擇以下選項之一：
   - **已停用**。
   - **已啟用，使用 DHCP 伺服器**，如果您希望將從 DHCP 伺服器接收的設定用於網路介面。
   - **已啟用，手動配置**，如果您希望使用手動設定的網路介面。
4. 如果您選擇了**已啟用，手動配置**，指定以下參數的值：
   a. 在**IP**欄位中，輸入網路介面的 IP 位址。
   b. 在**子網路遮罩**欄位中，指定網路介面的子網路遮罩。
   c. 在**閘道**文字方塊中，輸入閘道的 IP 位址。
5. 點擊**儲存**。

   將配置網路介面的設定。

設定預設網路路由

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

設定預設網路路由：

1. 在程式 Web 介面視窗中，選擇**設定**部分的**網路設定**子部分。
2. 在**網路路由**設定群組的**網路接口**下拉式清單中，選擇要為其設定網路路由的網路介面。
3. 在**閘道**文字方塊中，輸入閘道的 IP 位址。
4. 點擊**套用**。

   將配置預設網路路由。

設定代理伺服器連線設定

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要配置代理伺服器連線：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**網路設定**子部分。
2. 在**代理伺服器**設定群組中，將切換開關設定為**已啟用**。
3. 在**主機**欄位中，指定代理伺服器的 URL 或 IP 位址。
4. 在**連接埠**欄位中，指定用於連線到代理伺服器的連接埠。
5. 在**使用者名稱**欄位中，指定用於在代理伺服器上進行身分驗證的使用者名稱。
6. 在**密碼**欄位中，指定用於在代理伺服器上進行身分驗證的密碼。
7. 連線到本機位址時，如果您不想使用代理伺服器，請選擇**略過本機位址的代理伺服器**核取方塊。
8. 點擊**套用**。

   將設定代理伺服器連線設定。

   如果在儲存設定時發生錯誤，請將**使用代理伺服器**切換開關設定為**已停用**，然後將其設定回**已啟用**，再點擊**套用**按鈕。

設定郵件伺服器連線

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

該應用程式可以傳送有關警示和系統性能的通知。為此，您必須配置用於傳送通知的伺服器的設定。

若要設定用於傳送通知的伺服器：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**區段和**通知**子區段。
2. 前往**郵件伺服器配置**索引標籤。
3. 在**主機**欄位中，指定郵件伺服器的 IP 位址。
4. 在**連接埠**欄位中，指定連線到郵件伺服器的連接埠。
5. 在**電子郵件寄件者**欄位中，指定用來傳送通知的電子郵件地址。
6. 如果您想要在郵件伺服器上啟用身分驗證，請選擇**使用郵件收件者的 SMTP 身分驗證**核取方塊。
7. 在**使用者名稱**欄位中，指定用於在傳送通知的伺服器上進行身分驗證的使用者名稱。
8. 在**密碼**欄位中，指定用於在傳送通知的伺服器上進行身分驗證的密碼。
9. 傳送通知時，如果您想要使用 TLS 加密，請選擇**使用 TLS 加密**核取方塊。
10. 如果您想要驗證郵件伺服器的憑證，請選擇**驗證 TLS 加密**核取方塊。

    憑證指紋欄位會顯示郵件伺服器憑證的指紋。

    如果未選擇**驗證 TLS 加密**核取方塊，應用程式會將郵件伺服器的任何憑證視為受信任的憑證。

11. 點擊**套用**。

將配置用於傳送通知的伺服器的設定。

管理流量節省設定

應用程式可以儲存註冊事件時收到的流量。在註冊啟用流量節省的事件時，流量將儲存在 Central Node 伺服器的資料庫中。應用程式還可以根據流量下載請求，使用臨時流量傾印檔案直接將流量儲存在伺服器資料庫中。

應用程式以區塊的形式儲存流量資料。如果某個流量區塊與多個事件相關聯（對於短時間內記錄的事件），則該流量區塊不會在資料庫中重複。

要管理在伺服器資料庫中儲存流量的設定：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Central Node 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 轉到“**一般**”索引標籤。
5. 在**事件的流量**下，在**最大流量**欄位中指定要儲存的最大流量。
   您可以選擇大小限制的計量單位：**MB**或**GB**。
   編輯值時，還需要考慮到所有大小限制的總和不得超過伺服器指定的最大儲存容量。
6. 點擊**儲存**按鈕。

流量節省設定已修改。

管理儲存流量傾印檔案的設定

該應用程式將透過監控點接收的流量儲存為流量傾印檔案。應用程式使用這些檔案來分析傳入流量。您也可以使用這些檔案在應用程式中執行以下操作：

- 管理網路互動圖時下載流量
- 下載網路工作階段流量
- 下載事件的流量（流量傾印檔案可讓您載入事件的流量，即使相關事件類型的流量儲存功能已停用）

流量傾印檔案儲存在具有 Sensor 元件的伺服器的內部儲存中。如果您使用具有嵌入式 Sensor 的 Central Node 元件，流量傾印檔案將儲存在 Central Node 伺服器的內部儲存空間中。

應用程式暫時儲存流量傾印檔案。當流量到達時，如果檔案的總大小接近儲存設定的限制，應用程式會自動從儲存中刪除最舊的流量傾印檔案。您可以配置在內部儲存中儲存流量的設定。

若要設定將流量傾印檔案儲存到內部儲存：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Central Node 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 轉到“**一般**”索引標籤。

5. 如有必要，在“**篩選儲存的流量**”部分，啟用篩選並輸入基於網路封包的位址設定使用 Berkeley Packet Filter (BPF) 技術的篩選表達式。

> 篩選可以透過丟棄與篩選器不匹配的網路封包來減少儲存的流量的大小。但是，如果您依賴篩選，請考慮篩選後的流量可能無法提供應用程式進行高品質流量分析所需的所有資料。您需要以這樣的方式設定篩選，以便應用程式分析流量所需的所有網路封包都儲存在流量傾印檔案中。

6. 在“**流量傾印檔案**”下，使用“**最大磁碟區**”設定來設定儲存的流量傾印檔案的大小限制。

   您可以選擇大小限制的計量單位：**MB**或**GB**。

   在編輯值時，還需要考慮接收的流量總量、接收速率以及所有大小限制的總和不得超過節點指定的最大儲存容量。

7. 點擊**儲存**。

已配置將流量傾印儲存到內部儲存。

管理 Sensor 元件

Sensor 元件從網路流量和郵件流量接收資料。

> 若要管理該元件，您需要將 KATA 或 KATA+NDR 產品授權金鑰新增至應用程式。如果未新增金鑰，則元件管理不可用。

您可以在同一伺服器或不同伺服器上安裝 Sensor 和 Central Node 元件。安裝在獨立伺服器上的 Sensor 元件必須連線到具有 Central Node 元件的伺服器。如果您使用分散式解決方案和多組織用戶模式，請依照下列步驟，連線您要連線該元件的 PCN 或 SCN 伺服器上的 Sensor 元件。

不支援在分佈式解決方案和多租戶模式下使用 PCN 對 Sensor 元件進行集中管理。Sensor 元件只能從連線元件的特定 Central Node 伺服器進行設定。

將 Sandbox 元件連線到 Central Node

新增 Sensor 元件時，會在 Central Node 上產生一個配置包，其中包含 Sensor 元件的憑證和設定資料。新增的元件使用 Sensor 元件的 Web 介面進行連線。此元件的 Web 介面可讓您上傳設定包並透過以下方式連線元件：

- 使用通訊封包。

  在這種情況下，設定包將儲存為憑證受密碼防護的檔案。這個檔案被稱為*通訊封包*。必須將通訊封包上傳至 Sensor 元件的 Web 介面。上傳通訊封包後，Sensor 元件會自動連線到建立通訊封包的 Central Node。

- 透過網路自動傳輸。

  在這種情況下，設定包會透過網路傳送到具有 Sensor 元件的伺服器的指定 IP 位址。Sensor 處理設定包，基於它產生憑證簽章請求(CSR)，並將此請求傳送至 Central Node 元件。收到 CSR 後，CSR 的指紋會以字元序列的形式顯示在 Kaspersky Anti Targeted Attack Platform 的 Web 介面上。相同的指紋同時顯示在 Sensor 元件的 Web 介面上。終止連線之前必須確保指紋相同。

如果 Central Node 和 Sensor 元件之間的連線是在受信任媒體之外建立的，為了防護連線免於流量攔截，您需要使用支援您所在國家/地區批准的加密演算法的外部加密資訊防護設施。如果元件透過受信任媒體連線，例如，可以阻止第三方存取的伺服器機架內的跳線，則無需使用外部加密資訊防護設施。

使用通訊封包連線 Sensor 元件

若要使用通訊封包連線 Sensor 元件：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。

2. 點擊“**新增 Sensor**”。

   這將開啟“**新增 Sensor**”視窗。

3. 在“**Sensor 名稱**”欄位中，輸入要連線的 Sensor 元件的名稱。

   與 Central Node 的連線建立後，帶有元件的 Web 介面頁面的瀏覽器頁簽的標題將顯示您在此步驟配置的名稱。

4. 在“**伺服器位址**”欄位中，輸入要連線 Sensor 元件的 Central Node 伺服器的 IP 位址。

   如果 Central Node 部署為叢集，則需要輸入叢集中**設定為從 SPAN 連接埠接收鏡像流量**的處理伺服器的 IP 位址。

   您可以在安裝元件時啟用接收鏡像流量。如果您在安裝階段停用了流量接收：

   若要開啟從 SPAN 連接埠接收映像流量：

   1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。

   2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任一工作伺服器的管理主控台。

   3. 執行以下指令：

      ```
      kata-enable-span
      ```

      將啟用從 SPAN 連接埠接收映像流量。

5. 在“**Sensor IP 位址**”欄位中，輸入要連線到 Central Node 元件的 Sensor 元件伺服器的 IP 位址。

6. 在“**通訊資料套件中的憑證加密**”部分中，設定您想要使用的憑證防護密碼。

   密碼必須符合以下要求：

   - 包含 8 到 256 個 ASCII 字元。

   - 包含一個或多個拉丁字母的大寫字母。

   - 包含一個或多個拉丁字母的小寫字母。

- 包含一個或多個數字。
- 不包含連續四個或更多相同的字元。

7. 點擊“**建立通訊資料套件**”。您的瀏覽器儲存了下載的檔案。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。
8. 將已儲存的通訊資料包檔案放置在任何允許存取 Sensor 伺服器的電腦上。
9. 在放置通訊資料包檔案的電腦上，啟動命令列解釋器。
10. 執行以下指令：

    ```
    ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 元件的伺服器的 IP 位址>
    ```

    如果執行指令後出現*輸入的 MAC 已損毀。ssh_dispatch_run_fatal: 連線至 <Sensor 伺服器的 IP 位址> 連接埠 22：訊息身分驗證碼不正確*錯誤，請執行以下指令：

    ```
    ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 元件的伺服器的 IP 位址> -o "MACs hmac-sha2-256"
    ```

11. 在瀏覽器的位址欄中輸入：https://localhost:9444。
12. 在 Sensor Web 介面頁面上，點擊“**選擇檔案**”。

    這將開啟用於選擇檔案的標準瀏覽器視窗。
13. 指定通訊封包的路徑。
14. 點擊“開啟檔案”按鈕。
15. 檔案上傳完成後，輸入您在本說明的第 6 步中設定的憑證密碼。

    Sensor 元件與 Central Node 元件連線，之後在 Sensor 和 Central Node 元件的 Web 介面中就會出現連線資訊。

透過網路自動新增和連線 Sensor 元件

若要透過網路自動連線 Sensor 元件：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊“**新增 Sensor**”。

    這將開啟“**新增 Sensor**”視窗。
3. 轉到“**透過網路自動**”索引標籤。
4. 在“**Sensor 名稱**”欄位中，輸入要連線的 Sensor 元件的名稱。

    與 Central Node 的連線建立後，帶有元件的 Web 介面頁面的瀏覽器頁簽的標題將顯示您在此步驟配置的名稱。
5. 在“**伺服器位址**”欄位中，輸入要連線 Sensor 元件的 Central Node 伺服器的 IP 位址。

    如果 Central Node 部署為叢集，則需要輸入叢集中**設定為從 SPAN 連接埠接收鏡像流量**的處理伺服器的 IP 位址。

    您可以在安裝元件時啟用接收鏡像流量。如果您在安裝階段停用了流量接收：

若要開啟從 SPAN 連接埠接收映像流量：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。
2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任一工作伺服器的管理主控台。
3. 執行以下指令：

   ```
   kata-enable-span
   ```

   將啟用從 SPAN 連接埠接收映像流量。

6. 在"**Sensor IP 位址**"欄位中，輸入要連線到 Central Node 元件的 Sensor 元件伺服器的 IP 位址。

   應用程式與安裝了 Sensor 元件的伺服器建立連線，且應用程式的 Web 介面上會顯示一個提示，要求您確認收到的憑證簽章要求的指紋。

7. 在任何允許存取 Sensor 伺服器的電腦上，啟動命令列解釋器。
8. 執行以下指令：

   ```
   ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 元件的伺服器的 IP 位址>
   ```

   如果執行指令後出現*輸入的 MAC 已損毀。ssh_dispatch_run_fatal: 連線至 <Sensor 伺服器的 IP 位址> 連接埠 22：訊息身分驗證碼不正確*錯誤，請執行以下指令：

   ```
   ssh -4 -L 9444:localhost:9444 admin@<具有 Sensor 元件的伺服器的 IP 位址> -o "MACs hmac-sha2-256"
   ```

9. 在瀏覽器的位址欄中輸入：https://localhost:9444。

   瀏覽器中顯示 Sensor 元件的 Web 介面。Web 介面顯示一則訊息，其中包含有關傳送至 Central Node 元件的憑證簽章要求的指紋的資訊。

10. 確保代表憑證請求指紋的字元序列在 Sensor 和 Central Node 元件的 Web 介面中相同。
11. 在應用程式 Web 介面上，點擊按鈕確認收到的憑證簽章要求的指紋。

Sensor 元件與 Central Node 元件連線，之後在 Sensor 和 Central Node 元件的 Web 介面中就會出現連線資訊。

刪除 Sensor 元件

您可以從應用程式中刪除該元件。刪除元件也會刪除為其設定之任何整合的設定，並停止資料的接收與處理，因此建議您先執行下列操作：

- 規劃停機維護時間。
- 停用外部系統端與 Sensor 的所有整合。
- 以任何方便的方式保留 Sensor 端與外部系統整合的設定。
- 以任何方便的方式保留外部系統端 Sensor 整合的設定。

如有必要，您可以將已刪除的元件重新連線到 Central Node。

要刪除元件：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊**刪除**。

元件已刪除。

編輯獨立於 Central Node 安裝的 Sensor 設定

如果您已選擇網路協定從 SPAN 連接埠取得鏡像流量，並在將獨立 Sensor 連接到 Central Node**之前**配置了其檔案儲存大小或流量擷取頻寬，並且希望在連線**後**變更這些設定，我們建議您在變更這些設定時遵循以下方案：

1. 斷開 Sensor 與 Central Node 的連線。
   斷開 Sensor 連線只需將其刪除即可。
2. 準備 Sensor 以變更設定。
3. 按照說明變更設定。
4. 將 Sensor連線到 Central Node。

如果在未做好充分準備的情況下變更上述一項或多項設定，則與 Central Node 分開安裝的 Sensor 可能會變得不穩定。在這種情況下，元件在其卡片中的狀態開始頻繁變更。您可以透過斷開 Sensor 與 Central Node 的連線，然後再重新連線來解決此問題。

準備編輯獨立於 Central Node 安裝的 Sensor 設定

如果您在將獨立 Sensor 連線到 Central Node **之前**，已在獨立 Sensor 上選擇網路協定以從 SPAN 連接埠取得鏡像流量、設定檔案儲存大小或流量擷取頻寬，且想要在連線**之後**變更這些設定，則需要遵循以下步驟。

以下所述的所有步驟都必須在使用 `sudo -i` 指令提升使用者權限後，在處於技術支援模式的伺服器上執行。

要準備 Sensor 以變更設定：

1. 登入 Sensor 伺服器的主控台並執行以下命令：
   ```
   kata-sensor-tool stop-sensor
   ```
2. 登入 Sensor 所連線的 Central Node 伺服器的管理主控台，並執行以下命令：
   ```
   kata-sensor-tool clear-core-cookies
   ```
3. 返回 Sensor 伺服器的管理主控台並執行以下命令：
   ```
   kata-sensor-tool start-sensor
   ```

Sensor 已準備好變更設定。現在您可以按照說明的步驟根據需要變更設定。

管理 Sensor 伺服器的憑證

本節介紹如何管理具有 Sensor 元件的伺服器的 TLS 憑證。

憑證可以在應用程式管理員功能表中進行管理。

在 Sensor 伺服器的管理員功能表中為 Sensor 伺服器產生 TLS 憑證

若要為具有 Sensor 元件的伺服器建立 TLS 憑證，請在 Sensor 伺服器的管理員功能表中執行下列操作：

1. 在管理員功能表的主視窗中，選擇**程式設定**。
2. 按下 **Enter**。
   這將開啟管理員功能表的下一個視窗。
3. 選擇**管理伺服器憑證**。
4. 按下 **Enter**。
   這將開啟**憑證管理**視窗。
5. 在視窗的下部，選擇**產生新的**。
6. 按下 **Enter**。
   這將開啟一個視窗，其中包含有關建立憑證的資訊。
7. 點擊**產生**。
   憑證建立開始。請等待此過程完成。

憑證已建立。先前安裝的憑證的資料被覆蓋。

在 Sensor 伺服器的管理員功能表中上傳您自己的 TLS 憑證

您可以準備自己的 TLS 憑證並使用 SCP 將其上傳到 Sensor 伺服器。要獲取透過 SCP 協定上傳檔案的方法的更多詳細資訊，請參閱您要上傳其 TLS 憑證的電腦上安裝的作業系統檔案。

準備上傳到伺服器的 TLS 憑證檔案必須符合以下要求：

- 檔案必須包含憑證本身和用於連線的私人加密金鑰。
- 檔案必須是 PEM 格式。
- 檔案名稱必須為 kata.pem。
- 私鑰長度必須為 2048 位元或更長。

要獲取準備 TLS 憑證進行匯入的更多詳細資訊，請參閱 Open SSL 檔案。

若要使用 SCP 將您自己的 TLS 憑證上傳到 Sensor 伺服器，請在電腦的 SCP 介面中執行以下操作（範例中使用 Linux）：

1. 執行以下命令：`scp kata.pem admin@<具有 Sensor 元件的伺服器的 IP 位址>`：
2. 在密碼提示處，輸入用於管理 Sensor 伺服器的管理員功能表的管理員密碼，此密碼是在安裝時設定的。

TLS 憑證被上傳到 Sensor 伺服器。

若要在 Sensor 伺服器上套用上傳的 TLS 憑證，請在 Sensor 伺服器的管理員功能表中執行下列操作：

1. 在管理員功能表的主視窗中，選擇**程式設定**。
2. 按下 **Enter**。
   這將開啟管理員功能表的下一個視窗。
3. 選擇**管理伺服器憑證**。
4. 按下 **Enter**。
   這將開啟**憑證管理**視窗。
5. 在視窗的下部，選擇**從檔案安裝**。
6. 按下 **Enter**。

將套用憑證。先前安裝的憑證的資料將被覆蓋。

將 Sensor 伺服器的 TLS 憑證下載到您的電腦

您可以將 TLS 憑證從 Sensor 伺服器下載到任何可以透過 SCP 協定連線到 Sensor 伺服器的電腦。要取得透過 SCP 協定上傳檔案的方法的更多詳細資訊，請參閱您要將 TLS 憑證下載到的電腦上安裝的作業系統檔案。

若要透過 SCP 協定從具有 Sensor 元件的伺服器下載TSL 憑證，請在用於處理 SCP 協定的電腦介面中執行下列操作（以 Linux 作業系統為例）：

1. 執行以下命令：`scp admin@<具有 Sensor 元件的伺服器的 IP 位址>:ssl/kata.crt.`
2. 在密碼提示處，輸入用於在具有 Sensor 元件的伺服器的管理員功能表中工作的管理員密碼，此密碼是在安裝時設定的。

TLS 憑證將從具有 Sensor 元件的伺服器下載到目前目錄。

變更伺服器名稱

要重新命名 Central Node 伺服器：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Sensor 元件的卡片。

   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 轉到“**一般**”索引標籤。
5. 在“**Sensor 名稱**”欄位中，輸入新名稱。

   此名稱必須是唯一的（不能與其他元件的名稱相同）並且最多可包含 100 個字元。您可以使用英文字母、數字、空格以及特殊字元：_ 和-（例如，Server_1）。名稱必須以空格以外的任何有效字元開始和結束。
6. 點擊**儲存**按鈕。

伺服器將被重命名。

管理監控點

Kaspersky Anti Targeted Attack Platform 使用監控點接收和處理映像 SPAN 流量。可以為 Central Node 和 Sensor 元件新增和刪除監控點。

每個監控點必須與一個網路介面相關聯，該介面接收來自某個網段的流量副本。若要新增監控點，可以使用符合下列條件的網路介面：

- 網路介面類型：乙太網路。
- MAC 位址：不是 00:00:00:00:00:00。
- 網路介面專門用於接收網路流量的副本，不用於其他目的（例如，連線已安裝應用程式元件的伺服器）。

監控點可以啟用或停用。您可以停用監控點以暫時停止監控網路介面上接收流量副本的網段。當需要還原監控時，重新啟用此監控點即可。

> 停用或刪除監控點後，應用程式可能會在一段時間內記錄涉及該監控點的事件。這是因為當 Central Node 元件負載較高時，處理傳入流量可能會出現延遲。

監控點詳情顯示在該監控點所關聯的網路介面的卡片中。若有必要，可以重新命名監控點。

新增監控點

為了在節點的網路介面上接收和處理來自網路的流量，需要在該網路介面上新增一個監控點。

若要新增監控點至網路介面：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 在相關網路介面的卡片中，點擊**新增監控點**連結。
   這將開啟新增監控點的視窗。
3. 在**監控點名稱**欄位中，輸入監控點的名稱。
   您可以使用拉丁字母的大寫和小寫字母、數字以及 _ 和 - 字元。
   監控點名稱必須符合以下要求：
   - 是唯一的（未分配給任何其他監測點）。
   - 包含 1 至 100 個字元。
4. 點擊**新增監控點**。

監控點被加入。

重新命名監控點

您可以重新命名與網路介面關聯的監控點。

> 監控點的新名稱反映在重新命名後記錄的事件中。先前記錄的事件保留監控點的舊名稱。

若要重新命名監控點：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關網路介面的卡。
3. 這將開啟一個視窗，其中包含有關網路介面的資訊。
4. 點擊“**編輯**”。
5. 在“**監控點名稱**”欄位中，輸入新名稱。
   您可以使用拉丁字母的大寫和小寫字母、數字以及 _ 和 - 字元。
   監控點名稱必須符合以下要求：
   - 是唯一的（未分配給任何其他監測點）。
   - 包含 1 至 100 個字元。
6. 點擊**儲存**。

監控點被重新命名。

啟用監控點

如果監控點被停用，應用程式將不會接收或處理到達其網路介面的流量。如果要還原接收和處理流量，則必須啟用監控點。

您可以為一個元件或所有元件單獨或一次啟用監控點。

只有具有管理員角色的使用者才能啟用監控點。

要啟用監控點：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 執行以下操作之一：
   - 如果要啟用單個監控點，在相關元件的卡片中，點擊“**啟用**”按鈕。如果監控點已停用，則此按鈕可用。
   - 若要啟用所有監控點，在相關元件的卡片中，點擊“**全部啟用**”按鈕。如果元件具有已停用監控點的網路介面，則該按鈕可用。
   - 如果要啟用所有元件的所有監控點，請點擊工具列中的“**在所有節點上啟用**”連結。
3. 等待變更應用程式。

   選定的監控點已啟用。

停用監控點

如果您想暫時停止接收和處理該監控點網路介面上的流量，您可以停用該監控點。

您可以針對所有元件單獨停用監控點，也可以同時停用所有監控點。

若要停用監控點：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 執行以下操作之一：
   - 如果要停用單個監控點，請在相關元件的卡片中點擊“**停用**”按鈕。監控點啟用後該按鈕可用。
   - 若想停用所有監控點，在相關元件的卡片上，點擊“**全部停用**”按鈕。如果元件具有已啟用監控點的網路介面，則該按鈕可用。
   - 如果您要停用所有元件的所有監控點，請點擊工具列中的“**在所有節點上停用**”連結。
3. 等待變更得到套用。

   選定的監控點已停用。

正在刪除監控點

您可以刪除與網路介面關聯的監控點。如果網路介面不再用於接收流量，則可能需要刪除監控點。

如果需要暫時停止接收監控點網路介面上的流量（例如在維護調試期間），可以停用該監控點而不刪除它。

> 在監控點刪除之前從其接收到的流量不會從資料庫中刪除。此外，有關此監控點的資訊會儲存在記錄事件表中。

若要刪除監控點：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關網路介面的卡。
3. 這將開啟一個視窗，其中包含有關網路介面的資訊。
4. 點擊**刪除**。
   這將開啟一個確認提示視窗。如果監控點已啟用，應用程式將提示您停用該監控點。
5. 在提示視窗中確認刪除監控點。

該監控點已刪除。

配置掃描檔案的最大大小

> 如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要配置掃描檔案的最大大小：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Sensor 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 轉到“**其他**”索引標籤。
5. 將“**設定大小限制**”切換開關設定為“**已啟用**”。
6. 在“**計量單位**”欄位中，選擇一個計量單位。

7. 在“**空間**”欄位中，輸入檔案允許的最大大小。

8. 點擊**儲存**。

   将配置掃描檔案的最大大小。

如果要將掃描檔案的最大大小設定為大於 100 MB 的值：

1. 透過 SSH 協定或終端機進入 Sensor 伺服器的管理主控台。

2. 系統提示時，請輸入管理員使用者名稱和在安裝元件期間指定的密碼。

3. 顯示應用程式元件管理員功能表。

4. 選擇技術支援模式。

5. 按 ENTER。

6. 這將開啟技術支援模式確認視窗。

7. 確認您想要在技術支援模式下管理應用程式。為此，請選擇“是”並按 ENTER。

8. 若要檢視目前掃描檔案的大小限制，請執行下列命令：

   ```
   docker exec $(docker ps -q -f name=nta_core) grep body-limit
   /var/opt/kaspersky/kics4net/ids/client/templates/suricata.yaml.templ | grep -v '#'
   ```

9. 目前限制顯示在 request-body-limit 和 Response-body-limit 欄位中。目前限制以位元組為單位顯示。

10. 若要變更目前限制，請執行下列命令：

    ```
    exec $(docker ps -q -f name=nta_core) sed -i 's/<以位元組表示的先前值>/<以位元組表示的新值
    >/' /var/opt/kaspersky/kics4net/ids/client/templates/suricata.yaml.templ
    ```

11. 完成上述說明中的步驟 1–8。

    您可以將掃描檔案的最大大小設定為超過 100 MB。

配置與 Central Node 分開安裝的 Sensor 元件的伺服器上掃描檔案的最大大小

如果您在將獨立 Sensor 連線到 Central Node 之前選擇了網路協定以從其 SPAN 連接埠取得鏡像流量，並且想要在連線後變更這些設定，則您需要先執行變更設定之前的準備步驟，然後按照上述說明進行操作。

配置 HTTP 封包主體傾印

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要配置 HTTP 封包主體傾印：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Sensor 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 轉到**其他**索引標籤。
5. 在**傾印 HTTP 主體**部分：
   - 如果要啟用 HTTP 封包主體傾印，請將**啟用 http-body**切換開關設定為**已啟用**。
     預設情況下，切換開關位於**已停用**位置。
   - 如果要停用 HTTP 封包主體傾印，請將**啟用 http-body**切換開關設定為**已停用**。
6. 點擊**儲存**。

HTTP 封包主體傾印已啟用或停用。

配置透過 SMTP 與郵件伺服器整合

SMTP 流量可以透過兩種方式匯入Kaspersky Anti Targeted Attack Platform：作為映像流量（SPAN流量）的一部分，或透過 SMTP 與郵件伺服器整合。如果 SMTP 流量是作為 SPAN 流量的一部分匯入，應用程式只會擷取並掃描附件。在這種情況下，郵件主體和 URL 等郵件內容將無法進行分析。

若要掃描郵件的全部內容，您需要設定透過 SMTP 與郵件伺服器整合。

> 如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

若要設定透過 SMTP 與郵件伺服器整合：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Sensor 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 前往**SMTP 整合**索引標籤。
5. 如果要透過 SMTP 啟用與郵件伺服器的整合，請將**啟用 SMTP 整合**切換開關設為**已啟用**。
6. 在**目標網域**欄位中，指定郵件網域或子網域的名稱。該應用程式將掃描被傳送到指定網域的郵箱的電子郵件。
   若要停用網域或子網域，請以`!domain.tld`形式將其括起來。
   如果將郵件網域留給空白，應用程式將接收傳送至任何電子郵件信箱的郵件。

7. 在**用戶端**欄位中，指定允許應用程式透過 SMTP 協定與其互動的主機 IP 位址和/或子網路遮罩（採用 CIDR 表示法）。

   若要停用主機或子網路，請以 `!host` 形式將位址括起來。

   如果將此欄位留空，應用程式將收到以下訊息：

   - 如果您在**目標網域**欄位中指定了電子郵件網域，請從任何電子郵件信箱傳送。
   - 如果在**目標網域**欄位中未指定網域，則來自任何主機。

   > 如果你想置**目標網域**和**用戶端**欄位為空，您需要使用任何方法來限制能夠向應用程式傳送訊息的主機清單。

8. 如果要設定允許接收郵件的最大大小，請將**設定郵件大小**切換開關設定為**已啟用**。
9. 在"**計量單位**"欄位中，選擇一個計量單位。
10. 在"**空間**"欄位中，輸入檔案允許的最大大小。
11. 如果要設定與郵件伺服器的 SMTP 連線的 TLS 加密，請在**用戶端 TLS 安全級別**下，選擇下列選項之一：

    - **停用 TLS 加密**。

      該應用程式不會使用與郵件伺服器的連線的 TLS 加密。

    - **允許對傳入訊息進行 TLS 加密**。

      該應用程式將支援連線的 TLS 加密，但加密不是強制性的。

    - **要求對傳入訊息進行 TLS 加密**。

      該應用程式將僅透過加密通道接收訊息。

12. 點擊**下載 TLS 憑證**按鈕，將具有 Sensor 元件的伺服器的 TLS 憑證儲存在瀏覽器下載資料夾中的電腦上。

    郵件伺服器上的身分驗證需要此憑證。

13. 在**請求用戶端 TLS 憑證**設定群組中，選擇以下選項之一：

    - **不請求**。

      該應用程式不會驗證郵件伺服器的 TLS 憑證。

    - **請求**。

      該應用程式將從郵件伺服器請求 TLS 憑證（如果有）。

    - **要求**。

      該應用程式將僅從具有 TLS 憑證的郵件伺服器接收訊息。

14. 點擊**儲存**。

將設定透過 SMTP 與郵件伺服器整合。該應用程式將根據定義的設定掃描透過 SMTP 協定接收的電子郵件。

如果您已將 Central Node 和 Sensor 元件部署為叢集，則可以設定與郵件伺服器的高可用性整合。

若要設定與郵件伺服器的高可用性整合：

1. 在 Central Node 叢集對應網域的 DNS 伺服器上設定輪詢調度演算法。

2. 在郵件伺服器設定中指定此網域名稱。

   與郵件伺服器的整合將根據網域名稱進行配置。郵件伺服器將與叢集中的隨機伺服器進行通訊。如果該伺服器發生故障，郵件伺服器將與叢集中另一台健康的伺服器進行通訊。

對於叢集配置中的應用程式 7.0 版本，在與郵件伺服器整合時，傳送電子郵件訊息時可能會發生錯誤："451 4.3.0 錯誤：佇列檔案寫入錯誤"。

若要解決該錯誤，請執行以下操作：

1. 透過 SSH 或使用終端機進入任何叢集伺服器的管理主控台。

2. 系統提示時，輸入管理員使用者名稱和安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表中，選擇技術支援模式。

4. 按 Enter 鍵。

   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇是並按 ENTER。

6. 執行以下指令：

   `for addr in <叢集伺服器的 IP 位址（以空格分隔）>; do nc -zv $addr 10025; done`

   伺服器清單顯示在主控台上。

7. 在應用程式的 Web 介面中，在上述說明的第7 步驟中，指定在主控台上顯示`localhost [127.0.0.1] 10025 (?) open`字串的伺服器的 IP 位址。

   錯誤已解決。

如果您沒有為任何叢集伺服器取得`localhost [127.0.0.1] 10025 (?) open`字串，請聯絡技術支援。

在伺服器上安裝 7.0.3 版本的 Central Node 元件時，Kaspersky Anti Targeted Attack Platform 可能會拒絕透過 SMTP 接收的電子郵件。寄件者可能會收到"連線被拒絕"錯誤。

要消除限制：

1. 透過 SSH 或終端登入相關 Central Node 伺服器的管理主控台。

2. 系統提示時，請輸入管理員使用者名稱和安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表中，選擇技術支援模式。

4. 按 Enter 鍵。

   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇是並按 ENTER。

6. 執行以下指令：

```
sudo -i
```

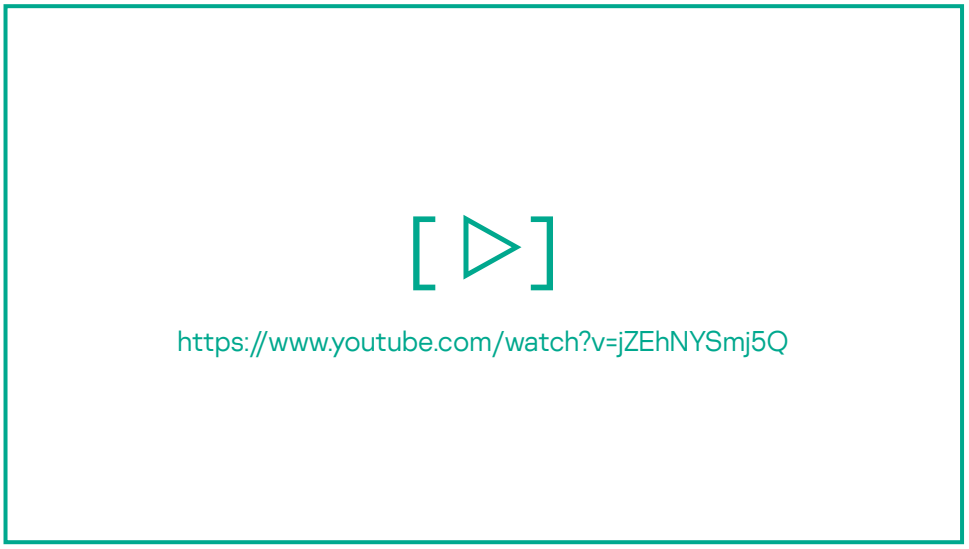
7. 執行以下指令：

   a. `docker exec $(docker ps -q -f name=preprocessor_span) supervisorctl restart preprocessor`

   b. `docker exec $(docker ps -q -f name=preprocessor_smtp) supervisorctl restart preprocessor`

限制已移除。

觀看視頻教程，了解如何設定 Central Node 以處理郵件流量並與 Kaspersky Secure Mail Gateway 整合。您可以在幫助頁面（見下方）播放視頻，或點擊連結https://youtu.be/jZEhNYSmj5Q?si=6OAp9ZHVWklL04Ch。



配置 Central Node 以處理郵件流量，並與 Kaspersky Secure Mail Gateway 整合

配置透過 ICAP 與代理伺服器整合

透過 ICAP 與具有回饋的代理伺服器整合，您可以防止惡意物件進入公司 LAN 並防止主機使用者存取惡意或網路釣魚網站。Kaspersky Anti Targeted Attack Platform 可作為 ICAP 伺服器，而您的代理伺服器則可作為 ICAP 用戶端。代理伺服器將 ICAP 請求傳送到 ICAP 伺服器。ICAP 伺服器執行掃描並將結果傳回代理伺服器。如果偵測到任何威脅，會向主機上的使用者顯示通知 HTML 頁面。

透過 ICAP 與代理伺服器整合時，存在某些限制：

如果在透過 ICAP 進行整合時遇到磁碟空間問題，請聯絡技術支援人員。

啟用和停用透過 ICAP 與代理伺服器整合

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

使用獨立代理伺服器時，Kaspersky Anti Targeted Attack Platform 預設不提供 ICAP 流量加密或 ICAP 用戶端身分驗證。應用程式管理員必須採取措施，透過使用流量隧道或 Iptables 確保代理伺服器和 Kaspersky Anti Targeted Attack Platform 之間的網路連線安全。

要啟用和停用透過 ICAP 與代理伺服器整合：

1. 在應用程式 Web 介面視窗中，選擇"**Sensor 伺服器**"區域。
2. 點擊相關 Sensor 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊"**編輯**"。
4. 轉到**ICAP 整合**索引標籤。
5. 執行以下操作：
   - 如果要透過 ICAP 啟用與代理伺服器的整合，請將**啟用 ICAP 整合**切換開關設為**已啟用**。
   - 如果要透過 ICAP 停用與代理伺服器的整合，請將**啟用 ICAP 整合**切換開關設定為**已停用**。

   透過 ICAP 與代理伺服器整合被啟用。

如果您已將 Central Node 和 Sensor 元件部署為叢集，則可以設定與代理伺服器的高可用性整合。

若要配置與代理伺服器的高可用性整合：

1. 在 Central Node 叢集對應網域的 DNS 伺服器上設定輪詢調度演算法。
2. 在代理伺服器設定中指定此網域名稱。

   與代理伺服器的整合將根據網域名稱進行配置。代理伺服器將與叢集中的隨機伺服器進行通訊。如果該伺服器發生故障，代理伺服器將與叢集中另一台健康的伺服器進行通訊。

啟用或停用 ICAP 流量即時掃描

如果您使用分散式解決方案和多組織用戶模式，請使用您要設定其參數的 PCN 或 SCN 伺服器 Web 介面。

如果啟用了透過 ICAP 與代理伺服器的整合，您可以啟用或停用 ICAP 流量即時掃描。

如果啟用 ICAP 流量即時掃描，Kaspersky Anti Targeted Attack Platform 會即時向ICAP 用戶端傳送有關掃描物件的資訊。這有助於防止下載惡意物件和點擊不受信任的連結。

要啟用或停用 ICAP 流量即時掃描：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Sensor 元件的卡片。

   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 前往**ICAP 整合**索引標籤。
5. 在**即時掃描**下面，選擇以下選項之一：
   - **已停用。**

     如果選擇此選項，ICAP 流量即時掃描將被停用。預設選擇此選項。
   - **已啟用，標準 ICAP 流量掃描。**

     啟用此類掃描後，將根據卡巴斯基安全網路的知識庫檢查檔案和 URL 的信譽，並由 Sandbox 元件、惡意軟體防護引擎和 YARA 模組掃描檔案。當檔案正在被 Sandbox 元件掃描時，它們仍然可用。
   - **已啟用，進階 ICAP 流量掃描。**

     啟用此類掃描後，將根據卡巴斯基安全網路的知識庫檢查檔案和 URL 的信譽，並由 Sandbox 元件、惡意軟體防護引擎和 YARA 模組掃描檔案。當檔案正在被 Sandbox 元件掃描時，它們不可用。
6. 在**提取使用者名稱**部分：

   如果您要從 ICAP 伺服器取得使用者名稱，請將**提取使用者名稱**切換開關欄位設為**已啟用**。如果需要使用 Base64 解碼，請選擇**使用 Base64 解碼**核取方塊。
7. 點擊**儲存**。

ICAP 流量的即時掃描已啟用或停用。

如果停用代理伺服器整合，ICAP 流量掃描也會停用，即使先前已啟用。掃描設定被保留，下次啟用代理伺服器整合時，ICAP 流量掃描將重新啟用。

檢視 ICAP 排除表將規則新增至 ICAP 排除項目當在掃描的檔案中偵測到威脅時，應用程式會發出警示。惡意軟體防護引擎和 YARA 模組的檔案掃描繼續正常運作。

配置 ICAP 流量即時掃描

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

只能在技術支援模式下才能配置在具有 Sensor 元件的獨立伺服器上進行即時 ICAP 流量掃描。要在技術支援模式下執行操作，我們建議聯絡技術支援。

您可以在具有 Central Node 和 Sensor 元件的伺服器上設定 ICAP 流量即時掃描，以對資料進行防毒掃描。掃描結果在通知 HTML 頁面上顯示為主機使用者。

要配置 ICAP 流量即時掃描：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**ICAP 流量掃描**子部分。

   ICAP 流量掃描設定頁面將顯示。

   預設情況下，在**通知**下面，與以下事件對應的頁面將會載入：

   - 如果在使用者要求的位址偵測到威脅，則會顯示在**連接被封鎖**欄位中上傳的頁面。
   - 如果在掃描檔案中偵測到威脅，則會顯示在**檔案已封鎖**欄位中上傳的頁面。

   預設情況下，分發套件中的HTML 頁面會載入到 Kaspersky Anti Targeted Attack Platform 中。您可以上傳自己的通知頁面並配置它們的顯示方式。通知頁面的大小不得超過 1.5 MB。如果上傳的通知頁面大於 1.5 MB，則會顯示錯誤。

2. 在**檔案块阈值**下面的**Sandbox 警示重要性**欄位中，從下拉清單中選擇一個值。根據卡巴斯基的專家意見，這些數值對應於警示對電腦或公司網路安全可能產生的影響。

   此設定可以採用以下值之一：

   - **高** 表示高重要性警示。預設選擇此選項。
   - **中** 表示中等重要性警示。
   - **低** 表示低重要性警示。

3. 在**掃描逾時**下面的**逾時**欄位中，指定檔案掃描時間。在掃描檔案時，其下載速度會降低。如果無法在指定時間內掃描檔案，則下載將以正常速度繼續。

   預設值為 10 分鐘。您可以設定任何大於 1 分鐘的值。

4. 點擊**套用**。

掃描使用指定的設定執行。

配置通知頁面的顯示

> 如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

在即時 ICAP 流量掃描期間，Kaspersky Anti Targeted Attack Platform 可以阻止 URL 導覽和檔案下載。當這些操作正在進行時，將向嘗試進行 URL 存取或檔案下載請求的主機上的使用者顯示 HTML 通知頁面。如果您想顯示自己的頁面而不是預設頁面，您可以上傳自己的自訂 HTML 頁面。

上傳通知頁面：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**ICAP 流量掃描**子部分。
2. 在**通知**部分，點擊您需要的欄位之一旁邊的**瀏覽**。
3. 這將開啟一個視窗；在該視窗中，選擇您的HTML 頁面。

4. 點擊**開啟**。

   您的頁面已上傳。

配置 SPAN 連接埠映像流量的記錄

透過 Kaspersky Anti Targeted Attack Platform，您可以節省 SPAN 連接埠映像流量，以便調查和偵測企業 LAN 範圍內的惡意活動。透過映像流量記錄，您可以對網路事件進行回顧分析並調查駭客的操作。流量以 PCAP 格式儲存為傾印。

若要儲存來自 SPAN 連接埠的鏡像流量，您需要啟用此流量的記錄並設定記錄功能。您也可以選擇網路協定，以供 Kaspersky Anti Targeted Attack Platform 在處理鏡像流量時從中提取物件和中繼資料。

觀看視頻教程，了解如何配置 Central Node 以透過 Sensor 元件處理 SPAN 流量。您可以在幫助頁面（見下方）播放視頻，或點擊連結https://youtu.be/9whcEY-5MAs?si=lZKy1WxtTM7kXWt5。

配置 Central Node 以透過 Sensor 元件處理 SPAN 流量

選擇用於從 SPAN 連接埠接收映像流量的網路協定

如果您使用分佈式解決方案和多組織用戶模式，請在 Sensor 元件連線的 PCN 或 SCN 伺服器的 Web 介面中執行設定操作。

要選擇從 SPAN 連接埠接收映像流量的網路協定：

1. 如果要選擇用於接收嵌入式 Sensor 的 SPAN 連接埠鏡像流量的網路協定，請透過 SSH 或使用終端登入具有該 Sensor 的 Central Node 伺服器的管理主控台。

2. 如果要選擇用於接收獨立於 Central Node 安裝的 Sensor 的 SPAN 連接埠鏡像流量的網路協定，請透過 SSH 或使用終端登入該 Sensor 伺服器的管理主控台。

3. 當系統提示時，請輸入管理員使用者名稱，以及在安裝應用程式期間設定的密碼。

   這將開啟 Sensor 元件的設定功能表。如果功能表未開啟，請輸入 `kata-admin-menu` 指令並 按 **ENTER** 鍵。

4. 前往**程式設定 → 設定流量擷取 → 設定擷取協定**區段， 使用 ↑、↓ 和 **ENTER** 鍵。所選行以紅色突出顯示。

   這將開啟一個視窗，您可以在其中啟用或停用從以下網路協定的 SPAN 連接埠接收映像流量：

   - **DNS**
   - **FTP**
   - **HTTP**
   - **HTTP2**
   - **SMTP**
   - **SMB**
   - **NFS**

   > 若要分析 NFS 流量，您必須掛載 NFS 分割區並指定協定版本。

   範例：

   對於 NFS v.4：

   ```
   mount -t nfs -o vers=4 -O uid=1000,iocharset=utf-8 <address>:/from/dir /to/dir
   ```

   對於 NFS v.3：

   ```
   mount -t nfs -o vers=3 -O uid=1000,iocharset=utf-8 <address>:/from/dir /to/dir
   ```

   如果啟用透過網路協定從 SPAN 連接埠接收鏡像流量，則 **[x]** 將顯示在網路協定名稱的右側。如果針對特定網路協定停用從 SPAN 連接埠接收鏡像流量，則 **[ ]** 將顯示在該協定名稱的右側。

   預設情況下，對所有網路協定（**HTTP2** 除外）啟用從 SPAN 連接埠接收鏡像流量。

   > 停用 HTTP 和/或 DNS 可能會導致執行資料庫更新時發生錯誤。

5. 如果要針對特定網路協定啟用或停用從 SPAN 連接埠接收鏡像流量，請使用 ↑、↓ 鍵選取該協定，然後按 **ENTER**。

6. 選擇包含**套用並完成**的行，然後按 **ENTER**。

用於從 SPAN 連接埠接收映像流量的網路協定被選擇。

在與 Central Node 分開安裝的 Sensor 元件的伺服器上選擇網路協定

如果您在將獨立 Sensor 連線到 Central Node 之前選擇了網路協定以從 SPAN 連接埠取得鏡像流量，並且想要在連線後變更這些設定，則您需要先執行變更設定之前的準備步驟，然後按照上述說明進行操作。

配置 SPAN 連接埠映像流量的記錄

如果您使用分佈式解決方案和多組織用戶模式，請在 Sensor 元件連線的 PCN 或 SCN 伺服器的 Web 介面中執行設定操作。

若要開啟從 SPAN 連接埠記錄映像流量：

1. 連線並配置外部儲存。
2. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
3. 點擊相關 Sensor 元件的卡片。

   這將開啟一個視窗，其中包含有關元件的資訊。
4. 點擊“**編輯**”。
5. 轉到**外部儲存**索引標籤。

   在**外部儲存**部分，**最舊的封包**欄位顯示外部儲存中第一次儲存的傾印的日期和時間。**最新封包**欄位顯示最後一次傾印儲存到外部儲存的日期和時間。
6. 如果要使用外部儲存，請將**連線外部儲存以儲存流量傾印檔案**切換開關設定為**已啟用**。

   預設情況下，切換開關位於**已停用**位置。
7. 執行以下操作：

   a. 在**最大大小**下，指定要儲存在儲存中的流量傾印檔案的最大大小。

      如果儲存中的傾印大小超過指定值，最早的傾印將被刪除，其總大小等於新傾印的大小。

      > 如果您減少最大傾印儲存大小，則最早的傾印將被刪除，其總大小等於設定的變更。

   b. 如果要限制流量資料的捕獲，請在**使用 BPF 進行過濾**下，將**啟用過濾**切換開關設為**已啟用**。流量篩選可以減少傾印儲存中的傾印大小並有利於流量分析。

      在**過濾表達式**欄位中，輸入過濾規則。BPF 篩選規則以 libpcap 格式撰寫。有關語法的更多詳細資訊，請參閱pcap-filter 手冊頁。

      篩選表達式範例：

      `tcp port 102` 或 `tcp port 502`

   c. 如果要配置流量傾印儲存時長，請在**儲存時間限制**下，將**定義儲存時間**切換開關設為**已啟用**。在**儲存時間（天）**欄位中，輸入您要儲存流量傾印的天數。當指定的期限結束時，傾印檔案將從儲存中刪除。

   d. 點擊**儲存**。

將設定記錄從 SPAN 連接埠接收的映像流量。

配置透過 POP3 與郵件伺服器整合

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

若要設定透過 POP3 與郵件伺服器整合：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關 Sensor 元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊“**編輯**”。
4. 轉到“**POP3 整合**”索引標籤。
5. 將“**啟用 POP3 整合**”切換開關設定為“**已啟用**”。
6. 在**郵件伺服器**欄位中，輸入需要設定整合的郵件伺服器的 IP 位址。
7. 在**連接埠**欄位中，指定連線到郵件伺服器的連接埠。
8. 在**接收頻率**欄位中，指定郵件伺服器連線頻率（以秒為單位）。
9. 如果要透過 POP3 使用與郵件伺服器的連線的 TLS 加密，請選擇**使用 TLS 加密**核取方塊。
10. 在**使用者名稱**欄位中，指定用於存取郵件伺服器的帳戶名稱。
11. 在**密碼**欄位中，指定用於存取郵件伺服器的密碼。

    郵件伺服器必須支援基本身分驗證。

12. 在**TLS 憑證**下拉式清單中，選擇以下選項之一：
    - **接受任何**。
    - **接受不受信任的自簽章憑證**。
    - **只接受受信任的**。

    與外部郵件伺服器建立連線時，建議僅設定受信任的 TLS 憑證。如果您接受不受信任的 TLS 憑證，則無法保證連線免受MITM 攻擊。儘管接受可信賴的 TLS 憑證也無法保證連線免受MITM 攻擊，但它是透過 POP3 協定與郵件伺服器整合的最安全的支援方法。

13. 如有必要，在**密碼套件**欄位中，修改透過 POP3 與郵件伺服器建立連線時所使用的 OpenSSL 設定。
    您可以透過點擊**說明**連結檢視有關 OpenSSL 的參考資訊。

14. 點擊**儲存**。

    將配置透過 POP3 與郵件伺服器整合。

如果您已將 Central Node 和 Sensor 元件部署為叢集，則可以設定與郵件伺服器的高可用性整合。

若要設定與郵件伺服器的高可用性整合：

1. 在 Central Node 叢集對應網域的 DNS 伺服器上設定輪詢調度演算法。

2. 在郵件伺服器設定中指定此網域名稱。

   與郵件伺服器的整合將根據網域名稱進行配置。郵件伺服器將與叢集中的隨機伺服器進行通訊。如果該伺服器發生故障，郵件伺服器將與叢集中另一台健康的伺服器進行通訊。

身分驗證政策

您可以為 Kaspersky Anti Targeted Attack Platform 使用者配置身分驗證政策。這些政策適用於所有具有**KATA 使用者帳戶**帳戶類型的 Kaspersky Anti Targeted Attack Platform 使用者，無論其獲指派的角色為何。

首次身分驗證成功後強制變更密碼

如果啟用此功能，則密碼將根據以下情況變更：

1. 管理員建立一個使用者帳戶。

2. Kaspersky Anti Targeted Attack Platform Web 介面中的使用者身分驗證。

3. 如果使用者在啟用此功能之前尚未變更其密碼，應用程式會在使用者下次登入 Web 介面時提示使用者變更帳戶密碼。舊密碼將無效。

使用者首次登入應用程式主 Web 介面被視為首次身分驗證。如果使用者返回並登入尺寸管理的 Web 介面或應用程式的管理員功能表，則不會顯示任何密碼變更提示。如果使用者帳戶用於將 SCN 連線到 PCN，則不會顯示密碼變更提示。

定期密碼變更

如果啟用了定期密碼變更，則應用程式會在管理員設定的期限到期後提示使用者變更密碼。倒數計時從變更帳戶密碼的那一刻開始，並針對每個使用者單獨進行追蹤。

終止非活動工作階段

如果使用者沒有執行任何操作（工作階段處於空閒狀態），我們建議終止此類工作階段。當使用者實際上已完成使用應用程式但未結束工作階段時，這可以降低未經授權存取 Kaspersky Anti Targeted Attack Platform 的風險。

關於身分驗證嘗試失敗的通知

頻繁嘗試登入 Web 介面或管理主控台失敗可能表示網路犯罪分子正在試圖透過暴力破解密碼來存取 Kaspersky Anti Targeted Attack Platform。為了防止此類未經授權的存取，我們建議啟用有關超出身分驗證嘗試失敗次數限制的通知。

分佈式解決方案和多租戶模式

在分佈式解決方案和多組織用戶模式下，PCN 上指定的身分驗證政策設定會套用至 SCN。

首次身分驗證成功後強制變更密碼

有關此功能的詳細資訊，請參閱"*身分驗證政策*"部分。

若要啟用在第一次成功身分驗證後強制變更密碼：

1. 在應用程式 Web 介面視窗中，選擇"**設定**"區域。
2. 前往"**身分驗證政策**"索引標籤。
3. 在"**首次身分驗證後變更密碼**"部分，設定"**請求密碼變更**"切換開關至"**已啟用**"。
4. 點擊**套用**。

   第一次身分驗證後強制變更密碼啟用。

強制定期變更密碼

有關此功能的詳細資訊，請參閱"*身分驗證政策*"部分。

若要啟用並配置強制定期變更密碼：

1. 在應用程式 Web 介面視窗中，選擇"**設定**"區域。
2. 前往"**身分驗證政策**"索引標籤。
3. 在**定期變更密碼**部分，設定**請求密碼變更**切換開關至**已啟用**。

4. 在**在此時間後變更密碼：**欄位中，輸入您想要在多少天後變更密碼。

5. 點擊**套用**。

指定期限後強制變更密碼啟用並配置。

終止非活動工作階段

如果使用者沒有執行任何操作（工作階段處於空閒狀態），我們建議終止此類工作階段。當使用者實際上已完成使用應用程式但未結束工作階段時，這可以降低未經授權存取 Kaspersky Anti Targeted Attack Platform 的風險。

若要啟用並配置非活動工作階段的終止：

1. 在應用程式 Web 介面視窗中，選擇"**設定**"區域。

2. 前往"**身分驗證政策**"索引標籤。

3. 在"**終止非活動工作階段**"部分，指定當使用者未執行任何操作時終止使用者工作階段的時間。在"**在此時間後終止非活動工作階段**"欄位中輸入時間（分鐘）。

4. 如果您想要在使用者空閒時無法存取"**控制板**"，請選取"**工作階段處於非活動狀態時鎖定控制板**"核取方塊。如果清除此核取方塊，則即使工作階段處於非活動狀態，使用者仍可檢視"**控制板**"。

5. 點擊**套用**。

不活動的使用者工作階段將在指定時間後終止。

關於身分驗證嘗試失敗的通知

頻繁嘗試登入 Web 介面或管理主控台失敗可能表示網路犯罪分子正在試圖透過暴力破解密碼來存取 Kaspersky Anti Targeted Attack Platform。為了防止此類未經授權的存取，我們建議啟用有關超出身分驗證嘗試失敗次數限制的通知。

若要啟用並設定有關失敗的身分驗證嘗試的通知：

1. 在應用程式 Web 介面視窗中，選擇"**設定**"區域。

2. 前往"**身分驗證政策**"索引標籤。

3. 在"**統計身分驗證嘗試次數**"區域中，將"**計數嘗試次數**"切換開關設定為"**已啟用**"。

4. 在"**計數期間**"欄位中，輸入您要計算失敗身分驗證嘗試次數的時間範圍。時間以分鐘為單位指定。如果使用者嘗試登入 Web 介面或管理主控台並連續失敗兩次以上，則會發生以下情況：

   - 有關使用者身分驗證嘗試失敗的記錄將寫入使用者活動日誌。

   - 如果已建立用於傳送有關過多次數身分驗證嘗試失敗的通知的規則（有關如何建立此類規則的資訊，請參閱下文），則會向通知規則中指定的位址傳送電子郵件訊息。該訊息包含有關失敗的使用者身分驗證嘗試的資訊。

在“**計數期間**”欄位中，您可以指定 0，在此情況下，無論各次嘗試之間經過多少時間，都會計算所有失敗的身分驗證嘗試。

5. 點擊**套用**。

系統會對失敗的身分驗證嘗試進行計數，如果超過指定的閾值（連續兩次身分驗證嘗試失敗），則會儲存有關此資訊以供審查。

若要啟用並設定有關超出失敗的身分驗證嘗試次數的通知：

請依照相關步驟，建立用於傳送應用程式元件運作通知的規則。建立規則時，請在“**元件**”下選取“**授權嘗試**”核取方塊。

如果在指定的時間間隔內連續發生超過兩次使用者身分驗證失敗的嘗試，系統會將包含失敗使用者身分驗證嘗試相關資訊的訊息，傳送至通知規則中指定的電子郵件地址（請參閱上方的“**計數期間**”設定）。

管理叢集

您可以檢視叢集中的伺服器表，向叢集新增伺服器，重新啟動伺服器，停用伺服器，啟用或停用叢集。如有必要，您可以增加儲存伺服器的磁碟空間。

檢視叢集的伺服器表

叢集伺服器表顯示在應用程式 Web 介面的“**叢集**”部分。

表包含以下資訊：

- **伺服器類型**—伺服器類型取決於其在叢集中的角色。

  以下值可以顯示：

  - **儲存**。
  - **處理**。

- **狀態**—伺服器狀態。

  以下值可以顯示：

  - **已連線**。
  - **未連線**。

- **主機名稱**—伺服器名稱。
- **IP**—伺服器的 IP 位址。
- **記憶體**—伺服器的 RAM 負載等級。
- **CPU**—伺服器的 CPU 負載水準。

- **操作**—您可以用伺服器執行的操作。

  可以執行以下操作：**刪除**。

將伺服器新增至叢集

要將伺服器新增至叢集，您需要在此伺服器上開始安裝 Kaspersky Anti Targeted Attack Platform，並依照步驟安裝元件。新增的伺服器顯示在叢集伺服器清單中。

增加儲存伺服器上的磁碟空間

您可以透過安裝額外的磁碟來增加正在執行的儲存伺服器上的磁碟空間。

> 如需透過額外磁碟的方式增加儲存伺服器的磁碟空間，您需要聯絡技術支援。

伺服器配置為技術支援模式。

重新啟動叢集中的伺服器

在重新啟動任何類型的伺服器之前，您需要確保同類型的另一台伺服器仍然處於活動狀態。我們強烈建議您一次重啟一台伺服器，並且在完成以下過程之一的所有步驟後，再重啟叢集中的下一台伺服器。

重啟叢集的處理伺服器

要重新啟動處理伺服器：

1. 找出叢集中哪些伺服器在 Docker Swarm 中具有“管理員”角色。為此，請在任意叢集伺服器上執行以下命令：

   `docker node ls`

   此指令顯示叢集伺服器清單。管理員角色指派給”管理員狀態“列中具有”領導者“或”可聯絡“屬性的伺服器。

2. 以任何方便的方式保存產生的伺服器清單。

   重新啟動後，可以使用這些伺服器來偵錯應用程式在叢集的處理伺服器之間所需的服務的遷移狀態。

3. 在元件的管理員選單中重新啟動處理伺服器。

4. 至少等待 5 分鐘。

5. 在具有管理員角色的伺服器上，檢查服務遷移到另一台處理伺服器的狀態：

   `docker service ls | grep -v configurator | grep ' 0/'`

   輸出應為空。這意味著所有服務已在另一台處理伺服器上成功啟動。

6. 根據需要重複步驟 5，直到輸出為空為止。

處理伺服器被重新啟動。然後您可以重新啟動下一個處理伺服器。

重新啟動儲存伺服器

若要重新啟動儲存伺服器：

1. 在元件的管理員選單中重新啟動儲存伺服器。
2. 至少等待 5 分鐘。
3. 在叢集中的任一台伺服器上，檢查叢集健康狀況：
   `$ceph -s`
   此指令應輸出 `HEALTH_OK` 狀態。
4. 根據需要重複步驟 3，直到顯示 `HEALTH_OK` 狀態為止。

儲存伺服器被重新啟動。然後您可以重新啟動下一個儲存伺服器。

停用伺服器

> 若要停用正在執行的伺服器，您需要聯絡技術支援。

如果伺服器發生故障，您可以自行停用它。

若要停用無法運作的處理伺服器：

1. 將新處理伺服器新增至叢集。
2. 從叢集中刪除伺服器。
3. 為新配置配置應用程式的大小。

處理伺服器將被停用。

若要停用無法運作的儲存伺服器：

1. 將新的儲存伺服器新增至叢集。
2. 聯絡技術支援以從叢集中刪除無法運行的伺服器。

儲存伺服器將被停用。

從叢集中刪除伺服器

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

被刪除的伺服器無法還原。確保所選伺服器不可運作。

若要從叢集中刪除伺服器：

1. 在應用程式 Web 介面視窗中，選擇**叢集**區域。
2. 在**操作**列中，點擊與您要刪除的伺服器相對的**刪除**連接。
3. 點擊**繼續**。

   刪除過程將開始。刪除可能需要大約一天的時間。有關已刪除伺服器的資訊將不會顯示在伺服器表中。

刪除伺服器後，您可以重新配置叢集中的伺服器或新增具有相同角色的伺服器，以保持相同等級的應用程式效能。

啟動和關閉叢集

要關閉或啟動叢集，我們建議聯絡技術支援。如果遇到應用程式運行狀況問題，請勿關閉或啟動叢集。

如果要關閉叢集中的健康伺服器，必須先關閉叢集，以免資料遺失。

關閉叢集：

1. 在應用程式 Web 介面中，前往**叢集**區段。
2. 點擊**關機**按鈕。

   應用程式的主要元件已停止。您現在可以關閉叢集伺服器的電源。

啟動叢集伺服器：

1. 如果之前未斷開伺服器的電源，請中斷伺服器的電源。
2. 開啟儲存伺服器的電源。
3. 啟動其餘伺服器。

   叢集伺服器將啟動。

叢集中的所有伺服器啟動大約需要90 分鐘。在所有叢集伺服器啟動之前，應用程式 Web 介面即可使用。然而，對於具有**資深安全員**、**安全官**、**安全稽核員**角色的使用者，應用程式 Web 介面不顯示應用程式功能表，而具有**管理員**的使用者只能管理**伺服器配置**區段。

我們強烈建議不要在叢集中的所有伺服器都啟動並執行先前管理應用程式的大小設定。

當叢集中的所有伺服器均正常運作時，應用程式 Web 介面功能表正常顯示。

有關 Central Node 和 Sensor 伺服器允許的最大CPU 和 RAM 負載的通知

在 Central Node 和 Sensor 伺服器的 CPU 和 RAM 上保持高負載可能會阻止應用程式元件運作。

您可以配置 Central Node 和 Sensor 伺服器上 CPU 和 RAM 的最大使用率；如果超過這些值，則為具有"**資深安全員**"、"**安全官**"和"**管理員**"角色的使用者提供的應用程式 Web 介面的"**控制板**"部分的上部會顯示一個黃色警告框。您也可以設定要傳送到一個或多個電子郵件信箱的通知，和用於將有關 CPU 和 RAM 負載的資訊傳送到支援該協定的外部系統的 SNMP 協定連線。

如果您已將 Central Node 和 Sensor 元件部署為叢集，則將為叢集中的每台伺服器單獨顯示警告。

具有**資深安全員**或者**安全官**角色的使用者還可以建立傳送通知的規則。在這種情況下，正確傳送通知需要配置伺服器的 CPU 和 RAM 的最大允許負載值，以及伺服器上的通知設定。

在傳送有關應用程式元件的通知的現有規則中，如果滿足以下條件，則會自動啟用 CPU 負載和 RAM 負載通知：當規則被建立時，在**元件**下面選擇**所有**核取方塊。

配置 Central Node 和 Sensor 伺服器允許的最大CPU 和 RAM 負載

在分佈式解決方案和多租戶模式下，您需要為要從其接收通知的每個 Central Node 伺服器設定 CPU 和 RAM 負載的最大允許負載值。如果您使用 Central Node 叢集，則可以在任何叢集伺服器上配置這些設定。

要配置 Central Node 和 Sensor 伺服器的 CPU 和 RAM 上允許的最大負載：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**一般設定**子部分。
2. 在**監控**下面:
   - 在**CPU 使用率超出此值時警告N% 持續M分鐘**欄位中，輸入允許的最大CPU 使用率以及可以維持最大負載的時間段。

     預設情況下，CPU 最大負載為 95%，持續 5 分鐘。

- 在**記憶體使用率超出此值時警告N% 持續M分鐘**欄位中，輸入允許的最大 RAM 使用率以及可以維持最大使用率的時間段。

  預設情況下，最大 RAM 使用率為 95%，持續 5 分鐘。

3. 點擊**套用**。

伺服器 CPU 和 RAM 的最大允許負載將得到配置。如果其中一個值在 Central Node 和/或 Sensor 伺服器上被超出，則在為具有"**資深安全員**"、"**安全官**"和"**管理員**"角色的使用者提供的應用程式 Web 介面的"**控制板**"部分的上部會顯示一個黃色警告框。

設定 SNMP 協定連線

您可以將有關 Central Node 和 Sensor 伺服器上的 CPU 和 RAM 負載的資訊傳送到支援SNMP 協定的外部系統。為此，您必須配置協定的連線。

如果 Central Node 元件被部署為叢集，則有關叢集中每個伺服器的 CPU 和 RAM 負載的資料將被傳送到外部系統。

若要在 Central Node 伺服器上設定 SNMP 協定連線：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**一般設定**子部分。

2. 在**SNMP**下面，選擇**使用 SNMP**核取方塊。

3. 在**協議版本**欄位中，選擇協定版本：

   - **v2c**

   - **v3**

4. 如果您選擇的是 **v2c** 協定版本，則在**社區字串**欄位中，輸入用於連線 Kaspersky Anti Targeted Attack Platform 的密碼。

5. 如果您選擇了 **v3**：

   a. 在**身分驗證協議**欄位中，選擇以下選項之一來檢查傳送到外部系統的資料的準確性和完整性：

      - **MD5**

      - **SHA256**

   b. 在**使用者名稱**欄位中，輸入使用者名稱。

   c. 在**密碼**欄位中，輸入身分驗證密碼。

   > 在**使用者名稱**和**密碼**欄位中配置的使用者名稱和密碼必須與在外部系統中建立帳戶時配置的使用者名稱和密碼相符。如果憑證不匹配，則無法建立連線。

d. 在**隱私權協議**欄位中，選擇加密類型：

- DES。
- AES。

e. 在**密碼**欄位中，輸入加密密碼。

> 在此欄位中配置的密碼必須與外部系統中配置的密碼相符。

Central Node 伺服器上的 SNMP 連線已配置。如果資料請求成功處理，外部系統的伺服器將顯示有關 Central Node 伺服器的 CPU 和 RAM 負載的資訊。

若要在 Sensor 伺服器上設定 SNMP 連線：

1. 透過 SSH 協定或終端機進入 Sensor 伺服器的管理主控台。
2. 當系統提示時，請輸入管理員使用者名稱，以及在安裝應用程式期間設定的密碼。
   顯示應用程式元件管理員功能表。
3. 請依照上述說明的步驟 2 至 5 進行操作。

Sensor 伺服器上的連線已設定。如果請求成功處理，外部系統的伺服器將顯示有關 Sensor 伺服器的 CPU 和 RAM 負載的資訊。

> 在分佈式解決方案和多組織用戶模式下，必須單獨設定每個 PCN、SCN 和 Sensor 伺服器的 SNMP 連線。

Kaspersky Anti Targeted Attack Platform 的 MIB 物件描述

下表提供了有關 Kaspersky Anti Targeted Attack Platform 的 MIB 物件的資訊。

有關 Central Node 和 Sensor 伺服器的硬碟、CPU 和 RAM 負載的資訊

有關 Central Node 和 Sensor 伺服器的硬碟、CPU 和 RAM 負載的資訊

象徵性名稱	敘述	物件識別碼（OID）
`dskTotal`	磁碟或分割區的總大小（KB）。	1.3.6.1.4.1.2021.9.1.6
`dskAvail`	磁碟上的可用空間（KB）。	1.3.6.1.4.1.2021.9.1.7
`dskUsed`	磁碟上的已使用空間（KB）。	1.3.6.1.4.1.2021.9.1.8
`dskPercent`	磁碟上已使用空間的百分比（%）。	1.3.6.1.4.1.2021.9.1.9
`laLoad`	1、5 和 15 分鐘的系統負載平均值。	1.3.6.1.4.1.2021.10.1.3
`memTotalReal`	總 RAM 大小（KB）。	1.3.6.1.4.1.2021.4.5

象徵性名稱	敘述	物件識別碼（OID）
`memAvailReal`	使用的 RAM 總量（KB）。	1.3.6.1.4.1.2021.4.6
`memTotalFree`	可用 RAM 總量（KB）。	1.3.6.1.4.1.2021.4.11

管理 Endpoint Agent 主機資訊

用作Endpoint Agent 元件的應用程式安裝在組織 IT 基礎架構中的各個電腦（以下也稱為"主機"）上。應用程式持續監控在這些主機上運行的處理程序、活動的網路連線和正在修改的檔案。

具有**資深安全員**、**安全官**、**安全稽核員**和**管理員**角色的使用者，可以在使用者對其資料具有存取權的租用戶之 Central Node 伺服器 Web 介面視窗的**Endpoint Agent**索引標籤上，評估從具有 Endpoint Agent 元件的主機接收資料的頻率。如果您使用分佈式解決方案和多組織用戶模式，PCN 伺服器的 Web 介面將顯示 PCN 及所有已連線 SCN 中具有 Endpoint Agent 元件的主機清單。

具有**管理員**角色的使用者可以為其有權存取資料的租用戶，設定顯示從具有 Endpoint Agent 的主機接收資料的頻率。

如果偵測到可疑的網路活動，具有**資深安全員**角色的使用者可針對其有權存取資料的租用戶，將任何具有 Kaspersky Endpoint Agent 的主機與網路隔離。在這種情況下，伺服器與 Central Node 元件和具有 Endpoint Agent 元件的主機之間的連線不會中斷。

為了在 Endpoint Agent 元件出現問題時提供支持，技術支援人員可能會要求您執行以下操作以進行偵錯（包括在技術支援模式下）：

- 啟動擴展診斷資訊的收集。
- 修改個體應用程式元件的設定。
- 修改用於儲存和傳送獲取的診斷資訊的設定。
- 配置要被攔截並儲存到檔案的網路流量。

技術支援人員會提供執行這些操作所需的所有資訊（步驟順序說明、要修改的設定、設定檔、指令碼、附加的命令列功能、偵錯模組、特定用途的實用程式和其他資源等），並會告知您出於偵錯目的所取得的資料的範圍。檢索到的診斷資訊儲存在使用者的電腦上。檢索到的資料不會自動傳送到卡巴斯基。

以上列出的操作只能在技術支援專家的指導和監督下進行。未按照本手冊或技術支援專家的說明變更應用程式設定，將會導致作業系統變慢或崩潰，降低電腦安全，並可能影響正在處理的資料的可用性和完整性。

在"Endpoint Agent"部分中選擇要管理的租戶

如果您使用的是分佈式解決方案和多組織用戶模式，在使用"**資產** → **Endpoint Agent**"部分之前，您必須選擇要檢視其資料的租用戶。

*若要選擇要在"**資產 → Endpoint Agent**"部分中管理的租用戶：*

1. 在應用程式 Web 介面功能表的上部，點擊租戶名稱旁的箭頭。
2. 在下拉清單中，選擇租戶。

所選租戶的資料將顯示。如果您想選擇其他租戶，請重複選擇租戶的步驟。

檢視獨立 Central Node 伺服器上具有 Endpoint Agent 元件的主機表

具有 Endpoint Agent 元件的主機表位於應用程式 Web 介面視窗的"**資產 → Endpoint Agent**"部分。

該表可以顯示以下資料：

- 主機數量和Endpoint Agent 元件的活動指示器：
  - **严重不活動**是很久以前從其收到最新資料的主機數量。
  - **警告**是長久以前從其收到最新資料的主機數量。
  - **正常活動**是最近從其收到最新資料的主機數量。
- **主機**—具有 Endpoint Agent 元件的主機名稱。
- **伺服器**—具有 Endpoint Agent 元件的主機所連線的伺服器名稱。
  如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄位。
- **IP**—安裝 Endpoint Agent 元件的電腦的 IP 位址。
- **作業係統**—安裝在具有 Endpoint Agent 元件的電腦上的作業系統版本。
- **產品授權**是用作 Endpoint Agent 元件的應用程式的產品授權金鑰的狀態。
- **版本**是充當 Endpoint Agent 元件角色的應用程式的版本。
- **活動** — Endpoint Agent 元件的活動指示器。可能值：
  - **正常活動**用於最近收到最新資料的主機。
  - **警告**用於很久以前從其收到最新資料的主機。
  - **严重不活動**用於非常久以前收到最新資料的主機。
- **最後一次連線**用於 Endpoint Agent 元件上次連線到 Central Node 伺服器時的日期和時間。

點擊表格中列的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **複製值到剪貼簿**。

檢視有關主機的資訊

若要檢視具有 Endpoint Agent 元件的主機的資訊：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。
2. 轉到"**Endpoint Agent**"索引標籤。
3. 選擇您想檢視資訊的主機。

   這將開啟一個視窗，其中包含有關主機的資訊。

此視窗包含以下資訊：

- 在**主機**部分：
  - **名稱**是具有 Endpoint Agent 元件的主機的名稱。
  - **IP** 是安裝 Endpoint Agent 元件的主機的 IP 位址。
  - **作業系統**是安裝了 Endpoint Agent 元件的主機上作業系統的版本。
  - **伺服器**—SCN 或 PCN 伺服器的名稱。僅在分散式解決方案和多組織用戶模式中顯示。
- 在**Endpoint Agent**部分：
  - **版本**是用作 Endpoint Agent 元件的應用程式版本。
  - **活動**是 Endpoint Agent 元件的活動指示器。可能值：
    - **正常活動**用於最近收到最新資料的主機。
    - **警告**用於很久以前從其收到最新資料的主機。
    - **严重不活動**用於非常久以前收到最新資料的主機。
  - **已連線到伺服器**—主機連線的 Central Node、SCN 或 PCN 伺服器的名稱。
  - **最後一次連線**—上次連線到 Central Node、SCN 或 PCN 伺服器的時間。
  - **產品授權金鑰狀態**是用作 Endpoint Agent 元件的應用程式的產品授權金鑰的狀態。

點擊具有主機名稱及其 IP 位址的連結可以執行以下操作：**複製值到剪貼簿**。

依主機名稱篩選並搜尋具有 Endpoint Agent 元件的主機

若要依主機名稱篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**主機**連結以開啟篩選配置視窗。
4. 如果您只想顯示隔離的主機，請選擇**僅顯示隔離的 Endpoint Agent**核取方塊。
5. 在下拉清單中，選擇以下篩選運算子之一：
   - **包含**
   - **不包含**
6. 在輸入欄位中，指定主機名稱的一個或多個字元。
7. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
8. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。
9. 點擊**套用**。

篩選配置視窗關閉。

表格將僅顯示與您設定的篩選條件相符的主機。

> 您可以同時使用多個篩選器。

根據已與網路隔離的 Endpoint Agent 元件篩選和搜尋主機

若要篩選或搜尋與網路隔離的具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**主機**連結以開啟篩選配置視窗。

4. 選擇**僅顯示隔離的 Endpoint Agent**核取方塊。

5. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

按 PCN 和 SCN 伺服器名稱篩選並搜尋具有 Endpoint Agent 元件的主機

如果使用分佈式解決方案和多組織用戶模式，您可以根據主機所連線的 PCN 和 SCN 伺服器的名稱篩選或尋找具有 Kaspersky Endpoint Agent 元件的主機。

若要按PCN 和 SCN 伺服器的名稱篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。

2. 轉到"**Endpoint Agent**"索引標籤。

   這將開啟主機表。

3. 點擊**伺服器**連結以開啟篩選配置視窗。

4. 選擇想要依其篩選或搜尋具有 Endpoint Agent 元件的主機的伺服器名稱旁的核取方塊。

5. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依電腦 IP 位址篩選並搜尋具有 Endpoint Agent 元件的主機

若要按在其上安裝應用程式的電腦的 IP 位址篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。

2. 轉到"**Endpoint Agent**"索引標籤。

   這將開啟主機表。

3. 點擊**IP**連結以開啟篩選配置視窗。

4. 在下拉清單中，選擇以下篩選運算子之一：

   - **包含**
   - **不包含**

5. 在輸入欄位中，指定電腦 IP 位址的一個或多個字元。您可以輸入 IPv4 格式的 IP 位址或子網路遮罩（例如，`192.0.0.1` 或 `192.0.0.0/16`）。

6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

7. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。

8. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依電腦上的作業系統版本篩選並搜尋具有 Endpoint Agent 元件的主機

若要根據安裝在電腦上的作業系統版本篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。

2. 轉到"**Endpoint Agent**"索引標籤。
   這將開啟主機表。

3. 點擊**作業係統**連結以開啟篩選設定視窗。

4. 在下拉清單中，選擇以下篩選運算子之一：

   - **包含**
   - **不包含**

5. 在輸入欄位中，指定作業系統版本的一個或多個字元。

6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

7. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。

8. 點擊**套用**。

   篩選配置視窗關閉。

表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依元件版本篩選並搜尋具有 Endpoint Agent 元件的主機

您可以按 Endpoint Agent 元件的角色中所使用的應用程式版本篩選主機。

若要按元件版本篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**版本**連結以開啟篩選設定視窗。
4. 在下拉清單中，選擇以下篩選運算子之一：
   - **包含**
   - **不包含**
5. 在輸入欄位中，指定用作 Endpoint Agent 元件的應用程式版本的一個或多個字元。
6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
7. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。
8. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依活動篩選並搜尋具有 Endpoint Agent 元件的主機

若要依其活動篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。

3. 點擊**活動**連結以開啟篩選配置視窗。
   選擇一個或多個活動指示器旁的核取方塊：

   - **正常活動**，如果您想尋找最近從其中接收到最後資料的主機。
   - **警告**，如果您想尋找前段時間從其中接收到最後資料的主機。
   - **严重不活動**，如果您想尋找很久以前從其中接收到最後資料的主機。

4. 點擊**套用**。

篩選配置視窗關閉。

表格將僅顯示與您設定的篩選條件相符的主機。

> 您可以同時使用多個篩選器。

為具有 Endpoint Agent 元件的主機快速建立篩選器

若要為具有 Endpoint Agent 元件的主機快速建立篩選器：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 執行下列操作以便將篩選條件快速新增至正在建立的篩選器：
   a. 將滑鼠遊標置於包含您希望將其作為篩選條件新增的表列值的連結上。
   b. 左鍵點擊。
      這將開啟要對值執行的操作清單。
   c. 在開啟的清單中，選擇下列其中一項操作：
      - **新增到篩選器**，如果您想將該值包含在篩選條件中。
      - **從篩選器中排除**，如果您想從篩選條件中排除該值。
4. 如果您想要新增多個篩選條件到正在建立的篩選器中，請執行操作以將每個篩選條件快速新增至正在建立的篩選器。

表格將僅顯示與您設定的篩選條件相符的主機。

為具有 Endpoint Agent 元件的主機重設篩選器

若要清除一個或多個篩選條件的 Endpoint Agent 主機篩選器：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
3. 點擊您想要清除其篩選條件的表列標題右側的 ☒。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   表格將僅顯示與您設定的篩選條件相符的主機。

配置 Endpoint Agent 元件的活動指示器

具有**管理員**角色的使用者可以定義被用作 Endpoint Agent 元件的應用程式的不活動持續時間如何被視為正常、低或極低，並且可以配置應用程式的活動指示器。具有**安全稽核員**角色的使用者可以檢視元件活動指示器的設定。具有**資深安全員**或者**安全官**角色的使用者可以在應用程式 Web 介面的“**Endpoint Agent**”部分中 Endpoint Agent 元件表的“**活動**”欄位中檢視您為 Endpoint Agent 元件配置的活動指示器。

要配置 Endpoint Agent 元件的活動指示器：

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分的**Endpoint Agent**子部分。
2. 在該部分名稱下的欄位中，輸入您想要顯示為**警告**和**严重不活動**的具有 Endpoint Agent 元件的主機處於非活動狀態的天數。

   預設值為 1 和 7。
3. 點擊**套用**。

Endpoint Agent 元件的活動指示器已配置。

刪除具有 Endpoint Agent 元件的主機

若要從**Endpoint Agent**表中刪除一台或多台主機：

1. 在應用程式 Web 介面視窗中，選擇**資產**區段。
2. 前往**Endpoint Agent**索引標籤。

3. 選擇要刪除的一台或多台主機旁的核取方塊。您可以透過選擇包含列標題的行中的核取方塊來選擇所有主機。

   控制面板出現在視窗的下部。

4. 點擊**刪除**。

5. 這將開啟操作確認視窗；在該視窗中，點擊**是**。

選定的主機將會被從**Endpoint Agent**表中移除。

主機移除後，Kaspersky Anti Targeted Attack Platform 的 Web 介面會發生以下變更：

- 您無法為已移除的主機建立工作、阻止規則或網路隔離規則。
- 如果先前為主機建立了阻止規則，則主機移除後，其在規則視窗中的名稱（**阻止於**欄位）會被隱藏。該規則繼續適用。

  如果該主機重新連線到 Central Node 伺服器，主機名稱將在**阻止於**欄位中還原，阻止規則將再次套用至該主機。

- 如果先前為主機建立了網路隔離規則，則該規則將繼續套用，直到規則中指定的時間到期。

  當該主機重新連線到 Central Node 時，該規則將會重新套用到該主機。

- 遠端主機上隔離物件的中繼資料將從Kaspersky Anti Targeted Attack Platform 隔離區中刪除。

  當該主機重新連線到 Central Node 伺服器時，Kaspersky Anti Targeted Attack Platform 隔離區中物件的中繼資料**不會**還原。您可以透過在命令列或卡巴斯基安全管理中心中清除主機上的隔離區來避免填滿隔離區。有關詳細資訊，請參閱您在 Endpoint Agent 元件角色中使用的應用程式的協助。

- 如果物件僅在一台主機上被**隔離檔案**工作隔離，且該主機已移除，則工作視窗中的**還原所有**按鈕將處於非活動狀態，因為檔案無法在已移除的主機上還原。

以被移除主機的名稱進行事件搜尋仍然可用。

自動刪除不活動的主機

您可以啟用或停用從**Endpoint Agent**表中自動移除不活動的主機。非活動主機是指在設定的時間內未連線到 Central Node 伺服器的主機。

*若要啟用或停用從**Endpoint Agent**表中自動移除不活動的主機：*

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分的**Endpoint Agent**子部分。

2. 在**自動刪除不活動的主機**下面，執行下列操作：

   - 如果您想啟用此功能，請將**刪除主機**切換開關移至**已啟用**。

   - 如果您想啟用此功能，請將**刪除主機**切換開關移至**已停用**。

3. 如果您啟用了此功能，請在**在此之後刪除**欄位中，指定未連線到 Central Node 元件的主機必須被視為不活動的天數。

   最小值為 1，最大值為 365。

自動移除不活動主機啟用或停用。

如果在**在此之後刪除**欄位中指定的值小於在**活動指示器**下面的**警告**和/或**严重不活動**欄位中指定的值，則主機被移除的時間早於在**控制板**部分中顯示不活動警告的時間。

主機移除後，Kaspersky Anti Targeted Attack Platform 的 Web 介面會發生以下變更：

- 您無法為已移除的主機建立工作、阻止規則或網路隔離規則。
- 如果先前為主機建立了阻止規則，則主機移除後，其在規則視窗中的名稱（**阻止於**欄位）會被隱藏。該規則繼續適用。

  如果該主機重新連線到 Central Node 伺服器，主機名稱將在**阻止於**欄位中還原，阻止規則將再次套用至該主機。
- 如果先前為主機建立了網路隔離規則，則該規則將繼續套用，直到規則中指定的時間到期。

  當該主機重新連線到 Central Node 時，該規則將會重新套用到該主機。
- 遠端主機上隔離物件的中繼資料將從Kaspersky Anti Targeted Attack Platform 隔離區中刪除。

  當該主機重新連線到 Central Node 伺服器時，Kaspersky Anti Targeted Attack Platform 隔離區中物件的中繼資料**不會**還原。您可以透過在命令列或卡巴斯基安全管理中心中清除主機上的隔離區來避免填滿隔離區。有關詳細資訊，請參閱您在 Endpoint Agent 元件角色中使用的應用程式的協助。
- 如果物件僅在一台主機上被**隔離檔案**工作隔離，且該主機已移除，則工作視窗中的**還原所有**按鈕將處於非活動狀態，因為檔案無法在已移除的主機上還原。

以被移除主機的名稱進行事件搜尋仍然可用。

配置與 Sandbox 元件的整合

您可以將一個 Sandbox 元件連線到多個 Central Node 元件。

以下步驟用於設定 Sandbox 元件和 Central Node 元件間的連線：

1. **建立連線到 Sandbox 元件的請求**

   您可以在管理員帳戶下的應用程式 Web 介面中建立請求。如果伺服器上安裝了多個 Central Node 元件，則需要為每個具有要連線到 Sandbox 元件的 Central Node 元件的伺服器建立請求。如果 Central Node 元件被部署為叢集，您可以從叢集中的任何伺服器建立連線請求。

2. **在 Sandbox Web 介面中處理連線請求**

   您可以接受或拒絕每個請求。

如果您要將多個 Sandbox 元件連線到單個 Central Node 元件，請確保您連接的 Sandbox 元件具有相同的用於掃描物件的作業系統集，以及同時執行的虛擬機的最大數量。

配置連線後，Sandbox 伺服器需要 5 到 10 分鐘才能準備好運作。在此期間，應用程式 Web 介面的**系統健康**視窗會顯示警告：*標準配置出現問題*。當伺服器準備好運行時，警告就會消失。

檢視具有 Sandbox 元件的伺服器表

具有**安全稽核員**角色的使用者可以檢視具有 Sandbox 元件的伺服器表。

具有 Sandbox 元件的伺服器表位於應用程式 Web 介面視窗的**Sandbox 伺服器**區段中，位於**伺服器**索引標籤上。

憑證指紋欄位顯示 Central Node 伺服器的 TLS 憑證指紋。

伺服器清單表包含以下資訊：

- **IP 和名稱** — 具有 Sandbox 元件的伺服器的 IP 位址或完全限定網域名稱。
- **憑證指紋** — 具有 Sandbox 元件的伺服器的憑證指紋。
- **授權** — 連線到 Sandbox 元件的請求狀態。
- **狀態** — 與 Sandbox 元件的連線狀態。

具有**安全官**角色的使用者無法檢視具有 Sandbox 元件的伺服器表。

使用 Sandbox 元件建立連線到伺服器的請求

若要透過應用程式 Web 介面建立使用 Sandbox 元件連線到伺服器的請求：

1. 在應用程式 Web 介面視窗中，選擇 **Sandbox 伺服器**區域。
2. 在視窗的右上角，點擊**新增**按鈕。
   這將開啟**Sandbox 伺服器連線**視窗。
3. 在**IP**欄位中，指定要連線的 Sandbox 元件所在伺服器的 IP 位址。
4. 點擊**獲取憑證指紋**。
   工作區顯示具有 Sandbox 元件的伺服器憑證的指紋。
5. 將取得的憑證指紋與 Sandbox Web 介面中**KATA 授權**區域內**憑證指紋**欄位所顯示的指紋進行比較。
   如果憑證指紋匹配，請執行說明的後續步驟。

   如果憑證指紋不匹配，確認該連線不是最佳選擇。確認**IP**欄位中的 IP 位址正確。

6. 在**名稱**欄位中，指定將在 Central Node 元件的 Web 介面中顯示的 Sandbox 元件名稱。
   此名稱與安裝 Sandbox 的主機名稱無關，可任意指定。

7. 如果要在連線後立即啟動與 Sandbox 的連線，請選取**啟用**核取方塊。

8. 點擊**新增**。

連線請求將顯示在 Sandbox 元件的 Web 介面中，您可以在其中接受、拒絕或撤銷它。

啟用和停用與 Sandbox 元件的連線

若要啟動與 Sandbox 元件的連線或停用它：

1. 在應用程式 Web 介面視窗中，選擇 **Sandbox 伺服器**區域。
   將顯示具有 Sandbox 元件的伺服器表。

2. 在**狀態**欄中包含相關伺服器的列上，執行下列操作之一：

   - 如果要啟動與 Sandbox 元件的連線，請將切換開關設定為**已啟用**。

   - 如果要停用與 Sandbox 元件的連線，請將切換開關設定為**已停用**。

3. 點擊**套用**。

與 Sandbox 元件的連線將變為活動狀態或將被停用。

刪除與 Sandbox 元件的連線

若要刪除與 Sandbox 元件的連線：

1. 在應用程式 Web 介面視窗中，選擇 **Sandbox 伺服器**區域。
   這將顯示安裝了 Sandbox 元件的電腦表。

2. 選擇包含您想要刪除的 Sandbox 元件連線的行中的核取方塊。

3. 在視窗的右上角，點擊**刪除**按鈕。

4. 在確認視窗中，點擊**是**。

將刪除與 Sandbox 元件的連線。

選擇掃描 Sandbox 中的物件時要使用的作業系統

您可以選擇一組作業系統，它們將用於產生使用 Sandbox 元件掃描物件的工作。在 Sandbox 伺服器上，您必須安裝具有作業系統的虛擬機，且作業系統須與設定的作業系統集相符。

若要選擇作業系統集：

1. 在應用程式 Web 介面視窗中，選擇**Sandbox 伺服器**區域。
2. 前往**設定**索引標籤。
3. 在**作業係統集合**下面，選擇以下選項之一：
   - **Windows 7**、**Windows 10**。
   - **CentOS 7.8**、**Windows 7**、**Windows 10**。
   - **Astra Linux 1.7**、**Windows 7**、**Windows 10**。
   - **自訂**。
4. 如果您選擇了**自訂**，在**集合組成**下面，選擇要包含在該集合中的作業系統旁的核取方塊。

   如果 Sandbox 伺服器上安裝了具有這些作業系統的虛擬機，則自訂作業系統將顯示在清單中。預設作業系統始終顯示在清單中，但如果未部署執行這些作業系統的虛擬機，則**未知**狀態會顯示在作業系統名稱旁邊。

Kaspersky Anti Targeted Attack Platform 將根據選定的集合建立掃描 Sandbox 中物件的工作。

如果 Sandbox 伺服器上安裝的作業系統集與 Central Node 伺服器上選擇的作業系統集不匹配，則該 Sandbox 伺服器不會傳送物件以進行掃描。如果有多個 Sandbox 伺服器連線到 Central Node 伺服器，則應用程式會將物件傳送到其安裝的作業系統與 Central Node 上選取的集合相符的 Sandbox 伺服器。

您可以在使用應用程式的過程中變更作業系統集。在這種情況下，您需要確保 Sandbox 伺服器的配置符合硬體需求。

在分佈式解決方案和多組織用戶模式下，PCN 伺服器上配置的作業系統集的設定不會被套用於連線到該 PCN 伺服器的 SCN 伺服器。您可以單獨為每個 PCN 和 SCN 伺服器選擇作業系統集。

從 Endpoint Agent 主機手動傳送檔案以供 Sandbox 掃描

您可以啟用並停用從具有 Endpoint Agent 元件的主機手動傳送檔案以供 Sandbox 元件掃描。如果啟用此功能，具有 Endpoint Agent 元件的主機的使用者可以使用 Sandbox 掃描任何他們認為不安全的檔案。

如果將 Kaspersky Endpoint Security for Windows 和/或 Kaspersky Endpoint Security for Linux 應用程式用作 Endpoint Agent 元件，並且為這些元件配置了與 Kaspersky Anti Targeted Attack Platform 的整合，則此功能可用。

傳送檔案進行掃描涉及以下步驟：

1. 在 Kaspersky Anti Targeted Attack Platform Web 介面中允許從具有 Endpoint Agent 元件的主機手動傳送檔案，以便由 Sandbox 元件進行掃描。
2. 傳送檔案以供 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 中的 Sandbox 元件掃描。

根據掃描結果，Kaspersky Anti Targeted Attack Platform 可能會在警示資料庫中記錄警示。這些警示的詳細資訊顯示在“**按攻擊向量分類的警示**”小工具中。

在分佈式解決方案和多租戶模式下，您必須在每個要使用 Sandbox 元件的 Central Node 伺服器上啟用手動傳送檔案以供 Sandbox 元件掃描的功能。如果 Central Node 元件被部署為叢集，您可以在叢集中的任何伺服器上啟用該功能。

如果您僅使用 KATA 功能（KATA 產品授權金鑰），則在 Kaspersky Anti Targeted Attack Platform Web 介面中，“**Endpoint Agent**”部分顯示已傳送檔案以供 Sandbox 元件掃描的主機清單。您可以檢視此清單和有關所選主機的資訊。

啟用和停用從 Endpoint Agent 主機手動傳送檔案以供 Sandbox 掃描

若要啟用或停用手動傳送要由 Sandbox 元件掃描的檔案：

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分的**Endpoint Agent**子部分。
2. 在“**手動將檔案從主機傳送到 Sandbox 進行分析**”下，執行以下操作：
   - 設定“**傳送檔案**”撥動開關至“**已啟用**”，如果您想啟用手動傳送檔案以供 Sandbox 元件掃描。
     預設情況下啟用此功能。
   - 設定“**傳送檔案**”撥動開關至“**已停用**”，如果您想要停用手動傳送檔案以供 Sandbox 元件掃描。
3. 點擊**套用**。

啟用或停用從 Endpoint Agent 主機手動傳送檔案以供 Sandbox 元件掃描。

配置與外部系統的整合

您可以設定 Kaspersky Anti Targeted Attack Platform 與外部系統的整合，以掃描儲存在這些系統中的檔案。它們的掃描結果將顯示在警示表中。郵件 Sensor也可以充當外部系統。

如果使用分佈式解決方案和多組織用戶模式，則需要設定外部系統與 PCN 或 SCN 伺服器的整合，以便從該系統掃描資料。

Kaspersky Anti Targeted Attack Platform 與外部系統的整合涉及以下過程：

1. **輸入整合設定並從外部系統建立整合請求。**

   有關輸入郵件感應器整合設定的更多詳情，請參閱 Kaspersky Secure Mail Gateway 說明 或 Kaspersky Security for Linux 郵件伺服器說明。

   若要整合其他外部系統，請使用 REST API。

2. **確認 Kaspersky Anti Targeted Attack Platform 的整合**

   外部系統必須使用唯一憑證在具有 Central Node 元件的伺服器上進行授權。如果是這種情況，將在 Kaspersky Anti Targeted Attack Platform 的介面中顯示單個整合請求。若要連線具有相同 IP 位址的多個外部系統，您必須為每個外部系統使用唯一憑證。

   使用一張憑證時，您只能設定與一個外部系統的整合。

3. **檢查外部系統和 Kaspersky Anti Targeted Attack Platform 之間的連線**

檢視外部系統表

外部系統表位於應用程式 Web 介面視窗的**外部系統**部分。表包含以下資訊：

- **Sensor** — 外部系統伺服器的 IP 位址或網域名稱。
- **類型** — 外部系統的類型（郵件感應器或其他系統）。
- **名稱** — 不是郵件感應器的整合外部系統的名稱。

  郵件感應器的此列中顯示破折號。
- **ID** — 外部系統的 ID。
- **憑證指紋** — 外部系統所在伺服器的 TLS 憑證指紋，用於與託管 Central Node 元件的伺服器建立加密連線。

  具有 Central Node 元件的伺服器的憑證指紋顯示在視窗上方的**憑證指紋**欄位中。
- **狀態** — 整合請求的狀態。

在分佈式解決方案和多租戶模式下，該表僅顯示已連線到您正在管理其 Web 介面的 Central Node 伺服器的外部系統資訊。

處理來自外部系統的請求

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

要處理來自外部系統的整合請求：

1. 在應用程式 Web 介面視窗中選擇"**外部系統**"區域。

   伺服器清單表顯示已連線的外部系統，以及從外部系統與 Kaspersky Anti Targeted Attack Platform 整合的請求。

2. 在包含整合請求的行中，執行下列操作之一：

   - 如果要配置與外部系統的整合，請點擊**接受**按鈕。
   - 如果您不想配置與外部系統的整合，請點擊**拒絕**按鈕。

3. 在確認視窗中，點擊**是**。

   將處理來自外部系統的整合請求。

從允許整合的清單中移除外部系統

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

在接受來自外部系統的整合請求後，可以從允許整合的清單中移除它。如果是這種情況，Kaspersky Anti Targeted Attack Platform 和外部系統之間的連線將會終止。

若要從允許整合的系統清單中移除外部系統：

1. 在應用程式 Web 介面視窗中選擇"**外部系統**"區域。

   伺服器清單顯示已新增的外部系統以及從外部系統與 Kaspersky Anti Targeted Attack Platform 整合的請求。

2. 在包含來自想要移除的外部系統整合請求的行中，點擊**刪除**按鈕。

3. 在確認視窗中，點擊**是**。

   外部系統將從允許整合的清單中移除。

配置處理來自郵件感應器的流量的優先順序

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

您可以啟用或停用處理來自郵件感應器的流量的最高優先順序。

若要啟用或停用處理來自郵件感應器的流量的最高優先順序：

1. 在應用程式 Web 介面視窗中選擇“**外部系統**”區域。

2. 執行以下操作之一：

   - 如果您想啟用處理來自郵件感應器的流量的最高優先順序，請開啟**最大掃描優先順序**參數名稱旁邊的切換開關。

   - 如果您想要停用處理來自郵件感應器的流量的最高優先順序，請關閉**最大掃描優先順序**參數名稱旁邊的切換開關。

將配置處理來自郵件感應器的流量的優先順序。

配置與 Kaspersky Managed Detection and Response 的整合

Kaspersky Managed Detection and Response（以下簡稱“MDR”）可偵測並防止用戶端基礎架構中的詐騙行為。MDR 提供持續的受管理防護，使組織能夠自動發現難以偵測的威脅，同時讓IT 安全人員專注於解決需要他們參與的問題。

Kaspersky Anti Targeted Attack Platform 取得資料並使用卡巴斯基安全網路串流將其傳送至 Kaspersky Managed Detection and Response。因此，參與 KSN 對於配置與 MDR 的整合很有必要。

只有當至少有一個 KATA 或EDR產品授權處於活動狀態時，才能與 MDR 整合。如果僅在應用程式中新增產品授權金鑰（僅 KATA 或僅EDR），則統計資訊僅限於該產品授權提供的功能。如果兩個產品授權金鑰都被新增到應用程式中，則會傳送完整的統計資料。

在配置 Kaspersky Anti Targeted Attack Platform 與 MDR 應用程式的整合之前，您必須從MDR 入口網站下載包含設定檔的壓縮檔案。

啟用 MDR 整合

確保已在應用程式中新增有效的產品授權金鑰並設定參與 KSN。否則 MDR 整合不可用。

若要啟用與 MDR 的整合：

1. 利用管理員帳戶登入應用程式 Web 介面。

2. 選擇**設定**部分的**KSN/KPSN 和 MDR**子部分。

3. 在**MDR 整合**下面，點擊**上傳**上傳設定檔。

   這將開啟檔案選擇視窗。

4. 選擇您在 MDR 入口網站註冊期間下載的壓縮檔案，然後點擊**開啟**。

視窗中將顯示有關 MDR 產品授權的以下資訊：

- **序號**。
- **到期日期**。
- **剩餘天數**。

與 MDR 的整合被啟用。在設定檔中配置的整合設定將被套用於所有連線的 Sensor 元件。MDR 開始使用透過 KSN 串流傳送的警示統計資料。

停用 MDR 整合

若要停用與 MDR 的整合：

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 選擇**設定**部分的**KSN/KPSN 和 MDR**子部分。
3. 在**MDR 整合**下面，點擊**刪除檔案**。
4. 在確認視窗中，點擊**是**。

設定檔將被刪除，MDR 整合將被停用。統計資訊仍會被傳送到 KSN 伺服器，但 MDR 不使用此資訊。

替換 MDR 設定檔

替換 MDR 設定檔：

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 選擇**設定**部分的**KSN/KPSN 和 MDR**子部分。
3. 在**MDR 整合**下面，點擊**替代檔案**。
   這將開啟檔案選擇視窗。
4. 選擇包含設定檔的新壓縮檔案，然後點擊**開啟**。
   MDR 產品授權資訊在應用程式 Web 介面中已更新。

設定檔被替換。新的整合設定將套用於所有連線的 Sensor 元件。

配置與 SIEM 系統的整合

Kaspersky Anti Targeted Attack Platform 可以在應用程式 Web 介面中發布有關使用者操作的資訊，並使用 Syslog 協定向組織中的 *SIEM 系統*發出警示。

您可以使用 TLS 加密進行資料傳輸。

如果您已將 Central Node 和 Sensor 元件部署為叢集，則可以使用下列選項之一配置與外部系統的高可用性整合：

- 使用輪詢調度演算法功能。
- 配置外部系統的設定，以便在發生網路錯誤時外部系統在叢集伺服器的 IP 位址之間進行切換。

若要使用輪詢調度演算法功能配置與外部系統的高可用性整合：

1. 在 Central Node 叢集對應網域的 DNS 伺服器上設定輪詢調度演算法。
2. 在郵件伺服器設定中指定此網域名稱。

   與外部系統的整合是基於網域名稱配置的。外部系統將與叢集中的隨機伺服器進行通訊。如果該伺服器發生故障，外部系統將與叢集中另一台健康的伺服器進行通訊。

觀看視頻教程，了解如何配置與 SIEM 系統的整合。您可以在幫助頁面（見下方）播放視頻，或點擊連結 https://youtu.be/xONoDN924Lk?si=AZ7pk7j8VE9xBVXf。

https://www.youtube.com/watch?v=xONoDN924Lk

配置 Central Node 以將 KATA 和 KEDR Expert 事件匯出到 KUMA

啟用和停用事件資訊記錄到遠端日誌

您可以設定有關 Web 介面中使用者操作的資訊的記錄以及遠端日誌中的警示。日誌檔案被儲存在安裝了 SIEM 系統的伺服器上。若要寫入遠端日誌，您必須設定與 SIEM 系統的整合。

若要啟用或停用在 Web 介面中記錄有關使用者操作的資訊以及向遠端日誌發出警示：

1. 在應用程式 Web 介面視窗，選擇**設定**部分的**SIEM 系統**子部分。
2. 如果要啟用/停用將 Web 介面中的使用者操作資訊記錄到遠端日誌，請執行下列其中一項操作：
   - 如果您想要在 Web 介面中啟用有關使用者操作的資訊記錄，請選擇**使用者活動**核取方塊。
   - 如果您想要停用在 Web 介面中記錄有關使用者操作的資訊，請清除**使用者活動**核取方塊。

3. 如果要啟用/停用將有關警示的資訊記錄到遠端日誌，請執行下列其中一項操作：

   - 如果要啟用警示資訊記錄，請選擇**偵測**核取方塊。
   - 如果您想停用警示資訊記錄，請清除**偵測**核取方塊。

   您可以同時選擇兩個核取方塊。

4. 點擊視窗下部的**套用**。

遠端日誌中的資訊記錄已啟用或停用。

> 具有**安全稽核員**角色的使用者只能檢視有關遠端日誌記錄設定的資訊。

配置 SIEM 系統整合的主要設定

要配置 SIEM 系統整合的主要設定：

1. 在應用程式 Web 介面視窗，選擇**設定**部分的**SIEM 系統**子部分。
2. 選擇“**使用者活動**”和/或“**偵測**”核取方塊。
   您可以選擇一個核取方塊或同時選擇兩個核取方塊。
3. 在**主機/IP**欄位中，輸入您的 SIEM 系統伺服器的 IP 位址或主機名稱。
4. 在**連接埠**欄位中，輸入用於連線到您的 SIEM 系統的連接埠號。
5. 在**協議**欄位中，選擇**TCP**或 **UDP**。
6. 在**主機 ID**欄位中，輸入主機 ID。具有該 ID 的主機被指定為 SIEM 系統日誌中的警示來源。
7. 在**心跳**欄位中，輸入向 SIEM 系統傳送訊息的間隔。
8. 點擊視窗下部的**套用**。

將配置與 SIEM 系統整合的主要設定。

> 具有**安全稽核員**角色的使用者只能檢視有關 SIEM 系統整合設定的資訊。

上傳 TLS 憑證

若要載入用來加密與 SIEM 系統的連線的 TLS 憑證：

1. 在應用程式 Web 介面視窗，選擇**設定**部分的**SIEM 系統**子部分。
2. 在**TLS 加密**部分，點擊**上傳**按鈕。
   這將開啟檔案選擇視窗。
3. 選擇要下載的 TLS 憑證檔案，然後點擊**開啟**按鈕。
   這將關閉檔案選擇視窗。
   TLS 憑證被新增到應用程式中。
4. 點擊視窗下部的**套用**。

上傳的 TLS 憑證將用於加密與 SIEM 系統的連線。

啟用和停用與 SIEM 系統的連線的 TLS 加密

若要啟用或停用與 SIEM 系統的連線的 TLS 加密：

1. 在應用程式 Web 介面視窗，選擇**設定**部分的**SIEM 系統**子部分。
2. 選擇**使用者活動**和/或**警示**核取方塊。
   您可以選擇一個核取方塊或同時選擇兩個核取方塊。
3. 在**TLS 加密**部分，請執行下列其中一項操作：
   - 如果您想啟用與 SIEM 系統的連線的 TLS 加密，請開啟**TLS 加密**參數名稱旁邊的切換開關。
   - 如果您想要停用與 SIEM 系統的連線的 TLS 加密，請關閉**TLS 加密**參數名稱旁邊的切換開關。

   > 只有在載入了TLS 憑證的情況下，**TLS 加密**設定的名稱旁邊的切換開關才可用。

4. 點擊視窗下部的**套用**。

將啟用或停用與 SIEM 系統的連線 TLS 加密。

有關警示的 syslog 郵件的內容和屬性

有關每個警示的資訊在單獨的 syslog 類別（syslog 工具）中傳輸，系統未使用該類別來傳遞來自其他來源的訊息。有關每個警示的資訊以 CEF 格式作為單獨的 syslog 郵件傳輸。如果警示是由針對性攻擊分析器模組產生的，則有關該警示的資訊將以 CEF 格式作為多個單獨的 syslog 訊息傳輸。

有關警示的 syslog 郵件的預設最大大小為 32 KB。超過最大大小的郵件最後會被截斷。

有關警示的每個系統日誌訊息的標題包含以下資訊：

- 格式化版本。

  目前版本號：`0`。目前欄位值：`CEF:0`。

- 供應商。

  目前欄位值：`AO Kaspersky Lab`。

- 應用程式名稱。

  目前欄位值：`Kaspersky Anti Targeted Attack Platform`。

- 應用程式版本

  目前欄位值：7.1.1.531。

- 偵測類型。

  見下表。

- 活動名稱。

  見下表。

- 偵測重要性。

  允許的欄位值：低、中、高或`0`（對於心跳訊息）。

- 其他資訊。

  例如：
  `CEF:0|AO Kaspersky Lab| Kaspersky Anti Targeted Attack Platform |7.1.1.531|url_web| 來自偵測的 Web 的 URL |Low|`

有關偵測的 syslog 訊息主體與顯示在應用程式 Web 介面中的偵測資訊相符。所有欄位均以“`<key>=<value>`”格式顯示。根據網路流量或郵件流量中是否發生偵測，以及根據產生偵測的技術，可以在系統日誌訊息的主體中傳輸各種金鑰。如果該值為空，則不傳輸參數。

參數以及訊息中包含的值顯示在下表中。

偵測類型	偵測名稱和說明	參數及其值的描述
file_web	偵測到來自 Web 的檔案 在網路流量中偵測到檔案。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <偵測的日期和時間，UTC>。 • dst = <目的地 IP 位址>。 • dpt = <目的地連接埠>。 • src = <來源 IP 位址>。 • spt = <來源連接埠>。 • shost = <偵測到檔案的主機名稱>。 • suser = <使用者名稱>。 • fName = <復合物件內檔案的名稱>。 • fsize = <復合物件中檔案的大小（以位元組為單位）>。 • fileType = <復合物件中檔案的格式>。 • fileHash = <復合物件中檔案的 MD5 雜湊>。 • KasperskyLabKATAcompositeFilePath = <復合物件的名稱>。 • KasperskyLabKATAcompositeFileSize = <復合物件的總大小（以位元組為單位）>。 • KasperskyLabKATAcompositeFileHash = <復合物件的 MD5 雜湊>。 • KasperskyLabKATAfileSHA256 = <復合物件的 SHA256 雜湊>。 • cs2 = <用於偵測檔案的技術>。 • cs3Label = <偵測到檔案的虛擬機的名稱>（僅限 Sandbox 元件）。 • cs1 = <根據卡巴斯基類別偵測到的物件的名稱>。 • cs3 = <用於掃描檔案的資料庫的版本>。 • app = <應用程式層協議名稱>（HTTP(S) 或 FTP）。 • requestMethod = <HTTP 請求方法>（僅適用於 HTTP(S) 協定）。 • requestClientApplication = <用戶端電腦的使用者代理>（僅適用於 HTTP(S) 協定）。 • request = <偵測到的物件的 URL>（僅適用於 HTTP(S) 協定）。 • requestContext = <HTTP referer 標頭>（僅適用於 HTTP(S) 協定）。
file_mail	偵測到郵件的檔案 在郵件流量中偵測到檔案。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <警示的日期和時間，UTC>。 • fName = <復合物件內檔案的名稱>。 • fsize = <復合物件中檔案的大小（以位元組為單位）>。 • fileType = <復合物件中檔案的格式>。 • fileHash = <復合物件中檔案的 MD5 雜湊>。 • KasperskyLabKATAcompositeFilePath = <復合物件的名稱>。 • KasperskyLabKATAcompositeFileSize = <復合物件的總大小（以位元組為單位）>。 • KasperskyLabKATAcompositeFileHash = <復合物件的 MD5 雜湊>。 • KasperskyLabKATAfileSHA256 = <復合物件的 SHA256 雜湊>。 • KasperskyLabKATAmailEnvelopeFrom = <寄件者電子郵件地址>（來自 Received 標頭）。 • KasperskyLabKATAmailFor = <收件者電子郵件地址>（來自 Received 標頭）。 • KasperskyLabKATAmailRecievedFromIp = <郵件傳遞鏈中第一台伺服器的 IP 位址>（來自 Received 標頭）。 • cs2 = <用於偵測檔案的技術>。 • cs3Label = <偵測到檔案的虛擬機的名稱>（僅限 Sandbox 元件）。 • cs1 = <根據卡巴斯基類別偵測到的物件的名稱>。 • cs3 = <用於掃描檔案的資料庫的版本>。 • externalId = <郵件訊息 ID>。 • suser = <寄件者的電子郵件信箱>。 • duser = <收件者的電子郵件信箱>。 • msg = <郵件主旨>。
ids	偵測到的 IDS 事件 偵測由入侵偵測系統模組產生。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • requestMethod = <HTTP 請求方法>（僅適用於 HTTP(S) 協定）。 • requestClientApplication = <用戶端電腦的使用者代理>（僅適用於 HTTP(S) 協定）。 • rt = <警示的日期和時間，UTC>。 • dst = <目的地 IP 位址>。 • dpt = <目的地連接埠>。 • src = <來源 IP 位址>。 • spt = <來源連接埠>。 • proto = <傳輸級協定的名稱>（TCP 或 UDP）。 • cs1 = <根據卡巴斯基類別偵測到的物件的類型>。 • cs2Label = <IDS 規則的名稱>。 • cs2 = <IDS 規則的編號>。 • cs3 = <入侵偵測系統模組資料庫版本>。 • requestMethod = <HTTP 請求方法>（僅適用於 HTTP 協定）。

偵測類型	偵測名稱和說明	參數及其值的描述
		• requestClientApplication = <用戶端電腦的使用者代理>（僅適用於 HTTP 協定）。 • request = <偵測到的物件的 URL>。
url_web	偵測到 Web 的 URL 網路流量中的 URL 信譽技術或 Sandbox 產生了一條警示。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <偵測的日期和時間，UTC>。 • dst = <目的地 IP 位址>。 • dpt = <目的地連接埠>。 • src = <來源 IP 位址>。 • spt = <來源連接埠>。 • shost = <偵測到檔案的主機名稱>。 • suser = <使用者名稱>。 • cs1 = <偵測到的物件的 URL 所屬的分類清單>。 • requestMethod = <HTTP 請求方法>。 • requestClientApplication = <用戶端電腦的使用者代理>。 • request = <偵測到的物件的 URL>。 • requestContext = <HTTP referer 標頭>。 • reason = <HTTP 回應代碼>。
url_mail	偵測到郵件的 URL 郵件流量中的 URL 信譽技術或 Sandbox 產生了一條警示。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <警示的日期和時間，UTC>。 • externalId = <郵件訊息 ID>。 • suser = <寄件者的電子郵件信箱>。 • duser = <收件者的電子郵件信箱>。 • KasperskyLabKATAmailEnvelopeFrom = <寄件者電子郵件地址>（來自 Received 標頭）。 • KasperskyLabKATAmailFor = <收件者地址>（來自 Received 標頭）。 • KasperskyLabKATAmailRecievedFromIp = <郵件傳遞鏈中第一台伺服器的 IP 位址>（來自 Received 標頭）。 • msg = <郵件主旨>。 • request = <偵測到的物件的 URL>。 • cs2 = <用於產生警示的技術>（ Sandbox 或 URL 信譽）。 • cs3Label = <偵測到檔案的虛擬機名稱>（僅適用於 Sandbox ）。 • cs1 = <根據卡巴斯基分類偵測到的物件類型清單>（適用於 Sandbox 元件）或 <類別清單>（適用於 URL 信譽）。 • cs3 = <用於掃描檔案的資料庫版本>（僅適用於 Sandbox ）。
dns	偵測到 DNS 請求 DNS 流量中的 URL 信譽技術產生了一則警示。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <偵測的日期和時間，UTC>。 • dst = <目的地 IP 位址>。 • dpt = <目的地連接埠>。 • src = <來源 IP 位址>。 • spt = <來源連接埠>。 • shost = <偵測到檔案的主機名稱>。 • suser = <使用者名稱>。 • cs2 = <網域名稱所屬的 URL 類別清單>。 • requestMethod = <DNS 訊息類型>（請求或回應）。 • flexString1 = <來自 DNS 請求的記錄類型>。 • dhost = <來自 DNS 請求的主機名稱>。 • cs1 = <DNS 回應中的網域名稱清單>。

偵測類型	偵測名稱和說明	參數及其值的描述
file_endpoint	偵測到端點的檔案 使用者電腦上的 Endpoint Agent 元件產生了一條警示，並且該警示包含檔案。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <警示的日期和時間，UTC>。 • src = <來源 IP 位址>。 • shost = <偵測到檔案的主機名稱>。 • fName = <復合物件內檔案的名稱>。 • fsize = <復合物件中檔案的大小（以位元組為單位）>。 • fileType = <復合物件中檔案的格式>。 • fileHash = <復合物件中檔案的 MD5 雜湊>。 • KasperskyLabKATAcompositeFilePath = <復合物件的名稱>。 • KasperskyLabKATAcompositeFileSize = <復合物件的總大小（以位元組為單位）>。 • KasperskyLabKATAcompositeFileHash = <復合物件的 MD5 雜湊>。 • KasperskyLabKATAfileSHA256 = <復合物件的 SHA256 雜湊>。 • cs2 = <用於偵測檔案的技術>。 • cs3Label = <偵測到檔案的虛擬機的名稱>（僅限 Sandbox 元件）。 • cs1 = <根據卡巴斯基類別偵測到的物件的名稱>。 • cs3 = <用於掃描檔案的資料庫的版本>。 • app = <應用程式層級通訊協定的名稱>（HTTP(S) 或 FTP）。 • FilePath = <Endpoint Agent 電腦上檔案的路徑>。
iocScanning	IOC 在端點上絆倒 此警示是在使用 Windows Endpoint Agent 元件對主機執行 IOC 掃描時產生的。 如果您使用 KEDR 功能，則可以使用此類警示。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <警示的日期和時間，UTC>。 • src = <來源 IP 位址>。 • shost = <偵測到檔案的主機名稱>。 • cs1 = <產生警示的 IOC 檔案的名稱>。
taaScanning	TAA 在事件資料庫上絆倒 IOA 事件分析產生的偵測。 如果您使用 KEDR 功能，則可以使用此類偵測。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <警示的日期和時間，UTC>。 • shost= <產生偵測的主機名稱>。 • cs1 = <產生警示的 IOA 規則的名稱>。
yaraScanningEP	YARA 在端點上絆倒 此警示是在使用 Windows Endpoint Agent 元件對主機執行YARA 掃描時產生的。 如果您使用 KEDR 功能，則可以使用此類警示。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • eventId = <偵測 ID>。 • rt = <警示的日期和時間，UTC>。 • src = <來源 IP 位址>。 • shost= <產生警示的主機名稱>。 • cs1 = <產生警示的 YARA 規則的名稱>。
heartbeat	包含元件狀態的定期訊息。	• dvchost = <具有 Central Node 元件的伺服器名稱>。 • rt = <事件的日期和時間，UTC>。 • KasperskyLabKATAcomponentName = <元件的名稱>。 • KasperskyLabKATAcomponentState = <元件的狀態>（0 – OK, >0 – 錯誤）。

管理連線器

本節包含有關 Kaspersky Anti Targeted Attack Platform 中的連線器的資訊。*連線器*是處理與 Kaspersky Anti Targeted Attack Platform 的通訊的特殊軟體模組，可允許在應用程式本身或在應用程式的幫助下執行管理工作。

連線器擴展了應用程式的功能，使其能夠與第三方系統互動。根據其功能目的，連線器可以將資料傳送到第三方系統（例如，將事件、應用程式訊息和稽核記錄傳送至 SIEM 系統）或從第三方系統取得資料。應用程式還可以使用連線器對裝置進行主動輪詢。

執行連線器軟體模組的電腦稱為*連線器部署節點*。您可以在任何可以透過網路存取 Central Node 伺服器的電腦上部署連線器（包括安裝了應用程式元件的節點，包括 Central Node 伺服器本身）。

連線器表和連線器類型表顯示在應用程式 Web 介面的**設定**部分、**連線器**子部分。只有具有管理員角色的使用者才能管理連線器和連線器類型。擁有**安全稽核員**、**安全官**和**資深安全員**角色的使用者可以檢視連線器和連線器類型。

連線器的功能取決於所選的*連線器類型*。您可以在將連線器新增至應用程式時選擇連線器類型。應用程式內建有以下類型的現成連線器：

- **Syslog**

  此連線器類型支援將資料轉送至 syslog 伺服器。

  新增 **Syslog** 連線器或編輯其設定時，配置連線器的一般設定以及**詳細資料**下的附加設定：

  - Syslog 伺服器位址
  - Syslog 伺服器連接埠
  - 資料傳輸協定

- **SIEM**

  此連線器類型支援將資料轉送至 SIEM 系統。

  當您新增 **SIEM** 連線器或編輯其設定時，配置連線器的一般設定以及**詳細資料**下的附加設定：

  - SIEM 系統伺服器位址
  - SIEM 系統伺服器連接埠
  - 資料傳輸協定

- **一般**

  這種類型的連線器類型允許連線使用 NDR API 的應用程式。

- **電子郵件**

  此連線器類型提供透過電子郵件轉發資料的功能。

  新增**電子郵件**連線器或編輯其設定時，設定連線器的一般設定以及**詳細資料**下的附加設定：

  - 用作電子郵件寄件者的位址。
  - 電子郵件的收件者位址。
  - 事件、應用程式訊息和稽核記錄的電子郵件主旨行。
  - 事件、應用程式訊息、稽核記錄、網路互動描述以及整個通知電子郵件訊息的文字描述範本。您可以在範本中使用變數。
  - 當傳送的通知數量達到最大限額時傳送的電子郵件的主旨和主體。
  - 每天傳送的最大電子郵件數。
  - 每條訊息中的最大通知數。指定可放入單個電子郵件訊息中的相同類型（事件、應用程式訊息或稽核記錄）的已註冊通知的最大數量。如果有更多已註冊的通知，則會產生額外的電子郵件訊息（在每日限制內）。

  為了使**電子郵件**連線器正常運作，您必須先設定郵件伺服器連線。

- **主動輪詢**

  此連線器類型提供具備設定控制和主動輪詢作業的主動裝置輪詢功能。

新增**主動輪詢**連線器或編輯其設定時，請設定連線器的一般設定，以及**詳細資料**下的其他設定：

- 使用連線器時應用程式使用者可以使用的主動輪詢方法。
- 允許或拒絕主動輪詢的裝置的被允許和被拒絕 IP 位址範圍。`0.0.0.0` 位址與所有可能的 IP 位址相符。

  如果某個位址既包含在允許的 IP 位址中，也包含在拒絕的 IP 位址中，Kaspersky Anti Targeted Attack Platform 會將其歸類為拒絕的 IP 位址。
- 其對應裝置可用於主動輪詢的位址空間名稱。如有必要，請在 **L3 位址空間**欄位中選擇 IP 位址的位址空間，並在 **L2 位址空間**欄位中選擇 MAC 位址的位址空間。

  > 如果選擇的位址空間與**預設**位址空間不同，請為該位址空間新增規則（或編輯現有規則）。此規則必須指定選擇此位址空間的連線器。規則設定會在變更位址空間時進行設定。

- **KUMA**

  此連線器類型提供與 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的整合。此類連線器的軟體模組與 Kaspersky Anti Targeted Attack Platform 分開分發。這種類型的連線器可讓您將有關裝置和風險的資訊傳送到 KUMA，以及在 KUMA 中執行命令來變更裝置狀態。新增連線器後，必須在 KUMA 中配置整合（建立與 Kaspersky Anti Targeted Attack Platform 的連線）。KUMA 連線器使用 Kaspersky Anti Targeted Attack Platform API 與 Central Node 伺服器互動。

  KUMA 連線器提供的整合涉及傳送有關裝置和風險的資訊，以及應用命令來改變裝置狀態。若要將事件傳送至 KUMA，您可以向 Kaspersky Anti Targeted Attack Platform 新增 **Syslog** 或 **SIEM** 連線器，並為此連線器指定與 KUMA 伺服器的連線設定。新增連線器後，需要在 KUMA 端配置一個收集器。

- **Cisco 交換機**

  此連線器類型透過思科網路交換機為裝置提供自動網路存取控制支援。

  新增 **Cisco 交換機**連線器或編輯其設定時，設定連線器的一般設定以及**詳細資料**下的附加設定：

  - 您想要在應用程式使用連線器執行的操作的事件中指定的開關的名稱。
  - 將連線器連線到交換機的定址資訊：IP 位址和 SSH 連接埠。
  - 透過 SSH 連線到交換機的憑證。
  - 在建立 SSH 連線之前，需要將公鑰與從網路交換機收到的公鑰進行配對；這樣做是為了防止網路中此裝置被欺騙。如果該值為空，則不執行檢查。
  - 用於限制裝置網路存取的方法。應用程式提供了基於MAC 位址（MAC ACL）、IP 位址（IP ACL）在交換機存取控制清單中建立拒絕規則的方法，以及透過停用裝置連線到的乙太網路連接埠的方法。

    > 若要使用停用乙太網路連接埠的方法，請設定交換機連線以防止多個裝置連線到一個連接埠。否則，停用乙太網路連接埠以阻止一個裝置也會阻止使用該連接埠連線到網路的所有裝置的網路存取。

  - 當變更網路存取限制方法時，此設定將重設拒絕規則。如果啟用此設定，變更方法將重置已設定的封鎖裝置的規則。
  - 此設定將網路裝置排除在網路存取限制方法之外。如果啟用此設定，則此方法不適用於**網路裝置**、**防火牆**、**交換機**、**虛擬交換機**、**路由器**、**虛擬路由器**、**Wi-Fi** 裝置。
  - 此設定僅套用拒絕規則於新裝置。若啟用此設定，此方法僅適用於已註冊事件類型代碼為 4000005003 的新裝置偵測事件的未經授權的裝置。

- 裝置表中*已授權*和*未授權*裝置的輪詢間隔。

- 此設定可讓您設定連線器重新啟動時有關被封鎖裝置的通知。如果啟用此設定，則在啟用或重新啟動連線器後，先前已套用網路存取限制的裝置清單將傳送至 Central Node 伺服器。

如有必要，您可以新增其他連線器類型，以促進資料交換或在應用程式與其他接收系統互動時提供執行管理工作的功能。

某些連接埠和協定用於連線器與 Central Node 伺服器的連線。

第三方系統代表應用程式使用者之一透過連線器進行連線。我們建議為每個連線器使用單獨的使用者帳戶。這將幫助您使用稽核記錄分析透過連線器執行的操作。

應用程式中的最大連線器數量為 20。連線器類型的最大數量為 100。

受管理和不受管理的連線器

應用程式可以使用受管理和不受管理的連線器。

如果連線器的軟體模組能夠在新增連線器後自動註冊並啟動，則該連線器是*受管理的*，並且當啟用或停用該連線器時，或當刪除該連線器時，這些模組能夠被管理。只有安裝了應用程式元件的節點才可以作為受管理的連線器的部署節點。

*不受管理的連線器*不提供受管理的連線器的功能。您必須在部署連線器的節點上手動註冊這樣的連線器、啟動、停止或刪除其軟體模組。當您啟用或停用不受管理的連線器時，應用程式會透過允許或拒絕與 Central Node 伺服器端的連線器的互動來反映這一點。

連線器和 Central Node 伺服器之間的連線使用憑證進行防護。當連線器新增至應用程式時，會產生連線器憑證。對於受管理的連線器的軟體模組，應用程式會自動傳送產生的憑證。當新增不受管理的連線器時（或在忽略受管理的連線器模式下新增受管理的連線器時），必須使用通訊封包手動上傳連線器軟體模組的憑證。如果需要為此類連線器更換憑證（頒發新憑證），則需要建立一個新的通訊封包並使用它來上傳新的憑證。替換受管理的連線器憑證的唯一方法是刪除並重新新增連線器。

將事件、應用程式訊息和稽核記錄傳送到第三方系統

您可以設定透過連線器將事件、應用程式訊息或稽核記錄（以下也稱為"註冊通知"）轉送到第三方系統。對於名為 **Syslog**、**SIEM** 和**電子郵件**的連線器類型，預設啟用傳送註冊通知的功能。對於 KUMA **連線器類型**，如果安裝了應用程式模組，則可以轉發已註冊通知。當使用新增至應用程式的其他連線器類型時，此功能是否可用取決於這些特定連線器類型的設定。

為每個連線器單獨配置註冊通知。當配置事件類型時，您可以選擇要透過連線器轉送的事件類型。建立連線器或編輯其設定時，您可以啟用或停用透過此連線器轉送所有應用程式訊息和所有稽核記錄。

電子郵件類型的連線器允許限制傳輸的資料量。對於此連線器類型，您可以設定有關新註冊的通知的電子郵件訊息的最大數量以及每個訊息中註冊的通知的最大數量。如果已傳送的電子郵件數量達到最大數量，則會向收件者傳送另一則訊息，通知他們已超出限制。此後，直到 Central Node 伺服器所在時區的當天結束為止，都不會傳送任何新訊息。

透過**電子郵件**連線器傳送的電子郵件訊息針對每種類型的註冊通知分別產生。也就是說，針對事件、應用程式訊息和稽核記錄產生不同的電子郵件訊息。

透過 **Syslog** 和 **SIEM** 類型的連線器轉送的已註冊通知的資訊的內容和順序在這些系統中可能與 Kaspersky Anti Targeted Attack Platform Web 介面中顯示的資訊的內容和順序不同。

透過 Cisco 交換機連線器自動控制裝置的網路存取

您可以透過 **Cisco 交換機** 連線器為裝置設定自動網路存取控制。這種類型的連線器與交換機交換訊息，以傳送命令來新增或刪除連線到交換機的裝置的網路存取拒絕規則（限制）。

裝置的網路存取控制由其狀態驅動。連線器在交換機上為具有"*未授權*"狀態的裝置建立拒絕規則，並在為裝置指派"*已授權*"狀態後刪除規則。

每個連線器只能與一個網路交換機交換資訊。

Cisco 交換機連線器用於僅限制那些詳細資訊包含其 MAC 位址的裝置的網路存取。而且，這些MAC 位址必須儲存在網路交換機的 ARP 表中。也就是說，具有這些 MAC 位址的裝置必須連線到連線器所連線的網路交換機。

連線器可以使用各種方法來限制裝置的網路存取。應用程式提供了基於MAC 位址（MAC ACL）、IP 位址（IP ACL）在交換機存取控制清單中建立拒絕規則的方法，以及透過停用裝置連線到的乙太網路連接埠的方法。

若要使用停用乙太網路連接埠的方法，請設定交換機連線以防止多個裝置連線到一個連接埠。否則，停用乙太網路連接埠以阻止一個裝置也會阻止使用該連接埠連線到網路的所有裝置的網路存取。

為了最大限度地降低連線器影響裝置的網路輔助功能的風險，您可以在配置連線器時啟用以下設定：

- 此設定將網路裝置排除在網路存取限制方法之外。如果啟用此設定，則此方法不適用於**網路裝置**、**防火牆**、**交換機**、**虛擬交換機**、**路由器**、**虛擬路由器**、**Wi-Fi** 裝置。
- 此設定僅套用拒絕規則於新裝置。若啟用此設定，此方法僅適用於已註冊事件類型代碼為 4000005003 的新裝置偵測事件的未經授權的裝置。

連線器透過 SSH 與網路交換機連線。SSH 連線憑證在連線器設定中指定並儲存。為了防護這些對於識別和身分驗證至關重要的敏感憑證，連線器會根據儲存的值驗證它收到的交換機公鑰，以防止交換機欺騙。在驗證收到的公鑰與連線器中儲存的公鑰匹配後，識別和身分驗證詳細資訊將傳送到交換機。

連線器根據其操作的結果記錄應用程式內的事件。這些事件類型透過外部技術記錄。產生以下事件標題：

- 重設<交換機名稱>的裝置拒絕規則

  當連線器因網路存取限制方法的變更而重設裝置先前定義的拒絕規則時，會記錄此類事件。

- 根據來自<交換機名稱>的資料，更新了關於<裝置名稱>的資訊，位址為<裝置 MAC 位址>

  此類事件表示連線器從交換機接收到某個裝置連線到某個連接埠的資訊。

- 在<交換機名稱>上為<裝置名稱>新增了裝置拒絕規則

  當連線器限制未經授權的裝置的網路存取時，會記錄此類事件。

- 刪除了<交換機名稱>上<裝置名稱>的拒絕規則

  當連線器成功刪除特定裝置的網路存取限制時，會記錄此類事件。

- <交換機名稱>先前已新增拒絕規則

  此類事件表明，連線器在開啟或重新啟動時發現特定交換機上存在預先存在的拒絕規則。

- 在未驗證公鑰的情況下與<交換機名稱>建立了 SSH 連線

  當連線器成功與交換機建立 SSH 連線但無法驗證其公鑰時，會記錄此類事件。我們建議驗證網路上沒有欺騙裝置，然後在連線器設定中儲存新的公鑰。

- 偵測到<交換機名稱>的公鑰不匹配

  當連線器偵測到交換機儲存的公鑰和接收的公鑰不符時，就會記錄此類事件。這會阻止與交換機的 SSH 連線。我們建議驗證網路上沒有欺騙裝置，並且交換機公鑰確實已變更，然後在連線器設定中儲存新的公鑰。

- 無法與交換機<交換機名稱>建立 SSH 連線：憑證不正確

  當連線器因連線器設定中指定的憑證（使用者名稱或密碼）不正確而無法與交換機建立 SSH 連線時，會記錄此事件。

- 未對交換機<交換機名稱>執行特權模式操作：密碼不正確

  當連線器沒有特權模式功能來新增和刪除交換機上的裝置拒絕規則時，會記錄此事件。這種情況下，請在連線器設定中輸入正確的特權模式密碼。

新增連線器

您可以根據應用程式中可用的連線器類型之一新增連線器。不受管理的連線器僅應基於自訂連線器類型建立。

在新增連線器之前，我們建議建立一個單獨的使用者帳戶，第三方系統將使用該帳戶連線到應用程式。為了使**電子郵件**連線器正常運作，您必須先設定郵件伺服器連線。

若要新增連線器：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**設定**”部分、“**連線器**”子部分。
3. 在“**連線器**”索引標籤上，點擊“**新增連線器**”以開啟詳細資料區域。
4. 配置連線器一般設定：
   a. 選擇相關的連線器類型並輸入連線器名稱。
   b. 若要新增不可管理的連線器（或配置為忽略可管理連線器功能的連線器），請輸入存取連線器憑證的密碼。

      使用定義的密碼，憑證將被加密在連線器的通訊資料包中。
   c. 指定 Central Node 伺服器的 IP 位址。

      連線器使用指定的位址連線到 Central Node。
   d. 指定要部署連線器的節點：
      - 如果要新增受管理的連線器，可以指定其中一個已安裝應用程式元件的節點作為連線器部署節點。
      - 如果要新增不受管理的連線器，則必須輸入要執行該連線器的軟體模組的電腦的 IP 位址。
   e. 選擇第三方系統將用於透過連線器連線到應用程式的使用者。您必須指定其中一個應用程式使用者的名稱。

5. 在**詳細資料**下，根據連線器的類型指定進階設定。如果連線器類型不允許管理進階設定，則**詳細資料**設定群組不會顯示在詳細資料區域中。

6. 如果連線器的類型允許轉送稽核記錄和應用程式訊息，請使用對應的核取方塊啟用或停用此資料的轉送。

7. 如果需要，請輸入連線器的描述。

8. 點擊**儲存**。

   新的連線器已新增至連線器表。

如果您新增了不受管理的連線器，Central Node 會為新的連線器產生通訊資料套件，然後您的瀏覽器會儲存下載的檔案。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。您需要將新的通訊封包的內容上傳到將使用連線器的應用程式。

檢視連線器表

連線器表顯示在**設定**區段、**連線器**子區段的**連線器**索引標籤上。

連線器設定顯示在表格以下列中：

- **名稱**。

  為連線器指定的名稱。

- **連線器 ID**。

  連線器建立時指定的 ID。

- **已啟用**。

  指示 Central Node 是否已準備好與連線器的軟體模組互動。如果此設定的值為**否**，則 Central Node 伺服器將不接受來自連線器應用程式模組的請求。

- **狀態**。

  連線器的軟體模組的狀態。可以有以下狀態：

  - **等待註冊**：新增不受管理的連線器或為不受管理的連線器建立新的通訊資料套件後，尚未透過此連線器建立連線。

  - **切換**：連線器的應用程式模組狀態從**關**切換到**開**，或從開切換到關。

  - **關**表示 Central Node 伺服器不接受來自連線器應用程式模組的請求。如果連線器是可管理的，則會向其應用程式模組傳送停止命令。

  - **開**表示已使用為此連線器建立的憑證，透過此連線器成功建立連線。

  - **錯誤**表示嘗試使用連線器的應用程式模組執行操作時發生錯誤。

- **類型**。

  連線器類型的圖示和名稱。

- **上次連線**。

  上次透過連線器連線的日期和時間。

- **可管理**。

  指示連線器是可管理的。如果設定為“**否**”，則連線器是不受管理的，或設定為忽略受管理的連線器功能。

- **變更時間**。

  連線器設定的最後修改日期和時間。

- **敘述**。

  為連線器指定的描述。

檢視連線器表時，您可以使用設定、篩選、搜尋和排序功能。

啟用或停用連線器

如果您想要暫時封鎖連線器的軟體模組連線到 Central Node 伺服器，您可以停用該連線器。如果您想還原連線，請啟用連線器。

若要啟用或停用連線器：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**設定**”部分、“**連線器**”子部分。
3. 在“**連線器**”索引標籤上，選擇要啟用或停用的連線器。

   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 根據需要點擊**啟用**或**停用**。

   這將開啟一個確認提示視窗。
5. 在提示視窗中，點擊**確定**。

編輯連線器設定

若要編輯連線器設定：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**設定**”部分、“**連線器**”子部分。
3. 在“**連線器**”索引標籤上，選擇相關連線器。

   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊“**編輯**”。

5. 按照與新增連線器相同的方式編輯設定。

   並非所有設定都可編輯。例如，您不能變更連線器的類型。

6. 點擊**儲存**。

變更顯示在連線器表的相應列中。如果您變更了連線器的名稱，新名稱將顯示在事件類型表的列標題中。

編輯不受管理連線器的某些設定會導致 Central Node 伺服器為連線器產生新的通訊資料套件（例如，如果您在忽略受管理連線器模式下變更 **syslog** 連線器的伺服器位址）。根據您的瀏覽器設定，可能會顯示一個視窗，您可以在其中變更要儲存的通訊封包的路徑和名稱。將新的通訊封包的內容上傳到使用連線器的應用程式。否則，該應用程式將無法透過該連線器建立新的連線。

為連線器建立新的通訊封包

當新增不受管理的連線器時，會自動為此連線器建立通訊套件。如有必要，您可以為連線器建立一個新的通訊封包（例如，如果來自舊通訊封包的憑證已洩露）。

建立新的通訊封包後，舊通訊封包中的憑證將失效。因此，下次透過此連線器連線第三方系統時，必須使用新的通訊封包。

若要為不受管理的連線器建立新的通訊封包：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 選擇“**設定**”部分、“**連線器**”子部分。

3. 在“**連線器**”索引標籤，選擇要為其建立新通訊套件的非可管理連線器。

   詳細資訊區域顯示在 Web 介面視窗的右側。

4. 點擊**取得新的通訊套件**。

   這將開啟**產生新的通訊套件**視窗。

5. 指定建立通訊封包的設定：

   - 第三方系統將用於透過連線器連線到應用程式的使用者的名稱。您必須指定其中一個應用程式使用者的名稱。

     我們推薦指定在新增連線器時指定的使用者名稱。如果需要指定不同的使用者名稱，我們建議選擇其他連線器未使用且未用於透過 Web 介面連線到 Central Node 的應用程式使用者。

   - 連線器的軟體模組正在運作的節點的位址。

   - 連線器憑證的密碼。指定的密碼用於加密連線器通訊封包中的憑證。

6. 點擊**建立通訊封包**。

伺服器為所選的連線器產生新的通訊封包，之後您的瀏覽器會儲存下載的檔案。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。將下載的通訊封包的內容上傳到使用連線器的應用程式。否則，該應用程式將無法透過連線器建立新的連線。

正在刪除連線器

當刪除受管理的連線器時，其軟體模組會在部署該連線器的節點上自動停止並刪除。

如果您想要刪除不受管理的連線器或處於忽略受管理的連線器模式的連線器，則必須在刪除連線器之前手動停止並刪除連線器的軟體模組。

若要刪除連線器：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**設定**”部分、“**連線器**”子部分。
3. 在“**連線器**”索引標籤上，選擇要刪除的連線器。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊**刪除**。
   這將開啟一個確認提示視窗。
5. 在提示視窗中確認刪除所選連線器。

新增和刪除連線器類型

連線器類型定義了連線器可用的功能以及這些功能中實現了哪些功能。您可以使用應用程式內建的兩種連線器類型（其供應商為卡巴斯基），或任何其他供應商提供的其他類型的連線器。

若要為應用程式新增連線器類型，您必須從供應商取得下列檔案：

- 用於安裝連線器軟體模組的檔案
- 連線器類型描述檔案

> 如果第三方供應商的連線器類型允許您在連線器中儲存存取第三方系統的使用者憑證，我們建議採取措施防護此類憑證免遭洩漏。為了最大限度地降低憑證被洩漏的風險，我們建議向此類帳戶授予必要的最低權限（僅足以透過連線器建立連線）。

連線器類型表顯示在**設定**區段的**連線器**子區段中，位於**連線器類型**索引標籤上。

檢視連線器類型表

連線器類型表顯示在**設定**區段的**連線器**子區段中，位於**連線器類型**索引標籤上。

連線器設定顯示在表格以下列中：

- **名稱**。

  供應商指定的連線器類型的名稱。

- **供應商**。

  連線器類型的供應商名稱。

- **版本**。

  連線器類型的版本號。

- **代碼**。

  連線器類型的唯一編號。

- **功能**。

  此類型的連線器必須具備的功能清單。

檢視連線器類型表時，您可以使用設定、篩選、搜尋和排序功能。

新增連線器類型

您可以使用連線器類型供應商提供的描述檔案將連線器類型新增至應用程式。連線器類型描述檔必須打包到 Zip 壓縮檔案。

您必須使用連線器類型供應商提供的檔案，手動安裝您要新增的連線器類型的連線器軟體模組。在您想要在新增連線器時指定為連線器部署節點的電腦上安裝軟體模組。

若要新增連線器類型：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**設定**”部分、“**連線器**”子部分。
3. 在**連線器類型**索引標籤上，點擊**新增連線器類型**以開啟詳細資料區域。
4. 點擊**瀏覽**以選擇連線器類型描述檔。
5. 點擊**儲存**。

   新的連線器類型被新增到連線器表中。

刪除連線器類型

刪除連線器類型時，應用程式將刪除有關該連線器類型的資訊，以及使用此類型新增的所有連線器。

若要刪除連線器類型：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**設定**”部分、“**連線器**”子部分。

3. 在“**連線器類型**”索引標籤上，選擇要刪除的連線器類型。

   詳細資訊區域顯示在 Web 介面視窗的右側。

4. 點擊“**刪除**”。

   這將開啟一個確認提示視窗。

5. 在提示視窗中確認刪除所選連線器類型。

6. 如果應用程式具有此類型的連線器，請確認也刪除這些連線器。

管理遠端連線的帳戶憑據 Secret

Kaspersky Anti Targeted Attack Platform 實作了 Secret 儲存。*Secret* 使您能夠安全地儲存和使用應用程式自動遠端連線到裝置所需的識別和身分驗證資訊。Secret 用於主動輪詢作業。

應用程式支援各種類型的 Secret。根據 Secret 的用途，您可以在新增或編輯 Secret 設定時選擇相關類型並輸入適當的資料。

將使用遠端連線協定進行裝置遠端連線所需的憑證儲存在 Secret。根據所選的輪詢方法，主動輪詢作業可以使用各種協定進行遠端連線。

> 為了確保安全地使用儲存在 Secret 中的身分和身分驗證詳細資訊，該應用程式實施了在連線到遠端裝置時防止 Secret 洩漏的防護。在應用程式中儲存從裝置收到的公鑰後，它會監控到這些裝置的所有後續遠端連線，並且在網路上發生裝置欺騙時不會傳送來自 Secret 的資訊。

Secret 的關鍵資訊（密碼或憑證私鑰），只有在建立 Secret 時輸入這些資訊時才能以純文字形式提供一次。儲存 Secret 後，其關鍵資訊將無法再檢視。您只能在編輯 Secret 時以新的關鍵資訊替代Secret 的關鍵資訊（例如，您可以輸入不同的密碼）。

您可以在**設定**區段的**Secret**子區段中管理 Secret。不能在應用程式中新增超過 500 個 Secret。

只有具有管理員角色的使用者才能管理 Secret。

新增 Secret

您可以將 Secret 新增到應用程式 Secret 儲存中。

要新增 Secret：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 選擇“**設定**”部分、“**Secret**”子部分。

3. 點擊“**新增 Secret**”。

   這將開啟詳細資訊區域。

4. 輸入 Secret 的名稱。

   Secret 名稱必須是唯一的（不得與其他 Secret 的名稱相符）且必須包含最多 256 個字元。您可以使用字母、數字、空格以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。Secret 名稱必須以空格以外的任何有效字元開始和結束。

5. 選擇 Secret 類型並配置其設定。

   您可以選擇以下類型的 Secret：

   - **僅密碼**：如果僅需要具有相關權限的使用者的密碼即可存取裝置配置資料，則使用此類 Secret。
   - **使用者名稱和密碼**：如果需要使用者名稱和密碼才能從裝置接收資料，則使用此類 Secret。
   - **使用者名稱和密碼，root 密碼**：如果需要使用者名稱和密碼才能從裝置接收資料，而對於具有管理員（root）權限的連線，也需要 root 密碼或以管理員權限處理請求的帳戶的密碼，則使用此類 Secret。
   - **使用者名稱和密碼，加密密碼**：如果需要使用者名稱和密碼才能從裝置接收資料，並且還需要加密密碼才能建立加密連線，則使用此類 Secret。
   - **混合** Secret 類型用於裝置輪詢的**遠端連線**方法。您可以為此類 Secret 指定以下設定：
     - 用於遠端連線裝置的使用者名稱。

       使用者名稱可以包含拉丁字母、數字、句點以及特殊字元：`_` 和 `-`。名稱必須以字母開頭，並以除句點之外的任何受支援的字元結尾。
     - **使用者密碼**：是否使用使用者密碼進行身分驗證。

       密碼可以包含最多 256 個 ASCII 字元。
     - **私密金鑰**：是否使用憑證的私密金鑰進行身分驗證。

       您可以手動輸入組成金鑰的字元序列，或透過點擊**從檔案複製**從憑證檔案上傳金鑰。您可以上傳 CRT、PEM 和 CER 格式的私鑰。如果私密金鑰檔案受密碼短語防護，請在上傳金鑰之前於**密碼短語**欄位中輸入密碼短語。

       > 要使用憑證的私鑰，您需要將此憑證的公鑰複製到將使用 Secret 進行遠端連線的所有裝置上。將公鑰複製到裝置的步驟無需 Kaspersky Anti Targeted Attack Platform 的參與。

     - **Root 使用者密碼**：如果以管理員(root) 權限連線網路元件時需要額外的密碼。在這種情況下，將以 root 身分或在網路裝置上設定為以管理員權限處理請求的使用者身分請求存取。

6. 點擊**儲存**。

檢視 Secret 表

遠端連線 Secret 表顯示在應用程式 Web 介面的“**設定**”→“**Secret**”部分。

有關 Secret 的資訊顯示在表的以下列中：

- **Secret 名稱**。

  應用程式對 Secret 使用的名稱。

- **建立日期**。

  將 Secret 新增到應用程式的日期和時間。

- **變更時間**。

  應用程式中Secret 最後修改的日期和時間。

檢視 Secret 表時，您可以使用配置、篩選、搜尋和排序功能。

連線到遠端裝置時防止 Secret 洩漏

Secret 中的識別和身分驗證詳細資訊僅套用於與選定用於主動輪詢作業的裝置的遠端連線。為了防護這些資訊在裝置欺騙的情況下免於可能的洩漏，應用程式會在傳送資訊之前驗證從裝置收到的公鑰。裝置使用公鑰建立 SSH 連線。公鑰可協助應用程式驗證是否與正確的裝置建立了 SSH 連線。驗證收到的公鑰與應用程式中儲存的公鑰匹配後，識別和身分驗證詳細資訊將被傳送到裝置。

儲存的裝置公開金鑰顯示在**一般**索引標籤上所選裝置的詳細資訊區域中。

在應用程式中接收並儲存裝置公鑰

預設情況下，Kaspersky Anti Targeted Attack Platform 中未配置任何裝置的公鑰。首次與該裝置建立 SSH 連線時，將接收並儲存裝置的公開金鑰，以便作為使用**主動輪詢**類型的連線器的主動輪詢工作的一部分進行掃描。所選秘密的識別和身分驗證詳細資訊將傳送到裝置，而無需檢查收到的公鑰。因此，在首次對選定的裝置啟動主動輪詢作業並與其建立 SSH 連線之前，請確保網路上沒有被欺騙的裝置。為此，您可以執行`ifconfig`來檢查應用程式中配置的裝置的 IP 位址是否與實際裝置網路介面上的 IP 位址相符。

重置已儲存的裝置公鑰

裝置上的 SSH 連線金鑰可能會隨著時間而改變。當裝置用戶目前的私鑰面臨洩漏風險時，他們可能會產生新金鑰。

當裝置上的私鑰發生變化時，對應的公鑰也會發生變化。變更公鑰後，應用程式將停止將 Secret 資訊傳送到該裝置，因為新的公鑰不再與應用程式中儲存的指紋相符。因此，作為主動輪詢作業一部分的任何後續裝置掃描都會以錯誤結束。

變更裝置上的公鑰後，您必須重置應用程式中儲存的該裝置目前已儲存的公鑰。這將允許在遠端連線裝置時再次使用這些 Secret。

重置已儲存的公鑰後，應用程式將在下次與裝置建立 SSH 連線時儲存新收到的公鑰。檢查網路上沒有欺騙裝置，類似於最初接收和儲存公鑰時。

只有具有“**資深安全員**”角色的使用者可以重置裝置已儲存的公開金鑰。

要重設已儲存的裝置公鑰：

1. 使用 Web 介面以**資深安全員**角色連線到 Central Node。

2. 選擇“**資產**”部分。

3. 在“**裝置**”索引標籤上，選擇要重置已儲存公開金鑰的裝置。

4. 右鍵點擊其中一個選定的裝置以開啟上下文功能表。

5. 在右鍵功能表中，選擇**重置公開金鑰**。

   這將開啟一個確認提示視窗。

6. 在提示視窗中，點擊**確定**。

編輯 Secret 的設定

編輯 Secret 設定時，您可以變更其類型或設定不同的憑證。

修改 Secret 設定（包括 Secret 名稱）後，新設定將套用於先前指定過 Secret 的主動輪詢作業。如果您變更 Secret 的類型，則當 Secret 的新類型與連線器設定不符時，下次啟動這些作業時可能會發生錯誤。

要編輯 Secret 的設定：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 選擇“**設定**”部分、“**Secret**”子部分。

3. 選擇您想要編輯的 Secret。

   詳細資訊區域顯示在 Web 介面視窗的右側。

4. 點擊**編輯**。

5. 根據需要編輯設定。您可以按照與新增 Secret時相同的方式編輯設定。

   Secret 的關鍵資訊（密碼和憑證的私密金鑰）不會公開顯示。您只能使用帶有憑證的欄位上方的連結將 Secret 的關鍵資訊替換為新的關鍵資訊。

刪除 Secret

您可以從 Kaspersky Anti Targeted Attack Platform Secret 儲存中刪除 Secret。

在刪除 Secret 之前，我們建議在使用該 Secret 的主動輪詢作業中指定不同的 Secret 或不同的輪詢方法。如果在主動輪詢作業中指定了已刪除的 Secret，則下次執行作業時會發生錯誤。

若要刪除 Secret：

1. 使用應用程式管理員帳戶登入 Web 介面。

2. 選擇“**設定**”部分、“**Secret**”子部分。

3. 選擇您想刪除的 Secret。

4. 點擊**刪除**。

   這將開啟一個確認提示視窗。

5. 在確認提示視窗中，確認刪除 Secret。

更新應用程式資料庫

應用程式資料庫（以下也稱為"資料庫"）是含有記錄的檔案，應用程式元件和模組會使用這些記錄來偵測組織 IT 基礎架構中發生的事件。

卡巴斯基的病毒分析師每天偵測到數百種新威脅（包括"零時差"弱點），並建立記錄來識別它們，將它們加入資料庫更新套件（或"更新套件"）。*更新套件*由一個或多個包含記錄的檔案組成，這些記錄可用於識別自上次更新套件發布以來偵測到的威脅。我們建議您定期接收更新包。安裝應用程式時，資料庫發布日期與應用程式發布日期相同，因此在安裝應用程式後必須立即更新資料庫。

應用程式會每 30 分鐘一次自動尋找卡巴斯基更新伺服器上的新更新包。預設情況下，如果由於某些原因應用程式資料庫在24 小時內未更新，Kaspersky Anti Targeted Attack Platform 會在應用程式 Web 介面視窗的**控制板**部分顯示此資訊。

如果不支援 Kaspersky Anti Targeted Attack Platform 的版本，則不會更新應用程式資料庫，並且應用程式 Web 介面的**系統健康**視窗的**控制板**部分，顯示*不再支援此版本的 Kaspersky Anti Targeted Attack Platform。請將應用程式升級為支援的版本*。警告。

您可以在應用程式生命週期頁面檢視目前支援哪些應用程式版本。

> 更新功能（包括病毒防護簽章更新和代碼庫更新）以及 KSN 功能可能無法在美國境內使用。

在分佈式解決方案和多組織用戶模式下，應用程式資料庫會在每個 PCN 和 SCN 伺服器上獨立更新。

如果您已將 Kaspersky Anti Targeted Attack Platform 部署在隔離網路或網際網路頻寬有限的網路中，則可以使用卡巴斯基更新公用程式設定應用程式資料庫更新。

選擇資料庫更新來源

> 如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

您可以選擇應用程式將下載資料庫更新的來源。更新來源可以是卡巴斯基伺服器、一個網路資料夾或組織的電腦上的本機資料夾。

選擇資料庫更新來源：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**一般設定**子部分。
2. 在**資料庫更新**部分，在**更新來源**下拉清單中，選擇下列值之一：
   - **卡巴斯基更新伺服器**。

     該應用程式透過 HTTP 連線到卡巴斯基更新伺服器並下載最新的資料庫。
   - **卡巴斯基更新伺服器（安全連線）**。

     該應用程式透過 HTTPS 連線到卡巴斯基更新伺服器並下載最新的資料庫。建議使用 HTTPS 進行資料庫更新。
   - **自訂伺服器**。

     應用程式連線到您的 FTP 或 HTTP 伺服器或電腦上包含應用程式資料庫的目錄，以下載最新資料庫。

     HTTP 必須用於 HTTP 伺服器和 Central Node 之間的通訊。在這種情況下不支援 HTTPS。
3. 如果選擇了**自訂伺服器**，請在該設定名稱下的欄位中，輸入 HTTP 伺服器上更新套件的 URL，或電腦上包含應用程式資料庫更新套件的資料夾的完整路徑。
4. 點擊**套用**。

應用程式資料庫更新來源已套用。

手動更新資料庫

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

若要開始手動更新資料庫：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**一般設定**子部分。
2. 在**資料庫更新**部分，點擊**啟動**按鈕。
3. 點擊**套用**。

應用程式資料庫更新開始。更新進度將顯示在按鈕右側。

使用卡巴斯基更新實用程式更新應用程式資料庫

如果您已將 Kaspersky Anti Targeted Attack Platform 部署在隔離網路或網際網路頻寬有限的網路中，則可以使用卡巴斯基更新實用程式設定應用程式資料庫更新。在這種情況下，該實用程式會將更新套件下載到組織內部部署網路以外的電腦，然後將其複製到您的 FTP 或 HTTP 伺服器。Kaspersky Anti Targeted Attack Platform 隨後會從此伺服器取得更新套件。

使用此實用程式設定應用程式資料庫更新涉及以下步驟：

1. 使用卡巴斯基更新實用程式下載更新套件

   首先，您需要聯絡卡巴斯基技術支援，並索取該實用程式的分發套件以及您可以從中下載更新的伺服器清單。

2. 將使用卡巴斯基更新實用程式取得的更新套件上傳至您的 FTP 或 HTTP 伺服器。

3. 選取您的 FTP 或 HTTP 伺服器作為資料庫更新來源。

使用卡巴斯基更新實用程式下載更新套件

您需要聯絡卡巴斯基技術支援，並要求提供該實用程式的分發套件，以及可用來下載更新的伺服器清單。

安裝卡巴斯基更新實用程式：

1. 將包含實用程式分發套件的資料夾下載到您的電腦。

2. 運行 UpdateUtility-Gui.exe 檔案。

3. 在開啟的視窗中，點選"**應用程式**"按鈕，然後選取**7.0-7.1** 選項左側的核取方塊。

4. 點選**"確定"**和**"套用"** 。

   該實用程式已安裝。您可以依照以下步驟下載服務套件。

若要使用卡巴斯基更新實用程式下載更新套件：

1. 在實用程式的主視窗中，點擊"**設定**"按鈕，然後選擇"**下載**"。

2. 在"**更新來源**"下，選擇"**其他**"，然後輸入用於下載更新的伺服器位址。

3. 點選"**確定**"和"**套用**" 。

4. 點擊"**啟動**"。

   更新套件被下載到執行該實用程式的電腦上。檔案已準備好上傳到您的 FTP 或 HTTP 伺服器。

更新使用 API 連線到 Central Node 的憑證

若要更新用於透過 Kaspersky Anti Targeted Attack Platform API 連線到 Central Node 伺服器的憑證，您需要取代 REST API 伺服器使用的憑證。您可以在**設定**區段的**連線伺服器**子區段中，於**REST API 伺服器**索引標籤上指定 REST API 伺服器的新憑證。

與工具整合以解包加密的 SSL/TLS 流量

Kaspersky Anti Targeted Attack Platform 接收來自協力廠商解密工具到標準網路介面的解密SSL/TLS 流量，對其進行處理和分析。在 Kaspersky Anti Targeted Attack Platform 中配置解密流量的接收和處理與配置映像 SPAN 流量的接收和處理類似；您需要在應用程式安裝期間啟用 SPAN 整合支援，並為接收流量的網路介面建立和啟用監控點（如果之前尚未建立和啟用）。

與未加密流量相比，在應用程式中接收解密流量會使流量處理負載增加 5 倍。有關 Central Node 伺服器硬體要求的詳細資訊，請參閱大小計算器。

當接收解密流量時，Kaspersky Anti Targeted Attack Platform 可能會處理並保留透過加密協定傳輸的機密資訊。例如，使用者名稱和密碼、銀行卡號。

對於安全人員：應用程式 Web 介面使用入門

本節適用於組織內負責資料安全的專家。它包含有關為企業 IT 基礎架構的安全性配置資源以及及時偵測威脅的資訊和說明。

該應用程式允許多個安全人員一起工作。

Kaspersky Anti Targeted Attack Platform 介面

該應用程式透過 Web 介面進行管理。應用程式 Web 介面的各個部分因使用者的角色不同而有所不同：管理員或高級安全官（**資深安全員**、**安全官**、**安全稽核員**）。

應用程式 Web 介面視窗包含如下內容：

- 應用程式 Web 介面視窗左側和下側的部分。
- 在應用程式 Web 介面視窗上部用於應用程式某些部分的頁簽。
- 應用程式 Web 介面視窗下側的工作區。

應用程式 Web 介面視窗的部分

應用程式 Web 介面為具有**資深安全員**、**安全官**和**安全稽核員**角色的使用者提供以下部分：

- **控制板**。包含 Kaspersky Anti Targeted Attack Platform 監控資料。
  對於具有**安全稽核員**角色的使用者，**控制板**視窗包含以下部分：**警示**、**系統健康**。
- **警示**。包含您有權存取的租用戶網路中的警示資訊。
- **網路流量事件**。有關網路流量中的事件和聚合事件的資訊。
- **威脅搜尋**。包含有關在您有權存取的租戶的主機上發現的事件的資訊。
- **工作**。包含可用於管理主機上的檔案和應用程式的工作的資訊。
- **阻止**。包含可用於管理在選定主機上檔案執行封鎖的政策的資訊。
- **自訂規則**：**TAA**、**入侵偵測**、**IOC**、**YARA**、**Sandbox**。包含用於管理使用者定義的規則的資訊。
- **儲存**：**檔案**和**隔離區**。包含用於管理隔離區和儲存中的物件的資訊。
- **資產**。包含具有 Kaspersky Endpoint Agent 元件的電腦及其設定的資訊。
- **網路地圖**：**網路互動圖**、**拓撲圖**、**網路工作階段**。包含不同時段裝置互動的資訊、網路中裝置實體連線圖、網路工作階段資訊。
- **風險和異常**。包含資訊系統資源所面臨的風險的資訊。

- **報告**：**產生的報告**和**範本**。包含報告建構器和產生的關於警示的報告清單。
- **日誌**：**應用程式訊息**。包含有關應用程式效能的資訊。
- **設定**：**連線器**、**Secret**、**IOC 掃描排程**、**Endpoint Agent**、**KPSN 信譽資料庫**、**通知規則**、**VIP 狀態**、**排除項目**、**允許規則**、**Sandbox 伺服器**、**壓縮檔案密碼**和**產品授權**。包含有關連線器設定的資訊、Secret 資訊、IOC 掃描計劃的資訊、Endpoint Agent 元件設定的資訊、以及在 KPSN 中發布物件以及根據警示中包含的資訊將 VIP 狀態分配給警示的設定、允許的物件清單、從掃描中排除的 IDS、TAA (IOA) 和 ICAP 規則、壓縮檔案密碼和新增的金鑰。

對於具有"**安全稽核員**"角色的使用者，應用程式的 Web 介面除了包含上面列出的部分外，還包含以下部分：

- **操作模式**。包含有關 PCN 和 SCN 伺服器以及分散式解決方案和多組織用戶模式中租用戶的資訊。
- **Sensor 伺服器**。包含有關 Central Node 元件和與其連線的 Sensor 元件的資訊。
- **Sandbox 伺服器**。包含有關 Central Node 元件與 Sandbox 元件的連線的資訊。
- **外部系統**。包含有關應用程式與郵件感應器整合的資訊。
- **伺服器配置**。包含有關應用程式的尺寸參數的資訊。

應用程式 Web 介面視窗的工作區

工作區顯示了您選擇在應用程式 Web 介面視窗的各個部分和頁簽上檢視的資訊。它還包含了可用於配置資訊顯示方式的控制元素。

選擇要在應用程式的 Web 介面中管理的租戶

如果您使用分散式解決方案和多組織用戶模式，並使用**資深安全員**或**安全官**帳戶，在開始使用 Web 介面之前，您必須在應用程式 Web 介面中選擇要管理的租用戶。

若要在應用程式的 Web 介面中選擇要管理的租戶：

1. 在應用程式 Web 介面功能表的上部，點擊租戶名稱旁的箭頭。
2. 在**選擇租戶**下拉清單中，選擇租用戶。

   您也可以開始在搜尋框中鍵入租戶的名稱，然後從搜尋結果清單中選擇租戶。

應用程式 Web 介面中的所有操作都會套用於所選租戶。如果您想選擇其他租戶，請重複選擇租戶的步驟。

> 具有**安全稽核員**角色的使用者無法在 Web 介面中選擇要管理的租用戶。

監控應用程式的效能

您可以使用應用程式 Web 介面視窗的**控制板**部分中的小工具來監控應用程式運作。您可以新增、刪除和移動小工具，配置小工具的顯示比例，以及選擇資料顯示時段。

關於小工具和佈局

您可以使用小工具來監控應用程式運作。

*佈局*是**控制板**區段中應用程式 Web 介面視窗工作區的外觀。您可以在版面配置中新增、刪除和移動小工具，以及配置小工具的比例。

如果使用的是分散式解決方案和多組織用戶模式，此部分將顯示所選租用戶的資訊。NDR 小工具僅顯示目前或選定節點的資訊。

預設情況下，此部分僅顯示有關使用者未處理的警示的資訊。若要也顯示有關已處理警示的資訊，請啟用視窗右上角的**顯示已關閉的警示**切換開關。

控制板部分顯示以下小工具：

- 警示：
  - **按狀態分類的警示**。顯示警示狀態，具体取決於處理警示的 Kaspersky Anti Targeted Attack Platform 使用者以及是否已處理該警示。
  - **按技術分類的警示**。顯示產生警示的應用程式模組或元件的名稱。
  - **按攻擊向量分類的警示**。根據攻擊的向量顯示偵測到的物件。
  - **按重要性排列的 VIP 警示**。顯示 VIP 身分警示的重要性，取決於這些警示可能對基於卡巴斯基經驗的電腦或企業區域網路安全性產生的影響。
  - **按重要性分類的警示**。顯示 Kaspersky Anti Targeted Attack Platform 使用者警示的重要性，取決於這些警示可能對基於卡巴斯基經驗的電腦或企業區域網路安全性產生的影響。

  每個小工具的左側部分顯示攻擊向量、警示重要性等級、警示狀態以及產生警示的掃描技術。每個小工具的右側部分顯示程式在小工具上選定的資料顯示時段期間警示被觸發的次數。

  點擊包含攻擊向量名稱、警示重要性等級、警示狀態和產生警示的掃描技術的連結，您將前往應用程式 Web 介面的**警示**區段，您可以在其中檢視相關警示。警示會根據選定的元素進行篩選。

- 前 10 個：
  - **網域**。警示中最常見的 10 個網域名稱。
  - **IP 位址**。警示中最常見的 10 個 IP 位址。
  - **寄件者電子郵件信箱**。警示中最常見的 10 個電子郵件寄件者。
  - **收件者電子郵件信箱**。警示中最常見的 10 個電子郵件收件者。

- **TAA 主機**。Targeted Attack Analyzer (TAA) 技術產生的事件和警示中最常出現的 10 台主機。

- **TAA 規則**。Targeted Attack Analyzer (TAA) 技術產生的事件和警示中最常出現的 10 個 TAA (IOA) 規則。

  此小工具會顯示所選時段內 TAA (IOA) 規則遭觸發的總次數。請注意，小工具中的觸發次數可能會大於警示卡片中顯示的已觸發 TAA (IOA) 規則的主機數量，因為同一規則可在同一主機上觸發多次（例如，當惡意的處理程序再次啟動時）。

  您可以在警示卡片中，於**掃描結果**下檢視已觸發 TAA (IOA) 規則的詳細資訊。

- **按 TAA 規則傳送到 Sandbox**。最常導致 Kaspersky Anti Targeted Attack Platform 傳送檔案以供 Sandbox 元件掃描的 10 個 TAA (IOA) 規則。

每個小工具的左側部分列出了網域、收件者的電子郵件信箱、郵件寄件者的 IP 位址和電子郵件信箱、主機名稱和 TAA (IOA) 規則名稱。每個小工具的右側部分顯示程式在小工具上選定資料顯示時段期間警示被觸發的次數。

點擊帶有每個網域名稱、收件者位址、IP 位址以及郵件寄件者位址的連接，您可以前往應用程式 Web 介面的**警示**部分，並檢視相關警示。

點擊帶有主機名稱和 TAA (IOA) 規則名稱的連接，轉到應用程式 Web 介面的**事件**部分，並檢視相關事件。

警示和事件基於所選元素進行篩選。

- NDR：

  - **網路流量事件得分**。選定時間段內事件按得分分佈的長條圖。長條圖對應分數的整數值。您可以將資料顯示模式變更為圓餅圖，並按嚴重性等級分佈事件。根據分數，事件的嚴重程度可能為*低*(0.0–3.9)、*中*(4.0–7.9)或*高*(8.0–10.0)。

  - **按技術劃分的網路流量事件**。在選定時間內，透過哪種事件註冊技術註冊了多少事件。

  - **裝置安全狀態**。依裝置安全狀態進行分佈。

  - **網路流量事件中頻繁出現的應用程式使用者**。根據選定時間段內的 EPP 應用程式資訊，在事件中註冊最頻繁的使用者名稱。

  - **網路流量事件中頻繁出現的應用程式**。根據選定時間段內的 EPP 應用程式資訊，在事件中註冊最頻繁的第三方應用程式。

  - **網路流量事件中頻繁出現的裝置**。選定時間段內事件中註冊最頻繁的裝置。

  - **按風險計數排名靠前的裝置**。在選定時間段內偵測到的風險的最常註冊的裝置。

  - **風險分數**。選定期間內風險按分數分佈的長條圖。長條圖對應分數的整數值。您可以將資料顯示模式變更為圓餅圖，以嚴重程度分佈風險。根據分數，風險的嚴重程度可能為*低*(0.0–3.9)、*中*(4.0–7.9) 或*高*(8.0–10.0)。

  - **自訂小部件**。您可以建立具有任意內容的小工具。例如，您可以使用自訂小工具，在**控制板**區段中以邏輯方式分隔小工具群組。

  - **裝置**。包含網路上的裝置的資訊（依裝置類別排列）。

  - **網路流量事件**。包含有關 NDR 事件和聚合事件的資訊，這些事件的上次可見日期和時間為最近。

  - **態勢感知**。有關目前已識別的系統安全威脅的通知（例如，偵測到 10 次未經授權的網路互動）。此小工具依重要性順序顯示通知。

  - **EPP 應用程式的防護**。受EPP 應用程式防護的電腦數量與未受 EPP 應用程式防護的電腦數量之比。餅圖中央顯示受防護和未受防護的電腦的總數。

如果 Kaspersky Anti Targeted Attack Platform 意識到滿足以下條件，則認為電腦受到 EPP 應用程式的防護：

- 電腦上安裝了 EPP 應用程式。
- 正在為 EPP 應用程式運行即時防護工作。
- EPP 應用程式與 Integration Server 的連線處於*活動*狀態。

如果至少有一個條件沒有滿足，則電腦被認為未受到 EPP 應用程式的防護。將針對 Kaspersky Anti Targeted Attack Platform 中所有包含 Windows 作業系統（任何版本）名稱作為所安裝作業系統的裝置，或裝置屬於下列類別之一，執行是否缺少EPP 應用程式防護的檢查：

- **伺服器**
- **工作站**

為了在 NDR 小工具中顯示正確的資訊，您必須配置 Central Node 和 Sensor 元件之間的日期和時間同步。

小工具僅顯示動態變化的基本資訊。如果您需要檢視詳細資訊（例如，有關有問題的裝置的資訊），您可以從**控制板**部分導航到應用程式 Web 介面的其他部分。您可以透過點擊小工具來導航 Web 介面。

新增小工具到目前佈局

若要新增小工具到目前佈局：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ≡ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 點擊**小部件**。
5. 在開啟的**管理小部件**視窗中：
   - 如果要新增與警示或規則關聯的小工具，請在**警示**或**前 10 個**清單中，選擇要新增的小工具旁的切換開關。
   - 如果要新增與 NDR 功能相關的小工具，請在 **[NDR]** 清單中，點擊要新增的小工具名稱旁的 + 按鈕。
6. 關閉**管理小部件**視窗並點擊**套用**。

小工具被新增到目前佈局。

在目前佈局中移動小工具

若要在目前佈局中移動小工具：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 在佈局中選擇要移動的小工具。
5. 點擊並按住小工具的上部可將小工具拖曳到佈局中的不同位置。
6. 點擊**套用**。

   目前佈局已儲存。

變更 NDR 小工具中資訊的顯示

新增 NDR 小工具後，它將根據預設設定顯示資訊。如果需要，您可以編輯顯示設定。

若要編輯 NDR 小工具顯示設定：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 在要配置的 NDR 小工具的右上角，點擊⚙按鈕。

   這將開啟顯示設定視窗。
5. 管理小工具的設定。

   根據所選的 NDR 小工具，視窗可能包含以下設定：

   - **變更名稱** – 如果勾選**變更名稱**核取方塊，您可以在**小工具名稱**欄位中為小工具定義任何名稱（不同於預設名稱）。自訂小工具中沒有**變更名稱**設定。
   - **小工具名稱** – 用於輸入與預設名稱不同的小工具名稱的欄位。
   - **編輯描述** – 如果勾選**編輯描述**核取方塊，您可以在**小工具描述**欄位中為小工具提供任何描述（不同於預設描述）。自訂小工具中缺少**編輯描述**設定。
   - **小工具描述** – 用於輸入與預設名稱不同的小工具名稱的欄位。
   - **重新整理週期** – 顯示的資訊更新的時間（以秒為單位）。

- **定義的背景** – 定義自訂小工具的背景顏色。您可以選擇與其中一個嚴重等級（**資訊**、**警告**或**嚴重**）相對應的背景顏色，或選取**中性**以停用背景著色。
- **顯示模式** – 決定資料在小工具中的顯示方式。您可以將資訊顯示配置為長條圖或圓餅圖。
- **將狀態為"已解決"的事件納入考量** – 如果選取**將狀態為"已解決"的事件納入考量**，小工具會顯示所有事件的資料。
- **包括已補救和已接受的風險** – 如果選取**包括已補救和已接受的風險**，小工具會顯示所有風險的資料。

6. 點擊**套用**。

從目前佈局移除小工具

若要從目前佈局移除小工具：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 點擊要從目前佈局移除的小工具右上角的 × 圖示。
   小工具被從應用程式 Web 介面視窗的工作區移除。
5. 點擊**套用**。

小工具被從目前佈局移除。

儲存佈局為 PDF

佈局中的 NDR 小工具未儲存至 PDF。

若要儲存佈局為 PDF：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ☰ 按鈕。
3. 在下拉清單中，選擇**儲存為 PDF**。
   這將開啟**另存為 PDF**視窗。
4. 在視窗下部的**佈局：**下拉清單中，選擇頁面方向。

5. 點擊**下載**。

   PDF 格式的佈局會儲存到您的電腦硬碟上的瀏覽器下載資料夾。

6. 點擊**關閉**。

配置小工具中的資料顯示週期

您可以設定在小工具中顯示資料的以下時段：

- **天**。
- **周**。
- **月份**。

對於 NDR 小工具，您可以使用以下時間段：

- **1 小時**
- **12 小時**
- **24 小時**
- **7 天**

您可以為每個單獨的 NDR 小工具配置一個資料顯示週期。

變更小工具中資訊的顯示

要配置小工具中一天的資料顯示（從早上 00:00 到晚上 11:59）：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在應用程式 Web 介面視窗右上角的資料顯示時段下拉清單中，選擇**天**。
3. 在**天**時段名稱右側的日曆中，選擇要在小工具中顯示資料的日期。

   控制板頁面上的所有小工具都會顯示選定時段的資料。

要在小工具上配置一週（週一到週日）的資料顯示：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在應用程式 Web 介面視窗右上角的資料顯示時段下拉清單中，選擇**周**。
3. 在**周**時段名稱右側的行事曆中，選擇要在小工具上顯示資料的週。

   控制板頁面上的所有小工具都會顯示選定時段的資料。

若要在小工具中顯示一個月（日曆月）的資料顯示：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在應用程式 Web 介面視窗右上角的資料顯示時段下拉清單中，選擇**月份**。
3. 在**月份**時段名稱右側的行事曆中，選擇要在小工具中顯示資料的月份。

   控制板頁面上的所有小工具都會顯示選定時段的資料。

變更小工具中資訊的顯示

若要配置 NDR 小工具中資訊的顯示：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在您要設定的 NDR 小工具的右上角，點擊代表您需要的時間間隔的按鈕。

   NDR 小工具顯示選定時間段的資訊。

配置小工具顯示縮放

您可以配置“警示”小工具的顯示比例。小工具右上角的≡圖示表示您可以配置該小工具的比例。

若要配置小工具的顯示比例：

1. 在應用程式 Web 介面視窗中，選擇**控制板**區域。
2. 在視窗的上部，點擊 ≡ 按鈕。
3. 在下拉清單中，選擇**自訂**。
4. 點擊小工具右上角的 ≡。
5. 在下拉清單中，選擇以下小工具顯示大小之一：
   - **1x1**。
   - **2x1**。
   - **3x1**。

   所選小工具的顯示比例已修改。
6. 為要設定顯示比例的所有小工具重複這些步驟。
7. 點擊**儲存**。

   小工具的顯示比例已配置。

“警示”類型小工具管理基礎知識

您可以設定所有“警示”小工具的顯示比例。

每個小工具的左側顯示用於小工具的顏色框。

範例：
按重要性分類的警示小工具顯示不同重要性的警示數量。
重要級別—根據 Kaspersky 的經驗，對於 Kaspersky Anti Targeted Attack Platform 使用者而言，警示重要性取決於此警示可能對電腦或企業 LAN 安全造成的影響。
在**按重要性分類的警示**小工具中，以下顏色對應於不同重要性等級：

- 紅色 — 警示具有高度重要性。
- 橙色 — 警示具有中度重要性。
- 綠色 — 警示具有較低重要性。

圖例的右側顯示了用於在小工具中顯示資料的所選時間段內每種類型的警示數量。

點擊具有每個警示類型的連結，您可以轉到應用程式 Web 介面的**警示**部分，檢視所有此類警示。警示將根據指定類型進行篩選。

範例：
按攻擊向量分類的警示小工具顯示**來自電子郵件的檔案**警示，它表示 Kaspersky Anti Targeted Attack Platform 在小工具的選定時段內從郵件流量中偵測到的檔案的數量。
點擊**來自電子郵件的檔案**連結可以開啟**警示**部分，顯示與在小工具選定時段內從郵件流量中偵測到的檔案相關的所有警示。資料將根據以下參數進行篩選：**物件類型** =檔案以及**物件來源**=郵件。

每個小工具的右側顯示資料列。縱軸顯示事件數，橫軸顯示警示的日期和時間。您可以編輯小工具中資料顯示的時間段，並選擇租用戶，以在小工具中顯示其資訊。

將滑鼠遊標放在每個資料列上，以顯示特定列所代表的時段內計數的警示數。預設顯示未處理的警示數。您可以透過選擇視窗右上角的**已處理**核取方塊來啟用已處理警示的顯示。在這種情況下，將顯示所有警示的總數。

事件小工具中的資訊

“**控制板**”部分的“**裝置**”小工具屬於 NDR 功能，並顯示有關應用程式已知裝置清單中的裝置的資訊。

此小工具提供以下資訊：

- 有關應用程式了解每個類別的多少台裝置的資訊。此資訊以類別圖示的形式顯示在小工具的上部。在每個類別圖示下，顯示該類別的裝置數量。如果應用程式已知的裝置清單包含有問題的裝置，則對應類別的圖示會帶有警告標記。
- 有問題的裝置類別清單。如果存在此類裝置，則該資訊將顯示在小工具的中間部分。用於顯示圖形元素的空間受小工具的大小限制。

有問題的裝置

在下列任何情況下，應用程式確定裝置存在問題：

- 裝置的狀態為*已授權*，安全狀態不是*正常*。
- 裝置具有*未授權*狀態。

如果任何裝置出現問題，則為清單中的每個類別顯示以下資訊：

- 包含類別圖示、文字描述以及存在問題的裝置數量的連結的行。
- 帶有裝置圖形表示的行。如果小工具有足夠的可用空間，則會顯示此行。行中的圖形的數量取決於 Web 瀏覽器視窗的目前大小。如果出現問題的裝置數量多於行中顯示的數量，則隱藏裝置的數量將以+ <设备数量>格式顯示在右側。

裝置圖形

裝置的圖形表示包括以下資訊：

- 裝置名稱。
- 裝置狀態。如果裝置的狀態為*未授權*，則顯示為圖示。
- 裝置安全狀態。顯示為圖形左邊框上的一條彩色線。線的顏色對應於*正常*、*警告*或*嚴重*狀態。

圖形會依以下順序顯示：

1. 帶有*未授權*狀態的裝置。
2. 有*嚴重*安全狀態的裝置。
3. 具有*警告*安全狀態的裝置。

從小工具導航到其他部分

您可以使用**裝置**小工具介面的元素導航到裝置表並顯示裝置的詳細資訊。可以使用以下選項來實現此目的。

前往裝置表並篩選表格

導航至裝置表並檢視所選類別中的所有裝置的資訊：

在**裝置**小工具的上部，點擊相關類別的圖示。

這將開啟包含裝置表格的**資產**部分。根據選定的裝置類別對表格進行篩選。

要導航到裝置表並檢視具有特定類別問題的裝置的資訊：

在有問題的裝置類別清單中，點擊包含相關類別裝置數量的連結。此連結顯示在帶有類別圖示和文字註釋**有問題**的行末。

這將開啟包含裝置表格的**資產**部分。表根據存在特定類別問題的裝置的 ID 進行篩選。

> 裝置表將根據您前往裝置表時**裝置**小工具中顯示的裝置 ID 進行篩選。導航到裝置表後，篩選條件不會更新。如果您想檢視目前有問題的裝置數量，可以再次前往**控制板**部分。

要轉到裝置表並檢視有關有問題的裝置的資訊：

在**裝置**小工具中，點擊代表相關裝置的圖形元素。

這將開啟包含裝置表格的**資產**部分。此表採用按裝置 ID 篩選的方式。

若要前往裝置表而不變更目前的表格篩選條件：

點擊“**裝置**”小工具中的“**顯示所有裝置**”。

這將開啟包含裝置表格的**資產**部分。此表顯示符合為裝置表配置的篩選條件的裝置。

轉至裝置表並搜尋表格

要轉到裝置表並在表中尋找裝置：

1. 在“**裝置**”小工具中，在“**搜尋裝置**”欄位中輸入搜尋查詢。
2. 點擊“**搜尋**”。

   這將開啟包含裝置表格的**資產**部分。表格中顯示符合您的搜尋條件的裝置。

事件小工具中的資訊

“**控制板**”部分中的“**網路流量事件**”小工具顯示有關 NDR 事件的一般資訊以及具有最近上次可見日期和時間的聚合事件。

此小工具顯示以下元素：

- 選定時間段內的 NDR 事件和聚合事件的直方圖。此資訊顯示在小工具的上部。直方圖以嚴重程度顯示 NDR 事件和聚合事件的分佈。
- 有關已註冊 NDR 事件和聚合事件的資訊清單，按最後可見日期和時間排序。此資訊顯示在小工具的中間部分。

NDR 事件和聚合事件的統計資訊

在 NDR 和聚合事件的分佈直方圖上，各列對應每個時間間隔的事件總數。長條圖中的顏色代表事件的嚴重等級。以下顏色對應於嚴重程度：

- 藍色。此顏色用於*低*嚴重等級的 NDR 事件和聚合事件。
- 黃色。此顏色用於*中*嚴重程度的 NDR 事件和聚合事件。
- 紅色。此顏色用於*高*嚴重程度的 NDR 事件和聚合事件。

您可以將滑鼠懸停在某個欄上來檢視有關它的資訊。彈出視窗顯示間隔的日期和時間，以及按嚴重程度劃分的 NDR 事件和聚合事件的數量。

時間間隔的長度取決於所選的顯示週期。您可以使用以下按鈕選擇直方圖的週期：

- **1 小時**：一小時週期，細分為一分鐘間隔。
- **12 小時**：12 小時週期，細分為一小時間隔。
- **24 小時**：24 小時週期，細分為一小時間隔。
- **7 天**：七天週期，細分為一天的間隔。

NDR 事件和聚合事件清單

“**網路流量事件**”小工具中的 NDR 事件和聚合事件清單以線上模式更新。具有最近的上次可見日期和時間的 NDR 事件和聚合事件位於清單頂部。

NDR 事件和聚合事件清單中顯示的元素數量受小工具大小的限制。

對於清單中的每個事件，都提供了以下資訊：

- NDR 事件或聚合事件的標題。
- 最後可見日期和時間。
- 代表 NDR 事件或聚合事件嚴重性的圖示：
  - – *低*嚴重等級
  - – *中*嚴重等級
  - – *高*嚴重等級

清單中的聚合事件以 標記。

從小工具導航到其他部分

您可以使用“**網路流量事件**”介面的控制項，前往事件表格並顯示 NDR 事件和聚合事件的詳細資訊。可以使用以下選項來實現此目的。

導覽至網路流量事件表並篩選表格

您可以透過點擊“**網路流量事件**”小工具清單中的事件來檢視 NDR 事件或聚合事件的詳細資訊。這樣做將開啟“**網路流量事件**”部分，其中的表格將根據所選 NDR 事件或聚合事件的 ID 進行篩選。篩選標準還包括從 NDR 事件或聚合事件的註冊日期和時間到目前時刻的時間段（不指定時間段的右邊界）。

如果想轉到網路流量事件表，但不改變“**網路流量事件**”部分中表格目前的篩選條件，請點擊“**網路流量事件**”小工具中的“**顯示所有事件**”連結。

導航至事件表並蒐索表格

要轉到裝置表並在表中尋找裝置：

1. 在“**網路流量事件**”小工具中，於“**搜尋事件**”欄位中輸入您的搜尋查詢。
2. 點擊“**搜尋**”。

   這將開啟“**網路流量事件**”部分。事件表顯示符合搜尋條件的 NDR 事件和聚合事件。

檢視應用程式模組和元件的工作狀況

如果應用程式的模組或元件遇到建議管理員檢視的錯誤，則會在應用程式 Web 介面的**控制板**區段上半部顯示黃色警告框。

具有“**管理員**”或“**安全稽核員**”角色的使用者可以存取有關使用者目前管理之 Central Node、PCN 或 SCN 伺服器的工作狀況資訊。

具有“**資深安全員**”、“**安全官**”或“**安全稽核員**”角色的使用者可以存取下列工作狀況資訊：

- 如果您使用的是獨立的 Central Node 伺服器，使用者可以存取有關使用者目前管理的 Central Node 伺服器的工作狀況的資訊。
- 如果您使用分散式解決方案和多組織用戶模式，且使用者正在管理 SCN 伺服器，則使用者可以存取該 SCN 伺服器針對使用者有權存取其資料之租用戶的工作狀況資訊。
- 如果您使用分散式解決方案和多組織用戶模式，且使用者正在管理 PCN 伺服器，則使用者可以存取該 PCN 伺服器和所有連線到該伺服器的 SCN 伺服器針對使用者有權存取其資料之租用戶的工作狀況資訊。

若要詳細了解應用程式模組及元件的工作情況，

點擊**檢視詳情**開啟**系統健康**視窗。

在**系統健康**視窗中，根據應用程式模組和元件的工作狀況會顯示以下圖示之一：

- OK 如果應用程式的模組和元件正常運作。
- 如果發現建議管理員注意的問題，則會顯示帶有問題數量的圖示（例如，1）。在這種情況下，詳細的問題資訊會顯示在**系統健康**視窗的右側。

系統健康視窗包含以下部分：

- **元件健康**包含應用程式執行所在之所有伺服器上的應用程式模組和元件運作狀態、隔離區以及資料庫更新資訊。

  例如：
  如果一個或多個應用程式元件的資料庫在 24 小時內未更新，則會在安裝應用程式模組和元件的伺服器名稱旁邊顯示 ! 圖示。
  要解決該問題，請確保可以存取更新伺服器。如果您使用代理伺服器連線到更新伺服器，請確保代理伺服器沒有與 Kaspersky Anti Targeted Attack Platform 伺服器連線相關的錯誤。

- **已處理**—傳入資料接收與處理狀態。狀態根據以下條件產生：
  - 從具有 Sensor 元件的伺服器、具有郵件感應器的伺服器或虛擬機、具有 Endpoint Agent 元件的主機接收資料的狀態。
  - 有關超出物件在佇列中等待應用程式模組和元件掃描的最長允許時間的資訊。
- **與伺服器的連線**—PCN 伺服器與已連線的 SCN 伺服器之間的連線狀態（如果您使用分佈式解決方案和多組織用戶模式，則會顯示）。

如果偵測到應用程式模組或元件的效能問題，您無法自行解決這些問題，請聯絡卡巴斯基技術支援。

管理技術

Kaspersky Anti Targeted Attack Platform 使用各種技術來分析網路流量。您可以單獨啟用或停用技術。對於裝置活動偵測（AM）技術，您可以選擇模式：學習模式或監控模式。

我們建議在預定的時間內啟用學習模式，以便應用程式在適當的時間自動將技術切換到監控模式。監控模式是技術的正常模式（與學習模式相反，在學習模式中應用程式僅累積資料以供將來使用）。設定學習模式時，您可以設定希望技術切換到監控模式的時間。

您可以為所有元件和監控點指定相同的技術設定，也可以為某些元件和/或監控點指定特殊設定。技術設定可以自動從父物件繼承到子物件。如果為元件或監控點啟用了技術繼承，則為父物件（Central Node 或 Sensor）指定的技術設定將套用於該物件。如果停用技術繼承，您可以為該元件或監控點上的技術配置特殊設定。

預設情況下，所有技術在應用程式安裝後均啟用。對於支援模式改變的技術，學習模式是預設啟用的。

啟用或停用技術

您可以啟用或停用 Central Node 和 Sensor 元件和監控點的技術。但是，如果在這些物件上停用技術繼承，則可以啟用和停用 Sensor 元件和監控點的技術。

一些技術包括可以單獨啟用或停用的方法。如果停用某種技術或方法，應用程式將不會監控使用該技術或方法的裝置互動。但是，您仍然可以管理與停用的技術或方法相關的應用程式設定（例如，新增或編輯規則）。

以下技術和方法支援啟用和停用：

- 資產管理，以下簡稱“AM”：
  - 裝置活動偵測。
  - 裝置資訊偵測。
  - 網路工作階段偵測。
- 入侵偵測，以下也稱為“IDS”：
  - 基於規則的入侵偵測。
  - ARP 欺騙偵測。
  - IP 協定異常偵測。
  - TCP 協定異常偵測。
  - 暴力攻擊和掃描偵測。

要改變技術和方法的狀態：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關元件或監控點的卡片。

   這將開啟一個視窗，其中包含有關元件或監控點的資訊。
3. 如果要為 Sensor 元件或監控點變更技術和方法的狀態，請將“**繼承伺服器技術**”切換開關設為“**已停用**”。
4. 使用視窗左側的切換開關來啟用或停用技術和/或方法。您可以透過點擊“**全部啟用**”或“**全部停用**”來同時啟用或停用所有技術和方法。
5. 啟用或停用某項技術或方法後，請等待變更套用完成。直到轉換至另一狀態完成之後，開關才會再次可用。

技術和方法的狀態被變更。

配置裝置活動偵測模式

您可以設定學習模式或啟用裝置活動偵測 (AM) 技術的監控模式。

若要變更和配置技術的模式：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關元件或監控點的卡片。
   這將開啟一個視窗，其中包含有關元件或監控點的資訊。
3. 如果要為 Sensor 元件或監控點配置技術模式，請將**繼承伺服器技術**切換開關設定為**已停用**。
4. 在技術名稱右側的下拉清單中，選擇一種模式（**學習**或**監控**）。
5. 選擇模式後，等待套用變更。在套用該模式之前，下拉清單中顯示“**變更**”狀態。
6. 如果您想指定技術必須從學習模式切換到監控模式的日期和時間，請點擊“**設定直到**”連結並選擇日期和時間。
   如果之前已配置日期和時間，則日期和時間將顯示在模式名稱旁邊。

技術的模式被配置。

管理技術繼承

如果您希望將為父物件配置的技術設定自動套用至 Sensor 元件或監控點，則可以啟用技術繼承。這表示 Sensor 元件取得 Central Node 元件的技術設定，而監控點取得新增監控點的元件（Central Node 或 Sensor）的設定。

如有必要，您可以停用 Sensor 元件或監控點的技術繼承。您可能需要這樣做來指定特殊的技術設定。

若要啟用或停用 Sensor 元件或監控點的技術繼承，請執行下列操作：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關元件或監控點的卡片。
   這將開啟一個視窗，其中包含有關元件或監控點的資訊。
3. 根據需要設定“**繼承伺服器技術**”切換開關。

Sensor 元件或監控點的技術繼承被啟用或停用。

檢視警示表

偵測到的針對企業 IT 基礎架構的針對性攻擊和入侵跡象將顯示為警示表。

警示表不會顯示至少符合以下條件之一的物件的資訊：

- 該物件在 KSN 資料庫中具有*受信任*信譽。
- 此物件由以下可信任供應商進行數位簽章：
  - Kaspersky。
  - Google。

- Apple。
- Microsoft。

有關這些警示的資訊會儲存到應用程式日誌中。您可以檢視該資訊。

當達到允許的最大警示數量時，應用程式日誌中的警示資訊每晚都會輪換：

- **(IDS) 入侵偵測系統**和**(URL) URL 信譽**元件產生的警示對於每個元件最多有 100000 個警示。
- 所有其他警示對於每個模組或元件最多有 20000 個警示。

如果您使用的是分佈式解決方案和多組織用戶模式，則在所有 SCN 上進行輪轉，然後再與 PCN 進行同步。同步後，所有已刪除的警示都會自動從 PCN 中刪除。

如果存在有效的 KATA+NDR 產品授權金鑰，則會產生 NDR 警示。產品授權金鑰過期後，已建立的警示仍然可供檢視，但不會建立新的警示。

警示表位於**警示**區段。它顯示一般的 KATA 警示和 NDR 警示。

> 預設情況下，此部分僅顯示有關使用者未處理的警示的資訊。若要也顯示有關已處理警示的資訊，請啟用視窗右上角的**顯示已關閉的警示**切換開關。

您可以按**已建立**或**已更新**、**重要級別**、**來源**、**目標**、**技術**和**狀態**欄對表中的警示進行排序。

警示表包含以下資訊：

1. **VIP**指定警示是否處於具有特殊存取權限的狀態。例如，具有**安全官**角色的使用者無法檢視 VIP 身分的警示。
2. **已建立**是建立警示的時間，**已更新**是警示更新的時間。
3. —根據卡巴斯基的經驗，對於 Kaspersky Anti Targeted Attack Platform 使用者而言，警示重要性取決於此警示可能對電腦或企業 LAN 安全造成的影響。

   警示可以具有以下重要性等級之一：

   - **高**，以符號標記—此警示具有高度重要性。
   - **中**，以符號標記—此警示具有中度重要性。
   - **低**，以符號標記—此警示的重要性較低。
4. **偵測到** — 偵測到的物件的一個或多個類別。例如，當應用程式偵測到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的檔案時，**偵測到**欄位就會對此警示顯示 Trojan-Downloader.JS.Cryptoload.ad 類別。
5. **詳細資訊**—警示摘要。例如：偵測到的檔案的名稱或惡意連結的 URL 位址。
6. **來源**—偵測到的物件來源位址。例如，這可以是傳送惡意檔案的電子郵件信箱，也可以是從中下載惡意檔案的 URL。
7. **目標**—偵測到的物件的目標位址。例如，這可以是組織的郵件網域（惡意檔案傳送到該郵件網域）的電子郵件信箱，也可以是企業 LAN 上的電腦（惡意檔案已下載到該電腦）的 IP 位址。
8. **技術**是掃描時產生警示的應用程式模組或元件的名稱。

技術列可能表示以下應用程式模組和元件：

- **(YARA) YARA**。
- **(SB) Sandbox** 。
- **(URL) URL 信譽**。
- **(IDS) 入侵偵測系統**。
- **(AM) 惡意軟體防護引擎**。
- **(TAA) 針對性攻擊分析器**。
- **(IOC) IOC**。
- **(NDR: IDS) 入侵偵測系統**。
- **(AA) 聚合警示**。

9. **狀態**—警示狀態取決於此警示是否由 Kaspersky Anti Targeted Attack Platform 的使用者處理。

   警示可具有以下狀態之一：

   - **新的**用於新警示。
   - **進行中**用於 Kaspersky Anti Targeted Attack Platform 使用者正在處理的警示。
   - **重新掃描**用於重新掃描物件而產生的警示。
   - **已關閉**用於已關閉的警示。如果**顯示已關閉的警示**切換開關已啟用，則已關閉的警示會顯示在表格中。

- **伺服器**是建立警示的伺服器名稱清單。伺服器屬於您在應用程式 Web 介面中管理的租用戶。如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄。
- **分配給**是對其指派了警示的使用者的名稱。

如果表格列中的資訊以連結形式顯示，您可以點擊該連結以開啟篩選器功能表，在功能表中選擇按此列進行篩選的設定。

警示更新和警示中的事件聚合涉及的特殊注意事項

如果在處理過程中發現與觸發的 TAA（IOA）規則具有相同 ID 的事件，**目標攻擊分析器**模組會更新警示中的主機清單和事件數量。更新於當日執行：從當日 00:00 到隔天 00:00。如果警示在更新時已關閉，系統會自動重新開啟它。

當同時滿足以下條件時，**入侵偵測系統**模組會在一個警示中合併已處理網路事件的資訊：

- 觸發規則的名稱，應用程式資料庫的版本以及來源都符合網路事件。
- 活動之間不超過 24 小時。

為滿足這些條件的所有網路事件顯示一個警示。警示通知僅包含有關第一個網路事件的資訊。

配置警示表顯示

您可以顯示或隱藏列並變更警示表中列的順序。

若要配置警示表顯示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。

2. 在表格的標題部分，點擊 ⚙ 。
   這將開啟**自訂表格**視窗。

3. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   > 必須選擇至少一個核取方塊。

4. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。

5. 如果要還原預設表格顯示設定，請點擊“**還原預設值**”。

6. 點擊**套用**。

警示表顯示已配置。

篩選、排序和搜尋警示

您可以篩選要在表格的一個或多個欄位的警示表中顯示的警示，或根據您指定的搜尋條件在某些表格列中搜尋警示。

您可以建立、儲存和移除篩選器，並根據已儲存的篩選器中指定的條件開始篩選和搜尋警示。

> 如果您使用分佈式解決方案和多組織用戶模式，則無法在 PCN 上儲存篩選器。

每個使用者的篩選器都儲存在建立它們的伺服器上。

您也可以按**已建立**或**已更新**、**重要級別**、**來源**、**目標**、**技術**和**狀態**欄對表中的警示進行排序。

> 預設情況下，此部分僅顯示有關使用者未處理的警示的資訊。若要也顯示有關已處理警示的資訊，請啟用視窗右上角的**顯示已關閉的警示**切換開關。

按 VIP 身分篩選警示

您可以根據☆條件在警示表中篩選和搜尋警示，該條件表示警示是否屬於具有特殊存取權限的警示。例如，具有**安全官**角色的使用者無法檢視 VIP 身分的警示。

若要按 VIP 身分篩選警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊**VIP** 列的標題以展開篩選器設定清單。

3. 配置警示篩選設定：

   - 如果您希望警示表僅顯示具有 VIP 身分的警示，請選擇**VIP**。

   - 如果您希望警示表顯示所有警示，請選擇**所有**。

   如果兩者均未選擇，則該表將顯示所有警示。

警示表僅顯示與您設定的篩選條件相符的警示。

按時間篩選並搜尋警示

您可以篩選警示，並根據以下條件在警示表中搜尋警示：**已建立**值，即警示的建立時間，以及**已更新**值，即警示更新的時間。

若要按時間篩選或搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊**已建立**或**已更新**連結開啟警示顯示時段清單。

3. 在下拉清單中，選擇下列警示顯示週期之一：

   - **所有**，如果您希望應用程式顯示表中所有警示。

   - **上一個小時**，如果您希望應用程式顯示表中最後一小時內發生的警示。

   - **最後一天**，如果您希望應用程式顯示表中最後一天內發生的警示。

   - **自訂範圍**，如果您希望應用程式顯示表中指定時段內發生的警示。

4. 如果您選擇了**自訂範圍**事件顯示範圍，請執行以下操作：

   a. 在開啟的日曆中，指定警示顯示時段的開始和結束日期。

   b. 點擊**套用**。

日曆關閉。

警示表僅顯示與您設定的篩選條件相符的警示。

按重要性等級篩選警示

您可以根據 **重要級別**條件篩選警示，該條件會根據 Kaspersky 的經驗，依此警示對電腦或公司區域網路安全可能產生的影響，向 Kaspersky Anti Targeted Attack Platform 使用者指出警示的重要性。

依重要性篩選警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊展開篩選器設定清單。
3. 選擇一個或多個以下警示重要性等級：
   - **低**，對於低重要性警示。
   - **中**，對於中重要性警示。
   - **高**，對於高重要性警示。

   如果未選擇值，表中將顯示所有重要性等級的警示。
4. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

按偵測到的物件的類別篩選和搜尋警示

您可以根據**偵測到**條件來篩選警示並在警示表中搜尋特定警示，該條件表示事件中偵測到的物件的一個或多個類別。例如，如果您希望表格顯示有關受特定病毒感染的檔案的警示，則可以根據此病毒的名稱設定篩選器。

若要依偵測物件的類別篩選或搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊**偵測到**連結以開啟篩選配置視窗。
3. 在下拉清單中，選擇下列警示篩選運算子之一：
   - **包含**
   - **不包含**
4. 在輸入欄位中，輸入類別名稱（例如，Trojan）或類別名稱中的幾個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

   警示表僅顯示與您設定的篩選條件相符的警示。

按取得的資訊篩選和搜尋警示

您可以根據“**詳細資訊**”條件來篩選警示並在警示表中搜尋特定警示，該條件引用了有關警示的簡要資訊。例如：偵測到的檔案的名稱或惡意連結的 URL 位址。

若要按取得的資訊篩選和搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇“**警示**”區域。

   這將開啟警示表。

2. 點擊**詳細資訊**連結以開啟篩選配置視窗。

3. 在左側的下拉清單中，選擇下列搜尋條件之一：

   - **詳細資訊**。搜尋將涵蓋偵測到的物件上的所有資料。
   - **ID**。
   - **檔案名稱**。
   - **檔案類型**。
   - **MD5**。
   - **SHA256**。
   - **URL**。
   - **網域**。
   - **使用者代理**。
   - **主旨**。
   - **HTTP 狀態**。
   - **物件來源**。
   - **物件類型**。
   - **自動傳送到 Sandbox**。
   - **TAA (IOA) 規則**。
   - **事件 ID (NDR)**。
   - **資產 ID (NDR)**。

4. 在右側的下拉清單中，選擇以下篩選運算子警示之一：

- **包含**。
- **不包含**。
- **等於**。
- **不等於**。

5. 在文字方塊中，輸入警示資訊的一個或多個字元。

6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

7. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

按來源位址篩選和搜尋警示

您可以根據**來源**條件來篩選警示並在警示表中搜尋特定警示，該條件表示警示的來源位址。例如，這可以是從其傳送惡意檔案的電子郵件信箱，也可以是企業 LAN 上的電腦（惡意檔案已下載到該電腦）的 IP 位址。

若要按來源位址篩選或搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊**來源**連結以開啟篩選配置視窗。

3. 在下拉清單中，選擇下列警示篩選運算子之一：

- **包含**
- **不包含**
- **匹配樣式**
- **與樣式不符**

4. 在文字方塊中，鍵入偵測到的物件的來源位址的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

按目的位址篩選並搜尋警示

您可以根據**目標**條件來篩選警示並在警示表中搜尋特定警示，該條件表示警示的目標位址。例如，這可以是組織的郵件網域（惡意檔案傳送到該郵件網域）的電子郵件信箱，也可以是企業 LAN 上的電腦（惡意檔案已下載到該電腦）的 IP 位址。

若要按目標位址篩選或搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊**目標**連結以開啟篩選配置視窗。
3. 在下拉清單中，選擇下列警示篩選運算子之一：
   - **包含**
   - **不包含**
   - **匹配樣式**
   - **與樣式不符**
4. 在文字方塊中，鍵入偵測到的物件的目標位址的一個或多個字元。
5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
6. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

按伺服器名稱篩選並搜尋警示

您可以根據**伺服器**條件在警示表中篩選和搜尋警示，該條件指示建立警示的伺服器名稱。

> 如果您使用分佈式解決方案和多組織用戶模式，則伺服器屬於您在應用程式 Web 介面中管理的租用戶。篩選僅在 PCN 上可用。

若要按伺服器名稱篩選或搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊**伺服器**展開建立警示的伺服器清單。

3. 選擇一個或多個伺服器名稱旁的核取方塊。

4. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

按技術名稱篩選並搜尋警示

您可以根據**技術**條件來篩選警示並在警示表中搜尋特定警示，該條件指示建立警示的應用程式模組或元件的名稱。

若要按技術名稱篩選警示：

1. 在應用程式 Web 介面視窗中，選擇“**警示**”區域。

   這將開啟警示表。

2. 點擊**技術**連結以開啟篩選配置視窗。

3. 在下拉清單中，選擇下列警示篩選運算子之一：

   - **包含**，如果您希望應用程式顯示由指定應用程式模組或元件產生的警示。
   - **不包含**，如果您希望應用程式隱藏由指定應用程式模組或元件產生的警示。
   - **等於**，如果您希望應用程式顯示由指定應用程式模組或元件產生的警示。
   - **不等於**，如果您希望應用程式隱藏由指定應用程式模組或元件產生的警示。

4. 在選定的警示篩選運算子右側的下拉清單中，選擇要用於篩選警示的技術的名稱：

   - **(YARA) YARA**。
   - **(SB) Sandbox**。
   - **(URL) URL 信譽**。
   - **(IDS) 入侵偵測系統**。
   - **(AM) 惡意軟體防護引擎**。
   - **(TAA) 針對性攻擊分析器**。
   - **(IOC) IOC**。
   - **(NDR: IDS) 入侵偵測系統**。
   - **(AA) 聚合警示**。

   例如，如果您希望應用程式顯示由 Sandbox 元件作為掃描結果產生的警示，請選擇“**包含**”篩選運算子以及 **(SB) Sandbox** 元件的名稱。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

依使用者處理狀態篩選和搜尋警示

您可以根據**狀態**條件篩選警示並在警示表中搜尋它們— 警示狀態取決於此警示是否由 Kaspersky Anti Targeted Attack Platform 使用者處理。

若要按 Kaspersky Anti Targeted Attack Platform 使用者對其的處理狀態來篩選或搜尋警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 若要將已處理的警示包含在篩選器中，請開啟視窗右上角的顯示已關閉的警示開關。

3. 點擊**狀態**連結以開啟可能的警示選項清單，這取決於 Kaspersky Anti Targeted Attack Platform 使用者對其的處理狀態。

4. 選擇以下值之一：

   - **新的**，如果您希望應用程式顯示尚未被任何使用者處理的新警示。
   - **進行中**，如果您希望應用程式顯示 Kaspersky Anti Targeted Attack Platform 使用者正在處理的警示。
   - **重新掃描**，如果您希望應用程式顯示重掃描引起的警示。
   - **已關閉**，如果您希望應用程式顯示已關閉的警示。如果啟用了**顯示已關閉的警示**切換開關，則此篩選器可用。

5. 點擊**套用**。

警示表僅顯示與您設定的篩選條件相符的警示。

按分配了警示的使用者的名稱篩選和搜尋警示

您可以透過“**分配給**”屬性在警示表中篩選或尋找警示，即分配了警示的使用者的名稱。

若要按分配了警示的使用者的名稱篩選或尋找警示：

1. 在應用程式 Web 介面視窗中，選擇“**警示**”區域。

   這將開啟警示表。

2. 點擊“**分配給**”連結以開啟篩選配置視窗。

3. 選擇您需要的使用者名稱旁的核取方塊。

如果您想在清單中尋找使用者名稱，請開始在文字方塊中輸入使用者名稱，然後選取找到的使用者名旁邊的核取方塊。

您可以選擇多個使用者名稱。

4. 點擊**套用**。

警示表中僅顯示指派給指定使用者的警示。

對表中的警示進行排序

您可以按**已建立**或者**已更新**、**重要級別**、**來源**、**目標**、**技術**和**狀態**列對表中的警示進行排序。

若要對警示表中的警示進行排序：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 如果您想按日期對警示進行排序，請點擊**已建立**右側的圖示之一（如果表格顯示警示建立日期）或**已更新**（如果表格顯示警示更新日期）列標題：

   - ↑ 在表格頂部顯示較新的警示。
   - ↓ 在表格頂部顯示較舊的警示。

3. 如果您想按重要性等級對警示進行排序，請點擊圖示右側的以下圖示之一：

   - ↑ 在表格頂部顯示重要性高的警示。
   - ↓ 在表格頂部顯示重要性低的警示。

4. 如果要按偵測到的物件的來源位址對警示進行排序，請點擊**來源**列標題右側的圖示之一：

   - ↑ 按升序排序。
   - ↓ 按降序排序。

5. 如果要按偵測到的物件的目的位址對警示進行排序，請點擊**目標**列標題右側的圖示之一：

   - ↑ 按升序排序。
   - ↓ 按降序排序。

6. 如果要按進行偵測的技術名稱對警示進行排序，請點擊**技術**列標題右側的圖示之一：

   - ↑ 按字母順序 A–Z 排序。
   - ↓ 按字母順序 Z–A 排序。

7. 如果您想按使用者處理狀態對警示進行排序，請點擊**狀態**列標題右側的圖示之一：

   - ↑ 按處理順序**新的 - 重新掃描 - 進行中 - 已關閉**對警示進行排序。
   - ↓ 按處理順序**已關閉 - 進行中 - 重新掃描 - 新的**對警示進行排序。

快速建立警示篩選器

若要快速建立警示篩選器：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。

2. 執行下列操作以便將篩選條件快速新增至正在建立的篩選器：

   a. 將滑鼠遊標置於包含您希望將其作為篩選條件新增的表列值的連結上。

   b. 左鍵點擊。
      這將開啟要對值執行的操作清單。

   c. 在開啟的清單中，選擇下列其中一項操作：

      - **新增到篩選器**，如果您想將該值包含在篩選條件中。

      - **從篩選器中排除**，如果您想從篩選條件中排除該值。

3. 如果您想要新增多個篩選條件到正在建立的篩選器中，請執行操作以將每個篩選條件快速新增至正在建立的篩選器。

警示表僅顯示與您設定的篩選條件相符的警示。

儲存篩選器

您可以將篩選器集儲存到警示表中。

若要儲存已套用的篩選器：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。

2. 為表格的一個或多個欄位配置篩選設定。

3. 點擊**儲存的篩選器**並選擇**儲存目前的篩選器**。
   篩選器將使用包含所選篩選設定的預設名稱進行儲存。

4. 如果您想要重新命名已儲存的篩選器：

   a. 點擊**儲存的篩選器**。
      顯示已儲存的篩選器的清單。

b. 將滑鼠懸停在篩選器上並點擊 。

c. 重新命名篩選器並點擊 。

篩選器已儲存。

重置警示篩選器

若要清除一個或多個篩選條件的警示篩選器：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊您想要清除其篩選條件的警示表列標題右側的 。

   > 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   警示表僅顯示與您設定的篩選條件相符的警示。

警示處理建議

有關AM（惡意軟體防護引擎）、SB（Sandbox）、YARA、IOC、IDS（入侵偵測系統）、NDR: IDS 和 AA 技術產生的警示的資訊顯示在視窗右側，包括有關處理這些警示的建議。

要檢視警示詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊包含想檢視其資訊的警示的行。

   這將開啟一個視窗，其中包含有關警示的資訊。

AM 警示處理建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示或事件的數量。

您可以遵循以下建議：

- 在**分類**下面，展開**尋找類似警示**清單。

一個可用於尋找類似警示的屬性清單、以及每個屬性的類似警示的數量將顯示。

選擇以下屬性之一：

- **通過 MD5**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**欄、MD5 雜湊篩選。您正在處理的警示中的檔案的 MD5 雜湊值以黃色突出顯示。
- **通過 SHA256**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**欄、SHA256 雜湊篩選。您正在處理的警示中的檔案的 SHA256 雜湊值以黃色突出顯示。
- **通過主機名稱**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的主機名稱以黃色突出顯示。
- **通過寄件者位址**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的電子郵件的寄件者位址以黃色突出顯示。
- **通過收件者位址**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**目標**列篩選。您正在處理的警示中的電子郵件的收件者位址以黃色突出顯示。
- **通過 URL**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**列、您正在處理的警示的 URL 篩選。

- 在**分類**下面，選擇**尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，由**RemoteIP**、**MD5**、**SHA256**、**URI**等選擇**偵測處理結果**事件類型和配置搜尋篩選器。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

  只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

- 在**調查**下面，選擇**尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，搜尋篩選器可依據例如 **RemoteIP**、**MD5**、**SHA256**、**URI** 進行設定。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

  只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

TAA 警示處理建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示或事件的數量。

您可以遵循以下建議：

- 在**分類**下面，展開**尋找類似警示**清單。

  一個可用於尋找類似警示的屬性清單、以及每個屬性的類似警示的數量將顯示。

  選擇以下屬性之一：

  - **按規則名稱（TAA 警示）**。點擊連結將在新的瀏覽器索引標籤中開啟**警示**警示表；警示按**偵測到**和**技術**列篩選，即用於建立警示的 TAA (IOA) 規則的名稱以及**(TAA) 針對性攻擊分析器**技術的名稱。
  - **按規則名稱（SB 警示）**。點擊連結將在新的瀏覽器索引標籤中開啟**警示**警示表；警示按**偵測到**和**技術**列篩選，即用於建立警示的 TAA (IOA) 規則的名稱以及**(SB) Sandbox**技術的名稱。

- 在**調查**下面，選擇**尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，搜尋篩選器可依據例如 **RemoteIP**、**MD5**、**SHA256**、**URI** 進行設定。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

  只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

SB 警示處理建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示或事件的數量。

您可以遵循以下建議：

- 在**分類**下面，展開**尋找類似警示**清單。

  一個可用於尋找類似警示的屬性清單、以及每個屬性的類似警示的數量將顯示。

  選擇以下屬性之一：

  - **通過 MD5**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**欄、MD5 雜湊篩選。您正在處理的警示中的檔案的 MD5 雜湊值以黃色突出顯示。
  - **通過 SHA256**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**欄、SHA256 雜湊篩選。您正在處理的警示中的檔案的 SHA256 雜湊值以黃色突出顯示。
  - **通過主機名稱**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的主機名稱以黃色突出顯示。
  - **通過寄件者位址**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的電子郵件的寄件者位址以黃色突出顯示。
  - **通過收件者位址**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**目標**列篩選。您正在處理的警示中的電子郵件的收件者位址以黃色突出顯示。
  - **通過 URL**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**列、您正在處理的警示的 URL 篩選。
  - **通過 Sandbox 中的 URL**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**表。警示按**詳細資訊**列、即您正在處理的警示的 URL 位址以及處理警示時 Sandbox 元件發現的相關所有 URL 篩選。

- 在**分類**下面，選擇**尋找類似的 EPP 事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，由**RemoteIP**、**MD5**、**SHA256**、**URI**等選擇**偵測處理結果**事件類型和配置搜尋篩選器。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

  只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

- 在**調查**下面，選擇**尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，搜尋篩選器可依據例如 **RemoteIP**、**MD5**、**SHA256**、**URI** 進行設定。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

  只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

IOC 警示處理建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示的數量。

您可以遵循以下建議：

- 在**分類**下面，選擇**通過主機名尋找類似警示**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的主機名稱以黃色突出顯示。
- 在**分類**下面，選擇**通過 IOC 尋找類似警示**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**偵測到**列、您正在處理的警示中的 IOC 檔案名稱篩選。
- 在**快速回應**部分，選擇**隔離 <主機名稱>**。這將開啟網路隔離規則建立視窗。

YARA 警示處理建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示或事件的數量。

您可以遵循以下建議：

- 在**分類**下面，展開**尋找類似警示**清單。

  一個可用於尋找類似警示的屬性清單、以及每個屬性的類似警示的數量將顯示。

  選擇以下屬性之一：

  - **通過 MD5**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**欄、MD5 雜湊篩選。您正在處理的警示中的檔案的 MD5 雜湊值以黃色突出顯示。
  - **通過 SHA256**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**欄、SHA256 雜湊篩選。您正在處理的警示中的檔案的 SHA256 雜湊值以黃色突出顯示。
  - **通過主機名稱**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的主機名稱以黃色突出顯示。
  - **通過寄件者位址**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的電子郵件的寄件者位址以黃色突出顯示。
  - **通過收件者位址**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**目標**列篩選。您正在處理的警示中的電子郵件的收件者位址以黃色突出顯示。
  - **通過 URL**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**列、您正在處理的警示的 URL 篩選。
- 在**分類**下面，選擇**通過主機名尋找類似警示**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，由**RemoteIP**、**MD5**、**SHA256**、**URI**等選擇**偵測處理結果**事件類型和配置搜尋篩選器。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

> 只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

- 在**調查**下面，選擇**尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，搜尋篩選器可依據例如 **RemoteIP**、**MD5**、**SHA256**、**URI** 進行設定。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

  只有當您使用 KEDR 功能並且已新增 KEDR 產品授權金鑰時，此操作才可使用。

- 在**快速回應**部分，選擇**隔離 <主機名稱>**。這將開啟網路隔離規則建立視窗。

IDS 警示處理建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示或事件的數量。

您可以遵循以下建議：

- 選擇應用程式 Web 介面視窗中"**分類**"部分的"**通過 IP 位址尋找類似警示**"子部分。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的主機名稱或 IP 位址以黃色突出顯示。

- 在**分類**下面，選擇**通過 URL 尋找類似警示**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**詳細資訊**列、URL 篩選。您正在處理的警示的 URL 以黃色突出顯示。

- 在**分類**下面，選擇**新增到排除項目**。

  這將開啟**將 IDS 規則新增到排除項目**視窗。如果要新增用於建立排除項警示的 IDS 規則，請在**敘述**欄位中輸入註釋並點擊**新增**。

  IDS 規則將會被新增到排除項目中，並顯示在應用程式 Web 介面中排除項目清單的**設定**部分、**排除項目**子部分、**IDS**索引標籤上。

- 在**調查**下面，選擇**通過 URL 尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，搜尋篩選器被設定為使用您正在處理的警示中的 **URI**。

- 在**調查**下面，選擇**通過 IP 位址尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中，搜尋篩選器被設定為使用您正在處理的警示中的 **RemoteIP**。

- 在**調查**部分，點擊**下載 IDS 工件**下載包含警示資料的檔案。

- 在**調查**部分，點擊**下載 PCAP 檔案**下載包含截獲的流量資料的檔案。

處理 NDR:IDS 和 AA 警示的建議

在視窗的右側部分，**建議**部分顯示您可以遵循的建議，以及與您正在處理的警示具有共同屬性的警示或事件的數量。

您可以遵循以下建議：

- 在**分類**下，選擇**通過源 IP 尋找類似警示**。點擊連結，即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示按**來源**列篩選。您正在處理的警示中的主機名稱或 IP 位址以黃色突出顯示。
- 在**分類**下，選擇**通過目標 IP 尋找類似警示**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示依**目標**欄篩選。您正在處理的警示中的主機名稱或 IP 位址以黃色突出顯示。
- 在**分類**下，選擇**通過 URL 尋找類似事件**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示依**詳細資訊**欄篩選。您正在處理的警示的 URL 以黃色突出顯示。
- 在**分類**下，選擇**通過入侵偵測規則尋找類似警示**。點擊連結即可在新的瀏覽器索引標籤中顯示**警示**警示表。警示依**詳細資訊**欄篩選。您正在處理的警示的掃描結果以黃色突出顯示。
- 在"**下載**"部分，點擊"**下載 PCAP 檔案**"下載包含截獲的流量資料的檔案。

檢視警示

Kaspersky Anti Targeted Attack Platform 的 Web 介面顯示使用者應該追蹤的以下類型的警示：

- 檔案已下載，或試圖將檔案下載到企業 LAN 電腦。應用程式在組織的本機網路的映像流量，或 HTTP 流量、FTP 流量以及 HTTPS 流量（如果管理員在代理伺服器上配置了 SSL 憑證更換）的 ICAP 資料裡偵測到此檔案。
- 檔案已傳送至企業 LAN 上的使用者的電子郵件信箱。應用程式在透過 POP3 或 SMTP 協定接收或從具有 Kaspersky Secure Mail Gateway 的虛擬機或伺服器（如果有在組織中使用）接收的電子郵件資訊副本中偵測到此檔案。
- 網站連結在企業 LAN 電腦上開啟。應用程式在組織的本機網路的映像流量，或 HTTP 流量、FTP 流量以及 HTTPS 流量（如果管理員在代理伺服器上配置了 SSL 憑證更換）的 ICAP 資料裡偵測到此網路連結。
- 偵測到在企業 LAN 電腦的 IP 位址或網域名稱上有網路活動發生。應用程式在組織的本機網路的映像流量中偵測到此網路活動。
- 在企業 LAN 電腦上的處理程序已啟動。應用程式偵測到使用安裝在屬於公司 IT 基礎架構的電腦上的 Endpoint Agent 元件的處理程序。

如果偵測到檔案，則在應用程式 Web 介面上將顯示以下資訊，具體取決於產生警示的應用程式模組或元件：

- 有關警示和偵測到的檔案的一般資訊（例如，在其上偵測到檔案的電腦的 IP 位址，以及偵測到的檔案的名稱）。
- 由AM 引擎執行的檔案病毒掃描結果。
- 由 Yara 模組執行的掃描檔案以檢查是否有入侵企業 IT 基礎架構的跡象的結果。
- Sandbox 元件執行的檔案行為分析的結果。
- 使用機器學習技術對雲端基礎架構中的 APK 執行檔進行分析的結果。

如果偵測到網站連接，應用程式 Web 介面中將顯示以下資訊，具體取決於產生警示的應用程式模組或元件：

- 有關警示和偵測到的網站連結的一般資訊（例如，在其上偵測到網站連結的電腦的 IP 位址，以及網站連結的位址）。
- 由 URL 信譽模組執行的連結掃描結果，旨在偵測惡意軟體跡象，釣魚 URL 位址以及駭客先前用於對企業 IT 基礎架構進行針對性攻擊的 URL 位址。

如果應用程式在企業 LAN 上偵測到電腦的 IP 位址或網域名稱的網路活動，則應用程式 Web 介面可能顯示以下資訊：

- 警示和偵測到的網路活動的詳細資訊。
- 由入侵偵測系統模組 (IDS) 執行的 Web 流量掃描結果，該掃描旨在根據預設規則偵測入侵企業 IT 基礎架構的跡象。
- 使用使用者定義的 IDS 規則執行的網路活動掃描的結果。

警示可由具有以下角色的使用者管理：“**安全官**”和“**資深安全員**”。具有“**安全稽核員**”角色的使用者可以檢視警示。

檢視警示詳細資訊

要檢視警示詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊包含想檢視其資訊的警示的行。

   這將開啟一個視窗，其中包含有關警示的資訊。

有關任何類型警示的一般資訊

警示詳情視窗的標題顯示警示 ID。根據警示是否具有 VIP 身分，☆ 或★圖示將顯示在狀態旁邊。

包含警示資訊的視窗的上部可能會顯示有關警示的以下一般資訊：

- **狀態**—警示狀態取決於此警示是否由 Kaspersky Anti Targeted Attack Platform 的使用者處理。
- **重要級別**—根據 Kaspersky 的經驗，對於 Kaspersky Anti Targeted Attack Platform 使用者而言，警示重要性取決於此警示可能對電腦或企業 LAN 安全造成的影響。
- **伺服器**是產生偵測的伺服器名稱。伺服器屬於您在應用程式 Web 介面中管理的組織。如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄。
- **主機** — 發生警示的電腦的網域名稱。
- **資料來源** — 資料來源。例如，SMTP Sensor 或 SPAN Sensor。

- **建立時間**是警示建立的時間。
- **更新時間**是更新警示詳情的時間。

您可以設定有關新警示的電子郵件通知。

物件資訊部分中的資訊

物件資訊部分可顯示有關偵測到的物件的以下事件資訊：

- 檔案名稱。

  為了擴大**複製值到剪貼簿**操作，請點擊帶有檔案名稱的連結。

- 檔案類型。例如，ExecutableWin32。

  在 Kaspersky TIP 上尋找按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。

  點擊**建立阻止規則**以阻止檔案運行。

  點擊**下載**將檔案下載到電腦的硬碟上。

  該檔案以密碼“infected”加密的 ZIP 壓縮檔案的形式下載。壓縮檔案內的檔案的名稱被檔案的 MD5 雜湊所替代。不顯示壓縮檔案內檔案的檔案副檔名。

- 檔案大小（以千位元組為單位）。
- **MD5** — 檔案的 MD5 雜湊。

  點擊具有**MD5**的連結將開啟一個清單，您可以從其中選擇以下操作之一：

  - **在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **建立阻止規則**。
  - **複製值到剪貼簿**。

- **SHA256** — 檔案的 SHA256 雜湊。

  點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

  - **在 Kaspersky TIP 上尋找**。
  - **在 virustotal.com 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **建立阻止規則**。
  - **複製值到剪貼簿**。

- **寄件者的電子郵件信箱** — 從中傳送包含檔案的郵件的電子郵件信箱。

- **收件者電子郵件信箱** — 包含檔案的郵件傳送到的一個或多個電子郵件信箱。
- **原始寄件者電子郵件信箱** — 從中傳送包含檔案的郵件的來源電子郵件信箱。
  此欄位由“已接收”標題中的資料填入。
- **原始收件者電子郵件信箱** — 包含檔案的訊息傳送到的來源電子郵件信箱。
  此欄位由“已接收”標題中的資料填入。
- **主旨** — 郵件主旨。
- **寄件者伺服器 IP** — 訊息傳遞鏈中第一個郵件伺服器的 IP 位址。
  點擊**寄件者伺服器 IP**連結將開啟一個清單，您可以從其中選擇以下操作之一：
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。
- **標頭** — 郵件訊息標題的擴充集合。例如，它可以包含有關郵件寄件者和收件者的電子郵件信箱，有關郵件中繼的郵件伺服器以及電子郵件中的內容類型的資訊。

“警示詳情”部分的資訊

警示詳細資訊部分可以顯示有關警示的以下資訊：

- 、 或 —根據 Kaspersky 的經驗，對於 Kaspersky Anti Targeted Attack Platform 使用者而言，警示重要性取決於此警示可能對電腦或企業 LAN 安全造成的影響。
- **時間**是警示建立的時間。
- **偵測到** — 偵測到的物件的一個或多個類別。例如，當應用程式偵測到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的檔案時，**偵測到**欄位就會對此警示顯示 Trojan-Downloader.JS.Cryptoload.ad 類別。
- **方法**—HTTP 請求方法。例如，Get、Post 或Connect。
- **URL** —偵測到的 URL。它還可能包含回應代碼。
  點擊具有 **URL** 的連結將開啟一個清單，您可以從其中選擇以下操作之一：
  - **通過 URL 在 Kaspersky TIP 上尋找**。
  - **通過網域名稱在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。
- **Referer**—使用者是透過此 URL 重新導向到需要關注的網站連結。在 HTTP 協定中，它是包含了請求來源URL 的用戶端請求頭之一。

- **目標 IP**—使用者或應用程式要求的資源的 IP 位址。

  點擊具有**目標 IP**的連結將開啟一個清單，您可以在其中選擇以下操作之一：

  - **在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。
- **使用者名稱**—其操作導致事件的使用者帳戶的名稱。
- **請求/回應**—請求和回應的長度。

“有關使用 NDR 技術進行掃描的資訊”部分中的資訊

“**關於使用 NDR 技術進行掃描的資訊**”部分可以顯示以下結果：

- **監控點**：導致註冊網路流量事件和建立警示的流量的監控點名稱。
- **網路接口 ID**：導致註冊網路流量事件和建立警示的流量的監控點 ID。

掃描結果部分的資訊

“**掃描結果**”部分可以顯示以下結果：

- 產生警示的應用程式模組或元件的名稱。
- 偵測到的物件的一個或多個類別。例如，可以顯示病毒名稱：Virus.Win32.Chiton.i。
- 產生警示的 Kaspersky Anti Targeted Attack Platform 模組和元件的資料庫版本。
- 應用程式模組或元件執行的警示掃描結果：
  - **YARA**—對 Central Node 接收的檔案和物件進行串流掃描的結果，或掃描具有 Endpoint Agent 元件的主機的結果。可能值：
    - 在YARA 規則下偵測到的檔案的類別（例如：可能會顯示 susp_fake_Microsoft_signer 類別名稱）。

      對於串流掃描顯示。

      點擊**建立阻止規則**以阻止檔案運行。

      在 Kaspersky TIP 上尋找按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。
    - 檔案路徑和/或記憶體傾印的名稱。

      使用 Kaspersky Endpoint Agent 元件掃描主機時顯示。

點擊具有檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

您可以點擊**建立工作**建立以下工作：

- **獲取資料** → **檔案**，**磁碟鏡像**，**記憶體傾印**。
- **刪除檔案**。
- **隔離檔案**。

點擊**建立阻止規則**以阻止檔案運行。

- **在 Kaspersky TIP 上尋找**按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。

  您可以點擊**在隔離區檢視**以顯示隔離物件的詳細資訊。

- **SB** （ Sandbox ）— Sandbox 元件執行的檔案行為分析的結果。

  您可以點擊**Sandbox 偵測**開啟一個視窗，其中包含有關檔案行為分析結果的詳細資訊。

  > 只有當 Sandbox 偵測該檔案時，才會顯示檔案行為分析結果。如果檔案上傳至系統，然後在 Sandbox 中掃描，但元件未偵測到威脅，則不會顯示結果。

  在 Kaspersky TIP 上尋找按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。

  點擊**建立阻止規則**以阻止檔案運行。

  您可以透過點擊**下載偵錯資訊**下載所有作業系統中檔案行為分析的詳細記錄。

  該檔案以密碼“infected”加密的 ZIP 壓縮檔案的形式下載。壓縮檔案內的已掃描檔案的名稱被檔案的 MD5 雜湊所替代。不顯示壓縮檔案內檔案的檔案副檔名。

  > 預設狀態下，用於儲存檔案行為掃描日誌的最大硬碟空間在所有作業系統上均為 300 GB。達到此限制後，應用程式將刪除舊的檔案行為掃描日誌，並用新日誌替代。

- **URL** （ URL 信譽 ）是惡意、網路釣魚 URL 或攻擊者先前用於對企業 IT 基礎架構進行針對性攻擊的 URL 的類別。

- **AM** （ 惡意軟體防護引擎 ） — 根據防毒資料庫偵測到的物件的類別。例如，可以顯示病毒名稱：Virus.Win32.Chiton.i。

  點擊該連結可顯示卡巴斯基威脅資料庫中物件的類別。

  在 Kaspersky TIP 上尋找按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。

  點擊**建立阻止規則**以阻止檔案運行。

  點擊**下載**將檔案下載到電腦的硬碟上。

- **TAA** （ 針對性攻擊分析器 ） — 有關使用針對性攻擊分析器技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

  點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

- **IOC** – 用於建立警示的 IOC 檔案的名稱。

  選擇 IOC 檔案以開啟包含 IOC 掃描結果的視窗。

  點擊**與警示相關的所有事件**以在新的瀏覽器索引標籤中顯示**威脅搜尋**事件表。在搜尋條件中配置搜尋篩選器，例如按**MD5**、**FileFullName**。篩選值由您正在處理的警示的屬性填入。例如，警示中檔案的 MD5 雜湊值。

- **AA**（聚合警示）意味著警示是由於處理 Kaspersky Anti Targeted Attack Platform 使用 NDR API 方法從第三方系統接收的聚合和嵌套 NDR 事件而建立的。這些事件使用 EXT 技術註冊。

- **NDR: IDS**（入侵偵測系統）意味著警示是由於處理 NDR 事件而建立的，該事件是由於檢測到流量中有指示攻擊的異常（例如，檢測到 ARP 欺騙指示器的 NDR 事件）而產生的。對應於導致建立警示的網路流量事件的名稱。

IDS 規則部分中的資訊

IDS 規則部分以十六進位編輯器矩陣的形式顯示有關 IDS（入侵偵測系統）技術發出的警示的資訊。

*十六進位編輯器*是用於編輯資料的應用程式，其中資料表示為位元組序列。

矩陣的上半部顯示 IDS 規則的長度。

矩陣的左側部分以文字格式顯示規則的資料。

IDS 規則部分的**規則詳情**子部分以 Suricata 格式顯示 IDS 規則的標題和 IDS 警示的資料。例如，它可以顯示有關流量方向的資訊（`flow`）、HTTP 請求方法（`http_method`）、HTTP 標頭（`http_header`）、安全性 ID（`sid`）。

URL 部分的資訊

在 **URL** 下方，會顯示觸發警示的 URL。

點擊 **URL** 連結將開啟一個清單，您可以從中選擇以下其中一項操作：

- **尋找事件**。
- **尋找警示**。
- **通過 URL 在 Kaspersky TIP 上尋找**。
- **通過網域名稱在 Kaspersky TIP 上尋找**。
- **複製值到剪貼簿**。

“偵測相關裝置的 IP 位址”部分的資訊

在“**警示相關裝置的 IP 位址**”下，顯示與警示相關的裝置資訊：

- **協議**。
- **來源 IP**。
- **來源 MAC**。
- **目標 IP**。
- **目的地 MAC**。

網路事件部分的資訊

網路事件部分可顯示使用者在電腦上造訪之網站連結的以下資訊：

- **日期**和**時間**—網路事件的日期和時間。
- **方法**—HTTP 請求的類型，例如 GET 或 POST。
- **來源 IP**—開啟網站連結之電腦的 IP 位址。
- **目標 IP**—開啟網站連結之電腦的 IP 位址。
- **URL** —HTTP 請求的類型（例如 GET 或 POST）以及網站的 URL。

  如果針對從流量中提取的檔案建立警示，則 URL 會指定用於傳輸從中提取檔案的流量的協定。可能的協定：HTTP、HTTPS、FTP、SMTP、POP3、SMB、NFS。

  點擊具有 URL 的連結將開啟一個清單，您可以從其中選擇以下操作之一：

  - **通過 URL 在 Kaspersky TIP 上尋找**。
  - **通過網域名稱在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。
- **使用者代理**—有關曾用於下載檔案、嘗試下載檔案或開啟網站連結的瀏覽器的資訊。它是 HTTP 請求中包含的文字字串，通常包含瀏覽器的名稱和版本以及用戶電腦上安裝的作業系統的名稱和版本。

Sandbox 掃描結果

只有當 Sandbox 偵測該檔案時，才會顯示檔案行為分析結果。如果檔案上傳至系統，然後在 Sandbox 中掃描，但元件未偵測到威脅，則不會顯示結果。

Sandbox 中的物件掃描結果視窗可以顯示以下詳細資訊：

- **檔案** — 掃描檔案的完整名稱和路徑。
- **檔案大小** — 檔案的大小。
- **MD5** — 檔案的 MD5 雜湊。
- 點擊具有**MD5**的連結將開啟一個清單，您可以從其中選擇以下操作之一：
  - **在 Kaspersky TIP 上尋找。**
  - **尋找事件。**
  - **尋找警示。**
  - **建立阻止規則。**
  - **複製值到剪貼簿。**
- **偵測到** — 偵測到的物件的一個或多個類別。例如，當應用程式偵測到感染了 Trojan-Downloader.JS.Cryptoload.ad 病毒的檔案時，**偵測到**欄位就會對此警示顯示 Trojan-Downloader.JS.Cryptoload.ad 類別。
- **處理時間** — 掃描檔案的時間。
- **資料庫版本** — 建立警示的 Kaspersky Anti Targeted Attack Platform 模組和元件資料庫的版本。

您可以點擊視窗右上角的**新的阻止規則**以防止檔案運行。

為 Sandbox 元件執行掃描的每個作業系統提供有關檔案行為分析結果的資訊。對於 Windows 7 作業系統（64 位元），您可以檢視兩種 Sandbox 元件掃描模式的檔案活動日誌：**快速掃描模式**和**完整日誌模式**。

以下活動日誌可用於每種掃描模式：

- **活動清單** — 作業系統中的檔案操作。
- **活動圖表** — 檔案分析過程的圖形表示。
- **HTTP 活動日誌** — 檔案的 HTTP 活動記錄。它包含以下資訊：
  - **目標 IP** — 此檔案試圖從作業系統轉到的 IP 位址。
  - **方法** — HTTP 請求方法，例如 GET 或 POST。
  - **URL** — 檔案試圖從作業系統開啟的網站連結的 URL。

點擊**目標 IP**列中的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **在 Kaspersky TIP 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

點擊 **URL** 列中的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **通過 URL 在 Kaspersky TIP 上尋找**。
- **通過網域名稱在 Kaspersky TIP 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

- **IDS 活動日誌** — 檔案的網路活動記錄。它包含以下資訊：
  - **來源 IP** — 在其中儲存檔案的主機的 IP 位址。
  - **目標 IP** — 此檔案試圖從作業系統轉到的 IP 位址。
  - **方法** — HTTP 請求方法，例如 GET 或 POST。
  - **URL** — 檔案試圖從作業系統開啟的網站連結的 URL。

  點擊**目標 IP**列中的連結將開啟一個清單，您可以從其中選擇以下操作之一：

  - **在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。

  點擊 **URL** 列中的連結將開啟一個清單，您可以從其中選擇以下操作之一：

  - **通過 URL 在 Kaspersky TIP 上尋找**。
  - **通過網域名稱在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。

- **DNS 活動日誌** — 檔案的 DNS 活動記錄。它包含以下資訊：
  - 請求類型（請求或回應）。
  - **DNS 名稱** — 伺服器的網域名稱。
  - **類型** — DNS 請求的類型，例如 A 或 CNAME。
  - **主機** — 與之互動的主機名稱或 IP 位址。

  點擊**DNS 名稱**或**主機**欄中的連結將開啟一個清單，您可以從其中選擇以下操作之一：
  - **在 Kaspersky TIP 上尋找**。
  - **尋找事件**。
  - **尋找警示**。
  - **複製值到剪貼簿**。
- **螢幕截圖** — 包含在檔案執行期間拍攝的螢幕截圖。

  您可以在應用程式 Web 介面中檢視螢幕截圖，或下載包含螢幕截圖的 Zip 壓縮檔案。

您可以點擊每個掃描模式（**快速掃描模式**和**完整日誌模式**）下方的**下載完整日誌**，將各作業系統中的檔案行為分析記錄下載到您的電腦上

IOC 掃描結果

根據處理物件的類型，入侵指標搜尋結果視窗指示器可能顯示以下資訊：

- **ARP 協議**：
  - ARP 表中的 IP 位址。
  - ARP 表中的物理位址。
- **DNS 記錄**：
  - DNS 記錄的類型和名稱。
  - 受防護電腦的 IP 位址。
- **Windows 日誌事件**：
  - 事件日誌中的條目 ID。
  - 日誌中的資料來源名稱。
  - 日誌名稱。
  - 使用者帳戶。
  - 事件時間。

- **檔案**：
  - 檔案的 MD5 雜湊。
  - 檔案的 SHA256 雜湊。
  - 檔案完整名稱（包括路徑）。
  - 檔案大小。
- **連接埠**：
  - 掃描時與其建立連線的遠端 IP 位址。
  - 掃描時與其建立連線的遠端連接埠。
  - 本機介面卡的 IP 位址。
  - 本機介面卡上開啟的連接埠。
  - 作為數字的協議（根據 IANA 標準）。
- **處理程序**：
  - 處理程序名稱。
  - 處理程序參數。
  - 處理程序檔案路徑。
  - 處理程序的 Windows ID (PID)。
  - 父處理程序的 Windows ID (PID)。
  - 啟動處理程序的使用者帳戶名稱。
  - 處理程序開始的日期和時間。
- **服務**：
  - 服務名稱。
  - 服務說明。
  - DLL 服務的路徑和名稱（對於 Svchost）。
  - 服務的可執行檔的路徑和名稱。
  - 服務的 Windows ID (PID)。
  - 服務類型（例如，核心驅動程式或介面卡）。
  - 服務狀態。
  - 服務運作模式。

- **使用者**：
  - 使用者帳戶名稱。
- **卷**：
  - 卷名。
  - 卷符。
  - 卷類型。
- **登錄檔**：
  - Windows 登錄機碼。
  - 登錄檔配置單元值。
  - 登錄機碼的路徑（沒有組態單元或值名稱）。
  - 登錄檔參數。
- **環境變量**：
  - 受防護電腦的實體（MAC）位址。
  - 系統（環境）。
  - 作業系統名稱和版本。
  - 受防護裝置的網路名稱。
  - 受防護電腦所屬的網域和群組。

IOC部分顯示 IOC 檔案的結構。如果處理的物件與 IOC 規則的條件匹配，則該條件會反白顯示。如果處理的物件符合多個條件，則整個分支的文字會被反白顯示。

主機部分中的資訊

主機部分顯示有關在其上觸發了 TAA (IOA) 規則的主機的以下資訊：

- **主機名稱**—事件在其中發生的電腦的 IP 位址或網域名稱。點擊連結將開啟**威脅搜尋**部分，其中有包含所選規則的 ID 和所選主機的搜尋條件。
- **IP**—事件在其中發生的電腦的 IP 位址。

  如果您使用動態 IP 位址，該欄位會顯示建立或更新警示時指派給電腦的 IP 位址。

  該應用程式不支援 IPv6。如果您使用的是 IPv6，則不會顯示電腦的 IP 位址。

- **事件數量**—主機上發生的事件數。
- **尋找事件**。點擊連結將開啟**威脅搜尋**部分，其中有包含所選規則的 ID 的搜尋條件。

“變更日誌”部分中的資訊

變更日誌部分可以顯示以下偵測資訊：

- 警示修改的日期和時間。
- 修改的作者。
  例如，**系統**或應用程式使用者名稱。
- 警示發生的修改。
  例如，警示可能被指派給 VIP 群組，或被標記為已處理。

傳送警示資料

您可以向卡巴斯基提供有關警示的資料（URL 信譽和“IOC”技術除外）進行進一步分析。

為此，您必須將警示資料複製到剪貼簿，然後透過電子郵件將其傳送至卡巴斯基。

警示資料可能包含被視為機密的組織資訊。您必須諮詢組織的安全部門並獲得批准，才能將此資料傳送到卡巴斯基以進行進一步分析。

若要將警示詳情複製到剪貼簿：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊包含想檢視其資訊的警示的行。
   這將開啟一個視窗，其中包含有關警示的資訊。
3. 點擊包含警示資訊的視窗下部的**向卡巴斯基提供警示詳細資訊**連接。
   這將開啟**顯示更多**視窗。
4. 檢視要傳送至卡巴斯基的警示資料。
5. 如果您想複製此資料，請點擊**複製到剪貼簿**按鈕。
   警示資料將被複製到剪貼簿。您將可以將其傳送到卡巴斯基進行進一步分析。

檢視警示關係

從警示卡中，您可以前往與此警示相關的事件、資產或網路工作階段表。

若要檢視警示的關係：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。

2. 開啟您想要檢視其關係的警示。

3. 在警示卡中，點擊“**顯示相關**”按鈕旁邊的箭頭。

4. 從清單中選擇警示關係：

   - **事件**。
   - **資產**。
   - **網路工作階段**。

   這將開啟 Web 介面中帶有關係表的相應部分。

在警示上執行的使用者操作

使用**資深安全員**或**安全官**帳戶管理應用程式 Web 介面時，您可以對警示採取以下操作：

- 為自己或應用程式 Web 介面其他使用者指派警示。
  您可以透過根據使用者處理狀態篩選警示來檢視指派給特定使用者的所有警示。

- 將警示標記為已處理。
  您可以透過根據使用者處理狀態篩選警示來檢視所有由特定使用者處理過的警示。

- 為警示新增註釋。
  您可以透過根據收到的資訊篩選警示，依註釋中的關鍵字找到有註釋的警示。

- 將警示標記為 VIP。
  此操作僅適用於具有**資深安全員**角色的使用者。具有此角色的使用者可以透過按 VIP 身分篩選警示來檢視具有 VIP 身分的所有警示。

> 具有**安全稽核員**角色的使用者可以檢視有關警示的資訊，但無法編輯此資訊。

將警示分配給特定使用者

具有“**資深安全員**”角色的使用者可以向自己或具有“**資深安全員**”或“**安全官**”角色的應用程式 Web 介面的其他使用者指派一個警示或多個警示。

若要為自己或應用程式 Web 介面其他使用者指派警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 選擇您想要指派給自己或其他使用者的一個或多個警示旁的核取方塊。

   您可以透過選擇表標題中的核取方塊來選擇所有警示。

3. 在視窗下部顯示的窗格中，透過點擊“**分配給**”按鈕右側的箭頭展開使用者清單。

4. 選擇您要為其指派警示的使用者。

   這將開啟操作確認視窗。您也可以留下評論，該評論將顯示在警示變更歷史記錄中。

5. 點擊**繼續**。

該警示將被指派給選定使用者。

您可以透過根據使用者處理狀態篩選警示來檢視指派給特定使用者的所有警示。

> 具有**安全稽核員**角色的使用者無法向自己或應用程式 Web 介面的其他使用者指派警示。具有**資深安全員**和**安全官**角色的使用者也無法將警示指派給具有**安全稽核員**角色的使用者。

具有**資深安全員**和**安全官**角色的使用者在管理警示時，可以將該警示指派給自己或具有**資深安全員**或**安全官**角色的應用程式 Web 介面其他使用者。

若要在管理警示時將警示指派給自己或其他使用者：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 開啟您想要指派給您自己或應用程式的其他使用者的警示。

   這將開啟警示卡。

3. 如果您要將警示指派給自己，請點擊**分配給 @我**。

4. 如果您要將警示分配給應用程式的另一個使用者，請點擊**分配給**按鈕右側的箭頭並選擇您想要指派警示的使用者。

此警示被指派給選定使用者。

標記單個警示處理的完成

> 具有**安全稽核員**角色的使用者無法指派和處理警示。

若要關閉警示表中的單個警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 在要關閉的警示的**狀態**列中，點擊警示的狀態。

3. 在操作清單中，選擇**關閉警示**。

   警示已關閉。

若要在管理警示時關閉警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 開啟您想關閉的警示。

3. 在視窗的右上角，點擊**關閉警示**。

   警示已關閉。如果警示已指派給其他使用者，它會被標記為已由您處理。

您可以根據使用者處理狀態篩選警示或透過使用**顯示已關閉的警示**切換開關來檢視所有由特定使用者處理過的警示。

如果在一天內（早 00:00 到晚 11:59）收到基於使用 TAA (IOA)、IDS 或 URL 技術的掃描的類似於已處理警示的警示，則應用程式會建立新警示或更新狀態為**新的**或者**進行中**的相同警示的資訊。

關閉NDR 警示時，與該警示關聯的聚合事件和嵌套NDR 事件將被標記為已解決，並且與這些事件關聯的其他警示也將關閉。如果重新開啟已關閉的 NDR 警示，則不會重新開啟相關的已關閉的 NDR 事件。

標記警示處理的完成

> 擁有“**安全官**”角色的使用者無法對警示執行批次操作。具有**安全稽核員**角色的使用者無法指派和處理警示。

若要關閉一個或多個警示：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 選擇要關閉的警示對面的核取方塊。

   您可以透過選擇表標題中的核取方塊來選擇所有警示。

3. 在視窗下部顯示的窗格中，點擊**關閉警示**按鈕。

   這將開啟操作確認視窗。

   您也可以留下評論，該評論將顯示在警示變更歷史記錄中。

4. 點擊**繼續**。

   選定的警示被關閉。如果警示已指派給其他使用者，它們被標記為已由您關閉。

您可以根據使用者處理狀態篩選警示或透過使用**“顯示已關閉的警示”**切換開關以檢視所有關閉的警示。

如果在一天內（早 00:00 到晚 11:59）收到基於使用 TAA (IOA)、IDS 或 URL 技術的掃描的類似於已處理警示的警示，則應用程式會建立新警示或更新狀態為**新的**或者**進行中**的相同警示的資訊。

關閉NDR 警示時，與該警示關聯的聚合事件和嵌套NDR 事件將被標記為已解決，並且與這些事件關聯的其他警示也將關閉。如果重新開啟已關閉的 NDR 警示，則不會重新開啟相關的已關閉的 NDR 事件。

修改 VIP 警示的狀態

具有**資深安全員**角色的使用者可以為警示指派 VIP 身分或清除警示的 VIP 身分。

要切換警示的 VIP 身分：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 選擇要為其變更VIP 身分的警示的核取方塊。

   您可以透過選擇表標題中的核取方塊來選擇所有警示。

3. 執行以下操作之一：

   - 如果您想將警示標記為 VIP，請點擊視窗下部出現的窗格中的**標記為 VIP**按鈕。
   - 如果要從警示中刪除 VIP 狀態，請在視窗下部顯示的窗格中的**“標記為 VIP”**下拉清單中選擇**“標記為非 VIP”**。

   這將開啟操作確認視窗。

   您也可以留下評論，該評論將顯示在警示變更歷史記錄中。

4. 點擊**繼續**。

警示的 VIP 身分已變更。

具有**資深安全員**和**安全稽核員**角色的使用者可以透過按 VIP 身分篩選警示來檢視具有 VIP 身分的所有事件。

為警示新增註釋

具有**資深安全員**和**安全官**角色的使用者可以向警示新增註釋。

若要為警示新增註解：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 選擇您要新增註釋的警示。

   這將開啟一個視窗，其中包含有關警示的資訊。

3. 在**變更日誌**部分下的註記輸入欄位中，為警示輸入註解。

4. 點擊**新增**。

   該註釋將新增到警示中，並顯示在該警示的**變更日誌**部分。

您可以透過根據收到的資訊篩選警示，依註釋中的關鍵字找到有註釋的警示。

> 具有**安全稽核員**角色的使用者可以檢視警示的註釋，但無法編輯註釋。

監控網路流量事件

該應用程式在分析網路流量時會註冊事件。網路流量分析是 NDR 功能的一部分。

網路流量事件（也稱為 *NDR 事件*）是包含相關資訊的記錄，這些資訊涉及偵測到網路流量中需要資訊安全專業人員注意的特定變更或狀況。NDR 事件被註冊並傳送到 Central Node。伺服器會處理收到的事件並將其儲存在資料庫中。

*聚合事件*是一種特殊事件，會在收到特定的 NDR 事件序列時註冊。聚合事件將具有一些共同特徵或與相同流程相關的 NDR 事件分組。

應用程式根據事件關聯規則註冊聚合事件。*事件關聯規則*描述掃描事件序列的條件。當偵測到符合規則條件的一系列 NDR 事件時，應用程式會註冊一個提及觸發規則名稱的聚合事件。聚合事件註冊的系統事件類型代碼為 8000000001。

事件關聯規則內建在應用程式中，無論安全性政策如何都會應用。

> 應用程式安裝後，使用原有的事件關聯規則。為了提高規則的有效性，卡巴斯基定期使用規則集更新資料庫。您可以透過安裝更新來更新關聯規則。

Kaspersky Anti Targeted Attack Platform 伺服器會根據註冊事件類型指定的設定來註冊 NDR 事件。您可以在"配置事件類型"部分配置這些設定。

為了減少不需要使用者注意的頻繁重複 NDR 事件的數量，您可以建立事件允許規則。滿足允許規則的 NDR 事件不會被註冊。例如，您可以使用允許規則暫時停用來自特定監控點的所有事件的註冊。您可以在"**設定**"部分的"**允許規則**"子部分中檢視事件的允許規則。為此類規則指明了 EVT 類型。

該應用程式將 NDR 事件和聚合事件儲存在 Central Node 的資料庫中。儲存記錄的總量不能超出配置的限制。如果數量超出限制，應用程式會自動刪除最舊的記錄。但是，如果配置了最短儲存期限，則刪除時間小於最短期限的記錄時，相應的訊息將記錄在應用程式訊息日誌中。您可以配置事件和事故儲存設定。

您可以在"**網路流量事件**"部分檢視有關 NDR 事件和聚合事件的資訊。此部分顯示有關 NDR 事件和聚合事件的詳細資訊，並允許從伺服器資料庫載入任何時期的資訊。

具有"**安全官**"或"**資深安全員**"角色的使用者可以使用網路流量事件操作。具有"**安全稽核員**"角色的使用者可以檢視事件。

如果存在有效的 KATA+NDR 產品授權金鑰，則會產生 NDR 事件。產品授權金鑰過期後，建立的事件仍然可供檢視，但不會建立相關警示。

NDR 事件分數和嚴重程度

Kaspersky Anti Targeted Attack Platform 中的 NDR 事件的評分範圍是 0.0 到 10.0。

如果 NDR 事件與裝置相關聯，則應用程式在計算分數時會考慮有關該裝置的可用資訊。該裝置的重要級別以及與該裝置相關的風險都被考慮在內。

事件類型表中為 NDR 事件類型指定的*基本分數*被用來作為計算分數的基準。

如果 NDR 事件未與裝置關聯，則該事件的分數等於基礎分數。

此分數決定了 NDR 事件的嚴重程度。根據分數的數值，NDR 事件可能具有以下嚴重程度之一：

- *低*（分數 0.0–3.9）

  低嚴重等級的 NDR 事件通常不需要立即回應。

- *中*（分數 4.0–7.9）

  中嚴重等級的 NDR 事件包含必須檢視的資訊。這些事件可能需要作出回應。

- *高*（分數 8.0–10.0）

  高嚴重程度的 NDR 事件包含可能產生嚴重影響的資訊。這些事件需要立即作出回應。

NDR 事件註冊技術

Kaspersky Anti Targeted Attack Platform 使用下列技術之一來記錄 NDR 事件：

- *入侵偵測* (IDS)

  此技術會記錄與偵測流量異常相關的 NDR 事件，這些異常是攻擊的指標（例如，NDR 事件可以記錄偵測到 ARP 欺騙的指標）。

- *外部* (EXT)

  此技術註冊 Kaspersky Anti Targeted Attack Platform 使用 NDR API 的方法從第三方系統接收的聚合和巢狀 NDR 事件。

- *資產管理* (AM)

  此技術會註冊涉及偵測流量中或從 EPP 應用程式接收的資料中的裝置資訊的 NDR 事件（例如，當發現裝置具有新的 IP 位址時，可以註冊 NDR 事件）。

- *端點防護平台* (EPP)

  該技術會為防護工作站和伺服器的卡巴斯基應用程式偵測到的威脅註冊 NDR 事件（例如，惡意軟體偵測事件）。

NDR 事件狀態

NDR 事件狀態允許應用程式顯示安全官處理收到的資訊的過程。

可以為 NDR 事件和聚合事件指派以下狀態：

- *新的*。

  當所有 NDR 和聚合事件在 Kaspersky Anti Targeted Attack Platform 中註冊時，都會指派到此狀態。

- *正在進行中*。

  您可以將此狀態指派給 NDR 事件和正在處理的聚合事件（例如，在調查註冊這些事件或事故的原因期間）。

- *已解決*。

  您可以將此狀態指派給 NDR 事件和已處理的聚合事件（例如，對其註冊原因的調查已結束）。

> 指派*已解決*狀態後，應用程式在決定裝置表和網路互動圖中顯示的裝置的安全狀態時，將忽略具有此狀態的 NDR 事件和聚合事件。

必須手動變更 NDR 事件和聚合事件的狀態。您可以按照從*新的*到*已解決*的順序依序分配狀態。但是，您可以跳過*正在進行中*狀態。變更 NDR 事件或聚合事件的狀態後，您無法重新指派先前的狀態之一。

如果將*已解決*狀態指派給聚合事件，則所有巢狀 NDR 事件的狀態將自動變更為*已解決*，且相關警示也會關閉。

如果為 NDR 事件指派了*已解決*狀態，則嵌套此 NDR 事件的聚合事件和相關警示不被關閉。

已註冊 NDR 事件表

您可以在以下位置檢視已註冊的 NDR 事件和聚合事件的表格：“**網路流量事件**”部分。

預設情況下，已註冊的 NDR 事件和聚合事件表會即時更新。表格頂部顯示具有最近的上次可見日期和時間值的事件。

> NDR 或聚合事件的最後可見日期和時間可能與其註冊的日期和時間不同。對於 NDR 事件，最後可見日期和時間可能會在該事件類型的再生期間更新。對於聚合事件，上次可見日期和時間會更新以符合巢狀 NDR 事件的上次可見日期和時間。

NDR 事件和聚合事件的參數顯示在表格的以下列中：

- **開始**。

  對於 NDR 事件，這是註冊事件的日期和時間。對於聚合事件，這是第一個嵌套事件的註冊日期和時間。您可以同時檢視日期和時間，或僅檢視日期或時間。若要選擇顯示的資訊，請選取**日期**和**時間**設定對面的核取方塊。

- **最後可見日期**

  對於 NDR 事件，這是 NDR 事件的最後可見的日期和時間。可能包含事件註冊的日期和時間，或如果事件註冊條件在再生期間內重複出現，則包含事件重複計數器遞增的日期和時間。重新產生計數器的值顯示在**出現總數**欄中。對於聚合事件，聚合事件中包含的事件中最新的最後可見日期和時間。如同**開始**欄，您可以同時檢視日期和時間，或僅檢視日期或時間。

- **標題**。

  為 NDR 事件類型配置的標題。

- **分數**。

NDR 事件的計算分數。此數值決定了 NDR 事件的嚴重等級。根據嚴重等級，分數可以下列其中一種顏色顯示：

- 紅色表示*高*嚴重等級事件。
- 黃色表示*中*嚴重等級事件。
- 藍色表示*低*嚴重等級事件。

- **來源**。

  網路封包的來源位址。您可以透過下列設定來啟用或停用顯示位址資訊的位址和連接埠（表格列中顯示的縮寫名稱在括號中指明）：**IP 位址**、**連接埠號 (P)**、**MAC 位址**、**VLAN ID (VID)**和**應用程式級位址**。如果在應用程式中新增了額外的位址空間，則可以在設定裝置表時使用**顯示位址空間**設定來啟用或停用位址空間名稱的顯示。

- **目的地**。

  網路封包的目標位址。位址資訊的顯示可以按照與**來源**列相同的方式配置。

- **協定**。

  註冊事件的應用層協定。

- **技術**。

  與用於註冊 NDR 事件的技術相對應的圖示。

- **總出現次數**。

  對於 NDR 事件，在再生期間內註冊 NDR 事件後的重複計數器的值。大於 1 的值表示註冊 NDR 事件的條件重複發生了N – 1 次。對於聚合事件，此列顯示值1。

- **ID**。

  已註冊的 NDR 或聚合事件的唯一識別碼。

- **應用程式**。

  有關導致註冊 NDR 事件的條件的應用程式的資訊。NDR 事件儲存從 EPP 應用程式收到的應用程式相關資訊。

- **應用程式使用者**。

  有關啟動**應用程式**欄中指定之應用程式的使用者帳戶資訊。

- **狀態**。

  與NDR 事件或聚合事件的狀態相對應的圖示。

- **敘述**。

  為 NDR 事件類型指定的描述。

- **結束**。

  對於 NDR 事件，指派*已解決*狀態的日期和時間，或 NDR 事件的再生期間。對於聚合事件，嵌套 NDR 事件的最新解決日期和時間。如同**開始**欄，您可以同時檢視日期和時間，或僅檢視日期或時間。

- **觸發的規則**。

  對於 NDR 事件，觸發時導致註冊 NDR 事件的處理程序控制規則或入侵偵測規則的名稱。對於聚合事件，觸發時導致註冊聚合事件的關聯規則的名稱。

- **監控點**。

  其流量觸發了NDR 事件註冊的監控點。

- **事件類型**。

  分配給 NDR 事件類型的數字代碼。

- **標記**。

  您可以將一組圖示指派給任何 NDR 或聚合事件，以便根據表中不存在的條件輕鬆找到 NDR 或聚合事件。

檢視網路流量事件表時，您可以設定、篩選、搜尋和排序記錄，以及導覽至相關項目。

配置已註冊事件表

您可以如下設定事件表的顯示：

- 顯示或隱藏資訊面板。
- 顯示或隱藏事故中包含的事件。
- 顯示或隱藏表格的列並重新排列列。

若要配置事件表顯示：

1. 在**網路流量事件**部分，點擊⚙圖示。

   這將開啟表格顯示配置視窗。

2. 如果要顯示狀態為*新*或*處理中*的事件數量的資訊面板，請勾選**顯示資訊面板**核取方塊。

3. 在**顯示嵌入式清單**下，選擇嵌套在聚合事件中的 NDR 事件的顯示模式：

   - **扁平**。在此模式下，事件表顯示所有 NDR 事件，而不考慮事件巢狀。
   - **樹形**。在這種模式下，聚合事件顯示為巢狀事件和其他聚合事件的樹。如果您希望無論目前的篩選和搜尋設定如何都顯示嵌套項，請選取**篩選時顯示嵌入事件**核取方塊。

4. 在**顯示的列**下，選取要在表中檢視的參數旁的核取方塊。您必須至少選擇一個參數。

5. 如果要以不同的順序顯示列，請選擇要在表中向左或向右移動的列的名稱，然後點擊具有向上和向下箭頭的按鈕。

   對於**開始**、**上次看到**和**結束**列，您也可以變更日期和時間值的顯示順序；對於**來源**和**目標**列，您可以變更網路封包的來源位址和目標位址的顯示順序。為此，請選擇要在表中向左或向右移動的值，然後點擊具有向上和向下箭頭的按鈕。

選定的列將按新順序顯示在**網路流量事件**部分的表中。

檢視嵌套在聚合事件內的事件

您可以使用下列模式在網路流量事件表中檢視嵌套在聚合事件中的 NDR 事件：

- 扁平模式。在此模式下，NDR 事件表顯示所有事件，而不考慮事件巢狀。
- 樹模式。在此模式下，聚合事件顯示為樹，可以使用聚合事件標題旁邊的+和−按鈕進行折疊和展開。

您可以在配置事件表時變更顯示模式。

檢視 NDR 事件的詳細資訊

NDR 和聚合事件的詳細資訊顯示在應用程式 Web 介面的**網路流量事件**部分之詳細資訊區域中。

若要檢視 NDR 或聚合事件的詳細資訊：

在**網路流量事件**部分中，選擇一個事件。

詳細資訊區域顯示在 Web 介面視窗的右側，顯示有關所選NDR 或聚合事件的詳細資訊。

變更 NDR 事件的狀態

您可以變更以下 NDR 事件和聚合事件的狀態：

- *新的*。此狀態可變更為*進行中*或*已解決*。
- *正在進行中*。此狀態可變更為*已解決*。

*已解決*狀態無法變更。

如果 NDR 事件與風險相關，則在為該事件指派*已解決*狀態時，您也可以將風險狀態變更為*已接受*。

若要在管理事件表時變更 NDR 事件和聚合事件的狀態：

1. 在事件表的**網路流量事件**部分中，選擇要變更其狀態的 NDR 事件或聚合事件。
2. 開啟工具列中的**變更狀態**下拉清單。
3. 在下拉清單中，選擇您想要指派的狀態的命令。
   下列情況下，下拉清單的某些項目不可用：
   - 如果選定的項目不包含 NDR 事件或具有*新*狀態的聚合事件，則**正在進行**項目不可用。
   - 如果選定的項目不包含 NDR 事件或具有*新*或*處理中*狀態的聚合事件，則**已解決**項目不可用。

> 如果選擇了所有符合目前篩選和搜尋條件的 NDR 事件和聚合事件，且選定項目的數量超過 1000 條，則應用程式不會檢查它們的狀態。在這種情況下，**進行中**和**已解決**項目均可使用。但是，**進行中**項目僅可用於為狀態為*新的*的事件和事故分配*進行中*狀態。

這將開啟一個確認提示視窗。

4. 如果選定的 NDR 事件與風險相關，並且您想要同時為所有這些風險分配*已接受*狀態，請選擇**指派與該事件相關的所有風險的已接受狀態**（如果選擇了單個事件）或**指派與該事件相關的所有風險的接受狀態**（如果選擇了多個事件）。

   當使用資產管理技術註冊某些類型的 NDR 事件時，風險可能會與事件相關。

5. 在提示視窗中，點擊**確定**。

新增標記

擁有**資深安全員**角色的使用者可以在應用程式 Web 介面的**網路流量事件**部分為 NDR 事件和聚合事件指派標記。

*標記*是一個圖示，可協助您根據表中不存在的條件來尋找 NDR 事件和聚合事件。

若要為 NDR 或聚合事件指派標記：

1. 在**網路流量事件**部分中，於包含 NDR 事件或聚合事件的資料列中，點擊☆欄。

2. 在顯示的功能表中，選擇要指派給此 NDR 事件或聚合事件的標記。

   您可以從應用程式提供的七個標記中選擇一個。每個標記的含義由您決定。

3. 如果需要移除標記，請在功能表中選擇**無標記**。

擁有**資深安全員**和**安全稽核員**角色的使用者可以檢視帶有標記的 NDR 事件或聚合事件。

將 NDR 事件複製到文字編輯器

您可以將有關 NDR 事件和聚合事件的資訊從網路流量事件表複製到任何文字編輯器。資訊從表中目前顯示的列中複製。

如果選擇的 NDR 事件和聚合事件不超過 200 個，則可以複製事件。

若要將 NDR 和聚合事件複製到文字編輯器：

1. 在**網路流量事件**區段中，選擇要複製到文字編輯器的 NDR 事件和聚合事件。

2. 右鍵點擊以開啟所選事件之一的上下文功能表。

3. 在上下文功能表中，選擇以下命令之一：

   - 如果選擇了單個 NDR 或聚合事件，則**複製事件的詳細資訊**。

   - 如果選擇了多個 NDR 事件或聚合事件，則**複製所選事件的詳細資訊**。

4. 開啟任意文字編輯器。

5. 在文字編輯器視窗中，貼上事件（例如，按 **Ctrl+v**）。

可在文字編輯器中編輯複製的事件資訊。有關多個事件的資訊以空白行分隔。

下載事件流量

檢視事件表時，您可以下載與已註冊的 NDR 事件和聚合事件相關的流量。流量被下載為 PCAP 檔案（如果選擇一個事件）或包含 PCAP 檔案的 ZIP 壓縮檔案中（如果選擇多個事件）。

如果在事件表中選擇的事件不超過 200 個（也計算嵌套在聚合事件內的事件），則可以下載流量。

事件的流量從應用程式資料庫下載。如果為這些事件啟用了流量儲存，則可以將流量儲存在已註冊的 NDR 事件的資料庫中。應用程式還可以在請求下載流量時，使用流量傾印檔案直接將流量儲存在資料庫中。這些檔案用於臨時儲存，並隨著新流量的到來自動刪除（輪換週期取決於流量量和應用程式儲存配置）。為確保流量可供下載，建議為相關事件類型啟用流量儲存，並根據流量累積率和事件註冊率設定資料庫中的流量儲存。

若要下載 NDR 事件或聚合事件的流量檔：

1. 在**網路流量事件**區段中，選擇您要下載流量的 NDR 事件和聚合事件。

2. 點擊**下載流量**。

3. 如果檔案產生需要很長時間（超過 15 秒），則檔案產生操作將成為背景操作。在這種情況下，請按照以下步驟下載檔案：

   a. 點擊應用程式 Web 介面功能表中的按鈕。

   這將開啟後台操作清單。

   b. 等待檔案產生操作完成。

   c. 點擊**下載檔案**按鈕。

您的瀏覽器儲存了下載的檔案。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。

建立用於將事件匯出至網路共用的目錄

您可以匯出事件並將包含匯出事件的檔案儲存在伺服器電腦的網路共用上。對於網路共用，您可以使用網路檔案系統 (NFS) 協議，該協議允許您在伺服器電腦的本機檔案系統中掛載另一台電腦的共用（例如，NFS 伺服器匯出點）。使用作業系統的標準工具建立目錄並安裝網路共用。

當使用 NFS 協定時，rpcbind 軟體套件會被在作業系統中啟動。請記住，攻擊者可能會嘗試使用此軟體套件進行某些類型的 DDoS 攻擊。為了消除入侵威脅，必須配置防火牆。在 CentOS Stream 中，我們建議使用 firewalld 實用程式來設定防火牆。

手動建立目錄並掛載網路共用

若要建立用於儲存檔案到網路共用的目錄：

1. 開啟作業系統的主控台。
2. 建立一個本機目錄，在其中掛載網路共用。為此，請輸入以下命令：
   `mkdir <本機目錄的完整路徑>`
   例如：
   `mkdir ~/nfsshare`
3. 建立目錄後，輸入掛載網路共用的命令：
   `sudo mount -t nfs <遠端電腦的名稱或 IP 位址>:\`
   `<網路共用的完整路徑>\`
   `<本機目錄的完整路徑>`
   例如：
   `sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare`
4. 確認掛載成功：
   `mount | grep <本機目錄的完整路徑>`
   例如：
   `mount | grep ~/nfsshare`
   如果掛載成功，顯示的資訊包含遠端電腦的名稱或 IP 位址、網路共用的名稱以及父目錄的名稱。

自動掛載網路共用

要在 CentOS 作業系統中設定網路共用的自動掛載：

以 root 身分開啟/etc/fstab 檔案進行編輯，並在檔案中新增下列行：

`<遠端電腦的名稱或 IP 位址>:<網路共用的完整路徑> <本機目錄的完整路徑> nfs defaults 0 0`

例如：

```
nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0
```

事件資料庫威脅追蹤

當管理應用程式 Web 介面時，您可以產生搜尋查詢並使用 IOC 和 YAML 檔案在事件資料庫中搜尋威脅以及您有權存取其資料的租戶。

若要透過事件資料庫形成搜尋查詢，您可以使用*產生器模式*或*原始碼模式*。

在產生器模式下，您可以使用包含欄位值類型和操作員選項的下拉清單來建立和修改搜尋查詢。

在原始碼模式下，您可以使用文字命令建立和修改搜尋查詢。

您可以上傳 IOC 檔案或包含 Sigma 規則的 YAML 檔案，並根據該檔案中指定的條件搜尋事件。

具有**資深安全員**角色的使用者也可以根據事件搜尋條件建立 TAA (IOA) 規則。

在建構器模式下搜尋事件

一個搜尋查詢最多可以包含 25 個條件。不支援在單個查詢中使用更多條件。

若要在建構器模式下定義事件搜尋條件：

1. 選擇應用程式 Web 介面視窗中的**威脅搜尋**區段、**產生器**索引標籤。

   這將開啟事件搜尋表單。

2. 在下拉清單中，選擇事件搜尋條件。

   您可以在*事件搜尋條件*區段中檢視事件搜尋條件描述。

3. 在下拉清單中，選擇運算子。

   有關可用運算子的清單，請參閱*運算子*區段。

   每種類型的欄位值都有其自己相關的一組運算子。例如，當選取**EventType**欄位值類型時，**=**和**!=**運算子將可用。

4. 根據選定的欄位值類型，執行下列操作之一：

   - 在該欄位中，指定您想要用於執行事件搜尋的一個或多個字元。
   - 在下拉清單中，選擇您想要執行事件搜尋的欄位值選項。

   例如，要根據使用者名稱搜尋完整匹配，請輸入使用者名稱。

5. 如果您想要新增條件，請使用**AND**或**OR**邏輯運算子，並重複新增條件的必要操作。

6. 如果您想要新增一組條件，請點擊**群組**按鈕並重複新增條件所需的操作。

7. 如果您想刪除一組條件，請點擊**移除群組**按鈕。

8. 如果您想搜尋在特定時段內發生的事件，請在**最後一天**下拉清單中選擇以下事件搜尋時段之一：

   - **最後一天**，如果您希望表格顯示在最後一天內找到的事件。
   - **上一個小時**，如果您希望表格顯示在最後一小時內找到的事件。
   - **上星期**，如果您希望表格顯示在最後一星期內找到的事件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內找到的事件。

9. 如果您選擇了**自訂範圍**:

   a. 在開啟的日曆中，指定事件顯示範圍的開始和結束日期。

   b. 點擊**套用**。

   日曆關閉。

10. 點擊**搜尋**。

    滿足搜尋條件的事件表將顯示。

    如果您使用分佈式解決方案和多組織用戶模式，找到的事件將按層分組：伺服器 – 租用戶名稱 – 伺服器名稱。

11. 點擊您要檢視其事件的伺服器的名稱。

    所選伺服器的主機表將顯示。事件分組層級顯示在表格上方。

您可以將產生器中建立的查詢轉換為原始碼模式下的事件搜尋查詢。

在原始碼模式下搜尋事件

一個搜尋查詢最多可以包含 25 個條件。不支援在單個查詢中使用更多條件。

在原始碼模式下定義事件搜尋條件：

1. 在應用程式 Web 介面視窗中，選擇**威脅搜尋**部分，**原始碼**頁簽。

   這將開啟一個表單，其中包含用於在原始碼模式下輸入事件搜尋條件的欄位。

2. 使用條件、運算子、邏輯運算子 OR 和 AND 以及分組條件的括號輸入事件搜尋條件。

   搜尋條件必須符合下列語法：<條件> <運算子> <條件值>。

   ```
   範例：
   EventType == 'filechange' AND
   (
   (
   FileName == '*example*' OR
   DllName == '*example*' OR
   DroppedName == '*example*' OR
   BlockedName == '*example*' OR
   InterpretedFileName == '*example*' OR
   InterpretedFiles.FileName == '*example*' OR
   TargetName == '*example*' OR
   HandleSourceName == '*example*' OR
   HandleTargetName == '*example*'
   ) OR
   UserName == '*example*'
   )
   ```

   您可以使用自動完成功能。為此，將遊標放在查詢行中，然後按 **Ctrl + Space**。

3. 如果您想搜尋在特定時段內發生的事件，請點擊**任何時候**按鈕並選擇以下某個事件搜尋時段：

   - **任何時候**，如果您希望表格顯示最早發現的記錄的事件。
   - **上一個小時**，如果您希望表格顯示在最後一小時內找到的事件。
   - **最後一天**，如果您希望表格顯示在最後一天內找到的事件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內找到的事件。

4. 如果您選擇了**自訂範圍**:

   a. 在開啟的日曆中，指定事件顯示範圍的開始和結束日期。

   b. 點擊**套用**。

   日曆關閉。

5. 點擊**搜尋**。

   滿足搜尋條件的事件表將顯示。

   如果您使用分佈式解決方案和多組織用戶模式，找到的事件將按層分組：**伺服器** – 租用戶名稱 – 伺服器名稱。

6. 點擊您要檢視其事件的伺服器的名稱。

   所選伺服器的主機表將顯示。事件分組層級顯示在表格上方。

轉換產生器查詢以在原始碼模式下搜尋事件

您可以將建構器中建立的查詢轉換為來源模式下的事件搜尋查詢。

當查詢被轉換時，其語法將適應在原始碼模式下搜尋事件。

要轉換查詢：

1. 選擇應用程式 Web 介面視窗中的**威脅搜尋**區段、**產生器**索引標籤。

   這將開啟事件搜尋表單。

2. 在下拉清單中，選擇事件搜尋條件。

   您可以在*事件搜尋條件*區段中檢視事件搜尋條件描述。

3. 在下拉清單中，選擇運算子。

   有關可用運算子的清單，請參閱*運算子*區段。

   每種類型的欄位值都有其自己相關的一組運算子。例如，當選取**EventType**欄位值類型時，**=**和**!=**運算子將可用。

4. 根據選定的欄位值類型，執行下列操作之一：

   - 在該欄位中，指定您想要用於執行事件搜尋的一個或多個字元。
   - 在下拉清單中，選擇您想要執行事件搜尋的欄位值選項。

例如，要根據使用者名稱搜尋完整匹配，請輸入使用者名稱。

5. 如果您想要新增條件，請使用**AND**或**OR**邏輯運算子，並重複新增條件的必要操作。
6. 如果您想要新增一組條件，請點擊**群組**按鈕並重複新增條件所需的操作。
7. 如果您想刪除一組條件，請點擊**移除群組**按鈕。
8. 如果您想搜尋在特定時段內發生的事件，請在**任何時候**下拉清單中選擇以下某個事件搜尋時段：
   - **任何時候**，如果您希望表格顯示最早發現的記錄的事件。
   - **上一個小時**，如果您希望表格顯示在最後一小時內找到的事件。
   - **最後一天**，如果您希望表格顯示在最後一天內找到的事件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內找到的事件。
9. 如果您選擇了**自訂範圍**:
   a. 在開啟的日曆中，指定事件顯示範圍的開始和結束日期。
   b. 點擊**套用**。

   日曆關閉。
10. 轉到**原始碼**索引標籤。
    將顯示警告，告知您轉換不可逆。
11. 點擊**轉換**。

該查詢被轉換為以原始碼模式搜尋事件的查詢。

事件搜尋條件

您可以使用下列條件在建構器模式下搜尋事件：

- **一般資訊**：
  - Host 是主機名稱。
  - HostIP 是主機的 IP 位址。
  - EventType 是事件的類型。
  - UserName 是使用者的名稱。
  - OsFamily 是作業系統家族。
  - OsVersion 是主機上使用的作業系統的版本。

- **TAA 屬性**：
  - IOAId 是 TAA (IOA) 規則 ID。
  - IOATag 是有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。
  - IOATechnique 是 MITRE 技術。
  - IOATactics 是 MITRE 政策。
  - IOAImportance 是指派給使用此 TAA (IOA) 規則產生的事件的重要性等級。
  - IOAConfidence 是置信度，取決於規則引起誤報的可能性。
- **檔案屬性**：
  - CreationTime 是事件建立時間。
  - FileName 是檔案的名稱。
  - FilePath 是檔案所在目錄的路徑。
  - FileFullName 是檔案的完整路徑。包括目錄路徑和檔案名稱。
  - ModificationTime 是檔案修改時間。
  - FileSize 是檔案的大小。
  - MD5 是檔案的 MD5 雜湊值。
  - SHA256 是檔案的 SHA256 雜湊。
  - SimilarDLLPath 是放置在標準搜尋路徑上的目錄中的惡意 DLL，使作業系統在原始 DLL 之前載入它。
- **Linux 處理程序**：
  - LogonRemoteHost 是發起遠端存取的主機的 IP 位址。
  - RealUserName 是使用者在系統中註冊時指派的使用者名稱。
  - EffectiveUserName 是用來登入系統的使用者名稱。
  - FileOwnerUserName 是檔案擁有者的名稱。
  - RealGroupName 是使用者群組的名稱。
  - EffectiveGroupName 是用於操作的使用者群組的名稱。
  - Environment 是系統環境變數。
  - ProcessType 是處理程序類型。
  - OperationResult 是操作結果。

- **處理程序已啟動**：
  - PID 是處理程序 ID。
  - ParentFileFullName 是父處理程序檔案的路徑。
  - ParentMD5 是父處理程序檔案的 MD5 雜湊值。
  - ParentSHA256 是父處理程序檔案的 SHA256 雜湊值。
  - StartupParameters 是處理程序啟動時使用的選項。
  - ParentPID 是父處理程序 ID。
  - ParentStartupParameters 是父處理程序的啟動設定。
- **遠端連線**：
  - HTTPMethod 是 HTTP 請求方法。例如，Get、Post 或 Connect。
  - ConnectionDirection 是連線的方向（傳入或傳出）。
  - LocalIP 是從其進行遠端連線嘗試的本機的 IP 位址。
  - LocalPort 是從其進行遠端連線嘗試的本機的 IP 位址。
  - RemoteHostName 是遠端連線嘗試目標的電腦的名稱。
  - RemoteIP 是遠端連線嘗試目標的電腦的 IP 位址。
  - RemotePort 是遠端連線嘗試目標的電腦的連接埠。
  - UR1 是向其發出 HTTP 請求的資源的位址。
  - TlsVersion 是協定的版本。
  - TlsSni 是伺服器名稱指示，也就是正在建立連線的資源的名稱。
  - TlsCertificateMd5 是 TLS 憑證的 MD5 雜湊值。
  - TlsCertificateSha1 是 TLS 憑證的 SHA1 雜湊。
  - TlsCertificateSubjectNames 是主要和次要 DNS 名稱。
  - TlsCertificateIssuerName 是憑證擁有者的組織名稱。
  - TlsCertificateSerialNumber 是憑證的序號。
  - TlsCertificateCheckResult 是憑證驗證結果。
  - TlsCipherSuite 是憑證的密碼套件。
  - TlsCertificateValidFrom 是計算憑證到期日的日期。
  - TlsCertificateValidTo 是憑證到期的日期。

- **DNS**：
  - DnsServerIpAddress 是DNS 伺服器的 IP 位址。
  - DnsQueryDomainName 是來自請求的網域。
  - DnsAnswerData 是回應資料。
  - DnsQueryTypeId 是記錄類型 ID。
- **LDAP**：
  - LDAPSearchFilter 是搜尋篩選器。
  - LDAPSearchDistinguishedName 是專有名稱。
  - LDAPSearchAttributeList 是搜尋屬性的清單。
  - LDAPSearchScope 是搜尋範圍。
- **命名管道**：
  - PipeName 是命名管道。
  - PipeOperationType 是命名管道操作的類型。
- **WMI**：
  - WmiOperationType 是 WMI 操作類型：*WMI 活動*或*WMI 事件使用者名稱*。
  - WmiHostName 是機器的名稱。
  - WmiUserName 是使用者名稱。
  - WmiNamespaceName 是命名空間。
  - WmiQuery 是查詢的文字。
  - WmiFilterName 是事件篩選器。
  - WmiConsumerName 是事件使用者的名稱。
  - WmiConsumerText 是事件使用者的原始碼。
- **登錄檔已修改**：
  - RegistryKey 是登錄機碼。
  - RegistryValueName 是登錄機碼的名稱。
  - RegistrationValue 是登錄機碼的資料。
  - RegistryOperationType 是登錄機碼操作的類型。

- RegistryPreviousKey 是上一個登錄機碼。
- RegistryPreviousValue 是登錄機碼的先前名稱。

- **系統事件日誌**：
  - WinLogEventID 是Windows 日誌中安全事件的類型 ID。
  - LinuxEventType 是事件的類型。此條件用於 Linux 和 MacOS 作業系統。
  - WinLogName 是日誌的名稱。
  - WinLogEventRecordID 是日誌條目 ID。
  - WinLogProviderName 是記錄事件的系統的 ID。
  - WinLogTargetDomainName 是遠端電腦的網域名稱。
  - WinLogObjectName 是發起事件的物件的名稱。
  - WinlogPackageName 是啟動事件的軟體套件的名稱。
  - WinLogProcessName 是啟動事件的處理程序的名稱。
- **偵測和處理結果**：
  - DetectName 是偵測到的物件的名稱。
  - RecordID 是觸發規則的 ID。
  - ProcessingMode 是掃描模式。
  - ObjectName 是物件的名稱。
  - ObjectType 是物件的類型。
  - ThreatStatus 是偵測模式。
  - UntreatedReason 是事件處理狀態。
  - ObjectContent（也適用於 AMSI 事件）是被傳送進行掃描的指令碼的內容。
  - ObjectContentType（也適用於 AMSI 事件）是指令碼內容的類型。
- **主控台互動輸入**：
  - InteractiveInputText 是在命令列中輸入的文字。
  - InteractiveInputType 是輸入類型（主控台或管道）。
- **檔案修改時間**：
  - FileOperationType 是檔案操作類型。
  - FilePreviousPath 是檔案先前所在目錄的路徑。

- FilePreviousName 是檔案先前的名稱。
- FilePreviousFullName 是檔案的完整名稱，包括檔案先前所在目錄的路徑和/或先前的檔案名稱。
- DroppedFileType 是修改後的檔案的類型。

- **代碼注入和處理程序存取**：
  - AccessMethod 是存取方法。
  - InjectAddress 是接收者程序的位址空間。
  - InjectedDllName 是注入的 DLL 的名稱。
  - ModifiedStartupParameters 是修改後的啟動參數。
  - InjectedDllPath 是注入的 DLL 的路徑。
  - CallTrace 是呼叫追蹤。
  - TargetStartupParameters 是用於啟動接收方程序的命令。
- **處理程序存取**：
  - AccessOperationType 是操作類型：*處理程序存取已開啟*或者*複製句柄*。
  - ProccessAccessRights 是請求的處理程序存取權限。
  - HandleSourceStartupParameters 是啟動來源句柄的指令。
  - HandletargetStartupParameters 是啟動目標句柄的指令。
- **其他**：
  - File type 是檔案的類型。
  - TlsJa3Md5 包含用戶端hello 封包中以下欄位的十進位位元組值：TLS 版本、密碼套件、TLS 協定延伸清單、橢圓曲線和橢圓曲線格式。
  - TlsJa3sMd5 包含伺服器 hello 封包中以下欄位的十進位位元組值：TLS 版本、密碼套件和 TLS 協定延伸清單。
  - DotNetAssemblyName 是.NET 程式集的名稱。
  - DotNetAssemblyFlags 包含 .NET 組合語言標誌。

若要以原始碼模式檢視事件搜尋欄位清單，您可以下載此檔案。

運算子

下表列出了在建構器模式和原始代碼模式下可用於搜尋的運算子。

可用於在建構器模式和原始碼模式下搜尋的運算子

建構器模式	原始碼模式
=	==
!=	NOT (example)
CONTAINS	==*example*
!CONTAINS	NOT (example=='*example*')
STARTS	=='example*'
!STARTS	NOT (example=='example*')
ENDS	=='*example'
!ENDS	NOT (example=='*example')

將表中的事件進行排序

您可以按**事件時間**、**事件類型**、**主機**和**使用者名稱**列對表中的事件進行排序。

將事件表中的事件排序：

1. 在應用程式 Web 介面視窗中選擇**威脅搜尋**區段。
   這將開啟**威脅搜尋**視窗。
2. 定義在產生器模式或原始碼模式下搜尋事件的條件。
   滿足搜尋條件的事件表將顯示。
3. 如果您想按時間對事件進行排序，請點擊**事件時間**欄位名稱右側的圖示之一：
   - ↑ 在表格頂部顯示較新的事件。
   - ↓ 在表格頂部顯示較早的事件。
4. 如果要按事件類型名稱對事件進行排序，請點擊**事件類型**列標題右側的圖示之一：
   - ↑ 按字母順序 A–Z 排序。
   - ↓ 按字母順序 Z–A 排序。
5. 如果要根據在其上產生警示的主機名稱對事件進行排序，請點擊**主機**欄位名稱右側的圖示之一：
   - ↑ 按字母順序 A–Z 排序。
   - ↓ 按字母順序 Z–A 排序。
6. 如果要根據主機的使用者名稱對事件進行排序，請點擊**使用者名稱**欄位名稱右側的圖示之一：
   - ↑ 按字母順序 A–Z 排序。
   - ↓ 按字母順序 Z–A 排序。

7. 如果要根據主機名稱或事件類型名稱對事件進行分組，請點擊**分組**下拉清單中的某個值：

   - **按主機名稱分組**，如果您想按主機名稱對事件進行分組。
   - **按事件類型分組**，如果您想要按事件類型的名稱將事件分組。

   如果事件按**主機**或者**事件類型**欄位排序，當事件按相似屬性分組時，排序結果將被清除。若要傳回排序結果，請從**分組**下拉清單選擇**分組**值。

預設情況下，表中的事件會按時間排序，最新的事件位於表的頂部。

您可以僅根據一種屬性對事件進行排序。

當以外語按事件類型排序時，事件將根據英語事件類型的內部名稱進行排序。

變更事件搜尋條件

*若要變更事件搜尋條件，請在應用程式 Web 介面視窗中的**威脅搜尋**區段執行以下操作：*

1. 點擊視窗上部包含事件搜尋條件的表單。
2. 選擇以下頁簽之一：
   - **產生器**，如果您想在產生器模式下變更事件搜尋條件。
   - **原始碼**，如果您想在原始代碼模式下變更事件搜尋條件。
3. 進行相關變更。
4. 點擊以下按鈕之一：
   - **重新整理**，如果您想使用新條件來重新整理目前事件搜尋。
   - **新搜尋**，如果您想執行新的事件搜尋。

   滿足搜尋條件的事件表將顯示。

搜尋“偵測”和“偵測處理結果”類型的事件

若要搜尋“偵測”和“偵測處理結果”類型的事件：

1. 選擇應用程式 Web 介面視窗中的**威脅搜尋**區段、**產生器**索引標籤。
   這將開啟事件搜尋表單。

2. 若要依處理狀態搜尋事件：

   a. 在**偵測和處理結果**群組的搜尋條件下拉式清單中，選擇 **ThreatStatus**。

   b. 在比較運算子下拉清單中，選擇以下選項之一：

      - **=**（等於）
      - **!=**（不等於）

   c. 在事件處理狀態下拉清單中，選擇下列選項之一：

      - **清洁物件**。
      - **物体已清除**。
      - **誤報**。
      - **使用者新增的物件**。
      - **物件已新增到排除清單中**。
      - **物件已刪除**。
      - **物件被隔離**。
      - **未找到物件**。
      - **物件已回溯**。
      - **無法處理物件**。
      - **物件未處理**。
      - **處理已終止**。
      - **未知**。

3. 若要依事件未被處理的原因搜尋事件：

   a. 在**偵測和處理結果**群組的搜尋條件下拉式清單中，選擇 **UntreatedReason**。

   b. 在比較運算子下拉清單中，選擇以下選項之一：

      - **=**（等於）
      - **!=**（不等於）

   c. 在事件未被處理的原因下拉清單中，選擇以下選項之一：

      - **已處理物件**。
      - **應用程式正在僅報告模式下執行**。
      - **備份物件失敗**。

- **複製物件失敗**。
- **裝置未準備好**。
- **物件被封鎖**。
- **無權執行操作**。
- **無法清除的物件**。
- **物件不可覆寫**。
- **未找到物件**。
- **磁碟上沒有可用空間**。
- **處理已取消**。
- **處理已推遲**。
- **處理工作已停止**。
- **讀取資料時出錯**。
- **原因不明**。
- **這是一個關鍵的系統物件**。
- **資料寫入錯誤**。
- **不支援資料寫入**。
- **物件寫防護**。

4. 如果您想要新增條件，請使用**AND**或**OR**邏輯運算子，並重複新增條件的必要操作。
5. 如果您想要新增一組條件，請點擊**群組**按鈕並重複新增條件所需的操作。
6. 如果您想刪除一組條件，請點擊**移除群組**按鈕。
7. 如果您想搜尋在特定時段內發生的事件，請在**任何時候**下拉清單中選擇以下某個事件搜尋時段：
   - **任何時候**，如果您希望表格顯示最早發現的記錄的事件。
   - **上一個小時**，如果您希望表格顯示在最後一小時內找到的事件。
   - **最後一天**，如果您希望表格顯示在最後一天內找到的事件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內找到的事件。
8. 如果您為找到的事件選擇了**自訂範圍**顯示時段：
   a. 在開啟的日曆中，指定事件顯示範圍的開始和結束日期。
   b. 點擊**套用**。

日曆關閉。

9. 點擊**搜尋**。

滿足搜尋條件的事件表將顯示。

使用 IOC 或 YAML 檔案中指定的條件搜尋事件

建立 IOC 檔案時，請在“**威脅搜尋**”部分檢視可用於搜尋事件的 IOC 術語清單。您可以透過從下面的連結下載檔案來檢視受支援的 IOC 術語清單。

在“**威脅搜尋**”部分搜尋事件的 IOC 術語

若要使用 IOC 或 YAML 檔案中指定的條件搜尋事件：

1. 在應用程式 Web 介面視窗中選擇**威脅搜尋**區段。

   這將開啟事件搜尋表單。

2. 點擊**匯入**。

   這將開啟檔案選擇視窗。

3. 選擇您想上傳的檔案，然後點擊“**開啟**”。

   檔案已上傳。

   在“**原始碼**”索引標籤上，包含事件搜尋條件的表單將顯示上傳的檔案中定義的條件。

   > 您可以搜尋符合這些條件的事件。您也可以變更上傳的檔案中定義的條件，或在原始碼模式下新增事件搜尋條件。

4. 如果您想搜尋在特定時段內發生的事件，請點擊**任何時候**按鈕並選擇以下某個事件搜尋時段：

   - **任何時候**，如果您希望表格顯示最早發現的記錄的事件。
   - **上一個小時**，如果您希望表格顯示在最後一小時內找到的事件。
   - **最後一天**，如果您希望表格顯示在最後一天內找到的事件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內找到的事件。

5. 如果您為找到的事件選擇了**自訂範圍**顯示時段：

   a. 在開啟的日曆中，指定事件顯示範圍的開始和結束日期。

   b. 點擊**套用**。

   日曆關閉。

6. 點擊**搜尋**。

一個與上傳的檔案中指定的條件相對應的事件表將會顯示。

根據事件搜尋條件建立 TAA (IOA) 規則

根據事件搜尋條件建立 TAA (IOA) 規則：

1. 在應用程式 Web 介面視窗中選擇**威脅搜尋**區段。
   這將開啟事件搜尋表單。
2. 使用建構器模式或原始碼模式執行事件搜尋。
3. 點擊**另存為 TAA (IOA) 規則**。
   這將開啟**新 TAA (IOA) 規則**視窗。
4. 在**名稱**欄位中，輸入規則的名稱。
5. 點擊**儲存**。

事件搜尋條件將被儲存。在**自訂規則**部分的 TAA（IOA）規則表中，在 Web 介面的**TAA**子部分中，新規則將以指定名稱顯示。

如果您要將事件搜尋條件儲存為使用者定義的 TAA (IOA) 規則，請避免使用下列欄位：

- IOAd。
- IOATag。
- IOATechnique。
- IOATactics。
- IOAImportance。
- IOAConfidence。

儲存使用者定義的 TAA (IOA) 規則時，應用程式可能沒有任何包含這些欄位資料的事件。當出現具有此資料的事件時，您先前建立的使用者定義欄位將無法按這些欄位標記事件。

具有**安全稽核員**和**安全官**角色的使用者無法根據事件搜尋條件建立 TAA (IOA) 規則。

事件資訊

如果您使用分散式解決方案和多組織用戶模式，則在使用 Web 介面管理應用程式時，您可以檢視您擁有其資料存取權的租用戶的事件資訊。

事件資訊顯示偵測到事件的 Endpoint Agent 電腦的本機時間戳記。應用程式管理員必須確保具有 Endpoint Agent 元件的電腦上的時間最新。

若要啟用所有租戶的事件顯示：

1. 在應用程式 Web 介面視窗中選擇**威脅搜尋**區段。
2. 開啟**在所有租戶中搜尋**切換開關。

   事件表顯示所有租戶的事件。

事件處理建議

事件視窗在事件樹和具有"**資深安全員**"角色的使用者的資訊文字之間的方塊中顯示按鈕，其中包含可用於處理此事件的動作。

您可以執行以下操作：

- **隔離 <主機名稱>** – 將偵測到事件且具有 Endpoint Agent 元件的主機從網路隔離。適用於所有事件類型。
- **建立阻止規則** – 禁止執行在事件中偵測到的檔案。不適用於"**USB 裝置**"事件。在 Windows 裝置上，它也不適用於"**系統事件日誌**"事件。
- **建立工作** – 建立一個工作。不適用於"**USB 裝置**"事件。在 Windows 裝置上，它也不適用於"**系統事件日誌**"事件。

此外，您可以透過點擊包含檔案名稱、路徑、MD5 或 SHA256 雜湊值以及主機名稱的連結來處理事件，同時在視窗下方檢視有關事件的文字資訊。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **殺死處理程序**。
  - **使用唯一的 PID 殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。
  - **進行取證**。
  - **隔離檔案**。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。

- 在 Kaspersky TIP 上尋找。
- 尋找事件。
- 尋找警示。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- **在 virustotal.com 上尋找**。
- 在儲存中尋找。
- 建立阻止規則。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
  - 執行應用程式。
- **複製值到剪貼簿**。

具有**安全稽核員**和**安全官**角色的使用者不會被顯示事件處理建議。

遵循建議隔離主機

若要遵循建議將主機與網路隔離：

1. 在建議框中選擇**隔離 <主機名稱>**。

   這將開啟您正在處理的事件中的主機的主機隔離設定視窗。

2. 在**此時間後停用隔離**欄位中，輸入以小時為單位的時間（1到9999），在此期間主機的網路隔離將處於活動狀態。

3. 在**主機隔離規則排除項目**設定群組中的**流量方向**清單中，選擇必須放行的網路流量方向：

   - **傳入/傳出**。
   - **傳入**。
   - **傳出**。

4. 在**IP**欄位中，輸入必須放行其網路流量的 IP 位址。

   > 如果您使用 Kaspersky Endpoint Agent 充當 Endpoint Agent 元件，則可以使用代理伺服器將 Kaspersky Endpoint Agent for Windows 與 Kaspersky Anti Targeted Attack Platform 連線。當您將此代理伺服器新增至排除項時，可透過代理伺服器存取的網路資源也會新增至排除項目。如果透過代理伺服器存取的網路資源已新增至排除項，但代理伺服器本身未被新增至排除項，則此類排除項無法運作。

5. 如果您選擇了**傳入**或**傳出**，請在**連接埠**欄位中輸入連接埠。

6. 如果您想要新增多個排除項，請點擊**新增**並重複上述步驟填寫**流量方向**、**IP**和**連接埠**欄位。

7. 點擊**儲存**。

主機隔離資訊顯示在Web 介面的**Endpoint Agent區段**中。

您也可以透過點擊警示資訊中的**隔離 <主機名稱>**連結，以及Web 介面的**Endpoint Agent區段**來建立網路隔離規則。

> 具有**安全稽核員**和**安全官**角色的使用者不能將主機與網路隔離。

遵循建議防止檔案運行

要遵循建議防止檔案運行：

1. 在建議框中，選擇**建立阻止規則**。

   這將開啟防護規則建立視窗，其中包含您正在處理的事件的檔案的 MD5 或 SHA256 雜湊值。

2. 配置以下設定：

   a. **狀態**是阻止規則的狀態：

      - 如果要啟用阻止規則，請將切換開關設為**開啟**。
      - 如果要停用阻止規則，請將切換開關設為**關閉**。

   b. **名稱** — 阻止規則的名稱。

   c. 如果您希望應用程式向應用程式防禦的電腦使用者顯示阻止規則觸發通知，請選擇**通知使用者阻止檔案執行**核取方塊。

   d. 如果要變更阻止規則的範圍，請配置**阻止於**設定：

      - 如果您想在所有伺服器的所有主機上套用阻止規則，請選擇**所有主機**。
      - 如果要在選定的伺服器上套用阻止規則，請選擇**指定伺服器**選項並在**伺服器**參數名稱的右側選擇要在其上套用阻止規則的伺服器名稱旁的核取方塊。

        僅當啟用分佈式解決方案和多組織用戶模式時，此選項才可用。
      - 如果您想在選定主機上套用阻止規則，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

3. 點擊**新增**。

   檔案運行防禦已建立。

所建立的防禦資訊顯示在Web 介面的**阻止**部分。

> 如果您選擇了**通知使用者阻止檔案執行**核取方塊並嘗試執行被阻止運行的檔案，則使用者會被通知該檔案觸發了執行阻止規則。

> 具有**安全稽核員**和**安全官**角色的使用者無法阻止檔案執行。

遵循建議建立工作

要遵循建議建立工作：

1. 點擊**建立工作**，然後在建議框中展開工作類型清單。

2. 選擇工作類型：

   - **殺死處理程序**。
   - **進行取證**。
   - **啟動 YARA 掃描**。
   - **管理服務**。

- **獲取處理程序記憶體傾印**。
- **獲取 NTFS 元檔案**。
- **執行應用程式**。
- **獲取檔案**。
- **刪除檔案**。
- **隔離檔案**。
- **從隔離區還原檔案**。

這將開啟工作建立視窗，其中包含您正在處理的事件的預設值（例如主機名稱、檔案路徑、檔案的 MD5 或 SHA256 雜湊值）。

3. 如果您想要修改事件的預設值，請編輯對應的欄位。
4. 如果您想為工作新增註釋，請在**敘述**框中輸入。
5. 如果您正在建立**殺死處理程序**、**刪除檔案**、**啟動 YARA 掃描**或**管理服務**工作，並且想要修改工作範圍，請變更**工作所有者**設定的值：
   - 如果您想要在所有伺服器的所有主機上執行工作，請選擇**所有主機**選項。
   - 如果要在選定的伺服器上執行工作，請選擇**指定伺服器**選項，並在**伺服器**參數名稱的右側，選取要在其上執行工作的伺服器名稱旁的核取方塊。

     僅當啟用分佈式解決方案和多租戶模式時，此選項才可用。
   - 如果您想要執行選定主機上的工作，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。
6. 點擊**新增**。

工作已建立。

已建立工作的資訊顯示在Web 介面的**工作部分**。

> 具有**安全稽核員**和**安全官**角色的使用者不能建立工作。

有關事件樹中事件的資訊

事件樹顯示在事件資訊視窗的上部。

事件樹包含以下資訊：

- 您正在檢視其資訊的事件。

  您正在檢視的事件顯示在右側。

- 父處理程序。

  父處理程序顯示在您正在檢視的事件的左側。如果您正在檢視的事件沒有父處理程序，則會顯示在其中註冊該事件的主機名稱。

點擊左側父處理程序的名稱將顯示啟動相關處理程序的處理程序，啟動處理程序是該處理程序的父處理程序。如果沒有父處理程序，則顯示主機名稱。

每個父處理程序名稱的右側顯示該處理程序所產生的事件總數。您可以檢視事件清單以及有關所選事件的資訊。

檢視事件樹中的父處理程序資訊

若要顯示正在檢視的事件的父處理程序資訊：

1. 使用建構器模式或原始碼模式執行事件搜尋。

   事件表將顯示。

2. 選擇您想檢視其資訊的事件。

   這將開啟一個視窗，其中包含有關事件的資訊。視窗上部將顯示事件樹。

3. 點擊父處理程序的名稱。

   在視窗的底部，**詳細資訊**索引標籤會顯示處理程序資訊，就正在被檢視的事件而言該處理程序是父處理程序。

檢視事件樹中有關父處理程序發起的事件的資訊

檢視父處理程序發起的所有事件的表：

1. 使用建構器模式或原始碼模式執行事件搜尋。

   事件表將顯示。

2. 選擇您想檢視其資訊的事件。

   這將開啟一個視窗，其中包含有關事件的資訊。事件資訊視窗的上部會顯示事件樹。

3. 點擊事件樹中的父處理程序名稱。

   在視窗底部，**詳細資訊**索引標籤會顯示相對於目前所檢視事件之父事件的相關資訊。

4. 前往**事件**索引標籤。

   由父處理程序啟動的所有事件的表將顯示。預設情況下，表中的事件會按時間排序，最新的事件位於表的頂部。

   您可以透過點擊相關事件所在行來檢視事件資訊。事件節點顯示在事件樹中。

若要顯示按類型分組的事件表：

1. 使用建構器模式或原始碼模式執行事件搜尋。

   事件表將顯示。

2. 選擇您想檢視其資訊的事件。

   這將開啟一個視窗，其中包含有關事件的資訊。事件資訊視窗的上部將顯示事件樹。

3. 點擊事件樹中父處理程序名稱右側的下拉清單。

   由父處理程序啟動的所有事件的清單將顯示。預設情況下，清單中的事件會按類型分組。

4. 在事件樹中，在父處理程序名稱右側的下拉清單中，選擇下列選項之一：

   - 如果要顯示父處理程序發起的所有事件，請點擊**所有事件**。

     由父處理程序啟動的所有事件的表將顯示。預設情況下，表中的事件會按時間排序，最新的事件位於表的頂部。

   - 如果要檢視由父處理程序發起的特定類型的所有事件，請選擇相關事件類型的名稱。

     由父處理程序啟動的所有事件的表將顯示，並按類型分組。

   您可以透過點擊相關事件所在行來檢視事件資訊。事件顯示在事件樹中。

檢視事件樹中的主機資訊

如果您正在檢視的事件或父處理程序沒有啟動它的處理程序，則事件樹中的處理程序節點將被替換為註冊事件或執行父處理程序的主機的節點。

若要檢視註冊事件或啟動父處理程序的主機的資訊：

1. 使用建構器模式或原始碼模式執行事件搜尋。

   事件表將顯示。

2. 選擇您想檢視其資訊的事件。

   這將開啟一個視窗，其中包含有關事件的資訊。視窗上部將顯示事件樹。

3. 點擊事件樹中的主機名稱。

   視窗的底部將顯示有關註冊事件的主機或正在執行的父處理程序的資訊。

檢視事件表

事件表在事件資料庫中的威脅搜尋完成後顯示在應用程式 Web 介面視窗中的**威脅搜尋**部分。您可以按**事件時間**、**事件類型**、**主機**和**使用者名稱**欄對表中的事件進行排序。

如果您使用分佈式解決方案和多組織用戶模式，表中的事件將按所選伺服器和租用戶的主機進行分組。

事件表包含以下資訊：

1. **事件時間**—偵測到事件的日期和時間。

2. **事件類型**，例如，**處理程序已啟動**。

3. **主機名稱**—產生警示的主機名稱。

4. **詳細資訊**—有關事件的資訊。

5. **使用者名稱**—具有 Endpoint Agent 元件的電腦上的使用者名稱，其使用者帳戶被用來偵測事件。

在事件表中，**詳細資訊**列會顯示**事件類型**列中每種事件類型的資料集（請參閱下表）。

事件類型列中每個事件類型在**詳細資訊**列中的資料集

事件類型	詳細資訊
處理程序已啟動	已啟動的處理程序檔案的名稱。SHA256 和 MD5 雜湊。
模組已載入	已載入的動態函式庫的名稱。SHA256 和 MD5 雜湊。
到遠端主機的連線	進行遠端連線嘗試的 URL。嘗試建立遠端連線的檔案的名稱。
阻止的應用程式（阻止規則）	阻止啟動的應用程式檔案的名稱。SHA256 和 MD5 雜湊。
檔案已封鎖	阻止啟動的檔案的名稱。SHA256 和 MD5 雜湊。
檔案已變更	建立的檔案的名稱。SHA256 和 MD5 雜湊。
系統事件日誌	用於在系統日誌中記錄事件的通道。事件類型 ID。
登錄檔已修改	登錄檔中機碼的名稱。<機碼中變數的名稱>=<變數的值>。
監聽的連接埠	伺服器位址和連接埠。監聽連接埠的處理程序檔案的名稱。
驅動程式已載入	載入的驅動程式的檔案名稱。SHA256 和 MD5 雜湊。
偵測	偵測到物件的檔案的名稱。偵測到的物件的名稱。SHA256 和 MD5 雜湊。
偵測處理結果	偵測到物件的檔案的名稱。偵測到的物件的名稱。SHA256 和 MD5 雜湊。
AMSI 掃描	掃描物件的名稱。指令碼的類型。被傳送以進行掃描的指令碼文字。
處理程序：解釋檔案執行	執行的檔案的名稱。SHA256 和 MD5 雜湊。
處理程序：主控台互動式輸入	命令文字。
處理程序已終止	已停止處理程序的檔案名稱。SHA256 和 MD5 雜湊。
DNS	正在尋找的網域名稱。資源記錄類型 ID。
LDAP	搜尋範圍和篩選器。
命名管道	管道名稱。管道操作類型。
WMI	WMI 操作類型。事件消費者原始碼。
代碼注入	包含鉤子過程的目標處理程序的檔案名稱或動態連結庫的名稱以及注入後傳遞控制權的函數的名稱。存取目標處理程序檔案的方法。目標處理程序檔案的 SHA256 和 MD5 雜湊。
處理程序存取	接收者處理程序檔案的名稱。事件的重要性。對流程檔案執行的操作類型。處理程序存取權限。
USB 裝置	所連線裝置的類型。所連線裝置的名稱。對所連線裝置的操作類型。系統磁碟指示器（如果連線的裝置是系統磁碟，則顯示此欄位）。

點擊包含事件類型名稱、資料、其他資訊和使用者名稱的連結將開啟一個清單，您可以從其中選擇要在物件上執行的操作。根據儲存格中的值，您可以執行下列操作之一：

- 對於單元格中的所有值：
  - **新增到篩選器**。
  - **從篩選器中排除**。
  - **複製值到剪貼簿**。

- 主機名稱：
  - 尋找事件。
  - 尋找警示。
  - 從網路隔離。
- 檔案名稱：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- MD5 雜湊：
  - 尋找事件。
  - 尋找警示。
  - 在 Kaspersky TIP 上尋找。
  - 建立阻止規則。
  - 在儲存中尋找。
- SHA256 雜湊值：
  - 尋找事件。
  - 尋找警示。
  - 在 Kaspersky TIP 上尋找。
  - 在 virustotal.com 上尋找。
  - 建立阻止規則。
  - 在儲存中尋找。

配置事件表顯示

您可以顯示或隱藏列並變更事件表中列的順序。

若要配置事件表顯示：

1. 使用建構器模式或原始碼模式執行事件搜尋。
   事件表將顯示。

2. 在表格的標題部分，點擊 ⚙ 。
   這將開啟**自訂表格**視窗。

3. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   > 必須選擇至少一個核取方塊。

4. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。

5. 如果要還原預設表格顯示設定，請點擊**預設**。

6. 點擊**套用**。

事件表的顯示已配置。

檢視有關事件的資訊

檢視活動詳情：

1. 在應用程式 Web 介面視窗中，選擇**威脅搜尋**部分、**產生器**或**原始碼**索引標籤。
   這將開啟事件搜尋表單。

2. 如果您使用的是分佈式解決方案和多組織用戶模式，並且希望為所有租用戶啟用事件顯示，請開啟**在所有租戶中搜尋**切換開關。

3. 使用產生器模式或原始碼模式執行事件搜尋。
   事件表將顯示。

4. 選擇您想檢視其資訊的事件。

這將開啟一個視窗，其中包含有關事件的資訊。

有關“處理程序已啟動”事件的資訊

顯示**處理程序已啟動**事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。

- **處理程序已啟動**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案**—處理程序檔名。
  - **處理程序 ID**—處理程序識別碼。
  - **啟動參數**—處理程序啟動設定。

    如果事件是由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄至事件資料庫，則會顯示**命令**欄位而非**啟動參數**欄位，也就是用於執行處理程序的命令。
  - **目前目錄**—處理程序的目前目錄
  - **MD5**—處理程序檔案的 MD5 雜湊。
  - **SHA256**—處理程序檔案的 SHA256 雜湊。
  - **大小**—處理程序檔案的大小。
  - **檔案類型**—處理程序檔案的類型。
  - **事件時間**—處理程序啟動時間。
  - **屬性修改時間**—處理程序檔案屬性改變的時間。
  - **建立時間**—處理程序檔案的建立時間。
  - **修改時間**—處理程序檔案的上次修改時間。
- **詳細資訊**部分：
  - **應用程式名稱**—例如，作業系統的名稱。
  - **供應者**—例如，作業系統的供應商。
  - **檔案描述**—例如，範例檔案。
  - **原始檔案名稱**—例如，ExampleFile.exe。
  - **簽章主旨**—核發檔案數位憑證的組織。
  - **簽章驗證結果**—例如，“無效”或“正常”。
  - **屬性**—依 Windows 分類的檔案屬性。例如，A（壓縮檔案）、D（目錄）或 S（系統檔案）。

如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中，則**詳細資訊**部分還包括以下欄位：

- **屬性**—處理程序檔的屬性。
- **處理程序類型**—例如，exec。
- **環境變量**—處理程序的環境變數。
- **真实使用者名稱**—在系統中註冊時指定的使用者名稱。
- **真实群組名稱**—使用者所屬的群組。
- **有效使用者名稱**—用於登入系統的使用者名稱。
- **有效群組名稱**—名稱被用於登入系統的使用者群組。
- **所有者使用者名稱**—建立了處理程序檔案的使用者的名稱。
- **所有者群組名稱**—其使用者可以修改或刪除處理程序檔案的群組的名稱。
- **檔案允許的功能**—可用於存取處理程序檔案的權限。如果事件由 Kaspersky Endpoint Security for Mac 記錄，則此欄位不會顯示。
- **檔案可繼承功能**—使用者群組對處理程序檔案的父目錄執行操作的權限。如果事件由 Kaspersky Endpoint Security for Mac 記錄，則此欄位不會顯示。
- **檔案有效能力**—目前與流程檔案相關的權限。如果事件由 Kaspersky Endpoint Security for Mac 記錄，則此欄位不會顯示。
- **從 URL 下載** — 下載處理程序檔案的 URL。
- **來源** — 取得處理程序檔案的訊息的中繼資料。
- **帳戶屬性** — 執行處理程序的使用者帳戶的標誌。
- **處理程序建立標誌** — 處理程序建立標誌。
- **符號連接** — 符號連結的路徑。
- **調用跟蹤** — 呼叫堆疊。

- **事件發起者**部分：
  - **檔案**—父處理程序檔案的路徑。
  - **處理程序 ID** — 父處理程序的識別碼。
  - **啟動參數** — 父處理程序啟動設定。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中而不是**啟動參數**欄位中，則顯示**命令**欄位，即用於運行父處理程序的命令。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。

- **系統資訊**部分：
  - **主機名稱** — 啟動了處理程序的主機的名稱。
  - **主機 IP** — 啟動了處理程序的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者帳戶類型** — 執行處理程序的帳戶類型。例如，管理員。
  - **登入類型** — 例如，使用正在執行的服務。
  - **使用者名稱** — 啟動該處理程序的使用者的名稱。
  - **作業系統版本**—主機上正在使用的作業系統的版本。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中，則**系統資訊**部分還顯示從其執行遠端登入的主機名稱的**從遠端主機登入**欄位。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

在 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 在事件資料庫中記錄的事件資訊中，您可以點擊包含檔案名稱或檔案路徑的連結以開啟一個清單，您可以在其中選擇以下操作之一:

- 尋找事件。
- 尋找警示。
- 運行獲取檔案工作。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料 → 檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Mac 事件資訊中，您可以點擊帶有檔案名稱或檔案路徑的連結來開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 運行**獲取檔案**工作。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- **在 virustotal.com 上尋找**。
- 在儲存中尋找。
- 建立阻止規則。
- **複製值到剪貼簿**。

有關“處理程序已終止”事件的資訊

顯示**處理程序已終止**事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- **處理程序已終止**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案**—處理程序檔名。
  - **處理程序 ID**—處理程序識別碼。

- **啟動參數**—處理程序啟動設定。

  如果事件是由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄至事件資料庫，則會顯示**命令**欄位而非**啟動參數**欄位，也就是用於執行處理程序的命令。

- **MD5**—處理程序檔案的 MD5 雜湊。

- **SHA256**—處理程序檔案的 SHA256 雜湊。

- **大小**—處理程序檔案的大小。

- **事件時間**—處理程序終止時間。

- **事件發起者**部分：

  - **檔案**—父處理程序檔案的路徑。

  - **處理程序 ID** — 父處理程序的識別碼。

  - **啟動參數** — 父處理程序啟動設定。

    如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中而不是**啟動參數**欄位中，則顯示**命令**欄位，即用於運行父處理程序的命令。

  - **MD5**—父處理程序檔案的 MD5 雜湊。

  - **SHA256**—父處理程序檔案的 SHA256 雜湊。

- **系統資訊**部分：

  - **主機名稱** — 啟動了處理程序的主機的名稱。

  - **主機 IP** — 啟動了處理程序的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者帳戶類型**—終止處理程序的帳戶類型。例如，管理員。

  - **使用者名稱** — 啟動該處理程序的使用者的名稱。

  - **作業系統版本**—主機上正在使用的作業系統的版本。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中，則**系統資訊**部分還顯示從其執行遠端登入的主機名稱的**從遠端主機登入**欄位。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。

- 尋找警示。

- 執行以下工作：
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

在 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 在事件資料庫中記錄的事件資訊中，您可以點擊包含檔案名稱或檔案路徑的連結以開啟一個清單，您可以在其中選擇以下操作之一:

- 尋找事件。
- 尋找警示。
- 運行獲取檔案工作。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - **刪除檔案**。

- 獲取檔案。
- 隔離檔案。
- 執行應用程式。

- 複製值到剪貼簿。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Mac 事件資訊中，您可以點擊帶有檔案名稱或檔案路徑的連結來開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 運行獲取檔案工作。
- 複製值到剪貼簿。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- 在儲存中尋找。
- 建立阻止規則。
- 複製值到剪貼簿。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- 在 virustotal.com 上尋找。
- 在儲存中尋找。
- 建立阻止規則。
- 複製值到剪貼簿。

有關“模組已載入”事件的資訊

顯示**模組已載入**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **模組已載入**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案**—已載入模組檔案的名稱。
  - **MD5**—已載入模組檔案的 MD5 雜湊。
  - **SHA256**—已載入模組檔案的 SHA256 雜湊。
  - **大小**—已載入模組的大小。
  - **事件時間**—模組載入的時間。
- **詳細資訊**部分：
  - **應用程式名稱**—例如，作業系統名稱。
  - **供應者**—例如，作業系統的供應商。
  - **檔案描述**—例如，範例檔案。
  - **原始檔案名稱**—例如，範例檔案。
  - **簽章主旨**—核發檔案數位憑證的組織。
  - **簽章驗證結果** — 例如，“簽名無效”或“簽名正常”。
  - **建立時間**—已載入模組的建立時間。
  - **修改時間**—已載入模組的上次修改日期。
  - **旁路路徑中的下一個 DLL**—此欄位包含可能取代現有程式庫而載入之 DLL 函式庫的路徑。

    如果滿足以下條件，則顯示該欄位：
    - 載入的 DLL 的來源不受信任。
    - 標準搜尋路徑中的資料夾包含具有相同名稱但不同雜湊值的程式庫。

- **事件發起者**部分：
  - **檔案** – 父處理程序檔案的路徑。
  - **MD5** – 父處理程序檔案的 MD5 雜湊。
  - **SHA256**–父處理程序檔案的 SHA256 雜湊。
- **系統資訊**部分：
  - **主機名稱**–載入了模組的主機的名稱。
  - **主機 IP**–載入了模組的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱**–載入了模組的使用者的名稱。
  - **作業系統版本**–主機上使用的作業系統版本。

點擊**模組已載入**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊**事件發起者**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。

    - 獲取檔案。
    - 進行取證。
    - 隔離檔案。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
    - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
    - **殺死處理程序**。
    - **刪除檔案**。
    - **隔離檔案**。
    - **執行應用程式**。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- **在 virustotal.com 上尋找**。
- 在儲存中尋找。
- 建立阻止規則。

- **複製值到剪貼簿**。

有關“遠端連線”事件的資訊

顯示**到遠端主機的連線**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **到遠端主機的連線**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **連線方向**是連線方向（傳入或傳出）。
  - **遠端 IP**—進行遠端連線嘗試的主機的 IP 位址。
  - **本機 IP** – 進行遠端連線嘗試的本機的 IP 位址。
  - **事件時間**—遠端連線嘗試的時間。
- **TLS**部分：
  - **版本**—通訊協定版本。
  - **SNI**—要連線的網站名稱。
  - **加密 SNI**—網站的加密名稱。
  - **憑證 MD5**—憑證檔案的 MD5 雜湊。
  - **憑證 SHA1**—憑證檔案的 SHA1 雜湊。
  - **憑證頒發者名稱**—簽署憑證的組織名稱。
  - **序號**—憑證的唯一編號。
  - **憑證驗證結果**—憑證驗證結果。
  - **憑證有效期自**—憑證開始生效的日期。
  - **憑證有效期至**—憑證到期的日期。
  - **JA3**—用戶端 hello 封包中以下欄位的十進位位元組值：TLS 版本、密碼套件、TLS 通訊協定擴充功能清單、橢圓曲線及橢圓曲線格式。若要分隔欄位，請使用“，”字元；要分隔每個欄位中的值，請使用“-”字元。

- **JA3S**—伺服器 hello 封包中以下欄位的十進位位元組值：TLS 版本、密碼套件及 TLS 通訊協定擴充功能清單。若要分隔欄位，請使用“，”字元；要分隔每個欄位中的值，請使用“-”字元。
- **JA3 MD5** — JA3 指紋。
- **JA3S MD5** — JA3S 指紋。

- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
- **系統資訊**部分：
  - **主機名稱**—進行遠端連線嘗試的主機名稱。
  - **主機 IP**—從其進行遠端連線嘗試的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱**—嘗試建立遠端連線的使用者名稱。
  - **作業系統版本**—主機上使用的作業系統版本。

點擊**到遠端主機的連線**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊**事件發起者**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。

- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。

- 在 Kaspersky TIP 上尋找。
- 在 virustotal.com 上尋找。
- 在儲存中尋找。
- 建立阻止規則。
- 複製值到剪貼簿。

“防護規則”事件資訊

包含其中觸發了阻止規則之事件資訊的視窗，也就是**阻止的應用程式（阻止規則）**類型的事件，會顯示以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **阻止的應用程式（阻止規則）**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案** — 被封鎖運行的檔案的名稱。
  - **啟動參數** — 用於嘗試執行檔案的參數。
  - **MD5** — 被阻止運行的檔案的 MD5 雜湊。
  - **SHA256** — 被阻止運作的檔案的 SHA256 雜湊。
  - **大小** — 被封鎖運作的檔案的大小。
  - **事件時間** — 觸發封鎖檔案啟動的時間。
- **詳細資訊**部分：
  - **應用程式名稱**—例如，作業系統的名稱。
  - **供應者**—例如，作業系統的供應商。
  - **檔案描述**—例如，範例檔案。
  - **原始檔案名稱**—例如，ExampleFile.exe。
  - **簽章主旨**—核發檔案數位憑證的組織。
  - **簽章驗證結果** — 例如，“簽名無效”或“簽名正常”。

- **建立時間** — 被封鎖運作的檔案的建立時間。
- **修改時間** — 被封鎖運作的檔案的上次修改日期。

- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
  - **處理程序 ID**—父處理程序的識別碼。
- **系統資訊**部分：
  - **主機名稱** — 觸發了封鎖檔案啟動的主機的名稱。
  - **主機 IP** — 觸發了封鎖檔案啟動的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱** — 帳戶用於執行檔案的使用者的名稱。
  - **作業係統版本**—主機上使用的作業系統版本。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **殺死處理程序**。
  - **使用唯一的 PID 殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。
  - **進行取證**。
  - **隔離檔案**。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料 → 檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - **刪除檔案**。
  - 獲取檔案。
  - **隔離檔案**。
  - 執行應用程式。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

有關“文件被封鎖”事件的資訊

顯示**檔案已封鎖**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **檔案已封鎖**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案**—被封鎖文件的名稱。
  - **MD5**—被封鎖文件的 MD5 雜湊。
  - **SHA256**—被封鎖文件的 SHA256 雜湊。
  - **事件時間**—文件被封鎖的時間。
  - **處理程序檔案** – 嘗試開啟文件之程序的檔案名稱。
  - **處理程序 MD5** – 嘗試開啟文件之程序的 MD5 雜湊。
  - **處理程序 SHA256** – 嘗試開啟文檔的程序的 SHA256 雜湊。
- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **MD5**—父處理程序檔案的 MD5 雜湊。

- **SHA256**—父處理程序檔案的 SHA256 雜湊。
- **處理程序 ID**—父處理程序的識別碼。

- **系統資訊**部分：
  - **主機名稱**—檔案被封鎖的主機的名稱。
  - **主機 IP**—檔案被封鎖的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱**—嘗試開啟檔案的使用者的名稱。
  - **作業係統版本**—主機上使用的作業系統版本。

點擊**檔案已封鎖**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊**事件發起者**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。

- 進行取證。
- 隔離檔案。

- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料** → **檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - **刪除檔案**。
  - 獲取檔案。
  - **隔離檔案**。
  - 執行應用程式。
  - **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。

- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

有關“檔案已修改”事件的資訊

顯示**檔案已變更**事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- 根據對檔案執行的操作類型，事件資訊中會顯示下列部分名稱之一：
  - **檔案建立時間**。
  - **檔案修改時間**。
  - **檔案已重命名**。
  - **檔案屬性已修改**。
  - **檔案已刪除**。
  - **檔案讀取**。
  - **已建立硬連接**。
  - **符號連接已建立**。
  - **檔案建立時間已修改**。

此部分可能會顯示以下資訊：

- **IOA 標記**—有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果資訊：用於建立警示的 TAA (IOA) 規則名稱。

  點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

  如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

- **檔案**—已建立、刪除或修改的檔案名稱。

- **MD5**—已建立、刪除或修改的檔案的 MD5 雜湊。

- **連接引用的檔案的 MD5**—所建立連結指向之檔案的 MD5 雜湊。

- **SHA256**—已建立、刪除或修改的檔案的 SHA256 雜湊。

- **連接引用的檔案的 SHA256**—所建立連結指向之檔案的 SHA256 雜湊。

- **符號連接**—所建立符號連結指向之檔案的完整名稱。

- **大小**—已建立、刪除或修改的檔案大小。

- **事件時間** — 偵測到事件的時間。

- **建立時間**—建立檔案的時間。

- **修改時間** — 檔案的上次修改時間。

- **屬性修改時間**—檔案屬性被修改的時間。

- **以前的版本**—先前版本檔案的名稱。

  > **以前的版本**欄位僅為**檔案已重命名**類型的操作顯示在事件詳細資訊中。

- **重啟後刪除檔案**—要刪除的檔案的狀態。

  如果應用了“刪除”操作的檔案在任何應用程式中開啟或被其他處理程序使用，則當這些處理程序在主機重新啟動後終止時，該檔案將被刪除。在這種情況下，**重啟後刪除檔案**顯示是。

  如果套用了“刪除”操作的檔案立即刪除，則**重啟後刪除檔案**欄位顯示否。

  > **重啟後刪除檔案**欄位僅為**檔案已刪除**類型的操作顯示在事件詳細資訊中。

如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中，則該部分還包括以下欄位：

- **檔案類型**—已建立、刪除或修改的檔案的副檔名。

- **檔案開啟標誌**—已建立、刪除或修改的檔案的開啟標誌的值。

- **所有者使用者名稱**—建立了檔案的使用者的名稱。

- **所有者群組名稱**—其使用者可以修改或刪除檔案的群組的名稱。

- **檔案允許的功能** — 可用於存取已建立、刪除或修改的檔案的權限。如果事件由 Kaspersky Endpoint Security for Mac 記錄，則此欄位不會顯示。
- **檔案可繼承功能** — 使用者群組對已建立、刪除或修改的檔案的父目錄執行操作的權限。如果事件由 Kaspersky Endpoint Security for Mac 記錄，則此欄位不會顯示。
- **檔案有效能力** — 目前與已建立、刪除或修改的檔案相關的權限。如果事件由 Kaspersky Endpoint Security for Mac 記錄，則此欄位不會顯示。

- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的路徑。
  - **MD5** — 父處理程序檔案的 MD5 雜湊。
  - **SHA256** — 父處理程序檔案的 SHA256 雜湊。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中，則**事件發起者**部分還包括以下欄位：

  - **環境變量** — 處理程序的環境變數。
  - **真實使用者名稱**—在系統中註冊時指定的使用者名稱。
  - **真實群組名稱**—使用者所屬的群組。
  - **有效使用者名稱**—用於登入系統的使用者名稱。
  - **有效群組名稱** — 名稱被用於登入系統的使用者群組。
- **系統資訊**部分：
  - **主機名稱** — 建立檔案的主機的名稱。
  - **主機 IP** — 在其上建立檔案的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱** — 建立了檔案的使用者的名稱。
  - **作業系統版本** — 主機上正在使用的作業系統的版本。

  如果事件由 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 記錄在事件資料庫中，則**系統資訊**部分還顯示從其執行遠端登入的主機名稱的**從遠端主機登入**欄位。

在包含執行操作的檔案資訊的部分中點擊包含檔案名或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。

- 執行以下工作：
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊**事件發起者**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

在 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Mac 在事件資料庫中記錄的事件資訊中，您可以點擊包含檔案名稱或檔案路徑的連結以開啟一個清單，您可以在其中選擇以下操作之一:

- 尋找事件。
- 尋找警示。
- 運行獲取檔案工作。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
  - **殺死處理程序**。

    - **刪除檔案**。
    - **隔離檔案**。
    - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
    - **殺死處理程序**。
    - **刪除檔案**。
    - **獲取檔案**。
    - **隔離檔案**。
    - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Mac 事件資訊中，您可以點擊帶有檔案名稱或檔案路徑的連結來開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 運行**獲取檔案**工作。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

有關“系統事件日誌”事件的資訊

顯示**系統事件日誌**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **系統事件日誌**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **事件時間** — 偵測到事件的時間。
  - **安全事件 ID** — Windows 記錄中安全性事件類型的識別碼。

  如果事件由 Kaspersky Endpoint Security for Linux 記錄在事件資料庫中，則**系統事件日誌**部分還包括以下欄位：

  - **事件類型** — 事件的類型。
  - **操作結果** — 例如，**成功**或**已失敗**。
- **事件資料**部分包含系統記錄資訊。資料範圍取決於 Windows 事件的類型。

  由 Kaspersky Endpoint Agent for Linux 記錄到事件資料庫的事件資訊中，不會顯示**事件資料**部分。

- **事件發起者**部分：
  - **檔案** — 處理程序檔名。
  - **處理程序 ID** — 處理程序識別碼。
  - **命令** — 用於執行父處理程序的命令。
  - **環境變量**—處理程序的環境變數。
  - **真實使用者名稱**—在系統中註冊時指定的使用者名稱。
  - **真實群組名稱**—使用者所屬的群組。

  "**事件發起者**"部分不顯示在由 Kaspersky Endpoint Agent for Windows 記錄到事件資料庫的事件的資訊中。

- **系統資訊**部分：
  - **主機名稱** — 發生事件的主機的名稱。
  - **主機 IP** — 在其上事件發生的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱** — 啟動了處理程序的使用者的名稱，該處理程序啟動了系統日誌記錄。
  - **作業系統版本**—主機上正在使用的作業系統的版本。

    Kaspersky Endpoint Security for Linux 記錄到事件資料庫的事件資訊還包括**從遠端主機登入**欄位，即從其執行遠端登入的主機的名稱。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊帶有檔案名稱或檔案路徑的連結來開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 運行獲取檔案工作。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。

- 執行以下工作：
  - **獲取資料** → **檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

有關“登錄檔變更”事件的資訊

顯示**登錄檔已修改**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- 根據對登錄檔執行的操作類型，事件資訊中會顯示以下部分名稱之一：
  - **登錄機碼已建立**
  - **登錄機碼已刪除**
  - **登錄檔已修改**
  - **查詢的登錄機碼**

- **登錄機碼已重命名**
- **登錄機碼已儲存**

此部分顯示以下資訊：

- **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

  點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

  如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

- **檔案**是儲存登錄機碼的檔案的完整路徑。

  > 此欄位會針對**登錄機碼已儲存**類型的事件顯示。

- **金鑰路徑**是被修改之登錄機碼的路徑
- **值名稱**：例如，RegistrySizeLimit
- **值資料**是登錄項目的值
- **值類型**：例如，REG_DWORD
- **事件時間**是修改登錄檔的時間

  當您變更登錄機碼的名稱或值時，您可能會看到其他欄位，其中包含有關登錄機碼修改之前的狀態的資訊：

  - 當登錄機碼名稱被修改時，會顯示**先前的金鑰路徑**欄位。
  - 當登錄值被修改時，會顯示**先前的值資料**欄位。
  - 當登錄值的類型被修改時，會顯示**先前的值類型**欄位。

- **事件發起者**部分：

  - **檔案**—父處理程序檔案的路徑。

    點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

    - **尋找事件**。
    - **尋找警示**。
    - **複製值到剪貼簿**。

    執行以下工作：

    - **殺死處理程序**。
    - **使用唯一的 PID 殺死處理程序**。
    - **刪除檔案**。

    - 獲取檔案。
    - 進行取證。
    - 隔離檔案。
- **MD5**—父處理程序檔案的 MD5 雜湊。
  點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：
    - **尋找事件**。
    - **尋找警示**。
    - 在 Kaspersky TIP 上尋找。
    - **在儲存中尋找**。
    - **建立阻止規則**。

  複製值到剪貼簿。
- **SHA256**—父處理程序檔案的 SHA256 雜湊。
  點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - **尋找事件**。
    - **尋找警示**。
    - 在 Kaspersky TIP 上尋找。
    - **在儲存中尋找**。
    - **建立阻止規則**。
    - **複製值到剪貼簿**。
- **系統資訊**部分：
  - **主機名稱**—在其上進行了登錄檔修改的主機的名稱。
    點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

    執行以下工作：
    - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
    - 殺死處理程序。
    - 刪除檔案。

- **隔離檔案**。
- **執行應用程式**。

- **主機 IP**—在其上進行了登錄檔修改的主機的 IP 位址。

  如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

  該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱**—在登錄檔中進行變更的使用者名稱。
- **作業系統版本**—主機上使用的作業系統版本。

有關“連接埠被偵聽”事件的資訊

顯示**監聽的連接埠**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **監聽的連接埠**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

  - **本機連接埠**—被監聽的連接埠。
  - **本機 IP**—連接埠被監聽的網路介面的 IP 位址。
  - **事件時間**—連接埠監聽時間。
- **事件發起者**部分：
  - **檔案**—父處理程序檔案的路徑。

    點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

    - **尋找事件**。
    - **尋找警示**。
    - **複製值到剪貼簿**。

執行以下工作：

- 殺死處理程序。
- 使用唯一的 PID 殺死處理程序。
- 刪除檔案。
- 獲取檔案。
- 進行取證。
- 隔離檔案。

- **MD5**—父處理程序檔案的 MD5 雜湊。
  點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：
  - **尋找事件**。
  - **尋找警示**。
  - 在 Kaspersky TIP 上尋找。
  - **在儲存中尋找**。
  - **建立阻止規則**。
  - **複製值到剪貼簿**。
- **SHA256**—父處理程序檔案的 SHA256 雜湊。
  點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：
  - **尋找事件**。
  - **尋找警示**。
  - 在 Kaspersky TIP 上尋找。
  - **在儲存中尋找**。
  - **建立阻止規則**。
  - **複製值到剪貼簿**。

- **系統資訊**部分：
  - **主機名稱** — 連接埠被監聽的主機的名稱。
    點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

執行以下工作：

- **獲取資料 → 檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
- **殺死處理程序**。
- **刪除檔案**。
- **隔離檔案**。
- **執行應用程式**。

- **主機 IP** — 連接埠被監聽的主機的 IP 位址。

  如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

  該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱** — 帳戶用於監聽連接埠的使用者的名稱。
- **作業係統版本**—主機上正在使用的作業系統的版本。

有關“驅動程式已載入”事件的資訊

顯示**驅動程式已載入**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- **驅動程式已載入**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

  - **檔案** — 載入的驅動程式檔案的名稱。
  - **MD5** — 載入的驅動程式檔案的 MD5 雜湊值。
  - **SHA256** — 載入的驅動程式檔案的 SHA256 雜湊值。
  - **大小** — 載入的驅動程式的大小。
  - **事件時間** — 驅動程式載入的時間。

- **詳細資訊**部分：
  - **應用程式名稱**—例如，作業系統的名稱。
  - **供應者**—例如，作業系統的供應商。
  - **檔案描述**—例如，範例檔案。
  - **原始檔案名稱**—例如，ExampleFile.exe。
  - **簽章主旨**—核發檔案數位憑證的組織。
  - **簽章驗證結果** — 例如，“簽名無效”或“簽名正常”。
  - **建立時間** — 載入的驅動程式的建立時間。
  - **修改時間** — 載入的驅動程式的上次修改時間。
- **系統資訊**部分：
  - **主機名稱** — 載入了驅動程式的主機的名稱。
  - **主機 IP** — 向其載入了驅動程式的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **使用者名稱** — 載入了驅動程式的使用者的名稱。
  - **作業係統版本**—主機上使用的作業系統版本。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料 → 檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

有關“DNS”事件的資訊

顯示**DNS**事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- **DNS**部分：
  - **IOA 標記**—有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **伺服器 IP**—DNS 伺服器的 IPv4 位址。
  - **查詢選項**—DNS 查詢選項。
  - **請求狀態**—DNS 查詢的狀態。
  - **網域名稱**—要解析 DNS 記錄的網域名稱。
  - **記錄類型 ID**—資源記錄的類型。
  - **回應資料**—DNS 伺服器對查詢的回應內容。
  - **事件時間**—傳送 DNS 查詢的時間。
- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
  - **處理程序 ID**—父處理程序的識別碼。

    如果事件由 Kaspersky Endpoint Agent for Linux 記錄在事件資料庫中，則**事件發起者**部分還包括以下欄位：
  - **環境變量**—處理程序的環境變數。
  - **真實使用者名稱**—在系統中註冊時指定的使用者名稱。
  - **真實群組名稱**—使用者所屬的群組。
  - **有效使用者名稱**—用於登入系統的使用者名稱。
  - **有效群組名稱** — 名稱被用於登入系統的使用者群組。

- **系統資訊**部分：
  - **主機名稱**—向 DNS 伺服器發出查詢的主機的名稱。
  - **主機 IP**—向 DNS 伺服器發出查詢的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

  - **從遠端主機登入**—用於遠端登入系統的主機名稱。
  - **使用者名稱** — 向 DNS 伺服器發出查詢的使用者的名稱。
  - **作業系統版本** — 主機上正在使用的作業系統的版本。

點擊帶有伺服器 IP 位址、記錄類型 ID 和使用者名的連結將開啟一個清單，您可以在其中執行以下操作之一：

- 尋找警示。
- **複製值到剪貼簿**。

點擊具有域名的連結將開啟一個清單，您可以在其中執行以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **複製值到剪貼簿**。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料** → **檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。
  - **刪除檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。
  - **隔離檔案**。
  - **執行應用程式**。
- **複製值到剪貼簿**。

點擊包含主機IP 位址的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

有關“LDAP”事件的資訊

顯示“**LDAP**”事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- **LDAP**區段：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **搜尋範圍**—LDAP 搜尋範圍。可以具有下列數值之一：ADS_SCOPE_BASE、ADS_SCOPE_ONELEVEL、ADS_SCOPE_SUBTREE。
  - **搜尋篩選器**—LDAP 搜尋篩選器。
  - **可分辨名稱**—LDAP 目錄條目的名稱。

- **搜尋屬性清單**—搜尋查詢中指定為要傳回的值的屬性。
- **啟動參數**—處理程序啟動設定。

- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
- **系統資訊**部分：
  - **主機名稱**—在其上執行 LDAP 搜尋的主機的名稱。
  - **使用者名稱**—其帳戶用於執行 LDAP 搜尋的使用者的名稱。
  - **作業係統版本**—主機上正在使用的作業系統的版本。

有關“命名管道”事件的資訊

顯示**命名管道**事件資訊的視窗包含下列詳細資料：

- 事件樹。
- 處理事件時可以執行的動作。
  根據命名管道操作的類型，事件資訊中會顯示下列部分名稱的其中一個：
  - **已建立管道**
  - **管道已連線**

  此部分顯示以下資訊：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。
    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。
    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案**—建立或連線到命名管道的程序的檔案名稱。
  - **事件時間**—建立或連線命名管道的時間。
- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。

- **系統資訊**部分：
  - **主機名稱**—建立或連線到命名管道的主機名稱。
  - **使用者名稱**—建立或連線到命名管道的使用者名稱。
  - **作業系統版本**—主機上正在使用的作業系統的版本。

點擊具有管道名稱的連結將開啟一個清單，您可以在其中執行以下操作之一：

- 尋找警示。
- **複製值到剪貼簿**。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 殺死處理程序。
  - 使用唯一的 PID 殺死處理程序。
  - 刪除檔案。
  - 獲取檔案。
  - 進行取證。
  - 隔離檔案。
- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。

- 在 Kaspersky TIP 上尋找。
- 在 virustotal.com 上尋找。
- 在儲存中尋找。
- 建立阻止規則。
- 複製值到剪貼簿。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 執行以下工作：
  - 獲取資料 → 檔案、取證、磁碟鏡像、記憶體傾印。
  - 殺死處理程序。
  - 刪除檔案。
  - 隔離檔案。
  - 執行應用程式。
- 複製值到剪貼簿。

點擊包含主機IP 位址的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 複製值到剪貼簿。

點擊具有使用者名稱的連結將開啟一個清單，您可以在其中執行以下操作之一：

- 尋找警示。
- 複製值到剪貼簿。

有關“WMI”事件的資訊

顯示“WMI”事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。

根據操作的類型，事件資訊中會顯示下列部分名稱的其中一個：

- **WMI 活動**
- **WMI 事件使用者名稱**

“**WMI 活動**”部分顯示以下資訊：

- **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

  點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

  如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

- **到遠端主機的連線**—遠端啟動 WMI 服務。如果服務是遠端啟動的，則欄位會顯示**是**。
- **机器名稱**—啟動 WMI 服務的主機名稱。
- **使用者名稱**—啟動 WMI 服務的使用者名稱。
- **名字空間**—WMI 命名空間。
- **查詢**—用於啟動 WMI 服務的指令。

“**WMI 活動**”部分顯示以下資訊：

- **到遠端主機的連線**—遠端啟動 WMI 服務。如果服務是遠端啟動的，則欄位會顯示**是**。
- **名字空間**—事件消費者的命名空間。
- **事件篩選器名稱**—事件消費者的篩選器的名稱。此欄位為**WMI 活動**事件類型顯示。
- **事件使用者名稱**—所建立的事件消費者的名稱。
- **事件使用者描述**—所建立的事件消費者的描述。此欄位為**WMI 事件使用者名稱**事件類型顯示。

- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的名稱。
  - **啟動參數**—父處理程序啟動設定。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
- **系統資訊**部分：
  - **主機名稱**—啟動 WMI 服務或建立事件消費者的主機的名稱。
  - **主機 IP**—啟動 WMI 服務或建立事件消費者的主機的 IP 位址。
  - **使用者名稱**—啟動 WMI 服務或建立事件消費者的使用者的名稱。
  - **作業係統版本**—主機上正在使用的作業系統的版本。

有關“警示”事件的資訊

顯示**偵測**類型事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- 在**詳細資訊**索引標籤的**偵測**區段中：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **偵測**—偵測到的物件的名稱。

    點擊物件連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - **對卡巴斯基威脅的看法**。
    - **複製值到剪貼簿**。
  - **最後一個操作**—對偵測到的物件採取的最後一個動作。
  - **物件名稱**—偵測到物件的檔案的完整名稱。
  - **MD5**—偵測到物件的檔案的 MD5 雜湊。
  - **SHA256**—偵測到物件的檔案的 SHA256 雜湊。
  - **物件類型**—物件類型（例如，檔案）。
  - **偵測模式**—產生警示的掃描模式。
  - **事件時間**—事件的日期和時間。
  - **記錄 ID**—資料庫中偵測記錄的 ID。
  - **資料庫版本**—用於產生警示的資料庫版本。
  - **內容**—被傳送進行掃描的指令碼的內容。

    您可以透過點擊**儲存到檔案**下載此資料。
- 在**詳細資訊**索引標籤上，在**事件發起者**部分：
  - **檔案**—父處理程序檔案的路徑。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- **複製值到剪貼簿**。

執行以下工作：

- 殺死處理程序。
- 使用唯一的 PID 殺死處理程序。
- 刪除檔案。
- 獲取檔案。
- 進行取證。
- 隔離檔案。

- **處理程序 ID** — 父處理程序的識別碼。
- **啟動參數** — 父處理程序啟動設定。
- **MD5**—父處理程序檔案的 MD5 雜湊。
- **SHA256**—父處理程序檔案的 SHA256 雜湊。

- 在**詳細資訊**索引標籤的**系統資訊**區段中：
  - **主機名稱**—產生警示的主機名稱。
    點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

    執行以下工作：
    - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
    - 殺死處理程序。
    - 刪除檔案。
    - 隔離檔案。
    - 執行應用程式。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Linux 事件資訊中，您可以點擊主機名稱連結開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 運行工作：獲取檔案、**刪除檔案**、**隔離檔案**、執行應用程式。
- **複製值到剪貼簿**。

在事件資料庫中記錄的 Kaspersky Endpoint Security for Mac 事件資訊中，您可以點擊帶有檔案名稱或檔案路徑的連結來開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 運行獲取檔案工作。
- **複製值到剪貼簿**。

- **主機 IP**—在其上產生警示的主機的 IP 位址。

  如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

  該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱**—使用者帳戶，用於完成對偵測到的物件執行的操作。
- **作業系統版本**—主機上正在使用的作業系統的版本。

- 在**歷史**索引標籤上，在表格中：
  - **類型**—事件類型：**偵測**或者**偵測處理結果**。
  - **敘述**—事件描述。
  - **時間**—偵測和偵測處理結果的日期和時間。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

有關“偵測處理結果”事件的資訊

顯示**偵測處理結果**類型事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- 在**詳細資訊**索引標籤上，在**偵測處理結果**下面：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **偵測**—偵測到的物件的名稱。

    點擊物件連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - **尋找事件**。
    - **對卡巴斯基威脅的看法**。
    - **複製值到剪貼簿**。
  - **最後一個操作**—對偵測到的物件採取的最後一個動作。
  - **MD5**—偵測到物件的檔案的 MD5 雜湊。
  - **SHA256**—偵測到物件的檔案的 SHA256 雜湊。
  - **物件類型**—物件類型（例如，檔案）。
  - **物件名稱**—偵測到物件的檔案的完整名稱。
  - **偵測模式**—產生警示的掃描模式。

- **事件時間**—事件的日期和時間。
- **記錄 ID**—資料庫中偵測記錄的 ID。
- **資料庫版本**—用於產生警示的資料庫版本。

- 在**詳細資訊**索引標籤上，在**事件發起者**下：
  - **檔案**—父處理程序檔案的路徑。
    點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

    執行以下工作：
    - 殺死處理程序。
    - 使用唯一的 PID 殺死處理程序。
    - 刪除檔案。
    - 獲取檔案。
    - 進行取證。
    - 隔離檔案。
  - **處理程序 ID** — 父處理程序的識別碼。
  - **啟動參數** — 父處理程序啟動設定。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
- 在**詳細資訊**索引標籤上，在**系統資訊**下：
  - **主機名稱**—產生警示的主機名稱。
    點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

    執行以下工作：
    - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
    - 殺死處理程序。

- 刪除檔案。
- 隔離檔案。

執行應用程式。

- **主機 IP**—在其上產生警示的主機的 IP 位址。

  如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

  該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱**—使用者帳戶，用於完成對偵測到的物件執行的操作。
- **作業系統版本**—主機上正在使用的作業系統的版本。

- 在**歷史**索引標籤上，在表格中：
  - **類型**是**偵測處理結果**事件的類型。
  - **敘述**—事件描述。
  - **時間**是警示處理結果的日期和時間。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- **在 virustotal.com 上尋找**。
- 在儲存中尋找。
- 建立阻止規則。
- **複製值到剪貼簿**。

有關“被解釋檔案運行”事件的資訊

顯示**處理程序：解釋檔案執行**事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- **處理程序：解釋檔案執行**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **檔案** — 檔案的名稱。
  - **MD5** — 檔案的 MD5 雜湊。
  - **SHA256** — 檔案的 SHA256 雜湊。
  - **大小** — 檔案的大小。
  - **建立時間** — 建立檔案的時間。
  - **修改時間** — 檔案的上次修改時間。
- **事件發起者**部分：
  - **檔案** — 父處理程序檔案的路徑。
  - **MD5** — 父處理程序檔案的 MD5 雜湊。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
  - **處理程序 ID**—父處理程序的識別碼。
- **系統資訊**部分：
  - **主機名稱** — 執行檔案的主機的名稱。
  - **主機 IP** — 在其上執行檔案的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱** – 帳戶用於執行檔案的使用者的名稱。
- **作業係統版本**–主機上使用的作業系統版本。

點擊**處理程序：解釋檔案執行**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **刪除檔案**。
  - **獲取檔案**。
  - **進行取證**。
  - **隔離檔案**。
- **複製值到剪貼簿**。

點擊**事件發起者**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **殺死處理程序**。
  - **使用唯一的 PID 殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。
  - **進行取證**。
  - **隔離檔案**。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
  - **獲取資料 → 檔案**、**取證**、**磁碟鏡像**、**記憶體傾印**。
  - **殺死處理程序**。

- **刪除檔案**。
- **隔離檔案**。
- **執行應用程式**。

- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

有關“AMSI 掃描”事件的資訊

顯示**AMSI 掃描**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- 在**AMSI 掃描**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

- **物件名稱**—掃描物件的名稱。
- **MD5**—掃描物件的 MD5 雜湊。
- **SHA256**—掃描物件的 SHA256 雜湊。
- **事件時間**—事件的日期和時間。
- **內容類型**—指令碼類型。

  應用程式提供兩種類型的指令碼：

  - 如果指令碼以文字呈現，則**內容類型**欄位顯示*文字*指令碼類型。
  - 如果指令碼以其他格式呈現，則**內容類型**欄位顯示*二進制*指令碼類型。
- **內容**—被傳送進行掃描的指令碼的內容。

  如果資料以文字呈現，您可以點擊**複製到剪貼簿**複製此資料；如果資料有不同的格式，請點擊**儲存到檔案**下載包含資料的檔案。

  > 如果應用程式注意到針對性攻擊跡象，則**內容**欄位會顯示在事件資訊中。

- 在**事件發起者**部分：
  - **檔案**—父處理程序檔案的路徑。

    點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

    - **尋找事件**。
    - **尋找警示**。
    - **複製值到剪貼簿**。

    執行以下工作：

    - **殺死處理程序**。
    - **使用唯一的 PID 殺死處理程序**。
    - **刪除檔案**。
    - **獲取檔案**。
    - **進行取證**。
    - **隔離檔案**。
  - **MD5**—父處理程序檔案的 MD5 雜湊。

    點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

    - **尋找事件**。
    - **尋找警示**。

- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

- **SHA256**—父處理程序檔案的 SHA256 雜湊。
  點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：
  - **尋找事件**。
  - **尋找警示**。
  - 在 Kaspersky TIP 上尋找。
  - **在儲存中尋找**。
  - **建立阻止規則**。
  - **複製值到剪貼簿**。

- 在**系統資訊**部分：
  - **主機名稱** – 產生偵測的主機名稱。
    點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

    執行以下工作：
    - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
    - 殺死處理程序。
    - 刪除檔案。
    - 隔離檔案。
    - 執行應用程式。
  - **主機 IP**—在其上建立警示的主機的 IP 位址。

    如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

    該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱**—用於在登錄檔中做出變更的使用者帳戶。
- **作業係統版本**—主機上正在使用的作業系統的版本。

有關“在主控台進行互動式命令輸入”事件的資訊

顯示**處理程序：主控台互動式輸入**事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- **處理程序：主控台互動式輸入**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。
  - **輸入類型**—被傳遞到主控台應用程式的命令輸入類型。

    該應用程式提供兩種輸入命令的方式：
    - 如果使用者在主控台應用程式中輸入命令，**輸入類型**欄位將顯示*主控台*命令輸入類型。
    - 如果命令被透過管道從另一個應用程式傳遞到主控台應用程式，**輸入類型**欄位將顯示*管道*命令輸入類型。
    - **輸入文字** — 在具有 Kaspersky Endpoint 元件的主機上的命令列（例如 CMD）中輸入的文字。

    您可以透過點擊位於**輸入文字**欄位中的**複製到剪貼簿**按鈕複製此文字。
  - **事件時間** — 偵測到事件的時間。
- **事件發起者**部分：
  - **檔案**—父處理程序檔案的路徑。

    點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：
    - **尋找事件**。
    - **尋找警示**。
    - **複製值到剪貼簿**。

    執行以下工作：
    - **殺死處理程序**。
    - **使用唯一的 PID 殺死處理程序**。
    - **刪除檔案**。

    - 獲取檔案。
    - 進行取證。
    - 隔離檔案。
  - **MD5**—父處理程序檔案的 MD5 雜湊。
    點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：
    - **尋找事件**。
    - **尋找警示**。
    - 在 Kaspersky TIP 上尋找。
    - **在儲存中尋找**。
    - **建立阻止規則**。
    - **複製值到剪貼簿**。
  - **SHA256**—父處理程序檔案的 SHA256 雜湊。
    點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - **尋找事件**。
    - **尋找警示**。
    - 在 Kaspersky TIP 上尋找。
    - **在儲存中尋找**。
    - **建立阻止規則**。
    - **複製值到剪貼簿**。
- **系統資訊**部分：
  - **主機名稱** — 在其上輸入指令的主機的名稱。
    點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：
    - 尋找事件。
    - 尋找警示。
    - **複製值到剪貼簿**。

    執行以下工作：
    - **獲取資料** → 檔案、取證、磁碟鏡像、記憶體傾印。
    - 殺死處理程序。
    - 刪除檔案。

- **隔離檔案**。
- **執行應用程式**。

- **主機 IP**—在其上輸入指令的主機的 IP 位址。

  如果您使用動態 IP 位址，該欄位會顯示建立事件時指派給主機的 IP 位址。

  該應用程式不支援 IPv6。如果您使用 IPv6，則不會顯示主機的 IP 位址。

- **使用者名稱**—被用於輸入指令的使用者帳戶。
- **作業系統版本**—主機上正在使用的作業系統的版本。

有關"代碼注入"事件的資訊

顯示"**代碼注入**"事件資訊的視窗包含以下詳情：

- 事件樹。
- 處理事件時可以執行的動作。
- **代碼注入**部分：
  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

  - **檔案**—目標處理程序檔案的路徑。
  - **處理程序 ID**—目標處理程序的識別碼。
  - **啟動參數**—目標處理程序的命令列選項。
  - **修改的啟動選項**—修改的目標處理程序命令列選項。

    如果使用 ARG_SPOOFING 方法注入代碼，則會顯示此欄位。

  - **MD5**—目標處理程序檔案的 MD5 雜湊。
  - **SHA256**—目標處理程序檔案的 SHA256 雜湊。
  - **存取方法**—存取目標處理程序的方法。

    此欄位可以具有以下值：WRITE_EXECUTABLE_MEMORY、SET_WINDOWS_HOOK、QUEUE_APC_THREAD、SET_THREAD_CONTEXT – .MAP_VIEW_OF_SECTION、CREATE_REMOTE_THREAD、ARG_SPOOFING。

- **位址空間**—目標處理程序位址空間中放置遠端執行程式碼的位址。

  如果使用 SET_WINDOWS_HOOK 或 aRG_SPOOFING 方法注入代碼，則不會填入此欄位。

- **系統調用參數**—啟動目標處理程序時使用的命令列。

- **DLL 名稱**—包含鉤子程序的 DLL 名稱，以及注入後控制權所傳遞至的功能名稱。

  如果使用 SET_WINDOWS_HOOK 方法注入代碼，則填入此欄位。

- **DLL 完整路徑** — 包含鉤子過程的 DLL 的路徑。

  如果使用 SET_WINDOWS_HOOK 方法注入代碼，則填入此欄位。

- **事件時間** — 代碼注入的時間。

- **調用跟蹤** — 攔截代碼注入相關功能時的 API 呼叫堆疊。

- **事件發起者**部分：

  - **檔案** — 父處理程序檔案的名稱。

  - **MD5**—父處理程序檔案的 MD5 雜湊。

  - **SHA256**—父處理程序檔案的 SHA256 雜湊。

- **系統資訊**部分：

  - **主機名稱** — 發生代碼注入的主機的名稱。

  - **使用者名稱** — 用於代碼注入的使用者帳戶的名稱。

  - **作業係統版本**—主機上正在使用的作業系統的版本。

有關“處理程序存取”事件的資訊

顯示**檔案已變更**事件資訊的視窗包含以下詳情：

- 事件樹。

- 處理事件時可以執行的動作。

- 根據對處理程序檔案執行的操作類型，事件資訊中會顯示以下部分名稱之一：

  - **處理程序存取已開啟**

  - **複製句柄**

  “**處理程序存取已開啟**”顯示以下資訊：

  - **IOA 標記** — 有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。

    點擊連結以顯示有關 TAA (IOA) 規則的資訊。如果規則是由卡巴斯基專家提供的，則它包含有關觸發的 MITRE 技術的資訊以及對事件進行反應的建議。

    如果在建立事件時觸發了 TAA (IOA) 規則，則會顯示該欄位。

- **檔案** — 接收者程序的名稱。
- **處理程序 ID** — 接收者處理程序的處理程序ID。
- **啟動參數** — 接收者程序的命令列選項。
- **MD5** — 接收者處理程序檔案的 MD5 雜湊。
- **SHA256** — 接收者處理程序檔案的 SHA256 雜湊。
- **存取權限** — 請求的處理程序存取權限。
- **大小** — 接收者處理程序檔案的大小。
- **事件時間** — 偵測到事件的時間。
- 建立時間 — 接收者處理程序檔案的建立時間。
- **修改時間** — 接收者處理程序檔案的上次修改時間。
- **屬性修改時間** — 接收者處理程序檔案屬性改變的時間。
- **調用跟蹤** — 呼叫堆疊。

"**複製句柄**"部分顯示以下資訊：

- **檔案** — 複製過程的檔案名稱。
- **MD5** — 複製處理程序檔案的 MD5 雜湊。
- **SHA256** — 複製處理程序檔案的 SHA256 雜湊。
- **建立時間** — 複製處理程序檔案的建立時間。
- **修改時間** — 複製處理程序檔案的上次修改時間。
- **屬性修改時間** — 複製處理程序檔案屬性改變的時間。
- **大小** — 複製處理程序檔案的大小。
- **處理程序 ID** — 重複處理程序的 ID。
- **啟動參數** — 複製程序的命令列選項。

對於此類型的事件，事件資訊還包括"**有關向其複製句柄的處理程序的資訊**"和"**有關從其複製句柄的處理程序的資訊**"部分。這些部分包含以下資訊：

- **檔案** — 處理程序檔名。
- **MD5** — 處理程序檔案的 MD5 雜湊。
- **SHA256** — 處理程序檔案的 MD5 雜湊。
- **處理程序 ID** — 處理程序標識符。
- **啟動參數** — 處理程序啟動設定。

    - **大小** – 處理程序檔案的大小。
    - **建立時間** – 處理程序檔案的建立時間。
    - **修改時間** – 檔案的上次修改時間。
    - **屬性修改時間** – 處理程序檔案屬性改變的時間。
- **事件發起者**部分：
    - **檔案** – 父處理程序檔案的路徑。
    - **MD5** – 父處理程序檔案的 MD5 雜湊。
    - **SHA256** – 父處理程序檔案的 SHA256 雜湊。
    - **啟動參數** – 父處理程序啟動設定。
- **系統資訊**部分：
    - **主機名稱** – 建立檔案的主機的名稱。
    - **使用者名稱** – 建立了檔案的使用者的名稱。
    - **作業系統版本** – 主機上正在使用的作業系統的版本。

在包含執行操作的檔案資訊的部分中點擊包含檔案名或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
    - **刪除檔案**。
    - **獲取檔案**。
    - **進行取證**。
    - **隔離檔案**。
- **複製值到剪貼簿**。

點擊**事件發起者**部分中包含檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 執行以下工作：
    - **殺死處理程序**。
    - **使用唯一的 PID 殺死處理程序**。

- 刪除檔案。
- 獲取檔案。
- 進行取證。
- 隔離檔案。

- **複製值到剪貼簿**。

點擊 **MD5** 連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- 在 Kaspersky TIP 上尋找。
- **在儲存中尋找**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊 **SHA256** 連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- 在 Kaspersky TIP 上尋找。
- **在 virustotal.com 上尋找**。
- 在儲存中尋找。
- 建立阻止規則。
- **複製值到剪貼簿**。

關於“USB 裝置”事件的資訊

顯示**USB 裝置**事件資訊的視窗包含以下詳細資訊：

- 事件樹。
- 處理事件時可以執行的動作。
- “**磁碟機已連線**”部分：
  - “**裝置名稱**”是已連線裝置的名稱。
  - “**裝置 ID**”是已連線裝置的 ID。

- “**裝置類型**”是已連線裝置的類型。
- “**系統磁碟機**”表示該裝置是系統磁碟機。可能的值：**是**、**否**。
- “**事件時間**”是裝置連線的時間。

- **系統資訊**部分：
  - “**主機名稱**”是裝置所連線的主機的名稱。
  - “**主機 IP**”是裝置所連線的主機的 IP 位址。
  - “**使用者名稱**”是帳戶用於執行檔案的使用者的名稱。
  - “**作業系統版本**”是主機上正在使用的作業系統的版本。

根據 Kaspersky TAA (IOA) 規則進行事件鏈掃描

有些網路攻擊只有透過檢視特定的事件序列才能偵測到。如果啟用了事件鏈掃描功能，Kaspersky Anti Targeted Attack Platform 會根據 Kaspersky TAA (IOA) 規則標記到達 Central Node 伺服器的事件，當偵測到可疑事件序列時，會在警示表中記錄警示。

您可以透過以下方式之一檢視由 Kaspersky TAA (IOA) 規則標記的事件：

- 透過對事件資料庫建立搜尋查詢，並使用下列條件：IOATag、IOAImportance、IOAConfidence。
- 檢視事件和警示時。

Kaspersky TAA (IOA) 規則無法編輯。如果您不希望應用程式為作為對您組織正常的主機活動的一部分產生的事件建立警示，您可以將 TAA (IOA) 規則新增至排除項目。每個 Kaspersky TAA (IOA) 規則只能建立一個排除項目。

在分佈式解決方案和多組織用戶模式下，您必須在要使用它的每個 Central Node 伺服器上啟用事件鏈掃描功能。如果 Central Node 元件被部署為叢集，您可以在叢集中的任何伺服器上啟用該功能。

使用掃描事件鏈的 TAA（IOA）規則會導致更高的系統資源使用率。如果您在使用應用程式時遇到效能問題，我們建議停用此功能。

在小工具中顯示事件鏈資訊的特殊注意事項

前 10 個小工具僅顯示有關觸發 TAA（IOA）規則的事件的資訊。小工具不會考慮先前發生並參與事件鏈但未觸發規則的事件。因此，小工具報告的事件數可能與您點擊帶有主機名稱和 TAA (IOA) 規則名稱的連結時顯示的事件數不符。

啟用或停用根據 Kaspersky TAA (IOA) 規則進行事件鏈掃描

若要啟用或停用根據 Kaspersky TAA (IOA) 規則進行事件鏈掃描

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分的**Endpoint Agent**子部分。
2. 在**對事件鏈使用 TAA (IOA) 規則**下，執行下列其中一項操作：
   - 如果要啟用該功能，請將**對事件鏈使用規則**切換開關設定為**已啟用**。
   - 如果要停用該功能，請將**對事件鏈使用規則**切換開關設定為**已停用**。

   預設情況下停用此功能。

已啟用或停用根據 Kaspersky TAA (IOA) 規則進行事件鏈掃描。

檢視由 Kaspersky TAA (IOA) 規則標記的事件

*若要在**警示**區段中檢視由所選 Kaspersky TAA (IOA) 規則標記的所有事件：*

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊**技術**列中的連結開啟篩選器配置視窗。
3. 在左側的下拉清單中，選擇**包含**。
4. 在右側的下拉清單中，選擇**（TAA）針對性攻擊分析器**技術。
5. 點擊**套用**。
   此表顯示 TAA 技術根據 TAA (IOA) 規則產生的警示。
6. 選擇一個警示，**偵測到**列為其顯示相關規則的名稱。
   這將開啟一個視窗，其中包含有關警示的資訊。
7. 在**掃描結果**下面，點擊帶有規則名稱的連結以開啟規則資訊視窗。
8. 這將開啟一個視窗；在該視窗中，點擊**事件**。

將顯示與所選TAA (IOA) 規則相符的事件表。

*若要在**威脅搜尋**區段中檢視由所選 Kaspersky TAA (IOA) 規則標記的所有事件：*

1. 在應用程式 Web 介面視窗中選擇**威脅搜尋**區段。
   這將開啟事件搜尋表單。
2. 定義搜尋條件並點擊**搜尋**按鈕。例如，您可以在產生器模式下在**TAA 屬性**群組中選擇事件搜尋條件。
   滿足搜尋條件的事件表將顯示。

3. 選擇一個事件。

4. 在**IOA 標記**設定右側，點擊規則名稱。

   這將開啟一個視窗，其中包含有關規則的資訊。

5. 這將開啟一個視窗；在該視窗中，點擊**事件**。

將顯示與所選TAA (IOA) 規則相符的事件表。

管理資產

*資產*是組織本機和內部網路中存在的所有裝置。要管理資產，您可以在 Kaspersky Anti Targeted Attack Platform Web 介面的"**資產**"區域檢視裝置表。您還可以在管理網路互動圖和拓撲圖時檢視有關裝置互動的資訊，並對裝置執行各種操作。

檢視裝置表

為了管理裝置，應用程式會產生一個裝置表。應用程式將表中的所有裝置視為已知裝置。

若要檢視裝置表：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。

2. 轉到"**裝置**"索引標籤。

   裝置表將顯示。

該表顯示以下資訊：

- **名稱**是代表應用程式中裝置的名稱。

- **裝置 ID** 是 Kaspersky Anti Targeted Attack Platform 中指派的裝置 ID。

- **狀態**是裝置狀態，決定裝置是否允許在公司 LAN 上活動。裝置可以具有以下狀態之一：

  - **已授權**。此狀態分配給允許在網路上活動的裝置。

  - **未授權**。此狀態指派給不允許在網路上活動的裝置。

  - **已存檔**。如果裝置不再使用或不得在網路上使用，或裝置長時間（30 天或更長時間）未處於作用中且有關該裝置的資訊尚未更新，則會為裝置指派此狀態。

- **位址資訊**列出了裝置的 MAC 和/或 IP 位址。如果裝置有多個網路介面，則每個網路介面可以有不同的 MAC 和/或 IP 位址。

- **類別**是表徵裝置功能用途的類別名稱。Kaspersky Anti Targeted Attack Platform 辨識以下裝置類別：

  - **伺服器**指部署了伺服器軟體的電腦。

  - **網路裝置**指網路設備（例如路由器、交換器）。

- **工作站**指固定式個人電腦或操作員工作站。
- **行動裝置**指具有運算功能的可攜式電子裝置。
- **筆記型電腦**指可攜式個人電腦。
- **印表機**指列印裝置。
- **UPS**指連線至電腦網路的不斷電系統。
- **網路攝影機**指進行視訊監控並傳輸數位影像資料的裝置。
- **閘道**指透過轉換各種介面（例如序列乙太網路），連線具有異質資料傳輸媒體和不同協定之網路的裝置。
- **儲存系統**指在記憶體系統內儲存資訊的裝置。
- **防火牆**指充當防火牆以掃描並封鎖不需要流量的裝置。
- **交換器**指以實體方式連接區域網路主機的裝置。
- **虛擬交換器**指以邏輯方式組合實體交換器或軟體交換器，以用於虛擬化系統的裝置。
- **路由器**指在電腦網路的各網段之間轉送網路封包的裝置。
- **虛擬路由器**指以邏輯方式組合實體路由器，或使用多個獨立路由和轉送表之路由器的裝置。
- **Wi-Fi**指為 Wi-Fi 網路中的裝置提供無線連線的存取點。
- **歷史資料伺服器**指具有封存資料的伺服器。
- **其他**指不屬於上述任何類別的裝置。

- **群組**是裝置在裝置群組樹中所屬群組的名稱（包含群組本身的名稱及其所有父群組的名稱）。
- **安全狀態**是裝置的安全狀態，由是否存在裝置相關事件決定。裝置可具有以下安全狀態之一：
  - **嚴重**。該裝置具有嚴重程度評分為 8.0 至 10.0 的相關事件。
  - **警告**。該裝置具有嚴重程度評分為 4.0 至 7.9 的相關事件。
  - **正常**。該裝置具有嚴重程度評分為 0.0 至3.9 的相關事件，或裝置沒有關聯事件。
- **重要性**是裝置的重要性。根據裝置的類別為其分配重要性。裝置可以具有以下重要性等級之一：
  - **高**。分配給**伺服器**類別的裝置。
  - **中**。分配給以下類別的裝置：**網路裝置**、**工作站**、**閘道**、**儲存系統**、**防火牆**、**交換機**、**虛擬交換機**、**路由器**、**虛擬路由器**、**Wi-Fi**、**歷史資料伺服器**。
  - **低**。分配給以下類別的裝置：**行動裝置**、**筆記型電腦**、**印表機**、**UPS**、**網路攝影機**或**其他**。
- **上次看到**是裝置上次記錄為活動的日期和時間。
- **風險**列出了針對裝置偵測到的風險類別。預設情況下，裝置表僅顯示目前風險的資訊。若要顯示所有風險的資訊，您可以在設定裝置表時選取**顯示已修復且已接受的風險**核取方塊。

- **上次修改**是上次修改裝置資訊的日期和時間。
- **已建立**是將裝置新增至裝置表的日期和時間。
- **OS**是裝置上安裝的作業系統的名稱。
- **硬體供應商**是裝置硬體供應商的名稱。在詳細資料區域中，此參數稱為**供應商**，並顯示在**硬體**下的**一般**索引標籤上。
- **硬體型號**是裝置型號的名稱。在詳細資料區域中，此參數稱為**型號**，顯示在**硬體**下的**一般**索引標籤上。
- **硬體版本**是裝置硬體的版本號。在詳細資料區域中，此參數稱為**版本**，顯示在**硬體**下的**一般**索引標籤上。
- **軟體供應商**是裝置軟體的供應商名稱。在詳細資料區域中，此參數稱為**供應商**，並顯示在**軟體**下的**一般**索引標籤上。
- **軟體名稱**是裝置軟體的名稱。在詳細資料區域中，此參數稱為**名稱**，顯示在**軟體**下的**一般**索引標籤上。
- **軟體版本**是裝置軟體的版本號。在詳細資料區域中，此參數稱為**版本**，顯示在**軟體**下的**一般**索引標籤上。
- **網路名稱**是代表網路上的裝置的名稱。
- **標籤**列出了分配給裝置的標籤。
- **EPP 應用程式**是裝置上安裝的 EPP 應用程式的簡稱（如果此應用程式已與 Kaspersky Anti Targeted Attack Platform 通訊）。
- **EPP 連線**是裝置上安裝的Endpoint Agent 元件與 Integration Server 的連線狀態。可以有以下狀態：
  - **活動**。自從應用程式上次連線到 Integration Server 以來，已過去不到 24 小時。
  - **不活動**。自從應用程式上次連線到 Integration Server 以來，已超過 24 小時。
  - **N/A**。連線狀態未知。
- **上次連線至 EPP** 是 Endpoint Agent 元件上次連線到 Integration Server 的日期。

檢視裝置資訊

若要檢視裝置資訊：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**裝置**”索引標籤。
3. 選擇您想檢視資訊的裝置。

這將開啟一個視窗，其中包含有關裝置的資訊。

此視窗可以包含以下資訊：

- 裝置資訊：
  - **安全狀態**是裝置的安全狀態，由裝置相關事件的存在決定。裝置可具有以下安全狀態之一：
    - **嚴重**。該裝置具有嚴重程度評分為 8.0 至 10.0 的相關事件。
    - **警告**。該裝置具有嚴重程度評分為 4.0 至 7.9 的相關事件。
    - **正常**。該裝置具有嚴重程度評分為 0.0 至3.9 的相關事件，或裝置沒有關聯事件。
  - **重要性**是該裝置對組織的重要性。根據裝置的類別為其分配重要性。裝置可以具有以下重要性等級之一：
    - **高**。分配給**伺服器**類別的裝置。
    - **中**。分配給以下類別的裝置：**網路裝置**、**工作站**、**閘道**、**儲存系統**、**防火牆**、**交換機**、**虛擬交換機**、**路由器**、**虛擬路由器**、**Wi-Fi**、**歷史資料伺服器**。
    - **低**。分配給以下類別的裝置：**行動裝置**、**筆記型電腦**、**印表機**、**UPS**、**網路攝影機**或**其他**。
  - **狀態**是裝置狀態，決定裝置是否允許在公司 LAN 上活動。裝置可以具有以下狀態之一：
    - **已授權**。此狀態分配給允許在網路上活動的裝置。
    - **未授權**。此狀態指派給不允許在網路上活動的裝置。
    - **已存檔**。如果裝置不再使用或不得在網路上使用，或裝置長時間（30 天或更長時間）未處於作用中且有關該裝置的資訊尚未更新，則會為裝置指派此狀態。
  - **類別**是表徵裝置功能用途的類別名稱。
  - **網路名稱**是代表網路上的裝置的名稱。
  - **群組**是裝置在裝置群組樹中所屬群組的名稱（包含群組本身的名稱及其所有父群組的名稱）。
- “**主要**”索引標籤：
  - **已建立**是將裝置新增至裝置表的日期和時間。
  - **上次修改**是上次修改裝置資訊的日期和時間。
  - **上次看到**是裝置上次記錄為活動的日期和時間。
  - **位址資訊**列出了裝置的 MAC 和/或 IP 位址。如果裝置有多個網路介面，則每個網路介面可以有不同的 MAC 和/或 IP 位址。
  - **硬體**包含有關裝置硬體特性的資訊。
  - **軟體**包含有關裝置軟體的資訊。
  - **Endpoint Agent** 包含有關 Endpoint Agent 元件的資訊。如果裝置上安裝了 Endpoint Agent 元件，則會顯示此部分。
  - **EPP 應用程式**包含在 Endpoint Agent 元件角色中使用的應用程式的資訊。

- **路由器**是標記裝置為路由裝置的屬性。

  如果應用程式無法自動確定路由裝置屬性，則必須手動設定該屬性。該屬性允許應用程式使用附加演算法來偵測透過路由器相互互動的裝置。

- **公開金鑰**是用於在建立 SSH 連線之前對裝置進行身分驗證以及作為安全稽核工作的一部分對裝置進行掃描的公開金鑰。

- **附加資訊**包含應用程式使用者指定的有關裝置的附加資訊（例如，裝置物理位置的描述）。

- **自訂欄位**是一組有關裝置的非標準資訊，由應用程式的使用者指定（例如，裝置的類別和防護等級）。一台裝置最多可以指定 16 個自訂欄位。

- **動態欄位**是使用裝置資訊偵測方法在流量中偵測到的一組擴展裝置資訊。如果應用程式偵測到擴充資訊，則會顯示一個欄位。

- **位址**索引標籤：

  - **DHCP 伺服器**是 DHCP 伺服器屬性。

    如果裝置具有 DHCP 伺服器屬性，則此欄位顯示**是**。

  - **DHCP 中繼**是 DHCP 中繼屬性。

    如果裝置具有 DHCP 中繼屬性，則此欄位顯示**是**。

  - **網路介面 <number>**包含有關裝置網路介面的資訊。

- **拓撲設定**索引標籤包含有關裝置最後一次活動輪詢的資訊，以及有關裝置與其他節點的連結的資訊。

- **裝置**索引標籤包含有關裝置的 BIOS 程式和 CPU、可用 RAM 和可用本機磁碟空間的數量以及正在使用的 USB 裝置和光碟機的資訊。如果使用硬體監控功能取得資訊，則會顯示資訊。

- **組態**索引標籤包含有關所取得的裝置組態的資訊。如果資訊是由組態監控工作取得的，則會顯示該資訊。

自動新增和更新裝置

應用程式可以自動將裝置新增至表格並更新裝置資訊。若要在 Kaspersky Anti Targeted Attack Platform 中啟用裝置自動新增和更新，您必須啟用和設定裝置活動偵測 (AM) 技術。如果啟用該技術，應用程式將使用從網路流量獲得的資料以及與 Endpoint Agent 元件的整合來新增和更新裝置資訊。

新增裝置時，應用程式使用下列範本設定預設裝置名稱：**裝置 <內部設備計數器值>**。裝置名稱中的這個內部計數器值可能與**裝置 ID**欄中顯示的裝置 ID 不符。

該應用程式可以根據裝置的 MAC 位址自動更新網路裝置的供應商資訊。為了透過 MAC 位址識別供應商，應用程式會在電氣電子工程師協會 (IEEE) 的開放資料庫中註冊的位址範圍內尋找裝置的 MAC 位址。如果透過 MAC 位址識別網路裝置的供應商，則應用程式會保留 IEEE 資料庫中的名稱。

安裝應用程式後，將使用 IEEE 資料庫的副本，其中包含有關應用程式目前版本發佈時的 MAC 位址和供應商的資訊。您可以透過安裝更新來保持 IEEE 資料庫的本機副本最新。

手動新增裝置

本節提供有關如何手動新增裝置的說明。您可以手動將新裝置新增至裝置表中。您必須指定要新增的裝置的 MAC 和/或 IP 位址。

> 新增的裝置的 MAC 位址和 IP 位址在這些位址所屬的位址空間內必須是唯一的。如果應用程式中新增了額外的位址空間，則可以將具有相同位址的裝置新增至不同的位址空間。

只有具有**資深安全員**角色的使用者才能手動新增裝置。

新增裝置後，您可以新增該裝置的處理程序監控設定。

在管理裝置表時新增裝置

若要在管理裝置表時新增裝置：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 在裝置表中的“**裝置**”索引標籤上，選擇要檢視資訊的裝置。

   這將開啟一個視窗，其中包含有關裝置的資訊。
3. 點擊“**新增裝置**”。
4. 在“**設定**”索引標籤的詳細資料區域中，在裝置資訊欄位中指定值。
5. 在“**位址資訊**”索引標籤的詳細資料區域中：

   a. 在“**DHCP 伺服器**”下拉清單中，如果裝置是 DHCP 伺服器，請選擇“**是**”。

   b. 在“**DHCP 中繼**”下拉清單中，如果裝置是 DHCP 中繼，請選擇“**是**”。

   在學習模式下，對於作為 DHCP 伺服器和 DHCP 中繼的裝置，這些屬性是自動指派的。您可以停用屬性的自動更新（請參閱這些說明的第 6 步）。

   在監控模式下，只有具有“**資深安全員**”角色的使用者可以編輯屬性。

   c. 在“**位址空間**”下拉清單中，選擇您希望裝置所屬的位址空間。

   d. 在“**MAC 位址**”欄位中，輸入裝置的 MAC 位址。

   e. 在“**IP 位址**”下拉清單中選擇 IP 位址分配類型（靜態或動態），並輸入裝置的 IP 位址。

   您可以為裝置的同一個網路介面指定多個 IP 位址。若要建立 IP 位址清單，請執行下列操作之一：

   - 如果要新增 IP 位址，請點擊“**新增 IP 位址**”。
   - 如果要刪除 IP 位址，請點擊 IP 位址欄位右側的🗑圖示。

如果裝置有多個網路介面，請建立網路介面清單：

- 若要新增網路介面，請點擊最後一個網路介面設定下方的“**新增介面**”。
- 若要刪除網路介面，請點擊網路介面名稱右側的×圖示（如果裝置有兩個或更多網路介面）。
- 如果您想要為網路介面輸入不同的名稱，請點擊目前名稱右側的✎圖示，然後在顯示的欄位中輸入新名稱。

6. 在“**設定**”和“**位址資訊**”索引標籤的詳細資料區域中，啟用或停用對裝置資訊某些元素的自動修改。為此，請點擊🔒或🔓圖示。

> 如果停用裝置 IP 位址的自動更新，則 IP 位址類型（靜態或動態）和位址空間資訊的自動更新也會被停用。

7. 在“**自訂欄位**”索引標籤的詳細資訊區域中，建立自訂欄位清單。
8. 點擊“**儲存**”。

   如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以•圖示標示。

裝置表中將出現一個“*已授權*”狀態的新裝置。

在管理拓撲圖時新增裝置

您可以在管理拓樸圖的同時將新裝置新增至裝置表。

若要在管理拓樸圖的同時將新裝置新增至裝置表：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
2. 前往“**拓撲圖**”索引標籤。
3. 點擊“**新增裝置**”。
4. 在“**設定**”索引標籤的詳細資料區域中，在裝置資訊欄位中指定值。
5. 在“**位址資訊**”索引標籤的詳細資料區域中：

   a. 在“**DHCP 伺服器**”下拉清單中，如果裝置是 DHCP 伺服器，請選擇“**是**”。

   b. 在“**DHCP 中繼**”下拉清單中，如果裝置是 DHCP 中繼，請選擇“**是**”。

   在學習模式下，對於作為 DHCP 伺服器和 DHCP 中繼的裝置，這些屬性是自動指派的。您可以停用屬性的自動更新（請參閱這些說明的第 6 步）。

   在監控模式下，只有具有“**資深安全員**”角色的使用者可以編輯屬性。

   c. 在“**位址空間**”下拉清單中，選擇您希望裝置所屬的位址空間。

   d. 在“**MAC 位址**”欄位中，輸入裝置的 MAC 位址。

   e. 在“**IP 位址**”下拉清單中選擇 IP 位址分配類型（靜態或動態），並輸入裝置的 IP 位址。

您可以為裝置的同一個網路介面指定多個 IP 位址。若要建立 IP 位址清單，請執行下列操作之一：

- 如果要新增 IP 位址，請點擊“**新增 IP 位址**”。
- 如果要刪除 IP 位址，請點擊 IP 位址欄位右側的圖示。

如果裝置有多個網路介面，請建立網路介面清單：

- 若要新增網路介面，請點擊最後一個網路介面設定下方的“**新增介面**”。
- 若要刪除網路介面，請點擊網路介面名稱右側的圖示（如果裝置有兩個或更多網路介面）。
- 如果您想要為網路介面輸入不同的名稱，請點擊目前名稱右側的圖示，然後在顯示的欄位中輸入新名稱。

6. 在“**設定**”和“**位址資訊**”索引標籤的詳細資料區域中，啟用或停用對裝置資訊某些元素的自動修改。為此，請點擊或圖示。

   如果停用裝置 IP 位址的自動更新，則 IP 位址類型（靜態或動態）和位址空間資訊的自動更新也會被停用。

7. 在“**自訂欄位**”索引標籤的詳細資訊區域中，建立自訂欄位清單。
8. 點擊“**儲存**”。

   如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以圖示標示。

裝置表中將出現一個“*已授權*”狀態的新裝置。

根據網路互動圖上的未知裝置節點新增裝置

在管理網路互動圖時，您可以根據代表應用程式無法辨識之裝置的節點，將新裝置新增至裝置表。

若要將無法辨識的裝置節點新增至裝置表中：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
2. 在**網路互動圖**索引標籤上，選擇代表應用程式無法辨識的裝置的節點。

   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊**新增至裝置表**。
4. 在“**設定**”索引標籤的詳細資料區域中，在裝置資訊欄位中指定值。
5. 在“**位址資訊**”索引標籤的詳細資料區域中：

   a. 在“**DHCP 伺服器**”下拉清單中，如果裝置是 DHCP 伺服器，請選擇“**是**”。

   b. 在“**DHCP 中繼**”下拉清單中，如果裝置是 DHCP 中繼，請選擇“**是**”。

   在學習模式下，對於作為 DHCP 伺服器和 DHCP 中繼的裝置，這些屬性是自動指派的。您可以停用屬性的自動更新（請參閱這些說明的第 6 步）。

在監控模式下，只有具有“**資深安全員**”角色的使用者可以編輯屬性。

c. 在“**位址空間**”下拉清單中，選擇您希望裝置所屬的位址空間。

d. **IP 位址**和**MAC 位址**欄位會自動填寫；我們不建議變更這些設定。

您可以為裝置的同一個網路介面指定多個 IP 位址。若要建立 IP 位址清單，請執行下列操作之一：

- 如果要新增 IP 位址，請點擊“**新增 IP 位址**”。
- 如果要刪除 IP 位址，請點擊 IP 位址欄位右側的圖示。

如果裝置有多個網路介面，請建立網路介面清單：

- 若要新增網路介面，請點擊最後一個網路介面設定下方的“**新增介面**”。
- 若要刪除網路介面，請點擊網路介面名稱右側的圖示（如果裝置有兩個或更多網路介面）。
- 如果您想要為網路介面輸入不同的名稱，請點擊目前名稱右側的圖示，然後在顯示的欄位中輸入新名稱。

6. 在“**設定**”和“**位址資訊**”索引標籤的詳細資料區域中，啟用或停用對裝置資訊某些元素的自動修改。為此，請點擊或圖示。

> 如果停用裝置 IP 位址的自動更新，則 IP 位址類型（靜態或動態）和位址空間資訊的自動更新也會被停用。

7. 在“**自訂欄位**”索引標籤的詳細資訊區域中，建立自訂欄位清單。

8. 點擊“**儲存**”。

如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以圖示標示。

裝置表中將出現一個“*已授權*”狀態的新裝置。網路互動圖上以前代表應用程式無法辨識的裝置的節點，現在代表應用程式已知的裝置。

根據拓樸圖上非管理交換器新增裝置

在管理拓樸圖時，您可以根據代表非管理型交換機的節點將新裝置新增至裝置表中。

若要將非管理型交換機節點新增至裝置表：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。

2. 在“**網路互動圖**”索引標籤上，選擇代表不受管理的交換機的節點。

詳細資訊區域顯示在 Web 介面視窗的右側。

3. 點擊**新增至裝置表**。

4. 在“**設定**”索引標籤的詳細資料區域中，在裝置資訊欄位中指定值。

5. 在“**位址資訊**”索引標籤的詳細資料區域中：

   a. 在“**DHCP 伺服器**”下拉清單中，如果裝置是 DHCP 伺服器，請選擇“**是**”。

   b. 在“**DHCP 中繼**”下拉清單中，如果裝置是 DHCP 中繼，請選擇“**是**”。

      在學習模式下，對於作為 DHCP 伺服器和 DHCP 中繼的裝置，這些屬性是自動指派的。您可以停用屬性的自動更新（請參閱這些說明的第 6 步）。

      在監控模式下，只有具有“**資深安全員**”角色的使用者可以編輯屬性。

   c. 在“**位址空間**”下拉清單中，選擇您希望裝置所屬的位址空間。

   d. 在“**MAC 位址**”欄位中，輸入裝置的 MAC 位址。

   e. 在“**IP 位址**”下拉清單中選擇 IP 位址分配類型（靜態或動態），並輸入裝置的 IP 位址。

      您可以為裝置的同一個網路介面指定多個 IP 位址。若要建立 IP 位址清單，請執行下列操作之一：

      - 如果要新增 IP 位址，請點擊“**新增 IP 位址**”。
      - 如果要刪除 IP 位址，請點擊 IP 位址欄位右側的🗑圖示。

      如果裝置有多個網路介面，請建立網路介面清單：

      - 若要新增網路介面，請點擊最後一個網路介面設定下方的“**新增介面**”。
      - 若要刪除網路介面，請點擊網路介面名稱右側的×圖示（如果裝置有兩個或更多網路介面）。
      - 如果您想要為網路介面輸入不同的名稱，請點擊目前名稱右側的✎圖示，然後在顯示的欄位中輸入新名稱。

6. 在“**設定**”和“**位址資訊**”索引標籤的詳細資料區域中，啟用或停用對裝置資訊某些元素的自動修改。為此，請點擊🔒或🔓圖示。

   > 如果停用裝置 IP 位址的自動更新，則 IP 位址類型（靜態或動態）和位址空間資訊的自動更新也會被停用。

7. 在“**自訂欄位**”索引標籤的詳細資訊區域中，建立自訂欄位清單。

8. 點擊“**儲存**”。

   如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以•圖示標示。

裝置表中將出現一個具有*已授權***狀態的新裝置。**拓撲圖上先前代表非管理型交換機的節點現在代表應用程式已知的裝置。

自動分配裝置狀態

在監控裝置活動時，應用程式可以根據所取得的裝置的 MAC 和/或 IP 位址自動為發現的裝置分配狀態。依目前資產管理模式指定狀態。

在學習模式下，應用程式將*已授權*狀態指派給所有裝置（新裝置以及先前已新增至表中的裝置），且先前已指派*未授權*狀態的裝置除外。

在監控模式下，分配的狀態取決於表現出活動的裝置是否為應用程式已知或不識別的裝置。在此模式下，狀態會根據以下規則指派：

- 如果裝置是新的（在發現時它在裝置表中不存在），則該裝置被分配到*未授權*狀態。
- 如果裝置存在於*已授權*或*未授權*狀態的裝置表中，則其狀態不會改變。
- 如果裝置存在於*已存檔*狀態的裝置表中，則該裝置被指派*未授權*狀態。

預設情況下，如果處於*已授權*狀態的裝置已處於不活動狀態超過 30 天，且在此期間裝置資訊沒有發生變化，則該裝置將自動指派為*已存檔*狀態。您可以停用在手動變更裝置狀態時自動指派*已存檔*狀態的功能（例如，為了防止很少連線到網路的裝置從*已授權*狀態變更為*未授權*）。

當使用**Cisco 交換機**類型的連線器時，裝置的網路存取可能會在這些裝置變為*未授權*狀態後被自動限制。您需要考慮此類連線器的指定設定，以防止因狀態改變而阻止必要的裝置。

根據條件自動對裝置進行分組

本節包含如何根據條件自動分組裝置的說明。您可以根據下列條件之一自動對裝置群組樹中的裝置進行分組：

- 屬於應用程式已知子網路的 IP 位址
- 裝置類別
- 裝置供應商

只有具有**資深安全員**角色的使用者才能自動分組裝置。

根據條件自動將裝置分組，從群組樹的根開始

若要根據條件自動將裝置分組，請從群組樹的根開始：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 在**網路地圖**區域的**網路互動圖**索引標籤上，點擊網路互動圖顯示區域左側工具列中的下列按鈕之一，以選擇分組條件：
   - 按子網路將裝置分組。
   - 按類別對裝置進行分組。
   - 依供應商將裝置分組。

   這將開啟一個提示視窗，您可以在其中選擇一個分組選項。
3. 若要基於位址空間按類別和供應商將裝置分組，請在提示視窗中選擇**考慮位址空間**核取方塊。

4. 根據您要執行的操作，點擊下列按鈕之一：

   - 若要按子網路將裝置分組，請點擊**分組**。
   - 若要根據裝置群組樹中所有群組中的位址空間按類別和供應商將裝置分組，請點擊**帶子群組**。
   - 若要僅根據裝置群組樹層次結構頂層的位址空間按類別和供應商將裝置分組，請點擊**僅限選定**。

   該應用程式識別符合所選分組條件的裝置，為這些裝置建立群組，並將裝置排列到這些群組中。

自動將裝置分組到選定的裝置群組中

若要自動將裝置分組到選定的裝置群組：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 在**網路地圖**部分，**網路互動圖**索引標籤上，選擇您想要自動分組裝置的群組。
3. 右鍵點擊以開啟上下文功能表。
4. 在上下文功能表中，選擇以下命令之一：

   - **按子網路分組**。
   - **按類別分組**。
   - **按供應商分組**。

   這將開啟一個提示視窗，您可以在其中選擇一個分組選項。

5. 若要基於位址空間按類別和供應商將裝置分組，請在提示視窗中選擇**考慮位址空間**核取方塊。
6. 在提示視窗中，根據您要執行的操作，點擊以下按鈕之一：

   - 若要按子網路將裝置分組，請點擊**分組**。
   - 如果要按類別或供應商將選定群組的所有子群組中的裝置進行分組，請點擊**帶有子群組**。
   - 如果您想要按類別或供應商僅對選定群組中的裝置進行分組，請點擊**僅選定**。

   該應用程式識別符合所選分組條件的裝置，為這些裝置建立群組並將裝置排列到這些群組中（其他群組中的裝置不受影響）。

手動將裝置分組

本節包含有關如何在群組樹中手動排列裝置的說明。只有具有高級安全官角色的使用者才能在群組樹中排列裝置。

將裝置新增至群組

若要在管理表時將單個裝置新增至群組：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 在**資產**部分的**裝置**索引標籤上，或在**網路地圖**部分選擇裝置。

   在**網路地圖**部分，您可以在網路互動圖及拓樸圖上選擇要新增至群組的裝置。

   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊**編輯**。
4. 在詳細資訊區域中，前往**設定**索引標籤。
5. 點擊**群組**欄位右側的 圖示。

   出現**在樹中選擇群組**視窗。
6. 在裝置群組樹中，選擇相關群組。

   如果相關的群組不在樹中，您可以在目前顯示的**在樹中選擇群組**視窗中將其新增。
7. 點擊**選擇**。

   所選組的路徑顯示在**群組**欄位。
8. 點擊詳細資料區中的**儲存**。

   如果裝置設定不包含所有必要的資訊或某些指定的設定無效，則此按鈕不可用。包含需要修正值之設定的索引標籤會以 圖示標示。

將多個裝置新增至一個群組

您可以在管理裝置表的同時將多個裝置新增至一個群組。

另外，在管理網路互動圖時，您可以將網路互動圖上的多個已知裝置新增至一個群組。您可以單獨選擇元件伺服器，也可以選擇包含所需裝置的折疊群組的一部分。當您選擇一個折疊的群組時，所有嵌套層級的子群組中的所有裝置也會被選取。

若要在管理表時將多個裝置新增至一個群組：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇**資產**區段。
3. 在**裝置**索引標籤上，選擇要新增至群組的裝置。
4. 右鍵點擊以開啟上下文功能表。
5. 在右鍵功能表中，選擇**群組管理** → **移至群組**。

   出現**在樹中選擇群組**視窗。

6. 在裝置群組樹中，選擇相關群組。
   如果相關的群組不在樹中，您可以在目前顯示的**在樹中選擇群組**視窗中將其新增。

7. 點擊**選擇**。
   所選群組的路徑顯示在**群組**欄。

若要在管理網路互動圖時將多個裝置新增至一個群組：

1. 使用 Web 介面以安全官或高階安全官角色連線到 Central Node。

2. 在**網路圖**區段的**網路互動圖**索引標籤上，選擇相關的元件伺服器和/或折疊群組。
   若要選擇多個元件伺服器和/或群組，請執行下列操作之一：

   - 按住**SHIFT**鍵，然後使用滑鼠選擇一個包含要選擇物件的矩形區域。

   - 按住**CTRL**鍵並點擊要選擇的每個物件。

3. 右鍵點擊以開啟上下文功能表。

4. 在右鍵功能表中，選擇**移至群組**。
   出現**在樹中選擇群組**視窗。

5. 在裝置群組樹中，選擇相關群組。
   如果相關的群組不在樹中，您可以在目前顯示的**在樹中選擇群組**視窗中將其新增。

6. 點擊**選擇**。
   選定的元件伺服器顯示在選定的群組內。

從群組中刪除裝置

若要在管理表時從群組中刪除單個裝置：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。

2. 在**資產**部分的**裝置**索引標籤上，或在**網路地圖**部分選擇裝置。
   在**網路地圖**區段中，您可以在網路互動圖和拓樸圖上選擇要從群組中刪除的裝置。
   詳細資訊區域顯示在 Web 介面視窗的右側。

3. 點擊**編輯**。

4. 在詳細資訊區域中，前往**設定**索引標籤。

5. 在**群組**欄位中，透過點擊欄位中的×圖示刪除群組路徑（如果定義了群組，則會顯示該圖示）。

6. 點擊“**儲存**”。
   如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以•圖示標示。

儲存裝置變更後，其**群組**值將被清除，並且裝置將被指派到群組樹的根層級。

從群組中刪除多個裝置

使用裝置表時，您可以從群組中刪除多個裝置。選擇從群組中刪除的裝置可以屬於同一組或不同的群組。

此外，在管理網路互動圖時，您可以從網路互動圖上的群組中排除多個已知裝置。您可以單獨選擇元件伺服器，也可以選擇包含所需裝置的折疊群組的一部分。當您選擇一個折疊的群組時，所有嵌套層級的子群組中的所有裝置也會被選取。

若要在管理表時從群組中刪除多個裝置：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇**資產**區段。
3. 在**裝置**索引標籤上，選擇要從群組中刪除的裝置。
4. 右鍵點擊以開啟上下文功能表。
5. 在右鍵功能表中，選擇**群組管理** → **從群組中刪除**。
   這將開啟一個確認提示視窗。
6. 在提示視窗中確認從群組中刪除裝置。

對於所有選定的裝置，**群組**值會被清除，並且這些裝置被指派到群組樹的根層級。

若要在管理網路互動圖時從群組中刪除多個裝置：

1. 使用 Web 介面以安全官或高階安全官角色連線到 Central Node。
2. 在**網路地圖**區段的**網路互動圖**索引標籤上，選擇展開群組和/或折疊群組中的元件伺服器。
   若要選擇多個元件伺服器和/或群組，請執行下列操作之一：
   - 按住**SHIFT**鍵，然後使用滑鼠選擇一個包含要選擇物件的矩形區域。
   - 按住**CTRL**鍵並點擊要選擇的每個物件。
3. 右鍵點擊以開啟上下文功能表。
4. 在右鍵功能表中，選擇**從群組中刪除**。
   這將開啟一個確認提示視窗。
5. 在提示視窗中確認從群組中刪除裝置。

對於所有選定的裝置，**群組**值會被清除，並且這些裝置會顯示在群組之外。

將帶有元件和群組的伺服器移至網路互動圖上的其他群組

您可以透過拖放網路互動圖上的物件來重新排列裝置群組樹中的元件伺服器和群組。裝置群組樹中移動的元件伺服器和群組的位置的變化方式與向群組中新增裝置或從群組中刪除裝置時的變更方式相同。

只有具有高級安全官角色的使用者才能將元件伺服器和群組移至其他群組。

若要將元件伺服器和/或群組移至其他群組：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 在**網路圖**區段的**網路互動圖**索引標籤上，選擇相關的元件伺服器和/或折疊群組。

   若要選擇多個元件伺服器和/或群組，請執行下列操作之一：

   - 按住**SHIFT**鍵，然後使用滑鼠選擇一個包含要選擇物件的矩形區域。
   - 按住 **CTRL** 鍵並點擊要選擇的每個物件。
3. 指向選定的物件之一（一個群組或一個元件伺服器）。
4. 按住 **CTRL** 鍵並將選定的物件拖曳到所需的群組中（如果要將選定的物件移至群組樹的最上層，則拖曳到群組外的任意空間）。

   這將開啟一個確認提示視窗。
5. 在提示視窗中確認所選物件的移動。

裝置群組樹

裝置組樹的目的是根據裝置的功能、位置或任何其他任意屬性來排列裝置。可以手動或自動將裝置分組（根據其所屬子網路的 IP 位址、類別或供應商）。

如果某個裝置不包含在任何群組中，則該裝置屬於群組樹的頂層。自動新增至表中的裝置預設不包含在任何群組中。

檢視裝置表時，您可以看到裝置屬於哪些群組。群組的路徑會顯示在**群組**欄中。裝置群組也顯示在網路互動圖上。但是，如果這些群組中的裝置不滿足在網路互動圖上過濾物件的設定，則可能不會顯示。

手動編輯裝置群組樹

您可以在使用裝置表、網路互動圖和拓樸圖時建立裝置群組樹。樹建立功能位於**建立群組樹**或**在樹中選擇群組**視窗。

只有具有高級安全官角色的使用者才能建立裝置群組樹。

若要使用裝置樹組編輯功能：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 在**資產**部分的**裝置**索引標籤上，或在**網路地圖**部分中，執行下列其中一項操作：

   - 透過點擊**設定群組**開啟**建立群組樹**視窗。

     資產部分中的**設定群組**按鈕位於工具列的**群組管理**下拉式清單中。

     網路地圖部分中的**設定群組**按鈕僅在**網路互動圖**索引標籤上可用。
   - 將裝置新增至群組時，開啟**在樹中選擇群組**視窗。您也可以在依**群組**欄篩選裝置表時開啟此視窗。

在**建立群組樹**或**在樹中選擇群組**視窗中對裝置群組樹所做的任何變更都會立即套用。

本節包含如何編輯裝置群組樹的說明。

新增群組

若要將群組新增至裝置群組樹：

1. 在**建立群組樹**或**在樹中選擇群組**視窗中，透過以下方式之一新增群組：
   - 如果樹為空，而您想要新增第一個群組，請點擊**新增**或按 **INSERT** 或 **ENTER**。
   - 若要新增與現有群組處於相同層次結構的群組，請選取該群組並按 **ENTER**。
   - 如果要將子群組新增至現有群組，請選擇該群組並點擊**新增**或按 **INSERT**。
2. 在文字方塊中輸入群組的名稱。
   您可以使用字母、數字、空格字元以及以下特殊字元：**! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /**。
   組名稱必須符合以下要求：
   - 以空格以外的任意字元開始和結束。
   - 最多包含 255 個字元。
   - 與同一父群組下的另一個組名名稱不同（不區分大小寫）。
3. 點擊文字方塊右側的✓圖示。

重新命名群組

若要將群組重新命名為裝置群組樹：

1. 在**建立群組樹**或**在樹中選擇群組**視窗，選擇要重新命名的群組。
2. 點擊**重新命名**或按**F2**。
3. 在文字方塊中輸入群組的新名稱。
   您可以使用字母、數字、空格字元以及以下特殊字元：**! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /**。
   組名稱必須符合以下要求：
   - 以空格以外的任意字元開始和結束。
   - 最多包含 255 個字元。
   - 與同一父群組下的另一個組名名稱不同（不區分大小寫）。
4. 點擊文字方塊右側的✓圖示。

新的群組名稱將顯示在新增至此群組或其子群組的裝置的裝置資訊中。

刪除群組

刪除群組不會刪除新增至該群組的裝置。已刪除群組中的裝置將移至裝置樹中與已刪除群組相同的層級。

若要從裝置群組樹中刪除群組：

1. 在**建立群組樹**或**在樹中選擇群組**視窗中，選擇要刪除的群組。
2. 點擊🗑圖示。
   這將開啟一個提示視窗，您可以在其中選擇刪除選項。
3. 在提示視窗中，根據您要執行的操作，點擊以下按鈕之一：
   - 如果只想刪除選定群組並保留其子群組，請點擊**僅選定**。
   - 如果要刪除選定組及其所有子群組，請點擊**帶有子群組**。

   這將開啟一個確認提示視窗。
4. 在提示視窗中，點擊**確定**。

移動群組

要在裝置組樹中移動裝置：

1. 在**建立群組樹**或**在樹中選擇群組**視窗，選擇要移動的群組。
2. 使用箭頭圖示或對應的快速鍵（**ALT+↓**、**ALT+↑**、**ALT+←**、**ALT+→**）將群組相對於樹的其他元素進行移動。如果無法執行操作，則該操作的圖示不可用。

搜尋群組

您可以使用**建立群組樹**或**在樹中選擇群組**視窗中的**搜尋群組**欄位，在裝置群組樹中找到相關群組。裝置群組樹顯示符合搜尋條件的群組。對於子群組，也會顯示其父群組。

更新樹

當您管理樹時，可以在 Central Node 上修改裝置群組樹的組成（例如，由連線到 Central Node 的另一個使用者）。

您可以透過點擊🔄圖示，在**建立群組樹**或**在樹中選擇群組**視窗中手動更新樹。

新增和刪除裝置標籤

本節提供有關如何新增或刪除裝置標籤的說明。您新增到裝置的標籤可以是任意的。

*裝置標籤*包含文字描述，可讓您快速尋找或篩選表中的裝置。您可以將任何您認為方便的文字描述儲存為標籤。一個裝置最多可以有 16 個標籤。每個裝置可以有自己的一組標籤。

裝置標籤清單顯示在裝置表的**標籤**欄位中。單元格中的標籤按字母順序排序。

只有具有高級安全官角色的使用者才能新增或刪除裝置標籤。

為單個裝置新增標籤

若要為一個裝置新增標籤：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 在**資產**部分的**裝置**索引標籤上，或在**網路地圖**部分選擇裝置。
   在**網路地圖**區段中，您可以選擇裝置以在網路互動圖和拓樸圖上新增標籤。
   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊**編輯**。
   在詳細資訊區域中，前往**設定**索引標籤。
4. 在**標籤**欄位中，輸入您想要用作標籤的文字描述。若要分隔標籤，可以使用**ENTER**鍵或 **;** 字元。
   您可以使用大寫和小寫字母、數字、空格，以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   標籤名稱必須符合以下要求：
   - 必須以任何允許的字元（空格除外）開頭及結尾。
   - 在裝置標籤清單中必須是唯一的（不區分大小寫）。
   - 包含 1 至255 個字元。
5. 如有必要，請點擊**複製標籤**以複製標籤清單。如果標籤清單不為空，則會顯示連結。
6. 點擊“**儲存**”。
   如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以 . 圖示標示。

為多個裝置新增標籤

您可以在管理裝置表時為多個裝置新增標籤。

另外，在管理網路互動圖和拓撲圖時，您可以為應用程式已知且在圖上以節點表示的裝置新增標籤。您可以單獨選擇節點，也可以選擇包含所需裝置的折疊組的一部分。當您選擇一個折疊的群組時，所有嵌套層級的子群組中的所有裝置也會被選取。

若要在管理表格時向多個裝置新增標籤：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇**資產**區段。
3. 在**裝置**索引標籤上，選擇要新增標籤的裝置。
4. 右鍵點擊其中一個選定的裝置以開啟上下文功能表。
5. 在右鍵功能表中，選擇**新增標籤**。
   這將開啟**新增標籤**視窗。
6. 在**標籤**欄位中，輸入您想要用作標籤的文字描述。若要分隔標籤，可以使用**ENTER**鍵或 **;** 字元。
   您可以使用大寫和小寫字母、數字、空格，以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   標籤名稱必須符合以下要求：
   - 必須以任何允許的字元（空格除外）開頭及結尾。
   - 在裝置標籤清單中必須是唯一的（不區分大小寫）。
   - 包含 1 至255 個字元。
7. 如有必要，請點擊**複製標籤**以複製標籤清單。如果標籤清單不為空，則會顯示連結。
8. 如果您要清除選定裝置的目前標籤清單並僅為這些裝置提供新標籤，請勾選**刪除現有**核取方塊。

   > 如果清除**刪除現有**核取方塊，則目前標籤清單將保留在每個裝置上。新標籤將附加到所有選定裝置的標籤清單中。對於某些選定的裝置，這可能會導致標籤總數超出限制（每個裝置最多 16 個標籤）。應用程式在新增標籤之前會檢查限制。

9. 點擊**確定**。
   如果輸入的標籤名稱不符合要求，或標籤清單為空且已清除**刪除現有**核取方塊，則該按鈕不可用。

若要在管理地圖時為多個裝置新增標籤：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇**網路地圖**部分。
3. 在**網路互動圖**或**拓樸圖**索引標籤上，選擇已知裝置和/或折疊群組的相關節點。
   若要選擇多個節點和/或群組，請執行下列操作之一：
   - 按住 **SHIFT** 鍵，然後使用滑鼠選擇一個包含要選擇的物件的矩形區域。
   - 按住 **CTRL** 鍵並點擊要選擇的每個物件。
4. 右鍵點擊其中一個選定的物件以開啟上下文功能表。
5. 在右鍵功能表中，選擇**新增標籤**。
   這將開啟**新增標籤**視窗。

6. 在**標籤**欄位中，輸入您想要用作標籤的文字描述。若要分隔標籤，可以使用**ENTER**鍵或 **;** 字元。

   您可以使用大寫和小寫字母、數字、空格，以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。

   標籤名稱必須符合以下要求：

   - 必須以任何允許的字元（空格除外）開頭及結尾。
   - 在裝置標籤清單中必須是唯一的（不區分大小寫）。
   - 包含 1 至255 個字元。

7. 如有必要，請點擊**複製標籤**以複製標籤清單。如果標籤清單不為空，則會顯示連結。

8. 如果您要清除選定裝置的目前標籤清單並僅為這些裝置提供新標籤，請勾選**刪除現有**核取方塊。

   > 如果清除**刪除現有**核取方塊，則目前標籤清單將保留在每個裝置上。新標籤將附加到所有選定裝置的標籤清單中。對於某些選定的裝置，這可能會導致標籤總數超出限制（每個裝置最多 16 個標籤）。應用程式在新增標籤之前會檢查限制。

9. 點擊**確定**。

   如果輸入的標籤名稱不符合要求，或標籤清單為空且已清除**刪除現有**核取方塊，則該按鈕不可用。

從單個裝置上刪除標籤

若要從一個裝置中刪除標籤：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。

2. 在**資產**部分的**裝置**索引標籤上，或在**網路地圖**部分選擇裝置。

   在**網路地圖**區段中，您可以在網路互動圖以及拓樸圖上選擇要刪除標籤的裝置。

   詳細資訊區域顯示在 Web 介面視窗的右側。

3. 點擊**編輯**。

   在詳細資訊區域中，前往**設定**索引標籤。

4. 在**標籤**欄位中，刪除不再需要的標籤：

   - 如果要刪除個別標籤，請點擊標籤名稱旁邊的 × 圖示。
   - 如果要刪除所有標籤，請使用**標籤**欄位右側的 × 圖示。

5. 點擊“**儲存**”。

   如果未在裝置設定中指定所有必要資訊，或設定了無效值，則此按鈕無法使用。包含需要修正值之設定的索引標籤會以 • 圖示標示。

清除多個裝置的標籤清單

您可以在管理裝置表時清除多個裝置的標籤清單。

另外，在管理網路互動圖和拓撲圖時，您可以清除應用程式已知且在圖上以節點表示之裝置的標籤清單。您可以單獨選擇節點，也可以選擇包含所需裝置的折疊組的一部分。當您選擇一個折疊的群組時，所有嵌套層級的子群組中的所有裝置也會被選取。

若要在管理表格時清除多個裝置的標籤清單：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇**資產**區段。
3. 在**裝置**索引標籤上，選擇要清除其標籤清單的裝置。
4. 右鍵點擊其中一個選定的裝置以開啟上下文功能表。
5. 在右鍵功能表中，選擇**新增標籤**。
   這將開啟**新增標籤**視窗。
6. 選取**刪除現有**核取方塊。
7. 點擊**確定**。

若要在管理地圖時清除多個裝置的標籤清單：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇**網路地圖**部分。
3. 在**網路互動圖**或**拓樸圖**索引標籤上，選擇已知裝置和/或折疊群組的相關節點。
   若要選擇多個節點和/或群組，請執行下列操作之一：
   - 按住 **SHIFT** 鍵，然後使用滑鼠選擇一個包含要選擇的物件的矩形區域。
   - 按住 **CTRL** 鍵並點擊要選擇的每個物件。
4. 右鍵點擊其中一個選定的物件以開啟上下文功能表。
5. 在右鍵功能表中，選擇**新增標籤**。
   這將開啟**新增標籤**視窗。
6. 選取**刪除現有**核取方塊。
7. 點擊**確定**。

回應

如果使用 KEDR 功能單元，可以透過建立工作將威脅回應操作套用至裝置。下表列出了應用程式中可用的回應操作以及建立工作所需的設定。

若要建立套用回應操作的工作：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 前往**裝置**索引標籤。
3. 勾選您要指派該工作的裝置的名稱左側的核取方塊。

   如果列出的裝置太多，您可以套用篩選器來顯示您需要的裝置。例如，您可以找到具有特定標籤的裝置，或屬於特定群組的裝置。
4. 在**回應**功能表中，選擇工作類型。

   這將開啟工作建立視窗。
5. 根據工作類型指定工作設定。

   下表列出了各項設定。
6. 點擊**儲存**。

工作已建立。工作建立後自動執行。

回應操作說明及建立工作的設定

回應操作	工作設定
終止處理程序 終止可能威脅裝置或企業區域網路安全的處理程序。	• **檔案路徑**是您要終止的處理程序的可執行檔的路徑，或您要刪除的檔案的路徑，具體取決於工作類型。 您也可以指定此檔案的備用資料串流路徑。在這種情況下，根據工作類型，將終止指定資料流的處理程序或刪除相關檔案。此檔案的其他資料流將保持不變。 • **MD5/SHA256**是要終止的處理程序的可執行檔或要刪除的檔案的 MD5 或 SHA256 雜湊值。該欄位是可選的。 • **敘述**是工作描述。該欄位是可選的。

回應操作	工作設定
刪除檔案 刪除指定裝置上的檔案。 此操作無法撤銷。	
獲取檔案 將裝置中的檔案複製到 Kaspersky Anti Targeted Attack Platform 的儲存中，並能夠下載檔案到本機電腦。 此工作只能分配給一台裝置。	• **檔案路徑**是您想要接收的檔案的路徑。 如果要求的檔案已連結到其他 NTFS 資料流，則執行該工作將產生請求的檔案連結到的 NTFS 資料流的所有檔案。 您也可以指定此檔案的備用資料串流的路徑。在這種情況下，您僅接收指定流的檔案。 • **MD5/SHA256**是要接收的檔案的 MD5 或 SHA256 雜湊。該欄位是可選的。 • **傳送以進行掃描**使用 Kaspersky Anti Targeted Attack Platform 掃描檔案。 • **敘述**是工作描述。該欄位是可選的。
取得取證 從 Kaspersky Anti Targeted Attack Platform 儲存中的指定裝置取得檔案、處理程序或自動執行點清單，並且能夠將下載資料到本機電腦。	• **資訊類型**是所收集資料的類型。有以下類型可用： • 處理程序清單獲取工作執行時主機上執行的處理程序清單。 • 自動執行點清單獲取自動執行點清單。 自動執行點清單包括有關新增到啟動資料夾或在登錄檔的 Run 鍵中註冊的應用程式的資訊，以及在帶有 Endpoint Agent 元件的主機啟動時以及使用者登錄指定主機上的作業系統時自動執行的應用程式的資訊。 **支援的自動執行點清單** Kaspersky Endpoint Agent 支援收集以下自動執行點的資料： • Logon。 • Run。 • Explorer。 • Shell。 • Office。 • Internet Explorer®。 • Tasks。 • Services。 • Drivers。 • Telephony。 • Cryptography。 • Debuggers。 • COM。 • Session Manager。 • Network。 • LSA。 • Applications。 • Codecs。 • Shellex。 • WMI。 • Unspecified。

回應操作	工作設定
	Kaspersky Endpoint Security 支援收集上述自動執行點以及以下內容： • BootLog • Browsers • DriverLog • EfiLoader • GroupPolicy • Logon • OsLoader • OsUpdate • Printer • Process • Scheduler • **檔案清單**獲取工作執行時儲存在所選資料夾或所有主機資料夾中的檔案清單。 • 如果您選擇**檔案清單**，則以下幾種資料來源類型可用： • 所有本機磁碟包含在工作執行時儲存在本機磁碟上所有資料夾中的檔案。 • **目錄**包括儲存在指定資料夾及其子資料夾中的檔案。 • 如果您選擇**目錄**，則以下設定可用： • **啟動目錄**是檔案搜尋的起始資料夾路徑。 您可以使用系統或使用者環境變數。 使用使用者定義的環境變數時，檔案清單包含有關設定了指定環境變數的所有使用者的資料夾中的檔案的資訊。如果使用者定義的環境變數覆蓋系統環境變量，則檔案清單將根據系統環境變數的值包含資料夾中檔案的資訊。 • **遮罩**是要包含在檔案清單中的檔案的遮罩。 • **備用資料流**啟用在檔案清單中記錄有關備用資料流的資訊。 如果要求的檔案已連結到其他 NTFS 資料流，則執行該工作將產生請求的檔案連結到的 NTFS 資料流的所有檔案。 • **最大嵌套級別**是應用程式在其中搜尋檔案的資料夾的最大嵌套層級。 • **排除項目**是要禁止在其中搜尋檔案資訊的資料夾的路徑。 • **敘述** — 工作描述。該欄位是可選的。
獲取登錄機碼 取得 Kaspersky Anti Targeted Attack Platform 儲存中指定登錄機碼及其值的清單，並可將資料下載到本機電腦。	• **登錄機碼** — 您想要取得的登錄機碼。 您可以採用以下格式之一輸入登錄機碼： • 相對於根金鑰。 例如，\REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。 • 相對於根金鑰的完整名稱。 例如，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。 • 相對於用縮寫代替根金鑰的完整名稱。 例如，HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。 如果要從 HKEY_CURRENT_USER 取得資料，您必須指定 HKEY_USERS 和使用者的 SID：HKEY_USERS\<SID of the user>。 • **敘述**是工作描述。該欄位是可選的。

回應操作	工作設定

啟動 YARA 掃描
使用 YARA 規則掃描處理程序、自動執行點和檔案。
	• **選擇規則**是規則的名稱。您可以輸入規則名稱或規則名稱中的字元序列，然後在清單中選擇規則。
	您可以新增多個規則。
	• **掃描**是掃描範圍。以下掃描範圍可用：
	  • **記憶體**掃描在執行工作時正在執行的處理程序。
	  應用程式不會掃描低優先順序的處理程序。
	  • **自動執行點**掃描從**進行取證**工作獲取的自動執行點。
	  若要掃描自動執行點，您必須指定先前為其執行過**進行取證**的裝置。
	  • **指定目錄**掃描在工作執行時位於指定資料夾及其所有嵌套資料夾中的檔案。
	  • **所有本機磁碟**掃描在工作執行時儲存在本機磁碟上所有資料夾中的檔案。
	  掃描所有本機磁碟可能會導致主機負載過高。
	• 如果您選擇**記憶體**，則以下設定可用：
	  • **處理程序**列出了要掃描的處理程序的短名稱或檔案遮罩。
	  應用程式掃描主機上執行的所有具有相同名稱的處理程序。
	  如果**處理程序**欄位留空，應用程式將掃描工作執行時正在運行的所有處理程序，除了 PID 小於 10 的處理程序和**排除項目**欄位中所列的處理程序。
	  • **排除項目**列出了要從掃描中排除的處理程序的完整名稱或檔案遮罩。
	  如果主機上正在執行多個具有相同名稱的處理程序，應用程式將從掃描中排除所有此類處理程序。
	• 如果您選擇**自動執行點**，則以下設定可用：
	  • 快速掃描所有自動執行點，但 COM 物件除外。
	  • **完整**掃描所有自動執行點及其關聯檔案。
	  如果您使用 Kaspersky Endpoint Security for Windows 作為 Endpoint Agent 元件，則無論選擇的設定為何，都會執行完整掃描。
	• 如果您選擇**指定目錄**，則下列設定可用：
	  • **指定目錄**是以C:\<目錄名稱>* 格式指定的目錄路徑。
	  • **排除項目**是以C:\<目錄名稱>* 格式指定的目錄路徑。
	• **最大掃描持續時間**是最大掃描持續時間。
	當該時間過去後，即使未套用某些規則來掃描主機，掃描也會停止。工作報告包含掃描停止時的最新結果。
	• **敘述** — 工作描述。該欄位是可選的。

管理服務
啟動、停止、暫停、刪除、還原指定裝置上的服務，或變更服務的啟動類型。
	• **服務名稱**是服務的名稱。
	• **MD5/SHA256**是服務的 MD5 或 SHA256 雜湊值。該欄位是可選的。
	如果您輸入從 DLL 載入的服務的雜湊值，Kaspersky Anti Targeted Attack Platform 會同時將指定的雜湊值與服務 DLL 的雜湊值和 Svchost 程序的雜湊值進行比較。
	• **操作**是您要對服務執行的操作。
	支援以下服務操作：
	  • **開始**。
	  • **停止**。
	  • **暫停**。

回應操作	工作設定
	• **還原**。 • **刪除**。 • **修改啟動類型**。 當您刪除某個服務時，該服務啟動的程序將繼續執行，直到系統重新啟動或該程序終止。 • 如果您選擇"**修改啟動類型**"，您需要在"**啟動類型**"欄位中選擇服務的啟動類型。 • **敘述** — 工作描述。該欄位是可選的。
隔離檔案 隔離受感染或疑似受感染的檔案。 必要時，您可以從隔離區還原檔案。	• **檔案路徑**—您想要刪除的檔案的路徑。 • **MD5/SHA256**—要刪除的檔案的 MD5- 或 SHA256 雜湊。該欄位是可選的。 • **敘述**是工作描述。該欄位是可選的。

啟動應用程式
執行應用程式或命令。
如有必要，您可以終止已啟動的處理程序。有關終止處理程序工作的更多詳細資訊，請參見上表。
	• 在**檔案路徑**和**工作目錄**欄位中，透過以下方式之一輸入值：
	  • 在**檔案路徑**欄位中，輸入可執行檔的完整路徑（例如，`C:\Windows\System32\ipconfig.exe`）。留下**工作目錄**欄位為空。
	  建立工作時，應用程式不會檢查指定的可執行檔路徑是否有效。
	  • 在**檔案路徑**欄位中，輸入可執行檔的名稱和副檔名（例如 `ipconfig.exe`）。在**工作目錄**欄位中，輸入工作目錄（例如 `C:\Windows\System32\`）。
	• **參數**是執行檔案或工作的其他選項（例如，`/all` 參數）。
	• **敘述** — 工作描述。該欄位是可選的。

建立預防規則 止檔案和處理程序在指定的裝置上啟動。 如有必要，您可以刪除、啟用或停用已建立的阻止規則。	• **狀態**—阻止規則的狀態。 • **MD5/SHA256**—您要阻止啟動的檔案或資料串流的 MD5 或 SHA256 雜湊。 • **名稱**是阻止規則的名稱。 • **通知使用者阻止檔案執行**向套用此阻止規則的電腦使用者顯示有關該阻止規則已啟動的通知。

監控裝置上的使用者

Kaspersky Anti Targeted Attack Platform 可以監控應用程式已知的裝置上的使用者帳戶。在監控使用者時，應用程式會自動取得有關在裝置作業系統中註冊的使用者帳戶的資訊。根據這些資訊，應用程式產生使用者表。

當取得有關使用者帳戶的資訊時，應用程式會使用此資訊監控裝置上的所有使用者帳戶，但某些本機系統使用者除外，這些使用者只有作業系統服務可以使用。例如，應用程式不會監控 Windows 裝置上的 LocalSystem 和 NetworkService 帳戶。

若要使用使用者監控功能，必須啟用資產管理方法來偵測裝置活動和裝置資訊。必須在所有具有從其接收資訊的應用程式元件的伺服器上啟用這些方法。

使用者監控基於從以下類型的來源收到的資訊：

1. **遙測 (Endpoint Agent)**

   當 Endpoint Agent 元件與 NDR 功能整合時，將收到有關裝置及其在這些裝置上執行的處理程序的資訊。

2. **外部來源**

   資訊接收自使用 NDR API 並向 Kaspersky Anti Targeted Attack Platform 傳送有關使用者的資訊的系統。

來源按來自這些來源的資訊的優先順序從高到低的順序列出。應用程式根據收到的資訊的優先順序來處理有關使用者的資訊。來自較高優先來源的使用者資訊可能會覆蓋來自其他來源的資訊。如果關於此類使用者的資訊是從**外部來源**獲得的，但是從這些來源收到的新資訊中缺少使用者，則應用程式也會自動從表中刪除使用者。

您可以在**資產**部分的**使用者**索引標籤上檢視有關使用者的資訊。

檢視使用者表時，您可以設定、篩選、搜尋和排序使用者，以及導覽至相關項目。所有使用者表最多可包含 200000 個使用者。

應用程式在表格中以及選定使用者的詳細資料區域中顯示有關裝置使用者的以下資訊：

- **使用者 ID** 是 Kaspersky Anti Targeted Attack Platform 中指派的使用者 ID。
- **使用者名稱**是不含裝置網域名稱或主機名稱的使用者帳戶名稱。
- **完整名稱**是包含裝置網域名稱或主機名稱的使用者帳戶名稱。
- **群組**列出了使用者所屬的使用者群組的名稱。
- **裝置**是裝置的名稱和位址。
- **來源**是有關使用者資訊的來源。
- **SID**是使用者的安全ID。
- **帳戶狀態**是與收到的啟用或停用帳戶的值對應的狀態。
- **鎖定**是與收到的帳戶阻止設定的值對應的狀態。
- **下次登入時變更密碼**是反映使用者是否必須在下次登入時變更密碼的屬性。
- **阻止使用者變更密碼**是反映是否禁止使用者變更使用者自己的密碼的屬性。
- **密碼有效期限**是與收到的啟用或停用使用者密碼有效期限限制的設定的值對應的狀態。
- **收到的資料**是上次收到有關使用者帳戶的資訊的日期和時間。
- **描述**是為使用者帳戶指定的描述。

在監控使用者時，應用程式使用**資產管理**技術註冊事件。事件註冊的系統事件類型代碼為4000005600。當裝置上自動新增、修改或刪除使用者帳戶時，會記錄事件。

您可以編輯事件類型的可用設定。

監控裝置上的檔案執行狀況

Kaspersky Anti Targeted Attack Platform 可以監控應用程式已知的裝置上的檔案執行情況。根據從 EPP 應用程式收到的資訊來監控檔案執行情況。根據這些資訊，應用程式產生一個可執行檔表。

要從 EPP 應用程式自動獲取有關檔案執行的資訊，必須滿足以下條件：

- 必須在裝置上安裝 Endpoint Agent。
- 必須啟用資產管理方法來偵測裝置活動和裝置資訊。

對於可執行檔案表，項目數量和儲存期限有以下限制：

- 可執行檔案的總數不得超過 100000 個。
  如果達到執行檔的最大數量，應用程式會自動刪除10% 的最舊條目。
- 在再次收到有關可執行檔執行的資訊之前，可執行檔的最長儲存期限為 90 天。
  如果在最大儲存期限到期之前沒有收到有關檔案執行的新資訊，應用程式將自動刪除該檔案的條目。

如果有必要，具有管理員角色的使用者可以手動刪除可執行檔。

若要檢視可執行檔表：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**可執行檔案**”索引標籤。

   可執行檔案表將顯示。

檢視可執行檔案表時，您可以設定、篩選、搜尋和排序檔案，以及導航至相關項目。

該表顯示以下資訊：

- **檔案 ID** 是 Kaspersky Anti Targeted Attack Platform 中指派的檔案 ID。
- **裝置**是裝置的名稱和位址。
- **名稱**是應用程式的名稱和版本，或檔案名稱。
- **接收日期**是上次接收有關檔案資訊的日期和時間。
- **產品**是儲存在裝置作業系統中的軟體產品的名稱。
- **產品版本**是裝置作業系統中已儲存的軟體產品的版本。
- **供應商**是應用程式供應商的名稱。
- **路徑**是檔案的完整路徑。
- **檔案大小**是檔案佔用的磁碟空間量。

- **MD5 雜湊**是使用 MD5 雜湊演算法計算的檔案核對總和。
- **SHA256 雜湊**是使用 SHA256 雜湊演算法計算的檔案核對總和。
- **簽章**是驗證檔案數位簽章的結果：**有效**（如果數位簽章驗證成功）或**無效**（例如，如果憑證已過期）。
- **建立日期**是檔案建立的日期和時間。
- **變更日期**是檔案最後修改的日期和時間。
- **來源**是檔案資訊的來源。
- **屬性**是檔案屬性的清單。
- **描述**是針對檔案設定的描述。

主動裝置輪詢作業

使用主動輪詢作業，您可以直接從裝置本身接收有關裝置及其配置的準確完整資訊，從而對受監控的裝置進行安全稽核。使用連線器實作主動輪詢。若要主動輪詢裝置，您需要為應用程式新增一個或多個**主動輪詢**連線器。

連線器提供不同的主動輪詢方法。*主動輪詢方法*規定了協定以及這些協定的命令和功能。內建**主動輪詢**連線器類型包含一組方法，這些方法支援透過應用層協定和一般協定進行主動輪詢。Kaspersky Anti Targeted Attack Platform 支援以下裝置主動輪詢方法：

- 透過 ARP 輪詢（僅適用於核心版本4.3 或更高版本的電腦）
- 透過 SMB 輪詢
- 透過 SNMP 輪詢
- 透過 SSH 輪詢
- 透過 WinRM HTTP 輪詢
- 透過 WinRM HTTPS 輪詢
- 透過 WMI 輪詢

這些方法可以讓您取得不同的裝置資訊集。您可以選擇配置主動輪詢時所需的資訊和要使用的方法。

一些方法使用 Secret 來連線裝置。裝置連線是使用新增到應用程式的 Secret 憑據建立的。

使用適當的方法，應用程式可以根據主動輪詢結果自動更新以下裝置資訊：

- 代表應用程式中的裝置的名稱
- 代表網路上的裝置的名稱（網路名稱）
- 裝置硬體供應商的名稱
- 裝置型號

- 裝置硬體的版本號
- 裝置軟體供應商的名稱
- 裝置軟體名稱
- 裝置軟體的版本號
- 裝置的網路介面的位址資訊
- 裝置上安裝的作業系統的名稱（僅適用於執行 Windows 和 Linux 作業系統的裝置）

有關應用程式支援的主動輪詢裝置的作業系統清單，請參閱附錄。

當新增裝置或編輯裝置資訊時，應用程式不會更新使用**自動更新**撥動按鈕停用自動更新功能的資料。該應用程式還評估接收到的裝置資訊的準確性，並且在某些情況下可能不會更新先前接收到的資訊。

一些主動輪詢方法支援偵測風險和利用獲取的裝置資訊修改拓撲圖。

您可以手動執行安全性稽核作業，也可以將計畫設定為自動執行每個作業。只有具有高階安全官角色的使用者才能執行主動輪詢作業。

使用主動輪詢功能時，必須牢記以下特殊注意事項和限制：

- 新增產品授權金鑰後，此功能可用。
- 用於主動輪詢裝置的連線器的應用程式模組需要透過網路存取裝置，以便向裝置傳送請求並接收資料。如果應用程式模組在安裝了應用程式元件的主機上運行，為了確保對裝置的網路存取，此電腦必須具有與要輪詢的裝置的網路連線的網路介面。如果監控點的網路介面接收映像的公司 LAN 流量（例如，來自網路交換器的 SPAN 連接埠），則這些網路介面不能用於此目的。
- 如果主動輪詢裝置誤解了活動輪詢的命令，則可能會出現意外問題。這些問題可能是由裝置的錯誤配置或高度專業化配置引起的。此外，網路配置中隱藏的錯誤也可能引發問題，而這些錯誤在裝置正常通訊時不會顯現出來。因此，主動輪詢裝置可能會帶來以下潛在後果的風險：
    - 裝置關閉
    - 裝置連線中斷
    - 裝置完全或部分故障
    - 運作速度比正常情況下慢
    - 網路和部件的其他潛在故障

新增主動輪詢作業

對於應用程式已知的裝置，您可以新增活動輪詢作業。

只有具有高階安全官角色的使用者才能新增主動輪詢作業。新增產品授權金鑰後，才可以新增主動輪詢作業。

使用精靈配置主動輪詢作業。此精靈可讓您逐步配置作業。完成設定後，您可以等待掃描按計畫開始或手動啟動作業。

新增活動輪詢作業時，您可以透過下列方式呼叫設定精靈：

- 新增具有空白設定的作業。為此：

  1. 選擇“**資產**”部分。

  2. 在“**主動輪詢**”索引標籤上，點擊“**新增作業**”。

  配置精靈的設定沒有預設值。

- 為所選裝置新增作業。為此：

  1. 選擇“**資產**”部分。

  2. 在“**裝置**”索引標籤上，選擇要為其新增主動輪詢作業的裝置。您可以選擇不超過 100 台裝置。

  3. 在裝置表上方的工具列中，開啟“**建立作業**”下拉清單，然後選擇“**主動輪詢**”。

  預設情況下，在配置精靈的設定中會建立由選定的裝置組成的裝置清單。

若要在設定精靈視窗中設定作業：

1. 閱讀警告視窗中的主動輪詢注意事項，並確認您接受使用主動輪詢模組所帶來的風險。

2. 在精靈的“**選擇裝置**”部分，建立要執行主動輪詢的裝置清單。最多可選擇 100 台裝置。

   您可以使用“**新增至作業**”和“**從作業中刪除**”按鈕建立裝置清單。要新增裝置，應用程式會開啟一個帶有裝置分類表的視窗。您可以將表格篩選和排序，以顯示所需的裝置。

3. 在精靈的“**選擇參數**”部分，選取要使用主動輪詢更新的特定裝置資訊的核取方塊。您也可以啟用風險偵測（“**風險**”核取方塊）和發現裝置的拓撲設定（“**拓撲設定**”核取方塊）。

4. 在精靈的“**選擇方法**”部分，執行下列操作：

   a. 選擇一個主動輪詢模組。

   b. 選取要用於取得裝置資訊、風險偵測和/或讀取拓撲設定的特定方法的核取方塊。

      可以使用的方法按提供主動輪詢裝置功能的連線器分組。此清單僅包含支援獲取所選資訊的方法。如果連線器無法用於所選裝置的主動輪詢，則不會顯示此連線器的可用方法（例如，如果連線器已停用，或者如果為連線器選擇了不包含所選裝置位址的位址空間）。

   c. 根據需要配置每個連線器的方法。例如，對於“**透過 SSH 進行輪詢**”，指定連接埠和憑據 Secret。

      > 如果尚未將具有所需憑證的 Secret 新增至應用程式中，您可以在不關閉設定精靈視窗的情況下在瀏覽器中開啟新頁簽，連線至伺服器並新增 Secret，然後使用設定精靈視窗中的按鈕重新整理 Secret 清單。

      > 我們不建議使用相同的 Secret 對網路上的裝置執行主動輪詢，因為這會對資訊安全等級產生負面影響。

      需要配置設定的方法以紅色突出顯示。若要更新設定，請點擊所需方法右側的⚙按鈕。

5. 在精靈的“**作業配置**”部分，配置其餘作業設定：

   a. 輸入作業的名稱和說明。

      您可以使用字母、數字、空格以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。作業名稱必須以空格以外的任何有效字元開始和結束。

      作業名稱不得超過 256 個字元。作業說明不得超過 4096 個字元。

   b. 若要根據排程運行作業，請啟用“**根據排程運行作業**”選項並設定計劃設定：

      - 在“**頻率**”下拉清單中，選擇執行作業的頻率：**每小時**、**每天**、**每週**或**每月**。
      - 根據所選的選項，指定設定值以定義精確的作業啟動時間。

      > 應用程式根據排程運行作業，前提是此作業的上一次運行已完成。如果在啟動排程作業時，其上次啟動的狀態為“*正在執行*”，則應用程式將跳過排程作業的執行。

6. 點擊“**建立作業**”或“**建立和執行**”關閉精靈。

   指定的設定顯示在作業詳細資料中。

編輯主動輪詢作業

只有具有高階安全官角色的使用者才能編輯主動輪詢作業。

若要編輯主動輪詢作業：

1. 選擇“**資產**”部分。
2. 在“**主動輪詢**”頁簽上，選擇要變更其設定的作業。
3. 點擊**“編輯”**。

   配置精靈啟動。所選作業的設定在配置精靈的設定中指定為預設值。

4. 在精靈的“**作業配置”**部分，配置其餘作業設定：

   a. 輸入作業的名稱和說明。

      您可以使用字母、數字、空格和以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。作業名稱必須以空格以外的任何有效字元開始和結束。

      作業名稱不得超過 256 個字元作業描述不得超過4096 個字元

   b. 若要根據排程運行作業，請啟用“**根據排程運行作業**”選項並設定計劃設定：

      - 在“**頻率**”下拉清單中，選擇執行作業的頻率：**每小時**、**每天**、**每週**或**每月**。
      - 根據所選的選項，指定設定值以定義精確的作業啟動時間。

應用程式根據排程運行作業，前提是此作業的上一次運行已完成。如果在啟動排程作業時，其上次啟動的狀態為“*正在執行*”，則應用程式將跳過排程作業的執行。

5. 點擊“**編輯作業**”關閉精靈。

   指定的設定顯示在作業詳細資料中。

檢視主動輪詢作業表

主動輪詢作業表顯示在**資產**區段的**主動輪詢**索引標籤上。

作業設定顯示在表格以下列中：

- **作業 ID**。
  Kaspersky Anti Targeted Attack Platform 中指派的作業 ID。
- **名稱**。
  代表應用程式中的作業的名稱。
- **敘述**。
  作業描述
- **建立日期**。
  將作業新增至應用程式的日期和時間。
- **變更時間**。
  應用程式中最後修改的日期和時間。
- **所選裝置**。
  為作業選擇的裝置數量。
- **排程**。
  有關應用程式運行作業所使用的計劃的資訊。
- **上次運行狀態**。
  作業上次執行時所有裝置掃描的結果狀態。
- **上次運行**。
  作業上次運行的日期和時間。
- **下次運行**。
  作業下次計畫運行的日期和時間。

檢視主動輪詢作業表時，您可以使用設定、篩選、搜尋和排序功能。

啟動和停止主動輪詢作業

您可以手動啟動和停止主動輪詢作業。當您啟動或停止作業時，應用程式將啟動或停止為此作業選擇的裝置上的所有掃描。

您可以根據上次作業執行的狀態停止或啟動該作業。例如，如果作業上次運行的狀態為"*正在運行*"，則無法啟動該作業。

只有具有高級安全官角色的使用者才能手動啟動和停止主動輪詢作業。

若要啟動主動輪詢作業：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇"**資產**"部分。
3. 在"**主動輪詢**"頁簽上，選擇要啟動的作業。

   详细信息区域显示在 Web 界面窗口的右側部分。
4. 點擊"**啟動**"。如果無法啟動作業，則該按鈕將被停用。

   Kaspersky Anti Targeted Attack Platform 啟動作業。您可以在作業詳細資料的**"運行"**標籤上檢視有關正在進行的裝置掃描的資訊。

若要停止主動輪詢作業：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇"**資產**"部分。
3. 在"**主動輪詢**"頁簽上，選擇要停止的作業。

   详细信息区域显示在 Web 界面窗口的右側部分。
4. 點擊"**停止**"。如果作業無法停止，則該按鈕將被停用。

檢視有關主動輪詢作業運行的一般資訊

您可以在作業表中檢視有關主動輪詢作業運作的一般資訊。該表顯示有關最近運行的資訊，但不包括有關裝置掃描的資訊。若要檢視所有作業運行的一般資訊，包括裝置掃描的資訊，請選擇作業，然後在詳細資訊區域開啟**運行**索引標籤。

有關主動輪詢作業運行的一般資訊包括以下內容：

- 作業或裝置掃描的狀態。

  可以有以下狀態：

  - **掛起** – 尚未傳送啟動掃描的命令。
  - **進行中** – 作業正在啟動，或掃描正在進行中。
  - **正在取消** – 正在停止作業或掃描的啟動。

- **已取消** – 已停止作業或掃描的啟動。
- **已完成** – 掃描已成功完成，或作業運行中的所有掃描都已成功完成。
- **錯誤** – 掃描過程中發生錯誤，或作業運行中的所有掃描中都發生錯誤。
- **部分成功** – 作業已完成，但部分成功：某些掃描的狀態為**已完成**，而某些掃描的狀態為**已取消**或**錯誤**。

- 啟動日期和時間。
- 結束日期和時間。
- 執行時間

檢視有關主動輪詢作業執行的報告

檢視主動輪詢作業運作的詳細資訊時，您可以檢視包含裝置掃描結果的報告。應用程式將為以下狀態完成的作業產生報告：**已完成**、**部分成功**、**已取消**和**錯誤**。

報告中顯示以下詳細資訊：

- 被掃描的裝置的名稱。
- 裝置設定更新狀態。
- 按更新狀態分組的裝置設定清單。
- 依執行狀態分組的方法清單。如果在使用某種方法時發生錯誤，應用程式將顯示其原因。

若要檢視主動輪詢作業執行的報告：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇“**資產**”部分。
3. 在“**主動輪詢**”頁簽上，選擇要檢視執行報告的作業。
   详细信息区域显示在 Web 界面窗口的右側部分。
4. 在詳細資料區域中，前往“**執行**”標籤並選擇所需的作業運行。
   详细信息区域显示在 Web 界面窗口的右側部分。詳細資訊區域顯示有關所選作業運行的詳細資訊。

刪除主動輪詢作業

您可以刪除主動輪詢作業。但是，您無法刪除上次執行狀態為“**正在執行**”或“**掛起**”的作業。

只有具有高階安全官角色的使用者才能刪除主動輪詢作業。

若要刪除主動輪詢作業：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇“**資產**”部分。
3. 在“**主動輪詢**”索引標籤上，選擇要刪除的作業。
4. 點擊**刪除**。

   這將開啟一個確認提示視窗。
5. 在提示視窗中，確認刪除作業。

   您只能刪除上次執行狀態不是“**正在執行**”或“**掛起**”的作業。如果所選作業中存在狀態為“**正在執行**”或“**掛起**”的作業，則會顯示對應的訊息。若要刪除此類作業，您必須先停止這些作業。

配置位址空間

Kaspersky Anti Targeted Attack Platform 監控裝置及其互動，同時考慮位址空間（以下也稱為“AS”）。*位址空間*用於根據某些屬性（例如，根據裝置所屬的網路段）將裝置位址分類為集合。

為了描述位址空間，應用程式使用規則和子網路清單。

*位址空間規則*是一組決定某個位址是否屬於該位址空間的參數。若要與位址空間關聯，MAC 或 IP 位址必須至少符合一條位址空間規則。如果一個位址與多個規則匹配，應用程式將選擇其規則以最不通用的方式定義關聯條件的位址空間（例如，如果規則中明確指定了該位址）。

*位址空間子網路*用於檢查應用程式發現的 IP 位址。根據發現的 IP 位址所屬的子網路類型，應用程式可能會執行不同的資產監控操作和互動控制操作。

您可以在**位址空間**索引標籤的**資產**區段中配置位址空間。每個位址空間由一個包含有關該位址空間的資訊的部分表示。此部分由標題和包含規則和子網表格的子部分組成。檢視有關位址空間的資訊時，您可以展開和折疊部分。

預設位址空間

預設情況下，應用程式配置了一個位址空間，即**預設**位址空間。此位址空間包含一條將所有 MAC 和 IP 位址與此位址空間關聯起來的規則。預設情況下，**預設**位址空間的子網路清單包含企業網路中最常用的一組標準子網路。

您無法編輯**預設**位址空間的規則或將其他規則新增至此位址空間。但是，具有高級安全官員角色的使用者可以編輯此位址空間中的子網路清單，以配置一組子網路，其中考慮到公司網路中裝置 IP 定址的設定方式。如果 Kaspersky Anti Targeted Attack Platform 接收來自EPP 應用程式的資料，應用程式可以使用這些資料自動將子網路新增至子網路清單。

附加位址空間

如有必要，除**預設**位址空間外，您還可以在應用程式中配置多個位址空間。您可以為新增的位址空間建立任意規則和子網路集合。符合所新增位址空間條件的位址將與這些位址空間相關聯。其餘位址仍與**預設**位址空間相關聯。

您可能需要新增位址空間，例如，如果您在不同的網段中使用具有相同位址的裝置。在這種情況下，在新增和配置位址空間後，應用程式可以透過應用程式新增至位址的附加屬性（即位址空間名稱）來消除位址資訊的歧義。

有關位址空間使用範例，請參閱附錄。

位址和位址空間的關係

當使用多個位址空間時，應用程式會將位址空間名稱屬性新增至應用程式物件中指定的所有位址：裝置、風險、規則、事件和其他物件。如果刪除所有非預設位址空間，則不再顯示位址的位址空間名稱屬性（位址空間屬性僅為事件中的位址和某些與裝置相關的風險保留）。

位址空間名稱屬性表示位址和位址空間之間的關係。與位址空間的關係使得位址依賴這些位址空間。

位址和位址空間之間的關係導致刪除位址空間時需要特別考慮以下事項：應用程式會自動刪除與所刪除位址空間關聯的所有位址。此類位址將從除事件之外的所有應用程式物件中刪除。當從物件中刪除位址時，應用程式會檢查該物件中是否還剩餘其他位址，如果沒有其他位址，應用程式也會刪除該物件本身（例如，裝置）。

關於位址空間規則

位址空間的規則顯示在位址空間描述內的**規則**區塊中。有關規則的資訊顯示在位址空間的標題列和規則表中。

位址空間規則設定顯示在表格以下列中：

- **來源**。

  位址資訊的資料來源類型和選定的資料來源清單。可能的資料來源類型如下：

  - **監控點** – 為規則選擇的監控點。
  - **整合伺服器** – 為規則選擇的整合伺服器（從所選整合伺服器接收的位址資訊資料將滿足位址空間規則）。
  - **主動輪詢模組** – 為規則選擇的主動輪詢模組連線器（從所選的主動輪詢模組接收到的位址資訊資料將滿足位址空間規則）。

  將要用作來源的物件新增至應用程式後，必須在位址空間規則中指定資料來源。例如，在新增連線器後，必須指定**主動輪詢模組**資料來源的連線器；連線器類型為**主動輪詢**。

- **OSI 模型層**

為位址空間規則所選定的 OSI（開放系統互連）網路協定堆疊層。您可以為 OSI 模型以下層的位址設定規則：

- **資料鏈路 (L2)** – MAC 位址。
- **網路 (L3)** – IP 位址。
- **資料鏈路和網路（L2 和 L3）** – MAC 位址和 IP 位址。

- **VLAN ID**。
  符合 IEEE 802.1q 標準的 VLAN 技術所使用的 VLAN ID。當用於位址空間規則時，**VLAN ID**可以採用下列值：
  - **任何** – VLAN 技術用於裝置之間的網路互動，可以使用任何 VLAN ID。
  - **不允許** – VLAN 技術不用於裝置之間的網路互動。
  - **任何或不使用** – VLAN 技術要么不用於裝置之間的網路互動，要么與任何 VLAN ID 一起使用。
  - **具有 VLAN ID 清單的固定值** – VLAN 技術用於裝置之間的網路互動，位址空間只能包含具有列出的 VLAN ID 之一的位址資訊。

- **IP 位址**
  包含在位址空間中的 IP 位址。您可以單獨指定位址，將其指定為範圍或 CIDR 子網路位址。

檢視規則表時，您可以使用設定功能（透過點擊⚙圖示）和搜尋功能。

關於位址空間子網

位址空間的子網路顯示在位址空間描述內的“**子網路**”區塊中。

該應用程式將發現的 IP 位址與位址空間子網清單進行匹配，並且根據 IP 位址是否屬於某些類型的子網，可以執行以下操作：

- 將具有其發現的 IP 位址的裝置新增至裝置表中並監控該裝置的活動。
- 在網路互動圖和拓撲圖上顯示具有其偵測到的 IP 位址的裝置作為其對應的節點類型（已知裝置、未知裝置或 WAN 節點）。
- 顯示網路互動圖上的連線，其中互動方之一是具有發現的 IP 位址的裝置。
- 根據配置的規則（互動控制規則、入侵偵測規則和關聯規則）掃描裝置與發現的 IP 位址的互動作用。
- 忽略具有發現的 IP 位址的裝置的活動。

位址空間規則的子網路設定顯示在表格的以下列中：

- **子網路**。
  無類別域間路由 (CIDR) 格式的子網路位址：<子網路基底位址>/<遮罩中的位數>。子網路位址顯示為表示子網路嵌套層次結構的樹。

- **類型**。

規定其用途的子網路類型。有以下類型可用：

- **私有，IT** – 用於作為資訊科技 (IT) 資源的裝置（例如檔案伺服器）的子網路。
- **私有，DMZ** – 位於非軍事區 (DMZ) 網路段內的裝置的子網，例如處理來自外部網路的請求的伺服器。
- **公用** – 被視為其他類型子網路中裝置的外部（全域）網路的子網路。此子網路的 IP 位址由網路互動圖上的 WAN 節點表示。
- **連結-本機** – 區域網路（未路由）一段內網路互動的子網路。

- **範圍**

  子網路中包含的 IP 位址範圍。

- **自動新增子網路**

  指示是否啟用或停用根據從 EPP 應用程式收到的資訊自動新增嵌套子網路。如果啟用此模式，應用程式將根據從 EPP 應用程式收到的資訊新增嵌套子網路。

檢視子網表時，您可以使用設定功能（透過點擊⚙圖示）以及篩選、搜尋和排序功能。

新增位址空間

如果您需要根據某些標準（例如，基於屬於網路段的裝置）將裝置位址分類為集合，則可以將位址空間新增至應用程式。

應用程式中的最大位址空間數為 100。

只有具有高階安全官角色的使用者才能新增位址空間。

若要新增位址空間：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇“**資產**”部分。
3. 在“**位址空間**”索引標籤上，點擊“**新增 AS**”開啟詳細資料區域。
4. 輸入位址空間的名稱。

   您可以使用字母、數字、空格字元以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。

   位址空間名稱必須符合以下要求：

   - 以空格以外的任意字元開始和結束。
   - 最多包含 255 個字元。
   - 不要重複使用另一個位址空間的名稱（不區分大小寫）。

   > 我們建議使用長度為 6-8 個字元或更短的位址空間。如果名稱包含較多字元，則某些資料表（例如裝置表）的儲存格中可能無法完整顯示位址資訊。

5. 如有必要，請輸入位址空間的文字描述。

6. 配置第一個位址空間規則的設定。

7. 如有必要，請點擊**新增規則**以新增並配置附加位址空間規則。

   位址空間中的規則總數不能超過 10 條。

8. 點擊**儲存**按鈕。

   如果未指定所有必要的設定，或某些設定無效，則此按鈕不可用。

位址空間索引標籤的下部將顯示一個單獨的區塊，其中包含有關新增的位址空間的資訊。

為資產管理建立子網路清單

本節包含可用於產生資產管理子網路清單的功能的資訊。

對於位址空間，您可以建立子網路清單，其中考慮到裝置定址在公司網路中的工作方式。本節提供有關使用功能產生子網路清單的說明。

如果 Kaspersky Anti Targeted Attack Platform 接收來自 EPP 應用程式的資料，應用程式可以使用這些資料自動將子網路新增至相應位址空間。如果發現的子網路嵌套在啟用了自動子網路新增模式的子網路內，應用程式會自動新增這些子網路。

只有具有高階安全官角色的使用者才能管理子網路清單。

新增子網路

若要新增子網路：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。

2. 選擇“**資產**”部分。

3. 在**位址空間**索引標籤上，展開包含要新增子網路之位址空間資訊的區塊。

4. 在“**子網路**”區塊的標題中，點擊 + 圖示。

   詳細資訊區域顯示在網頁介面視窗的右側。

5. 在“**子網路**”欄位中，以 CIDR 格式輸入子網路位址：<子網路的基底位址>/<遮罩中的位元數>。

6. 在“**類型**”下拉清單中，根據子網路的用途選擇子網路的類型。

7. 啟用或停用“**自動新增子網路**”切換開關，以根據從 EPP 應用程式收到的資料，啟用或停用自動新增嵌套子網路。

   如果啟用此模式，應用程式將根據從 EPP 應用程式收到的資訊在此子網路下方新增嵌套子網路。對於這些巢狀子網，預設類型是為目前子網路選擇的類型。

8. 點擊“**儲存**”按鈕。

子網路將會新增到樹的相應層級的子網路清單中。

編輯子網路設定

若要編輯子網路設定：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇“**資產**”部分。
3. 在“**位址空間**”索引標籤上，展開包含有關要編輯子網路設定的位址空間的資訊的區塊。
4. 展開“**子網路**”區塊並選擇相關子網路。
   詳細資訊區域顯示在 Web 介面視窗的右側。
5. 點擊“**編輯**”。
6. 根據您的需要，請執行以下操作：
   - 在“**子網路**”欄位中，以 CIDR 格式輸入子網路位址：<子網路的基底位址>/<遮罩中的位元數>。
     根子網路的位址無法編輯。
   - 在“**類型**”下拉清單中，根據子網路的用途選擇子網路的類型。

     > 變更子網路類型時，請記住新的子網路類型可能會影響應用程式使用子網路中的 IP 位址執行的操作。例如，如果您選擇“**公用**”類型，網路互動圖將不再顯示從該子網路指派 IP 位址的裝置的連結。

   - 啟用或停用“**自動新增子網路**”切換開關，以根據從 EPP 應用程式收到的資料，啟用或停用自動新增嵌套子網路。
     如果啟用此模式，應用程式將根據從 EPP 應用程式收到的資訊在此子網路下方新增嵌套子網路。對於這些巢狀子網，預設類型是為目前子網路選擇的類型。
7. 點擊“**儲存**”按鈕。

如果變更了“**子網路**”值，則子網路的樹狀層次結構層級也可能會變更。

刪除子網路

在位址空間的子網路清單中，您可以刪除樹中除根子網路（子網路 0.0.0.0/0）以外的任何子網路。

若要刪除子網路：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇“**資產**”部分。
3. 在“**位址空間**”索引標籤上，展開包含要從中刪除子網路的位址空間資訊的區塊。
4. 展開**子網路**區塊並選擇要刪除的子網路。
   詳細資訊區域顯示在 Web 介面視窗的右側。

5. 點擊**刪除**。

   這將開啟一個確認提示視窗。

6. 在提示視窗中，確認刪除子網路。

已刪除的子網路將從子網路清單中移除。如果刪除的子網包含巢狀子網，這些子網將保留在清單中（但是，這些子網在層次樹中的層級會發生變化）。

檢視所選子網路中具有 IP 位址的裝置的資訊

您可以檢視具有位址空間中選定子網路的 IP 位址的裝置的資訊。有關裝置的資訊顯示在裝置表中。裝置表會根據子網路位址自動套用篩選器。

若要檢視裝置表中有關裝置的資訊：

1. 選擇“**資產**”部分。

2. 在“**位址空間**”索引標籤上，展開帶有包含相關子網路的位址空間的資訊的區塊。

3. 展開“**子網路**”區塊並選擇您想要檢視裝置資訊的子網路。

   詳細資訊區域顯示在網頁介面視窗的右側。

4. 點擊“**顯示裝置**”。

這將開啟“**資產**”部分中的“**裝置**”索引標籤。裝置表是透過裝置位址資訊中的 IP 位址進行篩選的。

變更位址空間

對於新增的位址空間，您可以編輯其名稱、文字描述以及規則設定。但是，您無法為**預設**位址空間編輯任何這些內容。

您也可以為任何位址空間建立子網路清單（包括**預設**位址空間的子網路清單）。

管理位址空間的規則設定時，必須考慮此位址空間與應用程式物件（包括裝置、風險、規則、事件和其他物件）中指定的位址之間的關係。如果編輯位址空間的規則設定切斷了該位址空間與位址的關係，應用程式會自動刪除這些位址。如果這些物件沒有任何其他位址，這可能會導致物件本身（例如，裝置）被刪除。

只有具有高級安全官員角色的使用者才能編輯位址空間的名稱、文字描述和規則設定。

若要編輯位址空間的名稱、文字描述或規則設定：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。

2. 選擇“**資產**”部分。

3. 在“**位址空間**”索引標籤上，點擊包含相關位址空間資訊的區塊中的圖示。

   詳細資訊區域顯示在網頁介面視窗的右側。

4. 根據您的需要，請執行以下操作：

   - 輸入位址空間的名稱。
     您可以使用字母、數字、空格字元以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
     位址空間名稱必須符合以下要求：

     - 以空格以外的任意字元開始和結束。
     - 最多包含 255 個字元。
     - 不要重複使用另一個位址空間的名稱（不區分大小寫）。

     > 我們建議使用長度為 6-8 個字元或更短的位址空間。如果名稱包含較多字元，則某些資料表（例如裝置表）的儲存格中可能無法完整顯示位址資訊。

   - 輸入位址空間的描述。
   - 管理位址空間規則的設定。
   - 如有必要，請點擊**新增規則**以新增和配置其他位址空間規則，或使用×圖示刪除任何不必要的規則。
     位址空間中的規則總數不能超過 10 條。

5. 點擊**儲存**按鈕。
   如果未指定所有必要的設定，或某些設定無效，則此按鈕不可用。

6. 在提示視窗中，確認位址空間設定的變更。

刪除位址空間

您可以刪除已新增的位址空間。無法刪除“**預設**”位址空間。

> 刪除位址空間時，必須考慮此位址空間與應用程式物件（包括裝置、風險、規則、事件和其他物件）中指定的位址之間的關係。如果刪除某個位址空間會切斷該位址空間與位址的關係，則應用程式會自動刪除這些位址。如果這些物件沒有任何其他位址，這可能會導致物件本身（例如，裝置）被刪除。

只有具有高階安全官角色的使用者才能刪除位址空間。

若要刪除位址空間：

1. 使用 Web 介面以高階安全官角色連線到 Central Node。
2. 選擇“**資產**”部分。
3. 在“**位址空間**”索引標籤上，點擊包含要刪除的位址空間資訊的區塊中的🗑圖示。
   這將開啟一個確認提示視窗。
4. 在提示視窗中，確認刪除位址空間。

使用網路互動圖

網路互動圖是裝置之間發現的互動的直覺顯示。您可以使用網路互動圖來檢視有關各個時間段的裝置互動的資訊。

要檢視網路互動圖：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
2. 前往**網路互動圖**索引標籤。

   顯示網路互動圖。

以下物件可以顯示：

- 節點。這些物件代表網路封包的傳送者和接收者。
- 裝置群組。這些物件與裝置群組樹中的群組相對應。群組包含代表這些群組及其子群組中裝置的節點。
- 連結。這些物件代表節點之間的互動作用。

節點和連結根據一定時期內從流量或Endpoint Agent取得的資料出現在網路互動圖上。裝置組連續顯示。

您可以篩選節點和連結。預設情況下，網路互動圖以一小時的定義過濾期即時顯示物件。

網路互動圖可顯示最多 1000 個連線。

在網路互動圖上，可以突出顯示存在問題的物件。應用程式認為以下物件存在問題：

- 節點，如果其具有未處理的事件，且分數為 4.0 或更高，或它代表具有*未授權*狀態的裝置。
- 連接，如果其與分數為 4.0 或更高的事件有關。僅考慮在給定的物件篩選期間註冊的事件。事件的目前狀態未被考慮在內。
- 一個群組，如果它包含存在問題的裝置，或者這個群組中的節點具有存在問題的連結。考慮的物件可以屬於群組本身，也可以屬於任何嵌套層級的子群組。

網路互動圖上的節點

網路互動圖上的節點可以具有以下類型：

- 應用程式已知的裝置。此類型的節點代表裝置表中列出的裝置。
- 應用程式未知的裝置。此類型的節點代表具有唯一 IP 或 mAC 位址且未在裝置表中列出的裝置。這樣的節點可能出現在網路互動圖上，例如，如果您使用 `ping` 指令向不存在的裝置傳送網路封包。如果應用程式無法辨識的裝置節點總數（根據網路互動圖上的目前篩選設定）不超過 100，則會單獨顯示這些節點。如果存在更多這樣的裝置，則未知裝置由單個節點聯合表示。

顯示在代表應用程式已知的裝置的節點上的資訊

對於代表應用程式已知的裝置的節點，在最大縮放比例下，網路互動圖上會顯示以下資訊：

- 指定的裝置名稱。
- 裝置類別的圖示。
- 裝置的 IP 位址（如果沒有 IP 位址，則顯示 MAC 位址）。
- 根據以下條件的各種圖示：
  - 裝置是否設定“路由器”屬性
  - 裝置上是否安裝了 Endpoint Agent（圖示的顏色取決於其連線狀態）
  - 裝置是否具有*已存檔*狀態
- 節點左邊框上的粗線採用下列顏色之一，取決於裝置的安全狀態：
  - 綠色表示*正常*安全狀態
  - 黃色表示*警告*安全狀態
  - 紅色表示*嚴重*安全狀態

如果裝置具有*未授權*狀態或裝置的安全狀態不是*正常*，則節點的背景為紅色。

顯示在代表應用程式未知的裝置的節點上的資訊

對於代表應用程式未知的裝置的節點，在最大縮放比例下，網路互動圖上會顯示以下資訊：

- 如果節點代表單個未知裝置，則顯示該裝置的 IP 或 mAC 位址。如果節點代表多個未知裝置（一個節點包含超過 100 個應用程式未知的裝置），則會顯示**未知裝置**。
- 未知裝置及其狀態的圖示 。

代表應用程式未知的裝置的節點具有灰色背景。

網路互動圖上的裝置群組

屬於裝置群組樹的群組可以在網路互動圖上折疊或展開。折疊的群組顯示為類似於節點的圖示。擴充的群組顯示為包含節點和其他群組的框。

折疊組中顯示的資訊

如果某個群組被折疊，則當網路互動圖最大化時會顯示以下資訊：

- 群組的名稱。
- 網路互動圖上滿足目前過濾設定的裝置數量。此群組及其所有子群組中所有嵌套層級的裝置均被考慮在內。
- 所有嵌套層級的子群組的數量。

如果某個群組包含存在問題的裝置或連結（包括任何嵌套層級的子群組），則該群組的邊框將顯示為紅色。展開的群組上顯示的資訊

延伸組的框包含一個帶有群組名稱的標題列和一個用於顯示物件的區域。群組框顯示此群組中包含的裝置，以及其下嵌套層級的子群組。在群組中包含的裝置中，只有符合目前過濾設定的裝置才會顯示在網路互動圖上。

如果某個群組包含存在問題的裝置或連結（包括任何嵌套層級的子群組），則該方塊具有紅色背景。

折疊和展開組

您可以透過雙擊群組圖示來展開折疊的群組。您可以透過雙擊該群組框的標題列或點擊標題列中的來折疊展開的組。

若要同時展開多個折疊的組：

1. 在網路互動圖上，透過執行下列操作之一來選擇多個折疊組：
   - 按住**SHIFT**鍵，然後使用滑鼠選擇一個包含要選擇的群組的矩形區域。
   - 按住**CTRL**鍵並點擊要選擇的每個折疊組。
2. 點擊位於網頁互動圖顯示區域左側的工具列中的（如果選擇了至少一個折疊組，則該按鈕可用）。

要同時折疊所有展開的群組：

點擊位於網路互動圖顯示區域左側的工具列中的（如果至少展開了一個群組，則該按鈕可用）。

網路互動圖上的連結

根據偵測到的網路封包來識別網路互動圖上的連接，可以將該網路封包的來源位址和目標位址對應到節點的位址。

每個連結代表互動的雙方。連結中的通訊方可能是網路互動圖上的下列物件之一：

- 下列類型之一的節點：
  - 應用程式已知的裝置。
  - 應用程式未知的裝置。
  - 未知裝置的公用節點（如果連結顯示與此節點內的一個或多個未知裝置的互動）。
- 如果連結顯示與該群組中一個或多個裝置的互動，則為折疊的群組。

根據偵測互動時註冊的事件的分數，連結可以顯示為彩色線：

- 灰色表示互動未導致記錄任何事件或僅導致記錄分數為 0.0–3.9 的事件。
- 紅色表示互動已導致分數為 4.0 至 10.0 的事件被記錄。

對於連接，僅考慮在給定的物件篩選期間內註冊的事件。事件的目前狀態未被考慮在內。

應用程式將連結資訊儲存在 Central Node 上的資料庫中。儲存記錄的總量不能超出配置的限制。如果數量超出限制，應用程式會自動刪除 10% 的最舊記錄。在 Central Node 上配置資料儲存設定時，您可以設定網路互動圖的最大數量限制。

檢視物件詳細資訊

有關網路互動圖上顯示的物件的詳細資訊顯示在詳細資訊區域中。要顯示詳細資訊，您可以用滑鼠選擇一個物件（如果要檢視某個群組的詳細資訊，必須先折疊該群組）。

對於節點，將顯示以下資訊：

- 如果該節點代表應用程式已知的裝置，則詳細資訊區域將顯示與裝置表中相同的資訊。
- 如果節點代表應用程式未知的單個裝置，則詳細資訊區域將顯示裝置的 MAC 和/或 IP 位址（如果已新增額外的位址空間，則顯示位址空間的名稱）。
- 若選擇未知裝置的公用節點，則顯示下列資訊：
  - 考慮到目前的篩選設定，此節點包含的節點數。
  - **IP 位址**顯示未知裝置的 IP 位址數量和前 100 個 IP 位址（如果應用程式中新增了額外的位址空間，則顯示位址空間名稱）。如果某些未知的裝置節點具有 IP 位址，則會顯示此部分。
  - **MAC 位址**顯示未知裝置的 MAC 位址數量和前 100 個 MAC 位址（如果應用程式中新增了額外的位址空間，則顯示位址空間名稱）。如果某些未知的裝置節點具有 MAC 位址，則會顯示此部分。

對於群組，將顯示以下資訊：

- **父群組**顯示裝置組樹中群組的路徑。如果該組位於層次結構的頂層，則顯示**N/A（這是一個頂層組）**。
- 此群組及其所有嵌套層級的子群組中的裝置數量。
- 有關所選組及其所有嵌套層級的子群組中存在問題的物件的數量的資訊。如果不存在這樣的物件，則安全狀態顯示為*正常*。

對於連接，將顯示以下資訊：

- **嚴重程度**是與連結相關的事件的最高嚴重程度對應的圖示。如果沒有與連結關聯的事件，則顯示**無事件**。僅考慮在給定的物件篩選期間註冊的事件。事件的目前狀態未被考慮在內。
- 包含互動的第一方和第二方基本資訊的部分：
  - 如果未知裝置節點是互動的一方，則此部分顯示裝置的名稱或位址、類別和位址資訊（而對於應用程式已知的裝置，僅顯示參與互動的網路介面的位址資訊）。對於已知裝置，也會顯示裝置狀態。
  - 如果折疊群組是互動的一方，則此部分將顯示該群組的名稱以及它包含的裝置和子群組的數量。
  - 若未知裝置的公用節點是互動的一方，則此部分顯示節點的名稱、**未知裝置**、以及此節點所代表的節點數。
- **協定**是一個包含參與互動的協定清單的部分。對於每種協議，都會指示傳輸的資料量，該量是根據偵測到的網路封包計算得出的。如果互動的一方是未知裝置的公用節點，則不顯示該部分。

縮放網路互動圖

網路互動圖可以按 1–100% 的比例顯示。目前比例值顯示在位於網路互動圖顯示區域左側的工具列中。

若要變更網頁互動圖的比例，請執行以下操作：

使用滑鼠滾輪或位於目前比例值旁邊工具列中的 **+** 和 **–** 按鈕。

減少網路互動圖的比例會減少顯示節點和折疊組的資訊量。

當縮放等級低於 25% 時，圖示和文字資訊會隱藏在節點和折疊群組中。節點和折疊組的顯示變化如下：

- 在代表應用程式已知的裝置的節點上，裝置狀態在右上角顯示為彩色三角形：
  - 綠色表示裝置具有*已授權*狀態。
  - 紅色表示裝置具有*未授權*狀態。
  - 灰色表示裝置具有*已存檔*狀態。
- 在折疊的組上，右上角的三角形表示有問題的物件。此三角形填滿下列顏色之一：
  - 如果該群組不包含需要注意的物件，則顯示為綠色。
  - 如果該群組包含存在問題的物件，則顯示紅色。

定位網路地圖

如有必要，您可以手動或自動變更網路互動圖的位置。自動定位可讓您移動網路互動圖並變更其比例以顯示滿足定義的過濾器設定的所有節點以及所有擴充組。

若要手動定位網路互動圖：

1. 將滑鼠游標放置在網路互動圖上未被物件佔據的任何部分。
2. 按一下並按住滑鼠左鍵拖曳網路互動圖。

若要自動定位網路互動圖：

點擊互動圖顯示區域左側工具列中的按鈕。

網路互動圖的定位和比例將發生變化，以顯示所有節點和擴展組。

固定和取消固定節點和群組

預設情況下，節點和折疊組未固定在網路互動圖上。取消固定的節點和折疊的群組可以自動移動，以最佳化其他物件的顯示。

當節點和群組的定位被手動改變或在自動分配過程中發生變化時，它們將被固定。您也可以固定顯示的物件而不移動它們。

若要固定或取消固定物件而不移動它們，您可以使用下列控制項：

- 網路互動圖顯示區域左側工具列中的按鈕。您可以使用 和 按鈕固定或取消固定網路互動圖上顯示的所有節點和群組（包括擴充組中的節點）。
- 擴展組框的標題列中的按鈕。您可以點擊 或者 僅固定或取消固定擴充組框中（但不是在巢狀組框中）的節點和組。

如果網路互動圖包含可以套用對應動作的物件，則這些按鈕可用。

固定節點或摺疊群組的定位後， 圖示會出現在該元素的右上角（如果網路互動圖的比例不小於 25%）。您也可以使用此圖示取消固定物件。

固定的節點或群組留在原處。如果固定節點從網路互動圖中消失（例如，由於過濾），則該節點下次出現時將顯示在相同位置。

手動重新排列節點和群組

您可以以最方便的方式排列網路互動圖上的節點和群組，手動變更它們的位置。

已移動的節點和群組將被固定到新的位置。如有必要，您可以取消固定它們。

群組中包含的物件只能在該群組的框範圍內移動。

若要重新排列節點和/或折疊組：

1. 在網路互動圖上，選擇一個或多個與節點和/或折疊群組相對應的物件。

若要選擇多個節點和/或折疊群組，請執行下列操作之一：

- 按住 **SHIFT** 鍵，然後使用滑鼠選擇一個包含要選擇的物件的矩形區域。
- 按住 **CTRL** 鍵並點擊要選擇的每個物件。

2. 將選取的物件拖曳到您想要放置它們的位置。

節點和折疊組在移動後仍保持固定狀態。這些物件上會新增 圖示。

要重新定位展開的群組：

點擊展開的群組框的標題列並將其拖曳到新位置。

自動排列節點和群組

為了在網路互動圖上實現物件的最佳排列，您可以使用演算法自動變更節點和群組的位置（排列）。提供以下演算法：

- 徑向排列
- 與網格對齊

您可以將自動排列演算法套用至下列物件：

- 群組樹中層次結構頂層的所有顯示的節點和群組。使用位於網頁互動圖顯示區域左側的工具列中的 （徑向排列）按鈕和 （網格對齊排列）按鈕進行自動排列。
- 擴展組內顯示的所有節點和組。若要執行自動排列，您可以點擊擴充組框的標題列中的 （徑向排列）和 （與網格對齊）按鈕。
- 僅選定的節點和折疊的群組。在自動排列之前，您必須選擇展開群組內或層次結構頂層的至少三個節點和/或折疊群組。要選擇多個物件，您可以按住 **SHIFT** 鍵並在必要的物件周圍繪製一個選擇框，或者您可以按住 **CTRL** 鍵並點擊來選擇多個物件。使用位於網頁互動圖顯示區域左側的工具列中的 （徑向排列）按鈕和 （網格對齊排列）按鈕進行自動排列。

已自動排列的節點和群組將固定到新的位置。這些物件上會新增 圖示。如有必要，您可以取消固定它們。

在網路互動圖上搜尋節點

您可以根據有關節點的資訊在網路互動圖上搜尋這些節點。所有符合目前篩選條件的節點，包括折疊群組內的節點和網路互動圖顯示地區以外的節點。

對於表示應用程式已知的裝置的節點，將透過裝置表的所有欄位（**狀態**、**安全狀態**、**上次檢視**、**上次修改**和**建立時間**除外）執行搜尋。搜尋也是透過裝置自訂欄位的值來執行的。

如果找到與搜尋查詢相符的節點，則這些節點的輪廓將以黃色突出顯示。包含找到的節點的折疊組的輪廓以相同的方式突出顯示。同時，**“搜尋節點”**欄位右側出現以下元素：

- 搜尋結果中目前選定的物件（找到的節點或包含找到的節點的折疊組）的序數。
- 找到的物件（節點和/或包含找到的節點的折疊組）的總數。

  找到的物件總數不考慮折疊組中的節點數。如果您希望群組中的節點計入搜尋結果總數，請展開折疊的群組。

- 在找到的物件之間移動的箭頭。您可以按照名稱的字母順序在找到的物件之間移動。當移動到下一個物件時，網路互動圖會自動定位以顯示該物件。

若要在網路互動圖上尋找節點：

篩選網路互動圖上的物件

本節提供有關過濾網路互動圖上的物件以限制顯示的節點和連結數量的說明。

節點和連結的全面篩選

本節包含節點和連結全面篩選的說明。

使用時間線上的期間進行篩選

要篩選節點和連接，您可以在時間線上選擇一個時間段。時間軸顯示在網路互動圖視窗的下部。

時間軸包含以下元素：

- 時間軸的開始日期和時間。
- 記錄分數為 4.0 及以上的事件的時間段。這些時間段在刻度尺的下部顯示為紅色條。如果配置的時間軸長度超過七天，則不會顯示時間段。
- 篩選時間段。此時間段顯示為一條黃色條，兩端帶有拖曳手柄。
- 應用程式處理的流量圖。如果配置的時間軸長度超過七天，則不會顯示圖表。
- 時間軸的結束。根據篩選時間段，時間軸的結束會顯示為日期和時間（如果已指定日期和時間），或顯示為**現在**連結。

以下類型的篩選時間段是可能的：

- 以當下時刻為參考的時間段。這樣一個時間段的右端與當下時刻對應的時間線的右端重合。
- 不參考當下時刻的時間段。此類時間段可放置在時間軸的任何位置。

若要配置參考目前時刻按時間段篩選物件：

1. 點擊時間軸右側的**現在**按鈕。如果已經參考目前時刻定義了時間段，則不會顯示此按鈕。

2. 如果要指定不同的時間段長度，請執行下列其中一項操作：

   - 將黃色時間段條的左端拖曳到所需位置（時間段最大長度為 7 天）。

   - 點擊黃色時間段條上方的按鈕以開啟設定視窗，選取**錨定到邊界**核取方塊，然後選擇持續時間（**小時**、**天**、**7 天**），再點擊**確定**。

   網路互動圖僅顯示從指定時間段開始到目前時刻偵測到通訊的節點和連接。

若要配置按時間段進行篩選而不參考目前時刻：

1. 如果您要設定的時間段超出了時間軸的範圍，請變更時間軸的開始和/或結束日期和時間：

   a. 若要變更時間軸的開始日期和時間，請點擊時間軸左側的連結以開啟一個視窗，然後在該視窗中選擇以下選項之一：

      - **天**。

      - **7 天**。

      - **30 天**。

      - **設定日期**。對於此選項，請在開啟的欄位中指定日期和時間。

   b. 若要變更時間軸的結束日期和時間，請點擊時間軸右側的連結以開啟一個視窗，然後在該視窗中選擇以下選項之一：

      - **現在**。

      - **指定日期**。對於此選項，請在開啟的欄位中指定日期和時間。

2. 設定您想要的時間段。為此，請執行以下操作之一：

   - 將時間線上的時間段拖曳到您想要的位置。

   - 將時間線上黃色時間段條的一端或兩端移到您想要的時間段位置（時間段的最大長度為 7 天）。

   - 點擊黃色時間段條上方的按鈕以開啟設定視窗，然後選擇持續時間（**小時**、**天**、**7 天**）並點擊**確定**。

3. 如果時間段自動錨定到目前時刻（當您將時間段移動到最右側位置時，時間軸右側的**現在**按鈕不再顯示），且您不希望如此，請停用自動錨定。為此，請點擊黃色時間段條上方的按鈕以開啟設定視窗，取消選取**錨定到邊界**核取方塊，然後點擊**確定**。

按已註冊事件篩選

您可以設定網路互動圖以顯示與所選節點相關的事件中儲存其資訊的節點和連結。

如果在網路互動圖上選擇的節點不超過 200 個，則可以按事件進行過濾。您可以單獨選擇節點，也可以選擇包含所需裝置的折疊組的一部分。當您選擇一個折疊的群組時，所有嵌套層級的子群組中的所有裝置也會被選取。

您可以使用以下方式按事件進行篩選：

- 按事件進行初步篩選。使用此方法可以按僅與選取節點相關的事件篩選物件。
- 按事件進行附加篩選。如果已經執行了按事件進行的初步過濾（例如，從事件表切換到網路互動圖時），並且您還需要從網路互動圖上顯示的節點清單中過濾與另外選擇的節點相關的事件，則套用此方法。

若要根據初始事件篩選顯示節點和連結：

1. 在網路互動圖上，選擇一個或多個節點和/或折疊群組。

   若要選擇多個節點和/或群組，請執行下列操作之一：

   - 按住 **SHIFT** 鍵，然後使用滑鼠選擇一個包含要選擇的物件的矩形區域。
   - 按住 **CTRL** 鍵並點擊要選擇的每個物件。

2. 在網路互動圖上方的工具列中，開啟**事件篩選器**下拉清單。
3. 在下拉清單中，選擇**篩選器**。

網路互動圖僅顯示其資訊包含在與所選節點相關的事件中的節點和連結。位於網路互動圖上方的工具列顯示一個包含事件 ID 的清單（ID 按偵測到其相關事件的順序列出）。

若要使用按事件進行的附加篩選將節點和連結新增至顯示的物件：

1. 確保已按事件執行了初始篩選。為此，請檢查網路互動圖上方的工具列中是否有包含事件 ID 的清單。
2. 在網路互動圖上顯示的節點中，選擇您想要在過濾器中新增關聯事件的節點。

   詳細資訊區域顯示在 Web 介面視窗的右側。

3. 在網路互動圖上方的工具列中，開啟**事件篩選器**下拉清單。
4. 在下拉清單中，選擇**新增至篩選器**。

網路互動圖還顯示與所選節點相關的事件中包含其資訊的節點和連結。偵測到的事件的 ID 被新增到工具列中的 ID 清單中。

節點過濾

本節提供有關過濾節點的說明。

按裝置狀態篩選節點

若要按裝置狀態篩選節點：

1. 在網路互動圖上方的工具列中，開啟**裝置狀態**下拉清單。

   將顯示一個清單，其中包含應用程式已知裝置的狀態名稱（*未授權*、*已授權*、*已存檔*），以及應用程式無法識別之裝置的*未知裝置*狀態。

2. 在下拉清單中，選擇要用作網路互動圖上顯示的節點的篩選條件的狀態核取方塊。

3. 點擊**確定**。

網路互動圖僅顯示與所選狀態的裝置相對應的節點。

按裝置安全狀態篩選節點

若要依裝置安全狀態篩選節點：

1. 在網路互動圖上方的工具列中，開啟**裝置狀態**下拉清單。
   將顯示一個清單，其中包含裝置的安全狀態名稱（*正常*、*警告*、*嚴重*）。

2. 在下拉清單中，選取需要在網路互動圖上顯示的節點的安全狀態的核取方塊。

3. 點擊**確定**。

網路互動圖僅顯示與所選安全狀態的裝置相對應的節點。

按裝置類別篩選節點

若要按裝置類別篩選節點：

1. 在網路互動圖上方的工具列中，開啟**裝置類別**下拉清單。
   將顯示一個清單，其中包含應用程式已知的裝置類別名稱以及未知裝置的特殊類別。

2. 在下拉清單中，選擇要用作網路互動圖上顯示的節點的篩選條件的類別的核取方塊。

3. 點擊**確定**。

網路互動圖僅顯示與所選類別的裝置相對應的節點。

顯示並隱藏連結到已篩選節點的節點

過濾節點後，網路互動圖僅顯示滿足定義的過濾設定的節點。此外，要使節點顯示在網路互動圖上，它必須與另一個顯示的節點有連線（連結）。如果根據指定的過濾參數，網路互動圖未顯示與某個節點互動的任何節點，則該節點也不會顯示在網路互動圖上。篩選以相同的方式套用於未知裝置的公用節點：如果不是所有與未知裝置節點有互動的節點，則該節點被排除在未知裝置的公用節點的節點清單之外。

如有必要，您可以啟用網路互動圖來顯示與過濾節點相關的所有節點。所有曾經互動過的節點都會和篩選後的節點一起顯示（無論目前的篩選條件如何）。

若要顯示或隱藏與已篩選節點關聯的節點：

使用網路互動圖上方工具列中的**“連結裝置”**切換開關。

篩選連結

本節提供有關過濾連結的說明。

按嚴重性分數篩選連接

要根據嚴重性分數過濾網路互動圖上的連結：

1. 在網路互動圖上方的工具列中，開啟**連結分數**下拉清單。

   將顯示事件嚴重性等級和範圍的清單：低（0.0–3.9）、中（4.0–7.9）、高（8.0–10.0）；以及**無事件**項，其可讓您篩選沒有註冊事件的連結。

2. 在下拉清單中，選取要按其進行篩選的嚴重性等級的核取方塊。

3. 點擊**確定**。

網路互動圖僅顯示與具有所選嚴重性等級的事件相關的連結。

按通訊協定篩選連接

若要按通訊協定過濾網路互動圖上的連結：

1. 在網路互動圖上方的工具列中，開啟**協定**下拉清單。

   這將開啟一個視窗，其中顯示以協議堆疊樹形式顯示的協議表。您可以使用包含下一層協定的協定名稱旁邊的**+**和**-**按鈕來控制樹節點的顯示。

   表列包含以下資訊：

   - **協定**是協定堆疊樹中協定的名稱。
   - **EtherType** 是由乙太網路協定封裝的下一層協定編號（如果該協定有指定的編號）。以十進制格式顯示。
   - **IP 編號**是由 IP 協定封裝的下一層協定編號（如果該協定有指定的編號）。僅為屬於 IP 協定結構的協定指定。以十進制格式顯示。

2. 如有必要，請使用表格上方的搜尋欄來尋找所需的協議。

3. 在協定清單中，選取要在搜尋條件中使用的協定的核取方塊。

   如果選取或清除包含巢狀協定的協定的核取方塊，則也會自動選取或清除所有巢狀協定的核取方塊。

4. 點擊**確定**。

網路互動圖僅顯示使用所選協定的連結。

按 OSI 模型層篩選連接

您可以按照與 Open Systems Interconnection (OSI) 網路協定棧的層相對應的互動層來篩選連結。

要根據 OSI 網路模型的層次過濾網路互動圖上的連接，請執行以下操作：

1. 在網路互動圖上方的工具列中，開啟 **OSI 模型層**下拉清單。

將顯示 OSI 模型層名稱清單：

- **資料連結**。此層包括使用 MAC 位址與裝置通訊的連線。
- **網路**。此層包括使用 IP 位址與裝置通訊的連線。

2. 在下拉清單中，選取其連結需要在網路互動圖上顯示的 OSI 模型層的核取方塊。
3. 點擊**確定**。

只有屬於所選 OSI 模型層的連結才會顯示在網路互動圖上。

重置篩選條件

您可以將指定的節點和連結篩選條件重設為其預設條件。

若要重設網路互動圖上定義的過濾器設定，請執行下列操作：

在網路互動圖上方的工具列中，點擊“**預設篩選器**”（如果指定了非預設篩選條件，則顯示該按鈕）。

網路互動圖將顯示在指定時間內偵測到通訊的所有節點和連結。

儲存和載入網路互動圖的顯示設定

本節包含管理網路互動圖的顯示設定的資訊。

應用程式可讓您儲存網路互動圖的目前顯示設定。一組可儲存的顯示設定稱為*視圖*。您可以使用視圖套用已儲存的網路互動圖的顯示設定（例如，在進行某些變更後快速還原顯示設定，或在不同電腦上使用網路互動圖）。

當儲存了網頁互動圖視圖時，會儲存以下顯示設定：

- 縮放等級
- 網路互動圖定位
- 固定節點和群組的位置
- 節點和連結的篩選

您最多可以儲存並使用 10 個視圖。

只有具有“管理員”角色的使用者可以管理視圖清單（包括將目前顯示設定儲存為視圖）。然而，所有具有“管理員”、“安全稽核員”、“資深安全員”和“安全官”角色的使用者都可以檢視視圖清單並將視圖套用到網路互動圖。

新增視圖並儲存網路互動圖的目前顯示設定

若要i新增視圖並儲存網路互動圖的目前顯示設定

1. 使用**管理員**憑據登入 Kaspersky Anti Targeted Attack Platform Web 介面。
2. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
3. 前往**網路互動圖**索引標籤。
4. 點擊**管理視圖**按鈕開啟**設定網路地圖視圖**視窗。
5. 點擊**新增**。
6. 在文字方塊中輸入檢視的名稱。
   您可以使用字母、數字、空格字元以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   視圖名稱必須符合以下要求：
   - 以空格以外的任意字元開始和結束。
   - 最多包含 100 個字元。
   - 不重複使用另一個視圖的名稱（不區分大小寫）。
7. 點擊文字方塊右側的✓圖示。

重新整理視圖並儲存網路互動圖的目前顯示設定

若要更新視圖並儲存網路互動圖的目前顯示設定

1. 使用**管理員**憑據登入 Kaspersky Anti Targeted Attack Platform Web 介面。
2. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
   前往**網路互動圖**索引標籤。
3. 點擊**管理視圖**按鈕開啟**設定網路地圖視圖**視窗。
4. 選擇要儲存目前網路互動圖顯示設定的視圖。
5. 點擊“**覆蓋**”。
   這將開啟一個確認提示視窗。
6. 在提示視窗中確認儲存所選視圖中的目前設定。

重新命名網路互動圖視圖

若要重新命名視圖：

1. 使用**管理員**憑據登入 Kaspersky Anti Targeted Attack Platform Web 介面。
2. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
3. 前往**網路互動圖**索引標籤。
4. 點擊**管理視圖**按鈕開啟**設定網路地圖視圖**視窗。
5. 選擇要重新命名的視圖。
6. 點擊目前視圖名稱右側的圖示。
7. 在文字方塊中輸入視圖的新名稱。
   您可以使用字母、數字、空格字元以及以下特殊字元：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   視圖名稱必須符合以下要求：
   - 以空格以外的任意字元開始和結束。
   - 最多包含 100 個字元。
   - 不重複使用另一個視圖的名稱（不區分大小寫）。
8. 點擊文字方塊右側的圖示。

刪除網路互動圖視圖

若要刪除視圖：

1. 使用**管理員**憑據登入 Kaspersky Anti Targeted Attack Platform Web 介面。
2. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
3. 前往**網路互動圖**索引標籤。
4. 點擊**管理視圖**按鈕開啟**設定網路地圖視圖**視窗。
5. 選擇您想刪除的視圖。
6. 點擊**刪除**。
   這將開啟一個確認提示視窗。
7. 在提示視窗中確認刪除所選視圖。

將視圖中儲存的設定套用至網路互動圖

若要將視圖中儲存的設定套用到網路互動圖：

1. 使用**管理員**憑據登入 Kaspersky Anti Targeted Attack Platform Web 介面。
2. 在應用程式 Web 介面視窗中，選擇"**網路地圖**"區域。
3. 前往**網路互動圖**索引標籤。
4. 點擊**管理視圖**按鈕開啟**設定網路地圖視圖**視窗。
5. 在清單中，選擇您要套用的視圖。
6. 點擊**套用**。
   這將開啟一個確認提示視窗。
7. 在提示視窗中，確認套用所選的視圖。

監控網路工作階段

Kaspersky Anti Targeted Attack Platform 可以掃描流量以偵測裝置所建立的用於連線其他裝置的網路工作階段。應用程式註冊偵測到的網路工作階段並儲存資訊，可協助您分析裝置的網路活動並從流量傾印檔案下載傳輸的網路封包的資料。與網路互動圖上的連結不同，註冊的網路工作階段允許您獲得有關裝置互動的更細粒度的資訊，部分原因是對用於互動的不同連接埠和協議的工作階段進行了獨立註冊。

如果對資產管理技術啟用了網路工作階段偵測方法，則應用程式會偵測網路工作階段。在分析到達監控點的流量時以及接收來自 Endpoint Agent 元件的資訊時可以執行網路工作階段偵測。

每個註冊的網路工作階段都包含有關參與互動的兩個裝置之間的連線的資訊。網路工作階段的特徵在於互動方的位址資訊（MAC 和/或 IP 位址）、連接埠號以及用於連線的應用程式協定。網路工作階段中的第一個裝置通常是發起向其他裝置傳送網路封包的裝置。

您可以在*Kaspersky Anti Targeted Attack Platform 偵測到的協定*部分中檢視 Kaspersky Anti Targeted Attack Platform 偵測到的完整協定清單。

如果一分鐘內沒有傳送任何網路封包，或相關節點或監控點上的網路工作階段偵測技術已停用，則認為網路工作階段已關閉。

當偵測到過多的網路工作階段時，應用程式將應用以下工作階段註冊限制：

- 使用同一應用程式協定的兩方互動方之間註冊的工作階段數每分鐘不得超過 1000 個。
- 雙方註冊的工作階段總數每分鐘不得超過 5000 次。

該應用程式將有關網路工作階段的資訊儲存在 Central Node 伺服器上的資料庫中。儲存記錄的總量不能超出配置的限制。如果數量超出限制，應用程式會自動刪除10% 的最舊記錄。

在分佈式解決方案和多組織用戶模式下，SCN 伺服器的網路工作階段資訊不會顯示在 PCN 上。

網路工作階段表

若要檢視網路工作階段清單：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
2. 前往“**網路工作階段**”索引標籤。

   顯示網路工作階段表。

表包含以下資訊：

- **狀態**是網路工作階段的狀態。註冊的網路工作階段可以具有以下狀態之一：
  - **活動**。在註冊網路工作階段時會指派此狀態，並且只要裝置在此工作階段內持續傳送網路封包，此狀態就會保留。
  - **已關閉**。如果一分鐘內沒有傳送任何網路封包，或相關節點或監控點上的網路工作階段偵測技術已停用，則將此狀態指派給網路工作階段。
- **面 1**是網路互動一端的 MAC 和/或 IP 位址。可以開啟或關閉 MAC 和 IP 位址的顯示。
- **面 1 連接埠**是互動第一端的連接埠號碼。
- **面 2**是網路互動的另一端的 MAC 和/或 IP 位址。可以開啟或關閉 MAC 和 IP 位址的顯示。
- **面 2 連接埠**是互動的第二端的連接埠號碼。
- **裝置 1**是應用程式已知的裝置名稱，對應的是互動第一方的位址資訊。
- **裝置 2**是應用程式已知的裝置名稱，對應的是互動的第二方的位址資訊。
- **傳輸協定**是網路工作階段中使用的傳輸協定的名稱。
- **應用協定**是網路工作階段中使用的應用層協定的名稱。
- **目前速度**是網路工作階段的目前資料傳輸速率。
- **平均速度**是網路工作階段的平均資料傳輸速率。
- **總傳輸量**是網路工作階段期間傳輸的位元組數。
- **監控點**列出了已接收網路工作階段流量的監控點的名稱。
- **開始**是網路工作階段中第一個網路封包的日期和時間，或是由 EPP 應用程式的資料定義的時間段的開始日期和時間。
- **最後一次互動**是網路工作階段中最後一個網路封包的日期和時間，或者是由 EPP 應用程式的資料定義的時間段的結束日期和時間（如果在網路工作階段中僅收到一個封包，則該值與**開始**相同）。
- **封包數**是網路工作階段期間傳輸的網路封包的數量。

檢視網路工作階段表時，您可以設定、篩選和排序網路工作階段，以及導覽至相關項目和匯出資料。

檢視網路工作階段詳細資訊

有關網路工作階段的詳細資訊包括來自網路工作階段表的資訊，以及啟動網路工作階段時處於活動狀態的應用程式的名稱（如果 Kaspersky Anti Targeted Attack Platform 能夠確定應用程式的名稱）。

若要檢視網路工作階段的詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
2. 前往“**網路工作階段**”索引標籤。
3. 點擊與相關工作階段相關的行。

   這將開啟一個視窗，其中包含有關網路工作階段的資訊。

下載網路工作階段流量

檢視網路工作階段表時，您可以下載與所選網路工作階段相關的流量。流量以 PCAP 檔案形式下載。為了僅下載您需要的資料，您可以設定網路封包篩選。

應用程式從流量傾印檔案儲存下載網路工作階段的流量。可以從 Sensor 安裝過程中自動建立的內部儲存以及已連線的外部儲存下載流量。

下載網路工作階段流量時，請考慮以下事項：

- 僅可下載分析到達監控點的流量時註冊的網路工作階段的流量。如果網路工作階段是根據從 Endpoint Agent 元件收到的資訊註冊的，則您無法下載此類工作階段的流量。
- 流量傾印檔案暫時儲存在儲存中，並隨著新流量的到來自動刪除（輪換週期取決於流量量和應用程式儲存配置）。如果相應的流量傾印檔案已從儲存中刪除，則您無法下載網路工作階段的流量。

若要下載網頁工作階段流量：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。
2. 前往“**網路工作階段**”索引標籤。
3. 選取您想要下載其流量的網路工作階段旁的核取方塊。

   您最多可以選擇 100 個網路工作階段。
4. 點擊**下載流量**。

   詳細資訊區域顯示在 Web 介面視窗的右側。
5. 執行以下操作：

   - 如果您想要下載特定時間內的流量，請使用**流量下載期限**設定來設定界限。

     預設情況下，選擇最長可能的期限，從建立最早網路工作階段的日期和時間開始，到選擇的最新工作階段結束的日期和時間結束。如有必要，您可以在此期限內移動邊界，或為其中一個邊界設定空值（例如，為右邊界設定空值以下載尚未結束的工作階段的新流量）。

- 在**下載量限制**下，設定最大下載流量。

  如果下載的流量超過指定的限制，則會丟棄最新的流量。

- 如有必要，請在**按監控點篩選**下啟用篩選，並指定獲得所需流量的監控點。

  預設情況下，指定取得選定網路工作階段的流量的監控點。

- 如有必要，請在**按位址空間篩選**部分中啟用篩選，並指定所選網路工作階段的網路封包中的位址所屬的位址空間（如果向應用程式新增其他位址空間，則會顯示此部分）。

  預設情況下，指定在應用程式中建立的所有位址空間。

- 如有必要，請在**使用 BPF 篩選**下啟用篩選，並輸入使用 BPF（Berkeley Packet Filter）技術透過所選網路工作階段的網路封包中的位址參數進行篩選的表達式。

  篩選表達式的範例：
  `tcp port 102 or tcp port 502`

- 如有必要，請在**使用正規表達式篩選**下啟用篩選，並輸入正規表達式，以便根據所選網路工作階段的網路封包的有效負載資料進行篩選。

  篩選表達式範例：
  `^test.+xABxCD`

6. 點擊**下載**。

您的瀏覽器儲存了下載的檔案。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。

搜尋網路封包

您可以尋找並檢視與所選網路封包相關的流量。如果有必要，您可以下載發現的流量的傾印。

若要尋找與選定的網路封包相關的流量：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。

2. 轉到“**網路工作階段**”索引標籤。

3. 點擊“**在封包中搜尋**”。

   這將開啟帶有網路封包搜尋設定的視窗。

4. 執行以下操作：

   - 在“**要下載的流量期限**”欄位中，設定您想要搜尋網路封包的範圍。

   - 如有必要，請在“**使用 BPF 篩選**”下啟用篩選，並輸入使用 BPF（Berkeley Packet Filter）技術透過所選網路工作階段的網路封包中的位址參數進行篩選的表達式。BPF 篩選表達式的寫入格式為 libpcap。有關語法的更多詳細資訊，請參閱“pcap-filter 手冊頁”。

     篩選表達式的範例：
     `tcp port 102 or tcp port 502`

- 如有必要，請在“**使用正規表達式篩選**”部分啟用篩選，並輸入基於網路封包中的有效負載資料進行篩選的表達式。

  篩選表達式範例：
  `^test.+xABxCD`

- 如果需要，請在“**按監控點篩選**”下啟用篩選，並指定要從中取得流量的監控點。

- 如有必要，請在“**按位址空間篩選**”下啟用篩選，並指定網路封包中的位址所屬的位址空間。

5. 點擊“**搜尋**”。

   表格顯示符合篩選條件的資料。

6. 如果您想要下載找到的網路封包的傾印，請點擊“**下載**”。

原始網路流量傾印以 PCAP 格式下載。

預先配置網路封包搜尋規則

您可以使用使用 BPF 和正規表達式的預先設定規則在流量中進行搜尋。

若要使用預先配置規則搜尋網路封包：

1. 在應用程式 Web 介面視窗中，選擇“**網路地圖**”區域。

2. 轉到“**網路工作階段**”索引標籤。

3. 點擊“**在封包中搜尋**”。

   這將開啟帶有網路封包搜尋設定的視窗。

4. 在“**要下載的流量期限**”欄位中，設定您想要搜尋網路封包的範圍。

5. 在下表中，從**使用 BPF 進行篩選**或**使用正規表達式進行篩選**欄複製篩選表達式，並將其貼到 Web 介面中用於搜尋網路封包的對應區段。

6. 點擊“**搜尋**”。

表格顯示符合篩選條件的資料。

預先配置的規則如下表所列。

規則目的	使用 BPF 進行篩選	使用正規表達式進行篩選
按 IP 位址搜尋流量	host <位址>	
搜尋兩台主機之間的流量	host <位址 1> and host <位址 2>	
搜尋單個 TCP 工作階段的流量	tcp <連接埠 1> and host <位址 1> and tcp <連接埠 2> and host <位址 2>	
按多個 IP 位址搜尋流量	host <位址1> or host <位址 2> or host <位址N>	
尋找來自一組主機的所有 DNS 查詢	udp and dst port 53 and (src host <位址 1> or src host <位址 2> or src host <位址 N>)	
搜尋 HTTP 流量		" HTTP/"
搜尋 DNS 流量	udp dst port 53 or tcp dst port 53	
使用針對特定網域的 GET 請求搜尋 HTTP 流量	tcp port 80 or tcp port 8000 or tcp port 8080 or tcp port 8888	GET.{1,1000}<網域>
搜尋特定主機的 ICMP 流量	icmp and host <位址>	
搜尋以純文字傳輸的身分驗證資料	tcp port 80 or tcp port 8000 or tcp port 8080 or tcp port 8888 or port ftp or port smtp or port imap or port pop3 or port telnet	"pass=|pwd=|log=|login=|user=|username=|pw=|passw=|passwd=|password=|pass:|user:|username |user|VXNlcm5hbWU6|UGFzc3dvcmQ6|LOGIN |USER|PASS "
搜尋主機作為用戶端的 TCP 工作階段	tcp[tcpflags] = tcp-syn and host <address>	

規則目的	使用 BPF 進行篩選	使用正規表達式進行篩選
在給定子網路中搜尋 HTTP 流量	`net xx.xx.xx.xx/yy and (port 8080 or port 80)`	
搜尋本機互動流量	`ip and src net (10 or 172.16/12 or 192.168/16) and dst net (10 or 172.16/12 or 192.168/16)`	
搜尋與網路上物件互動的流量	`ip and not (src net (10 or 172.16/12 or 192.168/16) and dst net (10 or 172.16/12 or 192.168/16)) and not multicast and not broadcast and not net 169.254/16`	
根據 HTTP 流量中的 UserAgent 欄位搜尋流量	使用者代理：	

Kaspersky Anti Targeted Attack Platform 偵測到的協定

Kaspersky Anti Targeted Attack Platform 偵測到的協定如下表所示。

Kaspersky Anti Targeted Attack Platform 偵測到的協定

類別	協議
鏈路層協定	ARP
	RARP
	Ethernet I
	Ethernet II
	MPLS
	MPLS multi
	STP
	LLDP

類別	協議
網路層協定	IPv4
	IPv6
	IPv6 encapsulated
	IPX
	IS-IS 透過 IP
	IS-IS 透過 Ethernet I
	IS-IS 透過 Ethernet II
	Loopback
	DHCP
	VRRP
傳輸層協定	TCP
	UDP
	SCTP
	GRE
	ICMP
	IGMP
	PIM
	PRP
	QTP 透過 UDP
遠端存取和管理	RDP
	SSH
	Telnet
	RLOGIN 透過 TCP
	RSH 透過 TCP
	VNC
	AeroAdmin
	AmmyyAdmin
	AnyDesk
	TeamViewer 透過 TCP
	TeamViewer 透過 UDP
	遠端實用程式
	Srv Tcp DameWare Mini Remote Control
	Radmin 透過 TCP

類別	協議
資料傳輸	AFP 透過 TCP
	FTP 透過 TCP
	Tftp 透過 TCP
	Tftp 透過 UDP
	SFTP 透過 TCP
	SMB 透過 UDP
	Smb2 透過 TCP
	Smb2 透過 UDP
	Smb3 透過 TCP
	Smb3 透過 UDP
	BitTorrent
	NFS
名稱和網路服務解析	DNS
	DNS LLMNR 透過 TCP
	DNS LLMNR 透過 UDP
	mDNS 透過 UDP
郵件協定	IMAP
	POP3
	SMTP
時間同步	NTP
	PTP
身分驗證和目錄	Kerberos
	LDAP
	LDP 透過 UDP
	RADIUS
Web 協定和安全	HTTP 透過 TCP
	HTTPS
	WebSocket
	安全通訊端層
通訊協定	VoIP: SIP
	IRC
	MSNP 透過 TCP
	MSNP 透過 UDP
多媒體與串流媒體	Flash Media Server 透過 TCP
	Voice IP：SIP
	MQTT
雲端和檔案共用服務	DropBox sync 透過 UDP
	Napster 透過 TCP

類別	協議
服務和診斷協議	ICMP
	Syslog
	Ident 透過 TCP
	SNMP
路由和高可用性	HSRP 透過 UDP
	GLBP 透過 UDP
	RIP
	EIGRP
隧道和 VPN	L2TP
	PPTP 透過 TCP
	Tor 透過 TCP
	Tor 透過 UDP
應用程式和資料庫	Microsoft SQL
	MySQL
	Oracle
	DB2
	Tns 透過 TCP
	Tns 透過 UDP
偵測	SSDP 透過 UDP
工作階段層協定	NetBIOS 透過 TCP
	NetBIOS 透過 UDP
輔助協議	Finger 透過 TCP
專門的協議	Bitcoin 透過 TCP

監控風險

Kaspersky Anti Targeted Attack Platform 可以偵測資訊系統資源所面臨的風險。應用程式根據流量分析結果和接收到的裝置資訊識別風險。

偵測到的風險可屬於以下類別：

- 弱點。偵測到的裝置弱點屬於此類別。
- 配置問題。此類別包括因配置不正確而導致的安全風險，以及在寫入和讀取裝置配置時洩漏資料的風險。
- 不安全的網路架構。此類別包括與偵測到的不安全的網路互動、裝置、協定和軟體相關的風險；由於授權裝置處於非活動狀態而導致的風險；以及由於 EPP 應用程式在裝置上不存在或未完全發揮作用而導致的風險。

每個風險的評分從 0.0 到 10.0。在計算風險評分時，應用程式會考慮與偵測到的風險相關的裝置的可用資訊。在計算分數時，應用程式會考慮裝置的重要等級以及與該裝置相關的其他風險。*基準分數*被用作計算的初始值。弱點類別中風險的基本評分遵循通用弱點評分系統(CVSS)。其餘風險類別，基本分數取自風險類型表。

風險資訊被上傳到 Central Node 上的偵測到的風險資料庫。資料庫中儲存的記錄總數不能超過指定的限制。如果數量超出限制，應用程式會自動刪除10% 的最舊記錄。您可以在配置儲存設定時設定偵測到的風險資訊的最大大小。

偵測到的風險資料庫的內容顯示在應用程式 Web 介面的“**風險**”部分。您也可以在“**資產**”部分的“**裝置**”索引標籤上檢視裝置風險概述。

關於弱點類別中的風險

當應用程式偵測到企業 LAN 上受監控裝置中的弱點時，就會記錄弱點風險。*弱點*是裝置軟體或硬體中的缺陷，攻擊者可以利用該缺陷破壞資訊系統或取得未經授權的資訊存取。

應用程式透過分析可用的裝置資訊來偵測弱點。可以幫助識別裝置已知弱點的資訊將與*已知弱點資料庫*中的某些欄位進行比較。已知弱點的資料庫已內建於應用程式中。該資料庫由卡巴斯基專家維護，包含有關最相關或最常見的裝置弱點的資訊。

已知弱點資料庫包含弱點的描述以及受這些弱點影響的裝置的描述。此外，該資料庫還以文字或公用資源連結的形式包含防護系統的建議。已知弱點資料庫包含來自各種來源（可能包括裝置和軟體供應商以及各種安全組織）的描述和建議。資料庫中的描述和建議都是英文的。

應用程式安裝後，使用原有的已知弱點資料庫。您可以透過安裝更新來保持資料庫最新。

Kaspersky Anti Targeted Attack Platform 將有關裝置的可用資訊與已知弱點資料庫中描述受弱點影響的裝置的欄位進行比較。應用程式使用以下裝置資訊來偵測弱點：

- **硬體供應商**。
- **硬體型號**。
- **硬體版本**。
- **軟體供應商**。如果在裝置資訊中找不到軟體供應商資訊，Kaspersky Anti Targeted Attack Platform 將重複使用**硬體供應商**值。
- **軟體名稱**。如果在裝置資訊中找不到軟體名稱，Kaspersky Anti Targeted Attack Platform 將重複使用**硬體型號**值。
- **軟體版本**。

在已知弱點資料庫中，裝置描述以 CPE (Common Platform Enumeration) 格式儲存。應用程式將可用的裝置資訊與這些描述進行比較，自動將資訊轉換為 CPE 格式。對於每個弱點，符合描述的內容會列在風險詳細資訊區域的**符合的 CPE**部分中。

識別弱點的主要參數是其在 Common Vulnerabilities and Exposures (CVE) 清單中的 ID。此識別號稱為*CVE ID*。如果弱點尚未有 CVE ID，則指定從其他公用資源取得的帶有弱點描述的 ID。

Kaspersky Anti Targeted Attack Platform 支援取得俄羅斯聯邦技術和出口管制局（FSTEC）在資訊安全威脅資料庫（以下也稱為“BDU”）中提供的弱點ID 和描述連結。如果下載的弱點資訊包含來自 FSTEC's BDU 的此類資訊，則應用程式會以“BDU:<year> -<number>“格式的對應 ID 的形式顯示此資訊。

持續風險管理流程的實施方案

風險偵測功能允許在您的資訊系統中實施持續（週期性）風險管理。為了幫助您管理風險，Kaspersky Anti Targeted Attack Platform 提供了有關偵測到的風險的資訊，您可以使用這些資訊採取必要的補救或緩解措施。

持續風險管理流程的實施方案涉及以下步驟：

1. **清點裝置清單**

   此步驟使用裝置活動偵測和裝置資訊偵測方法執行（必須啟用這些方法）。此步驟，應用程式會自動偵測新裝置並更新裝置資訊。如果未自動偵測到網路上的某些裝置，則需要手動新增它們或從外部項目匯入它們。

   您必須在裝置設定中啟用自動更新，以取得確定裝置分類和操作特性的所有資訊（例如，型號和軟體版本）。如果由於某種原因無法自動更新此類資訊，則必須手動保持此資訊的最新狀態。

2. **被動或主動掃描時的風險偵測**

   應用程式使用有關裝置的可用資訊被動掃描裝置是否有風險。應用程式還分析公司 LAN流量中的網路互動以偵測風險。風險偵測透過風險偵測方法實現（必須啟用該方法）。

   您也可以主動輪詢裝置以快速取得其資訊。在對裝置進行主動輪詢時，如果選擇了相應的風險分析方法，您還可以偵測特定類型的風險。若要主動輪詢裝置，您需要為應用程式新增一個或多個**主動輪詢**連線器。

   在更新應用程式已知弱點資料庫後，或新增或更新用於匹配的裝置資訊後（例如，儲存軟體型號和版本資訊後），會自動偵測弱點類別的風險。

3. **對偵測到的風險進行評分和分類**

   對於偵測到的每一個風險，應用程式都會計算一個分數。分數反映風險的嚴重程度。根據分數，風險的嚴重程度可以是*低*（分數 0.0–3.9）、*中*（分數 4.0–7.9）或*高*（分數 8.0–10.0）。

   根據嚴重性等級和分數，並考慮到資訊系統中裝置的特殊使用方式，您可以根據重要性對偵測到的風險進行分類。如果您評估風險不大，則可以手動變更其狀態，將*活動*狀態（偵測後預設指派）變更為*已接受*狀態，例如，如果無法重現利用弱點的先決條件。當改變風險狀態時，我們建議新增或編輯評論。

   所有需要採取措施的風險都應保持*活動*狀態。

4. **補救措施**

   在此步驟中，您必須對偵測到的風險採取補救或緩解措施。為此，請檢查偵測到的所有*活動*風險，從分數最高的風險開始。在您的資訊系統中採取必要的措施（例如，修補裝置的弱點，安裝修復該弱點的軟體更新，如果不可能，則將該裝置與外部網路隔離）。對於某些風險（例如，弱點），提供了建議操作的資訊。

   > Kaspersky Anti Targeted Attack Platform 不參與修復偵測到的風險。

5. **驗證補救措施**

   此步驟與掃描時的風險偵測類似。完成此步驟後，風險表中將不再有任何*活動*風險。

   對於應用程式在被動掃描期間偵測到的大多數風險（例如，弱點），如果偵測這些風險的條件不再滿足，應用程式將自動指派*已修復*狀態。例如，在裝置的軟體版本發生變更後，應用程式會將因先前指定的弱點軟體版本而註冊的弱點風險指派為*已修正*狀態。*已修復*狀態也被指派給已知弱點資料庫中不再具有描述的風險（如果下載更新後從資料庫中刪除了描述）。

   當裝置被移除時，應用程式也會刪除與這些裝置相關的風險。

   如果修復後，偵測風險的條件沒有改變（例如，存在弱點的裝置與外部網路隔離，但是該裝置的資訊沒有改變），則可以手動將*已接受*狀態指派給此風險。當改變風險狀態時，我們建議新增或編輯評論。

   某些風險無法自動指派*已修正*狀態（例如，無法將*已修正*自動指派給在裝置主動輪詢期間偵測到的風險）。對於此類風險，您還必須在風險補救完成後手動指派*已接受*狀態。

   如果某個風險與某個事件相關聯，您可以在將事件狀態變更為*已解決*的同時為該風險指派*已接受*狀態。

檢視風險表

風險表顯示在應用程式 Web 介面視窗的**風險和異常**部分。

風險設定顯示在表格以下列中：

- **類別**。

  風險類別的名稱。

- **名稱**。

  風險名稱。對於弱點類別的風險，使用偵測到的弱點的 CVE ID（如果沒有 CVE ID，則顯示從其他帶有弱點描述的公用資源中取得的 ID）。

- **CVE**。

  對於弱點類別的風險：偵測到的弱點的 CVE ID。

- **BDU**。

  對於弱點類別的風險：BDU 資料庫中弱點的 ID。如果具有不同 BDU ID 的多個弱點與具有 CVE ID 的一個弱點相對應，則該欄位會列出所有此類 ID。

- **風險 ID**。

  風險的唯一 ID。

- **分數**。

  計算出的風險評分。該數值決定了風險的嚴重程度。根據嚴重級別，分數可以用以下顏色之一顯示：

  - 紅色表示*高*嚴重等級風險。
  - 黃色表示*中*等嚴重等級風險。
  - 藍色表示*低*嚴重等級風險。

  對於*活動*風險，分數的顏色很鮮豔。對於*已修復*或*已接受*風險，分數顏色較淡。

  在詳細資料區域中，此設定稱為**基本分數**。

- **面 1**。

  網路互動一方的位址資訊（針對某些風險類型有提示）。可以分別開啟或關閉 MAC 位址和 IP 位址的顯示。如果在應用程式中新增了額外的位址空間，則在設定風險表時，可以使用**顯示位址空間**設定啟用或停用位址空間名稱的顯示。

- **面 2**。

  網路互動另一方的位址資訊（針對某些風險類型有提示）。位址資訊的顯示可以按照與**面 1**列相同的方式配置。

- **裝置組**。

  偵測到風險的裝置所在群組的名稱（包含群組本身的名稱及其所有父群組的名稱）。

- **裝置**。

  裝置的名稱和位址。

- **來源**。

  對於弱點類別的風險：將其資訊上傳到已知弱點資料庫的來源的名稱。在詳細資訊區域中，此設定稱為**弱點來源**。

- **狀態**。

目前風險狀態。可以有以下狀態：

- 首次偵測到風險時，預設會指派*活動*狀態（如果風險已被指派*已修復*狀態，則在重複偵測時也會指派）。如果風險目前狀態為*已接受*，您也可以手動為風險指派*活動*狀態。
- 如果偵測風險的條件不再滿足，則會自動指派*已修復*狀態。
- 如果風險評估為無關緊要，或所採取的補救措施沒有導致自動分配*已修復*狀態，則可以手動將*已接受*狀態指派給風險。

- **偵測於**。

  偵測到風險的日期和時間。

- **最後狀態變更**。

  上次風險狀態變更的日期和時間。

- **匹配的 CPE**。

  對於弱點類別的風險：儲存在已知弱點資料庫中的裝置描述。這些是與裝置表中的裝置資訊相符的描述。

檢視風險表時，您可以設定、篩選、搜尋和排序檔案，以及導航至相關項目。

檢視風險資訊

風險詳情包括風險表中的資訊以及以下欄位：

- **風險類型**是風險類型的代碼。
- **描述**是針對風險類型或弱點指定的描述。
- **基礎分數**是計算風險分數的初始值。

對於弱點類別的風險，以下欄位和欄位群組中會顯示附加資訊：

- **CVSS 向量**是用於計算 CVSS 弱點分數的指標記錄。
- **攻擊條件**是對弱點被利用所必須滿足的條件的描述。
- **影響**是利用弱點可能造成的後果的描述。
- **緩解**列出了修復弱點的建議（例如，有關建議在裝置上安裝某個軟體版本的資訊）。
- **連結**列出了可以提供有關該弱點的更多資訊的公用資源的連結。
- **CVE 歷史**列出了弱點被識別、確認和在公用來源中發布的日期。

若要檢視風險資訊：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**裝置**”索引標籤。
3. 點擊**風險**欄中的弱點名稱（CVE ID 或其他弱點 ID）。

   這將開啟一個視窗，其中包含有關弱點的資訊。

手動變更風險狀態

在管理“**風險和異常**”區段時，您可以手動將任何風險的狀態從*活動*變更為*已接受*，反之亦然。在管理“**資產**”區段時，您只能變更弱點類別風險的狀態，並且只能從*活動*變更為*已接受*。

在將*已解決*狀態指派給與該風險關聯的事件時，您也可以將*已接受*狀態指派給風險。

若要手動變更風險狀態：

1. 開啟風險詳情區域或風險詳情視窗。
2. 開啟**變更狀態**下拉清單。
3. 根據您想要指派給風險的狀態，從下拉清單中選擇以下選項之一：
   - 如果您想將風險狀態從*活動*變更為*已接受*，請選擇**已接受**。
   - 如果您想將風險重新指派為*活動*狀態，請選擇**活動**。

   這將開啟一個確認提示視窗。
4. 如果選定的風險具有相關事件，並且您想要同時將*已解決*狀態指派給所有這些事件，請勾選**將“已解決”狀態指派給所有相關事件**核取方塊。

   當使用資產管理技術註冊某些類型的事件時，風險可能會與事件相關。
5. 在提示視窗中，點擊**確定**。

使用裝置表時檢視風險詳細資訊

使用裝置表時，您可以檢視有關在裝置上偵測到的風險的資訊。對於每個具有弱點類別風險的裝置，都會顯示偵測到的弱點的名稱（作為 CVE ID 或其他弱點 ID）。如果在裝置上偵測到其他類別的風險，則會顯示該裝置的這些風險類別名稱。當選擇裝置時，弱點名稱和風險類別將顯示在**風險**欄位和詳細資料區域中。

預設情況下，裝置表僅顯示有關*活動*風險的資訊。如有必要，您可以在配置裝置表時勾選**顯示已修復和已接受的風險**核取方塊以顯示所有風險的資訊。

為了表明風險的嚴重等級，弱點和類別的名稱採用以下顏色：

- 紅色表示*高*嚴重等級風險。
- 黃色表示*中等*嚴重等級風險。
- 藍色表示*低*嚴重等級風險。

對於*活動*風險，名稱的顏色很鮮豔。對於*已修復*或*已接受*的風險，名稱的顏色較暗。

如果裝置存在相同類別的風險，則該類別的名稱將以所有風險中嚴重等級最高的顏色顯示。

如果您想檢視風險詳情，可以點擊弱點名稱和類別名稱。點擊弱點名稱（作為 CVE ID 或其他弱點 ID）將開啟弱點詳細資訊視窗。點擊風險類別名稱將前往經過篩選的風險表，顯示該裝置所選類別的風險。

檢視裝置表時，您可以根據風險篩選裝置。您也可以透過弱點名稱（作為 CVE ID 或其他弱點ID）搜尋裝置。

配置 NDR 事件類型

*事件類型*決定註冊事件時使用的參數：標題、描述、基本分數和註冊設定。在 Kaspersky Anti Targeted Attack Platform 中，您可以檢視事件類型的設定、編輯某些事件類型的設定、配置自動儲存流量和透過連線器轉送已註冊事件。

檢視事件類型表

應用程式中提供的事件類型顯示在應用程式 Web 介面的**設定**部分、**事件類型**子部分中。

事件類型表包含*系統事件類型*。這些事件類型是由應用程式在安裝過程中建立的，不能從清單中刪除。應用程式中實現的事件註冊技術使用不同的系統事件類型集。

在某些系統事件類型的基礎上，您可以設定*使用者定義的事件設定*，以便在特定情況下註冊事件時使用。可以為外部系統技術的事件類型（代碼 4000005400）定義使用者定義的設定，以便使用NDR API註冊事件。

註冊事件時，使用者定義的設定優先。如果沒有使用者定義的設定，則使用系統事件類型中配置的設定。

以下設定可用於事件類型：

- **代碼** – 事件類型的唯一編號（識別碼）。在事件類型表中，編號會與事件標題一起顯示在**代碼和標題**欄位中。在已註冊事件表中，事件類型 ID 顯示在**事件類型**欄位中。
- **標題** – 以文字和/或變數形式呈現的事件標題的內容。系統事件類型可以使用僅特定於這些類型事件的變數，或一般變數，這些也可以在使用者定義的設定中使用。在事件類型表中，標題的內容會與事件類型編號一起顯示在**代碼和標題**欄位中。在已註冊事件表中，標題文字和/或接收的變數值顯示在**標題**欄位中。
- **基本分數** – 用於計算註冊事件的分數的初始值。如果一個事件類型可以有不同的基本分數，則會顯示最大值。此設定顯示在事件類型表中。
- **技術** – 用於事件註冊的技術。此設定顯示在事件類型表中。

- **描述** – 描述事件類型的附加文字。與標題類似，可以包含變數。此設定不會顯示在事件類型表中。您可以在所選事件類型的詳細資訊區域中檢視描述。在已註冊事件表中，描述文字和/或變數結果值顯示在**描述**欄位中。

- **<收件者連線器名稱>** – 應用程式用於將事件轉送至第三方系統的連線器的名稱。該應用程式僅向第三方系統傳送配置為透過連線器傳送的類型的事件。每個連線器（透過此連線器配置將事件轉送到第三方系統）都顯示在風險類型表的單獨欄位中。此設定不會顯示在所選事件類型的詳細資訊區域中。

- **事件再生期** – 事件再次註冊所需的最長時間。如果在指定的時間段過去之前重複事件註冊的條件，則不註冊新的事件，但是會增加先前註冊的事件的重複次數的計數器，並且會更新事件最後發生的日期和時間。在此期限結束後，當註冊事件的條件再次出現時，應用程式將註冊該類型的新事件。再生期從最後一次註冊此類事件的時刻開始計算。例如，如果再生週期設定為 8 小時，並且註冊此事件的條件在前一個事件發生兩小時後再次出現，則不會註冊新事件。如果在 8 小時或更晚之後偵測到該情況，則會記錄新事件。此設定不會顯示在事件類型表中。您可以在所選事件類型的詳細資訊區域中檢視和設定此設定。

  對於已註冊的事件，再生期可能比配置的早到期。如果事件被指派了*已解決*狀態，或 Central Node 電腦重新啟動，則允許在設定的時間之前重複註冊事件。

- **儲存流量** – 此設定啟用或停用在註冊事件時自動儲存流量。此設定不會顯示在事件類型表中。您可以在所選事件類型的詳細資訊區域中檢視和設定此設定。

  如果停用了流量的自動儲存，則可以在註冊此類事件後一段時間手動下載流量。當應用程式收到下載流量的請求時，它會在其臨時產生的流量傾印檔案中搜尋網路封包。如果在流量傾印檔案中找到必要的網路封包，則下載這些封包（首先儲存在資料庫中）。

檢視事件類型表時，您可以使用設定、篩選、搜尋和排序功能。

編輯系統事件類型的設定

若要編輯系統事件類型的設定：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”部分、“**事件類型**”子部分。
2. 在事件類型表中，選擇您要編輯的事件類型。

   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊“**編輯**”。
4. 編輯可編輯的設定：再生週期和流量節省設定。
5. 點擊**儲存**。

配置自動儲存系統事件類型的流量

當編輯事件類型時，您可以啟用或停用註冊事件時自動儲存流量的功能。如果啟用了流量節省，資料庫將儲存導致事件註冊的網路封包，以及在註冊事件的網路工作階段中偵測到的事件註冊之前和之後的封包。流量節省設定決定要節省多少網路封包以及時間限制。

如果某個事件類型的自動流量節省功能已停用，且該事件類型配置了啟用流量節省的使用者定義的設定，則您只能在註冊該類型的事件後的特定時間範圍內下載流量。在這種情況下，應用程式使用流量傾印檔案來下載流量。這些檔案會被暫時儲存，並會在新流量到達時自動刪除。從這些檔案下載流量時，當您為事件類型啟用流量儲存時，資料庫中將儲存與預設配置相同的網路封包。

> 只有當註冊事件時，應用程式才會在資料庫中儲存流量。如果在再生期間再次出現註冊此事件的條件，則該時刻的流量不會儲存在資料庫中。

您可以為任何事件類型啟用和配置流量節省。

如果為聚合事件（即系統事件類型 8000000001）啟用了流量節省，則應用程式在註冊聚合事件時會儲存所有嵌套事件的流量。儲存嵌套事件的流量時，將套用為聚合事件指定的設定。但是，直接為聚合事件中嵌套的事件類型指定的流量節省設定將覆蓋為聚合事件指定的設定。也就是說，嵌套事件的流量會按照針對這些事件類型指定的設定進行儲存，如果沒有指定此類設定，則使用聚合事件的設定。

若要為事件類型啟用和配置流量節省：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”部分、“**事件類型**”子部分。
2. 在事件類型表中，選擇您要編輯的事件類型。

   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊“**編輯**”。
4. 將“**儲存流量**”切換開關設定為“*已啟用*”。
5. 配置事件註冊之前的流量儲存。為此，請在“**事件前的封包總數**”和/或“**到事件發生的時間（毫秒）**”中指定相關值。零表示未套用該設定。如果在這兩個欄位中都指定了值，則應用程式將儲存與指定值之一相符的最小數量的封包。
6. 配置事件註冊後的流量儲存。為此，請在“**事件後的封包總數**”和/或“**事件後的時間（毫秒）**”中指定相關值。零表示未套用該設定。如果在這兩個欄位中都指定了值，則應用程式將儲存與指定值之一相符的最小數量的封包。

   > 對於某些技術（特別是深度包偵測），註冊後在事件中儲存的封包可能比流量節省設定中配置的要少。這是由於流量監控技術的特殊性所造成的。
7. 點擊**儲存**。

配置透過連線器轉送事件

配置系統事件類型時，您可以指定希望 Kaspersky Anti Targeted Attack Platform 將已註冊事件轉送至第三方系統的連線器。Kaspersky Anti Targeted Attack Platform 可以同時透過多個連線器傳送事件資訊。

若要設定透過連線器將事件轉送到第三方系統：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”部分、“**事件類型**”子部分。
2. 確保事件類型表顯示帶有您需要的連線器的列。

   如果缺少相關連線器的列，請檢查列顯示設定。如果連線器尚未被新增到連線器清單中，請新增它。

3. 在事件類型表中，選擇要啟用或停用透過連線器轉送的事件類型。
   如果您選擇單個事件類型，則詳細資料區域將顯示在 Web 介面視窗的右側。

4. 執行以下操作之一：

   - 如果您選擇一種事件類型，請點擊詳細資料區域中的**選擇連線器**。
   - 如果選擇多種事件類型，請點擊視窗上部的**選擇連線器**。

   這將開啟**事件收件者連線器**視窗。

5. 選取要將事件轉送到第三方系統的連線器旁的核取方塊。

6. 點擊**確定**。

Kaspersky Anti Targeted Attack Platform 中的常見替換變數

您可以使用通用變數來替代 Kaspersky Anti Targeted Attack Platform 中的目前值。您可以在以下設定中使用常用變數：

- 事件註冊的使用者定義的設定中的事件標題和描述
- 使用電子郵件連線器的事件轉發、應用程式資訊或稽核記錄的設定

若要將通用變數插入輸入欄位中：

開始以$ 字元開頭輸入變數的名稱，然後從顯示的清單中選擇通用變數。

通用變數可用於不同設定中的內插，取決於變數的用途（請參閱下表）。

變數	敘述	用法
`$communications`	網路互動描述字串（每個網路互動一個字串），指定網路封包的協定以及傳送者和接收者的位址	• 用於註冊事件的使用者定義的設定。 • 透過連線器轉發事件的設定。
`$dst_address`	網路封包接收者位址（根據協定提供的資訊，可以是 IP 位址、連接埠號、MAC 位址和/或其他位址資訊）	• 用於註冊事件的使用者定義的設定。
`$extra.<paramName>`	使用 `AddEventParam` 功能為外部系統或 Lua 指令碼新增的附加變數	• 用於註冊事件的使用者定義的設定。
`$monitoring_point`	其流量導致事件被註冊的監控點的名稱	• 用於註冊事件的使用者定義的設定。 • 透過連線器轉發事件的設定。
`$occurred`	註冊的日期和時間	• 用於註冊事件的使用者定義的設定。 • 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$protocol`	記錄事件的應用程式層協定的名稱	• 用於註冊事件的使用者定義的設定。
`$src_address`	網路封包傳送者位址（根據協定提供的資訊，可以是 IP 位址、連接埠號、MAC 位址和/或其他位址資訊）	• 用於註冊事件的使用者定義的設定。
`$technology_rule`	事件中規則的名稱。	• 用於註冊事件的使用者定義的設定。 • 透過連線器轉發事件的設定。
`$top_level_protocol`	頂級協議的名稱。	• 用於註冊事件的使用者定義的設定。
`$type_id`	事件類型、應用程式資訊或稽核條目的代碼。	• 用於註冊事件的使用者定義的設定（也可以使用 `$event_type_id` 變數）。 • 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$closed`	指派*已解決*狀態時的日期和時間或事件重新產生期間的日期和時間（對於非聚合事件的事件），或事故中包含的最後一個事件的註冊日期和時間（對於聚合事件）。	• 透過連線器轉發事件的設定。
`$count`	巢狀事件或聚合事件被觸發的次數	• 透過連線器轉發事件的設定。
`$description`	敘述	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$id`	已註冊事件、應用程式訊息或稽核條目的唯一 ID。	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$message_category`	已傳輸資料的類別（事件、應用程式訊息或稽核記錄）。	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$message_count`	傳輸的事件、應用程式訊息或稽核記錄的數量。	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$messages`	由包含資料清單的區塊組成的範本。	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$msg_line_templ`	電子郵件通知字串範本	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$node`	包含傳送資料的已安裝應用程式元件的節點。	• 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
`$result`	稽核條目中的操作結果。	• 透過連線器轉發稽核條目的設定。
`$score`	事件分數值。	• 透過連線器轉發事件的設定。
`$severity`	事件嚴重性等級。	• 透過連線器轉發事件的設定。
`$status`	應用程式訊息狀態	• 透過連線器轉發應用程式訊息的設定。
`$system_process`	導致訊息被註冊的應用程式處理程序	• 透過連線器轉發應用程式訊息的設定。
`$technology`	與事件相關的技術。	• 透過連線器轉發事件的設定。

$title	事件標題、訊息文字或已註冊的操作。	• 透過連線器轉發事件的設定。 • 透過連線器轉發應用程式訊息的設定。 • 透過連線器轉發稽核條目的設定。
$user	執行註冊的操作的使用者的名稱。	• 透過連線器轉發稽核條目的設定。

NDR 事件註冊技術

Kaspersky Anti Targeted Attack Platform 使用下列技術之一來記錄 NDR 事件：

- *入侵偵測* (IDS)

  此技術會記錄與偵測流量異常相關的 NDR 事件，這些異常是攻擊的指標（例如，NDR 事件可以記錄偵測到 ARP 欺騙的指標）。

- *外部* (EXT)

  此技術註冊 Kaspersky Anti Targeted Attack Platform 使用 NDR API 的方法從第三方系統接收的聚合和巢狀 NDR 事件。

- *資產管理* (AM)

  此技術會註冊涉及偵測流量中或從 EPP 應用程式接收的資料中的裝置資訊的 NDR 事件（例如，當發現裝置具有新的 IP 位址時，可以註冊 NDR 事件）。

- *端點防護平台* (EPP)

  該技術會為防護工作站和伺服器的卡巴斯基應用程式偵測到的威脅註冊 NDR 事件（例如，惡意軟體偵測事件）。

Kaspersky Anti Targeted Attack Platform 中的系統事件類型

為了註冊事件，Kaspersky Anti Targeted Attack Platform 使用在應用程式安裝期間自動建立的系統事件類型。

每種事件類型都屬於一種特定的事件註冊技術。

入侵偵測技術的系統事件類型

本文介紹了入侵偵測技術的系統事件類型（見下表）。

入侵偵測 (IDS) 系統事件類型

代碼	事件類型標題	註冊條件
4000003000	來自 $fileName 集（系統規則集）的規則被觸發	來系統規則集的入侵偵測規則被觸發。 事件類型的標題和描述中使用了以下變數： • $fileName：規則集的名稱 • $category：規則的類別 • $ruleName：規則的名稱 • $signature_id：規則的 ID（sid）

代碼	事件類型標題	註冊條件
4000003001	來自 $fileName 集（使用者自訂規則集）的規則被觸發	來自使用者自訂規則集的入侵偵測規則被觸發。 事件類型的標題和描述中使用了以下變數： • $fileName：規則集的名稱 • $category：規則的類別 • $ruleName：規則的名稱 • $signature_id：規則的 ID（sid） • $action：規則中定義的網路封包操作類型（Kaspersky Anti Targeted Attack Platform 中不執行 丟棄 或 拒絕 操作）
4000003002	偵測到暴力攻擊或掃描的跡象	偵測暴力破解或掃描攻擊的規則被觸發。 在事件類型描述中，$ruleName 變數用於規則名稱。
4000004001	在 ARP 回復中偵測到 ARP 欺騙的症狀	偵測到 ARP 封包中存在位址欺騙的跡象：多個與 ARP 請求無關的 ARP 對應。 事件類型的描述中使用了以下變數： • $senderIp: 被欺騙的 IP 位址 • $targetIp：目標主機的 IP 位址 • $attackStartTimestamp：偵測到第一個 ARP 對應的時間
4000004002	在 ARP 請求中偵測到 ARP 欺騙的症狀	偵測到 ARP 封包中存在位址欺騙的跡象：從同一MAC 位址向不同目的地發出的多個 ARP 請求。 事件類型的描述中使用了以下變數： • $senderIp: 被欺騙的 IP 位址 • $targetIp：目標主機的 IP 位址 • $attackStartTimestamp：偵測到第一個 ARP 對應的時間
4000005100	偵測到 IP 協定異常: 組裝 IP 封包時發生資料衝突	偵測到 IP 協定異常：重疊 IP 封包片段中的資料不符。
4000005101	偵測到 IP 協定異常: 超過碎片 IP 封包大小	偵測到 IP 協定異常：重新組裝後碎片 IP 封包的實際總大小超出允許的限制。
4000005102	偵測到 IP 協定異常: IP 封包的初始片段的大小小於預期	偵測到 IP 協定異常：IP 封包的初始片段的大小小於允許的最小值。
4000005103	偵測到 IP 協定異常: 誤相關片段	偵測到 IP 協定異常：正在組裝的 IP 封包的片段包含有關碎片封包長度的不同資訊。
4000002701	偵測到 TCP 協定異常: 重疊 TCP 段中的內容替換	偵測到 TCP 協定異常：封包包含不同內容的重疊 TCP 段。
4000000003	測試事件 (IDS)	偵測到測試網路封包（啟用了基於規則的入侵偵測）。

資產管理技術的系統事件類型

本文介紹了資產管理技術的系統事件類型（見下表）。

資產管理(AM) 技術的系統事件類型

代碼	事件類型標題	註冊條件
4000005003	偵測到位址為 ' + $owner_ip_or_mac + ' 的新裝置'	當資產監控處於監控模式時，會透過偵測到的 IP 或 mAC 位址自動新增裝置，而表中的其他裝置則未指定該位址。 應用程式在註冊該事件的時候，可能會同時為該裝置註冊**未經授權的裝置**風險。在這種情況下，風險和事件之間建立了關係。 事件類型的標題和描述中使用了以下變數： • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址 • $asset_name – 裝置的指定名稱 • $assigned_mac – 指派的 MAC 位址（如果已定義） • $owner_ip – 分配的 IP 位址（如果已定義） • $asset_id – 裝置的 ID
4000005004	收到關於位址為 ' + $owner_ip_or_mac + ' 的裝置的新資訊	當資產監控處於監控模式時，裝置資訊會根據從流量收到的資訊自動更新。 事件類型的標題和描述中使用了以下變數： • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址 • $asset_name – 裝置名稱 • $updated_params – 更新資訊清單 • $asset_id – 裝置的 ID

代碼	事件類型標題	註冊條件
4000005005	偵測到 IP 位址衝突$owner_ip	當資產監控處於監控模式時，偵測到指定 IP 位址的裝置未使用該 IP 位址。 事件類型的標題和描述中使用了以下變數： • $owner_ip – IP 位址 • $challenger_asset_name – 使用該 IP 位址的裝置名稱 • $challenger_mac – 使用該 IP 位址的裝置的 MAC 位址 • $asset_name – 在其設定中指定了該 IP 位址的裝置的名稱 • $owner_mac – 在其設定中指定了該 IP 位址的裝置的 MAC 位址 • $challenger_ips_list：使用該 IP 位址的裝置的其他IP 位址清單 • $asset_id – 在其設定中指定了該 IP 位址的裝置的 ID • $challenger_id – 使用該 IP 位址的裝置的 ID
4000005006	偵測到來自位址 $owner_ip_or_mac 的流量，該位址被指派給具有"已存檔"狀態的裝置	當資產監控處於監控模式時，或根據從 EPP 應用程式收到的資料，偵測到具有"*已存檔*"狀態的裝置活動。 應用程式在註冊該事件的時候，可能會同時為該裝置註冊**未經授權的裝置**風險。在這種情況下，風險和事件之間建立了關係。 事件類型的標題和描述中使用了以下變數： • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址 • $asset_name – 裝置名稱 • $last_seen_timestamp – 裝置最後一次出現在網路中的日期和時間 • $asset_id – 裝置的 ID
4000005007	偵測到具有 MAC 位址 $owner_mac 的裝置的新IP 位址 $new_ip_addr	當資產監控處於監控模式時，偵測到裝置使用的新IP 位址。 事件類型的標題和描述中使用了以下變數： • $new_ip_addr – 偵測到的 IP 位址 • $owner_mac – 裝置的 MAC 位址 • $asset_name – 裝置名稱 • $owner_ips_list – 裝置的其他 IP 位址清單 • $asset_id – 裝置的 ID
4000005008	新的 MAC 位址（$owner_mac）被新增到 IP 位址為 $owner_ip 的裝置	在資產管理監控模式下，僅指定了 IP 位址的網路介面（裝置處於*未授權*或*已存檔*狀態），會自動新增 MAC 位址。 事件類型的標題和描述中使用了以下變數： • $owner_mac – 偵測到的裝置的 MAC 位址 • $owner_ip – 裝置的 IP 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID
4000005009	新的 IP 位址 $owner_ip 被新增到 MAC 位址為$owner_mac 的裝置	在資產管理監控模式下，僅指定了 MAC 位址的網路介面（裝置處於*未授權*或*已存檔*狀態），會自動新增 IP 位址。 事件類型的標題和描述中使用了以下變數： • $owner_ip – 偵測到的裝置的 IP 位址 • $owner_mac – 裝置的 MAC 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID
4000005010	偵測到 IP 位址為$owner_ip 的裝置的新 MAC 位址 $new_mac_addr	當資產監控處於監控模式時，偵測到裝置使用的新MAC 位址（此裝置已停用位址資訊的自動更新）。 事件類型的標題和描述中使用了以下變數： • $new_mac_addr – 偵測到的 MAC 位址 • $owner_ip – 裝置的 IP 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID
4000005011	在從 EPP 應用程式接收到的裝置資料中偵測到MAC 位址 $owner_mac 變更為 $challenger_mac	根據從EPP 應用程式接收到的資訊，裝置的 MAC 位址已更新。 事件類型的標題和描述中使用了以下變數： • $owner_mac – 裝置的舊 MAC 位址 • $challenger_mac – 裝置的新MAC 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID
4000005012	在從 EPP 應用程式接收的資料中發現裝置$asset_name 的新位址資訊	在從EPP 應用程式接收的資料中發現裝置的新位址資訊。如果裝置位址資訊的變更尚未被應用程式處理，則會註冊此類事件，如事件 4000005009 或4000005010。 事件類型的標題和描述中使用了以下變數： • $asset_name – 裝置名稱 • $detected_epp_addresses – 位址資訊 • $asset_id – 裝置的 ID

代碼	事件類型標題	註冊條件
4000005013	從 EPP 應用程式接收資料後，在裝置位址 $conflicted_epp_assets 中偵測到衝突	根據從 EPP 應用程式收到的資訊，偵測到 Kaspersky Anti Targeted Attack Platform 中多個裝置的位址存在衝突。根據來自 EPP 應用程式的資訊，這些位址屬於同一裝置。 事件類型的標題和描述中使用了以下變數： • $conflicted_epp_assets – 偵測到具有衝突位址的裝置 • $unaccepted_epp_addresses – 屬於同一裝置的位址
4000005014	從 EPP 應用程式資料新增了子網路 $subnet_mask	從 EPP 應用程式取得資訊後，新子網路會自動新增至已知子網路清單。該子網路被新增到一個位址空間，其中資料來源可以是從 EPP 應用程式獲取資訊的 Integration Server。如果存在多個這樣的位址空間，則選擇包含最適合子網路的位址空間來自動新增新的巢狀子網路。 事件類型的標題和描述中使用了以下變數： • $subnet_mask – 子網路位址 • $subnet_type – 子網路類型
4000005016	偵測到 IP 位址為 $owner_ip 的未授權的 DHCP 伺服器	位址為 $owner_ip_or_mac 的 $asset_name 裝置（ID：$asset_id）被辨識為未經授權的 DHCP 伺服器。 事件類型的標題和描述中使用了以下變數： • $asset_id – 裝置的 ID • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址
4000005017	偵測到 IP 位址為 $owner_ip 的未授權的 DHCP 中繼	位址為 $owner_ip_or_mac 的 $asset_name 裝置（ID：$asset_id）被辨識為未經授權的 DHCP 中繼。 事件類型的標題和描述中使用了以下變數： • $asset_name – 裝置名稱 • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址
4000005600	偵測到位址為 $owner_ip_or_mac 的裝置上的使用者清單發生變化	在控制裝置上的使用者時偵測到使用者資訊發生變化。 事件類型的標題和描述中使用了以下變數： • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID • $added_asset_users – 已新增的使用者清單 • $modified_asset_users – 修改後的使用者清單 • $removed_asset_users – 已刪除的使用者清單
4000005601	在位址為 $owner_ip_or_mac 的裝置上的應用程式清單中偵測到變更	在監控裝置上的應用程式和修補程式時偵測到有關裝置上應用程式的資訊已被修改。 事件類型的標題和描述中使用了以下變數： • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID • $added_asset_apps – 已新增的應用程式清單 • $removed_asset_apps – 已刪除的應用程式清單
4000005602	在位址為 $owner_ip_or_mac 的裝置上偵測到修補程式清單中的變更	在監控裝置上的應用程式和修補程式時偵測到裝置修補程式資訊已修改。 事件類型的標題和描述中使用了以下變數： • $owner_ip_or_mac – 裝置的 IP 或 mAC 位址 • $asset_name – 裝置名稱 • $asset_id – 裝置的 ID • $added_asset_patches – 已新增修補程式的清單 • $removed_asset_patches – 已刪除修補程式的清單
4000005603	在裝置上的組態元件 $inventory_loc_key 中偵測到變更	在監控裝置配置時，根據裝置掃描結果與先前的配置進行比較時偵測到配置元件中的變更（對於在**僅更新**和/或**壓縮檔案版本**配置處理模式下執行的作業）。 事件類型的標題和描述中使用了以下變數： • $inventory_loc_key – 設定元件的名稱 • $device_config_inventory_changed_format – 在配置元件中偵測到的變更
4000005604	與裝置上的參考配置元件 $inventory_loc_key 相比偵測到差異	監控裝置配置時，根據裝置掃描結果發現與參考配置元件相比存在差異（對於在**與基準比較**配置處理模式下執行的作業）。 事件類型的標題和描述中使用了以下變數： • $inventory_loc_key – 設定元件的名稱 • $device_config_diverged_format – 與參考配置元件相比偵測到差異
4000005700	遠端連線裝置時偵測到公鑰不匹配	遠端連線到裝置時，偵測到收到的裝置公鑰與應用程式中儲存的值不符。裝置掃描已取消。 事件類型的描述中使用了以下變數： • $asset_name – 裝置名稱 • $new_asset_sshpublickey – 收到的公鑰 • $old_asset_sshpublickey – 儲存的公鑰

代碼	事件類型標題	註冊條件
4000005701	裝置主動輪詢期間偵測到公鑰不匹配	在主動輪詢裝置時，偵測到接收到的裝置公鑰與應用程式中儲存的值不符。已取消該裝置的主動輪詢。 事件類型的描述中使用了以下變數： • $asset_name – 裝置名稱 • $new_asset_sshpublickey – 收到的公鑰 • $old_asset_sshpublickey – 儲存的公鑰
4000000004	測試事件 (AM)	偵測到測試網路封包（啟用了裝置活動偵測方法）。

外部系統技術的系統事件類型

本文介紹了外部系統技術的系統事件類型（見下表）。

外部系統 (EXT) 技術的系統事件類型

代碼	事件類型標題	註冊條件
8000000001	聚合事件	偵測到滿足關聯規則條件的事件序列。 當註冊聚合事件時，關聯規則中的標題和描述將被用作事件的標題和描述。
4000005400	來自外部系統的事件	使用 NDR API 從外部系統接收的事件。 當註冊事件時，標題和描述由外部系統決定。

端點防護平台技術的系統事件類型

本文介紹了 Endpoint Protection Platform 的系統事件類型（見下表）。

使用 Endpoint Protection Platform (EPP) 技術的系統事件類型

代碼	事件類型標題	註冊條件
4000005500	特定於網路攻擊的活動	Integration Server 收到有關觸發 EPP 應用程式的網路威脅防護元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005501	連線不受信任的外部裝置	Integration Server 收到有關觸發 EPP 應用程式的裝置控制元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005502	嘗試運行未經授權或不受信任的應用程式	Integration Server 收到有關觸發 EPP 應用程式的裝置控制元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005503	指定監控範圍中被禁止的檔案操作	Integration Server 收到有關觸發 EPP 應用程式的檔案完整性監控元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005504	指定監控範圍內的檔案被修改	Integration Server 收到有關觸發 EPP 應用程式的基線檔案完整性監控元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005505	網路連線不被防火牆規則允許	Integration Server 收到有關觸發 EPP 應用程式的防火牆管理元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005506	指定監視範圍內的系統登錄修改	Integration Server 收到有關觸發 EPP 應用程式的登錄存取監視器元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005507	日誌分析規則被觸發	Integration Server 收到有關觸發 EPP 應用程式的日誌審查元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。

代碼	事件類型標題	註冊條件
4000005508	嘗試利用受防護處理程序中的弱點	Integration Server 收到有關觸發 EPP 應用程式的弱點防護元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005509	嘗試惡意加密網路檔案資源	Integration Server 收到有關觸發 EPP 應用程式的反加密勒索元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005510	嘗試連線到 Wi-Fi 網路	Integration Server 收到有關觸發 EPP 應用程式的 Wi-Fi 控制元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005512	偵測到受感染或可能受感染的物件	Integration Server 收到有關觸發 EPP 應用程式的即時檔案防護元件的資訊。 在事件類型的描述中，$epp_event_description 變數被用於來自 EPP 應用程式的資訊。
4000005513	Sigma 規則 $sigmaAlertTitle 已觸發	Integration Server 收到有關觸發 Endpoint Agent 元件 Sigma 規則的資料。 事件類型的標題和描述中使用了以下變數： • $sigmaAlertTitle – Sigma 規則名稱 • $sigma_detection_type – 偵測技術 • $sigma_object_type – 觸發 Sigma 規則的物件類型 • $sigma_object_name – 觸發 Sigma 規則的物件名稱或第一個觸發的 Sigma 規則的名稱 • $sigma_status – 偵測狀態

配置風險類型

*風險類型*定義在 Kaspersky Anti Targeted Attack Platform 中註冊風險時所使用的設定：風險的名稱、類別和基本分數。您可以檢視風險類型的設定，並在必要時變更某些風險類型的基本分數。

安裝後，應用程式使用原始風險類型清單。您可以透過安裝更新來更新和新增支援的風險類型。

檢視風險類型表

風險類型表顯示在應用程式 Web 介面的“**設定**”區域、“**風險類型**”子區域下。

風險類型顯示在表格以下列中：

- **代碼**。

  風險類型的唯一編號。在已註冊風險表中，風險類型的編號顯示在所選風險的詳細資訊區域。

- **名稱**。

  風險類型表中顯示的風險類型名稱。註冊風險時，其名稱可能與所使用風險類型的名稱不完全相符。某些風險類型的名稱可能被完全替換為已註冊風險的其他名稱。例如，具有此類名稱的風險類型包括“**外部系統風險**”類型的風險。如果註冊了此類風險，應用程式將保留風險資訊來源中指定的風險名稱（例如，在使用 NDR API 的外部系統中）。

- **類別**。

  風險類別的名稱。

- **基本分數**

  用於計算註冊風險得分的基線。在註冊除外部系統風險外的所有風險時，將套用配置的基本分數。名為**來自外部系統的風險**的風險類型的基本分數為零。必須在使用 NDR API 註冊風險的外部系統中指定此類風險的基本分數。

檢視風險類型表時，您可以使用設定、篩選、搜尋和排序功能。

變更風險類型的基本分數

無法變更名為**來自外部系統的風險**的風險類型的基本分數。如果註冊了此類風險，則該風險的基本分數必須由風險資訊來源提供（例如，使用 NDR API 的外部系統）。

若要變更風險類型的基本分數：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”部分、“**風險類型**”子部分。
2. 在風險類型表中，選擇您想要變更基本分數的風險類型。

   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊“**編輯**”。
4. 輸入新的基本分數。
5. 點擊**儲存**。

管理儲存風險的設定

您可以變更儲存的風險的最大總大小限制。

若要變更風險儲存設定：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**Sensor 伺服器**”部分。
3. 選擇 Central Node 伺服器的卡。

   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊“**編輯**”。

   在詳細資料區域，會顯示頁簽，您可以在其中管理伺服器的設定。
5. 在**一般**索引標籤上，移至**風險**索引標籤，並使用**最大容量**設定來設定儲存風險的大小限制。

   您可以選擇大小限制的計量單位：**MB**或**GB**。

   編輯值時，還需要考慮到所有大小限制的總和不得超過節點指定的最大儲存容量。
6. 如有必要，請使用**儲存時間（天）**設定啟用風險的最短儲存時間，並指定最短天數。
7. 點擊**儲存**。

管理 Endpoint Agent 主機資訊

用作Endpoint Agent 元件的應用程式安裝在組織 IT 基礎架構中的各個電腦（以下也稱為"主機"）上。應用程式持續監控在這些主機上運行的處理程序、活動的網路連線和正在修改的檔案。

具有**資深安全員**、**安全官**、**安全稽核員**和**管理員**角色的使用者，可以在使用者對其資料具有存取權的租用戶之 Central Node 伺服器 Web 介面視窗的**Endpoint Agent**索引標籤上，評估從具有 Endpoint Agent 元件的主機接收資料的頻率。如果您使用分佈式解決方案和多組織用戶模式，PCN 伺服器的 Web 介面將顯示 PCN 及所有已連線 SCN 中具有 Endpoint Agent 元件的主機清單。

具有**管理員**角色的使用者可以為其有權存取資料的租用戶，設定顯示從具有 Endpoint Agent 的主機接收資料的頻率。

如果偵測到可疑的網路活動，具有**資深安全員**角色的使用者可針對其有權存取資料的租用戶，將任何具有 Kaspersky Endpoint Agent 的主機與網路隔離。在這種情況下，伺服器與 Central Node 元件和具有 Endpoint Agent 元件的主機之間的連線不會中斷。

為了在 Endpoint Agent 元件出現問題時提供支持，技術支援人員可能會要求您執行以下操作以進行偵錯（包括在技術支援模式下）：

- 啟動擴展診斷資訊的收集。
- 修改個體應用程式元件的設定。
- 修改用於儲存和傳送獲取的診斷資訊的設定。
- 配置要被攔截並儲存到檔案的網路流量。

技術支援人員會提供執行這些操作所需的所有資訊（步驟順序說明、要修改的設定、設定檔、指令碼、附加的命令列功能、偵錯模組、特定用途的實用程式和其他資源等），並會告知您出於偵錯目的所取得的資料的範圍。檢索到的診斷資訊儲存在使用者的電腦上。檢索到的資料不會自動傳送到卡巴斯基。

以上列出的操作只能在技術支援專家的指導和監督下進行。未按照本手冊或技術支援專家的說明變更應用程式設定，將會導致作業系統變慢或崩潰，降低電腦安全，並可能影響正在處理的資料的可用性和完整性。

配置具有 Endpoint Agent 元件的主機表的顯示

若要檢視具有 Endpoint Agent 元件的主機表：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。
2. 轉到"**Endpoint Agent**"索引標籤。

   顯示具有 Endpoint Agent 元件的主機表。

如果您使用分佈式解決方案和多組織用戶模式，則該表包含有關具有 Endpoint Agent 元件的主機的資訊，主機已連線到 PCN 和所有 SCN 伺服器。

該表可以顯示以下資料：

- Endpoint Agent 元件的活動指示器和主機數量：
  - **严重不活動**是很久以前從其收到最新資料的主機數量。
  - **警告**是長久以前從其收到最新資料的主機數量。
  - **正常活動**是最近從其收到最新資料的主機數量。
- **主機**—具有 Endpoint Agent 元件的主機名稱。
- **伺服器**是具有 Endpoint Agent 元件的主機所連線之伺服器的名稱。
  如果您使用分佈式解決方案和多組織用戶模式，則會顯示此欄位。
- **IP**是安裝 Endpoint Agent 元件的主機的 IP 位址。
- **作業係統**是安裝在具有 Endpoint Agent 元件之主機上的作業系統版本。
- **版本** — 安裝的 Endpoint Agent 元件版本。
- **活動** — Endpoint Agent 元件的活動指示器。
  - **正常活動**用於最近收到最新資料的主機。
  - **警告**用於很久以前從其收到最新資料的主機。
  - **严重不活動**用於非常久以前收到最新資料的主機。
- **最後一次連線**用於 Endpoint Agent 元件上次連線到 Central Node 伺服器時的日期和時間。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- 執行以下工作：
  - **殺死處理程序**。
  - **刪除檔案**。
  - **使用唯一的 PID 殺死處理程序**。
  - **獲取檔案**。
  - **進行取證**。
  - **隔離檔案**。
  - **執行應用程式**。
- **新的阻止規則**。

- **從網路隔離**。
- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

> 可用操作清單取決於 Endpoint Agent 元件的類型：適用於 Windows、Linux 或 Mac（有關詳細資訊，請參閱"*應用程式的操作原則*"部分）。

點擊具有 IP 的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **尋找警示**。
- **複製值到剪貼簿**。

如果您僅使用 KATA 功能（KATA 鍵），則在點擊主機名稱連結後顯示的清單中，您可以執行以下操作：

- **尋找警示**（顯示給具有"**資深安全員**"角色的使用者）。
- **新增到篩選器**。
- **從篩選器中排除**。
- **複製值到剪貼簿**。

點擊表格中任何其他列中的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **複製值到剪貼簿**。

配置具有 Endpoint Agent 元件的主機表的顯示

您可以顯示或隱藏列並變更具有 Endpoint Agent 元件的主機表中的列順序。

配置具有 Endpoint Agent 元件的主機表的顯示：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。
2. 轉到"**Endpoint Agent**"索引標籤。
3. 在表格的標題部分，點擊 ⚙ 。

4. 這將開啟**自訂表格**視窗。

5. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   必須選擇至少一個核取方塊。

6. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。

7. 如果要還原預設表格顯示設定，請點擊**預設**。

8. 點擊**套用**。

   具有 Endpoint Agent 元件的主機表的顯示得到配置。

檢視有關主機的資訊

若要檢視具有 Endpoint Agent 元件的主機的資訊：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。

2. 轉到"**Endpoint Agent**"索引標籤。

3. 選擇您想檢視資訊的主機。

   這將開啟一個視窗，其中包含有關主機的資訊。

此視窗包含以下資訊：

- 推薦組：
  - 點擊**警示**連結將開啟包含選定主機的篩選條件的**警示**部分。
  - 點擊事件連結將開啟包含選定主機的篩選條件的**威脅搜尋**部分。
  - 點擊**受阻止規則影響的事件**連結將開啟包含選定主機和**阻止的應用程式（阻止規則）**事件類型的搜尋條件的**威脅搜尋**部分。

  如果您僅使用KATA 功能（KATA 鍵），則只有"**警示**"連結顯示在建議部分。

- 在**詳細資訊**索引標籤上，**主機**部分顯示以下資訊：
  - **名稱**是具有 Endpoint Agent 元件的主機的名稱。
  - **IP** 是安裝 Endpoint Agent 元件的主機的 IP 位址。
  - **作業系統**—安裝了 Endpoint Agent 元件的主機上的作業系統版本。

- 在**詳細資訊**索引標籤上，**Endpoint Agent**部分顯示以下資訊：
  - **版本**是安裝的 Endpoint Agent 元件版本。
- **活動**是Endpoint Agent 元件的活動指示器。可能值：
  - **正常活動**用於最近收到最新資料的主機。
  - **警告**用於很久以前從其收到最新資料的主機。
  - **严重不活動**用於非常久以前收到最新資料的主機。
- **伺服器**—SCN 或 PCN 伺服器的名稱。僅在分散式解決方案和多組織用戶模式中顯示。
- **已連線到伺服器**—Central Node 伺服器的名稱。
- **最後一次連線**—上次連線到 Central Node、SCN 或 PCN 伺服器的時間。
- **產品授權金鑰狀態**—例如，“OK”。
- 在**阻止規則**索引標籤上，您可以檢視被阻止在主機上執行或開啟的檔案的 MD5 或 SHA256 雜湊值。將顯示以下資訊：
  - **名稱**—檔案的名稱。
  - **狀態**—阻止規則的狀態。
  - **雜湊**—雜湊演算法。

  如果您僅使用 KATA 功能（KATA 鍵），則不顯示“**阻止規則**”索引標籤。

- 在**工作**索引標籤上，您可以檢視主機上執行了哪些工作。將顯示以下資訊：
  - **建立時間**—工作建立日期和時間。
  - **名稱**—工作名稱。
  - **詳細資訊**—為其建立了工作的檔案或資料串流的完整路徑。
  - **狀態**—工作完成狀態。

  如果您僅使用 KATA 功能（KATA 鍵），則不顯示“**工作**”索引標籤。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 執行以下工作：
  - **殺死處理程序**。
  - **刪除檔案**。
  - **獲取檔案**。

    - **進行取證**。
    - **隔離檔案**。
    - **執行應用程式**。
- **新的阻止規則**。
- **從網路隔離**。
- **尋找事件**。
- **尋找警示**。
- **新增到篩選器**。
- **從篩選器中排除**。
- **複製值到剪貼簿**。

可用操作清單取決於 Endpoint Agent 元件的類型：適用於 Windows、Linux 或 Mac（有關詳細資訊，請參閱"*應用程式的操作原則*"部分）。

點擊具有 IP 的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

如果您僅使用 KATA 功能（KATA 鍵），則在點擊主機名稱和 IP 位址連結後顯示的清單中，您可以執行以下操作：

- **尋找警示**。
- **複製值到剪貼簿**。

依主機名稱篩選並搜尋具有 Endpoint Agent 元件的主機

若要依主機名稱篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。
2. 轉到"**Endpoint Agent**"索引標籤。
   這將開啟主機表。
3. 點擊**主機**連結以開啟篩選配置視窗。
4. 如果您只想顯示隔離的主機，請選擇**僅顯示隔離的 Endpoint Agent**核取方塊。

5. 在下拉清單中，選擇以下篩選運算子之一：

- **包含**
- **不包含**

6. 在輸入欄位中，指定主機名稱的一個或多個字元。

7. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

8. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。

9. 點擊**套用**。

篩選配置視窗關閉。

表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

根據已與網路隔離的 Endpoint Agent 元件篩選和搜尋主機

若要篩選或搜尋與網路隔離的具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。

2. 轉到"**Endpoint Agent**"索引標籤。
   這將開啟主機表。

3. 點擊**主機**連結以開啟篩選配置視窗。

4. 選擇**僅顯示隔離的 Endpoint Agent**核取方塊。

5. 點擊**套用**。

篩選配置視窗關閉。

表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

按 PCN 和 SCN 伺服器名稱篩選並搜尋具有 Endpoint Agent 元件的主機

如果使用分佈式解決方案和多組織用戶模式，您可以根據主機所連線的 PCN 和 SCN 伺服器的名稱篩選或尋找具有 Kaspersky Endpoint Agent 元件的主機。

若要按PCN 和 SCN 伺服器的名稱篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**伺服器**連結以開啟篩選配置視窗。
4. 選擇想要依其篩選或搜尋具有 Endpoint Agent 元件的主機的伺服器名稱旁的核取方塊。
5. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依電腦 IP 位址篩選並搜尋具有 Endpoint Agent 元件的主機

若要按在其上安裝應用程式的電腦的 IP 位址篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**IP**連結以開啟篩選配置視窗。
4. 在下拉清單中，選擇以下篩選運算子之一：
   - **包含**
   - **不包含**
5. 在輸入欄位中，指定電腦 IP 位址的一個或多個字元。您可以輸入 IPv4 格式的 IP 位址或子網路遮罩（例如，`192.0.0.1` 或 `192.0.0.0/16`）。
6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

7. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。

8. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依電腦上的作業系統版本篩選並搜尋具有 Endpoint Agent 元件的主機

若要根據安裝在電腦上的作業系統版本篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。

2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。

3. 點擊**作業係統**連結以開啟篩選設定視窗。

4. 在下拉清單中，選擇以下篩選運算子之一：

   - **包含**

   - **不包含**

5. 在輸入欄位中，指定作業系統版本的一個或多個字元。

6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

7. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。

8. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

依元件版本篩選並搜尋具有 Endpoint Agent 元件的主機

您可以按 Endpoint Agent 元件的角色中所使用的應用程式版本篩選主機。

若要按元件版本篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**版本**連結以開啟篩選設定視窗。
4. 在下拉清單中，選擇以下篩選運算子之一：
   - **包含**
   - **不包含**
5. 在輸入欄位中，指定用作 Endpoint Agent 元件的應用程式版本的一個或多個字元。
6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
7. 如果要刪除篩選條件，請點擊該欄位右側的 🗑 按鈕。
8. 點擊**套用**。

   篩選配置視窗關閉。

   表格將僅顯示與您設定的篩選條件相符的主機。

> 您可以同時使用多個篩選器。

依活動篩選並搜尋具有 Endpoint Agent 元件的主機

若要依其活動篩選或搜尋具有 Endpoint Agent 元件的主機：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊**活動**連結以開啟篩選配置視窗。

選擇一個或多個活動指示器旁的核取方塊：

- **正常活動**，如果您想尋找最近從其中接收到最後資料的主機。
- **警告**，如果您想尋找前段時間從其中接收到最後資料的主機。
- **严重不活動**，如果您想尋找很久以前從其中接收到最後資料的主機。

4. 點擊**套用**。

篩選配置視窗關閉。

表格將僅顯示與您設定的篩選條件相符的主機。

您可以同時使用多個篩選器。

為具有 Endpoint Agent 元件的主機快速建立篩選器

若要為具有 Endpoint Agent 元件的主機快速建立篩選器：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 執行下列操作以便將篩選條件快速新增至正在建立的篩選器：
   a. 將滑鼠遊標置於包含您希望將其作為篩選條件新增的表列值的連結上。
   b. 左鍵點擊。
      這將開啟要對值執行的操作清單。
   c. 在開啟的清單中，選擇下列其中一項操作：
      - **新增到篩選器**，如果您想將該值包含在篩選條件中。
      - **從篩選器中排除**，如果您想從篩選條件中排除該值。
4. 如果您想要新增多個篩選條件到正在建立的篩選器中，請執行操作以將每個篩選條件快速新增至正在建立的篩選器。

表格將僅顯示與您設定的篩選條件相符的主機。

為具有 Endpoint Agent 元件的主機重設篩選器

若要清除一個或多個篩選條件的 Endpoint Agent 主機篩選器：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
3. 點擊您想要清除其篩選條件的表列標題右側的 ⊠。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   表格將僅顯示與您設定的篩選條件相符的主機。

刪除具有 Endpoint Agent 元件的主機

若要從**Endpoint Agent**表中刪除一台或多台主機：

1. 在應用程式 Web 介面視窗中，選擇**資產**區段。
2. 前往**Endpoint Agent**索引標籤。
3. 選擇要刪除的一台或多台主機旁的核取方塊。您可以透過選擇包含列標題的行中的核取方塊來選擇所有主機。

   控制面板出現在視窗的下部。
4. 點擊**刪除**。
5. 這將開啟操作確認視窗；在該視窗中，點擊**是**。

   選定的主機將會被從**Endpoint Agent**表中移除。

主機移除後，Kaspersky Anti Targeted Attack Platform 的 Web 介面會發生以下變更：

- 您無法為已移除的主機建立工作、阻止規則或網路隔離規則。
- 如果先前為主機建立了阻止規則，則主機移除後，其在規則視窗中的名稱（**阻止於**欄位）會被隱藏。該規則繼續適用。

  如果該主機重新連線到 Central Node 伺服器，主機名稱將在**阻止於**欄位中還原，阻止規則將再次套用至該主機。
- 如果先前為主機建立了網路隔離規則，則該規則將繼續套用，直到規則中指定的時間到期。

  當該主機重新連線到 Central Node 時，該規則將會重新套用到該主機。

- 遠端主機上隔離物件的中繼資料將從Kaspersky Anti Targeted Attack Platform 隔離區中刪除。

  當該主機重新連線到 Central Node 伺服器時，Kaspersky Anti Targeted Attack Platform 隔離區中物件的中繼資料**不會**還原。您可以透過在命令列或卡巴斯基安全管理中心中清除主機上的隔離區來避免填滿隔離區。有關詳細資訊，請參閱您在 Endpoint Agent 元件角色中使用的應用程式的協助。

- 如果物件僅在一台主機上被**隔離檔案**工作隔離，且該主機已移除，則工作視窗中的**還原所有**按鈕將處於非活動狀態，因為檔案無法在已移除的主機上還原。

以被移除主機的名稱進行事件搜尋仍然可用。

限制來自 Endpoint Agent 的遙測

預設情況下，Kaspersky Anti Targeted Attack Platform 會處理從 Endpoint Agent 收到的*所有*事件資料（遙測）。透過限制遙測量，您可以減少儲存和處理遙測的伺服器的負載。有限遙測包括有關事件本身的完整資訊以及有關觸發這些事件的處理程序的最重要的資訊。與事件相關的其他處理程序的資訊被排除。

擁有"**資深安全員**"角色的使用者可以限制遙測量。擁有"**管理員**"或"**安全稽核員**"角色的使用者可以檢視遙測限制設定，但不能管理這些設定。具有"**安全官**"角色的使用者無權存取遙測設定。

若要限制 Endpoint Agent 的遙測量，請執行下列操作：

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分的**Endpoint Agent**子部分。
2. 在"**遙測**"下，選擇"**受限制**"。
3. 點擊視窗下部的**套用**。

   遙測受到限制。

限制 Central Node 和 SCN 遙測的特殊注意事項

點擊"**套用**"後，可能會顯示"*限制接收資料的範圍失敗*"訊息。這表示某些使用者定義的 TAA（IOA）規則不允許限制遙測，因為這些規則包含在遙測受限時不會處理的欄位。您可以停用或刪除此類規則。

需要停用或刪除的規則清單顯示在警告視窗的"**要停用或修改的 TAA 規則**"標題下。您可以透過點擊"**複製清單**"複製這些規則的清單，並以您想要的任何方式儲存清單。警告視窗中的"**轉到 TAA 規則**"按鈕會將您帶至使用者定義的 TAA（IOA）規則部分。

限制 PCN 遙測的特殊考慮

Kaspersky Anti Targeted Attack Platform 不會檢查 PCN 上活動的使用者定義的 TAA (IOA) 規則是否能夠在有限的遙測下保持功能。我們建議採取措施測試每個使用者定義的 TAA (IOA) 規則。

測試有限遙測模式下使用者定義的 TAA (IOA) 規則的功能涉及以下步驟：

1. 啟用有限遙測模式。

2. 根據規則中的請求代碼搜尋事件。

   若要按規則中的程式碼搜尋事件，請開啟規則視窗，然後點擊“**執行查詢**”按鈕。開始搜尋後，“**威脅搜尋**”視窗將會開啟。

   如果視窗包含符合搜尋條件的事件表，則 TAA (IOA) 規則有效。如果視窗在 PCN 名稱旁顯示“*伺服器錯誤：請求失敗*”錯誤，則表示該規則不起作用。

3. 停用或刪除不起作用的 TAA (IOA) 規則。

   如果您想要刪除或停用在 PCN 上不起作用的規則，但仍想在 SCN 上套用該規則，則需要在要套用該規則的每個 SCN 的 Web 介面中建立類似的規則。

   如果您不想停用或刪除任何規則，請不要限制遙測。

使用 Endpoint Agent 元件對主機進行網路隔離

在回應威脅時，具有“**資深安全員**”角色的使用者可以在事件調查期間隔離包含帶有風險的偵測物件的主機。

網路隔離本身不是威脅回應操作。當主機的網路隔離處於活動狀態時，安全管理人員應自行採取措施調查事件。您可以在建立網路隔離規則時配置主機網路隔離的時長。

為確保隔離主機的正常運行，建議滿足以下條件：

- 在啟用網路隔離規則之前，在主機上建立本機管理員帳戶或將網域帳戶資料儲存到快取。
- 啟用網路隔離規則時，請勿使用 Central Node 元件變更伺服器的憑證和 IP 位址。

隔離的主機可以透過網路存取以下資源：

- 具有 Central Node 元件的伺服器。
- 應用程式資料庫更新來源（卡巴斯基更新伺服器或自訂來源）。
- KSN 服務的伺服器。
- 新增至網路隔離規則排除項目的主機。

如果主機上的 Endpoint Agent 元件關閉，以及在開啟該元件或使用該元件重新啟動電腦後的一段時間內，主機的網路隔離可能會處於非活動狀態。

如有必要，您可以透過以下方式之一停用網路隔離：

- 使用 KEDR API 請求。
- 透過在 Kaspersky Anti Targeted Attack Platform Web 介面中刪除網路隔離規則。

- 透過命令列。

  有關透過命令列停用網路隔離的更多資訊，請參閱Kaspersky Endpoint Security for Windows 說明。

應用網路隔離時請考慮一些限制。

建立一個網路隔離規則

若要建立一個網路隔離規則：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。

   這將開啟主機表。
3. 選擇您要啟用或停用網路隔離規則的主機。

   這將開啟一個視窗，其中包含有關主機的資訊。
4. 點擊**隔離**。
5. 在**此時間後停用隔離**欄位中，輸入以小時為單位的時間（1 到 9999），在此期間主機的網路隔離將處於活動狀態。
6. 在**主機隔離規則排除項目**設定群組中的**流量方向**清單中，選擇必須放行的網路流量方向：
   - **傳入/傳出**。
   - **傳入**。
   - **傳出**。
7. 在**IP**欄位中，輸入必須放行其網路流量的 IP 位址。

   > 如果您使用 Kaspersky Endpoint Agent 充當 Endpoint Agent 元件，則可以使用代理伺服器將 Kaspersky Endpoint Agent for Windows 與 Kaspersky Anti Targeted Attack Platform 連線。當您將此代理伺服器新增至排除項時，可透過代理伺服器存取的網路資源也會新增至排除項目。如果透過代理伺服器存取的網路資源已新增至排除項，但代理伺服器本身未被新增至排除項，則此類排除項無法運作。
8. 如果您選擇了**傳入**或**傳出**，請在**連接埠**欄位中輸入連接埠。
9. 如果您想要新增多個排除項，請點擊**新增**並重複上述步驟填寫**流量方向**、**IP**和**連接埠**欄位。
10. 點擊**儲存**。

將主機與網路隔離。

您也可以透過點擊事件資訊和警示資訊中的**隔離 <主機名稱>**連結，建立網路隔離規則。

具有**安全稽核員**和**安全官**角色的使用者無法建立網路隔離規則。

網路隔離功能不適用於使用 Kaspersky Endpoint Security 11.4 for Linux 作為 Endpoint Agent 元件的主機。

新增網路隔離規則中的排除項

若要將排除新增至先前建立的網路隔離規則：

1. 在應用程式 Web 介面視窗中，選擇"**資產**"區域。
2. 轉到"**Endpoint Agent**"索引標籤。
   這將開啟主機表。
3. 從網路隔離規則中選擇要為其建立排除項目的被隔離主機。
   這將開啟一個視窗，其中包含有關主機的資訊。
4. 點擊**新增到排除項目**連結以展開**主機隔離規則排除項目**設定群組。
5. 選擇不得封鎖的網路流量方向：
   - **傳入/傳出**。
   - **傳入**。
   - **傳出**。
6. 在**IP**欄位中，輸入必須放行其網路流量的 IP 位址。
7. 如果您選擇了**傳入**或**傳出**，請在**連接埠**欄位中輸入連接埠。
8. 如果您想要新增多個排除項，請點擊**新增**並重複上述步驟填寫**流量方向**、**IP**和**連接埠**欄位。點擊**儲存**。

將新增網路隔離規則排除。

具有**安全稽核員**和**安全官**角色的使用者無法建立網路隔離規則的排除項目。

刪除網路隔離規則

若要刪除網路隔離規則：

1. 在應用程式 Web 介面視窗中，選擇“**資產**”區域。
2. 轉到“**Endpoint Agent**”索引標籤。
   這將開啟主機表。
3. 點擊您要刪除網路隔離規則的主機的名稱以開啟該主機的操作功能表。
4. 選擇**刪除主機隔離規則**操作。
   這將開啟操作確認視窗。
5. 點擊**是**。

主機的網路隔離規則被刪除。

具有**安全稽核員**和**安全官**角色的使用者無法刪除網路隔離規則。

與網路隔離相關的限制

使用網路隔離時存在一些限制：

- 在主機上啟用網路隔離規則時，將中斷所有目前連線，且 VPN 連線將無法使用。
- 如果在啟用網路隔離規則時應用程式管理員使用 Central Node 元件替代伺服器的憑證，則無法停用該規則。
- 該應用程式阻止隔離主機與活動目錄伺服器的連線。如果作業系統設定需要連線到活動目錄服務以進行授權，則隔離主機的使用者將無法登入系統。

根據 Kaspersky TAA (IOA) 規則自動從 Kaspersky Endpoint Agent 主機傳送檔案以供 Sandbox 元件掃描

如果啟用了此功能，應用程式可以自動從具有 Endpoint Agent 元件的主機傳送檔案，以便根據 Kaspersky TAA (IOA) 規則使用 Sandbox 元件進行掃描。檔案傳送按照以下原則：

1. Kaspersky Anti Targeted Attack Platform 檢查事件資料庫並標記與 TAA (IOA) 規則相符的事件。
2. 如果在TAA (IOA) 規則中找到相關條件，Kaspersky Anti Targeted Attack Platform 將會傳送檔案供 Sandbox 元件進行掃描。

   Sandbox 元件掃描檔案的請求不會顯示在 Kaspersky Anti Targeted Attack Platform Web 介面中。

3. 根據掃描結果，應用程式可能會建立警示。

   您可以透過按照**詳細資訊**–**自動傳送到 Sandbox**屬性篩選警示來檢視以此方式建立的警示。

如果啟用了自動傳送供 Sandbox 元件掃描的檔案，元件處理的流量會變得非常大。如果 Sandbox 元件伺服器無法支援增加的負載，處理請求佇列中的某些物件將被替換為被自動傳送進行掃描的處理檔案請求。

為了避免從處理請求佇列中掉落物件，您可以：

- 部署額外的 Sandbox 伺服器。
- 停用自動傳送要由 Sandbox 元件掃描的檔案。
- 將最常導致 Kaspersky Anti Targeted Attack Platform 傳送檔案以供 Sandbox 元件進行掃描的 TAA (IOA) 規則新增至排除項目中。

  有關 Kaspersky Anti Targeted Attack Platform 傳送檔案以供 Sandbox 元件進行掃描的最常用規則的資訊顯示在**按 TAA 規則傳送到 Sandbox**小工具中。您可以將此小工具新增至目前佈局。

  當您將檔案新增至排除項時，根據此規則的事件標記和警示建立也會停止。

下表列出了可以自動傳送供 Sandbox 元件掃描的檔案。

可自動傳送供 Sandbox 元件進行掃描的檔案清單

事件類型	檔案類型
處理程序已啟動	已啟動處理程序的檔案及其父處理程序的檔案。
模組已載入	已載入模組的檔案及其父處理程序的檔案。
到遠端主機的連線	父處理程序檔案。
阻止的應用程式（阻止規則）	被阻止運行的應用程式的檔案及其父處理程序的檔案。
檔案已封鎖	被阻止運行的文件的檔案及其父處理程序的檔案。
檔案已變更	已建立、刪除或修改的檔案和父處理程序的檔案。
系統事件日誌	處理程序檔（僅適用於 Linux）。

事件類型	檔案類型
登錄檔已修改	父處理程序檔案。
監聽的連接埠	父處理程序檔案。
驅動程式已載入	載入的驅動程式的檔案。
偵測	偵測到的檔案及其父處理程序的檔案（如果有）。
偵測處理結果	偵測到的檔案及其父處理程序的檔案（如果有）。
AMSI 掃描	處理程序的檔案。
處理程序：解釋檔案執行	已啟動的檔案及其父處理程序的檔案。
處理程序：主控台互動式輸入	父處理程序檔案。

有關被傳送供 Sandbox 元件進行掃描的檔案的資訊不會顯示在 Kaspersky Anti Targeted Attack Platform Web 介面中。

啟用並停用從具有 Endpoint Agent 元件的主機自動傳送檔案以供 Sandbox 元件掃描

若要啟用或停用自動傳送檔案以供 Sandbox 元件根據 Kaspersky TAA (IOA) 規則進行掃描：

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分的 **Endpoint Agent** 子部分。
2. 在**自動將檔案傳送到 Sandbox**下：
   - 設定**傳送檔案**切換開關至**已啟用**，如果您想啟用檔案自動傳送功能。
     預設情況下啟用此功能。
   - 設定**傳送檔案**切換開關至**已停用**，如果您想停用檔案自動傳送功能。
     停用此功能不會影響TAA (IOA) 規則的運作；僅自動傳送檔案會被停用。
3. 點擊**套用**。

根據 Kaspersky TAA (IOA) 規則自動傳送要由 Sandbox 元件掃描的檔案已啟用或停用。

在分散式解決方案和多組織用戶模式下，根據 PCN 伺服器上設定的 Kaspersky TAA (IOA) 規則自動傳送檔案供 Sandbox 元件掃描的設定，也適用於連線到該 PCN 伺服器的 SCN 伺服器。如有必要，您可以單獨啟用或停用每個選定 SCN 伺服器上的檔案自動傳送。

選擇掃描 Sandbox 中的物件時要使用的作業系統

具有**資深安全員**角色的使用者可以選擇一組作業系統作為建立由 Sandbox 元件掃描物件的工作的基礎。Sandbox 伺服器必須安裝與所選集相符的虛擬機。

您可以檢視伺服器上部署的 Sandbox 伺服器和虛擬機的清單。

具有**安全稽核員**角色的使用者可以檢視Sandbox 伺服器清單以及一組作業系統的設定。具有**安全官**角色的使用者無法檢視此部分。

檢視具有 Sandbox 元件的伺服器表

具有**安全官**角色的使用者無法檢視具有 Sandbox 元件的伺服器表。

具有**資深安全員**角色的使用者可以檢視具有 Sandbox 元件的伺服器表。

若要檢視具有 Sandbox 元件的伺服器表：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**Sandbox 伺服器**子部分。
2. 選擇**伺服器**索引標籤。

   一個表格將顯示，其中包含 Sandbox 伺服器清單。

表包含以下資訊：

- **IP 和名稱** — 具有 Sandbox 元件的伺服器的 IP 位址或完全限定網域名稱。
- **授權** — 連線到 Sandbox 元件的請求狀態。
- **狀態** — 與 Sandbox 元件的連線狀態。
- **憑證指紋** — 具有 Sandbox 元件的伺服器的憑證指紋。
- **虛擬機**—在伺服器上建立的虛擬機清單。

選擇掃描 Sandbox 中的物件時要使用的作業系統

若要選擇作業系統集：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**Sandbox 伺服器**子部分。
2. 前往**設定**索引標籤。
3. 在**作業係統集合**下面，選擇以下選項之一：
   - **Windows 7**、**Windows 10**。
   - **CentOS 7.8**、**Windows 7**、**Windows 10**。

- **Astra Linux 1.7**、**Windows 7**、**Windows 10**。
- **自訂**。

4. 如果您選擇了**自訂**，在**集合組成**下面，選擇要包含在該集合中的作業系統旁的核取方塊。

   如果 Sandbox 伺服器上安裝了具有這些作業系統的虛擬機，則自訂作業系統將顯示在清單中。預設作業系統始終顯示在清單中，但如果未部署執行這些作業系統的虛擬機，則**未知**狀態會顯示在作業系統名稱旁邊。

Kaspersky Anti Targeted Attack Platform 將根據選定的集合建立掃描 Sandbox 中物件的工作。

如果 Sandbox 伺服器上安裝的作業系統集與 Central Node 伺服器上選擇的作業系統集不匹配，則該 Sandbox 伺服器不會傳送物件以進行掃描。如果有多個 Sandbox 伺服器連線到 Central Node 伺服器，則應用程式會將物件傳送到其安裝的作業系統與 Central Node 上選取的集合相符的 Sandbox 伺服器。

您可以在使用應用程式的過程中變更作業系統集。在這種情況下，您需要確保 Sandbox 伺服器的配置符合硬體需求。

在分佈式解決方案和多組織用戶模式下，PCN 伺服器上配置的作業系統集的設定不會被套用於連線到該 PCN 伺服器的 SCN 伺服器。您可以單獨為每個 PCN 和 SCN 伺服器選擇作業系統集。

管理工作

在伺服器上建立工作、具有**資深安全員**角色的使用者對具有連線到伺服器的 Endpoint Agent 元件的所有主機有無限的（root）存取權。

在應用程式的 Web 介面中，具有**資深安全員**角色的使用者可以透過建立和刪除工作來管理主機上的檔案和應用程式。

在分佈式解決方案和多組織用戶模式下，**殺死處理程序**、**進行取證**、**獲取登錄機碼**、**啟動 YARA 掃描**、**管理服務**、**執行應用程式**、**刪除檔案**、**從隔離區還原檔案**、**隔離檔案**工作可以具有以下類型之一：

- **全球** — 在 PCN 伺服器上建立。這些工作適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。工作屬於使用者為其使用 Web 介面管理程式的租戶。
- **本機** — 在 SCN 伺服器上建立。這些工作僅適用於連線到此 SCN 伺服器的主機。工作屬於使用者為其使用 Web 介面管理程式的租戶。

獲取檔案、**獲取處理程序記憶體傾印**、**獲取 NTFS 元檔案**、**獲取磁碟鏡像**、**獲取記憶體傾印**工作僅在指定主機上執行，無論應用程式的運作模式為何。

最長工作執行時間為 24 小時。如果此時工作未完成，則執行暫停。

具有**資深安全員**角色的使用者可以管理他們有權存取其資料的租戶的所有工作。

具有**安全官**角色的使用者無權存取工作。

具有**安全稽核員**角色的使用者可以檢視工作表以及有關所選工作的資訊。

檢視工作表

工作表包含已建立工作的清單，位於應用程式 Web 介面視窗的**工作**部分。您可以檢視所有工作或僅檢視您（目前使用者）建立的工作。

您可以使用位於視窗右上角的**僅我的**切換開關，顯示或隱藏您建立的工作。預設啟用顯示目前使用者建立的工作。

工作表包含以下資訊：

- **時間** — 工作建立日期和時間。
- **類型**是工作的類型，取決於應用程式的操作模式和在其上建立工作的伺服器。

  工作可以是以下類型之一：

  - **全球** — 在 PCN 伺服器上建立。這些工作適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。工作屬於使用者為其使用 Web 介面管理程式的租戶。
  - **本機** — 在 SCN 伺服器上建立。這些工作僅適用於連線到此 SCN 伺服器的主機。工作屬於使用者為其使用 Web 介面管理程式的租戶。
- **名稱** — 工作名稱。

  點擊具有工作類型名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

  - **新增到篩選器**。
  - **從篩選器中排除**。
  - **複製值到剪貼簿**。
- **詳細資訊** — 為其建立工作的檔案或資料串流的完整路徑，或共用網路資源的路徑。

  點擊包含有關檔案或資料流路徑的資訊的連結將開啟一個清單，您可以在其中選擇以下操作之一：

  - **新增到篩選器**。
  - **從篩選器中排除**。
  - **複製值到剪貼簿**。
- **伺服器** — 具有 PCN 或 SCN 角色的伺服器的名稱，工作在該伺服器上執行。

  如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄位。
- **主機** — 在其上執行工作的主機名稱。

  僅當您使用獨立的 Central Node 伺服器時才會顯示此欄位。
- **建立者** — 建立工作的使用者名稱。

  > 如果只顯示目前使用者建立的工作，則不顯示該列。

- **狀態** — 工作完成狀態。
  工作可以具有以下狀態之一：
  - **等待**。
  - **進行中**。
  - **已完成**。

檢視有關工作的資訊

檢視工作詳細資訊：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 選擇您想檢視資訊的工作。

這將開啟一個視窗，其中包含有關工作的資訊。

根據工作類型，視窗可以包含以下資訊：

- **狀態** — 工作完成狀態。
- **敘述**—工作描述。
- **檔案路徑**—檔案或資料串流的路徑。
- **資訊類型**—所收集資料的類型。
- **登錄機碼**—您想要取得的登錄機碼的路徑。
- **處理程序 ID**—處理程序識別碼。
- **遮罩**—資料清單中所包含的檔案的遮罩。
- **元檔案**—您想要取得的 NTFS 中繼檔。
- **卷**—您要從中接收中繼檔、磁碟映像或記憶體傾印的磁碟機的名稱。
- **共用路徑**—共用網路資源的路徑。
- **儲存的檔案**—因為工作執行收到的檔案的連結。
- **最大嵌套級別**—應用程式搜尋檔案的資料夾的最大嵌套層級。
- **排除項目**—禁止在其中搜尋和掃描檔案的資料夾。
- **掃描範圍**—依照 YARA 規則掃描的資料夾。
- **操作**—為服務執行的操作。

該應用程式支援以下服務操作：

- **開始**。
- **停止**。
- **暫停**。
- **還原**。
- **刪除**。
- **修改啟動類型**。

- **最大掃描持續時間**—最大工作執行時間，之後掃描將停止。
- **SHA256**—要接收的檔案的 SHA256 雜湊。
- **執行身分**—使用本機系統名稱執行應用程式的選項。
- **建立者** — 建立工作的使用者名稱。
- **租戶**—租用戶名稱。僅當使用分散式解決方案和多組織用戶模式時顯示。
- **建立時間**—建立工作的時間。
- **完成時間**—工作完成時間。
- **報告**—選定主機上的工作結果。

建立獲取檔案工作

您可以從具有 Endpoint Agent 元件的主機擷取檔案。為此，您必須建立一個獲取檔案工作。

要下載的檔案不得超過 100 MB。如果檔案超過 100 MB，工作將結束並出現錯誤。

若要建立獲取檔案工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**新增**按鈕，並在**獲取資料**下拉清單中選擇**檔案**。
   這將開啟工作建立視窗。
3. 配置以下設定：
   a. **檔案路徑**—您想要接收的檔案路徑。
      如果要求的檔案已連結到其他 NTFS 資料流，則執行該工作將產生請求的檔案連結到的 NTFS 資料流的所有檔案。
      您也可以指定此檔案的備用資料串流的路徑。在這種情況下，您僅接收指定流的檔案。

建立工作時，應用程式不會檢查您要接收的檔案的指定路徑是否有效。

b. **MD5/SHA256**—您要接收的檔案的 MD5 或 SHA256 雜湊。該欄位是可選的。

c. 如果您不想掃描檔案，則清除**傳送以進行掃描**核取方塊。
預設已選擇該核取方塊。

d. **敘述**是工作描述。該欄位是可選的。

e. **主機**是主機的名稱或 IP 位址。
您只能指定一台主機。

4. 點擊**新增**。

將建立獲取檔案工作。工作建立後自動執行。

透過此工作接收的檔案將被放入儲存中。如果取得檔案工作成功完成，則可以將接收的檔案下載到本機。

如果您使用分佈式解決方案和多組織用戶模式，則壓縮檔案將被放置在主機所連線之 Central Node 伺服器的儲存中，而該主機是在**主機**欄位中指定的。

您也可以從工作報告視窗下載該檔案。

若要從工作報告視窗下載檔案：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
這將開啟工作表。

2. 開啟您想複製的取得檔案工作。

3. 在**報告**部分，點擊主機的名稱或 IP 位址。
這將開啟一個視窗，其中包含有關檔案的資訊。

4. 點擊**下載**。

該檔案將被儲存到瀏覽器下載資料夾中的本機電腦。

具有**安全稽核員**角色的使用者無法建立獲取檔案工作。

具有**安全官**角色的使用者無權存取工作。

建立取證收集工作

您可以從選定的 Endpoint Agent 主機取得檔案、處理程序和自動執行點的清單。為此，您必須建立取證收集工作。

若要建立取證收集工作：

1. 在應用程式網頁介面視窗中，選擇“**工作**”區域。

   這將開啟工作表。

2. 點擊**新增**按鈕並在**獲取資料**下拉清單中選擇**取證**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. **資訊類型**是所收集資料的類型。選擇一項、多項或所有設定旁的核取方塊：

      - **處理程序清單**，如果您想要取得工作執行時主機上執行的處理程序清單。

      - **自動執行點清單**，如果您想取得自動執行點的清單。

        自動執行點清單包括有關新增到啟動資料夾或在登錄檔的 Run 鍵中註冊的應用程式的資訊，以及在帶有 Endpoint Agent 元件的主機啟動時以及使用者登錄指定主機上的作業系統時自動執行的應用程式的資訊。

        支援的自動執行點清單

        Kaspersky Endpoint Agent 支援收集以下自動執行點的資料：

        - Logon。
        - Run。
        - Explorer。
        - Shell。
        - Office。
        - Internet Explorer®。
        - Tasks。
        - Services。
        - Drivers。
        - Telephony。
        - Cryptography。
        - Debuggers。
        - COM。
        - Session Manager。
        - Network。
        - LSA。

- Applications。
- Codecs。
- Shellex。
- WMI。
- Unspecified。

Kaspersky Endpoint Security 支援收集上述自動執行點以及以下內容：

- BootLog
- Browsers
- DriverLog
- EfiLoader
- GroupPolicy
- Logon
- OsLoader
- OsUpdate
- Printer
- Process
- Scheduler

- **檔案清單**，如果您想要取得工作執行時儲存在所選資料夾或所有主機資料夾中的檔案清單。

b. 如果您選擇了**檔案清單**核取方塊，在**來源類型**設定群組中選擇以下選項之一：

- **所有本機磁碟**，如果您希望檔案清單包含工作執行時儲存在本機磁碟上所有資料夾中的檔案。
- **目錄**，如果您希望檔案清單包含工作執行時間儲存在指定資料夾及其子資料夾中的檔案。

c. 如果您選擇了**目錄**，請在**啟動目錄**欄位中指定檔案搜尋應從其開始的資料夾路徑。

您可以使用以下前綴：

- 系統環境變數。
- 使用者定義的環境變數。

  使用使用者定義的環境變數時，檔案清單包含有關設定了指定環境變數的所有使用者的資料夾中的檔案的資訊。如果使用者定義的環境變數覆蓋系統環境變量，則檔案清單將根據系統環境變數的值包含資料夾中檔案的資訊。

d. 在**主機**欄位中，輸入要指派工作的主機的 IP 位址或名稱。

您可以指定多個主機。

e. 如有必要，您可以為資料夾中的檔案指定以下搜尋條件：

- **遮罩**是要包含在檔案清單中的檔案的遮罩。
- **備用資料流**是啟用在檔案清單中記錄備用資料串流的資訊的核取方塊。

  如果要求的檔案已連結到其他 NTFS 資料流，則執行該工作將產生請求的檔案連結到的 NTFS 資料流的所有檔案。

  預設已選擇該核取方塊。
- **最大嵌套級別**是應用程式在其中搜尋檔案的資料夾的最大嵌套層級。
- **排除項目**是要禁止在其中搜尋檔案資訊的資料夾的路徑。
- **敘述**是工作描述。

4. 點擊**新增**。

取證收集工作已建立。工作建立後自動執行。

作為工作的結果，應用程式將 ZIP 壓縮檔案放置在儲存中；壓縮檔案包含包含所選資料的檔案。如果工作成功完成，您可以將壓縮檔案下載到本機。

具有**安全稽核員**角色的使用者無法建立取證收集工作。

具有**安全官**角色的使用者無權存取工作。

建立登錄機碼檢索工作

您可以從所選具有 Endpoint Agent 元件的主機擷取登錄機碼。為此，您必須建立登錄機碼檢索工作。

若要建立登錄機碼檢索工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**按鈕，並在**獲取資料**下拉清單中選擇**登錄機碼**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. **登錄機碼** — 您想要取得的登錄機碼。

   您可以採用以下格式之一輸入登錄機碼：

   - 相對於根金鑰。

     例如，\REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。
   - 相對於根金鑰的完整名稱。

     例如，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。

- 相對於用縮寫代替根金鑰的完整名稱。

  例如，HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator。

> 如果要從 HKEY_CURRENT_USER 取得資料，您必須指定 HKEY_USERS 和使用者的 SID：HKEY_USERS\<SID of the user>。

b. **敘述**是工作描述。該欄位是可選的。

c. 在**主機**欄位中，輸入要指派工作的主機的名稱或 IP 位址。

   您可以指定多個主機。

4. 點擊**新增**。

登錄機碼檢索工作已建立。工作建立後自動執行。

作為工作的結果，應用程式將 ZIP 壓縮檔案放置在儲存中；該壓縮檔案包含一個 .reg 檔案，其中包含所有登錄機碼以及建立工作時指定的項目下的值的清單。您可以將壓縮檔案下載到本機。

如果工作導致錯誤，壓縮檔案檔案將包含錯誤的描述。

> 具有**安全稽核員**角色的使用者無法建立此工作。

> 具有**安全官**角色的使用者無權存取工作。

建立 NTFS 中繼檔檢索工作

您可以從所選具有 Endpoint Agent 元件的主機擷取NTFS 中繼檔。為此，您必須建立 NTFS 中繼檔檢索工作。

若要建立 NTFS 中繼檔檢索工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**按鈕，並在**獲取資料**下拉清單中選擇**NTFS 元檔案**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. **元檔案**是您可以使用該工作取得的中繼檔清單。透過選擇相應的核取方塊來選擇相關中繼檔。

      您可以選擇多個中繼檔。

   b. **卷**是您要從中取得中繼檔的磁碟名稱。

      預設指定係統盤。您可以以 `<drive letter>:` 格式輸入不同磁碟的路徑。

   c. **敘述**是工作描述。該欄位是可選的。

d. **主機**是要指派工作的主機的名稱或 IP 位址。

您只能指定一台主機。

4. 點擊**新增**。

NTFS 中繼檔建立工作已建立。工作建立後自動執行。

工作完成後，應用程式會將包含所選中繼檔的 Zip 壓縮檔案放置在儲存中。您可以將壓縮檔案下載到本機。

如果工作導致錯誤，壓縮檔案檔案將包含錯誤的描述。

如果您使用分佈式解決方案和多組織用戶模式，則壓縮檔案將被放置在主機所連線之 Central Node 伺服器的儲存中，而該主機是在**主機**欄位中指定的。

如果下載選定的元檔案耗盡了儲存容量，則儲存中的物件將被輪換。如果某元檔案大於總儲存容量，則不會下載它。

具有**安全稽核員**角色的使用者無法建立此工作。具有**安全官**角色的使用者無權存取工作。

建立處理程序記憶體傾印檢索工作

您可以從所選具有 Endpoint Agent 元件的主機擷取處理程序記憶體傾印。為此，您必須建立處理程序記憶體傾印檢索工作。

建立處理程序記憶體傾印檢索工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

這將開啟工作表。

2. 點擊**新增**按鈕並在**獲取資料**下拉清單中選擇**處理程序記憶體傾印**。

這將開啟工作建立視窗。

3. 配置以下設定：

a. **處理程序 ID**是要取得其記憶體傾印的處理程序的 ID。

b. **MD5/SHA256**是要取得其記憶體傾印的程序的檔案的 MD5 或 SHA256 雜湊值。該欄位是可選的。

c. **敘述**是工作描述。該欄位是可選的。

d. **主機**是要指派工作的主機的名稱或 IP 位址。

您只能指定一台主機。

4. 點擊**新增**。

建立處理程序記憶體傾印檢索工作。工作建立後自動執行。

此工作會在儲存中建立一個ZIP 壓縮檔案，其中包含一個包含處理程序資訊的檔案和一個處理程序記憶體傾印檔案。您可以將壓縮檔案下載到本機。

如果工作導致錯誤，壓縮檔案檔案將包含錯誤的描述。

如果您使用分佈式解決方案和多組織用戶模式，則壓縮檔案將被放置在主機所連線之 Central Node 伺服器的儲存中，而該主機是在**主機**欄位中指定的。

具有**安全稽核員**角色的使用者無法建立此工作。

具有**安全官**角色的使用者無權存取工作。

建立磁碟映像檢索工作

您可以從選定的 Kaspersky Endpoint Agent for Windows 主機擷取磁碟映像。為此，您必須建立 NTFS 磁碟映像檢索工作。

產生的檔案只能儲存到共用網路資源。

建立磁碟映像檢索工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**新增**按鈕，並在**獲取資料**下拉清單中選擇**磁碟鏡像**。
   這將開啟工作建立視窗。
3. 配置以下設定：
   a. **共用路徑**—共用網路資源的路徑。
      您需要以通用命名約定 (UNC) 格式指定路徑：`\\server\share\path`。
   b. **使用者名稱**—用於存取共用網路資源的帳戶使用者名稱。
   c. **密碼**—用於存取共用網路資源的帳戶密碼。
   d. 在**磁碟類型**下，選擇以下其中一個選項：
      - **邏輯**。
      - **物理的**。
   e. 如果您選擇了**邏輯**，請在**卷**欄位中輸入 `%SystemDrive%` 變數或不含冒號和斜線的磁碟機代號。
   f. 如果您選擇了**物理的**，請在**物理磁碟機**欄位中輸入磁碟號。
   g. 如果您希望在儲存時將檔案分為多個部分，請選擇**將檔案拆分為多個部分**核取方塊。
   h. 如果您選擇了該核取方塊，請在**部分大小，GB**欄位中指定已儲存檔案的一部分的最小大小。
      最小部分大小必須大於 1 GB。

i. **敘述**—工作描述。該欄位是可選的。

j. **主機**—您想要指派工作的主機的 IP 位址或名稱。

4. 點擊**新增**。

磁碟映像檢索工作將會建立。工作建立後自動執行。

應用程式會將包含一個或多個 EWF 或 RAW 格式檔案的檔案放置在網路共用中。您可以將檔案從 RAW 格式轉換為 EWF 格式。

具有**安全稽核員**角色的使用者無法建立工作。

具有**安全官**角色的使用者無權存取工作。

將檔案從 RAW 轉換為 EWF 格式

Kaspersky Endpoint Security 將磁碟映像儲存為 RAW 格式。檔案也可以被壓縮到壓縮檔案中。特殊的 Python 指令碼允許將檔案從 RAW 格式轉換為 EWF 格式。該指令碼不斷在指定資料夾中尋找 RAW 檔案。如果偵測到此類檔案，指令碼會自動將檔案轉換為 EWF 格式。

Convert_to_ewf_monitor.py 指令碼

為了使指令碼正常工作，電腦上必須安裝以下軟體：

- 用於存取專家見證壓縮格式(EWF) 檔案的 Libewf 函式庫。

  libewf 庫是開源軟體。

  建議將庫檔案和指令碼檔案放在同一資料夾中。

- Python 直譯器。

若要啟用磁碟映像檔的轉換：

1. 啟動命令列解釋器。

2. 變更為指令碼所在的資料夾。

3. 執行以下指令：

```
py Convert_to_ewf_monitor.py --source <來源檔案資料夾的完整路徑> [其他設定]
```

EWF 轉換指令碼參數

參數	敘述
`--source <資料夾的完整路徑>`	指令碼在其中尋找來源檔案的資料夾的完整路徑。該指令碼也會在指定路徑的子資料夾中尋找檔案。這是一個強制參數。
`--destination <資料夾的完整路徑>`	指令碼在其中儲存轉換後的檔案的資料夾的完整路徑。資料夾結構被保留。預設情況下，指令碼將轉換後的檔案儲存在 `source` 參數中指定的資料夾中。
`--delete`	轉換成功後刪除來源檔案。如果轉換失敗，指令碼會跳過刪除來源檔案，您可以重試。
`--ewftool <資料夾的完整路徑>`	ewfacquirestream.exe 檔案的完整路徑。路徑必須包含檔案名稱。預設情況下，指令碼嘗試在指令碼所在的資料夾中尋找 ewfacquirestream.exe 檔案。

參數	敘述
`--name_mask <正規表達式>`	用於尋找要轉換的來源檔案的正規表達式。如果您需要轉換單個檔案，可以使用此選項。預設情況下，該指令碼使用`^diskdump_`正規表達式來尋找檔案。
`--convert_single_dump`	找到要轉換的單個檔案。成功轉換單個檔案後，指令碼結束。
`--workers_num <檔案數量>`	指令碼可以同時轉換的來源檔案的最大數量。您可以使用此設定來最佳化指令碼的效能。預設情況下，該指令碼一次最多可以轉換四個檔案。
`--log_level <記錄等級>`	記錄級別。預設情況下，指令碼使用DEBUG 日誌記錄等級。
`--ewftool <資料夾的完整路徑>`	儲存日誌檔案的完整路徑。該路徑必須包含日誌檔案的檔案名稱。預設情況下，指令碼在解釋器主控台上顯示事件。

範例：
```
PS D:\Folder\Script\> py convert_to_ewf_monitor.py --source E:/Folder --destination E:/EWF --delete --log_path
E:/Folder/Logs.txt
```

建立 RAM 傾印檢索工作

您可以從所選具有 Endpoint Agent 元件的主機擷取 RAM 傾印。為此，您必須建立記憶體傾印檢索工作。

產生的檔案只能儲存到共用網路資源。

若要建立記憶體傾印檢索工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**新增**按鈕並在**獲取資料**下拉清單中選擇**記憶體傾印**。
   這將開啟工作建立視窗。
3. 配置以下設定：
   a. **共用路徑**—共用網路資源的路徑。
      您需要以通用命名約定 (UNC) 格式指定路徑：`\\server\share\path`。
   b. **使用者名稱**—用於存取共用網路資源的帳戶使用者名稱。
   c. **密碼**—用於存取共用網路資源的帳戶密碼。
   d. **敘述**—工作描述。該欄位是可選的。
   e. **主機**—您想要指派工作的主機的 IP 位址或名稱。
4. 點擊**新增**。

RAM 傾印檢索工作已建立。工作建立後自動執行。

結果，應用程式會將 RAW 檔案或包含 RAW 檔案的壓縮檔案放置在共用網路資源上。

具有**安全稽核員**角色的使用者無法建立工作。

具有**安全官**角色的使用者無權存取工作。

建立處理程序終止工作

如果您認為在電腦上執行的程序可能威脅到電腦或企業 LAN 的安全，您可以終止該處理程序。

若要建立處理程序終止工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**並選擇**殺死處理程序**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. **檔案路徑** — 您想要終止的處理程序檔案的路徑。

      您也可以指定此檔案的備用資料串流的路徑。在這種情況下，只會終止指定資料流的處理程序。將執行此檔案的其他流的處理程序。

   b. **MD5/SHA256**—要終止的程序檔案的 MD5 或 SHA256 雜湊。該欄位是可選的。

   c. **敘述**是工作描述。該欄位是可選的。

   d. **工作所有者** — 工作範圍：

      - 如果您想在所有伺服器的所有主機上執行工作，請選擇**所有主機**選項。
      - 如果要在選定的伺服器上執行工作，請選擇**指定伺服器**選項，並在**伺服器**參數名稱的右側，選取要在其上執行工作的伺服器名稱旁的核取方塊。

        僅當啟用分散式解決方案和多組織用戶模式時，此選項才可用。

      - 如果您想要執行選定主機上的工作，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

4. 點擊**新增**。

   將建立處理程序終止工作。工作建立後自動執行。

具有**安全稽核員**角色的使用者無法建立處理程序終止工作。

具有**安全官**角色的使用者無權存取工作。

建立工作以使用 YARA 規則掃描主機

您可以使用 YARA 規則掃描具有 Endpoint Agent 元件的主機。為此，您必須建立一個**啟動 YARA 掃描**工作。您可以建立工作：

- 在**工作**部分。

  在這種情況下，在建立工作時，您必須選擇要用於掃描主機的 YARA 規則。

- 在**自訂規則**部分，**YARA**子部分。

  在這種情況下，將建立一個工作來使用選定的 YARA 規則掃描主機。

*若要使用 YARA 規則建立掃描具有 Kaspersky Endpoint Agent 元件的主機的工作，請在**工作**部分：*

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**並選擇**啟動 YARA 掃描**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. **選擇規則**是規則的名稱。您可以輸入規則名稱或規則名稱中的字元序列，然後在清單中選擇規則。

   您可以新增多個規則。

   b. **掃描**是掃描範圍。您可以選擇以下選項之一：

   - **記憶體**，如果您想要掃描工作執行時正在執行的處理程序。

     應用程式不會掃描低優先順序的處理程序。

   - **自動執行點**，如果您想掃描從**進行取證**工作獲取的自動執行點。

     若要掃描自動執行點，您必須指定先前為其執行過**進行取證**的主機。

   - **指定目錄**，如果您想要掃描在工作執行時位於指定資料夾及其所有嵌套資料夾中的檔案。

   - **所有本機磁碟**，如果您希望掃描工作執行時儲存在本機磁碟上所有資料夾中的檔案。

     掃描所有本機磁碟可能會導致主機負載過高。

   c. 如果您選擇了**記憶體**，必要時請執行以下操作：

   - 在**處理程序**欄位中，輸入要掃描的處理程序的短名稱或檔案遮罩。

     應用程式掃描主機上執行的所有具有相同名稱的處理程序。

     如果**處理程序**欄位留空，應用程式將掃描工作執行時正在運行的所有處理程序，除了 PID 小於 10 的處理程序和**排除項目**欄位中所列的處理程序。

- 在**排除項目**欄位中，輸入要從掃描中排除的處理程序的完整名稱或檔案遮罩。

  如果主機上正在執行多個具有相同名稱的處理程序，應用程式將從掃描中排除所有此類處理程序。

d. 如果您選擇了**自動執行點**，在**掃描類型**欄位中，選擇掃描類型：

- **快速**。

  在這種情況下，將掃描除 COM 物件之外的所有自動執行點。

- **完整**。

  在這種情況下，將掃描所有自動執行點以及與其相關的檔案。

> 如果您使用 Kaspersky Endpoint Security for Windows 作為 Endpoint Agent 元件，則無論選擇的設定為何，都會執行完整掃描。

e. 如果您選擇了**指定目錄**：

- 在**指定目錄**欄位中，以 C:\<directory name>* 格式指定目錄路徑。

- 在**排除項目**欄位中，以 C:\<directory name>* 格式指定目錄路徑。

f. **最大掃描持續時間**是最大掃描持續時間。

  當該時間過去後，即使未套用某些規則來掃描主機，掃描也會停止。工作報告包含掃描停止時的最新結果。

g. **敘述**是工作描述。該欄位是可選的。

h. **工作所有者**是工作範圍：

- 如果您想要在所有伺服器的所有主機上執行工作，請選擇**所有主機**選項。

- 如果要在選定的伺服器上執行工作，請選擇**指定伺服器**選項，並在**伺服器**參數名稱的右側，選取要在其上執行工作的伺服器名稱旁的核取方塊。

  僅當啟用分散式解決方案和多組織用戶模式時，此選項才可用。

- 如果您想要執行選定主機上的工作，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

*若要在**自訂規則**區段的**YARA**子區段中，建立使用 YARA 規則掃描 Kaspersky Endpoint Agent for Windows 主機的工作：*

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**區段的**YARA**子區段。

2. 選擇掃描主機時要使用的規則左側的核取方塊。

   控制面板出現在視窗的下部。

3. 點擊**啟動 YARA 掃描**。

4. 執行上述說明的步驟 3。

工作建立完成。工作建立後自動執行。

如果掃描偵測到任何威脅，Kaspersky Anti Targeted Attack Platform 會建立對應的警示。

具有**安全稽核員**角色的使用者無法建立使用 YARA 規則掃描主機的工作。

具有**安全官**角色的使用者無權存取工作。

建立服務管理工作

您可以在具有 Endpoint Agent 元件的所選主機上遠端啟動、停止、暫停或還原服務，以及刪除服務或變更啟動類型。為此，您必須建立服務管理工作。

建立服務管理工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**並選擇**管理服務**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. 在**服務名稱**欄位中，輸入服務名稱。

   b. 在**MD5/SHA256**欄位中，輸入服務的 MD5 或 SHA256 雜湊值。該欄位是可選的。

   如果您輸入從 DLL 載入的服務的雜湊值，Kaspersky Anti Targeted Attack Platform 會同時將指定的雜湊值與服務 DLL 的雜湊值和 Svchost 程序的雜湊值進行比較。

   c. 在**操作**欄位中，選擇您要對服務執行的操作。

   該應用程式支援以下服務操作：

   - **開始**。
   - **停止**。
   - **暫停**。
   - **還原**。
   - **刪除**。
   - **修改啟動類型**。

   當您刪除某個服務時，該服務啟動的程序將繼續執行，直到系統重新啟動或該程序終止。

   d. 如果您選擇了**修改啟動類型**，請在**啟動類型**中選擇服務的啟動類型。

   e. **敘述**是工作描述。該欄位是可選的。

f. **工作所有者**是工作範圍：

- 如果您想要在所有伺服器的所有主機上執行工作，請選擇**所有主機**選項。
- 如果要在選定的伺服器上執行工作，請選擇**指定伺服器**選項，並在**伺服器**參數名稱的右側，選取要在其上執行工作的伺服器名稱旁的核取方塊。

  僅當啟用分散式解決方案和多組織用戶模式時，此選項才可用。
- 如果您想要執行選定主機上的工作，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

4. 點擊**新增**。

服務管理工作已建立。工作建立後自動執行。

強烈建議不要停止、暫停、刪除服務或變更影響主機功能的服務啟動類型。

不建議管理的服務清單

- AVP*。
- BFE。
- CertPropSvc。
- CoreMessagingRegistrar。
- CryptSvc。
- DcomLaunch。
- Dhcp。
- DispBrokerDesktopSvc。
- EventLog。
- EventSystem。
- LanmanServer。
- LanmanWorkstation。
- LSM。
- mpssvc。
- Netlogon。
- Netman。
- PlugPlay。
- PolicyAgent。
- Power。
- ProfSvc。
- RasMan。
- RpcEptMapper。
- RpcS。
- SamSs。
- SCardSvr。
- SecurityHealthService。
- SessionEnv。
- Spooler。
- SstpSvc。
- TermService。
- UmRdpService。
- UserManager。
- UsoSvc。
- VaultSvc。
- W32Time。
- WebClient。
- Winmgmt。
- WlanSvc。
- wscsvc。

具有**安全稽核員**角色的使用者無法建立服務管理工作。

具有**安全官**角色的使用者無權存取工作。

建立應用程式執行工作

您可以建立應用程式運行工作或命令執行工作。

如果在執行工作時標準輸出檔案或錯誤輸出檔案的大小達到 100 KB，則會從檔案中刪除一些資料。該檔案不包含所有資料。

若要建立運行應用程式或執行命令的工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**並選擇**執行應用程式**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. 在**檔案路徑**和**工作目錄**欄位中，透過以下方式之一輸入值：

      - 在**檔案路徑**欄位中，輸入可執行檔的完整路徑（例如，`C:\Windows\System32\ipconfig.exe`）。留下**工作目錄**欄位為空。

        建立工作時，應用程式不會檢查指定的可執行檔路徑是否有效。

      - 在**檔案路徑**欄位中，輸入可執行檔的名稱和副檔名（例如 `ipconfig.exe`）。在**工作目錄**欄位中，輸入工作目錄（例如 `C:\Windows\System32\`）。

   b. 在**參數**欄位中，輸入用於執行檔案或工作的其他選項（例如 `/all` 參數）。

   c. 在**敘述**欄位中，輸入工作描述。該欄位是可選的。

d. 配置**工作所有者**設定，即工作範圍：

- 如果您想要在所有伺服器的所有主機上執行工作，請選擇**所有主機**選項。
- 如果要在選定的伺服器上執行工作，請選擇**指定伺服器**選項，並在**伺服器**參數名稱的右側，選取要在其上執行工作的伺服器名稱旁的核取方塊。

  僅當啟用分散式解決方案和多組織用戶模式時，此選項才可用。
- 如果您想要執行選定主機上的工作，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

4. 點擊**新增**。

應用程式運行工作或命令執行工作已建立。工作建立後自動執行。

範例：
若要在 IP 位址為 `10.10.10.1` 的主機上執行 `ipconfig /all` 命令：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**新增**並選擇**執行應用程式**。
   這將開啟工作建立視窗。
3. 配置以下設定：
   a. 在**檔案路徑**和**工作目錄**欄位中，透過以下方式之一輸入值：
      - 在**檔案路徑**欄位中，輸入 `C:\Windows\System32\ipconfig.exe`。留下**工作目錄**欄位為空。
      - 在**檔案路徑**欄位中，輸入 `ipconfig.exe`。在**工作目錄**欄位中，輸入 `C:\Windows\System32\`。

   b. 在**參數**欄位中，輸入 `/all`。

   c. 在**敘述**欄位中，輸入工作描述。

   d. 選擇**指定主機**工作範圍。

   e. 在**主機**欄位中，開始輸入 IP 位址 `10.10.10.1` 的字元，當下面的搜尋結果下拉清單中顯示該 IP 位址時，選擇它。
4. 點擊**新增**。

具有**安全稽核員**角色的使用者不能建立應用程式運行工作或命令執行工作。

具有**安全官**角色的使用者無權存取工作。

建立檔案刪除工作

若要建立檔案刪除工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。

2. 點擊**新增**並選擇**刪除檔案**。

   這將開啟工作建立視窗。

3. 配置以下設定：

   a. **檔案路徑** — 您想要刪除的檔案的路徑。

      您也可以指定此檔案的備用資料串流的路徑。在這種情況下，只會刪除指定的資料流。此檔案的其他資料流將保持不變。

   b. **MD5/SHA256** — 要刪除的檔案的 MD5- 或 SHA256 雜湊。該欄位是可選的。

   c. **敘述**是工作描述。該欄位是可選的。

   d. **工作所有者** — 工作範圍：

      - 如果您想在所有伺服器的所有主機上執行工作，請選擇**所有主機**選項。
      - 如果要在選定的伺服器上執行工作，請選擇**指定伺服器**選項，並在**伺服器**參數名稱的右側，選取要在其上執行工作的伺服器名稱旁的核取方塊。

        僅當啟用分散式解決方案和多組織用戶模式時，此選項才可用。

      - 如果您想要執行選定主機上的工作，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

4. 點擊**新增**。

將建立檔案刪除工作。工作建立後自動執行。

如果該檔案已被另一個處理程序封鎖，則該工作將顯示為*已完成*狀態，但該檔案僅在主機重新啟動後才會刪除。建議在主機重新啟動後檢查檔案是否成功刪除。

不支援從已映射的網路磁碟機中刪除檔案。

具有**安全稽核員**角色的使用者無法建立檔案刪除工作。

具有**安全官**角色的使用者無權存取工作。

建立檔案隔離工作

如果您認為具有 Endpoint Agent 元件的電腦上存在感染檔案或疑似感染檔案，可以透過將其放入隔離區中將其隔離。

若要建立檔案隔離工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**新增**並選擇**隔離檔案**。
   這將開啟工作建立視窗。

3. 配置以下設定：

   a. 在**檔案路徑**欄位中，輸入要隔離的檔案路徑。

   b. 在**MD5/SHA256**欄位中，輸入要隔離的檔案的 MD5 或 SHA256 雜湊值。該欄位是可選的。

   c. **敘述**是工作描述。該欄位是可選的。

   d. 在**主機**欄位中，輸入要指派工作的主機的名稱或 IP 位址。
      您可以指定多個主機。

   e. 點擊**新增**。

檔案隔離工作已建立。工作建立後自動執行。
作為工作結果：

- 檔案將被從其所在電腦的資料夾中刪除，並移至同一電腦上的隔離目錄，該目錄是在配置用作 Endpoint Agent 元件的應用程式期間指定的。
- 在應用程式 Web 介面的**工作**區域工作清單中，會顯示工作的執行資訊。
- 在**儲存**區域的**隔離區**子區域檔案清單中，會顯示已隔離檔案的資訊。

如果檔案已被另一個處理程序封鎖，工作會顯示為*已完成*狀態，但只有在主機重新啟動後，檔案才會被放入隔離區。建議在主機重新啟動後檢查工作是否已成功完成。

如果您嘗試隔離可執行檔並且該檔案目前正在運行，則檔案隔離工作可以完成但會有**拒絕存取**錯誤。

若要解決此問題，請為此檔案建立處理程序終止工作，然後嘗試再次建立檔案隔離工作。

具有**安全稽核員**角色的使用者無法建立檔案隔離工作。

具有**安全官**角色的使用者無權存取工作。

建立隔離檔案還原工作

如果您認為先前隔離的檔案是安全的，則可以將其從隔離區還原到主機。

若要從隔離區建立還原檔案的工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**新增**並選擇**從隔離區還原檔案**。
   這將開啟工作建立視窗。
3. 配置以下設定：
   a. **敘述** — 工作描述。該欄位是可選的。
   b. **檔案搜尋** — 隔離區中檔案的名稱。
4. 點擊**新增**。

從隔離區還原檔案的工作已建立。工作建立後自動執行。

將檔案從隔離區還原到主機後，有關該檔案的中繼資料將保留在儲存區中的物件表中。

在分佈式解決方案和多組織用戶模式下，在 SCN 伺服器上被隔離的檔案無法在 PCN 伺服器上還原。您可以在建立隔離檔案工作的 SCN 伺服器上還原檔案。

具有**安全稽核員**角色的使用者無法建立從隔離區還原檔案的工作。

具有**安全官**角色的使用者無權存取工作。

建立工作副本

要複製工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 開啟您想複製的工作。
3. 點擊**複製**。
   這將開啟工作建立視窗。將複製所有工作設定。

4. 如果您想要修改工作設定，請根據正在複製的工作類型編輯一項或多項設定。

5. 點擊**新增**。

將建立選定工作的副本。

具有**安全稽核員**角色的使用者無法複製工作。

具有**安全官**角色的使用者無權存取工作。

刪除工作

如果您在工作執行時將其刪除，則可能不會儲存工作結果。

如果您刪除成功完成的檔案下載工作，則該檔案也會被刪除。

若要刪除工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。

2. 開啟您想刪除的工作。

3. 點擊**刪除**。
   這將開啟操作確認視窗。

4. 點擊**是**。

該工作將被刪除。

刪除全部或多個工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。

2. 選擇要刪除的工作旁邊的核取方塊。
   您可以透過選取包含列標題的行中的核取方塊來選擇所有工作。

3. 在視窗下部顯示的窗格中，點擊**刪除**。
   這將開啟操作確認視窗。

4. 點擊**是**。

選定的工作被刪除。

具有**安全稽核員**角色的使用者無法刪除工作。

具有**安全官**角色的使用者無權存取工作。

依建立時間篩選工作

若要按建立時間篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。

2. 點擊**時間**連結以開啟工作篩選功能表。

3. 選擇以下工作顯示時段之一：

   - **所有**，如果您希望應用程式顯示表中建立的所有工作。
   - **上一個小時**，如果您希望應用程式顯示表中最後一小時建立的工作。
   - **最後一天**，如果您希望應用程式顯示表中最後一天建立的工作。
   - **自訂範圍**，如果您希望應用程式顯示表中指定期間建立的工作。

4. 如果您選擇了**自訂範圍**工作顯示時段：

   a. 這將開啟日曆；在日曆中，指定工作顯示期間的開始日期和結束日期。

   b. 點擊**套用**。

   日曆關閉。

工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

按類型篩選工作

如果您使用分散式解決方案和多組織用戶模式，您可以按工作類型篩選工作。

若要按類型篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**類型**連結以開啟工作篩選功能表。

3. 選擇以下工作顯示選項之一：

   - **所有**，如果您想顯示所有工作，無論其類型為何。
   - **全球**，如果您只想顯示在 PCN 伺服器上建立的工作。這些工作適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。工作屬於使用者為其使用 Web 介面管理程式的租戶。
   - **本機**，如果您只想顯示在 SCN 伺服器上建立的工作。這些工作僅適用於連線到此 SCN 伺服器的主機。工作屬於使用者為其使用 Web 介面管理程式的租戶。

工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

按名稱篩選工作

若要按名稱篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**名稱**連結以開啟工作篩選功能表。

3. 選擇一個或多個核取方塊：

   - **殺死處理程序**。
   - **執行應用程式**。
   - **進行取證**。
   - **啟動 YARA 掃描**。
   - **管理服務**。
   - **獲取檔案**。

- **刪除檔案**。
- **隔離檔案**。
- **還原檔案**。

4. 點擊**套用**。

工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

按檔案名稱和路徑篩選工作

您可以根據**詳細資訊**條件— 檔案或資料流的名稱和路徑來篩選工作。

若要依照檔案或資料流的名稱和路徑篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**詳細資訊**連結以開啟工作篩選配置視窗。
3. 在右側的下拉清單中，選擇**詳細資訊**。
4. 在左側下拉清單中，選擇下列篩選運算子工作之一：
   - **包含**。
   - **不包含**。
   - **等於**。
   - **不等於**。
5. 在輸入欄位中，指定檔案名稱或路徑的一個或多個字元。
6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
7. 點擊**套用**。

工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

依描述篩選工作

您可以透過**敘述**條件、即建立工作時所新增的工作描述來篩選工作。

若要依描述篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。
2. 點擊**詳細資訊**連結以開啟工作篩選配置視窗。
3. 在左側的下拉清單中，選擇**敘述**。
4. 在右側的下拉清單中，選擇下列工作篩選運算子之一：
   - **包含**。
   - **不包含**。
   - **等於**。
   - **不等於**。
5. 在輸入欄位中，指定檔案名稱或路徑的一個或多個字元。
6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
7. 點擊**套用**。

工作表將僅顯示與您設定的篩選條件相符的工作。

> 您可以同時使用多個篩選器。

按伺服器名稱篩選工作

如果您使用分佈式解決方案和多組織用戶模式，您可以根據套用工作的伺服器來篩選工作。

若要按應用程式工作的伺服器篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。

2. 點擊**伺服器**連結以開啟工作篩選功能表。

3. 選擇要顯示其工作的伺服器名稱旁的核取方塊。

   工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

根據建立工作的使用者的名稱篩選工作

若要根據建立工作的使用者名稱篩選工作，必須顯示所有工作。如果只顯示目前使用者建立的工作，則無法依使用者名稱篩選工作。

依照建立工作的使用者的名稱篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**建立者**連結以開啟工作篩選功能表。

3. 在下拉清單中，選擇下列工作篩選運算子之一：

   - **包含**
   - **不包含**

4. 在輸入欄位中，指定使用者名稱的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

   工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

按處理狀態篩選工作

要根據使用者處理工作的狀態篩選工作：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。

   這將開啟工作表。

2. 點擊**狀態**連結以開啟工作篩選功能表。

3. 選擇一個或多個核取方塊：

   - **等待**。
   - **進行中**。
   - **已完成**。

4. 點擊**套用**。

工作表將僅顯示與您設定的篩選條件相符的工作。

您可以同時使用多個篩選器。

清除工作篩選器

若要清除一個或多個篩選條件的工作篩選器：

1. 在應用程式網頁介面視窗中，選擇**工作**區域。
   這將開啟工作表。

2. 點擊您想要清除其篩選條件的表列標題右側的 ⊠。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選器將會被清除。

工作表將僅顯示與您設定的篩選條件相符的工作。

管理政策（阻止規則）

在應用程式 Web 介面中工作時，具有**資深安全員**角色的使用者可以管理選定主機上檔案和處理程序的阻止規則。例如，您可以阻止執行您認為在具有 Endpoint Agent 元件的選定主機上使用不安全的應用程式。該應用程式透過使用 MD5 和 SHA256 雜湊演算法基於檔案雜湊識別檔案。您可以建立、啟用、停用、刪除和修改防止規則。此外，您還可以點擊阻止規則表中帶有雜湊演算法名稱的連結來尋找觸發了阻止規則的物件、事件或警示，例如“**尋找事件**”、“**尋找警示**”、“**在 Kaspersky TIP 上尋找**”或“**在 virustotal.com 上尋找**”。

在分散式解決方案和多組織用戶模式下，阻止規則可以有以下類型：

- **全球** — 在 PCN 上建立。這些阻止規則適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。
- **本機** — 在 SCN 伺服器上建立。這些阻止規則僅適用於連線到此 SCN 伺服器的主機。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。

具有**資深安全員**角色的使用者可以為他們有權存取其資料的租用戶建立、編輯、刪除、啟用、停用和匯入阻止規則。

具有**安全官**角色的使用者無權存取政策。

具有**安全稽核員**角色的使用者可以檢視檔案執行阻止規則和處理程序執行阻止規則表，以及所選阻止規則的資訊，但不能編輯規則。

在與選定主機建立授權連線之後，所有阻止規則變更都會套用到主機上。如果與主機沒有連線，則舊的阻止規則將繼續套用於主機。對阻止規則的變更不會影響已在執行的處理程序。

阻止規則可以根據預設新增的預設政策（以下也稱為"預設"）自動建立。開啟預設時，阻止規則將根據 Sandbox 元件的中度或高嚴重性警示建立。這樣建立的阻止規則會根據檔案的 MD5 雜湊值來阻止執行該檔案。具有**資深安全員**角色的使用者可以啟用和停用預設。

分散式解決方案和多組織用戶模式不支援預設。

對於自動建立或匯入的阻止規則，可以套用與手動建立的規則相同的操作。

您只能為每個檔案雜湊建立一條阻止規則。

系統中支援的最大阻止規則數量為 50000 條。

僅當 Endpoint Agent 元件在主機上執行時才會強制執行阻止規則。如果在啟動元件之前或在主機上關閉元件之後嘗試執行檔案，則該檔案不會被阻止運行。

只有當 Endpoint Agent 元件與 Central Node 伺服器整合時，您才可以使用政策管理選定主機上的檔案和處理程序執行封鎖規則；為此，您必須使用 Kaspersky Anti Targeted Attack Platform 的 Web 介面。

如果您使用 Kaspersky Endpoint Security for Windows 作為 Endpoint Agent 元件，則必須考慮到該應用程式支援阻止執行具有某些副檔名的 Office 格式檔案和某些指令碼解釋器。

檢視阻止規則表

防止規則表位於應用程式 Web 介面視窗的**阻止**部分。

表包含以下資訊：

1. **類型**是規則的類型，取決於應用程式的操作模式和產生規則的伺服器的角色：

   - **全球** — 在 PCN 上建立。這些阻止規則適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。

   - **本機** — 在 SCN 伺服器上建立。這些阻止規則僅適用於連線到此 SCN 伺服器的主機。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。

2. **名稱** — 阻止規則的名稱。

3. **建立者**—其帳戶被用於建立規則的使用者名稱。

4. **檔案雜湊值**—套用於識別檔案的雜湊演算法。
   可以基於以下雜湊演算法之一識別檔案：

   - **MD5**。
   - **SHA256**。

   點擊具有雜湊演算法名稱的連結將開啟一個清單，您可以檢視檔案雜湊並從其中選擇以下操作之一：

   - **新增到篩選器**。
   - **從篩選器中排除**。
   - 在 Kaspersky TIP 上尋找。
   - **在 virustotal.com 上尋找**（適用於 SHA256）。
   - 尋找事件。
     執行此操作時，將開啟**威脅搜尋**部分，其中具有根據您選定的雜湊已經篩選的事件。
   - 尋找警示。
     執行此操作時，**警示**部分將開啟，其中具有根據您選定的雜湊已經篩選的警示。
   - 啟用阻止規則。
   - 停用阻止規則。
   - 刪除阻止規則。
   - **複製值到剪貼簿**。

5. **伺服器**是具有 PCN 或 SCN 角色的伺服器名稱，阻止規則會套用至這些伺服器。
   如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄位。

6. **主機**是具有 Central Node 元件且阻止規則套用至其主機之伺服器的名稱。
   僅當您使用獨立的 Central Node 伺服器時才會顯示此欄位。

7. **狀態**是阻止規則的目前狀態。
   阻止規則可具有下列狀態之一：

   - **已啟用**。
   - **已停用**。

配置阻止規則表顯示

您可以顯示或隱藏列以及變更阻止規則表中列的順序。

若要設定防止規則表顯示：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表

2. 在表格的標題部分，點擊 ⚙ 。
   這將開啟**自訂表格**視窗。

3. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   > 必須選擇至少一個核取方塊。

4. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。

5. 如果要還原預設表格顯示設定，請點擊**預設**。

6. 點擊**套用**。

阻止規則表顯示已設定。

檢視防止規則

檢視防止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表

2. 選擇要檢視的防禦規則。

阻止規則包含以下資訊：

- 事件連結會開啟**威脅搜尋**區段，其中包含所選阻止規則的搜尋條件。
- **狀態**是阻止規則的目前狀態。
  阻止規則可具有下列狀態之一：
  - **已啟用**。
  - **已停用**。
- **詳細資訊**索引標籤包含以下資訊：
  - **MD5/SHA256**是遭阻止執行的檔案雜湊。
    點擊**MD5/SHA256**連結會開啟一個清單，您可以從中選擇下列其中一項操作：
    - 在 Kaspersky TIP 上尋找。
    - **尋找事件**。

- **尋找警示**。
- **複製值到剪貼簿**。

- **名稱**是阻止規則或遭阻止執行的檔案名稱。
- **類型**是規則的類型，取決於應用程式的操作模式和產生規則的伺服器的角色：
  - **全球** — 在 PCN 上建立。這些阻止規則適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。
  - **本機** — 在 SCN 伺服器上建立。這些阻止規則僅適用於連線到此 SCN 伺服器的主機。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。
- **通知**是**通知使用者阻止檔案執行**設定的狀態。
- **阻止於**是套用阻止規則的主機清單。

  如果阻止措施在所有主機上生效，則顯示**所有主機**部分。

- **變更日誌**索引標籤包含對阻止措施所做的變更清單：變更時間、變更阻止措施的使用者名稱，以及對阻止措施採取的操作。

建立阻止規則

為系統檔案建立防護規則時，封鎖檔案運作的主機可能無法正常運作。Kaspersky Anti Targeted Attack Platform 不會檢查為哪種類型的檔案建立防護規則。

若要建立阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。

   這將開啟防禦規則表

2. 點擊**新增**。
3. 選擇**建立規則**。

   這將開啟防止規則建立視窗。

4. 配置以下設定：
   a. **狀態**是阻止規則的狀態：
      - 如果要啟用阻止規則，請將切換開關設為**開啟**。
      - 如果要停用阻止規則，請將切換開關設為**關閉**。

   b. **MD5/SHA256**—您要阻止其啟動之檔案或資料串流的 MD5 或 SHA256 雜湊。

   c. **名稱** — 阻止規則的名稱。

d. 如果您希望應用程式向應用程式防禦的電腦使用者顯示阻止規則觸發通知，請選擇**通知使用者阻止檔案執行**核取方塊。

> 如果您選擇了**通知使用者阻止檔案執行**核取方塊並嘗試執行被阻止運行的檔案，則使用者會被通知該檔案觸發了執行阻止規則。

e. **阻止於**是阻止規則的範圍：

- 如果您想在所有伺服器的所有主機上套用阻止規則，請選擇**所有主機**。
- 如果要在選定的伺服器上套用阻止規則，請選擇**指定伺服器**選項並在**伺服器**參數名稱的右側選擇要在其上套用阻止規則的伺服器名稱旁的核取方塊。

  僅當啟用分佈式解決方案和多組織用戶模式時，此選項才可用。
- 如果您想在選定主機上套用阻止規則，請選擇**指定主機**選項並在**主機**欄位中列出這些主機。

> 如果您使用的是版本早於 12.2 的 Kaspersky Endpoint Security for Linux 作為 Endpoint Agent 元件，則防護規則建立功能不可用。建立防防止則時，如果您選擇裝有 Kaspersky Endpoint Security for Linux 的主機或所有主機作為規則範圍，則該規則不會套用或僅套用於裝有 Kaspersky Endpoint Security for Windows 的主機。

5. 點擊**新增**。

   將建立檔案啟動阻止。

您也可以匯入阻止規則。

> 具有**安全稽核員**角色的使用者無法建立檔案啟動阻止規則。

> 具有**安全官**角色的使用者無法存取阻止規則。

匯入阻止規則

對於要阻止運行的檔案，您可以匯入具有 MD5 和 SHA256 雜湊值的檔案。對於每個雜湊值，Kaspersky Anti Targeted Attack Platform 會建立單獨的阻止規則。

> 匯入檔案的最大大小為 10 MB。每行只允許一個雜湊。

若要匯入阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。

   這將開啟防禦規則表

2. 點擊**新增**。

3. 選擇**匯入規則**。

   這將開啟阻止規則匯入視窗。

4. 配置以下設定：

   a. **狀態**是阻止規則的狀態：

      - 如果要啟用所有匯入的阻止規則，請將切換開關設為**開啟**。
      - 如果要停用所有匯入的阻止規則，請將切換開關設為**關閉**。

   b. 如果您希望應用程式向套用阻止措施的電腦使用者顯示阻止規則觸發通知，請選擇**通知使用者阻止檔案執行**核取方塊。

> **阻止於**欄位無法編輯。預設情況下，在 PCN 伺服器上建立的阻止規則將套用於連線到該 PCN 伺服器的所有主機以及連線到該 PCN 伺服器的所有 SCN 伺服器（如果您使用的是分散式解決方案和多組織用戶模式）。

5. 點擊**瀏覽**上傳包含要為其建立阻止規則的檔案雜湊的檔案。

   這將開啟檔案選擇視窗。

6. 選擇您想上傳的檔案，然後點擊“**開啟**”。

   這將關閉檔案選擇視窗。

7. 點擊**新增**。

規則已匯入。

> 具有**安全稽核員**角色的使用者無法匯入檔案啟動阻止規則。

> 具有**安全官**角色的使用者無法存取阻止規則。

啟用和停用阻止規則

若要啟用或停用阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。

   這將開啟防禦規則表

2. 在包含要啟用或停用之阻止規則的列中，於**狀態**欄執行下列其中一項操作：

   - 如果要啟用阻止規則，請將切換開關設為**已啟用**。

     將啟用您選定的阻止規則。

- 如果要停用阻止規則，請將切換開關設為**已停用**。
  將停用您選定的防止規則。

具有**安全稽核員**角色的使用者無法啟用或停用阻止規則。

具有**安全官**角色的使用者無權存取使用政策在選定主機上啟動檔案和處理程序的阻止規則。

啟用和停用預設

要啟用或停用預設：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表
2. 選擇“**預設**”索引標籤。
3. 在要啟用或停用的預設行中，在**狀態**列中，將切換開關設定為**已啟用**或者**已停用**。

預設被啟用或停用。停用預設後，先前自動建立的所有阻止規則都不會被刪除。

刪除阻止規則

您可以刪除單個阻止規則或多個阻止規則，或同時刪除所有阻止規則。

刪除單個阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表
2. 點擊您想刪除的阻止規則。
   這將開啟阻止規則詳情視窗。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

阻止規則被刪除。

刪除全部或多個阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表
2. 選擇要刪除的阻止規則旁的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有阻止規則。

3. 在視窗下部顯示的窗格中，點擊**刪除**。
   這將開啟操作確認視窗。

4. 點擊**是**。

選定的阻止規則將被刪除。

具有**安全稽核員**角色的使用者無法刪除阻止規則。

具有**安全官**角色的使用者無權存取使用政策在選定主機上啟動檔案和處理程序的阻止規則。

按名稱篩選阻止規則

若要依名稱篩選防止規則：

1. 在應用程式 Web 介面視窗中選擇"**阻止**"區域。
   這將開啟防禦規則表

2. 點擊**名稱**連結以開啟阻止篩選功能表。

3. 在下拉清單中，選擇以下防禦篩選運算子之一：

   - **包含**

   - **不包含**

4. 在文字方塊中輸入防止規則名稱的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

阻止規則表僅顯示與您設定的篩選條件相符的阻止規則。

您可以同時使用多個篩選器。

按類型篩選阻止規則

如果您使用分散式解決方案和多組織用戶模式，則可以按類型篩選阻止規則。

按類型篩選阻止規則：

1. 在應用程式 Web 介面視窗中選擇"**阻止**"區域。
   這將開啟防禦規則表

2. 點擊**類型**連結以開啟阻止規則篩選功能表。

3. 選擇以下選項之一來顯示阻止規則：

   - **所有**，如果您想顯示所有阻止規則（無論其類型為何）。

   - **全球**，如果您只想顯示在 PCN 上建立的阻止規則。這些阻止規則適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。

   - **本機**，如果您只想顯示在 SCN 伺服器上建立的阻止規則。這些阻止規則僅適用於連線到此 SCN 伺服器的主機。防止規則屬於使用者在應用程式 Web 介面中管理的租戶。

阻止規則表僅顯示與您設定的篩選條件相符的阻止規則。

您可以同時使用多個篩選器。

按檔案雜湊篩選阻止規則

要按檔案雜湊來篩選阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。

   這將開啟防禦規則表

2. 點擊**檔案雜湊值**連結以開啟阻止規則篩選功能表。

3. 在下拉清單中，選擇以下防禦篩選運算子之一：

   - **包含**

   - **不包含**

4. 在文字方塊中，輸入檔案雜湊的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

阻止規則表僅顯示與您設定的篩選條件相符的阻止規則。

您可以同時使用多個篩選器。

按伺服器名稱篩選阻止規則

如果您使用的是分佈式解決方案和多組織用戶模式，您可以根據阻止規則應用的伺服器來篩選阻止規則。

若要依伺服器名稱篩選阻止規則：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表
2. 點擊**伺服器**連結以開啟阻止規則篩選功能表。
3. 選擇要用於篩選阻止規則的伺服器旁的核取方塊。
4. 點擊**套用**。

阻止規則表僅顯示與您設定的篩選條件相符的阻止規則。

> 您可以同時使用多個篩選器。

清除阻止規則篩選器

若要清除一個或多個篩選條件的阻止規則篩選器：

1. 在應用程式 Web 介面視窗中選擇“**阻止**”區域。
   這將開啟防禦規則表
2. 點擊您想要清除其篩選條件的阻止規則表列標題右側的 ⊠。

   > 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   阻止規則表僅顯示與您設定的篩選條件相符的阻止規則。

管理使用者定義的規則

您可以使用TAA、IDS、IOC和YARA規則，為公司的 IT 基礎架構配置額外的安全性。

具有**資深安全員**角色的使用者可以使用自訂**TAA**、**IDS**、**IOC**和**YARA**規則：載入和刪除規則檔案、檢視規則清單，以及編輯選定的規則。

具有**安全稽核員**角色的使用者可以檢視自訂**TAA**、**IDS**、**IOC**和**YARA**規則清單以及所選規則的屬性，但無法編輯。

具有**安全官**角色的使用者可以檢視自訂**TAA**、**IOC**和**YARA**規則清單以及所選規則的屬性，但無法編輯。

使用入侵指標 (IOC) 和攻擊指標 (IOA) 進行威脅搜索

Kaspersky Anti Targeted Attack Platform 使用兩種類型的指示器進行威脅搜尋：*IOC*（入侵指標）和 *IOA*（攻擊指標）。

IOC 是有關惡意物件或惡意活動的一組資料。Kaspersky Anti Targeted Attack Platform 使用符合 OpenIOC 標準的 IOC 檔案，該標準是用於描述入侵指標的開放式標準。IOC 檔案包含一組與事件指標進行比較的指標。如果比較的指標匹配，應用程式將該事件視為偵測並建立警示。如果掃描偵測到物件資料與多個 IOC 檔案之間的精確匹配，則警示的可能性會增加。

IOA（也稱為"TAA (IOA) 規則"）是包含系統中可疑活動描述的規則，該活動可能是針對性攻擊的跡象。Kaspersky Anti Targeted Attack Platform 掃描應用程式的事件資料庫，並標記與 TAA (IOA) 規則描述的行為相符的事件或事件鏈。使用*串流掃描*技術，對從受防護裝置接收到的事件進行連續即時掃描。

由卡巴斯基專家建立的 TAA (IOA) 規則得到 TAA（針對性攻擊分析器）技術的使用，與應用程式資料庫一起更新。它們不會顯示在應用程式的介面中，並且無法編輯。

您可以使用 OpenIOC 格式的 IOC 檔案新增使用者定義的 IOC和TAA (IOA) 規則，以及基於事件資料庫搜尋條件建立 TAA (IOA) 規則。

下表包含入侵指標 (IOC) 和攻擊指標 (IOA) 的比較分析。

IOC 和 IOA 指標比較

特徵	使用者定義的 IOC 規則中的 IOC	使用者定義的 TAA (IOA) 規則中的 IOA	卡巴斯基專家所建立的 TAA (IOA) 規則中的 IOA
掃描範圍	具有 Endpoint Agent 元件的電腦	應用程式事件資料庫	應用程式事件資料庫
掃描機制	定期掃描	串流掃描	串流掃描
可以被新增到掃描排除項目	無。	不需要。 具有**資深安全員**角色的使用者可以根據需要編輯自訂 TAA (IOA) 規則中的指標文字。	是。

如果使用的是分佈式解決方案和多組織用戶模式，此部分將顯示所選租用戶的資訊。

管理使用者定義的 TAA (IOA) 規則

自訂 TAA (IOA) 規則是根據事件資料庫搜尋條件建立的。例如，當您認為不安全的應用程式在具有 Endpoint Agent 元件的電腦上啟動時，您希望 Kaspersky Anti Targeted Attack Platform 產生事件警示，您可以：

1. 手動向事件資料庫產生搜尋查詢，或上傳帶有入侵指標的 IOC 檔案或帶有 Sigma 規則的 YAML 檔案來偵測此應用程式。

   建立 IOC 檔案時，請在"**威脅搜尋**"部分檢視可用於搜尋事件的 IOC 術語清單。您可以透過從下面的連結下載檔案來檢視受支援的 IOC 術語清單。

   在"**威脅搜尋**"部分搜尋事件的 IOC 術語

2. 根據事件搜尋條件建立自訂 TAA (IOA) 規則。

   當 Central Node 伺服器收到與建立的 TAA (IOA) 規則相符的事件時，Kaspersky Anti Targeted Attack Platform 就會產生警示。

您也可以根據已載入的 IOC 檔案中的條件建立 TAA (IOA) 規則。為此：

1. 尋找與所選檔案的條件相對應的事件。

2. 根據所選檔案中的事件搜尋條件建立 TAA (IOA) 規則。

在分佈式解決方案和多組織用戶模式下，TAA (IOA) 規則可以有以下類型之一：

- **全球** — 在 PCN 伺服器上建立。這些規則用於掃描此 PCN 伺服器以及連線到此 PCN 伺服器的所有 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。

- **本機** — 在 SCN 伺服器上建立。這些規則用於掃描此 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。

下表總結了使用者規則和卡巴斯基規則之間的差異。

TAA（IOA）規則對比

特徵	使用者定義的 TAA (IOA) 規則	Kaspersky TAA (IOA) 規則
關於回應事件的建議	否	是 您可以在警示訊息中檢視推薦
與 MITRE ATT&CK 資料庫中的技術對應	否	是 您可以根據 MITRE 資料庫在警示資訊中檢視 技術描述
在TAA（IOA）規則表中顯示	是	否
能夠停用此規則的資料庫查找	停用規則	將規則新增至 TAA 排除項
能夠刪除或新增規則	您可以在應用程式的 Web 介面中刪除或新增規則	規則與應用程式資料庫 一起更新並且不能被使用者刪除
搜尋其中觸發了 TAA (IOA) 規則的警示和事件	使用 TAA (IOA) 規則資訊視窗中的**警示**和**事件**連結	使用警示訊息視窗中的**警示**和**事件**連結

具有**資深安全員**角色的使用者可以建立、匯入、刪除、啟用或停用 TAA (IOA) 規則，以及從掃描中排除 Kaspersky TAA (IOA) 規則。具有**安全官**或者**安全稽核員**角色的使用者可以使用 TAA（IOA）規則在事件和警示資料庫中搜尋針對性攻擊跡象、感染物件和可能受感染的物件，並檢視 TAA（IOA）規則表和TAA（IOA）規則資訊。

檢視 TAA（IOA）規則表

如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

使用者定義的 TAA (IOA) 規則表包含有關用於掃描事件和建立警示的 TAA (IOA) 規則的資訊；該表位於應用程式 Web 介面視窗的**自訂規則**部分，**TAA**子部分。

表包含以下資訊：

1. — 指派給使用此 TAA (IOA) 規則產生的警示的重要性等級。

重要性等級可以採用以下其中一個值：

- **– 低**。
- **– 中**。
- **– 高**。

2. **類型**是規則的類型，取決於應用程式的操作模式和產生規則的伺服器的角色：
   - **全球** — 在 PCN 伺服器上建立。這些規則用於掃描此 PCN 伺服器以及連線到此 PCN 伺服器的所有 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。
   - **本機** — 在 SCN 伺服器上建立。這些規則用於掃描此 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。
3. **置信** – 置信度取決於規則引起誤報的可能性：
   - **高**。
   - **中**。
   - **低**。

   置信度越高，誤報的可能性就越低。
4. **名稱** – 規則名稱。
5. **伺服器**是規則適用的 PCN 或 SCN 角色伺服器名稱。
   如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄。
6. **警示** – 要求根據資料庫中的事件與規則條件的匹配來儲存警示資訊。
   - **已啟用** – 使用指定的針對性攻擊分析器 (TAA) 技術在警示表中為此事件建立一筆記錄。
   - **已停用** – 不顯示在警示表中。
7. **狀態** – 事件掃描中規則的使用狀態：
   - **已啟用** – 規則正在被使用。
   - **已停用** – 該規則未被使用。

根據事件搜尋條件建立 TAA (IOA) 規則

根據事件搜尋條件建立 TAA (IOA) 規則：

1. 在應用程式 Web 介面視窗中選擇**威脅搜尋**區段。
   這將開啟事件搜尋表單。
2. 使用建構器模式或原始碼模式執行事件搜尋。

3. 點擊**另存為 TAA (IOA) 規則**。

   這將開啟**新 TAA (IOA) 規則**視窗。

4. 在**名稱**欄位中，輸入規則的名稱。

5. 點擊**儲存**。

事件搜尋條件將被儲存。在**自訂規則**部分的 TAA（IOA）規則表中，在 Web 介面的**TAA**子部分中，新規則將以指定名稱顯示。

如果您要將事件搜尋條件儲存為使用者定義的 TAA (IOA) 規則，請避免使用下列欄位：

- IOAd。
- IOATag。
- IOATechnique。
- IOATactics。
- IOAImportance。
- IOAConfidence。

儲存使用者定義的 TAA (IOA) 規則時，應用程式可能沒有任何包含這些欄位資料的事件。當出現具有此資料的事件時，您先前建立的使用者定義欄位將無法按這些欄位標記事件。

> 具有**安全稽核員**和**安全官**角色的使用者無法根據事件搜尋條件建立 TAA (IOA) 規則。

匯入 TAA (IOA) 規則

您可以從 IOC 檔案或具有 Sigma 規則的 YAML 檔案匯入 TAA (IOA) 規則，並使用這些規則掃描事件並產生針對性攻擊分析器警示。

要匯入 TAA (IOA) 規則：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。

   這將開啟 TAA (IOA) 規則表。

2. 點擊**匯入**。

   這將在您的本機電腦上開啟檔案選擇視窗。

3. 選擇您想上傳的檔案，然後點擊**開啟**。

   這將開啟**新 TAA (IOA) 規則**視窗。

4. 如果要啟用掃描事件資料庫的規則，將**狀態**切換開關設定為**已啟用**。

5. 在**詳細資訊**索引標籤上的**名稱**欄位中，輸入規則的名稱。

6. 在**敘述**欄位中，輸入有關規則的任何附加資訊。

7. 在**重要級別**下拉清單中，選擇要指派給使用此 TAA (IOA) 規則產生的警示的重要性等級。
   - **低**。
   - **中**。
   - **高**。
8. 在**置信**下拉清單中，根據您的估計選擇此規則的置信等級：
   - **低**。
   - **中**。
   - **高**。
9. 在**套用到**下面，選擇與要對其應用規則的伺服器對應的核取方塊。
10. 在**查詢**索引標籤上，驗證定義的搜尋條件。如有必要，請進行變更。
11. 點擊**儲存**。

    使用者定義的 TAA (IOA) 規則被匯入到應用程式中。

> 您也可以在**威脅搜尋**部分中透過儲存事件資料庫搜尋條件新增 TAA (IOA) 規則。

檢視自訂 TAA (IOA) 規則詳細資訊

若要顯示有關 TAA (IOA) 規則的資訊：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。

   這將開啟 TAA (IOA) 規則表。
2. 選擇您想檢視資訊的規則。

   這將開啟一個視窗，其中包含有關規則的資訊。

此視窗包含以下資訊：

- 點擊**警示**連結即可在新的瀏覽器標籤中顯示警示表。警示將根據針對性攻擊分析器技術和您正在處理的 TAA (IOA) 規則的名稱進行篩選。
- 點擊**尋找事件**連結以在新的瀏覽器標籤中顯示事件表。此表按規則名稱篩選。
- 點擊**執行查詢**連結以在新的瀏覽器標籤中顯示事件表。此表按規則名稱篩選。事件搜尋條件將使用您正在處理的 TAA (IOA) 規則中的資訊進行填充。例如，`EventType=`處理程序已啟動 `AND FileName CONTAINS <`您正在處理的規則的名稱`>`。您可以編輯事件搜尋查詢。

- 點擊**IOA ID**連結顯示應用程式分配給每個規則的 ID。

  ID 無法修改。您可以點擊**複製值到剪貼簿**按鈕複製ID。

- **狀態** – 在事件資料庫掃描中使用規則。

詳細資訊頁簽包含以下資訊：

- **名稱**是您在新增規則時指定的規則的名稱。
- **敘述**是有關您指定的規則的任何附加資訊。
- **重要級別**是對新增規則時使用者指定的事件對電腦或公司 LAN 安全的可能影響的估計。
- **置信**是取決於新增規則時使用者定義的誤報可能性的置信度。
- **類型**是規則的類型，取決於產生它的伺服器的角色：
  - **全球** — 在 PCN 伺服器上建立。這些規則用於掃描此 PCN 伺服器以及連線到此 PCN 伺服器的所有 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。
  - **本機** — 在 SCN 伺服器上建立。這些規則用於掃描此 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。
- **套用到** – 伺服器的名稱，包含在其上套用規則的 Central Node 元件。

查詢標籤顯示正在被檢查的查詢的原始碼。點擊視窗上部的**執行查詢**連結可轉到**威脅搜尋**部分並執行事件搜尋查詢。

搜尋其中觸發了 TAA (IOA) 規則的警示和事件

若要搜尋並顯示由使用者定義的 TAA (IOA) 規則觸發所建立的警示和事件：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。

   這將開啟 TAA (IOA) 規則表。

2. 選擇您要檢視觸發結果的規則。

   這將開啟一個視窗，其中包含有關規則的資訊。

3. 執行以下操作之一：
   - 如果您想檢視 TAA（IOA）規則觸發產生的警示，請點擊**警示**轉至警示資料庫。

     警示表將在新的瀏覽器標籤中開啟。

   - 如果您想檢視 TAA（IOA）規則觸發產生的事件，請點擊**事件**轉至事件資料庫。

     事件表將在新的瀏覽器標籤中開啟。

若要搜尋並顯示由使用者定義的 TAA (IOA) 規則觸發所建立的警示和事件：

若要搜尋並顯示由 Kaspersky TAA (IOA) 規則觸發所建立的警示和事件：

1. 在應用程式 Web 介面視窗中，選擇“**警示**”區域。

   這將開啟警示表。

2. 點擊**技術**列中的連結開啟篩選器配置視窗。

3. 在左側的下拉清單中，選擇**包含**。

4. 在右側的下拉清單中，選擇**（TAA）針對性攻擊分析器**技術。

5. 點擊**套用**。
   此表顯示 TAA 技術根據 TAA (IOA) 規則產生的警示。

6. 選擇一個警示，**偵測到**列為其顯示相關規則的名稱。
   這將開啟一個視窗，其中包含有關警示的資訊。

7. 在**掃描結果**下面，點擊帶有規則名稱的連結以開啟規則資訊視窗。

8. 執行以下操作之一：

   - 如果您想檢視 TAA（IOA）規則觸發產生的警示，請點擊**警示**轉至警示資料庫。
     警示表將在新的瀏覽器標籤中開啟。

   - 如果您想檢視 TAA（IOA）規則觸發產生的事件，請點擊**事件**轉至事件資料庫。
     事件表將在新的瀏覽器標籤中開啟。

若要搜尋並顯示由 Kaspersky TAA (IOA) 規則觸發所建立的警示和事件：

篩選與搜尋 TAA (IOA) 規則

若要依所需條件篩選或搜尋 TAA (IOA) 規則：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。
   這將開啟 TAA (IOA) 規則表。

2. 根據篩選條件，執行以下操作：

   - **按重要性**

     a. 點擊圖示以開啟 IOA 規則篩選配置視窗。

     b. 選擇要包含在篩選條件中的重要性等級旁的核取方塊：

        - **低**。

        - **中**。

        - **高**。

     c. 點擊**套用**。

- **按規則類型**

  a. 點擊**類型**連結以開啟篩選配置視窗。

  b. 選擇以下選項之一：

    - **所有** — 所有規則。
    - **全球** — 在 PCN 伺服器上建立的規則。這些規則用於掃描此 PCN 伺服器以及連線到此 PCN 伺服器的所有 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。
    - **本機** — 在 SCN 伺服器上建立的規則。這些規則用於掃描此 SCN 伺服器上的事件。掃描的事件屬於使用者在應用程式 Web 介面中管理的租戶。

- **按置信度**

  a. 點擊**置信**連結以開啟篩選配置視窗。

  b. 選擇要新增到篩選條件的置信度旁邊的核取方塊。

    - **低**。
    - **中**。
    - **高**。

  c. 點擊**套用**。

- **按規則名稱**

  a. 點擊**IOA 標記**連結以開啟篩選配置視窗。

  b. 輸入 IOA 規則名稱的一個或多個字元。

  c. 點擊**套用**。

- **按伺服器名稱**

  a. 點擊**伺服器**連結以開啟篩選配置視窗。

  b. 選擇要包含在篩選條件中的租戶或租戶中的伺服器旁的核取方塊。

  c. 點擊**套用**。

- **透過基於規則的警示產生**

  a. 點擊**警示**連結以展開篩選器設定清單。

  b. 選擇以下選項之一：

    - **所有**。
    - **已啟用**。
    - **已停用**。

- **按規則狀態**

  a. 點擊**狀態**展開篩選器設定清單。

  b. 選擇以下選項之一：

  - **所有**。
  - **已啟用**。
  - **已停用**。

此表僅顯示與指定條件相符的規則。

> 您可以同時使用多個篩選器。

重置 TAA (IOA) 規則篩選器

若要根據一個或多個篩選條件清除 TAA (IOA) 規則篩選器：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。
   這將開啟 TAA (IOA) 規則表。
2. 點擊要為其清除篩選條件的規則表的列標題右側的 ✕。

   > 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   此表僅顯示與指定條件相符的規則。

啟用和停用 TAA (IOA) 規則

具有**資深安全員**角色的使用者可以啟用或停用一個或多個規則，也可以同時啟用或停用所有規則。

若要在掃描事件時啟用或停用 TAA (IOA) 規則的使用：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。
   這將開啟 TAA (IOA) 規則表。
2. 在具有相關規則的行中，選擇或清除**狀態**列中的核取方塊。

掃描事件時使用規則會啟用或停用。

若要在掃描事件時啟用或停用所有或多個 TAA (IOA) 規則：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。

   這將開啟 TAA (IOA) 規則表。

2. 選擇要啟用或停用其使用的規則左側的核取方塊。

   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。

   控制面板出現在視窗的下部。

3. 點擊**啟用**或者**停用**啟用或停用所有規則。

掃描事件時使用所選規則被啟用或停用。

在分佈式解決方案和多租户模式下，您只能在 PCN 伺服器上管理全局 TAA（IOA）規則。您可以在有權存取的租户的 SCN 伺服器上管理本機 TAA (IOA) 規則。

具有**安全稽核員**和**安全官**角色的使用者無法啟用或停用 TAA (IOA) 規則。

修改 TAA (IOA) 規則

具有**資深安全員**角色的使用者可以修改自訂 TAA (IOA) 規則。卡巴斯基建立的規則無法編輯。

在分佈式解決方案和多租戶模式下，您只能編輯在目前伺服器上建立的 TAA (IOA) 規則。因此，在 PCN 的 Web 介面中，您只能編輯在 PCN 上建立的規則。在 SCN 的 Web 介面中，您只能編輯在 SCN 上建立的規則。

要編輯TAA (IOA) 規則：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。

   這將開啟 TAA (IOA) 規則表。

2. 選擇要修改的規則。

   這將開啟一個視窗，其中包含有關規則的資訊。

3. 進行相關變更。

4. 點擊**儲存**。

角色設定已修改。

具有**安全稽核員**和**安全官**角色的使用者無法根據事件搜尋條件修改 TAA (IOA) 規則。

刪除 TAA (IOA) 規則

具有**資深安全員**角色的使用者可以刪除一條或多條 TAA (IOA) 規則，或同時刪除所有規則。

在分佈式解決方案和多租戶模式下，您只能刪除在目前伺服器上建立的 TAA (IOA) 規則。因此，在 PCN 的 Web 介面中，您只能刪除在 PCN 上建立的規則。在 SCN 的 Web 介面中，您只能刪除在 SCN 上建立的規則。

若要刪除自訂 TAA (IOA) 規則：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。
   這將開啟 TAA (IOA) 規則表。
2. 選擇您想刪除的規則。
   這將開啟一個視窗，其中包含有關規則的資訊。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

規則被刪除。

若要刪除全部或多個自訂 TAA (IOA) 規則：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**TAA**子部分。
   這將開啟 TAA (IOA) 規則表。
2. 選擇您要刪除的規則左側的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。
   控制面板出現在視窗的下部。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

所選檔案將被刪除。

您無法刪除卡巴斯基定義的 TAA (IOA) 規則。如果您不想使用 Kaspersky TAA (IOA) 規則進行掃描，請將其新增至排除項目。

具有**安全稽核員**和**安全官**角色的使用者無法根據事件搜尋條件修改TAA (IOA) 規則。

管理使用者定義的 IOC 規則

您可以使用 IOC 檔案在事件資料庫和具有 Endpoint Agent 元件的電腦上搜尋入侵指標。例如，如果您收到了有關目前正在傳播的惡意軟體的第三方訊息，您可以：

1. 建立一個包含惡意軟體入侵指標的 IOC 檔案，並將其上傳到 Kaspersky Anti Targeted Attack Platform 的 Web 介面。

2. 尋找與所選 IOC 檔案的條件相對應的事件。

   您可以檢視此類事件，如果您希望 Kaspersky Anti Targeted Attack Platform 為選定事件產生警示，您可以建立 TAA (IOA) 規則。

3. 啟用自動使用選定的 IOC 檔案來搜尋具有 Endpoint Agent 元件的電腦上的入侵指標。

4. 如果在掃描電腦時 Endpoint Agent 元件偵測到入侵指標，Kaspersky Anti Targeted Attack Platform 會產生警示。

   您可以按技術名稱篩選，在警示表中找到這些警示。

5. 配置在具有 Endpoint Agent 元件的電腦上使用 IOC 檔案搜尋入侵指標的計畫。

在分佈式解決方案和多組織用戶模式下，IOC 檔案可以有以下類型：

- **本機** — 上傳到 SCN 伺服器的 IOC 檔案。這些 IOC 檔案用於搜尋連線到 SCN 伺服器的 Kaspersky Endpoint Agent 主機上的入侵指標。

- **全球** — 上傳到 PCN 伺服器的 IOC 檔案。這些 IOC 檔案用於搜尋連線到 PCN 伺服器的 Kaspersky Endpoint Agent 主機以及連線到 PCN 伺服器的所有 SCN 伺服器上的入侵指標。

IOC 檔案是以 .ioc 副檔名儲存的文字檔。建立 IOC 檔案時，請檢視您在Endpoint Agent角色中使用的應用程式支援的 IOC 術語清單。您可以透過從下面的連結下載檔案來檢視受支援的 IOC 術語清單。

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security 12 for Linux

若要使此功能正常運作，必須為 IOC 術語“Indicator”和“IndicatorItem”設定“id”屬性。如果至少有一個 IOC 檔案缺少該屬性，則應用程式在發現入侵指標相符項時將不會產生警示；不僅不會為此檔案產生警示，也不會為所有其他 IOC 檔案產生警示。

Kaspersky Endpoint Security 11.4 for Linux 和 Kaspersky Endpoint Security for Mac 不支援 IOC 檔案。

透過雜湊查找檔案的 IOC 檔案範例

```
<?xml version="1.0" encoding="us-ascii"?>

<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
id="UUID 格式的唯一 ID" last-modified="規則最後修改日期，格式為 YYYY-MM-DDThh:mm:ss"
xmlns="http://schemas.mandiant.com/2010/ioc">

<short_description>規則名稱</short_description>

<authored_by>規則名稱</authored_by>

<authored_date>檔案建立日期，格式為 YYYY-MM-DDThh:mm:ss</authored_date>

<links />

<definition>

<Indicator operator="OR" id="UUID 格式的唯一 ID">

<IndicatorItem id="UUID 格式的唯一 ID" condition="is">

<Context document="FileItem" search="FileItem/Md5sum" type="mir" />

<Content type="md5">檔案的 MD5 雜湊值</Content>

</IndicatorItem>

</Indicator>

</definition>

</ioc>
```

每個 IOC 檔案只能包含一條規則。規則可以具有任意複雜度。

具有**資深安全員**角色的使用者可以匯入 IOC 檔案、刪除 IOC 檔案或將 IOC 檔案下載到電腦上，啟用或停用使用 IOC 檔案搜尋入侵指標，以及配置在裝有 Endpoint Agent 元件的電腦上搜尋入侵指標的計畫。

具有**安全官**和**安全稽核員**角色的使用者可以檢視 IOC 檔案清單和有關所選檔案的資訊，並將 IOC 檔案匯出到電腦。

檢視 IOC 檔案表

> 如果您使用分佈式解決方案和多組織用戶模式，請使用要為其設定參數的 PCN 或 SCN 伺服器的 Web 介面。

IOC 檔案表包含有關用於在安裝了 Endpoint Agent 元件的電腦上進行掃描的 IOC 檔案的資訊；您可以在應用程式 Web 介面視窗的**自訂規則**區段、**IOC**子區段中找到該表。

IOC 檔案表包含以下資訊：

1. — 將指派給使用此 IOC 檔案產生的警示的重要性等級。

重要性等級可以採用以下其中一個值：

- — 低重要性。
- — 中重要性。
- — 高重要性。

2. **類型**是 IOC 檔案的類型，取決於應用程式操作模式和 IOC 檔案上傳到的伺服器：
   - **本機**是上傳到 SCN 伺服器的 IOC 檔案。這些 IOC 檔案用於搜尋主機上的入侵指標，這些主機具有連線到 SCN 伺服器的 Endpoint Agent 元件。
   - **全球**是上傳到 PCN 伺服器的 IOC 檔案。這些 IOC 檔案用於搜尋具有連線到 PCN 伺服器的 Endpoint Agent 元件的主機上以及連線到 PCN 伺服器的所有 SCN 伺服器上的入侵指標。
3. **名稱**是 IOC 檔案的名稱。
4. **伺服器**是規則適用的 PCN 或 SCN 角色伺服器名稱。

   如果您使用的是分佈式解決方案和多組織用戶模式，則會顯示此列。
5. **自動掃描**是自動掃描具有 Endpoint Agent 元件的主機時使用 IOC 檔案。

   使用此 IOC 檔案掃描主機可能具有以下狀態之一：
   - **已啟用**。
   - **已停用**。

檢視有關 IOC 檔案的資訊

要檢視 IOC 檔案詳細資訊：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**IOC**子部分。

   這將開啟 IOC 檔案表。
2. 選擇您想檢視資訊的 IOC 檔案。

這將開啟一個視窗，其中包含有關 IOC 檔案的資訊。

此視窗包含以下資訊：

- 點擊**尋找警示**連結可開啟**警示**部分，其中包含填入了所選 IOC 檔案名稱的篩選條件。
- 點擊**尋找事件**連結可開啟**威脅搜尋**部分，其中包含填入了所選 IOC 檔案的入侵指標的搜尋條件。
- 點擊**下載**連結將開啟 IOC 檔案下載視窗。
- **自動掃描**是自動掃描具有 Endpoint Agent 元件的主機時使用 IOC 檔案。
- **名稱**是 IOC 檔案的名稱。
- **重要級別**是必須指派給使用此 IOC 檔案產生的警示的重要性等級。

重要性等級可以採用以下其中一個值：

- — 低重要性。
- — 中重要性。
- — 高重要性。

- **套用到** — 顯示租用戶名稱以及與基於此 IOC 檔案掃描的事件關聯的伺服器名稱（在分佈式解決方案和多組織用戶模式下）。
- **XML** — 以 XML 格式顯示 IOC 檔案內容。

上传 IOC 檔案

不支援具有用於網域使用者的 UserItem 屬性的 IOC 檔案。

要上傳 IOC 檔案：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
   這將開啟 IOC 檔案表。
2. 點擊**匯入**。
   這將在您的本機電腦上開啟檔案選擇視窗。
3. 選擇您想上傳的檔案，然後點擊**開啟**。
4. 指定以下參數：
   a. **自動掃描**是自動掃描具有 Endpoint Agent 元件的主機時使用 IOC 檔案：
      - **已啟用**。
      - **已停用**。
   b. **名稱**是 IOC 檔案的名稱。
   c. **重要級別**是必須指派給使用此 IOC 檔案產生的警示的重要性等級：
      - **低**。
      - **中**。
      - **高**。
   d. **套用到**是租用戶名稱以及想要使用此 IOC 檔案掃描的伺服器名稱（在分佈式解決方案和多組織用戶模式下）。
5. 點擊**儲存**。

IOC 檔案將以 XML 格式上傳。

下載 IOC 檔案到電腦

您可以將之前上傳的 IOC 檔案下載到電腦上。

要下載 IOC 檔案：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
   這將開啟 IOC 檔案表。
2. 選擇您想下載的 IOC 檔案。
   這將開啟一個視窗，其中包含有關 IOC 檔案的資訊。
3. 根據您的瀏覽器設定，點擊**下載**連結將檔案儲存到預設資料夾或指定儲存檔案的資料夾。

該 IOC 檔案將會被儲存到瀏覽器下載資料夾中的電腦。

掃描主機時啟用和停用 IOC 檔案的自動使用

您可以啟用或停用自動使用 IOC 檔案來搜尋具有 Endpoint Agent 元件的主機上的入侵指標。

若要啟用或停用自動使用 IOC 檔案來搜尋具有 Endpoint Agent 元件的主機上的入侵指標：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
   這將開啟 IOC 檔案表。
2. 在包含要啟用或停用其使用的 IOC 檔案的行中，在**狀態**列中，將切換開關設定為以下位置之一：
   - **已啟用**。
   - **已停用**。

自動使用 IOC 檔案來搜尋具有 Endpoint Agent 元件的主機上的入侵指標已啟用或停用。

具有**安全稽核員**和**安全官**角色的使用者無法啟用或停用自動套用 IOC 檔案。

刪除 IOC 檔案

要刪除 IOC 檔案：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
   這將開啟 IOC 檔案表。

2. 選擇您想刪除的 IOC 檔案。
   這將開啟一個視窗，其中包含有關 IOC 檔案的資訊。

3. 點擊**刪除**。

IOC 檔案將被刪除。

具有**安全稽核員**和**安全官**角色的使用者無法刪除 IOC 檔案。

在 IOC 掃描結果中搜尋警示

若要尋找並檢視所選 IOC 檔案的掃描結果：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
   這將開啟 IOC 檔案表。

2. 選擇您想檢視掃描結果的 IOC 檔案。
   這將開啟一個視窗，其中包含有關 IOC 檔案的資訊。

3. 點擊**尋找警示**轉至警示資料庫。
   警示表將在新的瀏覽器標籤中開啟。

您也可以透過按技術名稱篩選警示來檢視所有 IOC 檔案的掃描結果。

使用 IOC 檔案搜尋事件

要檢視使用 IOC 檔案找到的事件：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
   這將開啟 IOC 檔案表。

2. 選擇用於在事件資料庫中搜尋事件的 IOC 檔案。
   這將開啟一個視窗，其中包含有關 IOC 檔案的資訊。

3. 點擊**尋找事件**轉至事件資料庫。
   事件表將在新的瀏覽器標籤中開啟。

篩選並搜尋 IOC 檔案

若要依要求的條件篩選或搜尋 IOC 檔案：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
2. 這將開啟 IOC 檔案表。根據篩選條件，執行以下操作：
   - **按重要性**
     a. 點擊圖示開啟 IOC 檔案的篩選配置視窗。
     b. 選擇一個或多個以下重要性等級：
       - **低**。
       - **中**。
       - **高**。
     c. 點擊**套用**。
   - **按檔案名稱**
     a. 點擊**名稱**連結以開啟 IOC 檔案篩選配置視窗。
     b. 輸入 IOC 檔案名稱的一個或多個字元。
     c. 點擊**套用**。
   - **按下自動掃描的狀態（已啟用/停用）**
     a. 點擊**自動掃描**連結以開啟 IOC 檔案的篩選配置視窗。
     b. 選擇以下選項之一：
       - **已啟用**。
       - **已停用**。

IOC 檔案表將僅顯示與您設定的篩選條件相符的 IOC 檔案。

> 您可以同時使用多個篩選器。

清除 IOC 檔案篩選器

要清除一個或多個篩選條件的 IOC 檔案篩選器：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**IOC**子部分。
2. 這將開啟 IOC 檔案表。點擊您想要清除其篩選條件的 IOC 檔案表列標題右側的 ✕。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   IOC 檔案表將僅顯示與您設定的篩選條件相符的 IOC 檔案。

配置 IOC 掃描排程

您可以設定在具有 Endpoint Agent 元件的主機上使用 IOC 檔案搜尋入侵指標的計畫。

具有**安全稽核員**和**安全官**角色的使用者無法設定使用 IOC 檔案搜尋入侵指標的計畫。

若要設定在具有 Endpoint Agent 元件的主機上使用 IOC 檔案搜尋入侵指標的計畫：

1. 在應用程式 Web 介面的視窗中，選擇**設定**部分，**Endpoint Agent**子部分，**IOC 掃描排程**設定群組。
2. 在**啟動時間**下拉清單中，選擇搜尋入侵指標的開始時間。該時間是在您正在執行設定的 Central Node 伺服器的時區中指定的。

   如果 Endpoint Agent 取得新的掃描排程的時間晚於**IOC 掃描排程**中指定的時間，下一次掃描將於第二天的指定時間啟動。
3. 在**最大掃描持續時間**下拉清單中，選擇完成入侵指標搜尋的時間限制。
4. 點擊**套用**。

   儲存變更後，使用具有 Endpoint Agent 元件的主機上的 IOC 檔案搜尋入侵指標的新計畫立即生效。入侵指標搜尋結果顯示在警示表中。

管理使用 IOC 檔案搜尋入侵指標僅限於 Kaspersky Anti Targeted Attack Platform Web 介面提供的功能。沒有提供管理入侵指標搜尋的替代方法。

如果您以 Endpoint Agent 元件的角色使用 Kaspersky Endpoint Security for Windows，請確保IOC 檔案符合要求。您還必須考慮到，將 RegistryItem 資料類型新增至 IOC 搜尋範圍時，應用程式僅分析某些登錄機碼。

有關 IOC 檔案和被掃描登錄機碼要求的更多詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 線上說明：

- 登錄檔中的 IOC 掃描範圍（RegistryItem）。
- IOC 檔案要求。

管理使用者定義的入侵偵測規則

為了偵測網路流量中的入侵，您可以使用入侵偵測規則和使用內建演算法的其他入侵偵測方法。當在流量中偵測到攻擊指標時，Kaspersky Anti Targeted Attack Platform 會記錄*入侵偵測*技術事件。

> 需要有效的 KATA 或 KATA + NDR 產品授權金鑰來管理使用者定義的入侵偵測規則。

*入侵偵測規則*描述可能表示網路攻擊的流量異常。規則包含入侵偵測系統用於分析流量的條件。

如果啟用了基於規則的入侵偵測方法，則套用入侵偵測規則。您可以啟用或停用方法。

您可以使用以下類型的規則集：

- 系統規則集。這些規則集由卡巴斯基提供，用於偵測最常見攻擊或不必要的網路活動的指標。系統規則集在安裝應用程式後立即可用。您可以透過安裝更新來更新系統規則集。如果有必要，您可以為這些規則建立掃描排除項目。有關詳細資訊，請參閱*管理入侵偵測規則排除項目*和*管理 NDR 事件的允許規則*部分。
- 使用者定義的規則集。這些是您自己上傳的規則集。您上傳的檔案必須包含定義入侵偵測規則的資料結構。您要上傳的檔案必須都位於同一目錄中，並且必須具有 .rules 副檔名。自訂規則集的名稱與從其上傳規則集的檔案的名稱相符。

  使用者定義的入侵偵測規則集顯示在**自訂規則 → 入侵偵測**部分。

該應用程式支援所有上傳的規則集中總共最多 50000 條規則。您最多可以上傳 100 個規則集。

> 從使用者自訂規則集載入的規則可能包含流量分析條件，導致應用程式註冊過多的規則觸發事件。在這種情況下，您必須記住，註冊過多事件會影響入侵偵測系統的效能。

可以啟用或停用入侵偵測規則集。如果啟用了基於規則的入侵偵測方法，則在流量分析期間將套用已啟用規則集中的規則。如果停用某個規則集，則不會套用該規則集中的規則。

上傳規則集時，應用程式會檢查其中包含的規則。如果在規則中發現任何錯誤，應用程式將封鎖此類規則並且不會套用它們。如果在規則集的所有規則中發現錯誤或規則集不包含任何規則，則應用程式將停用此規則集。

當在流量中偵測到已啟用集的規則中指定的條件時，應用程式會註冊規則觸發事件。使用系統事件類型進行註冊，其代碼如下：

- 4000003000 – 對於涉及系統規則集中的規則被觸發的事件
- 4000003001 – 對於涉及使用者定義規則集中的規則被觸發的事件

使用者定義的規則集可以包含從其他入侵偵測和防護系統獲得的規則。當處理這些規則時，應用程式不會執行套用於網路封包的指定操作（例如，丟棄和拒絕操作）。當入侵偵測規則觸發時，Kaspersky Anti Targeted Attack Platform 僅記錄一個事件。

Kaspersky Anti Targeted Attack Platform 事件分數的數值與入侵偵測規則中的優先順序值相對應（請參閱下表）。

規則優先順序與事件分數的對應關係

入侵偵測規則中的優先順序值	Kaspersky Anti Targeted Attack Platform 事件分數
四個或以上	2.5
3	4.5
2	6.5
1	9

您可以在**設定** → **事件類型**下配置註冊入侵偵測事件的設定。

您可以在已註冊事件表中檢視入侵偵測事件。

在分散式解決方案和多組織用戶模式下，使用者定義的入侵偵測規則可以有以下類型之一：

- 在 PCN 伺服器上建立。這些規則用於掃描 PCN 伺服器上的流量。
- 在 SCN 伺服器上建立。這些規則用於掃描 SCN 伺服器上的流量。

具有**資深安全員**角色的使用者可以上傳、啟用或停用使用者定義的入侵偵測規則集，以及將卡巴斯基定義的入侵偵測規則新增至掃描排除項目。具有**安全稽核員**角色的使用者可以檢視使用者定義的偵測規則集。具有**安全官**角色的使用者無權存取使用者定義的入侵偵測規則。

檢視入侵偵測規則表

使用者定義的入侵偵測規則表位於應用程式 Web 介面視窗的“**自訂規則**”部分，“**入侵偵測**”子部分。

表包含以下資訊：

- **規則集**是規則集的名稱。
- **建立者**是上傳規則檔案的使用者名稱。
- **狀態**是規則的目前狀態。規則可具有下列狀態之一：**已啟用**、**已停用**。
- **規則**是規則集中規則的狀態。可顯示以下狀態之一：*正常*、*所有規則都有錯誤*、*部分規則有錯誤*。
- **檔案大小**是已上傳規則檔案的大小。
- **上次更新**是檔案上傳的日期。

如有需要，您可以自訂表格中欄的顯示。

配置入侵偵測規則表的顯示

您可以自訂入侵偵測規則表中列的顯示。

若要自訂入侵偵測規則表的顯示：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**入侵偵測**子部分。

2. 在表格的標題部分，點擊 ⚙ 。
   這將開啟**自訂表格**視窗。

3. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   必須選擇至少一個核取方塊。

4. 如果要重新排列欄，請點擊 ⌄ 或 ⌃ ，將含有參數的列移至新位置。

5. 關閉表格設定視窗。

入侵偵測規則表顯示已配置。

其他入侵偵測方法

為了偵測入侵，您可以使用以下附加方法：

- 偵測 ARP 封包中偽造位址的跡象（ARP 欺騙）。

  如果啟用了 ARP 欺騙偵測，Kaspersky Anti Targeted Attack Platform 會檢查 ARP 封包中指定的位址並偵測低階中間人 (MITM) 攻擊的指標。在使用 ARP 協定的網路中，這種類型的攻擊表現為在流量中發現虛假 ARP 訊息。

  當偵測到 ARP 欺騙指標時，應用程式會註冊入侵偵測技術事件。使用系統事件類型進行註冊，其代碼如下：

  - 4000004001 用於偵測與 ARP 請求無關的多個 ARP 回應的事件。
  - 4000004002 用於偵測從同一 MAC 位址到不同收件者的多個 ARP 請求的事件。

- TCP 協定異常偵測。

  如果啟用了 TCP 協定異常偵測，Kaspersky Anti Targeted Attack Platform 將掃描受支援的應用程式層協定中資料流的 TCP 段。

  當 Kaspersky Anti Targeted Attack Platform 偵測到包含不同內容的重疊 TCP 段的封包時，它會記錄入侵偵測技術事件。事件註冊的系統事件類型代碼為 4000002701。

- IP 協定異常偵測。

  如果啟用了 IP 協定異常偵測，Kaspersky Anti Targeted Attack Platform 將會掃描片段化的 IP 封包。

  當偵測到 IP 封包組裝錯誤時，應用程式會註冊入侵偵測技術事件。使用系統事件類型進行註冊，其代碼如下：

  - 4000005100 用於在 IP 封包組裝過程中偵測資料衝突的事件（IP 片段重疊）
  - 4000005101 用於偵測超過最大允許大小的 IP 封包的事件（IP 片段溢位）
  - 4000005102 用於偵測初始片段小於預期（IP 片段太小）的 IP 封包的事件
  - 4000005103 用於偵測 IP 封包片段的誤關聯事件（誤關聯片段）

- 暴力攻擊和掃描偵測。

  啟用暴力攻擊和掃描偵測後，Kaspersky Anti Targeted Attack Platform 會檢查網路活動統計資料，以偵測暴力攻擊、拒絕服務攻擊、掃描、網路服務欺騙和其他異常的指標。

  此方法使用內建規則。當觸發規則時，應用程式會註冊入侵偵測技術事件。這些事件使用被指派代碼 4000003002 的系統事件類型進行註冊。

您可以啟用或停用方法。無論入侵偵測規則是否存在或是否啟用，都可以應用其他入侵偵測方法。其他偵測方法使用內建演算法。

啟用和停用入侵偵測規則集

入侵偵測規則集可以*啟用*或*停用*。如果停用某個規則集，則該規則集中的任何規則都不會用於入侵偵測。

啟用或停用選定的規則集時，入侵偵測系統將在安裝了應用程式元件（Central Node 和 Sensor）的所有電腦上重新啟動。必須重新啟動才能套用變更。

只有擁有**資深安全員**角色的使用者可以改變入侵偵測規則集的狀態。

若要變更入侵偵測規則集的狀態：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**入侵偵測**子部分。
2. 選取要變更其狀態的規則集旁的核取方塊。
3. 右鍵點擊以開啟上下文功能表。
4. 在上下文功能表中，選擇以下命令之一：
   - 如果要啟用所選規則集中所有已停用的規則集，請選擇**啟用**。
   - 如果要停用所選規則集中所有已啟用的規則集，請選擇**停用**。
   - 如果要反轉所有選定規則集的狀態，請選擇**變更選定規則集的狀態**。此選項可讓您在安裝了應用程式元件的所有電腦上快速啟用和停用具有不同狀態的選定規則集：要套用變更，您只需在這些電腦上重新啟動一次入侵偵測系統。
5. 在確認視窗中，點擊“**確定**”。

入侵偵測規則集的狀態發生改變。

載入和替換使用者定義的入侵偵測規則集

您可以將入侵偵測規則集從檔案上傳到應用程式中。要上傳到應用程式，具有入侵偵測規則描述的檔案必須位於同一資料夾中並具有 .rules 副檔名。檔案名稱不得包含下列字元：`\ / : * ? , " < > |`

從檔案上傳的入侵偵測規則會作為使用者定義的規則集保存在應用程式中。規則集的名稱與上傳規則集的檔案的名稱相同。

> 從檔案上傳規則集時，目前使用者自訂規則集將從表中刪除並替換為新規則集。

只有擁有“**資深安全員**”角色的使用者可以上傳使用者定義的入侵偵測規則集。

要上傳和替換使用者定義的入侵偵測規則集：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**入侵偵測**子部分。
2. 在工具列中，點擊"**取代所有使用者定義的規則**"按鈕。
3. 在確認視窗中，點擊"**確定**"。

   這將開啟檔案上傳視窗。
4. 選擇包含所需文件的資料夾，然後點擊按鈕從該資料夾上傳檔案。

   規則集表顯示新的使用者自訂規則集。所有沒有錯誤的規則集均已啟用。
5. 檢查上傳的規則集是否有錯誤。

   有關偵測到的錯誤的資訊顯示在"**規則**"列中。如果沒有錯誤，則會顯示"*正常*"狀態。如果規則集包含錯誤，您可以點擊"**詳細資料**"以檢視有關它們的詳細資訊。
6. 如有必要，請啟用或停用規則集（包括狀態為"*某些規則有錯誤*"的規則集）。

使用者自訂的入侵偵測規則集被上傳。

刪除使用者定義的入侵偵測規則集

您可以刪除從檔案上傳到應用程式中的所有使用者定義的入侵偵測規則集。無法選擇要刪除的使用者自訂規則集。如果您只想使用應用程式中目前的某些規則集，可以將包含這些規則集的檔案複製到單獨的資料夾中，用該資料夾中的規則集取代所有使用者定義的規則集。

只有擁有"**資深安全員**"角色的使用者可以刪除使用者定義的入侵偵測規則集。

若要刪除使用者自訂的入侵偵測規則集：

1. 在應用程式 Web 介面的視窗中，選擇**自訂規則**部分，**入侵偵測**子部分。
2. 在工具列中，點擊**刪除所有使用者定義的規則**按鈕。
3. 在確認視窗中，點擊"**確定**"。

   這將打開一個視窗，用於選擇包含入侵偵測規則檔案的資料夾。

所有使用者定義的入侵偵測規則集將從表中刪除。

管理使用者定義的 YARA 規則

您可以使用 YARA 規則作為 YARA 模組資料庫來掃描在 Central Node 接收的檔案和物件，並使用 Endpoint Agent 元件掃描主機。

在分散式解決方案和多組織用戶模式下，自訂 YARA 規則可以具有以下類型之一：

- **全球** — 在 PCN 伺服器上建立。這些規則被用來掃描在 PCN 伺服器以及連線到該 PCN 伺服器的所有 SCN 伺服器上收到的檔案和物件。掃描的檔案和物件屬於使用者在應用程式 Web 介面中管理的租戶。
- **本機** — 在 SCN 伺服器上建立。這些規則被用來掃描在 SCN 伺服器上收到的檔案和物件。掃描的檔案和物件屬於使用者在應用程式 Web 介面中管理的租戶。

在管理應用程式 Web 介面時，具有**資深安全員**角色的使用者可以使用應用程式 Web 介面將 YARA 規則檔案匯入 Kaspersky Anti Targeted Attack Platform。

具有**安全稽核員**和**安全官**角色的使用者只能檢視 YARA 規則。

檢視 YARA 規則表

使用者定義的 YARA 規則表包含有關用於掃描檔案和物件以及建立警示的 YARA 規則的資訊；該表顯示在應用程式 Web 介面視窗中的**自訂規則**部分，**YARA**子部分。

表包含以下資訊：

- **已建立**是規則建立時間。
- **重要性** — 根據卡巴斯基的經驗，對於 Kaspersky Anti Targeted Attack Platform 使用者而言，警示重要性取決於此警示可能對電腦或企業 LAN 安全造成的影響。

  預設情況下，透過上傳的 YARA 規則掃描產生的警示被分配高重要性。
- **類型**是規則的類型，取決於應用程式的操作模式和產生規則的伺服器的角色：
  - **全球** — 在 PCN 伺服器上建立。這些規則被用來掃描在 PCN 伺服器以及連線到該 PCN 伺服器的所有 SCN 伺服器上收到的檔案和物件。掃描的檔案和物件屬於使用者在應用程式 Web 介面中管理的租戶。
  - **本機** — 在 SCN 伺服器上建立。這些規則被用來掃描在 SCN 伺服器上收到的檔案和物件。掃描的檔案和物件屬於使用者在應用程式 Web 介面中管理的租戶。
- **名稱** — 規則的名稱。
- **檔案名稱**是從中匯入規則的檔案的名稱。
- **建立者**是用於匯入規則的帳戶的使用者的名稱。
- **伺服器**是伺服器的名稱，具有對其應用規則的 PCN 或 SCN 角色。

  如果您使用的是分佈式解決方案和多租戶模式，則會顯示此列。
- **流量掃描**流掃描檔案和物件到達 Central Node 時規則的使用：
  - **已啟用** – 規則正在被使用。
  - **已停用** – 該規則未被使用。

配置 YARA 規則表顯示

您可以顯示或隱藏列並變更表中列的順序。

若要設定表格顯示：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。

   這將開啟 YARA 規則表。

2. 在表格的標題部分，點擊 ⚙ 。
   這將開啟**自訂表格**視窗。

3. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   > 必須選擇至少一個核取方塊。

4. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。

5. 如果要還原預設表格顯示設定，請點擊**預設**。

6. 點擊**套用**。

表格顯示已配置。

匯入 YARA 規則

要匯入 YARA 規則：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。

2. 點擊**上傳**。
   這將開啟檔案選擇視窗。

3. 選擇您想上傳的 YARA 規則檔案，然後點擊"**開啟**"。
   這將關閉檔案選擇視窗並開啟**匯入 YARA 規則**視窗。

   > 上傳檔案的最大允許大小為 20 MB。

   報告顯示在視窗的下部。報告表包含以下資訊：

   - 可以成功匯入的規則數量。
   - 不匯入的規則數量（如果有）。
     對於每條無法匯入的規則，都會列出其名稱。

4. 選擇**流量掃描**，如果要使用匯入的規則對在 Central Node 接收的物件和資料進行串流掃描。

5. 如有必要，請在**敘述**欄位中輸入任何附加資訊。

   > **重要級別**欄位無法編輯。預設情況下，由上傳的 YARA 規則產生的警示被分配高重要性等級。

6. 在**套用到**下面，選擇與要對其應用規則的伺服器對應的核取方塊。未選取核取方塊的伺服器不會使用上傳的規則進行掃描。如果清除了租用戶行（清單第一行）的核取方塊，則以後新增的該租用戶的伺服器也不會使用上傳的規則進行掃描。

   僅當您使用分佈式解決方案和多組織用戶模式時才會顯示"**套用到**"設定群組。

7. 點擊**儲存**。

匯入的規則顯示在 YARA 規則表中。

檢視 YARA 規則詳細資訊

要檢視 YARA 規則詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。

   這將開啟 YARA 規則表。

2. 選擇您想檢視資訊的規則。

這將開啟一個視窗，其中包含有關規則的資訊。

此視窗包含以下資訊：

- 點擊**警示**連結即可在新的瀏覽器標籤中顯示警示表。警示將根據針對性攻擊分析器技術和您正在處理的 TAA (IOA) 規則的名稱進行篩選。
- **啟動 YARA 掃描**連結將開啟工作建立視窗。
- **下載**連結可讓您下載包含 YARA 規則的檔案。
- **規則名稱**是檔案中指定的規則的名稱。
- **流量掃描**流掃描檔案和物件到達 Central Node 時規則的使用：
- **類型**是規則的類型，取決於產生它的伺服器的角色：
  - **全球** — 在 PCN 伺服器上建立。這些規則被用來掃描在 PCN 伺服器以及連線到該 PCN 伺服器的所有 SCN 伺服器上收到的檔案和物件。掃描的檔案和物件屬於使用者在應用程式 Web 介面中管理的租戶。
  - **本機** — 在 SCN 伺服器上建立。這些規則被用來掃描在 SCN 伺服器上收到的檔案和物件。掃描的檔案和物件屬於使用者在應用程式 Web 介面中管理的租戶。
- 重要級別是分配給根據此規則掃描而建立的警示的重要性等級。

  預設情況下，透過上傳的 YARA 規則掃描產生的警示被分配高重要性。
- **敘述**是有關您指定的規則的任何附加資訊。
- **套用到** – 伺服器的名稱，包含在其上套用規則的 Central Node 元件。

篩選並搜尋 YARA 規則

若要依所需條件篩選或搜尋 YARA 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。
   這將開啟 YARA 規則表。

2. 根據篩選條件，執行以下操作：

   - **按建立時間**

     a. 點擊**已建立**連結以開啟篩選設定視窗。

     b. 選擇以下選項之一：

     - **任何時候**如果您希望表顯示任何時間建立的規則。
     - **上一個小時**，如果您希望應用程式顯示表中最後一小時建立的規則。
     - **最後一天**，如果您希望應用程式顯示表中最後一天建立的規則。
     - **自訂範圍**，如果您希望應用程式顯示表中在指定時段內建立的規則。

     c. 如果您選擇了**自訂範圍**，請選擇該期間的開始日期和結束日期，然後點擊**套用**。

   - **按規則名稱**

     a. 點擊**規則名稱**連結以開啟篩選功能表。

     b. 在下拉清單中，選擇以下篩選運算子之一：

     - **包含**
     - **不包含**

     c. 在文字方塊中，鍵入規則名稱或規則名稱中的字元序列。

     d. 點擊**套用**。

   - **按檔案名稱**

     a. 點擊**檔案名稱**連結以開啟篩選功能表。

     b. 在下拉清單中，選擇以下篩選運算子之一：

     - **包含**
     - **不包含**

     c. 在輸入欄位中，鍵入檔案名稱或檔案名稱中的字元序列。

     d. 點擊**套用**。

- **按上傳規則檔案的使用者名稱**

  a. 點擊**建立者**連結以開啟篩選功能表。

  b. 在下拉清單中，選擇以下篩選運算子之一：

  - **包含**
  - **不包含**

  c. 在文字方塊中，鍵入使用者名稱或使用者名稱中的字元序列。

  d. 點擊**套用**。

- **按規則狀態**

  a. 點擊**流量掃描**連結以展開篩選器設定清單。

  b. 選擇以下選項之一：

  - **所有。**
  - **已啟用。**
  - **已停用。**

此表僅顯示與指定條件相符的規則。

您可以同時使用多個篩選器。

清除 YARA 規則篩選器

要清除 YARA 規則篩選器的一個或多個篩選條件：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。
   這將開啟 YARA 規則表。

2. 點擊要為其清除篩選條件的規則表的列標題右側的 。
   如果要清除多個篩選條件，請採取步驟單獨清除每個篩選條件。

選定篩選器將會被清除。

此表僅顯示與指定條件相符的規則。

啟用和停用 YARA 規則

具有**資深安全員**角色的使用者可以啟用或停用一個或多個規則，也可以同時啟用或停用所有規則。

在分散式解決方案和多租戶模式下工作時，您只能啟用或停用在目前伺服器上建立的 YARA 規則。這意味著在 PCN 的 Web 介面中，您只能啟用或停用在 PCN 伺服器上建立的規則。在 SCN 的 Web 介面中，您只能啟用或停用在 SCN 伺服器上建立的規則。

如果在 PCN 和 SCN 伺服器上啟用了同名的 YARA 規則，則掃描檔案和物件時PCN 規則優先於 SCN 規則。

若要啟用或停用用於流掃描到達 Central Node 的檔案和物件的 YARA 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。
   這將開啟 YARA 規則表。
2. 在具有相關規則的行中，選擇或清除**流量掃描**列。

此規則針對到達 Central Node 的流掃描檔案和物件啟用或停用。

若要啟用或停用所有或多個 YARA 規則以流掃描到達 Central Node 的檔案和物件：

1. 在程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。
2. 選擇要啟用或停用其使用的規則左側的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。
   控制面板出現在視窗的下部。
3. 點擊**啟用**或者**停用**啟用或停用所有規則。

所選規則針對到達 Central Node 的流掃描檔案和物件啟用或停用。

刪除 YARA 規則

要刪除 YARA 規則:

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。
   這將開啟 YARA 規則表。
2. 選擇您想刪除的規則。
   這將開啟一個視窗，其中包含有關規則的資訊。
3. 點擊**刪除**。
4. 這將開啟操作確認視窗；在該視窗中，點擊**是**。

規則被刪除。

要刪除全部或多個 YARA 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**YARA**子部分。
   這將開啟 YARA 規則表。

2. 選擇您要刪除的規則左側的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。
   控制面板出現在視窗的下部。

3. 點擊**刪除**。

4. 這將開啟操作確認視窗；在該視窗中，點擊**是**。

所選檔案將被刪除。

具有**安全稽核員**和**安全官**角色的使用者無法刪除 YARA 規則。

管理儲存和隔離區中的物件

儲存區被用來儲存必須被傳送進行掃描的檔案以及執行工作所獲得的檔案：**獲取檔案**，**從隔離區還原檔案**，**進行取證**，**獲取 NTFS 元檔案**，**獲取登錄機碼**，**獲取處理程序記憶體傾印**。

儲存位於 Central Node 伺服器上。

您可以按照以下方式管理儲存中的物件：刪除、下載、上傳和傳送待掃描的物件，以及篩選物件清單。

Kaspersky Anti Targeted Attack Platform 將儲存中的物件顯示為物件表。

如果您使用分佈式解決方案和多組織用戶模式，儲存位於 PCN 和 SCN 伺服器上。PCN 伺服器的 Web 介面顯示有關使用者有權存取的租用戶的所有已連線 SCN 的儲存資訊。

具有**資深安全員**角色的使用者可以使用工作將物件副本放入儲存，或使用 PCN 或 SCN 伺服器上的 Kaspersky Anti Targeted Attack Platform Web 介面將物件上傳到儲存，該伺服器用於管理使用者有權存取的租用戶。

具有**安全官**角色的使用者只能處理同一使用者在 PCN 或 SCN 伺服器上建立的工作中收到的檔案，該伺服器用於管理使用者有權存取的租用戶。

如果您認為某個檔案具有威脅，可以使用 Endpoint Agent 元件將其在電腦上隔離。隔離檔案的中繼資料會顯示在 Kaspersky Anti Targeted Attack Platform Web 介面的**儲存**區段、**隔離區**子區段中。

*Kaspersky Anti Targeted Attack Platform 伺服器上的隔離區*是 Kaspersky Anti Targeted Attack Platform 解決方案伺服器端的儲存區域，用於儲存在 Endpoint Agent 電腦上隔離之物件的中繼資料；這些資料位於 Kaspersky Anti Targeted Attack Platform Web 介面的**儲存**區段、**隔離區**子區段中。

您可以管理隔離物件：從隔離區還原物件，以及將 Endpoint Agent 電腦上隔離之物件的副本上傳到 Kaspersky Anti Targeted Attack Platform 的儲存。

Kaspersky Anti Targeted Attack Platform 以表格形式顯示有關隔離物件的資訊。

儲存的最大容量是在設定應用程式規模時決定的。一旦超過此閾值，應用程式就開始從儲存區中移除最早的物件副本。當佔用的空間量再次低於閾值時，應用程式停止從儲存區中刪除物件的副本。

可以放置在儲存中的物件的最大大小為1GB。

由於從隔離區還原物件所需的中繼資料，物件的實際大小可能大於物件的表觀大小。隔離物件時，會考慮其實際大小。加密檔案可能以解密形式傳送（取決於加密設定），壓縮檔案會按原樣傳送。

檢視放入儲存空間的物件表

放入儲存中的物件表位於應用程式 Web 介面視窗的**儲存**部分，**檔案**子部分。

放入儲存區中的物件表包含以下資訊：

1. **類型**是將物件放入儲存區的方法。
   可以採用以下方法：
   - — 該物件透過以下方式之一放置在儲存中：
     - **獲取檔案**工作已執行。
     - 收到了在具有 Endpoint Agent 元件的主機上被隔離的物件的副本（在**儲存**部分，**隔離區**子部分，在選單中選擇了對具有物件目錄的連結的**從隔離區獲取檔案**操作）。
   - — 該物件透過以下方式之一放置在儲存中：
     - **進行取證**工作已執行。
     - **獲取處理程序記憶體傾印**工作已執行。
     - **獲取登錄機碼**工作已執行。
     - **獲取 NTFS 元檔案**工作已執行。
   - — 物件是由使用者在**儲存**部分的**檔案**子部分中手動下載的。
2. **物件** — 有關該物件的資訊。例如，檔案名稱或檔案路徑。
3. **掃描結果** — 物件掃描結果。
   掃描結果顯示為以下其中一個值：
   - **未偵測到** — 掃描的結果是，應用程式未偵測到針對性攻擊、疑似感染物件或可疑活動的跡象。
   - **錯誤** — 物件掃描以錯誤結束。
   - **進行中** — 物件掃描尚未完成。
   - **未掃描** — 物件未被傳送以進行掃描。
   - **偵測到** — 掃描的結果是，應用程式偵測到針對性攻擊、疑似感染物件或可疑活動的跡象。

4. **伺服器**是具有 PCN 或 SCN 角色的伺服器的名稱。從中接收物件的主機連線到此伺服器。
   如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄。

5. **來源** — 從中接收物件的主機的 IP 位址或名稱，或上傳物件的使用者帳戶的名稱。

6. **儲存時間** — 物件放入儲存的日期和時間。

7. **操作** — 可以對物件執行的操作。如下操作可用：

   - — 刪除儲存中的物件。
   - — 將儲存中的物件傳送至惡意軟體防護引擎、YARA 和 Sandbox 技術進行掃描。
   - — 將物件從儲存下載到您的電腦。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **下載**。
- **傳送檔案進行掃描**。
- **尋找事件**：
  - **檔案路徑**。
  - **MD5**。
  - **SHA256**。
- **尋找警示**：
  - **檔案路徑**。
  - **MD5**。
  - **SHA256**。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

使用 Web 介面檢視有關手動放置在儲存中的物件的資訊

若要檢視被手動放置在儲存中的物件的資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 在表中，選擇帶有您要檢視其資訊的 圖示的物件。
   這將開啟物件詳細資訊視窗。

此視窗包含以下資訊：

- **檔案名稱** — 檔案的名稱。
- **大小** — 檔案的大小。
- **MD5** — 檔案的 MD5 雜湊。
- **SHA256** — 檔案的 SHA256 雜湊。
- **上傳時間** — 上傳使用者手動上傳物件的時間。
- **使用者名稱** — 手動將物件上傳到儲存區的使用者帳戶名稱。
- **掃描結果** — 應用程式的物件掃描結果。

在 Kaspersky TIP 上尋找按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。

點擊**建立阻止規則**以阻止檔案運行。

您可以點擊**下載**將檔案下載到電腦的硬碟上。

點擊具有檔案名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

點擊具有“**MD5**”的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **在 Kaspersky TIP 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊具有“**SHA256**”的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- 在 Kaspersky TIP 上尋找。
- **在 virustotal.com 上尋找**。
- 尋找事件。
- 尋找警示。
- 建立阻止規則。
- **複製值到剪貼簿**。

檢視有關透過獲取檔案工作放置在儲存中的物件的資訊

*查看有關被“**獲取檔案**”或者“**從隔離區獲取檔案**”工作放置在儲存中的物件的資訊：*

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 在表中，選擇帶有您要檢視其資訊的圖示的物件。
   這將開啟物件詳細資訊視窗。

此視窗包含以下資訊：

- 推薦組。以下建議可顯示：
  - “工作”連結開啟將物件放入儲存的工作。
  - “警示 ”連結可開啟警示，其中包含被放置在儲存中的物件。
  - “隔離的物件”連結會開啟隔離物件的中繼資料。
- 物件 — 檔案名稱或路徑。
- **大小** — 檔案的大小。
- **MD5** — 檔案的 MD5 雜湊。
- **SHA256** — 檔案的 SHA256 雜湊。
- **儲存時間** — 物件放入儲存區的時間。
- **租戶** — Central Node、PCN 或 SCN 伺服器所屬租戶的名稱。
- **伺服器** — Central Node、PCN 或SCN 伺服器的名稱。從中接收物件的主機連線到此伺服器。
- **主機** — 接收物件的主機的名稱。
- **掃描結果** — 應用程式的物件掃描結果。

點選“Sandbox 偵測”顯示檔案行為分析結果的詳細資訊。

> 只有當 Sandbox 偵測該檔案時，才會顯示檔案行為分析結果。如果檔案上傳至系統，然後在 Sandbox 中掃描，但元件未偵測到威脅，則不會顯示結果。

在 Kaspersky TIP 上尋找按鈕允許在 Kaspersky Threat Intelligence Portal 上查找檔案。

點擊**建立阻止規則**以阻止檔案運行。

您可以點擊**下載**將檔案下載到電腦的硬碟上。

點擊具有檔案名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

點擊具有“**MD5**”的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **在 Kaspersky TIP 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊具有“**SHA256**”的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

檢視有關透過獲取資料工作放置在儲存中的物件的資訊

*看有關被**進行取證**、**獲取處理程序記憶體傾印**、**獲取登錄機碼**、**獲取 NTFS 元檔案**工作放置在儲存中的物件的資訊：*

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。

   這將開啟物件表。

2. 在表中，選擇帶有您要檢視其資訊的圖示的物件。
   這將開啟物件詳細資訊視窗。

此視窗包含以下資訊：

- **物件**是檔案名稱或路徑。
- **大小** — 檔案的大小。
- **MD5** — 檔案的 MD5 雜湊。
- **SHA256** — 檔案的 SHA256 雜湊。
- **儲存時間** — 物件放入儲存區的時間。
- **主機** — 接收物件的主機的名稱。

您可以點擊**下載**將檔案下載到電腦的硬碟上。

點擊具有檔案名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

點擊具有“**MD5**”的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **在 Kaspersky TIP 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

點擊具有“**SHA256**”的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **在 Kaspersky TIP 上尋找**。
- **在 virustotal.com 上尋找**。
- **尋找事件**。
- **尋找警示**。
- **建立阻止規則**。
- **複製值到剪貼簿**。

從儲存下載物件

如果您认為儲存區中的某個物件是安全的，可以將它下載到本機電腦。

下載受感染物件可能會對本機電腦的安全構成威脅。

要下載儲存區中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 在包含要下載的物件名稱的行的右側部分，點擊 。

該檔案將被儲存到瀏覽器下載資料夾中的本機電腦。檔案以 ZIP 壓縮檔案形式下載，並受密碼“infected”防護。

將物件上傳到儲存

如果需要掃描特定物件，可以將此物件上載到儲存空間並傳送以進行掃描。

要上傳物件到儲存區中：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 在視窗的右上角，點擊**上傳**。
   這將開啟檔案選擇視窗。
3. 選擇您想上傳到儲存的物件。
4. 如果要將副檔名為 .lnk 的檔案上傳到存儲：
   a. 在“**檔案名**”欄位中，輸入 *.lnk 並按 **Enter**。
   b. 選擇物件。
5. 點擊**開啟**。

物件將被上傳到儲存並顯示在物件表中。

具有**安全稽核員**角色的使用者無法將物件上傳到儲存。

傳送儲存中的物件進行掃描

您可以使用惡意軟體防護引擎和 YARA 技術對包含 Central Node 元件以及 Sandbox 元件的儲存區物件進行掃描。

在以下情況下，建議從儲存區傳送要掃描的物件：

- 放入儲存區時掃描物件已停用。
- 應用程式資料庫已更新。
- 手動將物件上傳到儲存區。

若要從儲存傳送物件進行掃描：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 點擊您想掃描的物件。
   這將開啟物件詳細資訊視窗。
3. 點擊**掃描**。
   物件掃描將開始。
   物件掃描完成後，其狀態將顯示在物件表中。

您也可以透過點擊被放置在儲存中的物件表中的物件資訊行的右側部分的🔍傳送儲存中的物件進行掃描。

> 具有**安全稽核員**角色的使用者無法掃描儲存中的物件。

刪除儲存中的物件

若要刪除儲存區中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 點擊您想刪除的物件。
   這將開啟物件詳細資訊視窗。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

該物件將從儲存區中刪除。

您也可以透過點擊被放置在儲存中的物件表中的物件資訊行的右側部分的🗑刪除儲存中的物件。

若要從儲存中刪除所有或多個物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 選擇要從儲存中刪除的物件旁邊的核取方塊。
   您可以透過選取包含列標題的行中的核取方塊來選取所有物件。
3. 在視窗下部顯示的窗格中，點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

選定的物件將從儲存中刪除。

具有**安全稽核員**角色的使用者無法刪除儲存中的物件。

按物件類型篩選儲存中的物件

若要依類型篩選儲存區中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 點擊**類型**連結以開啟物件篩選功能表。
3. 選擇一個或多個核取方塊：
   - **由“獲取檔案”工作上傳**，如果您希望表格顯示被**獲取檔案**和**從隔離區還原檔案**工作放置在儲存中的物件。
   - **通過 Web 介面上傳**，如果您希望表格顯示使用者使用 Kaspersky Anti Targeted Attack Platform Web 介面上傳的物件。
   - **由“獲取資料”工作上傳**，如果您希望表格顯示被**進行取證**、**獲取 NTFS 元檔案**、**獲取登錄機碼**、**獲取處理程序記憶體傾印**工作放置在儲存中的物件。
4. 點擊**套用**。

物件表將僅顯示與您設定的篩選條件相符的物件。

您可以同時使用多個篩選器。

按物件描述篩選儲存中的物件

若要按物件描述篩選儲存中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 點擊**物件**連結以開啟物件篩選功能表。
3. 在下拉式清單中，選擇以下選項之一：
   - **檔案路徑**
   - **MD5**。
   - **SHA256**
4. 在下拉清單中，選擇下列物件篩選運算子之一：
   - **包含**。
   - **不包含**。
   - **等於**。
   - **不等於**
   - **匹配樣式**
   - **與樣式不符**
5. 在輸入欄位中，指定物件描述的一個或多個字元。
6. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。
7. 點擊**套用**。

物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

根據掃描結果篩選儲存中的物件

若要依這些物件的掃描結果篩選儲存中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。

2. 點擊**掃描結果**連結以開啟物件篩選功能表。

3. 選擇一個或多個核取方塊：

   - **未偵測到**。
   - **錯誤**。
   - **進行中**。
   - **未掃描**。
   - **偵測到**。

4. 點擊**套用**。

   物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

根據 Central Node、PCN 或 SCN 伺服器的名稱篩選儲存中的物件

若要按 Central Node、PCN 或 SCN 伺服器的名稱篩選儲存中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。

   這將開啟物件表。

2. 點擊**伺服器**連結以開啟物件篩選功能表。

3. 選擇要在儲存中篩選物件的伺服器對面的一個或多個核取方塊。

4. 點擊**套用**。

   物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

按物件來源篩選儲存中的物件

若要依從中接收物件的來源篩選儲存區中的物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。

   這將開啟物件表。

2. 點擊**來源**連結以開啟物件篩選功能表。

3. 在下拉清單中，選擇下列物件篩選運算子之一：

   - **包含**
   - **不包含**

4. 在輸入欄位中，指定手動上傳物件的使用者帳戶的 IP 位址、主機名稱或名稱的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

根據物件放置在儲存中的時間篩選物件

若要按物件被放入儲存時的時間篩選物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。

2. 點擊**儲存時間**連結以開啟物件篩選功能表。

3. 選擇以下物件顯示時段之一：

   - **所有**，如果您希望表格顯示放入儲存區中的所有物件。
   - **上一個小時**，如果您希望表格顯示在最後一個小時內放入儲存區中的物件。
   - **最後一天**，如果您希望表格顯示在最後一天內放入儲存區中的物件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內放入儲存區中的物件。

4. 如果您選擇了**自訂範圍**物件顯示時段：

   a. 在開啟的日曆中，指定物件顯示時段的開始和結束日期。

   b. 點擊**套用**。

物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

清除儲存物件篩選器

要清除一個或多個篩選條件的儲存物件篩選器：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**檔案**子部分。
   這將開啟物件表。
2. 點擊您想要清除其篩選條件的儲存物件列標題右側的 ✕。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   物件表將僅顯示與您設定的篩選條件相符的物件。

檢視在具有 Kaspersky Endpoint Agent 元件的電腦上被隔離的物件表

可以在應用程式 Web 介面的**儲存**部分、**隔離區**子部分中找到具有 Endpoint Agent 元件的電腦上的被隔離物件表。

Kaspersky Anti Targeted Attack Platform 伺服器可儲存在具有 Endpoint Agent 元件的電腦上被隔離的物件的中繼資料。這些物件本身被儲存在偵測到威脅物件的每台電腦上的特殊儲存中。

在具有 Endpoint Agent 元件的電腦上被隔離的物件表包含以下資訊：

1. **物件** — 有關該物件的資訊。例如，檔案名稱或檔案路徑。
2. **來源**—物件被隔離所在電腦的 IP 位址或主機名稱，該電腦具有 Endpoint Agent 元件。
3. **儲存時間**—物件被隔離的日期和時間。
4. **狀態**—物件的狀態。

物件資訊行的右側部分包含按鈕：

- 您可以點擊 🗑 刪除 Kaspersky Anti Targeted Attack Platform 伺服器上物件的中繼資料。
- 您可以點擊 ↻ 在具有 Endpoint Agent 元件的電腦上從隔離區還原物件。
- 您可以點擊 將物件從具有 Endpoint Agent 元件的電腦上的隔離區複製到 Kaspersky Anti Targeted Attack Platform 伺服器。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **下載**。
- **傳送檔案進行掃描**。
- **尋找事件**：
  - **檔案路徑**。
  - **MD5**。
  - **SHA256**。
- **尋找警示**：
  - **檔案路徑**。
  - **MD5**。
  - **SHA256**。
- **複製值到剪貼簿**。

點擊具有主機名稱的連結將開啟一個清單，您可以從其中選擇以下操作之一：

- **新增到篩選器**。
- **從篩選器中排除**。
- **尋找事件**。
- **尋找警示**。
- **複製值到剪貼簿**。

檢視被隔離物件的資訊

若要檢視在具有 Endpoint Agent 元件的電腦上被隔離的物件的資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。
2. 在表格中，選擇要檢視其資訊的物件。
   這將開啟物件詳細資訊視窗。

此視窗包含以下資訊：

- 推薦組。工作推薦可以顯示，這是一個可開啟**工作**部分的連結；這是隔離了物件的工作。
- **類型**是被隔離物件的類型。
  可以使用以下類型的物件：
  - — 檔案。
  - — 處理程序記憶體傾印。
- **物件** — 檔案名稱或路徑。
- **狀態**是檔案的狀態（檔案是否可以從隔離區還原）。
- **來源**是在其上隔離物件、具有 Endpoint Agent 元件的電腦的名稱。
- **記錄時間**是物件被隔離的日期和時間。
- **操作**是檔案的狀態（檔案是否可以從隔離區還原）。
  如下操作可用：
  - — 從隔離區中刪除檔案。
  - — 取得 Kaspersky Anti Targeted Attack Platform 伺服器上的檔案副本。

點擊具有檔案名稱或檔案路徑的連結將開啟一個清單，您可以在其中選擇以下操作之一：

- 尋找事件。
- 尋找警示。
- **複製值到剪貼簿**。

從隔離中還原物件

若要在具有 Endpoint Agent 元件的電腦上從隔離區還原物件：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。
2. 在表格中，選擇要在具有 Endpoint Agent 元件的電腦上從隔離區還原的物件。
   這將開啟物件詳細資訊視窗。
3. 點擊視窗下部的**還原**。
   這將開啟**工作**部分和**從隔離區還原檔案**工作。
4. 在**敘述**欄位中，輸入工作描述。
5. 點擊**新增**。

檔案被從隔離區還原。

您也可以點擊在具有 Endpoint Agent 元件的電腦上被隔離的物件表的物件資訊行的右側部分的，運行工作以從隔離區還原檔案。

在分佈式解決方案和多組織用戶模式下，在 SCN 伺服器上被隔離的檔案無法在 PCN 伺服器上還原。您可以在建立隔離檔案工作的 SCN 伺服器上還原檔案。

具有**安全稽核員**角色的使用者無法從隔離區還原物件。

取得 Kaspersky Anti Targeted Attack Platform 伺服器上被隔離物件的副本

您要下載其副本的物件不得超過 100 MB。如果物件超過 100 MB，工作將結束並出現錯誤。

要將在具有 Kaspersky Endpoint Agent 元件的電腦上被隔離的物件複製到 Kaspersky Anti Targeted Attack Platform 伺服器：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。

   這將開啟物件表。

2. 在表格中，選擇要在具有 Endpoint Agent 元件的電腦上從隔離區還原的物件。

   這將開啟物件詳細資訊視窗。

3. 點擊視窗下部的**獲取檔案**。

   這將建立一個工作，用於取得在具有 Endpoint Agent 元件的電腦上被隔離的物件的副本。如果工作成功完成，物件的副本將上傳到 Kaspersky Anti Targeted Attack Platform 伺服器。物件會顯示在應用程式 Web 介面的**儲存**部分、**檔案**子部分中，位於放置在儲存中的物件表內。

   已建立工作的資訊顯示在**工作** Web 介面部分中。

您也可以將具有 Endpoint Agent 元件的電腦上的隔離物件複製到 Kaspersky Anti Targeted Attack Platform 伺服器，方法是點擊具有 Endpoint Agent 元件的電腦上的隔離物件表中物件資訊行右側的。

具有**安全稽核員**角色的使用者無法從隔離區取得物件的副本。

從表格中移除隔離物件的資訊

要從 Kaspersky Anti Targeted Attack Platform表中刪除在具有 Kaspersky Endpoint Agent 元件的電腦上被隔離的物件的資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。

   這將開啟物件表。

2. 點擊要從表格中刪除其資訊的物件。
   這將開啟物件詳細資訊視窗。

3. 點擊**刪除**。
   這將開啟操作確認視窗。

4. 點擊**是**。

有關在具有 Endpoint Agent 元件的電腦上被隔離的物件的資訊將被從表中刪除。

您也可以從表中刪除具有 Endpoint Agent 元件的電腦上的被隔離物件的資訊，方法是點擊隔離物件表中物件資訊行的右側部分中的🗑。

> 具有**安全稽核員**角色的使用者無法從表中刪除有關隔離物件的資訊。

按物件類型篩選有關隔離物件的資訊

若要按物件類型篩選被隔離物件的詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。

2. 點擊**類型**連結以開啟物件篩選功能表。

3. 選擇一個或多個核取方塊：

   - **檔案**，如果您希望表顯示被隔離物件的中繼資料。

   - **處理程序記憶體傾印**，如果您希望表顯示被隔離傾印的中繼資料。

4. 點擊**套用**。

物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

按物件描述篩選有關隔離物件的資訊

若要按物件描述篩選被隔離物件的詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。

2. 點擊**物件**連結以開啟物件篩選功能表。

3. 在下拉清單中，選擇下列物件篩選運算子之一：

   - **包含**
   - **不包含**

4. 在輸入欄位中，指定物件描述的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

   物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

按主機名稱篩選有關隔離物件的資訊

若要依隔離物件的主機名稱篩選被隔離物件的詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。

2. 點擊**來源**連結以開啟物件篩選功能表。

3. 在下拉清單中，選擇下列物件篩選運算子之一：

   - **包含**
   - **不包含**

4. 在輸入欄位中，指定主機名稱的一個或多個字元。

5. 若要使用不同條件新增篩選條件，請點擊 + 並指定篩選條件。

6. 點擊**套用**。

   物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

按時間篩選有關隔離物件的資訊

若要按物件被隔離時的時間篩選被隔離物件的詳細資訊：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。
2. 點擊**儲存時間**連結以開啟物件篩選功能表。
3. 選擇以下物件顯示時段之一：
   - **所有**，如果您希望表格顯示所有物件。
   - **上一個小時**，如果您希望表格顯示在最後一小時內被隔離的物件。
   - **最後一天**，如果您希望表格顯示在最後一天內被隔離的物件。
   - **自訂範圍**，如果您希望表格顯示在指定時段內被隔離的物件。
4. 如果您選擇了**自訂範圍**物件顯示時段：
   a. 在開啟的日曆中，指定物件顯示時段的開始和結束日期。
   b. 點擊**套用**。

物件表將僅顯示與您設定的篩選條件相符的物件。

> 您可以同時使用多個篩選器。

重置有關隔離物件資訊的篩選器

若要清除一個或多個篩選條件的篩選器：

1. 在應用程式 Web 介面視窗中，選擇**儲存**部分，**隔離區**子部分。
   這將開啟物件表。
2. 點擊您想要重設其篩選條件的隔離物件表列標題右側的 ⊠。

   > 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選器將會被清除。

物件表將僅顯示與您設定的篩選條件相符的物件。

管理報告

具有“**資深安全員**”角色的使用者可以使用 Kaspersky Anti Targeted Attack Platform 管理有關應用程式警示的報告：建立報告範本、基於範本建立報告、檢視和刪除報告和報告範本。

具有“**安全稽核員**”角色的使用者可以檢視報告和報告範本，並從範本建立報告。

可以使用以下類型的報告：

- 一般報告。這些報告的範本可在“**報告**”部分的“**範本**”子部分找到。您可以在“**報告**”部分的“**產生的報告**”子部分管理產生的報告。

  您可以根據您的產品授權管理應用程式的所有模式下的報告範本和報告。報告根據指定時間段內的警示選擇產生。如果您使用分佈式解決方案和多組織用戶模式，則選擇也可以基於租用戶和該租用戶的伺服器。

- NDR 功能報告。可在“**報告**”部分，“**報告 (NDR)**”子部分找到。

  如果您新增 KATA+NDR 產品授權金鑰，則可以管理報告範本和報告。根據產生報告的節點的資料，根據指定時間段內的警示選擇產生報告。

管理常見報告

在管理應用程式 Web 介面時，具有“**資深安全員**”角色的使用者可以管理有關應用程式警示的 KATA 報告：建立報告範本、基於範本建立報告、檢視和刪除報告和報告範本。

具有“**安全稽核員**”角色的使用者可以檢視 KATA 報告和報告範本以及從範本建立報告。

若要建立 KATA 報告：

1. **建立報告範本。**
2. **根據範本建立報告。**

檢視範本和報告的表格

範本和報告顯示在應用程式 Web 介面視窗的**報告**部分中。

“**產生的報告**”子部分包含一個報告表。表包含以下資訊：

- **建立時間**—報告建立的日期和時間。
- **報告名稱**—根據範本建立的報告名稱。
- **時期**—報告產生的時段。
- **伺服器**是規則所套用之具有 PCN 或 SCN 角色的伺服器名稱。

  如果您使用分散式解決方案和多組織用戶模式，則會顯示此欄。

- **建立者**—建立報告的使用者名稱。
- **狀態**—報告狀態（檔案是否可以下載）。

範本子部分顯示範本表。表包含以下資訊：

- **建立時間**—建立範本的日期和時間。
- **更新時間**—上次修改範本的日期和時間。
- **報告名稱**—範本的名稱。
- **建立者**—建立範本的使用者名稱。

建立範本

建立報告範本時，您需要指定要在報告中顯示的所有資訊：報告名稱，其描述，表格、圖表或映像的可用性。您也可以選擇要在報告中顯示的資料並定義報告元素的位置。

在介面的“**報告**”部分、“**產生的報告**”子部分中建立報告時，您只能選擇用於建立報告的範本和資料顯示週期。

為每個資料樣本建立了一個新的報告範本。

若要建立範本：

1. 在應用程式 Web 介面視窗中，選擇**報告**部分，**範本**索引標籤。

   這將開啟範本表。

2. 點擊**新增**。

   這將開啟範本建立視窗。此視窗在浮動視窗中包含報告主體和報告建構器。您可以將報告建構器移至Web 介面視窗的工作區。

3. 在視窗右上角的**範本名稱**欄位中，鍵入要指派給從此範本建立的報告的名稱。例如，**技術警示**。

   當在該範本中建立所有報告時，該名稱顯示在“**報告**”部分、“**產生的報告**”子部分的表中。

4. 代替**報告標題**文字，輸入建立報告後將在報告中顯示的報告名稱。如果您不想新增報告名稱，可以刪除**報告標題**文字並將此報告部分留空。

   您可以使用範本產生器中**文字**部分的按鈕來設定文字格式。

5. 代替**報告說明**文字，輸入建立報告後將在報告中顯示的報告描述。如果您不想新增報告描述，可以刪除**報告說明**文字並將此報告部分留空。

   您可以使用範本設計器中**文字**部分的按鈕來設定文字格式。

6. 使用報告建構器新增一個或多個報告元素：

- **表**。
- **餅狀圖**。
- **鏡像**。

7. 如果您選擇新增映像，**鏡像**視窗將會開啟。執行以下操作：

   a. 點擊**上傳**。

   b. 上傳圖像。例如，您可以上傳公司徽標。

   c. 在上傳按鈕右側的清單中，選擇報告頁面上圖像的對齊方式：**左邊**、**權限**或**中心**。

   d. 點擊**套用**。

8. 如果您選擇新增圓餅圖，**警示屬性餅圖**視窗將會開啟。執行以下操作：

   a. 在**名稱**欄位中，輸入餅圖的名稱。例如，**按技術排列的前 5 名警示**。您也可以將該欄位留空。

   b. 在**資料來源**清單中，選擇要為其建立餅圖的警示屬性。例如，**技術**。

   c. 在**片數**欄位中，指定圓餅圖的最大磁區數。

      建立報告時，應用程式會選擇最常遇到的資料。例如，如果您指定了5 個磁區並希望按技術建立餅圖，則應用程式將顯示產生警示數量最多的5 種技術的圓餅圖。產生較少警示的技術未包含在圖表中。

   d. 點擊**套用**。

9. 如果您選擇新增表格，**警示表**視窗將開啟。執行以下操作：

   a. 在**可用列**欄位中，雙擊以選擇要新增至報告表中的警示屬性。

      選定的屬性將會被移至**選定的列**欄位。您可以在**可用列**和**選定的列**欄位之間拖曳列名稱，並變更報告表中的列順序。

      例如，如果您將**技術**、**偵測到**和**建立時間**屬性移到**選定的列**欄位，已建立報告的表格將顯示產生警示的技術、偵測到的物件清單以及警示產生的時間。

   b. 如果您想按**狀態**屬性篩選警示，請選擇要在報告中顯示其資料的警示處理狀態旁的核取方塊。

   c. 如果您想按**技術**屬性篩選警示，請選擇要在報告中顯示其資料的應用程式模組和元件名稱旁的核取方塊。

   d. 如果您想按**重要級別**屬性篩選警示，請選擇要在報告中顯示其資料的警示重要性等級旁的核取方塊。

   e. 如果您想按**VIP 狀態**篩選警示，請在清單中選擇**VIP**。報告中僅顯示具有 VIP 身分的警示。

   f. 點擊**套用**。

10. 點擊視窗右上部的**儲存**按鈕。

一個新範本將被建立。

具有**安全稽核員**和**安全官**角色的使用者無法建立報告範本。

根據範本建立報告

若要基於範本建立報告：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。

2. 點擊**新增**。
   這將開啟**新報告**視窗。

3. 執行以下操作：

   a. 在**範本**下拉清單中，選擇以下範本之一以建立報告。

   b. 在**時期**下面，選擇以下選項之一：

      - **上一個小時**，如果您希望報告包含最近一小時內應用程式運行的資訊。
      - **最後一天**，如果您希望報告包含最後一天內應用程式運行的資訊。
      - **過去 7 天**，如果您希望報告包含最近一周內應用程式運行的資訊。
      - **過去 30 天**，如果您希望報告包含最近一月內系統運行的資訊。
      - **自訂**，如果您希望報告包含指定時段內系統運作的資訊。

4. 如果您已選擇**自訂**顯示時段以取得有關應用程式運行的資訊：

   a. 在開啟的日曆中，指定將產生報告的時段的開始和結束日期。

   b. 點擊**套用**。

5. 如果您使用分佈式解決方案和多組織用戶模式，請在**伺服器**設定群組中，選擇要將其資料包含在報告中的租用戶和伺服器旁的核取方塊。

6. 點擊**建立**。

建立的報告顯示在報告表中。您可以下載報告以便在電腦上檢視。

具有**安全官**角色的使用者無法建立報告範本。

檢視報告

要檢視報告：

1. 在程式 Web 介面視窗中，選擇“**報告**”部分，“**產生的報告**”子部分。
   這將開啟報告表。
2. 選擇要檢視的報告。

該報告將在瀏覽器的新分頁中開啟。

將報告下載到本機

若要將報告下載到您的電腦：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。
2. 在包含要檢視的報告的行中，點擊 圖示。
   報告以 HTML 格式儲存到本機電腦上您指定的資料夾。
   若要檢視報告，您可以使用任何允許您檢視 HTML 檔案的應用程式（例如瀏覽器）。

編輯範本

編輯範本：

1. 在應用程式 Web 介面視窗中，選擇**報告**區段、**範本**索引標籤。
2. 這將開啟範本表。選擇您想要編輯的範本。
   這將開啟範本編輯視窗。
3. 您可以編輯以下設定：
   - **範本名稱**是基於此範本建立所有報告時，顯示在**報告**區段、**產生的報告**子區段之表格中的報告名稱。
   - **報告標題**是建立報告後顯示在報告中的報告名稱。
     您可以使用範本產生器中**文字**區段的按鈕來設定文字格式。
   - **報告說明**是建立報告後顯示在報告中的報告描述。
     您可以使用範本產生器中**文字**部分的按鈕來設定文字格式。
   - **鏡像**。您可以上傳或刪除映像。

- **餅狀圖**。您可以變更以下餅圖設定：
  - **名稱**。
  - **資料來源**。
  - **片數**。

  點擊**套用**。
- **表**。您可以變更以下表設定：
  - **選定的列**。您可以在**可用列**和**選定的列**欄位之間拖曳列名稱，並變更報告表中的列順序。
  - **狀態**。
  - **技術**。
  - **重要級別**。
  - **VIP 狀態**。

4. 選擇以下方法之一來儲存範本：

- 如果您想將變更套用至目前範本，請點擊**儲存**按鈕。
  範本已修改。
- 如果要建立新範本，請輸入範本名稱，然後點擊**另存為**。

  > 新範本的名稱不能與已有範本的名稱相同。

  新範本將被儲存。

> 具有**安全稽核員**和**安全官**角色的使用者無法編輯範本。

按名稱篩選範本

若要按名稱篩選範本：

1. 在應用程式 Web 介面視窗中，選擇**報告**部分，**範本**索引標籤。
2. 這將開啟範本表。點擊**報告名稱**連結以開啟範本篩選功能表。
3. 在下拉清單中，選擇下列範本篩選運算子之一：
   - **包含**
   - **不包含**
4. 輸入範本名稱的一個或多個字元。

5. 如果您想為篩選器新增篩選條件，請點擊篩選運算子清單下的 + 按鈕並重複指定篩選條件的序列。

6. 點擊**套用**。

範本表將僅顯示與您設定的篩選條件相符的範本。

根據建立範本的使用者的名稱篩選範本

若要依照建立該範本的使用者的名稱篩選範本：

1. 在應用程式 Web 介面視窗中，選擇**報告**部分，**範本**索引標籤。

2. 這將開啟範本表。點擊**建立者**連結以開啟用於篩選範本的功能表。

3. 在下拉清單中，選擇下列範本篩選運算子之一：

   - **包含**

   - **不包含**

4. 輸入使用者名稱的一個或多個字元。

5. 如果您想為篩選器新增篩選條件，請點擊篩選運算子清單下的 + 按鈕並重複指定篩選條件的序列。

6. 點擊**套用**。

範本表將僅顯示與您設定的篩選條件相符的範本。

按建立時間篩選範本

若要按建立時間篩選報告範本：

1. 在應用程式 Web 介面視窗中，選擇**報告**部分，**範本**索引標籤。

2. 這將開啟範本表。點擊**建立時間**連結以開啟用於篩選範本的功能表。

3. 選擇以下範本顯示時段之一：

   - **所有**，如果您希望應用程式顯示表中建立的所有範本。

   - **上一個小時**，如果您希望應用程式顯示表中最後一小時建立的範本。

   - **最後一天**，如果您希望應用程式顯示表中最後一天建立的範本。

   - **自訂範圍**，如果您希望應用程式顯示表中在指定時段內建立的範本。

4. 如果您選擇了**自訂範圍**範本顯示時段：

   a. 這將開啟日曆；在日曆中，指定範本顯示期間的開始日期和結束日期。

   b. 點擊**套用**。

範本表將僅顯示與您設定的篩選條件相符的範本。

清除範本篩選器

若要清除一個或多個篩選條件的範本篩選器：

1. 在應用程式 Web 介面視窗中，選擇**報告**部分，**範本**索引標籤。
2. 這將開啟範本表。點擊要為其清除篩選條件的範本表列標題右側的。

> 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選器將會被清除。

範本表將僅顯示與您設定的篩選條件相符的範本。

刪除範本

若要刪除範本：

1. 在應用程式 Web 介面視窗中，選擇**報告**部分，**範本**索引標籤。
2. 這將開啟範本表。選擇包含您想要刪除的範本的行中的核取方塊。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

您選定的範本將會被刪除。

> 具有**安全稽核員**和**安全官**角色的使用者無法刪除範本。

按建立時間篩選報告

若要按建立時間篩選報告：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。
2. 點擊**建立時間**連結以開啟報告篩選功能表。
3. 選擇以下報告顯示時段之一：
   - **所有**，如果您希望應用程式顯示表中建立的所有報告。
   - **上一個小時**，如果您希望應用程式顯示表中最後一小時建立的報告。
   - **最後一天**，如果您希望應用程式顯示表中最後一天建立的報告。
   - **自訂範圍**，如果您希望應用程式顯示表中在指定時段內建立的報告。
4. 如果您選擇了**自訂範圍**報告顯示時段：
   a. 在開啟的日曆中，指定報告顯示時段的開始和結束日期。
   b. 點擊**套用**。

報告表將僅顯示與您設定的篩選條件相符的報告。

按名稱篩選報告

若要按名稱篩選報告：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。
2. 點擊**報告名稱**連結以開啟報告篩選功能表。
3. 在下拉清單中，選擇以下報告篩選運算子之一：
   - **包含**
   - **不包含**
4. 在文字方塊中輸入報告名稱的一個或多個字元。
5. 如果您想為篩選器新增篩選條件，請點擊篩選運算子清單下的 + 按鈕並重複指定篩選條件的序列。
6. 點擊**套用**。

報告表將僅顯示與您設定的篩選條件相符的報告。

以具有 Central Node 元件的伺服器名稱篩選報告

若要按具有 Central Node 元件的伺服器名稱篩選報告：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。
2. 點擊**伺服器**連結以開啟報告篩選功能表。
3. 選擇要用於篩選報告的伺服器對面的核取方塊。
4. 點擊**套用**。

報告表將僅顯示與您設定的篩選條件相符的報告。

根據建立報告的使用者的名稱篩選報告

若要依照建立該報告的使用者的名稱篩選報告：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。
2. 點擊**建立者**連結以開啟報告篩選功能表。
3. 在下拉清單中，選擇以下報告篩選運算子之一：
   - **包含**
   - **不包含**
4. 輸入使用者名稱的一個或多個字元。
5. 如果您想為篩選器新增篩選條件，請點擊篩選運算子清單下的 + 按鈕並重複指定篩選條件的序列。

報告表將僅顯示與您設定的篩選條件相符的報告。

清除報告篩選器

若要清除一個或多個篩選條件的報告篩選器：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。

2. 點擊要為其清除篩選條件的報告表列標題右側的 ⊠。

> 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選器將會被清除。

報告表將僅顯示與您設定的篩選條件相符的報告。

刪除報告

若要刪除應用程式操作報告：

1. 在程式 Web 介面視窗中，選擇**報告**部分、**產生的報告**子部分。
   這將開啟報告表。
2. 選擇包含您想要刪除的報告的行中的核取方塊。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

選定的報告將被刪除。

> 具有**安全稽核員**和**安全官**角色的使用者無法刪除報告。

管理 NDR 報告

您可以使用 Kaspersky Anti Targeted Attack Platform 來取得包含應用程式儲存的各種資訊的報告。Kaspersky Anti Targeted Attack Platform 以 PDF 檔案形式產生報告。應用程式可以將報告檔案傳送至電子郵件信箱。

您可以在“**報告**”區段的“**報告 (NDR)**”子區段中，透過“**產生的報告**”索引標籤檢視產生之報告的相關資訊並將其匯出至檔案。

可能有以下類型的 NDR 報告範本：

- 系統範本，在應用程式安裝期間自動建立。在報告範本表中，系統範本顯示為圖示。您無法刪除系統範本。
  Kaspersky Anti Targeted Attack Platform 支援以下系統報告範本：
  - 清查報告。
    包含有關裝置、系統命令的資訊，以及裝置上使用的協定和偵測到的風險。
  - 系統安全報告。
    包含有關裝置的安全狀態、註冊的事件、偵測到的風險以及與外部網路上的裝置互動的資訊。

- 執行摘要。

  包含有關裝置和系統安全狀態的簡要資訊。

- 完整報告。

  包含有關裝置和系統安全狀態的完整資訊。

- 自訂範本，透過複製範本手動建立。您可以複製系統或自訂範本。只有具有高級安全官角色的使用者才能複製報告範本。

報告中的資訊以單獨的資訊區塊呈現。每份 Kaspersky Anti Targeted Attack Platform 報告均包含一組固定的資訊區塊，這些資訊區塊按固定順序排列。報告中使用的資訊區塊及其描述如下表所列。

在報告中使用資訊區塊

資訊塊的名稱	清查報告	系統安全報告	執行摘要	完整報告
裝置類別	✓	—	✓	✓
裝置供應商	✓	—	✓	✓
裝置作業系統	✓	—	✓	✓
擁有最多風險的裝置。	✓	✓	—	✓
態勢感知	—	✓	✓	✓
網路中的新裝置	✓	—	—	✓
流量最大的協議	✓	—	—	✓
與其他節點連接最多的裝置	✓	—	—	✓
網路流量	✓	—	✓	✓
通用協定	✓	—	✓	✓
裝置安全狀態	—	✓	✓	✓
按狀態劃分的裝置分佈	—	✓	—	✓
事件統計	—	✓	—	✓
依偵測技術分佈的事件	—	✓	—	✓
發生事件最多的裝置	—	✓	—	✓
最關鍵的事件	—	✓	—	✓
最常觸發的惡意活動偵測規則	—	✓	—	✓
有存取公用資源標誌的裝置	—	✓	—	✓
透過遠端控制協定的連線	—	✓	—	✓
活動風險	—	✓	✓	✓

檢視 NDR 報告範本表

您可以在應用程式的 Web 介面中檢視報告範本表，在“**報告**”部分、“**報告 (NDR)**”子部分的“**報告範本**”索引標籤上。

報告範本設定顯示在表格以下列中：

- **名稱**。

  報告範本名稱。圖示顯示在系統報告範本名稱旁邊。

- **排程**。

  有關 Kaspersky Anti Targeted Attack Platform 基於範本自動產生報告所使用的時間表的資訊。如果具有“**資深安全員**”角色的使用者在報告範本中配置了計劃則顯示計劃資訊。如果未配置排程，則該列顯示“**已停用**”。

- **類型/用途**。

  上次修改報告範本的使用者的姓名。對於具有預設設定的系統範本，會顯示“**系統**”。

- **最後報告**。

  上次根據報告範本產生報告的時間。

- **目的地**。

  表示已設定電子郵件報告收件者的圖示。以下圖示具有以下含義：

  - – 定義了報告接收者。
  - – 未定義報告接收者。

檢視 NDR 報告範本詳細資訊

若要檢視報告範本資訊：

在“**報告**”部分、“**報告 (NDR)**”子部分的“**報告範本**”索引標籤上，選擇相關範本。

詳細資訊區域顯示在 Web 介面視窗的右側。詳細資訊區域顯示所有指定的詳細資訊。

報告範本的詳細資訊包括以下欄位：

- **名稱**是報告範本的名稱。
- **類型/使用者**是最後修改報告範本的使用者的名稱。對於具有預設設定的系統範本，會顯示“**系統**”。
- **期限**是 Kaspersky Anti Targeted Attack Platform 根據範本產生的報告涵蓋的時間段。
- **修改時間**是範本最近一次變更的時間。
- **上次報告**是根據範本產生上次報告的時間。
- **下次開始（當地時間）**是根據範本開始產生下一個報告的時間。如果為報告範本配置了計劃，則會顯示此設定。
- **排程**顯示有關 Kaspersky Anti Targeted Attack Platform 用於根據範本自動產生報告的排程的資訊。如果為報告範本配置了計劃，則會顯示此設定。

收件者位址是 Kaspersky Anti Targeted Attack Platform 向其傳送產生的報告的電子郵件信箱。如果為報告範本配置了收件者位址，則會顯示此設定。

檢視 NDR 報告表

您可以在應用程式的 Web 介面中檢視報告表，在“**報告**”部分、“**報告 (NDR)**”子部分、“**產生的報告**”索引標籤上。

報告設定顯示在表格以下列中：

- **ID**。
  報告的唯一 ID。
- **報告名稱**。
  產生的報告的名稱。
- **範本名稱**。
  用於產生報告的範本的名稱。
- **開始**。
  報告產生開始的日期和時間。
- **狀態**。
  報告狀態。報告可以具有以下狀態之一：
  待處理。該報告正在排隊等待產生。當同時產生多個報告時，報告可能處於*待處理*狀態。
  進行中。報告正在產生。
  錯誤。產生報告時出現錯誤。
  完成。報告已成功產生。
  正在取消。正在取消報告產生。
  已取消。報告產生已取消。
- **使用者**。
  啟動報告產生或配置基於範本運行報告的排程的使用者的名稱。
- **運行類型**。
  報告產生類型：手動或排程。
- **已完成**。
  報告產生結束的日期和時間。

根據範本手動產生 NDR 報告

您可以根據範本手動開始產生報告。

要開始產生報告：

1. 選擇“**報告**”部分，然後“**報告 (NDR)**”子部份。
2. 在“**報告範本**”頁簽，選擇要用於產生報告的一個或多個範本。
   當選擇多個範本時，應用程式將同時根據這些範本產生報告。您最多可以選擇 10 個範本。

3. 在報告範本表上方的工具列中，點擊“**取得報告**”。

   Kaspersky Anti Targeted Attack Platform 開始產生報告。

   您將被帶到“**產生的報告**”頁簽，顯示正在產生的報告的狀態。報告產生後，Kaspersky Anti Targeted Attack Platform 會將 PDF 格式的報告檔案傳送至報告範本中指定的電子郵件信箱。如果報告範本中未定義電子郵件信箱，您可以在“**產生的報告**”頁簽上單獨手動將產生的報告匯出到檔案。報告檔案的最大大小為 10 MB。

如果有必要，您可以取消報告的產生。

複製 NDR 報告範本

您可以透過複製現有的報告範本來建立自訂範本。您可以複製系統範本或自訂範本。複製範本時，您無法選擇要在報告中包含哪些資訊區塊或重新排列它們。

應用程式中的最大範本數量為5000 個。

若要複製報告範本：

1. 選擇“**報告**”部分，然後“**報告 (NDR)**”子部份。

2. 在“**報告範本**”索引標籤，選擇相關範本。

   詳細資訊區域顯示在 Web 介面視窗的右側。

3. 點擊“**建立新範本**”。

4. 在“**名稱**”欄位中，編輯報告範本的名稱。

   您可以使用拉丁字母和西里爾字母、數字、空格字元以及-、–、_ 字元。

   報告範本的名稱必須符合以下要求：

   - 不要重複使用另一個報告範本的名稱（不區分大小寫）。
   - 最多包含 100 個字元。

   從更新後的範本產生的報告的名稱將反映範本的新名稱。

5. 在“**資料週期**”下拉清單中，選擇您想要在報告中取得系統資訊的時間段。

   您可以使用應用程式在過去 24 小時、7 天、30 天、去年或手動配置的時間範圍內收到的資訊產生報告。

6. 如果需要按排程產生報告，請開啟“**按排程產生報告**”切換開關並設定排程：

   a. 在“**頻率**”下拉清單中，選擇產生報告的頻率：**每小時**、**每天**、**每週**或**每月**。

   b. 根據所選的選項，指定設定值以最佳化報告產生開始時間。

7. 如有必要，請使用“**收件者位址**”欄位輸入您要將產生的報告傳送到的電子郵件地址。如果需要指定報告的其他收件人，請點擊“**新增收件人位址**”並輸入電子郵件信箱。

   報告收件者的最大數量為 20。

8. 點擊**儲存**。

新報告將會新增到報告範本表中。

編輯 NDR 報告範本

若要編輯報告範本的設定：

1. 選擇“**報告**”部分，然後“**報告 (NDR)**”子部份。
2. 在“**報告範本**”索引標籤，選擇相關範本。
   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊“**編輯**”。
4. 在“**名稱**”欄位中，編輯報告範本的名稱。
   您可以使用拉丁字母和西里爾字母、數字、空格字元以及-、–、_ 字元。
   報告範本的名稱必須符合以下要求：
   - 不要重複使用另一個報告範本的名稱（不區分大小寫）。
   - 最多包含 100 個字元。

   從更新後的範本產生的報告的名稱將反映範本的新名稱。
5. 在“**資料週期**”下拉清單中，選擇您想要在報告中取得系統資訊的時間段。
   您可以使用應用程式在過去 24 小時、7 天、30 天、去年或手動配置的時間範圍內收到的資訊產生報告。
6. 如果需要按排程產生報告，請開啟“**按排程產生報告**”切換開關並設定排程：
   a. 在“**頻率**”下拉清單中，選擇產生報告的頻率：**每小時**、**每天**、**每週**或**每月**。
   b. 根據所選的選項，指定設定值以最佳化報告產生開始時間。
7. 如有必要，請使用“**收件者位址**”欄位輸入您要將產生的報告傳送到的電子郵件地址。如果需要指定報告的其他收件人，請點擊“**新增收件人位址**”並輸入電子郵件信箱。
   報告收件者的最大數量為 20。
8. 點擊**儲存**。

變更將顯示在報告範本表的相應列中。

將 NDR 報告匯出到檔案

您可以將產生的報告匯出為 PDF 檔案。

要將報告匯出到檔案：

1. 在**報告**區段中，選擇**報告 (NDR)**子區段。
2. 在**產生的報告**索引標籤上，選擇相關報告。
   這些報告會依照目前伺服器連線工作階段中最後啟動的報告的 ID 進行篩選。若要顯示所有產生的報告，請點擊**預設篩選器**重設篩選器設定。如果有必要，您可以按您選擇的時間段配置篩選。

詳細資訊區域顯示在 Web 介面視窗的右側。

3. 點擊**匯出**。

瀏覽器儲存報告檔案。預設情況下，報告檔案的名稱採用 <報告名稱>_<產生報告的日期和時間> 格式。根據您的瀏覽器的設定，螢幕上可能會顯示一個視窗，您可以在其中指定下載檔案的路徑和名稱。

刪除 NDR 報告範本

只能刪除自訂報告範本。

若要刪除報告範本：

1. 選擇“**報告**”部分，然後“**報告 (NDR)**”子部份。
2. 在“**報告範本**”索引標籤上，選擇一個或多個要刪除的報告範本。
3. 點擊**刪除**。

   系統範本不能被刪除。在報告範本表中，系統範本顯示為圖示。
4. 在顯示的提示視窗中，確認刪除報告範本。

刪除 NDR 報告

若要刪除報告：

1. 選擇“**報告**”部分，然後“**報告 (NDR)**”子部份。
2. 在“**產生的報告**”頁簽上，選擇一個或多個要刪除的報告。

   報告表中的報告會依照目前伺服器連線工作階段中最後啟動的報告的 ID 進行篩選。若要顯示所有產生的報告，請點擊**預設篩選器**重設篩選器設定。如果有必要，您可以按您選擇的時間段配置篩選。

   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊**刪除**。
4. 在顯示的提示視窗中，確認刪除報告。

取消 NDR 報告產生

您只能取消處於“**進行中**”狀態的報告的產生。

若要取消報告產生：

1. 選擇“**報告**”部分，然後“**報告 (NDR)**”子部份。
2. 在“**產生的報告**”索引標籤上，選擇要取消的、狀態為“**進行中**”的報告。
   詳細資訊區域顯示在 Web 介面視窗的右側。
3. 點擊“**取消**”。
4. 在彈出的提示視窗中，確認取消報告。

此請求完成後，報告狀態變更為“**已取消**”。

管理儲存報告檔案的設定

您可以變更儲存的報告檔案的最大總大小限制。

若要編輯報告檔案儲存設定：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**Sensor 伺服器**”部分。
3. 選擇本機主機（IP 位址 0.0.0.0）的卡。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊“**編輯**”。
   在詳細資料區域，會顯示頁簽，您可以在其中管理伺服器的設定。
5. 在“**一般**”索引標籤上的“**報告**”下，使用“**最大磁碟區**”設定為儲存的報告檔案設定大小限制。
   您可以選擇大小限制的計量單位：**MB**或**GB**。
   編輯值時，還需要考慮到所有大小限制的總和不得超過節點指定的最大儲存容量。
6. 如有必要，請使用“**儲存時間（天）**”設定來限制報告檔案的儲存時間，並以天為單位指定時間。
7. 點擊**儲存**。

管理將 VIP 身分指派給警示的規則

具有**資深安全員**角色的使用者可以建立、刪除、修改、匯入和匯出用於向警示分配 VIP 身分的規則清單。

您可以建立以下類型的規則：

- **IP**。VIP 身分將指派給與電腦的此 IP 位址關聯的新警示。
- **主機名稱**。VIP 身分將指派給與該主機名稱關聯的新警示。
- **電子郵件信箱**。VIP 身分將指派給與此電子郵件信箱關聯的新警示。

具有**安全稽核員**角色的使用者可以檢視和匯出用於將 VIP 身分指派給警示的規則清單。

具有**安全官**角色的使用者無法檢視為警示指派 VIP 身分的規則清單。

檢視 VIP 身分分配規則表

用於指派 VIP 身分的規則表位於應用程式 Web 介面的**設定**部分，**VIP 狀態**子部分。

表包含以下資訊：

- **標準** — 將條目新增至規則清單的條件。
- **值** — 條件的值。
- **敘述** — 建立規則時指定的附加資訊。

建立 VIP 身分分配規則

若要新增用於將 VIP 身分指派給警示的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 在應用程式 Web 介面視窗的右上角，點擊**新增**。
   這將開啟新增規則的視窗。
3. 在**標準**下拉清單中，選擇下列規則類型之一：
   - **IP**，如果您想為電腦 IP 位址新增規則。
   - **主機**，如果您想要新增主機名稱規則。
   - **電子郵件信箱**，如果您想為電子郵件信箱新增規則。
4. **值**欄位中輸入必要的值。
   例如，如果在**標準**下面您選擇了**電子郵件信箱**，請在**值**欄位中輸入您要新增的電子郵件信箱。
5. 在**敘述**欄位中，根據需要輸入其他資訊。
6. 點擊**新增**。

規則已新增。VIP 身分將被指派給與新增的 IP 位址、主機名稱或電子郵件信箱關聯的新警示。

具有**安全稽核員**角色的使用者無法建立 VIP 身分分配規則。

具有**安全官**角色的使用者無法檢視為警示指派 VIP 身分的規則清單。

刪除 VIP 身分分配規則

若要刪除為警示指派 VIP 身分的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 選擇您想要從清單中移除的每條規則左側的核取方塊。
3. 如果您想要刪除所有規則，請選擇清單上方的核取方塊。
4. 在應用程式 Web 介面視窗的右上角，點擊**刪除**。
   操作確認視窗將顯示。
5. 點擊**是**。

所選檔案將被刪除。

具有**安全稽核員**角色的使用者無法刪除 VIP 身分分配規則。

具有**安全官**角色的使用者無法檢視為警示指派 VIP 身分的規則清單。

修改 VIP 身分分配規則

若要修改為警示指派 VIP 身分的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 選擇要修改的規則。
   這將開啟規則編輯視窗。
3. 對**標準**、**值**和**敘述**欄位進行必要的變更。
4. 點擊**儲存**。

規則已修改。

具有**安全稽核員**角色的使用者無法修改 VIP 身分分配規則。

具有**安全官**角色的使用者無法檢視為警示指派 VIP 身分的規則清單。

匯入 VIP 身分分配規則清單

若要匯入用於向警示指派 VIP 身分的規則清單：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 點擊**匯入**。
   系統將提示您確認清單匯入。

   匯入的用於將 VIP 身分指派給警示的規則清單將替代目前的 VIP 身分警示指派規則清單。

3. 點擊**是**。
   這將開啟檔案選擇視窗。
4. 選擇包含要匯入的規則清單的 JSON 檔案，然後點擊**開啟**。
   這將關閉檔案選擇視窗。

清單已匯入。

匯出從掃描中排除的資料清單

若要匯出掃描排除項清單：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 在應用程式 Web 介面視窗的右上角，點擊**匯出**。

包含匯出的掃描排除項目清單的 JSON 檔案被儲存在電腦上的瀏覽器下載資料夾中。

按 VIP 身分指派規則類型篩選和搜尋

若要依規則類型篩選或搜尋 VIP 身分指派規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 點擊**標準**連結以開啟篩選配置視窗。

3. 選擇規則類型旁邊的一個或多個核取方塊：

   - **IP**。
   - **主機**。
   - **電子郵件信箱**。

4. 點擊**套用**。

   篩選配置視窗關閉。

   表將僅顯示與您設定的篩選條件相符的規則。

> 您可以同時使用多個篩選器。

按 VIP 身分規則的值篩選和搜尋

若要依規則值篩選或搜尋 VIP 身分指派規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 點擊**值**連結以開啟篩選配置視窗。
3. 輸入規則值的一個或多個字元。
4. 點擊**套用**。

   篩選配置視窗關閉。

   表將僅顯示與您設定的篩選條件相符的規則。

> 您可以同時使用多個篩選器。

按 VIP 身分分配規則描述篩選和搜尋

若要依描述篩選或搜尋 VIP 身分指派規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。
2. 點擊**敘述**連結以開啟篩選配置視窗。

3. 輸入描述的一個或多個字元。

4. 點擊**套用**。

   篩選配置視窗關閉。

   表將僅顯示與您設定的篩選條件相符的規則。

您可以同時使用多個篩選器。

清除 VIP 身分分配規則篩選器

若要清除一個或多個篩選條件的 VIP 身分指派規則篩選器：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**索引標籤，**VIP 狀態**部分。

2. 點擊您想要清除其篩選條件的表列標題右側的 ☒。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   表將僅顯示與您設定的篩選條件相符的規則。

管理 NDR 事件的允許規則

Kaspersky Anti Targeted Attack Platform 可以監控裝置之間的網路互動。*允許規則*用於配置已授權和未授權的網路互動。所有符合活動允許規則的網路互動都被視為允許。當偵測到允許的互動時，應用程式不會記錄 NDR 事件或產生警示。

您可以檢視、建立、複製、修改、刪除、啟用或停用允許規則。

檢視允許規則表格

若要檢視允許規則表：

1. 在應用程式 Web 介面視窗中，選擇"**設定**"區域。

2. 轉到"**允許規則**"索引標籤。

   允許規則表將顯示。

表包含以下資訊：

- **規則 ID** 是該規則的唯一識別碼。
- **狀態**（◐ 圖示）表示規則的目前狀態（*已啟用*或*已停用*）。
- **規則類型**：對於停用事件註冊的規則，指定 EVT 類型。
- **協定/命令**定義了一組協定。
- **面 1**是網路互動一端的裝置名稱 / 位址資訊。您可以使用下列設定啟用或停用位址資訊中位址和連接埠的顯示：**MAC 位址**、**IP 位址**和**連接埠號**。如果在應用程式中新增了其他位址空間，您可以使用下列設定啟用或停用位址空間名稱的顯示：
  - **MAC 位址的 AS**：包含規則中的 MAC 位址的位址空間。只有當位址空間具有位址空間規則，且**資料鏈 (L2)**被選為 OSI 層時，此設定才能包含位址空間的名稱。
  - **IP 位址的 AS**：包含規則中的 IP 位址的位址空間。只有當位址空間具有位址空間規則，且**網路 (L3)**被選為 OSI 層時，此設定才能包含位址空間的名稱。
- **面 1**是網路互動另一端的裝置名稱 / 位址資訊。位址資訊的顯示可以按照與**面 1**列相同的方式配置。
- **評論**可讓您提供有關規則的其他資訊。
- **建立日期**是規則建立的日期和時間。
- **變更日期**是規則最後修改的日期和時間。
- **監控點**是事件中要指定的監控點的名稱。
- **事件類型**是事件類型的 ID 和標題。
- **源**提供有關規則來源的資訊。
- **系統 IDS 規則的 SID**是系統 IDS 規則的 ID。如果在建立允許規則時未指定 ID，則會顯示*所有規則*。

使用空白設定或範本中的設定建立允許規則

若要使用空白設定或範本中的設定建立允許規則：

1. 在應用程式 Web 介面視窗中，選擇**設定**區域。
2. 前往**允許規則**索引標籤。
3. 點擊**新增規則**。
4. 如果要使用範本中的設定，請在詳細資料區域中點擊**使用範本**，在開啟的視窗中選擇所需的範本，然後點擊**套用**。
5. 在**協定**欄位中，指定用於裝置之間互動的協定。

   選擇**協定**欄位將開啟視窗，其中以協定堆疊樹的形式顯示支援的協定表。您可以使用包含下一層協定的協定名稱旁邊的**+**和**-**按鈕來控制樹節點的顯示。

   如有必要，請使用表格上方的搜尋欄來尋找所需的協議。

要指定協定：

a. 在協定表中，選擇要為規則指定的協定。若要選擇協議，請點擊協議表左列中的按鈕。

b. 點擊**確定**。

如果您選擇應用程式可透過網路封包內容偵測到的協定，則會在**協定**欄位下方顯示對應的警告。

6. 如果必要，請在**註釋**欄位中輸入有關該規則的其他資訊。

7. 在**面 1**和**面 2**下，指定網路互動各方的可編輯位址資訊。根據所選的協定（或協定集），位址資訊可能包含 MAC 位址、IP 位址和/或連接埠號。如果已將其他位址空間新增至應用程式，您可以為位址指定位址空間的名稱。

   為了自動填寫網路互動端的位址資訊，您可以選擇應用程式已知的裝置。為此：

   a. 點擊**指定裝置位址**，開啟裝置選擇視窗。

   b. 在裝置選擇視窗中，選取要使用的裝置旁的核取方塊。

      裝置選擇視窗包含一個表格，您可以在其中設定欄的佈局和順序，也可以進行篩選、搜尋和排序，方式類似於**資產**區段中的裝置表格。

   c. 在裝置選擇視窗中點擊**確定**。

8. 在**事件類型**欄位中，指定事件中會指示其數值代碼的事件類型。

   選擇**事件類型**欄位會開啟一個視窗，其中包含可在允許規則中指定的事件類型清單。如有必要，請使用清單上方的搜尋欄來尋找所需的事件類型。若要指定事件類型，請在清單中選擇它並點擊**套用**。

9. 在**監控點**欄位中，指定事件中指示的監控點名稱。

   選擇**監控點**欄位會開啟一個視窗，其中包含已安裝應用程式元件的所有節點上的所有監控點清單。如有必要，請使用清單上方的搜尋欄來尋找所需的監控點名稱。若要指定監控點名稱，請在清單中選擇它並點擊**套用**。

10. 如果您不希望應用程式使用選定的系統 IDS 規則，掃描符合此允許規則條件的網路連線，請在**系統 IDS 規則的 SID**欄位中指定此規則的 ID。您可以在 IDS 警示的詳細資訊中檢視系統 IDS 規則的 SID。

    如果未指定 SID，應用程式將停用所有系統 IDS 規則對符合此允許規則的條件的網路互動的掃描。

11. 在詳細資料區域中，點擊**儲存**。

此規則被新增到允許規則表中。

從已註冊事件建立允許規則

若要從已註冊事件建立允許規則：

1. 在**網路流量事件**部分的事件表中，選擇您要基於其建立事件允許規則的事件。

2. 在詳細資料區域中，點擊**建立允許規則**。

   這將在瀏覽器視窗中開啟**允許規則**部分。在 Web 介面視窗的右側，規則設定編輯模式中顯示詳細資訊區域。新規則的設定使用已儲存的事件詳細資料中的值進行初始化。

3. 如有必要，編輯新規則的設定。為此，請按照建立最初為空白的設定的規則的步驟 4 至 12 進行操作。如果不需要編輯新規則的設定，請點擊**儲存**以儲存該規則。

根據已註冊的事件建立允許規則。

複製允許規則

若要從現有互動控制規則建立互動控制規則：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”區域。

2. 轉到“**允許規則**”索引標籤。

3. 選擇新規則所基於的規則。

4. 右鍵點擊以開啟上下文功能表。

5. 在右鍵功能表中，選擇**複製規則**。

   在 Web 介面視窗的右側，規則設定編輯模式中顯示詳細資訊區域。新規則的設定使用已儲存的事件設定的值進行初始化。

6. 根據需要編輯設定。為此，請按照建立規則的過程中所述的步驟 4–12 進行操作。

允許規則被複製。

編輯允許規則的設定

您可以編輯已啟用的允許規則的設定。停用的規則不可編輯。

若要編輯允許規則的設定：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”區域。

2. 轉到“**允許規則**”索引標籤。

3. 選擇要編輯其設定的規則。

   詳細資訊區域顯示在 Web 介面視窗的右側。

4. 點擊**編輯**。

5. 根據需要編輯設定。為此，請按照建立規則的過程中所述的步驟 4 至 12 進行操作。

6. 點擊**儲存**。

   角色設定已修改。

啟用或停用允許規則

允許規則可以處於“*已啟用*”或“*已停用*”狀態。預設情況下，規則在建立後處於啟用狀態。

若要變更允許規則的狀態：

1. 在應用程式 Web 介面視窗中，選擇“**設定**”區域。

2. 轉到“**允許規則**”索引標籤。

3. 在規則表中，選擇要變更其狀態的規則。

4. 點擊“**啟用**”或“**停用**”，以啟用或停用規則。每個按鈕都顯示所選的規則，其中包括可套用對應動作的規則。

   所選規則的狀態已改變。

刪除允許規則

您可以選擇性地刪除一個或更多允許規則。

要刪除允許規則:

1. 在應用程式 Web 介面視窗中，選擇“**設定**”區域。

2. 轉到“**允許規則**”索引標籤。

3. 在規則表中，選擇要刪除的允許規則。

4. 點擊**刪除**。

   這將開啟一個確認提示視窗。根據所選規則的狀態，提示提供以下選項：

   - 如果所有選取的規則都已啟用，應用程式會提示您刪除選取的規則、停用它們或取消操作。如果選擇了所有符合目前篩選和搜尋條件的規則，且選定規則的數量超過 1000 條，則不會檢查此條件。

   - 如果選定的規則包含已停用的規則或選擇了所有符合目前篩選和搜尋條件的規則，且選定的規則數量超過 1000 條，應用程式將提示您刪除選定的規則或取消操作。

5. 在提示視窗中，確認刪除規則。

   所選檔案將被刪除。

管理掃描排除項目清單

具有**資深安全員**角色的使用者可以建立、匯入和匯出*掃描排除項目*清單，即 Kaspersky Anti Targeted Attack Platform 視為安全且不會顯示在警示表中的資料清單。您可以為以下資料建立掃描排除規則：

- **MD5**。
- **格式**。
- **URL 遮罩**。
- **電子郵件收件者**。
- **電子郵件寄件者**。
- **來源 IP 或子網路**。
- **目標 IP 或子網路**。
- **使用者代理**。

具有**安全稽核員**和**安全官**角色的使用者可以檢視掃描排除規則清單，也可以將其匯出。

檢視從掃描中排除的資料表

若要檢視包含從掃描中排除的資料的表：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。

   這將開啟一個表格，其中包含 Kaspersky Anti Targeted Attack Platform 將視為安全且不會為其建立警示的資料清單。您可以透過點擊列標題中的連結來篩選規則。

表包含以下資訊：

- **標準** — 將條目新增至允許物件清單的條件。
- **值** — 條件的值。

新增掃描排除規則

若要新增至掃描排除項目：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 在應用程式 Web 介面視窗的右上角，點擊**新增**。
   這將開啟**新規則**視窗。
4. 在**標準**下拉清單中，選擇下列條件之一，將規則新增至掃描排除項目清單：
   - **MD5**。
   - **格式**。
   - **URL 遮罩**。
   - **電子郵件收件者**。
   - **電子郵件寄件者**。
   - **來源 IP 或子網路**。
   - **目標 IP 或子網路**。
   - **使用者代理**。
5. 如果選擇了**格式**，則從**值**下拉清單中選擇要新增的檔案格式。
   例如，您可以選擇 **MSOfficeDoc** 格式。
6. 如果您選擇了**MD5**、**URL 遮罩**、**電子郵件收件者**、**電子郵件寄件者**、**來源 IP 或子網路**、**目標 IP 或子網路**或者**使用者代理**，請在**值**欄位中輸入要新增至掃描排除項目清單的相關條件的值：
   - 如果您選擇了**MD5**，請在**值**欄位中輸入檔案的 MD5 雜湊值。
   - 如果您選擇了**URL 遮罩**，請在**值**欄位中輸入 URL 遮罩。
     您可以在遮罩中使用以下特殊字元：
     * – 任何字元序列。

     範例：
     如果您輸入 `*abc*` 作為遮罩，應用程式會將包含序列 `abc` 的任何 URL 視為安全。例如，`www.example.com/download_virusabc`

     ? – 符合任意單一字元。

     範例：
     如果您輸入 `example_123?.com` 作為遮罩，應用程式會將包含給定字元序列以及任何 `3` 之後的字元的 URL 視為安全。例如，`example_1234.com`

     如果 * 或 ? 字元是要新增至掃描排除項目清單中的完整 URL 的一部分，請在輸入 URL 時使用 \ 字元來轉義單個 * 、 ? 或其後的\字元。

範例：
您需要新增以下 URL 作為受信任位址：`www.example.com/download_virus/virus.dll?virus_name=`
您不想應用程式將 ? 作為特殊遮罩字元處理，因此您可以在 ? 之前新增 \ 字元。
新增至掃描排除項目清單的 URL 如下所示：`www.example.com/download_virus/virus.dll\?virus_name=`

- 如果您選擇了**電子郵件收件者**或者**電子郵件寄件者**，請在**值**欄位中輸入電子郵件信箱。
- 如果您選擇了**使用者代理**，請在**值**欄位中輸入包含瀏覽器資訊的**HTTP 請求的使用者代理程式標頭**。
- 如果您選擇了**來源 IP 或子網路**或者**目標 IP 或子網路**，請在**值**欄位中輸入位址或子網路（例如 255.255.255.0）。

在**URL 遮罩**、**電子郵件收件者**和**電子郵件寄件者**欄位中，您可以輸入包含西里爾字元的網域名稱。在這種情況下，位址將轉換為 Punycode 並根據應用程式設定進行處理。

7. 點擊**新增**。

此規則將會被新增到掃描排除項清單中。

具有**安全稽核員**和**安全官**角色的使用者無法新增掃描排除規則。

刪除掃描排除規則

若要從掃描排除項目中刪除一條或多條規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 選擇您想要從掃描排除項目清單中移除的每個規則左側的核取方塊。
   如果您想要刪除所有規則，請選擇清單上方的核取方塊。
4. 在視窗的下部，點擊**刪除**。
   操作確認視窗將顯示。
5. 點擊**是**。

選定的規則將會從掃描排除項目清單中刪除。

具有**安全稽核員**和**安全官**角色的使用者無法從掃描排除項目清單中刪除條目。

編輯新增到掃描排除項目的規則

若要編輯掃描排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 選擇要修改的規則。
   這會開啟**編輯規則**視窗。
4. 對**標準**和**值**欄位進行必要的變更。
5. 點擊**儲存**。

規則已修改。

具有**安全稽核員**和**安全官**角色的使用者無法編輯掃描排除項目清單中的規則。

匯出從掃描中排除的資料清單

若要匯出掃描排除項清單：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 在應用程式 Web 介面視窗的右上角，點擊**匯出**。

包含匯出的掃描排除項目清單的 JSON 檔案被儲存在電腦上的瀏覽器下載資料夾中。

依條件篩選掃描排除項目清單中的規則

若要依規則類型篩選掃描排除項目清單條目：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 點擊**標準**連結以開啟篩選配置視窗。

4. 選擇您要根據其篩選規則的條件旁邊的一個或多個核取方塊：

- **MD5**。
- **格式**。
- **URL 遮罩**。
- **電子郵件收件者**。
- **電子郵件寄件者**。
- **來源 IP 或子網路**。
- **目標 IP 或子網路**。
- **使用者代理**。

5. 點擊**套用**。

   篩選配置視窗關閉。

   掃描排除項目清單僅顯示符合您條件的規則。

> 您可以同時使用多個篩選器。

按值搜尋掃描排除項目清單中的規則

若要按值搜尋掃描排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 點擊**值**連結以開啟篩選配置視窗。
4. 輸入值字元。
5. 點擊**套用**。

   掃描排除項目清單僅顯示符合您條件的規則。

> 您可以同時使用多個篩選器。

重設掃描排除項目清單中的規則篩選器

若要依一個或多個篩選條件清除排除項清單記錄篩選器：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**掃描**索引標籤。
3. 點擊要為其清除篩選條件的掃描排除項目清單條目表中列標題右側的 ✕。

   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

   選定篩選器將會被清除。

   掃描排除項目清單僅顯示符合您條件的規則。

管理入侵偵測規則排除項目

具有**資深安全員**角色的使用者可以新增卡巴斯基入侵偵測規則來掃描排除項目。Kaspersky Anti Targeted Attack Platform 在透過排除的入侵偵測規則進行掃描時不會建立警示。然而，應用程式繼續使用*入侵偵測*(IDS)技術註冊 NDR 事件。

如果您想要建立精確的排除項目，例如，如果您不希望應用程式為特定來源位址註冊 NDR 事件或產生此類事件的警示，則需要新增允許規則。

您只能排除卡巴斯基入侵偵測規則。如果您不想在掃描時套用使用者定義的入侵偵測規則，可以停用或刪除該規則。

具有“安全稽核員”角色的使用者可以檢視新增到排除項目的入侵規則清單，並檢視所選規則的屬性。

具有“安全官”角色的使用者無法檢視新增至排除項目的入侵規則清單。

檢視新增至排除項目的入侵偵測規則表

若要檢視已新增至排除項目的入侵偵測規則表：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 前往**IDS**索引標籤。

   被排除的 IDS 規則表將會顯示。您可以透過點擊列標題中的連結來篩選規則。

表包含以下資訊：

- **建立時間** — 入侵偵測規則被新增到排除項目的日期和時間。
- **規則名稱** — 入侵偵測規則的名稱。
- **規則 ID** — Suricata 格式的入侵偵測規則的 ID (SID 或簽章 ID)。
- **敘述** — 入侵偵測規則描述。
- **建立者** — 帳戶被用於將入侵偵測規則新增至排除項目的使用者名稱。

將入侵偵測規則新增至排除項目

您可以從事件掃描中排除具有中等或高度重要性警示的卡巴斯基入侵偵測規則。

> 您只能排除卡巴斯基入侵偵測規則。如果您不想在掃描事件時套用使用者定義的入侵偵測規則，可以停用或刪除該規則。

若要將入侵偵測規則新增至排除項目：

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。
   這將開啟警示表。
2. 點擊**技術**列中的連結開啟篩選器配置視窗。
3. 在左側的下拉清單中，選擇**包含**。
4. 在右側的下拉清單中，選擇 **（IDS）入侵偵測系統**技術。
5. 點擊**套用**。
6. 如果您想篩選偵測，請點擊展開篩選參數清單並選擇所需的篩選器。
7. 選擇一個警示，**偵測到**列顯示相關入侵偵測規則的名稱。
   這將開啟一個視窗，其中包含有關警示的資訊。
8. 在視窗的右側的**建議**部分、**分類**子部分，點擊**新增到排除項目**。
   這將開啟**將 IDS 規則新增到排除項目**視窗。

9. 在**敘述**欄位中，輸入入侵偵測規則的描述。

10. 點擊**新增**。

    入侵偵測規則將被加入到排除項目中，並顯示在應用程式 Web 介面中的**設定**部分、**排除項目**子部分、**IDS**索引標籤上的排除項目清單中。此規則不再被用於建立警示。

具有**安全稽核員**角色的使用者無法修改允許物件清單中的條目。

具有**安全官**角色的使用者無權存取新增至排除項目的入侵偵測規則清單。

編輯新增至排除項目的入侵偵測規則的描述

*若要編輯已排除的入侵偵測規則的描述，請在"**警示**"部分：*

1. 在應用程式 Web 介面視窗中，選擇"**警示**"區域。
   這將開啟警示表。

2. 點擊**技術**列中的連結開啟篩選器配置視窗。

3. 在左側的下拉清單中，選擇**包含**。

4. 在右側的下拉清單中，選擇 **（IDS）入侵偵測系統**技術。

5. 點擊**套用**。

6. 如果您想篩選偵測，請點擊展開篩選參數清單並選擇所需的篩選器。

7. 選擇一個警示，**偵測到**列顯示相關入侵偵測規則的名稱。
   這將開啟一個視窗，其中包含有關警示的資訊。

8. 在視窗的右側的**建議**部分、**分類**子部分，點擊**編輯 IDS 排除項目**。
   這將開啟**編輯 IDS 排除項目**視窗。
   在**敘述**欄位中，編輯規則描述。
   點擊**儲存**。

被排除的入侵偵測規則的描述被修改。此規則不再被用於建立警示。

具有"**安全稽核員**"角色的使用者無法編輯入侵偵測規則描述。

具有**安全官**角色的使用者無權存取新增至排除項目的入侵偵測規則清單。

從排除項目中刪除入侵偵測規則

您可以從排除項目中刪除單個入侵偵測規則、多個規則或同時刪除所有規則。

若要將入侵偵測規則從排除項目中刪除：

1. 在應用程式 Web 介面視窗中，選擇“**設定**” → “**排除項目**”部分並轉到“**IDS**”頁簽。
2. 顯示排除的入侵偵測規則的清單。
3. 選擇要從排除項目中刪除的規則。
   這將開啟一個視窗，其中包含有關規則的資訊。
4. 點擊**刪除**。
   這將開啟操作確認視窗。
5. 點擊**是**。

該規則已從排除項目中刪除。此規則用於建立警示。

若要從排除項目中刪除所有或多個 IDS 規則：

1. 在應用程式 Web 介面視窗中，選擇“**設定**” → “**排除項目**”部分並轉到“**IDS**”頁簽。
2. 顯示排除的入侵偵測規則的清單。
3. 選取要從排除項目中刪除的規則旁的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。
4. 在視窗下部顯示的窗格中，點擊**刪除**。
   這將開啟操作確認視窗。
5. 點擊**是**。

選定的規則將被從排除項目中刪除。這些規則用於建立警示。

具有**安全稽核員**角色的使用者無法從排除項目中刪除入侵偵測規則。

擁有“**安全官**”角色的使用者無權存取入侵偵測規則的排除項目清單。

管理 TAA 排除項目

由卡巴斯基專家建立的TAA (IOA) 規則包含企業 IT 基礎架構中物件可疑行為的指標。Kaspersky Anti Targeted Attack Platform 可掃描應用程式的事件資料庫，並為與 TAA (IOA) 規則所描述的行為相符的事件建立警示。如果您不希望應用程式為作為組織正常的主機活動的一部分產生的事件建立警示，您可以將 TAA (IOA) 規則新增至排除項目。

被新增到排除項目的 TAA (IOA) 規則模式可以在以下模式下運作：

- 規則始終被排除在外。

  在這種情況下，Kaspersky Anti Targeted Attack Platform 不會將事件標記為與 TAA (IOA) 規則匹配，也不會根據該規則建立警示。

- 規則由條件補充。

  在這種情況下，TAA（IOA）規則由條件以搜尋查詢形式補充。Kaspersky Anti Targeted Attack Platform 不會將符合指定條件的事件標記為符合TAA (IOA) 規則。對於與 TAA (IOA) 規則相符但不符合應用的排除條件的事件，應用程式會標記事件並建立警示。

如果您使用分散式解決方案和多組織用戶模式，TAA 排除項目可以有以下類型：

- **本機**—在 SCN 伺服器上建立。這些排除項僅目適用於連線到此 SCN 伺服器的主機。排除項屬於使用者在應用程式 Web 介面中管理的租戶。

- **全球**—在 PCN 伺服器上建立。排除項適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。排除項屬於使用者在應用程式 Web 介面中管理的租戶。

具有**資深安全員**角色的使用者可以為其有權存取資料的租用戶建立、編輯和刪除排除項目。

具有**安全稽核員**和**安全官**角色的使用者只能檢視 TAA 排除項目清單以及所選排除項目的屬性。

對於每個 TAA (IOA) 規則，您只能建立一個本機或全域排除項目。

如果一條TAA (IOA) 規則在 SCN 伺服器和 PCN 伺服器上都建立了排除項，Kaspersky Anti Targeted Attack Platform 將根據PCN 伺服器上的排除設定處理事件。

檢視新增至排除項目的 TAA (IOA) 規則表

若要檢視被新增到排除項目的 TAA (IOA) 規則表：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。

2. 點擊**TAA**頁簽。

   被排除的 TAA (IOA) 規則表將會顯示。您可以透過點擊列標題中的連結來篩選規則。

表包含以下資訊：

- 是根據此 TAA (IOA) 規則掃描而產生的警示的重要性。

  重要性等級可以採用以下其中一個值：

  - – **低**。
  - – **中**。
  - – **高**。

- **類型**是規則的類型，取決於產生該規則的伺服器角色：

  - **本機**—在 SCN 伺服器上建立。這些排除項僅目適用於連線到此 SCN 伺服器的主機。排除項屬於使用者在應用程式網頁介面中管理的租用戶。
  - **全球**—在 PCN 伺服器上建立。排除項適用於連線到此 PCN 伺服器的主機以及連線到此 PCN 伺服器的所有 SCN 伺服器。排除項屬於使用者在應用程式 Web 介面中管理的租戶。

- **置信** – 置信度，取決於規則引起誤報的可能性：

  - **高**。
  - **中**。
  - **低**。

  置信度越高，誤報的可能性就越低。

- **排除規則**是新增至排除項之規則的運作模式。

  - **總是**表示一律排除此規則。在這種情況下，Kaspersky Anti Targeted Attack Platform 不會將事件標記為與 TAA (IOA) 規則匹配，也不會根據該規則建立警示。
  - **根據條件**表示如果新增了條件則排除該規則。在這種情況下，TAA（IOA）規則由條件以搜尋查詢形式補充。Kaspersky Anti Targeted Attack Platform 不會將符合指定條件的事件標記為符合TAA (IOA) 規則。對於與 TAA (IOA) 規則相符但不符合應用的排除條件的事件，程式會標記事件並建立警示。

- **名稱**是規則的名稱。

將 TAA (IOA) 規則新增到排除項目

> 您只能排除 Kaspersky TAA (IOA) 規則。如果您不想套用使用者定義的 TAA (IOA) 規則進行掃描事件，您可以停用該規則或將其刪除。

*要從**警示**部分將 TAA (IOA) 規則新增至排除項目：*

1. 在應用程式 Web 介面視窗中，選擇**警示**區域。

   這將開啟警示表。

2. 點擊**技術**列中的連結開啟篩選器配置視窗。

3. 在左側的下拉清單中，選擇**包含**。

4. 在右側的下拉清單中，選擇**（TAA）針對性攻擊分析器**技術。

5. 點擊**套用**。

   此表顯示 TAA 技術根據 TAA (IOA) 規則產生的警示。

6. 選擇一個警示，**偵測到**列為其顯示相關規則的名稱。

   這將開啟一個視窗，其中包含有關警示的資訊。

7. 在**掃描結果**下面，點擊帶有規則名稱的連結以開啟規則資訊視窗。

8. 在**TAA 排除項目**設定名稱右側，點擊**新增到排除項目**。

   這將開啟一個視窗，允許您將 TAA (IOA) 規則新增至排除項目。

9. 在**排除規則**欄位中，選擇排除操作模式：

   - **總是**，如果您不希望應用程式為與所選 TAA (IOA) 規則相符的事件建立警示。
   - **根據條件**，如果您不希望應用程式只為符合指定條件的事件建立事件。將為與 TAA (IOA) 規則相符的事件建立警示，並考慮了配置的排除條件。

     如果您選擇了**根據條件**：

     a. 點擊**配置附加條件**開啟事件搜尋表單。

     b. 如果您使用的是分佈式解決方案和多組織用戶模式，並且希望為所有租用戶啟用事件顯示，請開啟**在所有租戶中搜尋**切換開關。

     c. 在建構器模式下執行事件搜尋。

     一個表格將顯示，其中包含與給定指定排除條件的 TAA (IOA) 規則相符的事件。

     如果您使用分佈式解決方案和多租戶模式，則找到的事件將按層分組：伺服器– 租戶名稱– 伺服器名稱。

     d. 點擊您要檢視其事件的伺服器的名稱。

     所選伺服器的主機表將顯示。事件分組層級顯示在表格上方。

     > 如有必要，您可以變更事件搜尋條件。

     e. 點擊**新增排除項目**。

10. 如果您使用分佈式解決方案和多租戶模式，請在**套用到伺服器***欄位中選擇必須對其應用規則的租戶和伺服器的核取方塊。

11. 點擊**新增**。

TAA (IOA) 規則將會被新增到排除項目中，並顯示在應用程式 Web 介面中排除項目清單的**設定**部分、**排除項目**子部分、**TAA**頁簽上。此規則不再被用於建立偵測。

*要從**威脅搜尋**部分將 TAA (IOA) 規則加入排除項目：*

1. 選擇程式 Web 介面視窗中的**威脅搜尋**部分。

   這將開啟事件搜尋表單。

2. 定義搜尋條件並點擊**搜尋**按鈕。例如，您可以在產生器模式下在**TAA 屬性**群組中選擇事件搜尋條件。

   滿足搜尋條件的事件表將顯示。

3. 選擇一個事件。

4. 在**IOA 標記**設定右側，點擊規則名稱。

   這將開啟一個視窗，其中包含有關規則的資訊。

5. 在**TAA 排除項目**設定名稱右側，點擊**新增到排除項目**。

   這將開啟一個視窗，允許您將 TAA (IOA) 規則新增至排除項目。

6. 在**排除規則**欄位中，選擇排除操作模式：

   - **總是**，如果您不希望應用程式為與所選 TAA (IOA) 規則相符的事件建立警示。
   - **根據條件**，如果您不希望應用程式只為符合指定條件的事件建立事件。將為與 TAA (IOA) 規則相符的事件建立警示，並考慮了配置的排除條件。

     如果您選擇了**根據條件**：

     a. 點擊**配置附加條件**開啟事件搜尋表單。

     b. 如果您使用的是分佈式解決方案和多組織用戶模式，並且希望為所有租用戶啟用事件顯示，請開啟**在所有租戶中搜尋**切換開關。

     c. 在建構器模式下執行事件搜尋。

        一個表格將顯示，其中包含與給定指定排除條件的 TAA (IOA) 規則相符的事件。

        如果您使用分佈式解決方案和多租戶模式，則找到的事件將按層分組：伺服器– 租戶名稱– 伺服器名稱。

     d. 點擊您要檢視其事件的伺服器的名稱。

        所選伺服器的主機表將顯示。事件分組層級顯示在表格上方。

        > 如有必要，您可以變更事件搜尋條件。

     e. 點擊**新增排除項目**。

7. 點擊**新增**。

TAA (IOA) 規則將會被新增到排除項目中，並顯示在應用程式 Web 介面中排除項目清單的**設定**部分、**排除項目**子部分、**TAA**頁簽上。掃描事件時不再套用此規則。

建立要儲存為排除條件的搜尋查詢時，請避免使用下列欄位：

- IOAd。
- IOATag。
- IOATechnique。
- IOATactics。
- IOAImportance。
- IOAConfidence。

只有當 Kaspersky Anti Targeted Attack Platform 將事件標記為符合 TAA (IOA) 規則後，這些欄位才會顯示。

具有**安全稽核員**和**安全官**角色的使用者無法將 TAA (IOA) 規則新增至排除項目。

檢視新增至排除項目的 TAA (IOA) 規則

若要檢視新增至排除項目的 TAA (IOA) 規則：

1. 在應用程式 Web 介面視窗中，選擇**設定**區段、**排除項目**子區段，然後前往**TAA**索引標籤。
   被排除的 TAA (IOA) 規則表將會顯示。
2. 選擇要檢視的規則。

這將開啟一個視窗，其中包含有關規則的資訊。

此視窗包含以下資訊：

- **TAA (IOA) 規則**：點擊此連結可開啟一個視窗，其中包含與此規則對應的 MITRE 技術描述、回應事件的建議，以及誤報可能性的資訊。
- **ID**是應用程式指派給每個規則的 ID。
- **名稱**是您新增規則時所指定的規則名稱。
- **重要級別**是卡巴斯基專家所評估，事件可能對電腦或企業區域網路安全造成之影響的估計。
- **置信**是置信等級，取決於卡巴斯基專家所估計的誤報機率。
- **排除規則**是新增至排除項之規則的運作模式。
  - **總是**表示一律排除此規則。在這種情況下，Kaspersky Anti Targeted Attack Platform 不會將事件標記為與 TAA (IOA) 規則匹配，也不會根據該規則建立警示。
  - **根據條件**表示如果新增了條件則排除該規則。在這種情況下，TAA（IOA）規則由條件以搜尋查詢形式補充。Kaspersky Anti Targeted Attack Platform 不會將符合指定條件的事件標記為符合TAA (IOA) 規則。對於與 TAA (IOA) 規則相符但不符合應用的排除條件的事件，程式會標記事件並建立警示。

- **配置附加條件**：點擊此連結可開啟帶有搜尋條件的事件搜尋表單。
  如果在將 TAA (IOA) 規則新增至排除項時您選擇了**根據條件**模式並配置了一些搜尋條件，則顯示此欄位。
- 搜尋條件以 `<IOA ID> AND NOT <search criteria>` 格式配置。
  如果在將 TAA (IOA) 規則新增至排除項時您選擇了**根據條件**模式並配置了一些搜尋條件，則顯示搜尋條件。
- **套用到伺服器***是排除項目適用的主機。
  此欄位在分散式解決方案和多組織用戶模式下顯示。

從排除項目中刪除 TAA (IOA) 規則

您可以從排除項目中刪除單個 TAA (IOA) 規則、多個規則或同時刪除所有規則。

若要從排除項目中刪除 TAA (IOA) 規則：

1. 在應用程式 Web 介面視窗中，選擇**設定**區段、**排除項目**子區段，然後前往**TAA**索引標籤。
   被排除的 TAA (IOA) 規則表將會顯示。
2. 選擇要從排除項目中刪除的規則。
   這將開啟一個視窗，其中包含有關規則的資訊。
3. 點擊**刪除**。
   這將開啟操作確認視窗。
4. 點擊**是**。

該規則已從排除項目中刪除。建立警示或掃描事件時套用此規則。

若要從排除項目中刪除全部或多個 TAA (IOA) 規則：

1. 在應用程式 Web 介面視窗中，選擇**設定**區段、**排除項目**子區段，然後前往**TAA**索引標籤。
2. 被排除的 TAA (IOA) 規則表將會顯示。
3. 選取要從排除項目中刪除的規則旁的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。
4. 在視窗下部顯示的窗格中，點擊**刪除**。
   這將開啟操作確認視窗。
5. 點擊**是**。

選定的規則將被從排除項目中刪除。建立警示或掃描事件時將套用這些規則。

具有**安全稽核員**和**安全官**角色的使用者無法從排除項目中刪除 TAA (IOA) 規則。

管理 ICAP 排除項目

具有**資深安全員**的使用者可以建立 ICAP 排除項清單，即 Kaspersky Anti Targeted Attack Platform 不得掃描的資料清單。您可以為以下資料建立 ICAP 排除規則：

- **格式**。
- **使用者代理**。
- **MD5**。
- **URL 遮罩**。
- **來源 IP 或子網路**。

具有**安全稽核員**和**安全官**角色的使用者可以檢視 ICAP 排除規則清單。

在分佈式解決方案模式下，在 SCN 上建立的 ICAP 排除項適用於連線到該 SCN 的所有 Sensor 元件。在 PCN 上建立的 ICAP 排除項適用於安裝在與 PCN 相同的裝置上的 SCN 以及連線到該 SCN 的所有 Sensor 元件。

檢視 ICAP 排除表

若要檢視 ICAP 排除表：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。

   Kaspersky Anti Targeted Attack Platform 不得掃描的資料表將會顯示。您可以透過點擊列標題中的連結來篩選規則。

表列包含以下資訊：

- **值** — 條件的值。
- **標準** — 將條目新增至允許物件清單的條件。
- **狀態**是規則的狀態。

將規則新增至 ICAP 排除項目

如果資料規則之前尚未被新增到掃描排除規則中，則 ICAP 排除規則將得到處理。

若要將規則新增至 ICAP 排除項目：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。
3. 在應用程式 Web 介面視窗的右上角，點擊**新增**。
   這將開啟**新規則**視窗。
4. 將**狀態**切換開關移至所需的位置。
   預設情況下，切換開關位於**已啟用**位置。
5. 在**標準**下拉式清單中，選擇下列其中一個將規則新增至 ICAP 排除清單的條件：
   - **格式**。
   - **使用者代理**。
   - **MD5**。
   - **URL 遮罩**。
   - **來源 IP 或子網路**。
6. 根據所選條件，在**值**欄位中指定以下資訊：
   - 如果您選擇了**格式**，請從下拉式清單中選擇要新增的檔案格式。

     > 按格式新增 ICAP 排除規則時，無需掃描即可載入對應格式的網頁內容，且不影響網頁顯示。

   - 如果您選擇了**使用者代理**，請輸入包含瀏覽器資訊的 `HTTP` 請求的使用者代理程式標頭。
   - 如果您選擇了 **MD5**，請輸入檔案的 MD5 雜湊。
   - 如果您選擇了**URL 遮罩**，請輸入 URL 遮罩。
     您可以在遮罩中使用以下特殊字元：
     * – 任意**字元**序列。

     範例：
     如果您輸入 `*abc*` 作為遮罩，應用程式不會掃描任何包含序列 `abc` 的 URL。例如，`www.example.com/download_virusabc`

     ? – 任意單一**字元**。

     範例：
     如果您輸入`example_123?.com`作為遮罩，應用程式不會掃描任何包含給定字元序列以及任何 3 之後的字元的 URL。例如，`example_1234.com`

     如果 * 或 ? 字元是要新增至掃描排除項目清單中的完整 URL 的一部分，請在輸入 URL 時使用 \ 字元來轉義單個 * 、 ? 或其後的**字元**。

     範例：
     您需要新增以下 URL 作為受信任位址：`www.example.com/download_virus/virus.dll?virus_name=`
     您不想應用程式將 ? 作為特殊遮罩字元處理，因此您可以在 ? 之前新增 \ 字元。

新增至掃描排除項目清單的 URL 如下所示：`www.example.com/download_virus/virus.dll\?virus_name=`

> 在**URL 遮罩**欄位中，您可以輸入包含西里爾字元的網域名稱。在這種情況下，位址將轉換為 Punycode 並根據應用程式設定進行處理。

- 如果您選擇了**來源 IP 或子網路**，請輸入位址或子網路（例如255.255.255.0）。

7. 點擊**新增**。

該規則將被新增到 I CAP 排除項清單中。

> 具有**安全稽核員**和**安全官**角色的使用者無法新增 ICAP 排除規則。

從 ICAP 排除項目中刪除規則

若要從 ICAP 排除項目中刪除一條或多條規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。
3. 選擇您想要從 ICAP 排除項目清單中移除的每個規則左側的核取方塊。
   如果您想要刪除所有規則，請選擇清單上方的核取方塊。
4. 在視窗的下部，點擊**刪除**。
5. 這會開啟一個視窗；在該視窗中，點擊**是**確認刪除規則。

選定的規則將會從 ICAP 排除項清單中刪除。先前在 ICAP 排除規則中列出的資料現在由 Kaspersky Anti Targeted Attack Platform 進行掃描。

> 具有**安全稽核員**和**安全官**角色的使用者無法從 ICAP 排除項清單中刪除條目。

編輯或停用 ICAP 排除項目清單中的規則

若要編輯 ICAP 排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。
3. 選擇要修改的規則。
   這會開啟**編輯規則**視窗。

4. 對**狀態**、**標準**和**值**欄位進行必要的變更。

5. 點擊**儲存**。

   規則已修改。

若要停用 ICAP 排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。

2. 開啟**ICAP**索引標籤。

3. 在 ICAP 排除項目清單中要停用的規則右側，在**狀態**欄中，將切換開關移至**已停用**位置。

4. 這將會開啟一個視窗；在該視窗中，點擊**是**以確認停用規則。

   該規則被停用。

> 具有**安全稽核員**和**安全官**角色的使用者無法編輯或停用 ICAP 排除項目清單中的規則。

按條件篩選 ICAP 排除項目清單中的規則

若要依條件篩選 ICAP 排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。

2. 開啟**ICAP**索引標籤。

3. 點擊**標準**連結以開啟篩選配置視窗。

4. 選擇您要根據其篩選規則的條件旁邊的一個或多個核取方塊：

   - **格式**。
   - **使用者代理**。
   - **MD5**。
   - **URL 遮罩**。
   - **來源 IP 或子網路**。

5. 點擊**套用**。

   篩選配置視窗關閉。

ICAP 排除項清單僅顯示與指定篩選條件相符的規則。您可以按**值**和**狀態**列同時進行篩選。

按值篩選 ICAP 排除項目清單中的規則

若要依值篩選 ICAP 排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。
3. 點擊**值**連結以開啟篩選配置視窗。
4. 輸入一個值。
5. 點擊**套用**。

ICAP 排除項清單僅顯示與指定搜尋條件相符的規則。您可以按**標準**和**狀態**列同時進行篩選。

按狀態篩選 ICAP 排除項目清單中的規則

若要依狀態篩選 ICAP 排除項目清單中的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。
3. 點擊**狀態**連結以開啟篩選配置視窗。
4. 選擇某個值旁邊的核取方塊：
   - **已啟用**。
   - **已停用**。
5. 點擊**套用**。

ICAP 排除項清單僅顯示與指定搜尋條件相符的規則。您可以同時按**標準**和**值**列進行篩選。

重置 ICAP 排除項目清單中的規則篩選條件

若要清除 ICAP 排除項目清單中規則的篩選條件：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**排除項目**子部分。
2. 開啟**ICAP**索引標籤。
3. 點擊表格中要重設篩選條件之**值**、**標準**或**狀態**欄標題右側的。
   如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選條件將被清除。ICAP 排除項清單僅顯示與指定條件相符的規則。

管理 SPAN 連接埠的映像流量

管理 Web 介面時，具有**資深安全員**角色的使用者可以從 Sensor 元件伺服器的 SPAN 連接埠下載 PCAP 格式的鏡像流量傾印，並進行調查以偵測可疑活動。

> 如果您使用分佈式解決方案和多組織用戶模式，請在具有 Sensor 元件的伺服器所連線的 PCN 或 SCN 伺服器上執行相關步驟。

若要從 SPAN 連接埠下載映像流量：

1. 在應用程式 Web 介面視窗中，選擇"**Sensor 伺服器**"區域。
2. 點擊相關 Sensor 元件的卡片。

   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊**下載流量**。

   顯示下載選項視窗。

   在"**內部儲存**"部分，"**最舊的封包**"欄位顯示內部儲存中第一次儲存的傾印的日期和時間。在"**已使用/最大**"欄位中，第一個數字表示內部儲存的已佔用空間，第二個數字表示內部儲存的總大小。"**外部儲存**"部分顯示儲存狀態："**已連線**"或"**未連線**"。
4. 執行以下操作：

   - 在"**要下載的流量週期**"中，設定要下載流量傾印的期限範圍。

     > 如果您選擇的時間段內不存在記錄的流量，則當您點擊"**下載流量**"時，Kaspersky Anti Targeted Attack Platform 會建議選擇從第一次記錄的網路流量傾印到最後一次記錄的時間段。如果根本不存在記錄的傾印，則會顯示警告，指示指定時間內缺少資料。

   - 在"**下載量限制**"欄位中，您可以指定要下載的最大流量。

     如果下載的流量超過指定的限制，則會丟棄最新的流量。

   - 如果需要，請在"**按監控點篩選**"下啟用篩選，並指定要從中取得流量的監控點。

   - 如有必要，請在"**使用 BPF 篩選**"部分啟用篩選，並輸入使用 Berkeley Packet Filter (BPF) 技術的篩選表達式。BPF 篩選表達式的寫入格式為 libpcap。有關語法的更多詳細資訊，請參閱"pcap-filter 手冊頁"。

     篩選表達式的範例：
     ```
     tcp port 102 or tcp port 502
     ```

   - 如有必要，請在"**使用正規表達式篩選**"部分啟用篩選，並輸入基於流量中的有效負載資料進行篩選的表達式。

     篩選表達式範例：
     ```
     ^test.+xABxCD
     ```
5. 點擊**下載流量**。

來自 SPAN 連接埠的映像流量傾印以 PCAP 格式下載。

順序流量下載請求的建議

我們建議在傳送新的流量下載請求時考慮處理先前的流量下載請求所需的時間。

如果下一個流量下載請求在前一個流量下載請求完成之前到達，則傾印檔案下載可能會失敗，並且不會出現任何錯誤訊息。

請求處理時間取決於各種因素：搜尋範圍、要下載的流量大小以及 Sensor、伺服器和用戶端電腦之間的連線速度。

要下載的流量大小取決於客戶的要求；少量流量可以在幾秒鐘內下載。如果使用者嘗試下載所有可用流量，則下載速度限制為 50 Mbps。這個限制可以防護系統不會因為下載大量流量而導致過載。在 50 Mbps 的速度下，下載 1 GB 的流量大約需要 20 秒，下載1 TB 的流量大約需要 5.5 小時。

建立存檔的密碼清單

該應用程式不會掃描受密碼防護的壓縮檔案。您可以為在組織內交換檔案時使用的壓縮檔案建立最常遇到的密碼清單。如果這樣做，應用程式將在掃描壓縮檔案時嘗試清單中的密碼。如果其中一個密碼匹配，則將解鎖並掃描壓縮檔案。

應用程式設定中設定的密碼清單也會傳輸到具有 Sandbox 元件的伺服器。

若要建立壓縮檔案密碼清單：

1. 在應用程式 Web 介面視窗中，選擇**設定**部分的**壓縮檔案密碼**子部分。
2. 在**壓縮檔案密碼**欄位中，輸入應用程式用於密碼防護壓縮檔案的密碼。

   在新行上輸入每個密碼。您最多可以輸入 50 個密碼。
3. 點擊**套用**。

   將會建立壓縮檔案的密碼清單。掃描受密碼防護的 PDF 檔案以及 Microsoft Word、Excel® 和 PowerPoint® 檔案時，應用程式將使用定義清單中的密碼。

具有**安全稽核員**角色的使用者可以檢視壓縮檔案的密碼清單，但無法編輯它。

具有**安全官**角色的使用者無權存取此 Web 介面部分。

管理 Central Node 或 Sensor 伺服器資訊

擁有“**安全稽核員**”角色的使用者可以檢視有關具有 Central Node 和 Sensor 元件的伺服器的資訊。

有關具有 Central Node 或 Sensor 元件的伺服器的資訊顯示在應用程式 Web 介面視窗的“**Sensor 伺服器**”區域。

此部分顯示元件的卡片（左側）和在這些元件上偵測到的網路介面卡（每個元件的右側）。

Sensor 元件卡片上方是該 Sensor 所連線的 Central Node 元件卡片。

如果 Central Node 元件部署了嵌入式 Sensor，則該 Sensor 元件的名稱將在卡片上顯示為嵌入式 Sensor。

網路介面卡顯示以下資訊：

- 網路介面名稱
- 網路介面的 MAC 位址
- 網路介面的 IP 位址
- 網路介面頻寬

如果網路介面已經新增了監控點，則網路介面的卡片中將顯示該監控點的下列資訊：

- 監控點名稱。
- **技術模式**是技術繼承功能的狀態。它可以是**已啟用**或者**已停用**。

您可以檢視 Central Node 和 Sensor 元件以及在這些元件上發現的網路介面的詳細資訊。

若要檢視元件或網路介面詳細資料：

點擊其卡片。

Central Node 和 Sensor 元件的**設定**索引標籤顯示以下資訊：

- **狀態**是元件目前的狀態，以圖示和文字描述表示。
- **節點類型**表示應用程式元件：**Server**（Central Node 元件）或 **Sensor**（Sensor 元件）。
- **應用程式目前使用的磁碟空間**是應用程式檔案所佔用的磁碟空間。包括已安裝的檔案和應用程式在運行過程中建立的檔案。
- **應用程式可使用的最大磁碟空間**就是應用程式檔案可佔用的磁碟空間。包括已安裝的檔案和資料儲存規則中配置的所有空間限制的總和。該值不得超過可用磁碟空間量。
- **磁碟佔用**是所有檔案使用的磁碟空間。包括應用程式檔案、作業系統檔案和其他應用程式的檔案。此空間是根據包含元件檔案系統中 /var 目錄的磁碟來計算的。
- **可用磁碟空間**是未被檔案佔用的磁碟空間。此空間是根據包含元件檔案系統中 /var 目錄的磁碟來計算的。
- **總磁碟空間**是包含元件檔案系統中 /var 目錄的磁碟機上的磁碟空間總量。
- **BPF 篩選**指示是否啟用或停用使用基於網路封包中的位址參數的 Berkeley Packet Filter (BPF) 技術進行篩選。
- **流量傾印檔案的外部儲存**指示外部儲存的連線狀態。可能顯示以下狀態：**已連線**、**未連線**。
- **保留規則**指示應用程式資料的大小、項目數量和儲存期限的目前值和最大值。

對於 Sensor 元件，除了**設定**索引標籤之外，還會顯示**外部儲存**、**其他**、**ICAP 整合**、**POP3 整合**和**SMTP 整合**索引標籤。

- **外部儲存**索引標籤顯示有關鏡像 SPAN 流量之外部儲存組態的資訊。
- 在**其他**索引標籤上，會顯示以下資訊：
  - 掃描檔案大小上限是元件目前可掃描檔案大小的限制。
  - 傾印 HTTP 主體指示是否啟用或停用 HTTP 主體內容傾印。
- **ICAP 整合**索引標籤顯示透過 ICAP 與代理伺服器整合的設定。
- **POP3 整合**索引標籤顯示POP3 郵件伺服器整合設定。
- **SMTP 整合**索引標籤顯示SMTP 郵件伺服器整合設定。

對於未新增監控點的網路介面，詳細資料區中顯示以下資訊：

- **網路介面**是作業系統中網路介面的名稱。
- **連線**是表示網路線已連線到網路介面的乙太網路連接埠的圖示：
  - — 網路線已連線。
  - — 網路已斷開連線。

  啟用乙太網路連接埠指示模式時，圖示閃爍。
- **MAC 位址**是網路介面的 MAC 位址。
- **IP 位址**是網路介面的 IP 位址。如果網路介面上發現多個 IP 位址，則詳細資料區域中最多顯示 16 個 IP 位址。

如果網路介面上已經新增了監控點，則網路介面的卡片中會顯示以下資訊：

- **狀態**是監控點目前的狀態，以圖示和文字描述表示：
  - *正常*。監測點可用。
  - *切換*。監控點運作模式正在改變。
  - *錯誤*。切換監控點操作模式時偵測到錯誤。
- **連線**是表示網路線已連線到網路介面的乙太網路連接埠的圖示：
  - — 網路線已連線。
  - — 網路已斷開連線。

  啟用乙太網路連接埠指示模式時，圖示閃爍。
- **網路介面**是作業系統中網路介面的名稱。

- **模式**是監控點目前的模式：
  - *已啟用*。
  - *已停用*。
- 在**設定**索引標籤上：
  - **技術繼承**指示是否為伺服器啟用或停用技術繼承。
  - **MAC 位址**是網路介面的 MAC 位址。
  - **IP 位址**是網路介面的 IP 位址。

檢視伺服器設定

具有**安全稽核員**角色的使用者可以檢視分佈式解決方案和多組織用戶模式下的 Central Node 伺服器和 PCN 設定。

伺服器設定位於 Web 介面視窗的**設定**部分。在此部分中，您可以檢視以下資訊：

- **使用者**：
  - **使用者** — 使用者帳戶清單
  - **Active Directory 整合** — Active Directory 整合設定。
- **一般設定**：
  - **資料庫更新** — 資料庫更新。
  - **監控** — Central Node 和 Sensor 伺服器允許的最大硬碟空間使用量。
  - **SNMP** — SNMP 連線設定。
- **身分驗證政策** — 身分驗證政策設定。
- **憑證** — 伺服器憑證和具有 Endpoint Agent 元件的電腦的狀態。
- **日期和時間** — 伺服器日期和時間設定。
- **Endpoint Agent** — 與 Endpoint Agent 元件整合時可用的程式功能。
  - **遙測** — 配置從 Endpoint Agent 接收的資料的範圍。
  - **IOC 掃描排程** — IOC 掃描計劃的設定。
  - **自動將檔案傳送到 Sandbox** — 自動傳送要由 Sandbox 元件掃描的檔案。
  - **活動指示器** — Endpoint Agent 元件的活動指示器。
  - **自動刪除不活動的主機** — 自動從 Endpoint Agent 表中移除不活動的主機。

- **手動將檔案從主機傳送到 Sandbox 進行分析** — 手動傳送要由 Sandbox 元件掃描的檔案。
- **對事件鏈使用 TAA (IOA) 規則** — 使用 TAA（IOA）規則掃描事件鏈。預設情況下停用此功能。

- **ICAP 流量掃描** — 透過 ICAP 與代理伺服器整合的設定。
- **連線伺服器** — 作為 Endpoint Agent 元件的整合伺服器的伺服器。
- **連線器** — 連線器設定。
- **Secret** — 秘密的設定。
- **事件類型** — 事件類型的設定。
- **風險類型** — 風險類型的設定。
- **KSN/KPSN 和 MDR** — 參與卡巴斯基安全網路和卡巴斯基私人安全網路的設定以及啟用 MDR 整合。
- **KPSN 信譽資料庫** — 使用 KPSN 信譽資料庫的設定。
- **通知** — 通知設定。
- **SIEM 系統** — 與 SIEM 系統整合的設定。
- **VIP 狀態** — 將 VIP 身分指派給警示的規則清單。
- **排除項目** — 允許的物件清單、TAA 排除項目清單和 IDS 規則。
- **網路設定** — 網路介面參數的設定。
- **允許規則** — 控制網路上裝置互動的規則。
- **壓縮檔案密碼** — 壓縮檔案密碼清單。
- **產品授權** — 產品授權金鑰的狀態。

檢視具有 Sandbox 元件的伺服器表

具有**安全稽核員**角色的使用者可以檢視具有 Sandbox 元件的伺服器表。

具有 Sandbox 元件的伺服器表位於應用程式 Web 介面視窗的**Sandbox 伺服器**區段中，位於**伺服器**索引標籤上。

憑證指紋欄位顯示 Central Node 伺服器的 TLS 憑證指紋。

伺服器清單表包含以下資訊：

- **IP 和名稱** — 具有 Sandbox 元件的伺服器的 IP 位址或完全限定網域名稱。
- **憑證指紋** — 具有 Sandbox 元件的伺服器的憑證指紋。

- **授權** — 連線到 Sandbox 元件的請求狀態。
- **狀態** — 與 Sandbox 元件的連線狀態。

具有**安全官**角色的使用者無法檢視具有 Sandbox 元件的伺服器表。

檢視用於掃描 Sandbox 中物件的作業系統集的設定

具有**安全稽核員**角色的使用者可以檢視作業系統集的設定，這些設定被用作 Sandbox 元件建立掃描物件工作的基礎。Sandbox 伺服器必須安裝與所選集相符的虛擬機。

有關用於在 Sandbox 中掃描物件的作業系統集設定的資訊，位於應用程式 Web 介面視窗的**Sandbox 伺服器**部分中、**設定**索引標籤上。

Sandbox 元件可以在其上掃描物件的作業系統集顯示在**作業係統集合**下方。

屬於所選集的作業系統顯示在**集合組成**下方。

檢視外部系統表

具有**安全稽核員**角色的使用者可以檢視外部系統表。

外部系統表位於應用程式 Web 介面視窗的**外部系統**部分。

憑證指紋欄位顯示 Central Node 伺服器的 TLS 憑證指紋。

伺服器清單表包含以下資訊：

- **Sensor** — 外部系統伺服器的 IP 位址或網域名稱。
- **類型** — 外部系統的類型（郵件感應器或其他系統）。
- **名稱** — 不是郵件感應器的整合外部系統的名稱。
  郵件感應器的此列中顯示破折號。
- **ID** — 外部系統的 ID。
- **憑證指紋** — 伺服器的 TLS 憑證的指紋，外部系統用於與 Central Node 伺服器建立加密連線。

  具有 Central Node 元件的伺服器的憑證指紋顯示在視窗上方的**憑證指紋**欄位中。

- **狀態** — 整合請求的狀態。

具有**資深安全員**和**安全官**角色的使用者無法檢視外部系統表。

管理使用者定義的 Sandbox 規則

使用者自訂的檔案和 URL 掃描 Sandbox 規則允許將物件傳送到自訂虛擬機進行掃描。如果未新增任何規則，則不會在自訂虛擬機中掃描物件。若要在預設虛擬機器中傳送要掃描的物件，您不需要建立任何規則。預設情況下，Kaspersky Anti Targeted Attack Platform 會傳送需要掃描的物件進行掃描。

僅當存在自訂虛擬機器時，規則建立才可用。

具有**資深安全員**和**管理員**角色的使用者可以建立檔案掃描規則和 URL 掃描規則，編輯、刪除、啟用或停用規則。檔案掃描規則也可以被匯入和匯出。

在分散式解決方案模式下，您必須在要從中傳送檔案進行掃描的每個 PCN 和 SCN 伺服器上建立用於在自訂虛擬機中掃描檔案的規則。

具有**安全稽核員**角色的使用者可以檢視規則清單。具有**安全官**角色的使用者無法檢視此部分。

檢視使用者定義的 Sandbox 規則表

若要檢視使用者定義的 Sandbox 規則表：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的**Sandbox**小節。
2. 開啟**檔案**或者 **URL** 索引標籤。

   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。

使用者定義的檔案掃描規則表包含以下資訊：

- **已建立**是規則建立時間。
- **虛擬機**是檔案被傳送到進行掃描的虛擬機的名稱。
- **遮罩**是被傳送進行掃描的檔案的遮罩。
- **遮罩排除項目**是被從掃描中排除的檔案的遮罩。
- **檔案類別**是被傳送用於掃描的檔案類別。
- **狀態**是規則的狀態。它可以具有值**已啟用**和**已停用**。

使用者定義的 URL 掃描規則表包含以下資訊：

- **已建立**是規則建立時間。
- **虛擬機**是檔案被傳送到進行掃描的虛擬機的名稱。
- **狀態**是規則的狀態。它可以具有值**已啟用**和**已停用**。

配置 Sandbox 規則表顯示

您可以顯示或隱藏列並變更表中列的順序。

若要設定表格顯示：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 索引標籤。
   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。
3. 在表格的標題部分，點擊 。
   這將開啟**自訂表格**視窗。
4. 如果要在表格中顯示列，請選擇要在表格中顯示的參數名稱旁的核取方塊。
   如果要隱藏表中的參數，請清除該核取方塊。

   > 必須選擇至少一個核取方塊。

5. 如果要變更表格中列的順序，請將滑鼠遊標移至具有相關參數的行，點擊 ⠿ 並將該行移到新位置。
6. 如果要還原預設表格顯示設定，請點擊**預設**。
7. 點擊**套用**。

規則表顯示已配置。

篩選並搜尋 Sandbox 規則

若要依所需條件篩選或搜尋 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 頁簽。
3. 根據篩選條件，執行以下操作：
   - **按建立時間**
     a. 點擊**已建立**連結以開啟篩選設定視窗。
     b. 選擇以下選項之一：
       - **任何時候**如果您希望表顯示任何時間建立的規則。
       - **上一個小時**，如果您希望應用程式顯示表中最後一小時建立的規則。

- **最後一天**，如果您希望應用程式顯示表中最後一天建立的規則。
- **自訂範圍**，如果您希望應用程式顯示表中在指定時段內建立的規則。

c. 如果您選擇了**自訂範圍**，請選擇該期間的開始日期和結束日期，然後點擊**套用**。

- **按虛擬機名稱**

a. 點擊**虛擬機**開啟篩選設定視窗。

b. 輸入虛擬機名稱的一個或多個字元。

c. 點擊**套用**。

此表僅顯示與指定條件相符的規則。

您可以同時使用多個篩選器。

清除 Sandbox 規則篩選器

若要清除 Sandbox 規則篩選器的一個或多個篩選條件：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 頁簽。
3. 點擊要為其清除篩選條件的規則表欄標題右側的 ⊠。
   如果要清除多個篩選條件，請採取步驟單獨清除每個篩選條件。

選定篩選器將會被清除。

此表僅顯示與指定條件相符的規則。

檢視使用者定義的 Sandbox 規則資訊

若要檢視使用者定義的 Sandbox 規則資訊：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 頁簽。
3. 選擇您想檢視資訊的規則。

這將開啟一個視窗，其中包含有關規則的資訊。

有關使用者定義的檔案掃描規則的資訊視窗包含以下資訊：

- **狀態**是阻止規則的狀態。
- **虛擬機**是在其上根據此規則掃描檔案的虛擬機。
- **遮罩**是被傳送進行掃描的檔案的遮罩。
- **遮罩排除項目**是被從掃描中排除的檔案的遮罩。
- **檔案類別**是被傳送用於掃描的檔案類別。
- **檔案大小**是正在被掃描的檔案的大小。

有關使用者定義的 URL 掃描規則的資訊視窗包含以下資訊：

- **虛擬機**是掃描 URL 的虛擬機。
- **狀態**是阻止規則的狀態。

建立使用者定義的檔案掃描 Sandbox 規則

新增使用者定義的檔案掃描 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**索引標籤。
3. 點擊**新增**。
4. 選擇**建立規則**。
   這將開啟規則建立視窗。
5. 配置以下設定：
   a. **狀態**是阻止規則的狀態。如果您想要啟用該規則，請選擇該核取方塊。
   b. **虛擬機**是根據此規則掃描檔案的虛擬機。
      只能選擇具有自訂作業系統映像的虛擬機。這些虛擬機必須屬於在 Central Node 上所選的作業系統集。
   c. 至少指定以下值之一：遮罩或檔案類別。如果填寫所有欄位，則會針對與類別和大小條件或遮罩和大小條件相符且不是排除項目的檔案觸發規則。
      - **遮罩**是您要傳送進行掃描的檔案的遮罩。您可以指定多個值。
        若要指定遮罩，您可以使用 * 和 ? 萬用字元。其他通配符不受支援。
      - **遮罩排除項目**是必須從掃描中排除的檔案的遮罩。您可以指定多個值。
        若要指定排除遮罩，您可以使用 * 和 ? 萬用字元。其他通配符不受支援。
      - **檔案類別**是您要傳送進行掃描的檔案類別。您可以指定多個類別。
        您可以在檔案類別的副檔名清單部分中檢視每個類別的副檔名的完整清單。

- **檔案大小**是正在被掃描的檔案的大小。
- 如果要設定多個範圍，請點擊**新增檔案大小**。

6. 點擊**新增**。

   規則已建立。

如果要傳送壓縮檔案進行掃描，則必須考慮掃描壓縮檔案時涉及的特殊注意事項。

檔案掃描如下：

1. Kaspersky Anti Targeted Attack Platform 解壓縮檔案。
2. 壓縮檔案中與規則相符的檔案將被傳送以進行掃描。

具有 MSI 副檔名的檔案的掃描方式與壓縮檔案相同。

建立使用者定義的 URL 掃描 Sandbox 規則

新增使用者定義的 URL 掃描 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟 **URL** 索引標籤。
3. 點擊**新增**。
4. 選擇**建立規則**。
   這將開啟規則建立視窗。
5. 配置以下設定：
   a. **虛擬機**是將掃描 URL 的虛擬機。
      只能選擇具有自訂作業系統映像的虛擬機。這些虛擬機必須屬於在 Central Node 上所選的作業系統集。
   b. **狀態**是阻止規則的狀態。如果您想要啟用該規則，請選擇該核取方塊。
6. 點擊**新增**。

   規則已建立。

複製使用者定義的 Sandbox 規則

複製使用者定義的 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 頁簽。
3. 選擇相關規則。
4. 在規則視窗中，點擊**複製**。

   規則將與所有設定一起複製。如有必要，您可以變更設定的值。

匯入使用者定義的檔案掃描 Sandbox 規則

若要匯入使用者定義的檔案掃描 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**索引標籤。
3. 點擊**新增**。
4. 選擇**匯入規則**。
5. 這將開啟檔案上傳視窗。
6. 選擇您想匯入的檔案。
7. 點擊**開啟**。

   檔案已匯入。

編輯使用者定義的 Sandbox 規則

編輯使用者定義的 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 索引標籤。
   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。
3. 選擇一個規則。

   這將開啟規則編輯視窗。

您可以編輯以下欄位：

- 在使用者定義的檔案掃描 Sandbox 規則中：
  - **狀態**是阻止規則的狀態。如果您想要啟用該規則，請選擇該核取方塊。
  - **虛擬機**是根據此規則掃描檔案的虛擬機。
    只能選擇具有自訂作業系統映像的虛擬機。這些虛擬機必須屬於在 Central Node 上所選的作業系統集。
  - 至少指定以下值之一：遮罩或檔案類別。如果填寫所有欄位，則會針對與類別和大小條件或遮罩和大小條件相符且不是排除項目的檔案觸發規則。
    - **遮罩**是您要傳送進行掃描的檔案的遮罩。您可以指定多個值。
      若要指定遮罩，您可以使用 * 和 ? 萬用字元。其他通配符不受支援。
    - **遮罩排除項目**是必須從掃描中排除的檔案的遮罩。您可以指定多個值。
      若要指定排除遮罩，您可以使用 * 和 ? 萬用字元。其他通配符不受支援。
    - **檔案類別**是您要傳送進行掃描的檔案類別。您可以指定多個類別。
      您可以在檔案類別的副檔名清單部分中檢視每個類別的副檔名的完整清單。
    - **檔案大小**是正在被掃描的檔案的大小。
      如果要設定多個範圍，請點擊**新增檔案大小**。
- 在使用者定義的 URL 掃描 Sandbox 規則中：
  - **虛擬機**是將掃描 URL 的虛擬機。
    只能選擇具有自訂作業系統映像的虛擬機。這些虛擬機必須屬於在 Central Node 上所選的作業系統集。
  - **狀態**是阻止規則的狀態。如果您想要啟用該規則，請選擇該核取方塊。

啟用或停用使用者停用 Sandbox 規則

要啟用或停用 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 索引標籤。
   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。
3. 在具有相關規則的行中，選擇或清除**狀態**列中的核取方塊。

規則被啟用或停用。

若要啟用或停用所有或多個 Sandbox 規則的使用：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。
2. 開啟**檔案**或者 **URL** 索引標籤。
   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。

3. 選擇要啟用或停用其使用的規則左側的核取方塊。
   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。
   控制面板出現在視窗的下部。

4. 點擊**啟用**或者**停用**啟用或停用選定的規則。

選定的規則已啟用或停用。

匯出使用者定義的檔案掃描 Sandbox 規則

要匯出使用者定義的 Sandbox 規則以進行物件掃描：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。

2. 開啟**檔案**索引標籤。

3. 點擊**匯出**。

規則檔案被儲存到本機。該檔案以 JSON 格式下載。

刪除使用者定義的 Sandbox 規則

具有**資深安全員**角色的使用者可以刪除一個或多個使用者定義的 Sandbox 規則，或同時刪除所有規則。

若要刪除使用者定義的 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。

2. 開啟**檔案**或者 **URL** 索引標籤。
   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。

3. 選擇您想刪除的規則。
   這將開啟一個視窗，其中包含有關規則的資訊。

4. 點擊**刪除**。
   這將開啟操作確認視窗。

5. 點擊**是**。

規則被刪除。

若要刪除所有或多個使用者定義的 Sandbox 規則：

1. 在應用程式 Web 介面視窗中，選擇**自訂規則**部分的 **Sandbox** 小節。

2. 開啟**檔案**或者 **URL** 索引標籤。
   使用者定義的檔案或 URL 掃描 Sandbox 規則表將顯示。

3. 選擇您要刪除的規則左側的核取方塊。

   您可以透過選擇包含列標題的行中的核取方塊來選擇所有規則。

   控制面板出現在視窗的下部。

4. 點擊**刪除**。

   這將開啟操作確認視窗。

5. 點擊**是**。

所選檔案將被刪除。

檔案類別的副檔名清單

下表列出了檔案類別的副檔名。

檔案類別的副檔名

類別	
1C	.epf、.ert、.erf、.cf、.dt、.deb、.bsl、.os、.ertx、.xls、.xml、.html、.txt、.cfu、.rptdesign、.xdt、.xslt、.wsdl
Adobe Flash Player	.swf、.fla、.flv、.f4v、.f4p、.f4a、.f4b、.mxml、.as、.asc、.ascs、.asv、.fxp、.fxpl、.xfl、.swc、.cfx、.spl、.dcr、.dir、.dxr、.aam、.s
Java	.jar、.class、.war、.ear、.jad、.jnlp、.ser、.jsp、.jspx、.properties、.policy
Html	.html、.htm、.shtml、.xhtml、.xml、.svg、.mathml、.rss、.atom、.json、.mht、.mhtml、.webarchive
網路封包	.pcap、.pcapng、.cap、.netcap、.etl、.erf、.pkts、.pkt、.tcpdump、.snoop、.ngc、.dump、.cat、.smb、.vpcap、.dmp、.shb、.npl、
SAP	.abap、.adt、.bak、.cct、.cdp、.cpf、.dsc、.erd、.glo、.grc、.lis、.log、.lsa、.msg、.olap、.pgm、.prd、.sap、.sd、.se、.so、.spf、.tp
XML	.xml、.xsl、.xslt、.rdf、.rss、.opf、.svg、.wsdl、.xhtml、.xjb、.xmi、.xpl、.xsl-fo、.xquery、.xsd、.dtd、.xht、.atom、.mathml、.mml、.
壓縮檔案	.snb、.apk、.mht、.crx、.dd、.r01、.mpkg、.pup、.tbz、.ace、.arj、.bin、.cab、.cbr、.deb、.exe、.gzip、.one、.pak、.pkg、.ppt、.rpm
音訊	.a52、.adt、.dct、.dss、.dvf、.iklax、.ivs、.rm、.rmvb、.8svx、.amb、.avr、.cdda、.cvs、.cvsd、.cvu、.dts、.dvms、.fap、.fssd、.gsr
視訊	.drc、.f4a、.f4b、.f4p、.gifv、.mng、.mp2、.mpe、.mpv、.nsv、.roq、.svi、.3gp2、.3gpp2、.asx、.bin、.dat、.drv、.gtp、.moov、.spl
文件	.sxi、.odg、.svg、.vsd、.eps、.cwk、.wp、.ott、.asp、.cdd、.cpp、.dotm、.gpx、.indd、.kdc、.kml、.mdb、.mdf、.mso、.one、.pkg、
鏡像	.dib、.pdf、.mrw、.icns、.wdp、.fig、.epsf、.cur、.erf、.fts、.heif、.jfif、.jpe、.jps、.mng、.pam、.pbm、.pes、.pfm、.picon、.pnm、
Android 可執行檔案	.apk、.aab、.dex、.so、.jar、.aar、.class、.obb、.odex、.vdex、.vmx、.vmem、.img
Windows 可執行檔案	.cgi、.ds、.air、.cpp、.gadget、.hta、.jar、.msu、.paf.exe、.pwz、.thm、.vbs、.exe、.msi、.bat、.cmd、.com、.pif、.scr、.vb、.vbe、
可執行檔案	.rc、.p、.d、.asc、.bas、.cbl、.vbp、.iwb、.pb、.yml、.pika、.s19、.xt、.suo、.fsproj、.pbj、.pbxuser、.pyw、.xq、.cd、.sb、.sb2、.ise
磁碟鏡像	.img、.cue、.dsk、.vmdk、.vhd、.vhdx、.tc、.crypt、.dmgpart、.sparsebundle、.xva、.cif、.pqi、.udf、.fvd、.arc、.fcd、.gi、.giz、.im
Windows 事件日誌	.evt、.evtx、.log、.txt、.xml
Windows 登錄檔檔案	.reg、.dat、.pol、.hiv、.srd

類別	
字體	.bin、.ps、.sfd、.fnt、.afm、.ttf、.otf、.woff、.woff2、.eot、.svg、.dfont、.pfa、.pfb、.pfm、.fon、.suit、.bdf、.pcf、.snf、.ufo、.lib
資料庫檔案	.bup、.csv、.json、.xml、.myi、.sqlplan、.abs、.abx、.ac、.accdb、.accdc、.accde、.accdr、.accdt、.accdw、.accft、.adb、.ade、.a wal、.db2、.db3、.dbc、.dbf、.dbs、.dbt、.dbv、.dbx、.dcb、.dct、.dcx、.ddl、.dlis、.dp1、.dqy、.dsk、.dsn、.dtsx、.dxl、.eco、.ec

為 GosSOPKA 準備資料

您可以使用 kata-alert-export 實用程式取得 NDR 偵測資料和事件資料，其格式可匯入 GosSOPKA 系統。該實用程式包含在 Kaspersky Anti Targeted Attack Platform 分發套件中。

對於每個 NDR 偵測或事件，該實用程式會建立單獨的 XML 1.0 檔案 (UTF-8)，其中包含指定時間段內有關此偵測或事件的資訊。

為 GosSOPKA 準備偵測資料

要準備要傳送給 GosSOPKA 的偵測資料，您只需執行該實用程式。

為 GosSOPKA 準備 NDR 事件資料

準備要傳送到 GosSOPKA 系統的 NDR 事件資料涉及以下步驟：

1. 在 Kaspersky Anti Targeted Attack Platform Web 介面中建立連線器。

   建立一個一般類型的連線器並保存其通信封包。

   如果您使用分散式解決方案或多組織用戶模式，則在建立連線器的說明的步驟 4c 中，您需要指定您要從其接收資料的 PCN 或 SCN 伺服器的 IP 位址。如果您想從多個 Central Node 伺服器接收資料，則必須為每個伺服器建立一個連線器。

   如果 Central Node 元件被部署為叢集，則可以在建立連線器時輸入叢集中任意伺服器的 IP 位址。

2. 執行該實用程式。

   在建立連線器的說明的第 4c 步驟中建立連線器時指定的 IP 位址的 Central Node 伺服器上執行該實用程式。

記錄 NDR 偵測和事件資料時涉及的特殊注意事項

聚合警示被指定為根據 EXT 掃描結果註冊的事件所建立之警示的掃描技術。

執行用於準備 GosSOPKA 資料的實用程式

要執行為 GosSOPKA 準備資料的實用程式：

1. 將 gossopka_alert_exporter.tar.gz 檔案放在您想要取得資料的 Central Node 伺服器上。

2. 透過 SSH 或終端登入相關 Central Node 伺服器的管理主控台。

3. 系統提示時，請輸入管理員使用者名稱和在安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。

4. 在應用程式管理員功能表中，選擇**技術支援模式**。

5. 按下 **Enter**。

   這將開啟技術支援模式確認視窗。

6. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按 **ENTER**。

7. 執行以下指令：

   ```
   sudo -i
   ```

8. 解壓縮該實用程式的壓縮檔案：

   ```
   tar -xzvf gossopka_alert_exporter.tar.gz
   ```

9. 如果要獲取警示訊息，請執行以下命令：

   ```
   python3 export_main.py -s <yyyy-mm-ddThh:mm:ss> -b <yyyy-mm-ddThh:mm:ss>
   ```

10. 如果要獲取 NDR 警示和事件資訊，請執行以下命令：

    ```
    python3 export_main.py -s <yyyy-mm-ddThh:mm:ss> -b <yyyy-mm-ddThh:mm:ss> -c <通信封包路徑>
    ```

該實用程式已執行。

您也可以為此命令指定一個或多個參數（請參閱下表）。

實用程式命令列選項描述

必需的參數	參數	敘述
否	`--help`	幫助頁面。
否	`-m <id>`	供應商 ID (module_id)。 預設值為 `50`。在執行該實用程式之前，您需要聯絡 GosSOPKA 中心以取得分配給卡巴斯基的最新 ID。
是	`-s <yyyy-mm-ddThh:mm:ss>`	您想要獲取資訊的時間段的開始時間。
是	`-b <yyyy-mm-ddThh:mm:ss>`	您想要獲取資訊的時間段的結束時間。
否	`-o <目錄路徑>`	儲存檔案的目錄路徑。 預設值為 `/tmp`。
是的，如果您想取得 NDR 事件資料	`-c <通信封包的名稱，包括副檔名>`	建立連線器時所取得的通信封包的檔案名稱（含副檔名）。
是的，如果您想取得 NDR 事件資料	`-p <通信封包的密碼>`	建立連線器時指定的通信封包的密碼。
否	`-z<UTC 偏移量（分钟）>`	與 UTC 時區的偏移量（以分鐘為單位）。 預設值為 180（+3 小時）。
使用以下選項執行該實用程式的範例命令： `python3 export_main.py -s 2025-01-01T00:00:00 -b 2025-05-23T00:00:00 -c test.zip -o /home/administrator/export`		

該實用程式將以下檔案放置在選定的目錄中：

- Alert<偵測 ID>.xml.
- Event<事件 ID>.xml.

為每個偵測或事件建立一個單獨的檔案。如果目錄中已經包含同名檔案，則會被覆寫。

傳送通知

具有**管理員**、**資深安全員**或**安全官**角色的使用者可以設定將通知轉送到一個或多個電子郵件信箱。

您可以建立有關警示和系統運作狀況的通知。

通知包含應用程式 Web 介面的連結。確保分配給 Central Node 伺服器以供 DNS 伺服器使用的名稱正確，並且可以由 DNS 伺服器進行解析。如果名稱不正確或 DNS 伺服器無法對其進行解析，則通知中的 Web 介面連結將無法運作。

具有**安全稽核員**角色的使用者可以檢視用於傳送通知的規則清單、所選規則的屬性以及郵件伺服器連線設定，但無法編輯它們。

為了將通知正確傳送到電子郵件信箱，您必須先設定與郵件伺服器的連線。連線必須由**管理員**設定。

檢視傳送通知的規則表

傳送通知的規則顯示在應用程式 Web 介面視窗中的**設定**部分、**通知**子部分中。

用於傳送通知的規則表包含以下資訊：

- **類型**是用於傳送通知的規則類型。

  以下類型的規則是可能的：

  - **偵測**是用於傳送有關偵測的通知的規則。
  - **元件健康**是一個用於傳送有關應用程式元件操作的通知的規則。
- **主旨**—包含通知的訊息的主旨。
- **到**—傳送通知的電子郵件信箱。
- **狀態**—傳送通知的規則的狀態。

建立傳送有關偵測的通知的規則

若要建立傳送有關警示的通知的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。
2. 前往**通知規則**索引標籤。
3. 點擊**新增**。

   這將開啟**新規則**視窗。

4. 在**到**欄位中，輸入您想要向其傳送通知的一個或多個電子郵件信箱。

   如果用逗號分隔，可以輸入多個電子郵件信箱。

5. 在**主旨**欄位中，輸入通知訊息的主旨。

6. 如果您要讓應用程式將警示重要性插入郵件主旨，請將`%importance%`巨集新增至**主旨**欄位中。

7. 在“**通知類型**”欄位中，選擇“**偵測**”。

8. 在**偵測重要性**下拉清單中，選擇您想要傳送通知的最低警示重要性。

   例如，您可以設定僅轉發其警示具有高度重要性，或其警示具有中度或高度重要性的通知。

9. 如果要傳送有關與特定來源或目的地 IP 位址或子網路位址關聯的警示的通知，請在**來源或目的地**欄位中輸入 IP 位址和網路遮罩。

10. 如果要傳送有關與特定電子郵件傳送人或收件人位址關聯的警示的通知，請在**電子郵件**欄位中輸入電子郵件信箱。

11. 如果您想要傳送有關特定技術產生的警示的通知，請在**元件**下面選擇一種或多種技術名稱旁的核取方塊。

12. 點擊**新增**。

傳送有關警示通知的規則將被新增到規則清單中。若要將通知傳送到指定的電子郵件信箱，您必須啟用通知規則。通知將被傳送到為此規則配置的每個電子郵件信箱一次。

具有**管理員**和**安全稽核員**角色的使用者無法建立傳送警示通知的規則。

在分佈式解決方案模式下，您必須為每個下級伺服器（*次要 Central Node*，*SCN*）單獨建立通知。

建立用於傳送有關應用程式元件操作的通知的規則

若要建立用於傳送有關應用程式元件操作的通知的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 點擊**新增**。

   這將開啟**新規則**視窗。

4. 在**到**欄位中，輸入您想要向其傳送通知的一個或多個電子郵件信箱。

   如果用逗號分隔，可以輸入多個電子郵件信箱。

5. 在**主旨**欄位中，輸入通知訊息的主旨。

6. 如果您要讓應用程式將警示重要性插入郵件主旨，請將`%importance%`巨集新增至**主旨**欄位中。

7. 在**通知類型**欄位中，選擇**元件健康**。

8. 在**元件**下面，選擇您想要接收通知的應用程式功能區域名稱旁邊的核取方塊。

9. 點擊**新增**。

   傳送有關應用程式元件運行通知的規則會被新增到規則清單中。若要將通知傳送到指定的電子郵件信箱，您必須啟用通知規則。通知將被傳送到為此規則配置的每個電子郵件信箱一次。

具有**安全稽核員**角色的使用者無法建立用於傳送有關應用程式操作的通知的規則。

在分佈式解決方案模式下，通知是為每個下級伺服器（*次要 Central Node*，*SCN*）單獨配置的。

啟用和停用傳送通知的規則

若要啟用或停用傳送有關警示的通知的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 在**狀態**欄中，使用規則旁的切換開關啟用或停用傳送通知的規則。

   傳送有關警示通知的規則的狀態將被修改。

具有**安全稽核員**角色的使用者無法啟用或停用通知規則。

修改傳送通知的規則

若要編輯傳送通知的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 在傳送通知的規則清單中，選擇您要修改的規則。
   這會開啟**編輯規則**視窗。

4. 進行相關變更。

5. 點擊**儲存**。

   傳送通知的規則將被修改。

> 具有**安全稽核員**角色的使用者無法編輯傳送通知的規則。

刪除傳送通知的規則

若要刪除傳送通知的規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 選擇您要刪除的每個規則的名稱左側的核取方塊。
   如果您想要刪除所有規則，請選擇清單上方的核取方塊。

4. 點擊視窗下部的**刪除**。

5. 在確認視窗中，點擊**是**。

   所選檔案將被刪除。

> 具有**安全稽核員**角色的使用者無法刪除傳送通知的規則。

依規則類型篩選和搜尋通知轉送規則

若要依規則類型篩選或搜尋通知規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 點擊規則表中的⬚圖示以傳送通知。
   這將開啟篩選配置視窗。

4. 選擇以下選項之一：

- **所有**。
- **警示**。
- **元件健康**。

通知轉送規則表格將僅顯示與您設定的篩選條件相符的規則。

> 您可以同時使用多個篩選器。

根據通知主旨篩選和搜尋通知轉發規則

若要依通知主旨篩選或搜尋通知規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。
2. 前往**通知規則**索引標籤。
3. 點擊**主旨**連結以開啟篩選配置視窗。
4. 輸入通知主旨的一個或多個字元。
5. 點擊**套用**。

   篩選配置視窗關閉。

   通知轉送規則表格將僅顯示與您設定的篩選條件相符的規則。

> 您可以同時使用多個篩選器。

按電子郵件信箱篩選並搜尋通知轉送規則

若要按目標電子郵件信箱篩選或搜尋通知規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。
2. 前往**通知規則**索引標籤。
3. 點擊**到**連結以開啟篩選配置視窗。

4. 輸入電子郵件底子的一個或多個字元。

5. 點擊**套用**。

通知轉送規則表格將僅顯示與您設定的篩選條件相符的規則。

您可以同時使用多個篩選器。

根據狀態篩選和搜尋通知轉送規則

若要依狀態篩選或搜尋通知規則：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 點擊**狀態**連結以開啟篩選配置視窗。

4. 選擇狀態值旁邊的一個或多個核取方塊：

   - **已啟用**。

   - **已停用**。

5. 點擊**套用**。

篩選配置視窗關閉。

通知轉送規則表格將僅顯示與您設定的篩選條件相符的規則。

您可以同時使用多個篩選器。

清除通知轉送規則篩選器

若要清除一個或多個篩選條件的通知規則篩選器：

1. 在應用程式 Web 介面的主視窗中，選擇**設定**部分的**通知**子部分。

2. 前往**通知規則**索引標籤。

3. 點擊您想要清除其篩選條件的通知轉送規則表列標題右側的 ⊠。

> 如果要清除多個篩選條件，請執行必要的操作以清除每個篩選條件。

選定篩選器將會被清除。

通知轉送規則表格將僅顯示與您設定的篩選條件相符的規則。

管理日誌

本節包含有關管理 Kaspersky Anti Targeted Attack Platform 日誌的資訊。

在 Kaspersky Anti Targeted Attack Platform Web 介面中，您可以管理以下日誌：

- 使用者活動日誌。具有**管理員**角色的使用者可以管理日誌。具有**安全稽核員**角色的使用者可以下載日誌。
- NDR 功能的使用者活動記錄。具有**管理員**角色的使用者可以管理日誌。具有**安全稽核員**角色的使用者可以檢視日誌。

管理應用程式使用者活動日誌

應用程式 Web 介面中的某些使用者操作可能會導致 Kaspersky Anti Targeted Attack Platform 執行錯誤。您可以在應用程式 Web 介面中啟用使用者操作資訊的記錄，並在必要時透過下載日誌檔案檢視資訊。

有關 Sandbox 元件的 Web 介面和 Sensor 元件的管理員選單中的使用者操作的資訊都記錄在 Sandbox 和 Sensor 日誌中。

啟用和停用在活動日誌中記錄訊息

若要啟用或停用將 Kaspersky Anti Targeted Attack Platform Web 介面中的使用者操作資訊記錄到活動日誌中：

1. 選擇應用程式 Web 介面中的“**日誌**”部分的“**使用者活動**”子部分。
2. 執行以下操作之一：
   - 如果您想要啟用記錄有關使用者在應用程式 Web 介面中的操作的資訊，請設定“**事件記錄**”切換開關至“**已啟用**”位置。
   - 如果您想要停用記錄有關使用者在應用程式 Web 介面中的操作的資訊，請設定“**事件記錄**”切換開關至“**已停用**”位置。

     預設情況下啟用此功能。

有關使用者操作的資訊記錄在 user_actions.log 檔案中，該檔案儲存在 Central Node 伺服器的 /data/storage/volumes/siem_proxy/log-user-actions/ 目錄中。預設情況下，此文件中的記錄將保留 90 天，之後將被刪除。

若要檢視活動日誌記錄，您需要下載 user_actions.log 檔案。

您可以設定將應用程式 Web 介面中的使用者活動資訊記錄到遠端日誌。遠端日誌被儲存到安裝了 SIEM 系統的伺服器上。必須配置與 SIEM 系統的整合設定以寫入到遠端日誌。

在分佈式解決方案模式中，有關應用程式 Web 介面中的使用者操作的資訊記錄在使用者管理 Web 介面的相同伺服器的日誌中。有關影響 SCN 伺服器設定的 PCN 伺服器使用者操作的資訊記錄在 PCN 伺服器日誌中。

具有**安全稽核員**角色的使用者只能檢視用於將資訊記錄到活動日誌的設定。

下載活動日誌檔案

若要下載活動日誌檔：

1. 選擇應用程式 Web 介面中的"**日誌**"部分的"**使用者活動**"子部分。
2. 點擊**下載**。

該檔案將被保存到您本機的瀏覽器下載資料夾中。檔案以 ZIP 壓縮檔案形式下載。

在分佈式解決方案模式下，您只能下載在其 Web 介面中管理的伺服器的日誌檔案。

應用程式使用者活動日誌中的記錄

每個訊息的標題包含以下資訊：

- 格式化版本。
  目前版本號：`0`。目前欄位值：`CEF:0`。
- 供應商。
  目前欄位值：`AO Kaspersky Lab`。
- 應用程式名稱。
  目前欄位值：`Kaspersky Anti Targeted Attack Platform`。
- 應用程式版本
  目前欄位值：7.1.1.531。
- 事件類型。
  見下表。
- 活動名稱。
  見下表。
- 事件重要性。

目前欄位值：低。

範例：
```
CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|7.1.1.531|tasks|Managing tasks|Low|
```

CEF 訊息的所有欄位都具有“<金鑰>=<值>”格式。金鑰以及訊息中包含的值顯示在下表中。

事件類型	事件名稱和說明	關鍵及其價值描述
alerts	在警示上執行的使用者操作 警示操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。 • cs1label = <指派了警示的使用者>。 • externalId = <警示 ID>。
ep	管理具有 Endpoint Agent 元件的主機 對安裝了 Endpoint Agent 元件的主機所進行的操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。 • cs1label = <具有 Endpoint Agent 元件的主機的名稱>。
storage	管理儲存和隔離區中的物件 對儲存區和隔離區中物件進行的操作	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。 • cs1label = <放置在儲存區或隔離區中的檔案的名稱>。
sensors	管理 Sensor 元件 將 Sensor 元件連線到 Central Node 伺服器，修改元件設定。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
sb	配置與 Sandbox 元件的整合 將 Sandbox 元件連線到 Central Node 伺服器。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
ex_integration	配置與外部系統的整合 配置與外部系統的整合。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
ksn_kpsn_mdr	參與 KSN、KPSN 和 MDR 配置參與卡巴斯基安全網路、啟用或停用卡巴斯基私人安全網路的使用以及配置與 Kaspersky Managed Detection and Response 的整合。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
yara	管理 YARA 規則 YARA 規則操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。 • cs1label = <被上傳檔案的名稱>。
ioc	管理入侵指標	• dvchost = <Central Node 的主機

事件類型	事件名稱和說明	關鍵及其價值描述
	IOC 規則操作。	名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
ids	管理 IDS 規則 IDS 規則操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
taa	管理 TAA 規則 TAA (IOA) 規則操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
sb_rules	管理 Sandbox 規則 使用 Sandbox 規則的操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
prevention	管理防護規則 防護規則操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
exclusions	管理掃描排除項目 掃描排除規則操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
tasks	管理工作 工作操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
network_isolation	Endpoint Agent 主機的網路隔離 Endpoint Agent 主機的網路隔離。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
settings	設定 修改 Central Node 伺服器設定	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。 • src = <使用者的 IP 位址>。 • suser = <使用者名稱>。 • cs1 = <事件類型>。
vip	管理分配 VIP 狀態的規則 為警示指派 VIP 狀態的規則操作。	• dvchost = <Central Node 的主機名稱>。 • eventId = <事件 ID>。 • rt = <事件日期和時間>。

事件類型	事件名稱和說明	關鍵及其價值描述
		• `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。
`report`	管理報告 報告操作。	• `dvchost` = <Central Node 的主機名稱>。 • `eventId` = <事件 ID>。 • `rt` = <事件日期和時間>。 • `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。 • `cs1label` = <報告或報告範本的名稱>。
`mt`	管理 `CN`、`PCN` 和 `SCN` 伺服器 修改分散式解決方案和多組織用戶模式下主要 Central Node 和次要 Central Node 伺服器的設定。	• `dvchost` = <Central Node 的主機名稱>。 • `eventId` = <事件 ID>。 • `rt` = <事件日期和時間>。 • `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。
`user_account`	管理使用者帳戶 對使用者帳戶的操作。	• `dvchost` = <Central Node 的主機名稱>。 • `eventId` = <事件 ID>。 • `rt` = <事件日期和時間>。 • `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。 • `cs1label` = <建立或編輯其帳戶的使用者的名稱>。 • `cn1` = <失敗的授權嘗試次數>。
	授權嘗試失敗次數已超出 授權嘗試失敗次數超出限制。	
`notifications`	傳送通知 配置電子郵件通知。	• `dvchost` = <Central Node 的主機名稱>。 • `eventId` = <事件 ID>。 • `rt` = <事件日期和時間>。 • `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。
`license`	產品授權 管理產品授權金鑰。	• `dvchost` = <Central Node 的主機名稱>。 • `eventId` = <事件 ID>。 • `rt` = <事件日期和時間>。 • `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。
`system_health`	系統健康 檢查應用程式元件的健康狀況。	• `dvchost` = <Central Node 的主機名稱>。 • `eventId` = <事件 ID>。 • `rt` = <事件日期和時間>。 • `src` = <使用者的 IP 位址>。 • `suser` = <使用者名稱>。 • `cs1` = <事件類型>。 • `cs1label` = <元件物件>。 • `msg` = <檢查結果>。

如果同時對超過 30 個物件執行某項操作，則僅記錄該操作的一項。該條目包括有關操作的資訊以及執行該操作的物件的數量。

管理 NDR 使用者活動日誌

本節包含有關管理 NDR 功能日誌的資訊。

具有“**管理員**”角色的使用者可以管理記錄。具有“**安全稽核員**”角色的使用者可以檢視記錄。

使用任何類型的 Kaspersky Anti Targeted Attack Platform 產品授權金鑰時均可使用日誌。

管理日誌儲存設定

您可以編輯 Central Node 資料庫中日誌記錄儲存的設定。

若要變更日誌儲存設定：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇“**Sensor 伺服器**”部分。
3. 選擇 Central Node 伺服器的卡。
   詳細資訊區域顯示在 Web 介面視窗的右側。
4. 點擊“**編輯**”。
   在詳細資料區域，會顯示頁簽，您可以在其中管理伺服器的設定。
5. 在“**一般**”索引標籤的“**事件**”、“**稽核項目**”和“**應用程式訊息**”部分中配置下列設定：
   a. 使用“**最大磁碟區**”設定來設定儲存記錄的大小限制。您可以選擇該值的計量單位：**MB** 或 **GB**。
      編輯此設定時，請記住指定磁碟區的預計最大記錄數。您還需要考慮到所有大小限制的總和不得超過節點指定的最大儲存容量。
   b. 如有必要，請使用“**儲存時間（天）**”設定來限制記錄的儲存時間，並以天為單位指定時間。
6. 點擊**儲存**。

日誌儲存已配置。

啟用和停用使用者活動稽核

您可以啟用或停用 NDR 功能的使用者活動稽核。

使用者活動稽核預設啟用。

若要啟用或停用使用者活動稽核：

1. 利用管理員帳戶登入應用程式 Web 介面。
2. 轉至“**日誌**”部分，“**稽核**”子部分。
3. 使用工具列中的**使用者活動稽核**開關啟用或停用使用者活動稽核。
4. 等待變更得到套用。直到轉換至另一狀態完成之後，開關才會再次可用。

使用者活動稽核已啟用或停用。

檢視使用者活動稽核記錄

Kaspersky Anti Targeted Attack Platform 可以儲存有關 NDR 功能使用者執行的操作的資訊。如果啟用了使用者活動稽核，資訊將儲存在稽核日誌中。

您可以在使用 Web 介面連線到 Central Node 伺服器時檢視稽核記錄。如果需要，您也可以設定稽核記錄透過連線器傳送到第三方系統。

只有具有管理員角色的使用者才能檢視稽核記錄。

若要檢視稽核記錄：

1. 使用 Web 介面連線到 Central Node 伺服器。
2. 選擇**日誌**區段、**稽核**子區段。

   此表顯示符合指定篩選和搜尋條件的稽核記錄。

稽核記錄設定顯示在表格以下列中：

- **日期和時間**。
  記錄使用者活動資訊的日期和時間。
- **操作**。
  已註冊的使用者執行的操作。
- **結果**。
  已註冊操作的結果（成功或不成功）。
- **使用者**。
  執行註冊操作的使用者的名稱。
- **使用者節點**。
  執行註冊操作的節點的 IP 位址。
- **敘述**。
  有關註冊操作的其他資訊。

檢視稽核記錄表時，您可以使用設定、篩選、搜尋和排序功能。

設定追蹤日誌的最大儲存空間限制

有關 NDR 功能效能的資訊記錄在追蹤日誌中。您可以限制這些日誌所佔用的儲存空間。在這種情況下，當達到限制時，舊的追蹤記錄檔案將從 `/var/log/kaspersky` 目錄中刪除。

具有**管理員**角色的使用者可以管理日誌儲存。具有**安全稽核員**角色的使用者可以檢視這些設定。

要限制追蹤日誌佔用的空間量：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
3. 點擊相關 Sensor 元件的卡片。
4. 這將開啟一個視窗，其中包含有關元件的資訊。
5. 點擊“**編輯**”。
6. 轉到“**一般**”索引標籤。
7. 在**追蹤資料**欄位中，使用**最大容量**設定來設定記錄可佔用的最大空間。您可以選擇該值的計量單位：**MB** 或 **GB**。

追蹤日誌佔用的空間有限。

設定追蹤日誌的最大儲存空間限制

統計日誌記錄 NDR 功能的指標，例如接收到的網路封包的數量。您可以限制這些日誌所佔用的儲存空間。在這種情況下，達到限制時，舊的統計記錄檔案會從 `/var/log/kaspersky` 目錄中刪除。

具有**管理員**角色的使用者可以管理日誌儲存。具有**安全稽核員**角色的使用者可以檢視這些設定。

要限制統計日誌佔用的空間量：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
3. 點擊相關 Sensor 元件的卡片。
4. 這將開啟一個視窗，其中包含有關元件的資訊。
5. 點擊“**編輯**”。
6. 轉到“**一般**”索引標籤。
7. 在**統計資料**欄位中，使用**最大容量**設定來配置記錄可以佔用的最大空間。您可以選擇該值的計量單位：**MB** 或 **GB**。

統計日誌佔用的空間有限。

Sensor 使用者活動日誌。

元件的管理員選單中的使用者操作資訊會記錄在 Sensor 使用者活動記錄 (admin_menu.log) 中。

您可以按照*下載 Kaspersky Anti Targeted Attack Platform 記錄*章節中的說明，下載 Sensor 使用者活動記錄檔案。依照說明的步驟操作後，將在您選擇的目錄中產生一個名為 collect--<壓縮檔案下載日期>.tar.gz 的壓縮檔案。您可以在 /var/log/kaspersky/admin_menu/ 目錄中的此壓縮檔案中找到 Sensor 使用者活動日誌 (admin_menu.log)。

Sensor 元件管理員功能表中使用者操作的記錄

Sensor 元件的管理員選單中的使用者操作日誌(admin_menu.log) 中的記錄會依等級分組。

INFO 層級的記錄追蹤有關元件管理員選單中的使用者操作的資訊。

INFO 層級的事件記錄範例：

```
June 18 20:45:46 1 admin-menu - INFO Menu item pressed label=[Example ...]
```

WARNING 層級的記錄追蹤有關由於在 INFO 層級記錄的操作而發生的事件的資訊。此層級的資訊具有 CEF 訊息的格式。

每個訊息的標題包含以下資訊：

- 格式化版本。

  目前版本號：`0`。目前欄位值：`CEF:0`。

- 供應商。

  目前欄位值：`AO Kaspersky Lab`。

- 應用程式名稱。

  目前欄位值：`Kaspersky Anti Targeted Attack Platform`。

- 應用程式版本

  目前欄位值：7.1.1.531。

- 事件類型。

  見下表。

- 活動名稱。

  見下表。

- 事件重要性。

  目前欄位值：低。

  訊息頭範例：

  ```
  CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|7.1.1.531|user_account|Managing user
  accounts|Low|
  ```

CEF 訊息的所有欄位都具有“<金鑰>=<值>”格式。金鑰以及訊息中包含的值顯示在下表中。

事件類型	事件名稱和說明	關鍵及其價值描述
sensors	管理 Sensor 元件 伺服器管理，修改元件設定。	• dvchost =<具有 Sensor 元件的伺服器名稱>。 • eventId =<事件 ID>。 • rt =<事件日期和時間>。 • src =<使用者的 IP 位址>。 • suser =<使用者名稱>。 • cs1 =<事件類型>。
settings	設定 變更伺服器日期和時間設定，管理日誌。	• dvchost =<具有 Sensor 元件的伺服器名稱>。 • eventId =<事件 ID>。 • rt =<事件日期和時間>。 • src =<使用者的 IP 位址>。 • suser =<使用者名稱>。 • cs1 =<事件類型>。
user_account	管理使用者帳戶 變更管理員帳號的密碼，開始和結束使用者工作階段，進入技術支援模式。	• dvchost =<具有 Sensor 元件的伺服器名稱>。 • eventId =<事件 ID>。 • rt =<事件日期和時間>。 • src =<使用者的 IP 位址>。 • suser =<使用者名稱>。 • cs1 =<事件類型>。

Sandbox 日誌

Sandbox 元件記錄兩種類型的資訊：

- 系統日誌記錄了 Sandbox 中事件的詳細資訊。
- 使用者活動日誌記錄了 Sandbox 使用者在 Web 介面中的操作資訊。

您可以下載系統日誌和使用者活動日誌。

下載 Sandbox 系統日誌

Sandbox 系統日誌中的資訊以純文字形式儲存。儲存的資料涵蓋了過去 7 天。

要下載 Sandbox 系統日誌：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。
2. 在**系統日誌**設定群組中，點擊**下載**按鈕。

   下載可能會有一些延遲。等待檔案開始下載，不要重新整理頁面或再次點擊**下載**按鈕。下載 Sandbox 系統日誌可能需要很長時間。

   該檔案將被保存到您本機的瀏覽器下載資料夾中。

下載 Sandbox 使用者活動日誌

使用者活動日誌記錄了使用者在 Sandbox 網頁介面中的操作資訊。預設情況下，日誌中的資料保留 90 天。

若要下載 Sandbox 使用者活動日誌：

1. 在 Sandbox Web 介面視窗中，選擇**管理**部分。
2. 在“**使用者活動日誌**”下，點擊“**下載**”按鈕。

   user_actions.log 檔案將被保存到您本機的瀏覽器下載資料夾中。

應用程式使用者活動日誌中的記錄

Sandbox 使用者活動日誌中的記錄具有 CEF 格式（CEF 訊息）。透過檢視日誌記錄，您可以了解由於使用者操作而發生的事件。

```
安裝虛擬機映像的記錄範例：
CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform (Sandbox)|7.1.0.530|vm|Managing virtual
machines|Low| dvs=<IP> deviceExternalId=ubuntu-server eventId=1965096788380487496 rt=Apr 25 2025 04:59:16 src=<IP>
suser=admin cs1=installing the default image cs1label=CentOS7_x64-1.0.0.19888
```

上面的範例包含三組欄位：

- `CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform (Sandbox)|7.1.0.530|vm|Managing virtual machines|Low|` — 標題欄位。
- `dvs=<IP> deviceExternalId=ubuntu-server eventId=1965096788380487496 rt=Apr 25 2025 04:59:16 src=<IP> suser=admin cs1=installing the default image` — 所有記錄通用的 CEF 訊息本文欄位。
- `cs1label=CentOS7_x64-1.0.0.19888` — 具有物件之操作特有的欄位。例如，“安裝虛擬機映像”操作的物件是虛擬機映像，而 `cs1label` 欄位包含此映像的名稱。

標題欄位

每個訊息的標題包含以下資訊：

- 格式化版本。

  目前版本號：`0`。目前欄位值：`CEF:0`。
- 供應商。

  目前欄位值：`AO Kaspersky Lab`。
- 應用程式名稱。

  目前欄位值：`Kaspersky Anti Targeted Attack Platform`。
- 應用程式版本

  目前欄位值：7.1.1.531。
- 事件類型。

可以包含以下值之一：

- `user_account`
  與 Sandbox 使用者帳戶相關的事件。
- `settings`
  與 Sandbox 設定相關的事件。
- `kata`
  與 Sandbox 和 Central Node 之間的連線相關的事件。
- `vm`
  與 Sandbox 中部署的作業系統虛擬映像相關的事件。

- 標題中指定的事件名稱。
  可以包含以下值之一：
  - 管理使用者帳戶
    對使用者帳戶的操作。屬於 `user_account` 類型。
  - 授權嘗試失敗次數已超出
    授權嘗試失敗次數超出限制。屬於 `user_account` 類型。
  - 設定
    編輯 Sandbox 伺服器設定屬於設定類型。
  - 配置與 `KATA Central Node` 的整合
    配置與 Central Node 的整合。屬於 `kata` 類型。
  - 管理虛擬機
    使用虛擬機的操作。屬於 `vm` 類型。
- 事件重要性。
  目前欄位值：低。

所有事件通用的欄位

CEF 訊息的欄位具有“<金鑰>=<值>”格式。每個 CEF 訊息包含以下欄位：

- `dvs`
  Sandbox 伺服器的 IP 位址。
- 裝置外部 `ID`
  Sandbox 伺服器名稱。
- `eventId`
  事件 ID。

- `rt`
  事件日期和時間。
- `src`
  執行操作的使用者的 IP 位址。
- `suser`
  執行操作的使用者的名稱。
- `cs1`
  事件（見下表）。

事件的特殊欄位

事件和特殊欄位

cs1 欄位中指定的事件	特殊事件欄位
管理使用者帳戶	
變更管理員密碼	`cs1label` 密碼被變更的使用者的名稱。
登入	`cs1label` 授權的使用者的名稱。
登出	`cs1label` 結束工作階段的使用者的姓名。
授權嘗試失敗次數已超出	

授權嘗試失敗的次數	`cs1label`
	授權嘗試失敗所涉及的使用者名稱。
	`cn1`
	授權嘗試失敗的次數。

設定	
• 指派 DNS 伺服器使用的伺服器名稱 • 配置 DNS 設定 • 設定管理介面的設定 • 配置已處理物件進行網際網路存取的網路介面的設定 • 配置路由設定 • 設定代理伺服器連線設定 • 配置伺服器上的日期和時間 • 配置伺服器上的時區 • 配置與 NTP 伺服器的同步	`cs1label` 已變更設定的伺服器的名稱。
• 儲存配置 • 還原配置	`cs1label` 已儲存或還原設定的伺服器的名稱。
• 重新啟動伺服器 • 關閉伺服器	`cs1label` 重新啟動或關閉的伺服器的名稱。
• 下載記錄 • 下載使用者操作日誌	`cs1label` 下載日誌檔案的伺服器的名稱。
• 選擇資料庫更新來源 • 手動更新資料庫	`cs1label` 更新防毒資料庫或變更資料庫更新來源的伺服器的名稱。

cs1 欄位中指定的事件	特殊事件欄位
設定虛擬機的最大數量	`cs1label` 指定的虛擬機數量。
• 啟用授權嘗試失敗次數計數 • 停用授權嘗試失敗次數計數	`cs1label` 啟用或停用授權嘗試失敗次數計數的伺服器的名稱。

修改授權嘗試失敗次數的計數週期	`cs1label`
	變更授權嘗試失敗次數計數週期的伺服器的名稱。
	`cn1`
	計算授權嘗試失敗次數的分鐘數。

變更使用者工作階段鎖定時間	`cs1label`
	變更了使用者不活動最長持續時間的伺服器的名稱。
	`cn1`
	非活動使用者工作階段的最長持續時間（分鐘）。

配置與 KATA Central Node 的整合	
• 接受與 `KATA Central Node` 的連線 • 拒絕與 `KATA Central Node` 的連線 • 刪除與 `KATA Central Node` 的連線	`cs1label` 發起連線請求的 Central Node 的指紋。
管理虛擬機	
• 匯入預設映像 • 刪除預設映像 • 解壓縮預設映像	`cs1label` 正在上傳或刪除的虛擬機映像檔案的名稱。
• 安裝預設映像 • 刪除從預設映像部署的虛擬機 • 取消預設映像安裝	`cs1label` 已部署、刪除或取消安裝的虛擬機映像的名稱。
• 上傳 `ISO` • 刪除 `ISO`	`cs1label` 已上傳或刪除的 ISO 映像的名稱。
• 建立自訂範本 • 匯入自訂範本 • 匯出自訂範本 • 啟用自訂範本 • 停用自訂範本 • 停止自訂範本 • 刪除自訂範本	`cs1label` 已建立、匯入、匯出、啟用、停用、停止或刪除的自訂虛擬機範本的名稱。
• 下載 `manifest` 檔案 • 上傳調試符號	沒有特殊欄位。

• 將 `ISO` 掛載到自訂範本
• 從自訂範本卸載 `ISO`
	`cs1label`
	掛載了 ISO 映像或卸載了 ISO 映像的自訂虛擬機範本的名稱。
	`cs2label`
	已掛載或解除安裝的 ISO 映像的名稱。

• 從自訂範本建立自訂虛擬機 • 刪除自訂虛擬機 • 將自訂虛擬機狀態變更為“線上” • 將自訂虛擬機狀態變更為“已啟用”	`cs1label` 從自訂映像部署、已刪除或狀態已變更的虛擬機的名稱。

如果同時對超過 30 個物件執行某項操作，則僅記錄該操作的一項。該條目包括有關操作的資訊以及執行該操作的物件的數量。

下載 Kaspersky Anti Targeted Attack Platform 日誌

如果需要，您可以下載 Kaspersky Anti Targeted Attack Platform 的系統日誌檔案。為此，您必須使用 Kata-collect 指令碼來取得有關應用程式操作的資訊。

使用 Kata-collect 指令碼取得有關應用程式操作的資訊。

1. 登入您要透過 SSH 或終端取得資訊的伺服器的管理主控台。

   如果您在分散式解決方案和多組織用戶模式下使用 Kaspersky Anti Targeted Attack Platform，您需要在每部 Central Node 伺服器上執行這些步驟。如果您組織的基礎架構中有單獨安裝的 Sensor 元件，您也必須在具有此元件的伺服器上執行這些步驟。如果應用程式是以叢集形式部署，您必須在 Docker swarm 中具有"管理者"角色的其中一部伺服器上執行這些步驟。若要檢視伺服器的角色，請使用 `$ docker node ls` 指令。

2. 系統提示時，輸入管理員使用者名稱和安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。

4. 按下 **Enter**。

   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按**Enter**。

6. 透過執行以下命令來運行指令碼：

   `sudo kata-run.sh kata-collect --output-dir <路徑>`

您也可以為此命令指定一個或多個參數（請參閱下表）。

kata-collect 實用程式的參數

必需的參數	參數	敘述
是	`--output-dir <路徑>`	在指定路徑建立目錄， 其中<路徑>是您要儲存包含下載資料的檔案的目錄的絕對路徑或相對路徑。 如果不指定路徑，資料壓縮檔案預設會儲存在 /tmp/collect 目錄中。
否	`--no-prometheus`	跳過準備和傾印 prometheus 資料庫。 此參數顯著加快了指令碼的速度。
否	`--no-siem-logs`	跳過下載寫入 SIEM 系統的資料。
否	`--siem-logs-range-start <YYYY-MM-DD-HH>`	下載從該日期（含）開始寫入 SIEM 系統的資料。
否	`--siem-logs-range-end <YYYY-MM-DD-HH>`	下載以此日期（含）結束的寫入 SIEM 系統的資料。

範例：
使用按日期篩選的 SIEM 系統資料且不使用 Prometheus 資料庫來獲取有關應用程式操作的資訊的命令：

```
sudo kata-run.sh kata-collect --output-dir <路徑> --no-prometheus --siem-logs-range-start<YYYY-MM-DD-HH> --siem-logs-range-end<YYYY-MM-DD-HH>
```

指令碼完成後，collect--<壓縮檔案下載日期>.tar.gz 壓縮檔案被儲存到指定目錄。此壓縮檔案包含應用程式的系統日誌檔案。

檢視應用程式訊息

應用程式的訊息日誌儲存有關 NDR 功能的錯誤以及Kaspersky Anti Targeted Attack Platform 的系統處理程序執行的操作的資訊。

您可以在 Web 介面中檢視應用程式訊息。如果需要，您也可以設定應用程式訊息透過連線器傳送到第三方系統。

具有以下角色的使用者可以檢視應用程式訊息：**管理員**、**安全稽核員**、**安全官**或者**資深安全員**。

要檢視應用程式訊息：

1. 使用應用程式管理員帳戶登入 Web 介面。
2. 選擇"**設定**"部分、"**應用程式訊息**"子部份。

   表格顯示符合指定篩選和搜尋條件的應用程式訊息。

應用程式訊息設定顯示在表格的以下列中：

- **日期和時間**。

  註冊應用程式訊息的日期和時間。

- **狀態**。

  訊息狀態的名稱。訊息可以具有以下狀態之一：

  - 資訊性訊息的*正常操作*。
  - 有關非關鍵應用程式錯誤的訊息包括"*未知*"、"*故障*"。
  - 有關應用程式故障的訊息包括"*中度故障*、*嚴重故障*"、"*致命故障*"。

- **節點**。

  訊息到達的節點的名稱或 IP 位址。

- **系統處理程序**。

  導致訊息被註冊的應用程式處理程序。

- **資訊**。

  訊息的數字識別碼和文字。

檢視應用程式訊息表時，您可以使用篩選、搜尋和排序功能。

配置 Kaspersky Anti Targeted Attack Platform 系統日誌和警示的保留期

您可以配置 Central Node 元件資料庫中部分日誌和警示資料的保留時間，以及 Sensor 和 Sandbox 日誌的保留時間。預設情況下，當某項特定技術的警示數量達到 1000000 時，Central Node 資料庫中的警示資料就會輪替。日誌的預設保留期為 90 天。

您可以在 Central Node 或 Sensor 元件的管理員選單中設定 Central Node 和 Sensor 元件的日誌保留。您可以使用作業系統的標準工具來設定 Sandbox 日誌的保留。

您可以配置以下日誌的保留期：

- Central Node 或 Sensor：
  - Syslog。
  - user_actions.log，Web 介面中使用者操作的日誌。
  - kern.log，作業系統的核心事件日誌。
  - auth.log，Web 介面和元件管理員選單中使用者授權的日誌。
- Sandbox：
  - apt-history.log，更新日誌。
  - apt-audit.log，系統事件稽核日誌。
  - user_actions.log，Web 介面中使用者操作的日誌。
  - auth.log，Web 介面和元件管理員選單中使用者授權的日誌。

要配置Central Node 或 Sensor 日誌的保留期，以及 Central Node 資料庫中警示資料的保留期：

1. 如果要配置 Central Node 元件資料庫中日誌和警示資料的保留期，請使用 SSH 或終端登入 Central Node 伺服器的管理主控台。
2. 如果要配置 Sensor 日誌的保留期，請使用 SSH 或終端登入 Sensor 伺服器的管理主控台。
3. 系統提示時，請輸入管理員使用者名稱和安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。
4. 選擇**程式設定**。
5. 按 **ENTER**。

   這將開啟**選擇操作**視窗。
6. 選擇**配置偵測和記錄的儲存期限**。
7. 按下 **Enter**。

   這將開啟**配置儲存期限**視窗。

8. 選擇**變更儲存期限**。

   這將開啟**儲存期限**視窗。

9. 在**儲存期限**欄位中，指定記錄保留期（以天為單位）。您可以指定的最大日誌保留期限為 10000 天。

   預設值是 90。

10. 選擇**套用變更**。

    這將開啟**套用儲存期限**視窗。

11. 在顯示的視窗中，選擇**確定**。

Central Node 或 Sensor 日誌的保留期以及警示資料的保留期（當 Central Node 設定發生變更時）已配置。

要變更 Sandbox 日誌的保留期：

1. 如果要變更 apt-audit.log、apt-history.log、user-actions.log 日誌的保留期，請以 root 身分開啟 /etc/logrotate.d/apt-audit 檔案進行編輯，並變更相關日誌的“rotate”設定。

2. 如果要變更 auth.log 的保留期，請以 root 身分開啟 /etc/logrotate.d/auth 檔案進行編輯，並變更“rotate”設定。

   您可以指定的最大日誌保留期限為 10000 天。預設情況下，日誌保留期為 90 天。

已配置 Sandbox 日誌的保留期限。

檢視已傳送至 Kaspersky Anti Targeted Attack Platform 進行掃描的檔案的資訊

如果有必要，您可以檢視該檔案是否已在 Kaspersky Anti Targeted Attack Platform 中掃描，以及掃描結果為何。為此，您必須使用 Kata-collect 指令碼來取得有關應用程式操作的資訊。

要使用 Kata-collect 指令碼取得有關應用程式效能的資訊：

請依照"*下載 Kaspersky Anti Targeted Attack Platform 日誌*"部分所給予的說明的步驟進行操作。

完成說明的步驟後，包含 Kaspersky Anti Targeted Attack Platform 日誌檔案的 collect--<壓縮檔案下載日期>.tar.gz 壓縮檔案被放置在指定目錄中。接收並掃描的檔案資訊包含在日誌中，該日誌位於此壓縮檔案內的 /logs/kaspersky/siem/log-history/ 目錄中。如果某個檔案被排除在掃描之外，則有關該檔案的資訊也會反映在日誌中。

您可以透過名稱或 MD5 雜湊值找到任何檔案。

如果該檔案是由 Sensor 元件取得的，您可以透過以下欄位找到它：

- 檔案來源資訊：
  - 如果檔案是從流量中取得的，則為來源 IP 位址和目標 IP 位址。
  - 如果檔案是透過電子郵件收到的，則為寄件者電子郵件信箱和收件者電子郵件信箱。
  - 如果檔案是從外部系統接收的，則為外部系統的 IP 位址和 ID。
  - 如果檔案是從 Endpoint Agent 主機接收的，則為主機的 IP 位址和名稱。
  - 如果檔案是手動上傳至 Kaspersky Anti Targeted Attack Platform 的，則為使用者帳戶名稱。
- 來源類型：span、smtp、icap、pop3、external（外部系統）、endpoint（Endpoint Agent 主機）、upload（手動上傳的檔案）。
- 對於電子郵件訊息，會記錄 Message-ID 欄位。

檔案資訊日誌記錄的特殊注意事項

在日誌中搜尋檔案資訊時，請牢記以下有關檔案資訊日誌記錄的特殊注意事項：

- 檔案資訊被記錄兩次：從流量中取得檔案時和掃描檔案時。如果 Sensor 元件與您的基礎架構中的 Central Node 分開安裝，則檔案接收記錄將轉到 Sensor 元件的日誌，而檔案掃描記錄將轉到 Sensor 連線的 Central Node 元件的日誌。如果 Central Node 元件和 Sensor 安裝在同一台伺服器上，則兩個記錄都會寫入 Central Node 日誌。
- 對於複合檔案（例如，壓縮檔案或電子郵件），如果子檔案被Kaspersky Anti Targeted Attack Platform 技術之一掃描，則會記錄父檔案的雜湊值以及子檔案的名稱和雜湊值。

檔案 MD5 雜湊值的 apt-history 日誌記錄範例

下表列出了檔案 MD5 雜湊值的 apt-history 日誌記錄範例。

檔案 MD5 雜湊值的 apt-history 日誌記錄範例

日誌記錄	值
2024-06-11 02:37:03.645586 info apt-history: f0429d4845208857cd303df968ef545e enqueued am, priority: normal	該檔案已被接收並利用惡意軟體防護引擎技術進行處理。
2024-06-11 02:37:03.647434 info apt-history: external KSMG sensor with ip 10.0.0.0 provide file with name: File_Name 2024/2025, md5: f0429d4845208857cd303df968ef545e, msg_id: <87c13e55e789aa966089b6bf2e8c453b@localhost.localdomain>	從 Kaspersky Secure Mail Gateway 和 Kaspersky Security for Linux Mail Server 接收並在 Kaspersky Anti Targeted Attack Platform 中處理的物件的字串。 值得關注的訊息： • 外部 KSMG 感應器，IP 為 10.0.0.0 — Kaspersky Secure Mail Gateway 伺服器的 IP 位址 • File_Name 2024/2025 — 檔案名 • md5 — 正在掃描的檔案的 MD5 雜湊值 • msg_id — 訊息 ID
2024-06-11 02:37:03.847696 info apt-history: f0429d4845208857cd303df968ef545e engine am result {verdict: CLEAN, bases_version: 202406071010, detect_time: 2024-06-11 02:37:03.841275, rescan_priority: 3, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, multitask_details: {priority: background, tasks: {pdf: 1}}, scanEngines: [sb]}	使用惡意軟體防護引擎技術處理物件的結果。包括掃描後分配給物件的狀態(CLEAN)以及有關將用於額外掃描物件的技術的資訊(“scanEngines: [sb]”)。 值得關注的訊息： • multitask_details — 掃描工作的詳細資訊 • priority — 掃描的優先順序 可能的值是“background”、“must” • scanEngines — 掃描技術 可能的值是[yr]（代表 YARA）和[sb]（代表 Sandbox）。
2024-06-11 02:37:03.886784 info apt-history: f0429d4845208857cd303df968ef545e enqueued sb: {pdf: 1}, priority: low, sb_priority: background	該工作已傳送至 Sandbox 元件進行處理。 值得關注的訊息： • {pdf: 1} — 傳送以掃描的物件數量和類型 • low — 處理優先順序 可能的處理優先順序值為“low”、“medium”、“high”。 • background — Sandbox 元件處理的佇列類型。 可能的值是“background”、“must”
2024-06-11 02:37:04.179597 info apt-history: f0429d4845208857cd303df968ef545e delivered to sb, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, node: Server_Name, mtask_id: 900	該工作已傳送至 Sandbox 元件進行處理。 值得關注的訊息： • node:Server_Name — 具有 Sandbox 元件的伺服器的名稱 • mtask_id: 900 — 工作 ID
2024-06-11 02:38:44.515070 info apt-history: f0429d4845208857cd303df968ef545e sb result received, sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, node: Server_Name, mtask_id: 900, priority: low	已收到 Sandbox 元件處理物件的結果。

2024-06-11 02:38:44.783370 info apt-history: f0429d4845208857cd303df968ef545e engine sb result {bases_version: 202406102122, detect_time: 2024-06-11 02:38:44.776655, verdict: SILENT, hidden: True, details: [{file: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf, images: [{verdicts_info: {ScannerVersion: 1.22.3.34, ...}, hidden: True, verdict: SILENT, sb_id: fb15ec106318b0d54babce2379d956f7, image: Win7_x64, task_id: task0, file: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf, file_id: 1, filesize: 445856, md5: 0d87eebc9676214f35046a482150e537, tracing_mode: all_events, store_artifacts: False, bases_version: 202406102122, ids_bases_version: 202406101817, version: 1.22.3.34, suspicious_log: [], network_activity: {http: [], dns: []}}], verdict: SILENT, hidden: True, priority: 150}], md5_list: [], file_list: [], sb_hash: 77f5b6276dd9b1c534b6c9adcff86845, sb_names_map: {0: {md5: , name: }, 1: {md5: 0d87eebc9676214f35046a482150e537, name: //[From WCR <test@mail.com>][Date 11 Jun 2024 03:51:21][Subj Company_Name 2024/2025]/WCR-form.pdf}, 2: {md5: 71072dd9a36d7ce560cebc533ecb3cad, name: }}}

Sandbox 元件對所有虛擬機上的物件進行處理的結果。

值得關注的訊息：

- verdict — 掃描檔案的結果。根據在所有虛擬機上掃描檔案的結果產生。對於結果為 SILENT 的偵測，不會在偵測資料庫中建立任何記錄。
- hidden: True — 具有此結果的物件不需要 Kaspersky Anti Targeted Attack Platform 模組進一步掃描。
- details — 有關掃描虛擬機中的物件的資訊。包括以下欄位：
  - file — 用於顯示的檔案的名稱 (WCR-form.pdf)。在此記錄中，欄位包含以下資訊：
  - From — 寄件者電子郵件信箱。
  - Date — 事件的日期和時間。
  - Subj — 郵件主旨。
  - images — 有關在虛擬機中掃描物件的資訊。
  - verdicts_info — 檔案掃描的結果。對於掃描物件的每個虛擬機來說可能都不同。
  - hidden: True — 具有此結果的物件不需要 Kaspersky Anti Targeted Attack Platform 模組進一步掃描。
  - verdict — 在虛擬機上掃描檔案的結果。對於結果為 SILENT 的偵測，不會在偵測資料庫中建立任何記錄。
  - image — 執行檔的映像。
  - filesize — 檔案的大小。
  - md5 — 檔案的 MD5 雜湊。
  - tracing mode: all_events — 檔案啟動後執行的操作的記錄。
  - suspicious log [] — 檔案執行的惡意操作的記錄。

	該欄位沒有值，因為該檔案沒有執行任何惡意操作。 • network activity — 由檔案發起的網路活動。 • http [] — 該檔案未發出任何 HTTP 請求。 • dns [] — 該檔案未發出任何 DNS 請求。 “suspicious log”和 “network activity” 欄位僅記錄惡意活動的事實。如果您想檢視警示的詳細資訊，您可以在應用程式 Web 介面中進行檢視。 • priority — 掃描的優先順序 可能的值是 1 表示高、100 表示標準、150 表示後台掃描。 • md5_list — 掃描時產生警示的檔案的 MD5 雜湊值。 • file_list — 掃描時產生警示的檔案的名稱。 • sb_names_map — 在應用程式 Web 介面上的警示詳細資訊中顯示的檔案名稱。
2024-06-11 02:38:44.841529 info apt-history: New sb_detect for file alert: {id: 2720, victim: default, state: new, md5: f0429d4845208857cd303df968ef545e}	Sandbox 元件處理結果的資訊儲存在應用程式資料庫中。記錄以供內部使用。這並不表示應用程式的偵測資料庫中存在偵測。

管理 Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security 是一款安裝在企業 IT 基礎架構中的單個裝置上的應用程式。應用程式持續監控在這些裝置上運行的處理程序、活動的網路連線和正在修改的檔案。有關電腦上事件的資訊（遙測）將會傳送到 Kaspersky Anti Targeted Attack Platform 伺服器。Kaspersky Endpoint Security 也會向 Kaspersky Anti Targeted Attack Platform 伺服器傳送有關應用程式偵測到的威脅的資訊以及有關處理這些威脅的結果的資訊。

配置 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 的整合後，應用程式將執行工作、套用來自 Kaspersky Anti Targeted Attack Platform 的參數，並將遙測資料從受防護裝置傳送至 KATA Central Node 伺服器。有關 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 整合時可以執行哪些操作的更多詳細資訊，請參閱*應用程式的操作原理*部分。

有關管理 Kaspersky Endpoint Security 的詳細資訊，請參閱應用程式的線上說明：

- 安裝和刪除應用程式。
- 應用程式產品授權。

  要與 Kaspersky Anti Targeted Attack Platform 整合，除了 Kaspersky Endpoint Security 啟動金鑰之外，您還必須新增 Kaspersky Endpoint Detection and Response (KATA) 附加金鑰。有關應用程式產品授權的詳細資訊，請參閱 Kaspersky Endpoint Security 線上說明→與 EDR (KATA) 整合。
- 與 EDR (KATA) 整合。
- 配置遙測。
- 管理隔離區。
- 用於管理 Detection and Response KATA EDR 的命令：與 EDR (KATA) 整合。

管理 Kaspersky Endpoint Security for Linux

Kaspersky Endpoint Security for Linux 是安裝在運行 Linux 作業系統的單個裝置上的應用程式，這些裝置是企業 IT 基礎架構的一部分。應用程式持續監控在這些裝置上運行的處理程序、活動的網路連線和正在修改的檔案。有關電腦上事件的資訊（遙測）將會傳送到 Kaspersky Anti Targeted Attack Platform 伺服器。Kaspersky Endpoint Security for Linux 也會向 Kaspersky Anti Targeted Attack Platform 伺服器傳送有關應用程式偵測到的威脅的資訊以及有關處理這些威脅的結果的資訊。

配置 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 的整合後，應用程式將執行工作、套用來自 Kaspersky Anti Targeted Attack Platform 的參數，並將遙測資料從受防護裝置傳送至 KATA Central Node 伺服器。有關 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 整合時可以執行哪些操作的更多詳細資訊，請參閱*應用程式的操作原理*部分。

有關管理 Kaspersky Endpoint Security for Linux 的詳細資訊，請參閱應用程式的線上說明：

- 安裝、移除和更新應用程式。
- 使用命令列管理應用程式：
  - 產品授權金鑰管理：授權工作（產品授權，ID：9）。
  - 與 Kaspersky Anti Targeted Attack Platform 整合：與 Kaspersky Endpoint Detection and Response (KATA) 工作整合（KATAEDR，ID：24）。
- 使用卡巴斯基安全管理中心管理主控台和卡巴斯基安全管理中心雲端主控台管理應用程式：
  - 產品授權金鑰管理：要了解更多詳細資訊，請參閱*在 Web 主控台中管理工作 → 建立工作*和*工作設定 → 新增金鑰*。
  - 與 Kaspersky Anti Targeted Attack Platform 整合：要了解更多詳細資訊，請參閱*在 Web 主控台中管理政策 → 建立政策*和*政策設定 → 與 Kaspersky Endpoint Detection and Response (KATA) 整合*。

要與 Kaspersky Anti Targeted Attack Platform 整合，您無需在 Kaspersky Endpoint Security for Linux 中新增額外的產品授權金鑰。

管理 Kaspersky Endpoint Security for Mac

Kaspersky Endpoint Security for Mac 是一款安裝在運行 macOS 作業系統的單個裝置上的應用程式，這些裝置是企業 IT 基礎架構的一部分。應用程式持續監控在這些裝置上運行的處理程序、活動的網路連線和正在修改的檔案。有關電腦上事件的資訊（遙測）將會傳送到 Kaspersky Anti Targeted Attack Platform 伺服器。Kaspersky Endpoint Security for Mac 也會向 Kaspersky Anti Targeted Attack Platform 伺服器傳送有關應用程式偵測到的威脅的資訊以及有關處理這些威脅的結果的資訊。

配置 Kaspersky Endpoint Security for Mac 與 Kaspersky Anti Targeted Attack Platform 的整合後，應用程式將執行工作、套用來自 Kaspersky Anti Targeted Attack Platform 的參數，並將遙測資料從受防護裝置傳送至 KATA Central Node 伺服器。有關 Kaspersky Endpoint Security for Mac 與 Kaspersky Anti Targeted Attack Platform 整合時可以執行哪些操作的更多詳細資訊，請參閱*應用程式的操作原理*部分。

有關管理 Kaspersky Endpoint Security for Mac 的詳細資訊，請參閱應用程式的線上說明。

- 安裝、移除和更新應用程式。
- 應用程式產品授權。

  要與 Kaspersky Anti Targeted Attack Platform 整合，除了 Kaspersky Endpoint Security 啟動金鑰之外，您還必須新增Kaspersky Endpoint Detection and Response (KATA) 附加金鑰。有關應用程式授權的更多詳細資訊，請參閱 Kaspersky Endpoint Security 說明 → 應用程式的高級配置 → Endpoint Detection and Response (KATA)。
- 使用命令列管理應用程式：
- 使用卡巴斯基安全管理中心管理主控台和雲端主控台遠端管理應用程式：
  - 有關產品授權金鑰管理的詳細資訊，請參閱以下部分：建立工作→ 配置新增金鑰工作設定。
  - 有關與 Kaspersky Anti Targeted Attack Platform 整合的詳細資訊，請參閱以下部分：建立政策→ 配置偵測和回應設定→ 配置 Endpoint Detection and Response (KATA)。

備份和還原資料

您可以建立備份副本，並在發生故障或需要重新安裝 Kaspersky Anti Targeted Attack Platform 時從中還原資料。您可以在基於不同作業系統的 Kaspersky Anti Targeted Attack Platform 安裝之間還原資料。例如，您可以將基於 Ubuntu 的 Kaspersky Anti Targeted Attack Platform 的資料還原至基於 Astra Linux 的 Kaspersky Anti Targeted Attack Platform，反之亦然。

對於基於 Astra Linux 作業系統的應用程式部署，您可以在版本 7.1.2 的伺服器上建立該應用程式的備份副本，並在版本 7.1.1 的伺服器上還原它。

對於應用程式的其他版本，不支援從一個版本還原到另一個版本；要還原資料的應用程式版本必須與建立備份副本的伺服器上的應用程式版本相符。如果應用程式版本不匹配，則啟動還原時會顯示錯誤訊息，並終止還原處理程序。

若要建立 Central Node 伺服器的備份副本，您可以透過 SSH 或應用程式管理員選單連線到伺服器。

此流程的示意圖如下圖所示。

備份和還原資料

應用程式不提供自動執行下列操作的機制：

- 在特定條件下或按照排程建立備份副本。
  您可以使用外部自動化工具來執行這些操作。
- 從緊急復原區中的備份副本進行還原。
  在此情況下，您必須手動啟動還原。

透過從備份副本還原來複製安裝。

備份和還原 Central Node 伺服器的資料

此場景描述了在 Central Node 伺服器上建立和從備份還原資料的過程。

Central Node 伺服器上的資料備份和還原涉及以下步驟：

1. **準備建立備份副本**

   請確定要建立備份副本的 Central Node 已設定為接收來自 SPAN 連接埠的鏡像流量。如果尚未啟用從 SPAN 連接埠接收鏡像流量，您需要啟用此功能，並確定其正常運作。如果缺少此功能或此功能無法正常運作，建立備份副本期間將發生錯誤，且產生的壓縮檔案將不完整。從此類壓縮檔案還原資料將會失敗。

配置從 SPAN 連接埠接收映像流量

您可以在安裝元件時啟用接收鏡像流量。如果您在安裝階段停用了流量接收：

若要開啟從 SPAN 連接埠接收映像流量：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。
2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任一工作伺服器的管理主控台。
3. 執行以下指令：

   ```
   kata-enable-span
   ```

   將啟用從 SPAN 連接埠接收映像流量。

如何檢查從 SPAN 連接埠接收鏡像流量的功能是否已配置並正常運作

若要確保您要為其建立備份副本的 Central Node 已配置從 SPAN 連接埠接收鏡像流量，且此功能正常運作：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。
2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任何伺服器的管理主控台。
3. 按順序執行以下命令：

   a. `sudo -i`

   b. `docker service ls | grep -P '(nta|ID|_span)`

   REPLICAS 列中，nta_configurator_services 應顯示 0/1，nta_core 服務應顯示 1/1。輸出中的其他值表示服務運作異常或已停用。

2 建立備份副本

建立備份副本期間，某些應用程式功能無法使用。如需無法使用的功能清單，以及解除此限制的說明，請參閱建立備份副本時套用的限制。

您可以使用管理員功能表或在技術支援模式下建立備份副本：

如何在管理員功能表中建立備份副本

> Kaspersky Anti Targeted Attack Platform 的備份副本僅包含資料庫（警示資料庫、VIP 身分詳細資料、從掃描中排除的資料清單、通知）和 Central Node 或 PCN 設定。

1. 登入您要透過 SSH 或終端進行備份的伺服器的管理主控台。
2. 出現提示時，輸入管理員帳戶的使用者名稱和密碼。

   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表部分的清單中，選擇**系統管理**部分。
4. 按下 **Enter**。

   這將開啟操作選擇視窗。
5. 在操作清單中，選擇**備份/還原設定**。

6. 按下 **Enter**。
   這將開啟**備份/還原設定**視窗。

7. 在操作清單中，選擇**建立**。

8. 按下 **Enter**。
   這將開啟**備份設定**視窗。

9. 點擊**備份**。

備份副本已建立。

如何在技術支援模式下建立備份副本

1. 登入您要透過 SSH 或終端進行備份的伺服器的管理主控台。

2. 出現提示時，輸入管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。

4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。

6. 執行以下指令：
   ```
   sudo kata-run.sh kata-backup-restore backup
   ```

您也可以為此命令指定一個或多個參數 （請參閱下表）。

您也可以使用 `-h` 指令接收有關使用參數的提示。

建立備份副本的參數

必需的參數	參數	敘述
是	`-b` <路徑>	在指定路徑建立備份副本， 其中<path>是要建立備份副本的目錄的絕對路徑或相對路徑。
否	`-c`	儲存備份副本之前清除目錄。
否	`-d` <儲存檔案數>	指定目錄中儲存的最大備份檔案數，其中<number>是檔案數。
否	`-e`	將檔案儲存在儲存中。
否	`-q`	將檔案儲存在隔離區中。
否	`-a`	儲存等待重新掃描的檔案。
否	`-s`	儲存 Sandbox 工件。

否	-n	儲存 Central Node 或 PCN 設定。
No	-l <檔案路徑>	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

如果未定義其他設定，備份副本僅包含資料庫（警示資料庫、VIP 狀態詳細資訊、從掃描中排除的資料清單、通知）。

範例：

建立備份副本的指令：

```
sudo kata-run.sh kata-backup-restore backup -b <路徑> -c -d <儲存檔案數> -e -q -a -s -n -l <檔案路徑>
```

3 將備份副本儲存到硬碟

若要將備份副本儲存在電腦硬碟上，請執行以下命令：

`scp <用於在管理員功能表和伺服器管理主控台中工作的帳戶的名稱>@<伺服器的 IP 位址>:<備份檔案的名稱，格式為：data_kata_<建立備份副本的日期和時間>.tar>`

範例：

用於將於 2020 年4 月10 日10 時 00 分00 秒在"admin"帳戶下的 IP 位址為 10.0.0.10 的 Central Node 伺服器上建立的備份副本下載到電腦硬碟的命令：

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

備份副本儲存到您的電腦硬碟上的目前目錄。

4 重新安裝應用程式

移除並重新安裝 Kaspersky Anti Targeted Attack Platform。

安裝應用程式時，您需要為尋址伺服器指定與應用程式備份副本中指定的相同的網路遮罩。如果值不匹配，則嵌入式 Sensor 在應用程式還原後會遇到錯誤。如果需要，您可以還原該元件。

安裝後，您必須在應用程式新增與建立備份副本的伺服器上相同類型的產品授權金鑰（KATA、KATA + NDR、KEDR）。這對於還原備份副本中保存的所有 Central Node、PCN 或 SCN 設定是必要的。

5 將備份副本上傳至伺服器

透過執行以下命令將備份副本上傳到 Central Node 伺服器：

`scp <備份檔案的名稱，格式為：data_kata_<備份副本所建立的日期和時間>.tar> <用於在管理員功能表和伺服器管理主控台中工作的帳戶名稱>@<伺服器的 IP 位址>：`

範例：

用於將於 2020 年4 月10 日10 時 00 分00 秒建立的備份副本上傳到"admin"帳戶下的 IP 位址為 10.0.0.10 的 Central Node 伺服器的命令：

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

備份副本將上傳至 Central Node 伺服器的目前目錄。

6 從備份副本還原資料

您可以使用管理員功能表或在技術支援模式下從 Central Node 伺服器上的備份副本還原資料：

如何在管理員功能表中還原資料

1. 登入您要透過 SSH 或終端還原其資料的伺服器的管理主控台。
2. 出現提示時，輸入應用程式元件管理員帳戶的使用者名稱和密碼。

   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表部分的清單中，選擇**系統管理**部分。

4. 按下 **Enter**。
   這將開啟操作選擇視窗。

5. 在操作清單中，選擇**備份/還原設定**。

6. 按下 **Enter**。
   這將開啟**備份/還原設定**視窗。

7. 在包含應用程式備份副本的檔案清單中，選擇要從中還原伺服器設定的檔案。
   如果必要的檔案未列出，請將包含備份副本的檔案上傳到伺服器。

8. 按下 **Enter**。
   這將開啟操作選擇視窗。

9. 在操作清單中，選擇**還原 <備份檔案名稱，格式為：data_kata_<備份副本的建立日期和時間>.tar>**

10. 按下 **Enter**。
    這將開啟操作確認視窗。

11. 點擊**還原**。
    從備份副本還原伺服器資料的過程開始。

> 如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

如何在技術支援模式下還原資料

1. 登入您要透過 SSH 或終端還原其資料的伺服器的管理主控台。

2. 出現提示時，輸入應用程式管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。

4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。

6. 執行以下指令：

```
sudo kata-run.sh kata-backup-restore restore
```

   您也可以為此命令指定一個或多個參數（請參閱下表）。

   您也可以使用 `-h` 指令接收有關使用參數的提示。

資料還原參數

必需的參數	參數	命令描述
是	`-r <路徑>`	從包含備份副本的檔案中還原資料， 其中<path>是備份檔案的完整路徑。
否	`-l <檔案路徑>`	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

範例：

從備份副本還原資料的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路徑> -l <檔案路徑>
```

如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

伺服器設定的備份副本不包含記錄的映像網路流量的 PCAP 檔案。您可以透過從連線的儲存的 /data/volumes/dumps 目錄複製 PCAP 檔案來自行儲存和還原它們。還原資料後，您必須連線外部儲存。

如果在其上建立備份副本的 Central Node 伺服器的硬體配置與您計劃在其上還原伺服器設定的伺服器的硬體配置不同，您需要在還原後重新配置應用程式延伸設定。

備份和還原作為叢集部署的 Central Node 伺服器的資料

此方案描述了在作為叢集部署的 Central Node 伺服器上備份和還原資料的過程。

在作為叢集部署的 Central Node 伺服器上備份和還原資料涉及以下步驟：

1. **準備建立備份副本**

   請確定 Central Node 叢集中的其中一台伺服器已設定為接收來自 SPAN 連接埠的鏡像流量。如果尚未啟用從 SPAN 連接埠接收鏡像流量，您需要啟用此功能，並確定其正常運作。如果缺少此功能或此功能無法正常運作，建立備份副本期間將發生錯誤，且產生的壓縮檔案將不完整。從此類壓縮檔案還原資料將會失敗。

   找出叢集中已啟用處理來自 SPAN 連接埠之鏡像流量的伺服器

   若要判斷 Central Node 叢集中的哪一台伺服器已啟用處理來自 SPAN 連接埠的鏡像流量：

   1. 透過 SSH 或使用終端機進入任何叢集伺服器的管理主控台。
   2. 執行以下指令：

      ```
      sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
      ```

      叢集中啟用映像 SPAN 映像流量處理的工作伺服器的位址。

   配置從 SPAN 連接埠接收映像流量

   您可以在安裝元件時啟用接收鏡像流量。如果您在安裝階段停用了流量接收：

若要開啟從 SPAN 連接埠接收映像流量：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。
2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任一工作伺服器的管理主控台。
3. 執行以下指令：

   ```
   kata-enable-span
   ```

   將啟用從 SPAN 連接埠接收映像流量。

如何檢查從 SPAN 連接埠接收鏡像流量的功能是否已配置並正常運作

若要確保您要為其建立備份副本的 Central Node 已配置從 SPAN 連接埠接收鏡像流量，且此功能正常運作：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。
2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任何伺服器的管理主控台。
3. 按順序執行以下命令：

   a. `sudo -i`

   b. `docker service ls | grep -P '(nta|ID|_span)`

   REPLICAS 列中，nta_configurator_services 應顯示 0/1，nta_core 服務應顯示 1/1。輸出中的其他值表示服務運作異常或已停用。

2. **建立備份副本**

建立備份副本期間，某些應用程式功能無法使用。如需無法使用的功能清單，以及解除此限制的說明，請參閱建立備份副本時套用的限制。

您可以使用管理員功能表或在技術支援模式下建立備份副本：

如何在管理員選單中建立應用程式的備份副本

> Kaspersky Anti Targeted Attack Platform 的備份副本僅包含資料庫（警示資料庫、VIP 身分詳細資料、從掃描中排除的資料清單、通知）和 Central Node 或 PCN 設定。

1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。
2. 出現提示時，輸入管理員帳戶的使用者名稱和密碼。

   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表部分的清單中，選擇**系統管理**部分。
4. 按下 **Enter**。

   這將開啟操作選擇視窗。
5. 在操作清單中，選擇**備份/還原設定**。
6. 按下 **Enter**。

   這將開啟**備份/還原設定**視窗。

7. 在操作清單中，選擇**建立**。

8. 按下 **Enter**。
   這將開啟**備份設定**視窗。

9. 點擊**備份**。

備份副本已建立。

如何在技術支援模式下建立應用程式的備份副本

1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。

2. 出現提示時，輸入應用程式元件管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。

4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。

6. 指定叢集中啟用映像 SPAN 流量處理的工作伺服器的位址：
   ```
   sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
   ```
   叢集中啟用映像 SPAN 映像流量處理的工作伺服器的位址。

7. 使用 SSH 協定登入此伺服器的管理主控台：
   ```
   ssh admin@<步驟 6 中取得的伺服器位址>
   ```

8. 執行以下指令：
   ```
   sudo kata-run.sh kata-backup-restore backup
   ```

您也可以為此命令指定一個或多個參數 （請參閱下表）。

您也可以使用 `-h` 指令接收有關使用參數的提示。

建立備份副本的參數

必需的參數	參數	敘述
是	`-b <路徑>`	在指定路徑建立備份副本， 其中<path>是要建立備份副本的目錄的絕對路徑或相對路徑。
否	`-c`	儲存備份檔案之前清除目錄。
否	`-d <儲存檔案數>`	指定目錄中儲存的最大檔案數，其中<number>是檔案數。

否	-n	儲存 Central Node 或 PCN 設定。
No	-l <檔案路徑>	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

如果未定義其他設定，備份副本僅包含資料庫（警示資料庫、VIP 狀態詳細資訊、從掃描中排除的資料清單、通知）。

範例：

建立備份副本的指令：

```
sudo kata-run.sh kata-backup-restore backup -b <路徑> -c -d <儲存檔案數> -e -q -a -s -n -l <檔案路徑>
```

該應用程式的 7.1.2 版本不允許使用應用程式管理員選單建立備份副本。

3 將備份副本儲存到硬碟

若要將備份副本儲存在電腦硬碟上，請執行以下命令：

`scp <用於在管理員功能表和伺服器管理主控台中工作的帳戶的名稱>@<伺服器的 IP 位址>:<備份檔案的名稱，格式為：data_kata_<建立備份副本的日期和時間>.tar>`

範例：

用於將於 2020 年4 月10 日10 時 00 分00 秒在"admin"帳戶下的 IP 位址為 10.0.0.10 的 Central Node 伺服器上建立的備份副本下載到電腦硬碟的命令：

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

備份副本儲存到您的電腦硬碟上的目前目錄。

4 重新安裝應用程式

移除並重新安裝 Kaspersky Anti Targeted Attack Platform。

安裝應用程式時，您需要為尋址伺服器指定與應用程式備份副本中指定的相同的網路遮罩。如果值不匹配，則嵌入式 Sensor 在應用程式還原後會遇到錯誤。如果需要，您可以還原該元件。

安裝後，您必須在應用程式新增與建立備份副本的伺服器上相同類型的產品授權金鑰（KATA、KATA + NDR、KEDR）。這對於還原備份副本中保存的所有 Central Node、PCN 或 SCN 設定是必要的。

5 將備份副本上傳至伺服器

透過執行以下命令將備份副本上傳到 Central Node 伺服器：

`scp <備份檔案的名稱，格式為：data_kata_<備份副本所建立的日期和時間>.tar> <用於在管理員功能表和伺服器管理主控台中工作的帳戶名稱>@<伺服器的 IP 位址>：`

範例：

用於將於 2020 年4 月10 日10 時 00 分00 秒建立的備份副本上傳到"admin"帳戶下的 IP 位址為 10.0.0.10 的 Central Node 伺服器的命令：

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

備份副本將上傳至 Central Node 伺服器的目前目錄。

6 從備份副本還原資料

您可以使用管理員功能表或在技術支援模式下從 Central Node 伺服器上的備份副本還原資料：

如何在管理員選單中還原應用程式版本的資料

1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。
2. 出現提示時，輸入應用程式元件管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表部分的清單中，選擇**系統管理**部分。
4. 按下 **Enter**。
   這將開啟操作選擇視窗。
5. 在操作清單中，選擇**備份/還原設定**。
6. 按下 **Enter**。
   這將開啟**備份/還原設定**視窗。
7. 在包含應用程式備份副本的檔案清單中，選擇要從中還原伺服器設定的檔案。
   如果必要的檔案未列出，請將包含備份副本的檔案上傳到伺服器。
8. 按下 **Enter**。
   這將開啟操作選擇視窗。
9. 在操作清單中，選擇**還原 <備份檔案名稱，格式為：data_kata_<備份副本的建立日期和時間>.tar>**
10. 按下 **Enter**。
    這將開啟操作確認視窗。
11. 點擊**還原**。
    從備份副本還原伺服器資料的過程開始。

> 如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

> 如果網路介面名稱不匹配，執行上述說明的第 11 步後，系統將提示您選擇用於從 SPAN 連接埠接收映像流量的網路介面。

如何在技術支援模式下還原應用程式版本的資料

1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。
2. 出現提示時，輸入應用程式管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。
4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。
5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。

6. 透過執行以下命令啟動資料復原過程：

   ```
   sudo kata-run.sh kata-backup-restore restore
   ```

您也可以為此命令指定一個或多個參數（請參閱下表）。

您也可以使用 `-h` 指令接收有關使用參數的提示。

資料還原參數

必需的參數	參數	命令描述
是	`-r <路徑>`	從包含備份副本的檔案中還原資料， 其中<path>是備份檔案的完整路徑。
否	`-l <檔案路徑>`	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

範例：

從備份副本還原資料的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路徑> -l <檔案路徑>
```

如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

如果網路介面名稱不匹配，執行上述說明的第 6 步驟後，系統將提示您選擇用於從 SPAN 連接埠接收映像流量的網路介面。

如果要將應用程式版本 7.1.2 的資料還原到應用程式版本 7.1.1 或 7.1.2 的伺服器上，則需要使用以下說明。

如何在技術支援模式下還原應用程式版本 7.1.1 或 7.1.2 的資料

1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。

2. 出現提示時，輸入應用程式管理員帳戶的使用者名稱和密碼。

   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。

4. 按下 **Enter**。

   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。

6. 指定叢集中啟用映像 SPAN 流量處理的工作伺服器的位址：

   ```
   sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
   .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end
   }}'
   ```

   叢集中啟用映像 SPAN 映像流量處理的工作伺服器的位址。

7. 使用 SSH 協定登入此伺服器的管理主控台：

   ```
   ssh admin@<步驟 6 中取得的伺服器位址>
   ```

8. 透過執行以下命令啟動資料復原過程：

```
sudo kata-run.sh kata-backup-restore restore
```

您也可以為此命令指定一個或多個參數（請參閱下表）。

您也可以使用 -h 指令接收有關使用參數的提示。

資料還原參數

必需的參數	參數	命令描述
是	-r <路徑>	從包含備份副本的檔案中還原資料， 其中<path>是備份檔案的完整路徑。
否	-l <檔案路徑>	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

範例：

從備份副本還原資料的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路徑> -l <檔案路徑>
```

如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

如果網路介面名稱不匹配，執行上述說明的第 6 步驟後，系統將提示您選擇用於從 SPAN 連接埠接收映像流量的網路介面。

伺服器設定的備份副本不包含記錄的映像網路流量的 PCAP 檔案。您可以透過從已連線的外部儲存的 /data/volumes/dumps 目錄複製 PCAP 檔案來自行儲存和還原它們。還原資料後，您必須連線外部儲存。

如果在其上建立備份副本的 Central Node 伺服器的硬體配置與您計劃在其上還原伺服器設定的伺服器的硬體配置不同，您需要在還原後重新配置應用程式延伸設定。

分佈式解決方案和多租戶模式下 Central Node 伺服器的資料備份與還原

此場景描述了在分佈式解決方案或多租戶模式下部署的 Central Node 伺服器上備份和還原資料的過程。

要在使用分佈式解決方案和多租戶模式時備份和還原資料，您必須連線到層次結構中的每個 Central Node 伺服器，並按照以下說明的步驟進行操作。

備份和還原以分佈式解決方案或多租戶模式部署的 Central Node 伺服器上的資料涉及以下步驟：

1. **準備建立備份副本**

   請確定要建立備份副本的 Central Node 已設定為接收來自 SPAN 連接埠的鏡像流量。將 Central Node 部署為叢集時，必須在叢集中的一台伺服器上啟用此功能。如果尚未啟用從 SPAN 連接埠接收鏡像流量，您需要啟用此功能，並確定其正常運作。如果缺少此功能或此功能無法正常運作，建立備份副本期間將發生錯誤，且產生的壓縮檔案將不完整。從此類壓縮檔案還原資料將會失敗。

找出叢集中已啟用處理來自 SPAN 連接埠之鏡像流量的伺服器

若要判斷 Central Node 叢集中的哪一台伺服器已啟用處理來自 SPAN 連接埠的鏡像流量：

1. 透過 SSH 或使用終端機進入任何叢集伺服器的管理主控台。

2. 執行以下指令：

   ```
   sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
   .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end
   }}'
   ```

   叢集中啟用映像 SPAN 映像流量處理的工作伺服器的位址。

配置從 SPAN 連接埠接收映像流量

您可以在安裝元件時啟用接收鏡像流量。如果您在安裝階段停用了流量接收：

若要開啟從 SPAN 連接埠接收映像流量：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。

2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任一工作伺服器的管理主控台。

3. 執行以下指令：

   ```
   kata-enable-span
   ```

   將啟用從 SPAN 連接埠接收映像流量。

如何檢查從 SPAN 連接埠接收鏡像流量的功能是否已配置並正常運作

若要確保您要為其建立備份副本的 Central Node 已配置從 SPAN 連接埠接收鏡像流量，且此功能正常運作：

1. 如果 Central Node 安裝在伺服器上，請使用 SSH 或終端機登入相關伺服器的管理主控台。

2. 如果 Central Node 部署為叢集，請使用 SSH 或終端機登入叢集中任何伺服器的管理主控台。

3. 按順序執行以下命令：

   a. `sudo -i`

   b. `docker service ls | grep -P '(nta|ID|_span)`

   REPLICAS 列中，nta_configurator_services 應顯示 0/1，nta_core 服務應顯示 1/1。輸出中的其他值表示服務運作異常或已停用。

2 建立備份副本

建立備份副本期間，某些應用程式功能無法使用。如需無法使用的功能清單，以及解除此限制的說明，請參閱建立備份副本時套用的限制。

您可以使用管理員功能表或在技術支援模式下建立備份副本：

如何在管理員功能表中建立備份副本

Kaspersky Anti Targeted Attack Platform 的備份副本僅包含資料庫（警示資料庫、VIP 身分詳細資料、從掃描中排除的資料清單、通知）和 Central Node 或 PCN 設定。

1. 登入您要透過 SSH 或終端進行備份的伺服器的管理主控台。
2. 出現提示時，輸入管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表部分的清單中，選擇**系統管理**部分。
4. 按下 **Enter**。
   這將開啟操作選擇視窗。
5. 在操作清單中，選擇**備份/還原設定**。
6. 按下 **Enter**。
   這將開啟**備份/還原設定**視窗。
7. 在操作清單中，選擇**建立**。
8. 按下 **Enter**。
   這將開啟**備份設定**視窗。
9. 點擊**備份**。

備份副本已建立。

如何在技術支援模式下建立備份副本

1. 登入您要透過 SSH 或終端進行備份的伺服器的管理主控台。
2. 出現提示時，輸入管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。
4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。
5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。
6. 執行以下指令：
   ```
   sudo kata-run.sh kata-backup-restore backup
   ```

您也可以為此命令指定一個或多個參數 （請參閱下表）。

您也可以使用 `-h` 指令接收有關使用參數的提示。

建立備份副本的參數

必需的參數	參數	敘述
是	-b <路徑>	在指定路徑建立備份副本， 其中<path>是要建立備份副本的目錄的絕對路徑或相對路徑。
否	-c	儲存備份副本之前清除目錄。
否	-d <儲存檔案數>	指定目錄中儲存的最大備份檔案數，其中<number>是檔案數。
否	-e	將檔案儲存在儲存中。
否	-q	將檔案儲存在隔離區中。
否	-a	儲存等待重新掃描的檔案。
否	-s	儲存 Sandbox 工件。
否	-n	儲存 Central Node 或 PCN 設定。
No	-l <檔案路徑>	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

如果未定義其他設定，備份副本僅包含資料庫（警示資料庫、VIP 狀態詳細資訊、從掃描中排除的資料清單、通知）。

範例：

建立備份副本的指令：

```
sudo kata-run.sh kata-backup-restore backup -b <路徑> -c -d <儲存檔案數> -e -q -a -s -n -l <檔案路徑>
```

3 將備份副本儲存到硬碟

若要將備份副本儲存在電腦硬碟上，請執行以下命令：

`scp <用於在管理員功能表和伺服器管理主控台中工作的帳戶的名稱>@<伺服器的 IP 位址>:<備份檔案的名稱，格式為：data_kata_<建立備份副本的日期和時間>.tar>`

範例：

用於將於 2020 年4 月10 日10 時 00 分00 秒在"admin"帳戶下的 IP 位址為 10.0.0.10 的 Central Node 伺服器上建立的備份副本下載到電腦硬碟的命令：

```
scp admin@10.0.0.10:data_kata_2020_04_10T10_00_00.tar
```

備份副本儲存到您的電腦硬碟上的目前目錄。

4 重新安裝應用程式

移除並重新安裝 Kaspersky Anti Targeted Attack Platform。

資料只能從備份還原到具有 Central Node 角色的伺服器。如果在開始之前為伺服器指派 PCN 或 SCN 角色，則還原過程將會失敗。

安裝應用程式時，您需要為尋址伺服器指定與應用程式備份副本中指定的相同的網路遮罩。如果值不匹配，則嵌入式 Sensor 在應用程式還原後會遇到錯誤。如果需要，您可以還原該元件。

安裝後，您必須在應用程式新增與建立備份副本的伺服器上相同類型的產品授權金鑰（KATA、KATA + NDR、KEDR）。這對於還原備份副本中保存的所有 Central Node、PCN 或 SCN 設定是必要的。

5 將備份副本上傳至伺服器

透過執行以下命令將備份副本上傳到 Central Node 伺服器：

`scp <備份檔案的名稱，格式為：data_kata_<備份副本所建立的日期和時間>.tar> <用於在管理員功能表和伺服器管理主控台中工作的帳戶名稱>@<伺服器的 IP 位址>`：

範例：

用於將於 2020 年4 月10 日10 時 00 分00 秒建立的備份副本上傳到"admin"帳戶下的 IP 位址為 10.0.0.10 的 Central Node 伺服器的命令：

```
scp data_kata_2020_04_10T10_00_00.tar admin@10.0.0.10:
```

備份副本將上傳至 Central Node 伺服器的目前目錄。

6 **從備份副本還原資料**

您可以使用管理員功能表或在技術支援模式下從 Central Node 伺服器上的備份副本還原資料：

如何在管理員功能表中還原資料

1. 登入您要透過 SSH 或終端還原其資料的伺服器的管理主控台。
2. 出現提示時，輸入應用程式元件管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表部分的清單中，選擇**系統管理**部分。
4. 按下 **Enter**。
   這將開啟操作選擇視窗。
5. 在操作清單中，選擇**備份/還原設定**。
6. 按下 **Enter**。
   這將開啟**備份/還原設定**視窗。
7. 在包含應用程式備份副本的檔案清單中，選擇要從中還原伺服器設定的檔案。
   如果必要的檔案未列出，請將包含備份副本的檔案上傳到伺服器。
8. 按下 **Enter**。
   這將開啟操作選擇視窗。
9. 在操作清單中，選擇**還原 <備份檔案名稱，格式為：data_kata_<備份副本的建立日期和時間>.tar>**
10. 按下 **Enter**。
    這將開啟操作確認視窗。
11. 點擊**還原**。
    從備份副本還原伺服器資料的過程開始。

如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

如何在技術支援模式下還原資料

1. 登入您要透過 SSH 或終端還原其資料的伺服器的管理主控台。
2. 出現提示時，輸入應用程式管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。

3. 在應用程式管理員功能表的部分清單中，選擇**技術支援模式**部分。

4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。

5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按下 **Enter**。

6. 執行以下指令：

```
sudo kata-run.sh kata-backup-restore restore
```

您也可以為此命令指定一個或多個參數（請參閱下表）。

您也可以使用 -h 指令接收有關使用參數的提示。

資料還原參數

必需的參數	參數	命令描述
是	-r <路徑>	從包含備份副本的檔案中還原資料， 其中<path>是備份檔案的完整路徑。
否	-l <檔案路徑>	將命令執行結果儲存到檔案中，其中<檔案路徑>是事件日誌檔案的名稱，包括檔案的絕對路徑或相對路徑。

範例：
從備份副本還原資料的命令：

```
sudo kata-run.sh kata-backup-restore restore -r <路徑> -l <檔案路徑>
```

如果建立備份副本的伺服器和從備份副本還原資料的伺服器上的網路介面名稱相同，則會自動還原從 SPAN 連接埠接收映像流量的設定。

如果在其上建立備份副本的 Central Node 伺服器的硬體配置與您計劃在其上還原伺服器設定的伺服器的硬體配置不同，您需要在還原後重新配置應用程式延伸設定。

還原資料後，您不需要將 SCN 重新連線到 PCN：PCN 連線設定和連線的 SCN 清單將從備份副本中還原。

伺服器設定的備份副本不包含記錄的映像網路流量的 PCAP 檔案。您可以透過從連線的儲存的 /data/volumes/dumps 目錄複製 PCAP 檔案來自行儲存和還原它們。還原資料後，您必須連線外部儲存。

在分佈式解決方案和多租用戶模式下還原資料時適用的限制

在分佈式解決方案和多組織用戶模式下還原資料後，AM 技術建立的新警示可能不會顯示在警示表中。您可以檢查該限制是否適用於您，並在必要時採取措施修復它。

若要檢視警示表中是否顯示新警示，請執行下列操作：

1. 為您正在使用的 Sensor 啟用監控點。

2. 如果您使用的是獨立 Sensor，請使用 SHH 或終端登入該 Sensor 伺服器的管理主控台。

3. 如果您使用的是嵌入式 Sensor，請透過 SSH 或使用終端登入託管嵌入式 Sensor 的 Central Node 伺服器的管理主控台。

   如果 Central Node 部署為叢集，您需要登入啟用了映像 SPAN 流量處理的工作伺服器的管理主控台。

   如何找出此伺服器的位址

   1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。
   2. 出現提示時，輸入應用程式元件管理員帳戶的使用者名稱和密碼。

      顯示應用程式元件管理員功能表。
   3. 在應用程式管理員功能表部分的清單中，選擇“技術支援模式”部分。
   4. 按下“Enter”。

      這將開啟技術支援模式確認視窗。
   5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇是並按 Enter。
   6. 指定叢集中啟用映像 SPAN 流量處理的工作伺服器的位址：

      ```
      sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index
      .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
      ```

      叢集中啟用映像 SPAN 映像流量處理的工作伺服器的位址。
   7. 使用 SSH 協定登入此伺服器的管理主控台：

      `ssh admin@<步驟 6 中取得的伺服器位址>`

4. 系統提示時，輸入管理員使用者名稱和安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。
5. 在應用程式管理員功能表中，選擇技術支援模式。
6. 按Enter鍵。
7. 這將開啟技術支援模式確認視窗。
8. 確認您想要在技術支援模式下管理應用程式。為此，請選擇是並按 ENTER。
9. 執行以下指令：

   ```
   watch "curl http://127.0.0.1:9191/metrics | grep
   preprocessor_files_extracted_fromhttp"
   ```

   如果 *preprocessor_files_extracted_fromhttp* 欄位顯示 0，請依照下列步驟解除限制。

要在使用嵌入式 Sensor 時解除限制：

1. 透過 SSH 或使用終端登入託管嵌入式 Sensor 的 Central Node 伺服器的管理主控台。

   如果 Central Node 部署為叢集，您需要登入啟用了映像 SPAN 流量處理的工作伺服器的管理主控台。

如何找出此伺服器的位址

1. 透過 SSH 或使用終端機進入任何正常運作的叢集伺服器的管理主控台。
2. 出現提示時，輸入應用程式元件管理員帳戶的使用者名稱和密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表部分的清單中，選擇“技術支援模式”部分。
4. 按下“Enter”。
   這將開啟技術支援模式確認視窗。
5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇是並按 Enter。
6. 指定叢集中啟用映像 SPAN 流量處理的工作伺服器的位址：
   ```
   sudo docker node ls -q | sudo xargs docker node inspect -f '{{ if eq (index .Spec.Labels "infrastructure.span") "true" }}{{ .Description.Hostname }}{{ end }}'
   ```
   叢集中啟用映像 SPAN 映像流量處理的工作伺服器的位址。
7. 使用 SSH 協定登入此伺服器的管理主控台：
   `ssh admin@<步驟 6 中取得的伺服器位址>`

2. 透過執行以下命令提高使用者的權限。
   ```
   sudo -i
   ```
3. 執行以下指令：
   ```
   kata-sensor-tool reset
   kata-sensor-tool reset-core
   kata-sensor-tool init-embedded-sensor
   ```
4. 依照檢查新警示說明中的步驟，驗證警示表中是否顯示新警示。

限制已移除。

若要消除使用獨立於 Central Node 安裝在伺服器上的 Sensor 時的限制：

1. 在 Kaspersky Anti Targeted Attack Platform Web 介面中刪除連線的 Sensor。
2. 透過 SSH 協定或終端登入 Sensor 的管理主控台。
3. 透過執行以下命令提高使用者的權限。
   ```
   sudo -i
   ```
4. 執行以下指令：
   ```
   kata-sensor-tool reset
   ```
5. 將感測器重新連線至 Central Node。
6. 依照檢查新警示說明中的步驟，驗證警示表中是否顯示新警示。

限制已移除。

匯出資料的內容

Kaspersky Anti Targeted Attack Platform 可能包含使用者資料和其他機密資訊。Kaspersky Anti Targeted Attack Platform 管理員正在建立備份副本，更換安裝應用程式的裝置，或在其他可能需要永久刪除資料的情況下，必須採取措施確保此資料的安全。Kaspersky Anti Targeted Attack Platform 管理員負責存取儲存在應用程式伺服器上的資料。

以下資料**不會**從備份副本還原：

- 與 Sandbox 元件整合的設定

  從備份副本還原 Kaspersky Anti Targeted Attack Platform 後，Sandbox 不會自動連線至 Central Node。

- 與外部系統整合的參數（包括郵件 Sensor）。

  建立 Kaspersky Anti Targeted Attack Platform 的備份副本時，請注意，即使 Central Node 再次開始接收流量，外部系統也可能不會繼續向其傳送流量。

- 與 SIEM 系統整合的參數。
- 時區設定。
- 將資料寫入應用程式記錄的參數。
- 與 NDR 和 KEDR 功能區塊整合時，來自 Endpoint Agent 元件的遙測資料。
- 網路流量傾印。
- 在技術支援模式下對設定檔所做的變更。

從備份還原資料之前，您需要在還原應用程式的 Central Node 伺服器上清除以下內容：

- 應用程式資料庫。
- 儲存中的物件。
- 重新掃描期間產生的警示檔案。
- Sandbox 工件。
- 設定檔。
- Central Node 設定。

資料類型	匯出的資料	應用程式運行模式	部署方式

Central Node 設定，包括伺服器的 TLS 憑證。
Central Node 上的應用程式資料庫：
• 網路流量事件
• 警示和警示的 VIP 身分
• 風險和異常
• 工作及工作執行結果
• 預設和防護規則
• 使用者定義的 TAA (IOA) 規則和排除項
• 使用者定義的入侵偵測規則和排除項目
• 使用者定義的 YARA 規則
• IOC 檔案
• 掃描排除規則
• 決定允許哪些網路互動的規則
• 有關儲存中檔案的資訊
• 被隔離的物件的訊息
• 具有 Endpoint Agent 的電腦清單
• 具有 Endpoint Agent 的電腦連線設定
• 裝置資訊：
  • 裝置清查
  • 在裝置作業系統中註冊的使用者帳戶清單
  • 裝置上的可執行檔清單
  • 裝置的位址空間
• 分配給裝置的標籤
• 有關網路互動圖上裝置位置的資訊
• 一般報告和報告範本
• NDR 報告和報告範本
• 使用者帳戶資料
• 使用者活動日誌
• 網路工作階段資料
• 拓撲圖
• 通知
• 嵌入式 Sensor 的設定。
	Central Node 設定（如果已選擇）。
	預設為應用程式資料庫。
		獨立 Central Node 伺服器。	所有部署方法。

PCN 連線設定 已連線的 SCN 清單	是	分佈式解決方案和多租戶模式。	所有部署方法。
PCN 設定，包括伺服器的 TLS 憑證。	自訂	分佈式解決方案和多租戶模式。	所有部署方法。
SCN 設定，包括伺服器的 TLS 憑證。	自訂 適用於獨立的 Central Node 伺服器。	分佈式解決方案和多租戶模式。	所有部署方法。

資料類型	匯出的資料	應用程式運行模式	部署方式

PCN 上的應用程式資料庫：
• 網路流量事件
• 警示和警示的 VIP 身分
• 風險和異常
• 工作及工作執行結果
• 預設和防護規則
• 使用者定義的 TAA (IOA) 規則和排除項
• 使用者定義的入侵偵測規則和排除項目
• 使用者定義的 YARA 規則
• IOC 檔案
• 掃描排除規則
• 決定允許哪些網路互動的規則
• 有關儲存中檔案的資訊
• 被隔離的物件的訊息
• 具有 Endpoint Agent 的電腦清單
• 具有 Endpoint Agent 的電腦連線設定
• 裝置資訊：
  • 裝置清查
  • 在裝置作業系統中註冊的使用者帳戶清單
  • 裝置上的可執行檔清單
  • 裝置的位址空間
• 分配給裝置的標籤
• 有關網路互動圖上裝置位置的資訊
• 一般報告和報告範本
• NDR 報告和報告範本
• 使用者帳戶資料
• 使用者活動日誌
• 網路工作階段資料
• 拓撲圖
• 通知
• 嵌入式 Sensor 的設定。
	預設	分佈式解決方案和多租戶模式。	所有部署方法。

設定檔，MDR 整合檔案除外。	是	所有模式。	所有部署方法。
備份	自訂	所有模式。	非高可用性版本。
Sandbox 工件。	自訂	所有模式。	非高可用性版本。
重新掃描期間產生的警示檔案。	自訂	所有模式。	非高可用性版本。
建立應用程式的備份副本時在掃描佇列中的檔案。	無。	所有模式。	所有部署方法。
產品授權金鑰。	無。	所有模式。	所有部署方法。
事件資料庫。	無。	所有模式。	所有部署方法。
與 Central Node 分開安裝的 Sensor 的設定。			
與嵌入式 Sensor 的網路介面關聯的監控點的設定。			
網路介面設定。	無。	所有模式。	所有部署方法。
SPAN 流量傾印。	無。	所有模式。	所有部署方法。

建立備份副本時套用的限制

建立備份副本期間無法使用以下應用程式功能：

- 以下部分：**Sensor 伺服器**、**網路流量事件**、**網路地圖**、**風險和異常**、**連線器**、**整合伺服器**。
  切換至這些區段時，將顯示警告：*NDR 處理程序正在啟動。請稍候。*

- 使用連接器連線至 Kaspersky Anti Targeted Attack Platform。
- 從已連線至 NDR 功能區塊的 Endpoint Agent 傳輸遙測資料。
- 接收 ERSPAN 和 SPAN 流量。
  即使應用程式再次開始接受流量，外部系統也可能不會繼續將流量傳送至 Kaspersky Anti Targeted Attack Platform。
- 使用 API NDR 連線至 Kaspersky Anti Targeted Attack Platform。

如果伺服器上安裝了 Central Node，您可以啟動負責這些功能的服務，以解除這些限制。

若要啟動應用程式服務：

1. 透過 SSH 或終端登入 Central Node 伺服器的管理主控台。
2. 按順序執行以下命令：
   a. `sudo -i`
   b. `docker service scale kata_product_main_1_nta_database=1`
   c. `docker service scale kata_product_main_1_nta_core=1`
   d. `docker service scale kata_product_main_1_nta_syncer=1`

   服務已啟動。應用程式的所有功能均可使用。

從備份副本還原應用程式後還原嵌入式 Sensor

如果應用程式備份副本中的網路遮罩與用作復原基礎的應用程式中的網路遮罩不匹配，則嵌入式Sensor 在復原後會遇到錯誤。我們建議檢查目前網路遮罩以確定錯誤是由於不匹配造成的。

若要檢查網路遮罩的目前值，

選擇應用程式 Web 介面的“**Sensor 伺服器**”部分。

網路遮罩的目前值顯示在元件卡上的元件名稱下方。如果值不匹配，請按照說明中的步驟還原嵌入式Sensor。

> 還原元件後，ICAP 與代理伺服器的整合設定以及SMTP 和POP3 與郵件伺服器的整合設定將被重設。如果配置了從 Endpoint Agent 轉送流量到Sensor 伺服器的設定，則這些設定也將被重置。

要還原嵌入式 Sensor：

1. 在應用程式 Web 介面視窗中，選擇“**Sensor 伺服器**”區域。
2. 點擊相關元件的卡片。
   這將開啟一個視窗，其中包含有關元件的資訊。
3. 點擊**刪除**。

4. 元件卡被刪除。

5. 使用 SSH 或終端登入託管相關嵌入式 Sensor 的Central Node 伺服器的管理主控台。

6. 透過執行以下命令提高使用者的權限。

```
sudo -i
```

7. 執行以下指令：

```
kata-sensor-tool reset
kata-sensor-tool init-embedded-sensor
```

嵌入式 Sensor 已還原。有關元件的資訊顯示在**Sensor 伺服器**部分。

如果還原失敗，請聯絡技術支援。

升級 Kaspersky Anti Targeted Attack Platform

在安裝應用程式升級套件之前，建議先為每個要更新的 Central Node 伺服器的當前狀態建立備份，並從應用程式管理員功能表將其下載到硬碟。如果應用程式升級套件安裝失敗，或您需要重新安裝 Kaspersky Anti Targeted Attack Platform，您可以使用應用程式的備份副本。
我們也建議瞭解您要升級到之版本的限制。

您無法透過升級從應用程式的非高可用性版本遷移到高可用性版本，如果您使用的是應用程式的非高可用性版本，則只能在升級期間安裝非高可用性版本，反之亦然。

升級應用程式涉及以下步驟：

1. 升級 Sandbox 元件。

   應用程式沒有升級元件的程式。您必須安裝該元件的 7.1 版本。

   安裝元件後，您需要設定同時運行的虛擬機的最大數量。預設值為 48。

   在 VMware ESXi 虛擬機上安裝元件時，必須設定 *Sandbox 元件計算*部分所述的設定。

2. 升級 Central Node 元件。

   - 如果元件部署在 Ubuntu 作業系統上，您可以透過以下方式升級應用程式：

     - 從版本 7.0.3 到版本 7.1.1。

       在這種情況下，請按照以下說明之一進行操作：*升級安裝在伺服器上的 Central Node* 或*升級作為叢集安裝的 Central Node*。

     - 從版本 7.1 到版本 7.1.1。

       在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1 版升級到 7.1.1 版或 7.1.2 版*部分中的說明進行操作。

     - 從版本 7.1.1 到版本 7.1.3

       在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1 版升級到 7.1.1、7.1.2 版或 7.1.3 版*部分中的說明進行操作。

     - 從版本 7.1.3 到版本 7.1.7。

       在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1.3 版升級到 7.1.7 版*部分中的說明進行操作。

- 如果元件部署在 Astra Linux 作業系統上，並且您需要使用身分驗證版本的應用程式，則可以透過以下方式之一升級元件：

  - 從版本 7.0.3 到版本 7.1.1。

    在這種情況下，請按照以下說明之一進行操作：*升級安裝在伺服器上的 Central Node* 或*升級作為叢集安裝的 Central Node*。

  - 從版本 7.1 到版本 7.1.1。

    在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1 版升級到 7.1.1 版或 7.1.2 版*部分中的說明進行操作。

- 如果元件部署在 Astra Linux 作業系統上，且您不需要身分驗證，則可以透過以下方式之一升級元件：

  - 從版本 7.0.3 到版本 7.1.2。

    在這種情況下，請按照以下說明之一進行操作：*升級安裝在伺服器上的 Central Node* 或*升級作為叢集安裝的 Central Node*。

  - 從版本 7.1 到版本 7.1.2。

    在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1 版升級到 7.1.1 版或 7.1.2 版*部分中的說明進行操作。

  - 從版本 7.1.2 到版本 7.1.3。

    在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1 版升級到 7.1.1、7.1.2 版或 7.1.3 版*部分中的說明進行操作。

  - 從版本 7.1.3 到版本 7.1.7。

    在這種情況下，您需要按照*將 Kaspersky Anti Targeted Attack Platform 從 7.1.3 版升級到 7.1.7 版*部分中的說明進行操作。

  如果您正在使用該應用程式的 7.1.2 版本並想要切換到 7.1.1 版本，則可以部署 7.1.1 版本並將資料從 7.1.2 版本轉移到 7.1.1 版本。為此，您需要建立應用程式版本 7.1.2 的備份副本，並在 7.1.1 版本的伺服器上從該副本還原資料。有關更多資訊，請參閱備份和資料還原部分。

  對於其他版本的應用程式，只能從用同一個版本建立的備份副本進行還原。

> 如果您已經在單台伺服器或叢集上使用 Central Node 7.0.3 元件超過六個月，強烈建議您在升級前執行 fix_old_slots.sh 指令碼清理伺服器或叢集伺服器的磁碟。您可以透過聯絡技術支援服務來取得指令碼檔案及其使用說明。

7.0.3 之前的版本無法升級到 7.1.1 或 7.1.2 版本。如果您使用的是應用程式舊版本，則必須依下列順序將 Central Node 升級至版本 7.0.3：3.7 → 3.7.1、3.7.1 → 3.7.2、3.7.2 → 4.0、4.0 → 4.1、4.1 → 5.0、5.0 → 5.1、5.1 → 6.0、6.0 → 6.0.2、6.0.2 → 6.1、6.1 → 7.0.3。

如果您已經連線並配置了嵌入式 Sensor 的外部儲存，則更新後，您需要按照*還原 Sensor 元件外部儲存中的資料*說明的步驟進行操作。

3. 升級安裝在獨立伺服器上的 Sensor 元件。

   應用程式沒有升級元件的程式。您需要安裝該元件的 7.1.7 版本，同時牢記建議。

4. 升級 Endpoint Agent 元件：
   - Kaspersky Endpoint Security for Windows。
   - Kaspersky Endpoint Security for Linux。
   - Kaspersky Endpoint Security for Mac。

升級伺服器上安裝的 Central Node

在安裝應用程式升級套件之前，建議先為每個要更新的 Central Node 伺服器的當前狀態建立備份，並從應用程式管理員功能表將其下載到硬碟。如果應用程式升級套件安裝失敗，或您需要重新安裝 Kaspersky Anti Targeted Attack Platform，您可以使用應用程式的備份副本。
我們也建議瞭解您要升級到之版本的限制。

如果您使用分散式解決方案和多組織用戶模式，則需要依照下列步驟升級每個 Central Node，而無需斷開 SCN 與 PCN 的連線。

SCN 與 PCN 的斷開是不可逆的，您無法將 SCN 重新連線到任何 PCN 伺服器。

升級以升級套件形式提供。該軟體套件包含在應用程式分發套件中。

要升級伺服器上安裝的 Central Node：

1. 移除連線器、整合伺服器、允許整合的系統清單中的外部系統，以及與正在更新的 Central Node 分開安裝的 Sandbox 與 Sensor 元件。

   以下所述的所有步驟都必須在使用 `sudo -i` 指令提升使用者權限後，在處於技術支援模式的伺服器上執行。

2. 如果您已將 Central Node 從 6.1 或更早版本升級至 7.0.3 版本，請執行下列命令：

   ```
   rm -rf /data/upgrade/
   rm -rf /opt/upgrade_venv
   ```

   如果您從未升級到 7.0.3 版本，請跳過此步驟。

3. 將應用程式升級套件放置在 Central Node 伺服器的 `/data` 目錄中。

4. 透過 SSH 或終端機登入要執行升級的 Central Node 伺服器的管理主控台。

5. 請確保 /dev/sda2 分區上有超過 100 GB 的可用空間。

6. 解壓縮升級存檔：

   - 要升級到版本 7.1.1：

     ```
     tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru-zh.tar.gz -C /data/
     ```

- 要升級到版本 7.1.2：

  ```
  tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru-zh.tar.gz -C /data/
  ```

7. 透過執行以下命令安裝升級套件：

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py
   ```

   顯示使用者名稱輸入視窗。

8. 在顯示的視窗中，在**使用者名稱**欄位中，輸入具有管理員權限的使用者的名稱，選擇**確定**按鈕並按 **Enter**。

   預設值：**admin**。

9. 在顯示的視窗中，在**密碼**欄位中，輸入具有管理員權限的使用者的密碼，選擇**確定**按鈕並按 **Enter**。

   這將開啟一個視窗，用於輸入更新壓縮檔案的路徑。

10. 這將開啟一個視窗；在該視窗中，在**資料目錄**欄位中，輸入更新壓縮檔案的路徑，選擇**確定**按鈕並按 **Enter**。

    預設值：**/data/upgrade**

11. 在顯示的視窗中，選擇 NDR 功能的本地化語言。

    與 NDR 功能相關的應用程式部分將以所選語言顯示。

    一段時間後，主控台將顯示一則訊息，提示您關閉伺服器電源。

12. 顯示提示關閉伺服器電源的訊息後，請執行以下命令：

    ```
    poweroff
    ```

13. 掛載 Kaspersky Anti Targeted Attack Platform 7.1.1 基於 Ubuntu 的 ISO 映像 (kata-cn-7.1.1.531-inst.x86_64_en-ru-zh.iso)。如果您使用基於 Astra Linux 作業系統的 Kaspersky Anti Targeted Attack Platform，請依照說明建立 ISO 映像。

14. 從已安裝 iso 映像的裝置啟動。

15. 在 GRUB 功能表中，選擇**升級 KATA 7.0.3**。

16. 依照精靈的剩餘步驟完成伺服器上的升級。

17. 當升級結束時，透過 SSH 或終端登入到執行了升級的 Central Node 伺服器的管理主控台。

18. 執行下列命令刪除安裝程式的暫存檔案：

    ```
    rm -rf /data/upgrade /data/install_data
    ```

19. 執行以下指令：

    ```
    docker exec -it $(docker ps | grep nta_database | awk '{print $1}') psql -p 5433 -U postgres -d kics -c 'GRANT SELECT ON TABLE kics_webserver.wl_rule_attributes TO kics_webserver;'
    ```

Central Node 元件被升級。

升級後，您必須透過 SSH 或終端重新登入 Central Node 伺服器管理主控台。

在 Astra Linux 伺服器上升級 Central Node 7.0.3 時需要考慮的特殊事項

在 Astra Linux 伺服器上升級 Central Node 7.0.3 時，可能需要更多磁碟空間。如果磁碟空間不足，升級過程將中止，並顯示磁碟空間不足的訊息。

若要在磁碟空間不足時繼續升級：

1. 建立 Central Node 的備份副本並從應用程式的管理員功能表將其下載到您的硬碟磁碟機。
2. 使用該實用程式清理磁碟。

清理磁碟後即可還原升級。

在分佈式解決方案和多租用戶模式下升級後還原嵌入式 Sensor

將分佈式解決方案或多組織用戶模式中使用的Central Node 元件升級到 7.1.1、7.1.2 或 7.1.3 版本後，嵌入式 Sensor 可能會遺失。

要消除限制：

1. 如果在升級 Central Node 元件後，嵌入式Sensor 存在但被停用，請在 Web 介面中移除Sensor。
2. 透過 SSH 或使用終端登入您想要升級嵌入的 Sensor 的 Central Node 伺服器的管理主控台。
3. 系統提示時，輸入管理員使用者名稱和安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。
4. 在應用程式管理員功能表中，選擇技術支援模式。
5. 按 ENTER。
6. 這將開啟技術支援模式確認視窗。
7. 確認您想要在技術支援模式下管理應用程式。為此，請選擇“是”並按 ENTER。
8. 執行以下命令：

   ```
   docker service update --cap-add=CAP_DAC_OVERRIDE --cap-add=CAP_IPC_LOCK --cap-add=CAP_SYS_PTRACE kata_product_main_1_preprocessor_span
   ```
9. 如果嵌入式 Sensor 未還原，請執行以下命令清理資料庫：

   ```
   kata-sensor-tool reset-core
   ```

嵌入式 Sensor 會在大約一分鐘後還原。

清理 Central Node 伺服器磁碟

在 Astra Linux 伺服器上升級 Central Node 時，可能需要更多磁碟空間。如果磁碟空間不足，升級過程將中止，並顯示磁碟空間不足的訊息。您可以透過使用 kata-antiaptdb-cleaner 實用程式釋放 Central Node 伺服器磁碟上的磁碟空間來還原更新過程。當您將 Kaspersky Anti Targeted Attack Platform 升級到 7.1 版本時，此實用程式可用。

該實用程式可能會刪除以下資料：

- 警示資料，包括透過 YARA 技術掃描物件所產生的警示（如果執行該實用程式時指定了相關選項）。
- 偵測資料。
- NDR 事件資料。
- NDR 記錄資料。
- 風險資料。
- 裝置資料。

要使用該實用程式清理磁碟：

1. 透過 SSH 或終端登入要清除磁碟的 Central Node 伺服器的管理主控台。
2. 系統提示時，請輸入管理員使用者名稱和在安裝元件期間指定的密碼。
   顯示應用程式元件管理員功能表。
3. 在應用程式管理員功能表中，選擇**技術支援模式**。
4. 按下 **Enter**。
   這將開啟技術支援模式確認視窗。
5. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按 **ENTER**。
6. 透過執行以下命令安裝磁碟清理實用程式：
   ```
   pip install /data/upgrade/whl/kata_antiaptdb_cleaner/kata_antiaptdb_cleaner-1.0-py2.py3-none-any.whl
   ```
7. 執行以下指令：
   ```
   kata-antiaptdb-cleaner
   ```
   系統會提示您指定要保留資料的天數。預設情況下，保留最近 30 天的資料。
   如果您想保留 1 天的資料，請考慮從啟動實用程式那一刻起保留過去 24 小時的資料。

8. 執行以下操作之一：

   - 如果您要指定保留資料的天數，請輸入數字並按 **ENTER** 鍵。
   - 如果您要跳過此步驟並保留預設設定，請按 **ENTER** 鍵。

   該實用程式執行。資料根據指定的選項被刪除。資料刪除可能需要很長時間才能完成。

您也可以為此命令指定一個或多個參數（請參閱下表）。

實用程式命令列選項描述

必需的參數	參數	敘述
否	`--help`	幫助頁面。
否	`--days <天數>`	您想要保留資料的天數。較舊的資料被刪除。
否	`--clean-yara`	刪除使用 YARA 技術掃描物件時所建立的警示。
使用以下選項執行該實用程式的範例命令： `kata-antiaptdb-cleaner --days 40 --clean-yara`		

升級作為叢集安裝的 Central Node

在安裝應用程式升級套件之前，建議先為每個要更新的 Central Node 伺服器的當前狀態建立備份，並從應用程式管理員功能表將其下載到硬碟。如果應用程式升級套件安裝失敗，或您需要重新安裝 Kaspersky Anti Targeted Attack Platform，您可以使用應用程式的備份副本。
我們也建議瞭解您要升級到之版本的限制。

升級以升級套件形式提供。該套件包含在應用程式分發套件中。

如果您使用分佈式解決方案和多組織用戶模式，則需要依照下列步驟升級每個 Central Node，而無需斷開 SCN 與 PCN 的連線。

SCN 與 PCN 的斷開是不可逆的，您無法將 SCN 重新連線到任何 PCN 伺服器。

要升級作為叢集安裝的 Central Node：

1. 移除連線器、整合伺服器、允許整合的系統清單中的外部系統，以及與正在更新的 Central Node 分開安裝的 Sandbox 與 Sensor 元件。

   以下所述的所有步驟都必須在使用 `sudo -i` 指令提升使用者權限後，在處於技術支援模式的伺服器上執行。

2. 如果您將 Central Node 從 6.1 或更早版本升級到7.0.3 版本，請前往放置 7.0.3 升級套件的叢集伺服器並執行下列命令：

   ```
   rm -rf /data/upgrade/
   rm -rf /opt/upgrade_venv
   ```

如果您從未升級到 7.0.3 版本，請跳過此步驟。

3. 登入Central Node 叢集中的任何一台儲存伺服器，並檢查 Ceph 儲存是否正常運作。為此，請執行以下命令：

   `ceph -s | grep health:`

   如果傳回以下值，表示 Ceph 儲存健康：

   `health: HEALTH_OK`

   如果該值與 `health: HEALTH_OK` 不同，請聯絡技術支援。

4. 登入每台儲存伺服器並重新啟動 kata-osd-starter 服務：

   `systemctl restart kata-osd-starter`

5. 確保 Kafka 服務正常運作：

   a. 找出叢集中哪些伺服器在 Docker Swarm 中具有“管理員”角色。為此，請在任意叢集伺服器上執行以下命令：

      `docker node ls`

      顯示叢集伺服器的清單。檢視清單中的 `MANAGER STATUS` 欄位：如果伺服器在該欄位中有 `Leader` 或 `Reachable`，則表示它具有“管理員”角色。

   b. 執行以下指令：

      `docker service ps kata_product_main_1_schema_registry`

      檢視 `NODE` 列中的值以確定哪個伺服器具有 Schema Registry。

   c. 登入具有 Schema Registry 的伺服器並執行以下命令：

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

      如果您獲得包含主旨清單的 JSON，則表示 Kafka 服務正在執行。

6. 將應用程式升級套件放在 Docker swarm 中具有管理員角色的 Central Node 叢集伺服器上的 `/data` 目錄中。若要檢視角色，請使用 `$ docker node ls` 指令。

7. 透過 SSH 或終端機進入相關伺服器的管理主控台。

8. 請確保叢集中每台伺服器的 /dev/sda2 分區上有超過 100 GB 的可用空間。

9. 解壓縮升級存檔：

   - 要升級到版本 7.1.1：

     `tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru-zh.tar.gz -C /data/`

   - 要升級到版本 7.1.2：

     `tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru-zh.tar.gz -C /data/`

10. 透過執行以下命令安裝升級套件：

    `cd /data/upgrade/`

    `./run_kata_upgrade.py`

    顯示使用者名稱輸入視窗。

11. 在**使用者名稱**欄位中，輸入具有管理員權限的使用者的名稱，選擇**確定**按鈕並按 **Enter**。

    預設值：**admin**。

12. 在**密碼**欄位中，輸入具有管理員權限的使用者的密碼，選擇**確定**按鈕並按 **Enter**。

    這將開啟一個視窗，用於輸入更新壓縮檔案的路徑。

13. 在**資料目錄**欄位中，輸入更新壓縮檔案的路徑，選擇**確定**按鈕並按 **Enter**。

    預設值：**/data/upgrade**。

14. 在顯示的視窗中，選擇 NDR 功能的本地化語言。

    與 NDR 功能相關的應用程式部分將以所選語言顯示。

    一段時間後，主控台將顯示一則訊息，提示您關閉伺服器電源。

15. 透過 SSH 或終端連線到您要關閉的伺服器。

16. 執行 `poweroff` 命令。

17. 掛載 Kaspersky Anti Targeted Attack Platform 7.1.1 基於 Ubuntu 的 ISO 映像 (kata-cn-7.1.1.531-inst.x86_64_en-ru-zh.iso)。如果您使用基於 Astra Linux 作業系統的 Kaspersky Anti Targeted Attack Platform，請依照說明建立 ISO 映像。

18. 從已安裝 iso 映像的裝置啟動。

19. 在 GRUB 功能表中，選擇**升級 KATA 7.0.3**。

20. 依照精靈的剩餘步驟完成伺服器上的升級。

21. 升級完成後，進入步驟 6 所連線的伺服器主控台，輸入 `next`，然後按下 **`Enter`**。

    一個指令碼將被啟動來完成升級過程。更新完成後，主控台會顯示一則訊息，提示您關閉叢集中的下一台伺服器。

22. 對叢集中的每台伺服器重複步驟 14 到 20。

    最後要更新的伺服器是您在步驟 6 中連線的伺服器。對於該伺服器，省略步驟 20：

23. 使用 SSH 或終端登入已配置為從 SPAN 連接埠接收鏡像流量的叢集伺服器管理主控台。

24. 執行以下指令：

    ```
    docker exec -it $(docker ps | grep nta_database | awk '{print $1}') psql -p 5433 -U postgres -d kics -c 'GRANT SELECT ON TABLE kics_webserver.wl_rule_attributes TO kics_webserver;
    ```

25. 執行下列命令刪除安裝程式的暫存檔案：

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    對叢集中的每個伺服器重複此步驟。

Central Node 元件被升級。

更新元件後，您必須透過 SSH 或終端重新登入 Central Node 伺服器管理主控台。

將 Central Node 從版本 7.1 升級到版本 7.1.1 或 7.1.2

在安裝應用程式升級套件之前，建議先為每個要更新的 Central Node 伺服器的當前狀態建立備份，並從應用程式管理員功能表將其下載到硬碟。如果應用程式升級套件安裝失敗，或您需要重新安裝 Kaspersky Anti Targeted Attack Platform，您可以使用應用程式的備份副本。
我們也建議瞭解您要升級到之版本的限制。

如果您使用分散式解決方案和多組織用戶模式，則需要依照下列步驟升級每個 Central Node，而無需斷開 SCN 與 PCN 的連線。

SCN 與 PCN 的斷開是不可逆的，您無法將 SCN 重新連線到任何 PCN 伺服器。

升級以升級套件形式提供。該套件包含在應用程式分發套件中。

要更新 Central Node：

1. 移除連線器、整合伺服器、允許整合的系統清單中的外部系統，以及與正在更新的 Central Node 分開安裝的 Sandbox 和 Sensor 元件。

   以下所述的所有步驟都必須在處於技術支援模式的伺服器上，使用 `sudo -i` 指令提升使用者權限後執行。

2. 如果 Central Node 安裝在伺服器上：

   a. 將應用程式升級套件放置在 Central Node 伺服器的 `/data` 目錄中。

   b. 透過 SSH 或終端機登入要執行升級的 Central Node 伺服器管理主控台。

3. 如果 Central Node 作為叢集安裝

   a. 將應用程式升級套件放在 Docker swarm 中具有管理員角色的 Central Node 叢集伺服器上的 `/data` 目錄中。若要檢視角色，請使用 `$ docker node ls` 指令。

   b. 透過 SSH 或終端機進入相關伺服器的管理主控台。

4. 解壓縮壓縮檔案前，請執行以下指令刪除 `upgrade` 目錄：

   ```
   rm -rf /data/upgrade
   ```

5. 確保 /dev/sda2 檔案系統有超過 140 GB 的可用空間。

6. 解壓縮升級存檔：

   - 要升級到版本 7.1.1：

     ```
     tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru.tar.gz -C /data/
     ```

- 要升級到版本 7.1.2：

  ```
  tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru.tar.gz -C /data/
  ```

7. 透過執行以下命令安裝升級套件：

   - 要升級到版本 7.1.1：

     ```
     cd /data/upgrade/
     ./run_kata_upgrade.py --patch-version 711
     ```

   - 要升級到版本 7.1.2：

     ```
     cd /data/upgrade/
     ./run_kata_upgrade.py --patch-version 712
     ```

   顯示使用者名稱輸入視窗。

8. 在顯示的視窗中，在**使用者名稱**欄位中，輸入具有管理員權限的使用者的名稱，選擇**確定**按鈕並按 **Enter**。
   預設值：**admin**。

9. 在顯示的視窗中，在**密碼**欄位中，輸入具有管理員權限的使用者的密碼，選擇**確定**按鈕並按 **Enter**。
   這將開啟一個視窗，用於輸入更新壓縮檔案的路徑。

10. 這將開啟一個視窗；在該視窗中，在**資料目錄**欄位中，輸入更新壓縮檔案的路徑，選擇**確定**按鈕並按 **Enter**。
    預設值：**/data/upgrade**

11. 在顯示的視窗中，選擇 NDR 功能的本地化語言。
    與 NDR 功能相關的應用程式部分將以所選語言顯示。

12. 執行下列命令刪除安裝程式的暫存檔案：

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    如果您要升級部署為叢集的 Central Node，則必須在叢集中的每個伺服器上執行此命令。

Central Node 元件被升級。

更新完成後，我們建議重新啟動所有更新的 Central Node。如果 Central Node 是以叢集形式安裝，建議逐一重新啟動所有叢集伺服器。

將 Central Node 從版本 7.1.1 或 7.1.2 升級至版本 7.1.3

在安裝應用程式升級套件之前，建議先為每個要更新的 Central Node 伺服器的當前狀態建立備份，並從應用程式管理員功能表將其下載到硬碟。如果應用程式升級套件安裝失敗，或您需要重新安裝 Kaspersky Anti Targeted Attack Platform，您可以使用應用程式的備份副本。
我們也建議瞭解您要升級到之版本的限制。

如果您使用分散式解決方案和多組織用戶模式，則需要依照下列步驟升級每個 Central Node，而無需斷開 SCN 與 PCN 的連線。

SCN 與 PCN 的斷開是不可逆的，您無法將 SCN 重新連線到任何 PCN 伺服器。

升級以升級套件形式提供。該套件包含在應用程式分發套件中。

將 Kaspersky Anti Targeted Attack Platform 升級至版本 7.1.3 後，無法返回認證狀態（版本 7.1.1）。

要更新 Central Node：

1. 移除連線器、整合伺服器、允許整合的系統清單中的外部系統，以及與正在更新的 Central Node 分開安裝的 Sandbox 和 Sensor 元件。

   以下所述的所有步驟都必須在處於技術支援模式的伺服器上，使用 `sudo -i` 指令提升使用者權限後執行。

2. 如果 Central Node 安裝在伺服器上：

   a. 將應用程式升級套件放置在 Central Node 伺服器的 `/data` 目錄中。

   b. 透過 SSH 或終端機登入要執行升級的 Central Node 伺服器管理主控台。

3. 如果 Central Node 作為叢集安裝

   a. 將應用程式升級套件放在 Docker swarm 中具有管理員角色的 Central Node 叢集伺服器上的 `/data` 目錄中。若要檢視角色，請使用 `$ docker node ls` 指令。

   b. 透過 SSH 或終端機進入相關伺服器的管理主控台。

4. 解壓縮壓縮檔案前，請執行以下指令刪除 `upgrade` 目錄：

   ```
   rm -rf /data/upgrade
   ```

5. 確保 /dev/sda2 檔案系統有超過 140 GB 的可用空間。

6. 解壓縮升級存檔：

   ```
   tar xvf /data/kata-upgrade-7.1.3.533-x86_64_en-ru.tar.gz -C /data/
   ```

7. 透過執行以下命令安裝升級套件：

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py --patch-version 713
   ```

   顯示使用者名稱輸入視窗。

8. 在顯示的視窗中，在**使用者名稱**欄位中，輸入具有管理員權限的使用者的名稱，選擇**確定**按鈕並按 **Enter**。

   預設值：**admin**。

9. 在顯示的視窗中，在**密碼**欄位中，輸入具有管理員權限的使用者的密碼，選擇**確定**按鈕並按 **Enter**。

   這將開啟一個視窗，用於輸入更新壓縮檔案的路徑。

10. 這將開啟一個視窗；在該視窗中，在**資料目錄**欄位中，輸入更新壓縮檔案的路徑，選擇**確定**按鈕並按 **Enter**。
    預設值：**/data/upgrade**

11. 在顯示的視窗中，選擇 NDR 功能的本地化語言。
    與 NDR 功能相關的應用程式部分將以所選語言顯示。

12. 執行下列命令刪除安裝程式的暫存檔案：
    `rm -rf /data/upgrade /data/install_data`
    如果您要升級部署為叢集的 Central Node，則必須在叢集中的每個伺服器上執行此命令。

Central Node 元件被升級。

更新完成後，我們建議重新啟動所有更新的 Central Node。如果 Central Node 是以叢集形式安裝，建議逐一重新啟動所有叢集伺服器。

將 Central Node 從版本 7.1.3 升級至版本 7.1.7

在安裝應用程式升級套件之前，建議先為每個要更新的 Central Node 伺服器的當前狀態建立備份，並從應用程式管理員功能表將其下載到硬碟。如果安裝應用程式升級套件失敗，或需要重新安裝 Kaspersky Anti Targeted Attack Platform，您可以使用應用程式的備份副本。
我們也建議您了解要升級到的版本的限制。

如果您使用分佈式解決方案和多租用戶模式，則需要依照下列步驟升級每個 Central Node，而無需斷開 SCN 與 PCN 的連線。

SCN 與 PCN 的斷開是不可逆的，您無法將 SCN 重新連線到任何 PCN 伺服器。

升級以升級套件形式提供。該軟體套件包含在應用程式分發套件中。

要更新 Central Node：

1. 移除連線器、整合伺服器、允許整合的系統清單中的外部系統，以及Sandbox與正在更新的 Central Node 分開安裝的Sensor 元件。

2. 如果 Central Node 安裝在伺服器上：

   a. 將應用程式升級套件放置在 Central Node 伺服器的 `/data` 目錄中。

   b. 透過 SSH 或終端登入要執行升級的 Central Node 伺服器的管理主控台。

3. 如果 Central Node 作為叢集安裝

   a. 將應用程式升級套件放在 Docker swarm 中具有管理員角色的 Central Node 叢集伺服器上的 `/data` 目錄中。若要檢視角色，請使用 `$ docker node ls` 指令。

   b. 透過 SSH 或終端進入相關伺服器的管理主控台。

4. 在解壓縮檔案之前，請執行以下指令刪除升級目錄。

   ```
   rm -rf /data/upgrade
   ```

5. 確保 /dev/sda2 檔案系統有超過 140 GB 的可用空間。

6. 解壓縮升級存檔：

   ```
   tar xvf /data/kata-upgrade-7.1.7.537.1-x86_64_en-ru-zh.tar.gz -C /data/
   ```

7. 透過執行以下命令安裝升級套件：

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py --patch-version 717
   ```

   顯示使用者名稱輸入視窗。

8. 在顯示的視窗中，在“**使用者名稱**”欄位中，輸入具有管理員權限的使用者的名稱，選擇“**確定**”按鈕並按“**Enter**”。

   預設值：**admin**。

9. 在顯示的視窗中，在“**密碼**”欄位中，輸入具有管理員權限的使用者的密碼，選擇“**確定**”按鈕並按“**Enter**”。

   這將開啟一個視窗，用於輸入更新壓縮檔案的路徑。

10. 這將開啟一個視窗；在該視窗中，在“**資料目錄**”欄位中，輸入更新壓縮檔案的路徑，選擇“**確定**”按鈕並按 **Enter**。

    預設值：**/data/upgrade**

11. 在顯示的視窗中，選擇 NDR 功能的本地化語言。

    與 NDR 功能相關的應用程式部分將以所選語言顯示。

12. 執行下列命令刪除安裝程式的暫存檔案：

    ```
    rm -rf /data/upgrade /data/install_data
    ```

    如果您要升級部署為叢集的 Central Node，則必須在叢集中的每個伺服器上執行此命令。

Central Node 元件被升級。

> 更新完成後，我們建議重新啟動所有更新的 Central Node。如果 Central Node 作為叢集安裝，我們建議逐一重新啟動所有叢集伺服器。

升級安裝在獨立伺服器上的 Sensor

該應用程式沒有標準的升級過程。您必須安裝元件版本 7.1.7。

安裝該元件時適用以下建議：

1. 以方便的格式儲存 Sensor 元件的設定；例如，您可以製作螢幕截圖。如果您使用 BPF 和 Regexp 流量篩選，我們建議將篩選規則儲存到檔案中。

2. 安裝 Sensor 元件。

3. 將已安裝的 Sensor 元件連線到 Central Node 元件。

4. 手動還原您已儲存的 Sensor 元件設定。

5. 連線外部儲存。

6. 依照"*還原 Sensor 元件外部儲存中的資料*"說明的步驟，在使用先前版本的應用程式時還原儲存中已儲存的資料。

還原連線到 Sensor 元件的外部儲存上的資料

若要還原連線到 Sensor 元件的外部儲存空間上的資料

1. 如果要將資料還原到連線到嵌入式 Sensor 的外部儲存，請使用 SSH 或終端登入嵌入式 Sensor 所在的 Central Node 伺服器的管理主控台。

2. 如果要將資料還原到與 Central Node 分開安裝的Sensor 元件連線的外部儲存，請使用 SSH 或終端登入 Sensor 伺服器的管理主控台。

3. 系統提示時，請輸入管理員使用者名稱和在安裝元件期間指定的密碼。

   顯示應用程式元件管理員功能表。

4. 在應用程式管理員功能表中，選擇**技術支援模式**。

5. 按下 **Enter**。

   這將開啟技術支援模式確認視窗。

6. 確認您想要在技術支援模式下管理應用程式。為此，請選擇**是**並按 **ENTER**。

7. 執行以下指令：

   find /data/volumes/dumps/traffic -depth -maxdepth 2 -mindepth 2 -type f -exec mv {} /data/volumes/dumps/traffic \;

外部儲存中的資料已還原。

升級 Kaspersky Anti Targeted Attack Platform 時保留的資訊內容與數量

下表列出了 Kaspersky Anti Targeted Attack Platform 從版本 7.1 升級到版本 7.1.1 時保留的內容和資料量的資訊。

將應用程式從版本 7.1 升級到版本 7.1.1 時所保留的內容和資料量

資料類型	升級期間儲存的資料
Central Node 或 PCN 設定	所有資料，除了： • 產品授權金鑰 • Sensor 元件整合設定 • 與 Sandbox 元件整合的設定 • 用於從 Central Node 高可用性版本的 SPAN 連接埠接收映像流量的設定 • 記錄來自 SPAN 連接埠的映像網路流量傾印

資料類型	升級期間儲存的資料
Central Node 或 PCN 上的應用程式資料庫（警示資料庫、應用程式操作監控資料、自訂規則資料庫、工作、政策、已新增至排除項目的規則）。	所有資料，除了： • Kaspersky Anti Targeted Attack Platform 升級至版本 7.1 時在掃描佇列中的檔案。 • Kaspersky Anti Targeted Attack Platform 升級至版本 7.1 時在重新掃描佇列中的檔案。 • 報告資料。 • 允許規則。 • 連線器設定。 • 整合伺服器設定。 • 安裝更新時警示資料已超過 360 天。少於 360 天的警示資料得到保留。
事件資料庫。	所有資料。
儲存及隔離區	所有資料。
Sandbox 工件。	所有資料。

在管理員選單中管理應用程式元件

進入管理員選單之前，請確保以下事項屬實：

- 只能從您授予此類存取權限的電腦存取 Kaspersky Anti Targeted Attack Platform 管理員功能表和伺服器管理主控台。
- 您授予存取權限的電腦位於網路的安全範圍內。

  您可以使用 Iptables 命令列實用程式設定從某些電腦對 Kaspersky Anti Targeted Attack Platform 管理員功能表和伺服器管理主控台的存取。有關管理 iptables 的詳細資訊，請參閱 iptables 檔案。

要在元件管理員選單中開始：

1. 使用 SSH 或終端機登入 Central Node 或 Sandbox 伺服器的管理主控台。
2. 當系統提示時，請輸入管理員使用者名稱，以及在安裝應用程式期間設定的密碼。

   顯示元件管理員選單。

如何使用管理員選單

若要在選單項目之間移動，請按**向上**和**向下**方向鍵。

若要進入選取的選單區段，請按 **ENTER** 鍵。

若要返回上一層選單，請選擇**返回**並按 **ENTER** 鍵。

若要套用設定，請選擇**套用變更**並按 **ENTER** 鍵。

若要選擇水平排列的確認按鈕，請按**向右**和**向左**方向鍵。

若要按下選取的按鈕，請按 **ENTER** 鍵。

若要完成操作，請選擇**登出**。

Central Node 管理員選單

Central Node 選單包含以下選項：

- 閱讀最終使用者產品授權協議、KSN 聲明、隱私權政策或有關第三方代碼的資訊：

  法律資訊 → 顯示 EULA

  法律資訊 → 顯示 KSN 聲明

  法律資訊 → 顯示隱私權政策

  法律資訊 → 第三方代碼

- 選擇用於從 SPAN 連接埠接收鏡像流量的網路協定：

程式設定 → 配置流量擷取 → 設定擷取協定

預設情況下，對所有網路協定（**HTTP2** 除外）啟用從 SPAN 連接埠接收鏡像流量。

- 調整傳入流量的暫存大小：

  程式設定 → 配置儲存 → 變更流量熱環的大小

- 調整檔案儲存大小：

  程式設定 → 配置儲存 → 變更檔案儲存的大小

  "**變更流量熱環的大小**"和"**變更檔案儲存的大小**"區段提供有關傳入流量目前儲存大小以及可放置於儲存中的最大檔案大小的資訊。當您配置應用程式大小時，這些值會自動計算。我們強烈建議**不要**變更這些值。

- 配置系統記錄和偵測的保留期：

  程式設定 → 配置偵測和記錄的儲存期限 → 變更儲存期限

- 設定網路介面：

  網路設定 → 介面配置 → <network interface> → 配置類型

- 配置伺服器上的日期和時間：

  日期和時間設定 → 現在：<date and time> → 變更日期

  日期和時間設定 → 現在：<date and time> → 變更時間

- 變更伺服器的時區：

  日期和時間設定 → 配置時區

- 啟用或停用與 NTP 伺服器的同步：

  日期和時間設定 → 啟用 NTP 同步

- 新增或刪除 NTP 伺服器：

  日期和時間設定 → NTP：<N> 個項目 → 新增（新增新的 NTP 伺服器）

  日期和時間設定 → NTP：<N> 個項目 → <NTP server>（刪除先前新增的 NTP 伺服器）

- 檢視伺服器 SSH 金鑰：

  系統管理 → 顯示 SSH 主機金鑰

- 備份伺服器資料：

  系統管理 → 備份/還原設定 → 新增

- 從備份還原資料：

  系統管理 → 備份/還原設定 → <backup file name>

- 變更管理員密碼：

  系統管理 → 變更管理員密碼

- 進入技術支援模式：

  技術支援模式

- 下載系統日誌或刪除先前下載的日誌：

  下載系統記錄 → 新增（下載新的系統記錄）

  下載系統記錄 → <system log>（刪除先前下載的系統記錄）

- 重新啟動伺服器：

  重啟機器

- 關閉伺服器：

  關閉機器

- 完成管理管理員選單並退出：

  Logout

Sensor 管理員選單

> 如果您選擇了網路協定來從 SPAN 連接埠取得映像流量，在將獨立 Sensor 連線到 Central Node **之前**在其上配置了檔案儲存大小或流量擷取頻寬，並且想要在連線**後**變更這些設定，您需要按照以下步驟準備變更設定。完成準備後，即可變更設定。

Sensor 管理員選單包含以下選項：

- 閱讀最終使用者產品授權協議、KSN 聲明、隱私權政策或有關第三方代碼的資訊：

  法律資訊 → 顯示 EULA

  法律資訊 → 顯示 KSN 聲明

  法律資訊 → 顯示隱私權政策

  法律資訊 → 第三方代碼

- 查看伺服器使用的 TLS 憑證：

  程式設定 → 管理伺服器憑證 → 檢視憑證資訊

- 套用先前上傳的 TLS 憑證：

  程式設定 → 管理伺服器憑證 → 從檔案安裝

- 為伺服器產生新的 TLS 憑證：

  程式設定 → 管理伺服器憑證 → 產生新的

- 下載伺服器使用的的 TLS 憑證：

  程式設定 → 管理伺服器憑證 → 取得目前憑證

- 選擇用於從 SPAN 連接埠接收鏡像流量的網路協定：

  程式設定 → 配置流量擷取 → 設定擷取協定

  預設情況下，對所有網路協定（**HTTP2** 除外）啟用從 SPAN 連接埠接收鏡像流量。

- 配置流量擷取頻寬：

  程式設定 → 設定流量擷取 → 流量擷取頻寬（Mbps）

- 調整檔案儲存大小：

  程式設定 → 配置儲存 → 變更檔案儲存的大小

- 調整傳入流量的暫存大小：

程式設定 → 配置儲存 → 變更流量熱環的大小

> 本部分告知您傳入流量的目前儲存大小。當您配置應用程式大小時，會自動計算儲存大小。我們強烈建議**不要**變更此值。

- 限制傳送到 Central Node 進行掃描的檔案的大小：
  程式設定 → 配置物件處理 → 檔案大小限制
- 配置系統記錄和偵測的保留期：
  程式設定 → 配置偵測和記錄的儲存期限 → 變更儲存期限
- 啟用或停用代理伺服器：
  程式設定 → 配置代理 → 已啟用
- 設定代理伺服器 IP 位址：
  程式設定 → 配置代理 → 主機
- 設定代理伺服器連接埠：
  程式設定 → 配置代理 → 連接埠
- 設定代理伺服器身分驗證使用者名稱：
  程式設定 → 配置代理 → 使用者名稱
- 編輯代理伺服器整合設定：
  程式設定 → 配置代理 → 編輯
- 連線到本機網路位址時啟用和停用代理伺服器：
  程式設定 → 配置代理 → 本機位址
- 設定網路介面：
  網路設定 → 介面配置 → <network interface> → 配置類型
- 配置 DNS：
  網路設定 → DNS 解析器配置
- 配置伺服器上的日期和時間：
  日期和時間設定 → 現在：<date and time> → 變更日期
  日期和時間設定 → 現在：<date and time> → 變更時間
- 變更伺服器的時區：
  日期和時間設定 → 配置時區
- 啟用或停用與 NTP 伺服器的同步：
  日期和時間設定 → 啟用 NTP 同步
- 新增或刪除 NTP 伺服器：
  日期和時間設定 → NTP：<N> 個項目 → 新增（新增新的 NTP 伺服器）
  日期和時間設定 → NTP：<N> 個項目 → <NTP server>（刪除先前新增的 NTP 伺服器）

- 變更管理員密碼：
  密碼 → 變更系統管理員帳戶密碼
- 檢視伺服器 SSH 金鑰：
  系統管理 → 顯示 SSH 主機金鑰
- 設定 SNMP 連線：
  系統管理 → SNMPd 監控設定
- 進入技術支援模式：
  技術支援模式
- 下載系統日誌或刪除先前下載的日誌：
  下載系統記錄 → 新增（下載新的系統記錄）
  下載系統記錄 → <system log>（刪除先前下載的系統記錄）
- 重新啟動伺服器：
  重啟機器
- 關閉伺服器：
  關閉機器
- 完成管理管理員選單並退出：
  Logout

Sandbox 管理員選單

Sandbox 管理員選單包含以下選項：

- 進入技術支援模式：
  技術支援模式
- 設定網路介面：
  網路設定 → 管理介面
- 在 Sandbox 中設定虛擬機器的網際網路存取：
  網路設定 → 惡意軟體介面
- 配置網路路由：
  網路設定 → IPv4 路由
- 配置 DNS：
  網路設定 → DNS 設定
- 變更管理員密碼：
  變更系統管理員帳戶密碼

- 重新啟動伺服器：

  重啟機器

- 關閉伺服器：

  關閉機器

- 完成管理管理員選單並退出：

  Logout

使用 KATA 和KEDR API

您可以設定 Kaspersky Anti Targeted Attack Platform 與外部系統的整合，以管理威脅回應操作、掃描儲存在這些系統中的檔案、以及向外部系統提供對所有警示和事件的資訊的存取。

API 方法呼叫僅適用於被授權的外部系統。對於授權，應用程式管理員必須建立將外部系統與應用程式整合的請求。然後，管理員必須在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中處理該請求。

如果您已將 Central Node 和 Sensor 元件部署為叢集，則可以使用下列選項之一配置與外部系統的高可用性整合：

- 使用輪詢調度演算法功能。
- 設定外部系統，以便在發生逾時時外部系統可在叢集伺服器的 IP 位址之間切換。

若要使用輪詢調度演算法功能配置與外部系統的高可用性整合：

1. 在 Central Node 叢集對應網域的 DNS 伺服器上設定輪詢調度演算法。
2. 在郵件伺服器設定中指定此網域名稱。

與外部系統的整合是基於網域名稱配置的。外部系統將與叢集中的隨機伺服器進行通訊。如果該伺服器發生故障，外部系統將與叢集中另一台健康的伺服器進行通訊。

將外部系統與 Kaspersky Anti Targeted Attack Platform 整合

要開始使用 API，您需要將外部系統與 Kaspersky Anti Targeted Attack Platform 整合。外部系統必須在 Kaspersky Anti Targeted Attack Platform 伺服器上完成授權。

若要將外部系統與 Kaspersky Anti Targeted Attack Platform 整合：

1. 產生一個用於在 Kaspersky Anti Targeted Attack Platform 中授權的外部系統的唯一識別碼 – `sensorId`。
2. 為外部系統伺服器產生憑證。
3. 在 Kaspersky Anti Targeted Attack Platform 中建立來自外部系統且包含 `sensorId` 的任何請求。例如，您可以建立在 Kaspersky Anti Targeted Attack Platform 中掃描外部系統物件的請求。

Kaspersky Anti Targeted Attack Platform 的 Web 介面將顯示來自外部系統的授權請求。聯絡應用程式管理員以處理請求。

如果您需要變更外部系統伺服器憑證，請重複將外部系統與 Kaspersky Anti Targeted Attack Platform 整合的步驟。

用於掃描外部系統物件的 API

Kaspersky Anti Targeted Attack Platform 提供 HTTPS REST 接口，用於掃描儲存在外部系統中的物件。

對於掃描儲存在外部系統中的物件，建議使用以下 Kaspersky Anti Targeted Attack Platform 互動方案：

1. **建立使用 HTTP POST 方法掃描物件的請求**
2. **建立使用 HTTP GET 方法的掃描結果請求**

   API 介面是異步的，這表示 Kaspersky Anti Targeted Attack Platform 在後台掃描物件，而不是在外部系統請求時立即掃描。因此，您必須使用 HTTP GET 方法定期從外部系統傳送請求以接收掃描結果。傳送請求的建議頻率是每分鐘一次。

   您也可以在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中配置有關偵測到的物件的通知轉送。

3. **建立使用 HTTP 方法刪除掃描結果的請求 DELETE**

   您可以刪除掃描指定物件或所有物件的結果。

使用叢集

如果外部系統由組合成一個叢集的多台伺服器組成，建議對所有伺服器使用一個 ID（ sensorId ）。如果是這種情況，將在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中顯示整個系統的單個整合請求。如果需要區分各個伺服器接收的掃描結果，則可以為每台伺服器指派唯一的實例 ID（ sensorInstanceId ）。

限制

在 Kaspersky Anti Targeted Attack Platform 設定檔中設定來自外部系統的最大允許物件掃描請求數和掃描物件的最大允許大小。

如果超過允許的同時物件掃描請求的最大數量，Kaspersky Anti Targeted Attack Platform 將不會處理進一步的請求，直到物件掃描請求的數量小於允許的最大數量。在滿足此條件之前，將發出回傳代碼 429。您必須稍後再次嘗試掃描請求。

如果超出允許的最大物件大小，則 Kaspersky Anti Targeted Attack Platform 不會掃描物件。建立 HTTP POST 方法時會產生返回代碼 413。您可以使用 GET 方法檢視物件掃描限制清單，以了解物件允許的最大大小。

請求掃描物件

若要建立掃描物件的請求，請使用 HTTP POST 方法。例如，您可以使用 CURL 命令列實用程式建立請求。

您可以使用附加開關來設定執行 cURL 指令的參數（請參閱下表）。

有關 cURL 命令開關的更多資訊，請參閱 cURL 檔案。

命令語法

curl --cert <TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X POST "<Central Node 元件伺服器的URL>:<連接埠，預設為 443>/kata/scanner/v1/sensors/<sensorId>/scans?sensorInstanceId=<sensorInstanceId>" -F "content=<要掃描的檔案的路徑>" -F scanId=<掃描請求 ID> -F "objectType=file"

如果請求成功處理，將顯示 OK 狀態。

設定

參數	類型	敘述
sensorId	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
content	檔案	掃描物件的內容。
scanId	string	掃描請求的唯一 ID。它必須在外部系統中產生。它不能包含空格或特殊字元。請勿使用檔案名稱作為掃描請求 ID。 如果未定義此參數，則無法檢視掃描結果。
objectType	string	掃描物件的類型。 參數的可能值： 檔案 。
sensorInstanceId	string	外部系統實例的唯一 ID。組合成一個叢集的伺服器也被視為外部系統的實例。此參數是可選的。

返回值

返回碼	敘述
200	掃描物件的請求已成功建立。
401	需要授權。
429	超過的請求數。稍後重複該請求。
500	未知伺服器錯誤。稍後重複該請求。

輸入具有開關的命令的範例

```
curl --cert /root/cert.pem --key /root/server.key -
X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?
sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F "objectType=file"
```

請求掃描結果

若要建立接收掃描結果的請求，請使用 HTTP `GET` 方法。例如，您可以使用 cURL 命令列實用程式建立請求。

您可以使用附加開關來設定執行 cURL 指令的參數（請參閱下表）。

有關 cURL 命令開關的更多資訊，請參閱 cURL 檔案。

命令語法

```
curl --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X GET "<Central Node 元件伺服器的URL>:<連接埠，預設 443>/kata/scanner/v1/sensors/<sensorId>/scans/state?sensorInstanceId=<sensorInstanceId>&state=<您想要在掃描結果中顯示的一個或多個掃描狀態>"
```

如果請求傳送成功，則會顯示掃描物件的請求清單以及掃描這些物件的結果。掃描結果將會依照您在 `state` 參數中指定的狀態進行篩選。例如，如果您在掃描結果請求中指定 `state=processing,detect`，則應用程式將只顯示正在處理或應用程式在其中偵測到威脅的物件掃描請求。

設定

參數	類型	敘述
`sensorId`	string	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
`state`	array（字串元素類型）	物件掃描狀態。定義此參數後，將依狀態篩選掃描結果。 指示一種或多種狀態，以逗號分隔。 可以使用以下參數值： • `detect` • `not detected` • `processing` • `timeout` • `error`
`sensorInstanceId`	string	外部系統實例的唯一 ID。組合成一個叢集的伺服器也被視為外部系統的實例。此參數是可選的。

Response

HTTP 代碼：200

格式：JSON

```
type Response []Scans

type Scans struct {
ScanID integer `json:"scanId"`
State array `json:"state"`
}
```

返回值

返回碼	敘述
204	沒有內容。
404	未找到指定 ID 的掃描結果。
500	未知伺服器錯誤。稍後重複該請求。

如果要在掃描結果中顯示所有物件掃描狀態時輸入帶有開關的命令的範例

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/state?sensorInstanceId=instance1&state=detect,not%20detected,processing,error,timeout"
```

請求刪除掃描結果

若要建立刪除一個或多個物件的掃描結果的請求，請使用 DELETE 方法。例如，您可以使用 CURL 命令列實用程式建立請求。

命令語法

curl --cert <TLS 憑證檔案的路徑> --key <私密金鑰檔案的路徑> -X DELETE "<具有 Central Node 元件的伺服器的 URL>:<連接埠，預設為 443>/kata/scanner/v1/sensors/<sensorId>/scans/<scanId>"

如果請求成功處理，物件掃描結果將會被刪除。OK 狀態將顯示。

設定

參數	類型	敘述
sensorId	string	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
scanId	string	物件掃描請求的唯一 ID。如果未定義此參數，則將刪除所有物件的掃描結果。

返回值

返回碼	敘述
200	刪除掃描結果的請求已成功建立。
401	需要授權。
404	未找到指定 ID 的掃描結果。
500	未知伺服器錯誤。稍後重複該請求。

命令輸入範例

```
curl --cert /root/cert.pem --key /root/server.key -
X DELETE "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/1"
```

請求顯示物件掃描限制

若要建立請求以顯示應用程式對掃描物件的限制（例如，按大小），請使用 HTTP `GET`方法。例如，您可以使用 CURL 命令列實用程式建立請求。

命令語法

`curl --cert <TLS 憑證檔案的路徑> --key <私密金鑰檔案的路徑> -X GET "<具有 Central Node 元件的伺服器的 URL>:<連接埠，預設為 443>/kata/scanner/v1/sensors/<sensorId>/scans/filters"`

如果請求成功處理，將顯示應用程式的物件掃描限制。例如，`maxObjectSize`限制是您可以提交進行掃描的物件的最大允許大小。

設定

參數	類型	敘述
sensorId	string	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。

Response

HTTP 代碼：200

格式：JSON

```
type Response struct {
MaxObjectSize integer `json:"maxObjectSize"`
Version string `json:"version"`
}
```

返回值

返回碼	敘述
401	需要授權。
500	未知伺服器錯誤。稍後重複該請求。

命令輸入範例

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/filters"
```

外部系統可用於接收應用程式警示資訊的 API

Kaspersky Anti Targeted Attack Platform 提供一個 API，允許外部系統存取有關應用程式所有警示的資訊，而不僅僅是掃描這些外部系統中儲存的物件的結果。

為了僅接收符合特定條件的警示訊息，您可以在請求參數中指定篩選器。

> 應用程式不會根據先前的請求自動傳送有關新警示的資訊。必須傳送新請求才能接收最新資訊。

分佈式解決方案中操作的特殊注意事項

如果應用程式在分佈式解決方案模式下執行，必須為要從其接收警示資訊的每個 PCN 和 SCN 伺服器單獨配置與外部系統的整合。此限制是由於 PCN 伺服器的 Web 介面顯示所有警示資訊，但警示資料庫僅儲存已在該特定伺服器上註冊的那些警示。

請求顯示警示資訊

您可以建立請求，以取得有關由以下技術掃描產生的警示資訊：

- 惡意軟體防護引擎。
- Sandbox。
- YARA。
- URL 信譽。
- 入侵偵測系統。
- 入侵偵測系統 (NDR)。
- 聚合警示 (NDR)。

無法透過 API 查詢目標攻擊分析和 IOC 技術產生的警示資訊。

若要建立請求以顯示有關 Kaspersky Anti Targeted Attack Platform 警示的資訊，請使用 HTTP `GET` 方法。例如，您可以使用 CURL 命令列實用程式建立請求。

命令語法

`curl --cert <TLS 憑證檔案的路徑> --key <私鑰檔案的路徑> -X GET "<Central Node 元件伺服器的 URL>:<連接埠，預設為 443>/kata/scanner/v1/sensors/<sensorId>/detects?detect_type=<用於產生警示的一種或多種技術>&limit=<回應請求中的警示數量>&token=<請求 ID>"`

如果請求處理成功，您將在外部系統的伺服器上看到 Kaspersky Anti Targeted Attack Platform 產生的警示清單。

設定

參數	類型	敘述
`sensorId`	string	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
`detect_type`	Array	建立警示的技術。您可以指定以逗號分隔的技術清單。 可能值： • `am` – 惡意軟體防護引擎 • `sb` – Sandbox • `yara` – YARA • `url_reputation` – URL 信譽 • `ids` – 入侵偵測系統 • `NDR_Ids` – 入侵偵測系統 (NDR)。 • `NDR_External` – 聚合警示 (NDR)。 如果未指定此參數，則提供上述所有警示的資訊。

參數	類型	敘述
limit	integer	為了回應請求而為其提供資訊的物件的數量。允許的值：1 到 10000 之間的整數。 預設值為 1000。
token	string	請求 ID。如果指定該參數，則重複請求不會顯示先前請求獲得的警示資訊。這有助於避免在重複請求時出現有關相同警示的重複資訊。 如果未指定此參數，則提供有關所有警示的資訊。

Response

HTTP 代碼：200

格式：JSON

```
type Response struct {
Detects array `json:"detects"`
Token string `json:"token"`
}
```

返回值

返回碼	敘述
400	參數不正確。
429	超過的請求數。
401	需要授權。
500	未知伺服器錯誤。稍後重複該請求。

輸入具有開關的命令的範例

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a20307d"
```

傳輸資料的範圍

下表列出了為每個偵測傳輸的資訊。

警示傳輸的資訊範圍

參數	值	敘述
alertID	整數值。	警示 ID。
eventTimeStamp	日期和時間。	事件時間。
detectTimestamp	日期和時間。	Kaspersky Anti Targeted Attack Platform 資料庫中記錄警示資訊的時間。

參數	值	敘述
`importance`	以下值之一： • 高 • 中 • 低	警示重要性。
`objectSource`	以下值之一： • `web` • `mail` • `endpoint` • `external` • `dns`	偵測到的物件的來源。
`technology`	以下值之一： • `am` – 惡意軟體防護引擎 • `sb` – Sandbox • `yara` – YARA • `url_reputation` – URL 信譽 • `ids` – 入侵偵測系統	用於偵測物件的技術。
`objectType`	以下值之一： • 檔案。 • 電子郵件。 • 主機（用於遠端網域或主機）。	偵測物件的類型。 如果在電子郵件掃描期間執行偵測（電子郵件 物件類型），偵測詳細資訊還可能包含以下內容： • `mailFrom` – 郵件的來源位址 • `rcptTo` – 郵件的目標位址
`object`	取決於偵測物件的類型。	偵測物件的資料。
`detection`	取決於用於偵測物件的技術。	有關偵測到的威脅的資料。
`details`	取決於偵測到的物件的來源。	有關偵測到的物件的環境資料。

有關偵測到的物件的資料

下表列出了偵測到的物件的傳輸資料範圍，具體取決於物件的類型。

有關偵測到的物件的資料

	參數	資料類型	敘述	範例
file	processedObject.MD5	MD5	被傳送進行掃描的檔案或複合物件的 MD5 雜湊值。	1839a1e9621c58dadf782e131df3821f
	processedObject.SHA256	SHA256	被傳送進行掃描的檔案或複合物件的 SHA256 雜湊值。	7bbfc1d690079b0c591e146c4294305da1cee857e12db40f431
	processedObject.fileName	String	被傳送進行掃描的檔案或複合物件的名稱。	EICAR-CURE.com
	processedObject.fileType	String	被傳送進行掃描的檔案或複合物件的類型。	GeneralTxt
	processedObject.fileSize	Integer	被傳送進行掃描的檔案或複合物件的大小（以位元組為單位）。	184
	detectedObject.MD5	MD5	在其中偵測到威脅的檔案（簡單物件或複合物件中的檔案）的 MD5 雜湊值。	1839a1e9621c58dadf782e131df3821f
	detectedObject.fileName	String	在其中偵測到威脅的檔案（簡單物件或複合物件中的檔案）的名稱。	EICAR-CURE.com
	detectedObject.fileSize	integer	在其中偵測到威脅的檔案（簡單物件或複合物件中的檔案）的大小（以位元組為單位）。	184
URL	detectedObject	String	偵測到的物件的 URL。	http://example.com/link
host	detectedObject	Array	偵測到的物件所屬的網域清單。 對於 URL 技術以及具有 objectSource=dns 參數的物件，此清單可以包含多個域。	example.org，example.net

有關偵測到的威脅的資料

下表列出了偵測到的威脅的傳輸資料範圍，具體取決於用於產生警示的技術。

有關偵測到的威脅的資料

technology	參數	敘述	資料類型	範例
以下技術之一： • 惡意軟體防護引擎。 • YARA。 • 入侵偵測系統。	detect	偵測到的威脅的清單。	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	dataBaseVersion	用於掃描檔案的資料庫的版本。	integer	201811190706

technology	參數	敘述	資料類型	範例
Sandbox	detect	偵測到的威脅的清單。	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	image	掃描檔案的虛擬機映像的名稱。	String	Win7
	dataBaseVersion	資料庫版本採用以下格式：<用於掃描檔案的應用程式資料庫版本> / <IDS 模組資料庫版本>。	integer	201902031107/ 201811190706
URL 信譽	detect	偵測物件的 URL 信譽類別清單（適用於 URL 或主機類型的物件）。	Array	釣魚主機、惡意主機、殭屍網路 C&C (Backdoor.Win32.Mokes)

有關偵測到的物件的環境資料

下表列出了有關偵測到的物件的環境的傳輸資料的範圍，具體取決於物件的來源。

有關偵測到的物件的環境資料

物件的來源	參數	敘述	資料類型	範例
web	sourceIP	建立連線的電腦的 IP 位址。	IP 位址	192.0.2.0
	sourceHostname	建立連線的電腦的名稱。	字串	example.com
	destinationIp	與其建立了連線的電腦的 IP 位址。	IP 位址	198.51.100.0
	destinationPort	與其建立連線的電腦的連接埠。	integer	3128
	URL	被存取的 Web 資源的 URL。 IDS 技術可偵測沒有此參數。 對於 URL 技術偵測，此參數與 detectedObject 參數具有相同的值。	String	https://example.com:443/
	method	HTTP 請求方法。	String	Connect
	referrer	從起進行重新導向的 URL。	String	https://example.com:443/
	agentString	HTTP 請求的使用者代理標頭，包含用戶端應用程式的名稱和版本。	String	Mozilla/4.0
mail	mailFrom	寄件者的電子郵件信箱。	String	sender@example.com
	mailTo	以逗號分隔的收件者電子郵件信箱清單。	Array	recipient1@example.com，recipient2@example.com
	subject	郵件主旨。	String	'您是贏家'

物件的來源	參數	敘述	資料類型	範例
	messageId	電子郵件 ID。	String	1745028736.156014.1542897410859.JavaMail.svc_jira_pool
• endpoint • external	hostName	產生偵測的電腦的名稱。	String	computername.example.com
	IP	產生偵測的電腦的 IP 位址。	IP 位址	198.51.100.0
dns	sourceIP	發起 DNS 連線的電腦的 IP 位址。	IP 位址	192.0.2.0
	destinationIp	與其建立 DNS 連線的電腦（通常是 DNS 伺服器）的 IP 位址。	IP 位址	198.51.100.0
	destinationPort	與其建立 DNS 連線的電腦（通常是 DNS 伺服器）的連接埠。	integer	3128
	dnsMessageType	DNS 訊息類型： • Request • Response	String	Request
	dnsRequestType	以下DNS 請求類型之一： • A。 • AAA。 • CNAME。 • MX。	String	MX
	domainToBeResolved	來自DNS 請求的網域名稱。	字串	example.com

外部系統可用於接收應用程式事件資訊的 API

Kaspersky Anti Targeted Attack Platform 為外部系統提供 API，可用於存取有關應用程式註冊的事件的資訊。

若要僅接收符合特定條件的事件的資訊，您可以在請求參數中指定篩選器。

> 應用程式不會根據先前的請求自動傳送有關新事件的資訊。必須傳送新請求才能接收最新資訊。

新事件資訊在這些事件出現在 Kaspersky Anti Targeted Attack Platform 資料庫中後的兩個小時內即可檢索。

分佈式解決方案中操作的特殊注意事項

如果應用程式在分佈式解決方案模式下執行，必須為要從其接收事件的每個 PCN 和 SCN 伺服器單獨配置與外部系統的整合。此限制是由於 PCN 伺服器的 Web 介面顯示有關所有事件的資訊，但事件資料庫僅儲存已在該特定伺服器上註冊的事件。

查詢事件資訊的請求

若要建立獲取事件資訊的請求，請使用 HTTP GET 方法。

您可以使用附加開關來設定執行 cURL 指令的參數（請參閱下表）。

有關 cURL 命令開關的更多資訊，請參閱 cURL 檔案。

在第一次要求時，Kaspersky Anti Targeted Attack Platform 會建立一個 *ContinuationToken*（以下也稱為“權杖”）。應用程式在建立權杖時會傳送系統中可用的事件。建立新權杖時，Kaspersky Anti Targeted Attack Platform 會傳送建立此權杖時系統中可用的事件。

權杖包含有關最後傳輸的資料的資訊。如果您想接收上次請求後記錄的事件，則必須儲存已建立的權杖並在以後的請求中使用它。

命令語法

對於第一個請求：

```
curl --cert <TLS 憑證檔案的路徑> --key <私鑰檔案的路徑> -X GET "<Central Node 元件伺服器的URL>:<連接埠，預設為 443>/kata/events_api/v1/<external_system_id>/events"
```

如果請求處理成功，會顯示有關請求的事件和權杖值的資訊。

對於後續請求：

```
curl --cert <TLS 憑證檔案的路徑> --key <私鑰檔案的路徑> -X GET "<Central Node 元件伺服器的URL>:<連接埠，預設為
443>/kata/events_api/v1/<external_system_id>/events&continuation_token=<第一個請求收到的權杖值>"
```

如果請求處理成功，則會顯示自上次請求以來收到的事件的資訊。

您可以透過指定最大收集時間和事件數量以及事件篩選參數來建立輸出事件資訊的請求：

```
curl --cert <TLS 憑證檔案的路徑> --key <私鑰檔案的路徑> -X GET "<Central Node 元件伺服器的URL>:<連接埠，預設為 443>/kata/events_api/v1/<external_system_id>/events?filter=<事件篩選器>&max_timeout=<最大事件收集時間>&max_events=<最大事件數>&continuation_token=<第一個要求收到的權杖值>"
```

如果您為第一個請求指定了篩選參數的值，則不必在後續請求中指定它：篩選參數會從上一個請求中儲存下來，並且在後續請求中沒有傳遞新參數時使用。如果您不想使用篩選，請不要指定該參數的值。

設定

參數	類型	敘述
`external_system_id`	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
`filter`	string	事件篩選設定。這些是使用事件查詢語言設定的。
`max_timeout`	int	最大事件收集時間。按以下格式指定：PT<整數值>S。例如，PT300S。伺服器傳送在指定時間內收集的事件的資訊。 預設值為 5 分鐘。除非請求中另有指定，否則使用該值。 最大事件收集時間不得超過 5 分鐘。如果指定的值大於 5 分鐘，Central Node 伺服器將傳回錯誤。 等待事件的實際總時間可能會增加。
`max_events`	int	最大事件數 如果請求中未指定值，Kaspersky Anti Targeted Attack Platform 將根據安裝了 Endpoint Agent 元件的主機數量來計算該值。 典型配置的值範例： • 對於 1000 台主機：64000。 • 對於 5000 台主機：128000。 • 對於 10000 台主機：208000。 • 對於 15000 名主機：288000。 • 對於30000 台主機：528000。 請求中指定的值不得超過這些限制。
`continuation_token`	String	權杖值。

輸入帶有參數的命令的範例

```
curl --cert <TLS 憑證檔案的路徑> --key <私鑰檔案的路徑> -X GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events"
```

```
curl --cert <TLS 憑證檔案的路徑> --key <私密金鑰檔案的路徑> -X GET
"https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&continuation_token=
CiQyZDcyNjNiOS0zZmNlLTQxNzktYTdhOC03N2E0ZmUwNjNjMTkSBAgAEAoSBAgBEAMSBAgCEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

如果參數值包含特殊字元，則必須在請求中使用 URL 編碼或 `--data-urlencode` 選項。

帶有 URL 編碼參數的命令範例

```
curl --cert <TLS 憑證檔案的路徑> --key <私密金鑰檔案的路徑> -X GET
"https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&continuation_token=
CiQ%3Dcy%7ENiOS0zZmNlLTQxNzktYTdhOC03N2E0Z40%wNjNjMTkSBAgAEAoSBAgB%5EMSB%3CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

使用 `--data-urlencode` 選項之參數的命令範例

```
curl --cert <TLS 憑證的路徑> --key <私密金鑰檔案的路徑> --GET -d "max_events=64000" -d "max_timeout=PT300S" -d
"filter=EventType=='threatdetect'" --data-urlencode "continuation_token=
CiQ?Dcy~NiOS0zZmNlLTQxNzktYTdhOC03N2E0Z@wNjNjMTkSBAgAEAoSBAgB^MSB?CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw" https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-
3d23b20dd609/events
```

Response

HTTP 代碼：200

格式：JSON

```
type Response struct {
Events array `json:"events"`
ContinuationToken string `json:"continuationToken"`
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

用於篩選事件的查詢語言

事件篩選查詢語言支援以下函數和運算子：

- 功能：`in`。
- 字串或布林值的比較運算子：
  - `==`
  - `!=`
- 數字和變數的比較運算子：
  - `AND`
  - `OR`

- NOT
- ==
- !=
- >
- >=
- <
- <=

您可以在事件篩選欄位部分中檢視可用於篩選事件的欄位清單。

如果您想要接收有關不同類型事件的資訊，則必須為每種類型的事件建立單獨的請求。

```
EventType=='threatdetect' OR EventType=='threatprocessingresult'
```

支援數字和字串常數。字串常數必須帶單引號：`'example'`。字串常數支援萬用字元 * 和 ?。如果您不想使用這些字元作為通配符，則必須對它們進行轉義：`\*`，`\?`。另外，在字串常數中，必須對特殊字元進行轉義。

用於篩選事件的欄位

下表列出了用於篩選事件的欄位。

> 如果欄位值包含特殊字元，則必須使用 URL 編碼或請求中的 `--data-urlencode` 選項。

用於篩選事件的欄位清單

欄位名稱	類型	敘述
hostName	String	主機名稱。
HostIp	String	主機的 IP 位址。
EventType	String	事件類型。可能值： • process — 處理程序已開始。 • process_terminate — 處理程序已終止。 • module — 模組已載入。 • connection — WMI 遠端連線。 • applock — 防護規則。 • blockdocument — 檔案被封鎖。 • filechange — 檔案已修改。 • windowsevent — 系統事件日誌。 • registry — 登錄檔已修改。 • portlisten — 監聽的連接埠。 • driver — 驅動程式已載入。 • threatdetect — 警示。 • threatprocessingresult — 警示處理結果。 • amsiscan — AMSI 掃描。 • process_interpretated_file_run — 檔案的已解釋運行。 • process_console_interactive_input — 在主控台上互動式輸入指令。
UserName	String	使用者名稱。
OsFamily	String	作業系統系列。
OsVersion	String	主機上使用的作業系統版本。

欄位名稱	類型	敘述
Ioa.Rules.Id	String	TAA (IOA) 規則 ID。
Ioa.Rules.Name	String	有關使用 Targeted Attack Analyzer 技術進行檔案分析的結果的資訊：用於建立警示的 TAA (IOA) 規則的名稱。
Ioa.Rules.Techniques	String	MITRE 技術
Ioa.Rules.Tactics	String	MITRE tactic
Ioa.Severity	String	指派給使用此 TAA (IOA) 規則產生的事件的重要性等級。 可能值： • 低 • 中 • 高
Ioa.Confidence	String	置信度取決於規則引起誤報的可能性。 可能值： • 低 • 中 • 高
FileCreationTime	integer	檔案建立時間。
DllCreationTime	integer	DLL 建立時間。
DroppedCreationTime	integer	被修改檔案的建立時間。
InterpretedFileCreationTime	integer	被解釋檔案的建立時間。
FileName	String	檔案名稱。
DllName	String	DLL 名稱。
DroppedName	String	被修改檔案的名稱。
BlockedName	String	被封鎖檔案的名稱。
InterpretedFileName	String	被解釋檔案的名稱。
FilePath	String	檔案所在目錄的路徑。
DllPath	String	DLL 所在目錄的路徑。
DroppedPath	String	修改後的檔案所在目錄的路徑。
BlockedPath	String	被封鎖檔案所在目錄的路徑。
InterpretedFilePath	String	被解釋檔案所在目錄的路徑。
FileFullName	String	檔案的完整路徑。包括目錄路徑和檔案名稱。
DllFullName	String	DLL 的完整路徑。包括目錄路徑和檔案名稱。
DroppedFullName	String	被修改檔案的完整路徑。包括目錄路徑和檔案名稱。
BlockedFullName	String	被封鎖檔案的完整路徑。包括目錄路徑和檔案名稱。
DetectedName	String	被偵測檔案的完整路徑。包括目錄路徑和檔案名稱。
OriginalFileName	String	原始檔案的完整路徑。包括目錄路徑和檔案名稱。
InterpretedFileFullName	String	被解釋檔案的完整路徑。包括目錄路徑和檔案名稱。
FileModificationTime	integer	檔案修改時間。
DllModificationTime	integer	DLL 修改時間。
DroppedModificationTime	integer	被修改時間的修改時間。
InterpretedFileModificationTime	integer	被解釋時間的修改時間。
FileSize	integer	檔案大小。
DllSize	integer	DLL 大小。
DroppedSize	integer	修改後的檔案的大小。
InterpretedFileSize	integer	被解釋檔案的大小。

欄位名稱	類型	敘述
Md5	String	檔案的 MD5 雜湊。
DllMd5	String	DLL 的 MD5 雜湊
DroppedMd5	String	被修改檔案的 MD5 雜湊。
InterpretedMd5	String	被解釋檔案的 MD5 雜湊。
DetectedMd5	String	偵測到的檔案的 MD5 雜湊。
Sha256	String	檔案的 SHA256 雜湊。
DLLSha256	String	DLL 的 SHA256 雜湊。
DroppedSha256	String	被修改檔案的 SHA256 雜湊。
BlockedSha256	String	被封鎖檔案的 SHA256 雜湊。
InterpretedSha256	String	被解釋檔案的 SHA256 雜湊。
DetectedSha256	String	偵測到的檔案的 SHA256 雜湊。
HijackingPath	String	放置在標準搜尋路徑上的目錄中的惡意 DLL，以使作業系統在原始 DLL 之前載入它。
LogonRemoteHost	String	發起遠端存取的主機的 IP 位址。
RealUserName	String	使用者在系統中註冊時被指派的使用者名稱。
EffectiveUserName	String	用於登入系統的使用者名稱。
Environment	String	環境變量。
ProcessType	integer	處理程序類型。可能值： • 1 – exec • 2 – fork • 3 – vfork • 4 – clone
LinuxOperationResult	String	操作結果。可能值： • success • failed
SystemPid	integer	處理程序 ID。
ParentFileFullName	String	父處理程序檔案的路徑。
ParentMd5	String	父處理程序檔案的 MD5 雜湊。
ParentSha256	String	父處理程序檔案的 SHA256 雜湊。
StartupParameters	String	處理程序啟動選項。
ParentSystemPid	integer	父處理程序 ID。
ParentStartupParameters	String	父處理程序啟動設定。
method	String	HTTP 請求方法。
direction	String	連線方向。可能值： • inbound • outbound
LocalIp	String	進行遠端連線嘗試的本機的 IP 位址。
LocalPort	integer	嘗試進行遠端連線的本機電腦的連接埠。
RemoteHostName	String	作為遠端連線嘗試目標的電腦的名稱。
RemoteIp	String	作為遠端連線嘗試目標的電腦的 IP 位址。
RemotePort	integer	作為遠端連線嘗試目標的電腦的連接埠。
URI	String	對其發出 HTTP 請求的資源的位址。
KeyName	String	登錄機碼路徑。
ValueName	String	登錄檔值名稱。

欄位名稱	類型	敘述
ValueData	String	登錄檔值資料。
RegistryOperationType	integer	登錄檔操作的類型。可能值： • 0 – 登錄機碼已建立。 • 1 – 登錄機碼已刪除。 • 2 – 登錄檔已修改。 • 3 – 登錄機碼被重新命名。
PreviousKeyName	String	以前的登錄機碼路徑。
PreviousValueData	String	登錄檔值的先前名稱。
System.EventID.value	String	在 Windows 日誌中的安全性事件類型 ID。
LinuxEventType （此欄位用於取得 Linux 和 macOS 作業系統的事件日誌中所記錄的事件類型）	String	事件類型。可能值： • MemberAddedToGroup — 使用者帳戶已建立。 • UserAccountDeleted — 使用者帳戶已刪除。 • GroupCreated — 群組已建立。 • GroupDeleted — 群組已修改。 • MemberAddedToGroup — 使用者帳戶已新增至群組。 • UserPasswordChanged — 使用者帳戶密碼已變更。 • LinuxAuth — 在 Linux 或 macOS 中執行的身分驗證。 • LinuxSessionStart — Linux 或 macOS 工作階段已啟動。 • LinuxSessionEnd — Linux 或 macOS 工作階段已結束。 • ServiceStart — 服務已啟動。 • ChangeAccountExpirationDate — 帳戶到期日期已變更。 • OperatingSystemShuttingDown — 作業系統已關閉。 • OperatingSystemStarted — 作業係統已啟動。 • ModifyPromiscouslyMode — 混雜模式已修改。 • AuditdConfigurationChanged — 審核設定已修改。
System.Channel.value	String	日誌名稱。
System.EventRecordID.value	String	日誌中的條目 ID。
System.Provider.Name.value	String	記錄事件的系統的 ID。
EventData.Data.TargetDomainName.value	String	遠端電腦的網域名稱。
EventData.Data.ObjectName.value	String	發起事件的物件的名稱。
EventData.Data.PackageName.value	String	啟動事件的封包的名稱。
EventData.Data.ProcessName.value	String	啟動事件的處理程序的名稱。
VerdictName	String	偵測到的物件的名稱。
RecordId	integer	被觸發的規則 ID。
ProcessingMode	String	掃描模式。可能值： • Default — 預設。 • OnDemand — 按需。 • OnAccess — 存取時。 • OnExecute — 執行時。 • OnDownload — 下載時。 • OnStartup — 應用程式啟動時。 • OnMail — 傳送訊息時。 • OnPostpone — 已延遲掃描。 • OnDisinfect — 清除時。 • OnVulnerability — 掃描弱點時。 • OnFirstLaunch — 首次啟動時。 • OnEngineLoad — 系統啟動時。 • OnQuarantineRescan — 重新掃描儲存中的物件時。 • OnWebRequest — 根據網路請求。 • OnAmsiScan — AMSI 掃描時。 • OnSystemWatcherScan — 分析應用程式行為時。
DetectedName	String	物件的名稱。

欄位名稱	類型	敘述
DetectedObjectType	String	物件的類型。可能值： • 未知。 • 檔案。 • LogicalDrive — 邏輯磁碟機。 • PhysicalDisk — 實體磁碟。 • SystemMemory — 系統記憶體。 • MemoryProcess — 處理程序記憶體。 • MemoryModule — 記憶體模組。 • MailMsgRef — 電子郵件訊息的引用標題。 • MailMsgMime — MIME 附件。 • MailMsgBody — 電子郵件主體。 • MailMsgAttach — 電子郵件附件。 • StartUp — 啟動物件。 • Folder — 目錄。 • Script — 指令碼。 • Url — URL 位址。 • AmsiStream — AMSI 掃描流。
ThreatStatus	String	發現模式。可能值： • Untreated — 物件未處理。 • Untreatable — 物件無法被處理。 • NotFound — 物件找不到。 • Disinfected — 物件被清除。 • Deleted — 物件已刪除。 • Quarantined — 物件被移至隔離區。 • AddByUser — 使用者新增的物件。 • Clear — 物件未受感染。 • AddToExclude — 物件被新增到排除項目。 • Terminated — 處理終止。 • Clear — 物件未受感染。 • FalseAlarm — 誤報。 • RolledBack — 回溯到之前的狀態。 • IpNotBlocked — IP 位址未被封鎖。 • IpBlocked — IP 位址被封鎖。 • IpCannotBeBlocked — 無法封鎖 IP 位址。 • IpBlockIsNotRequired — 不需要 IP 位址阻止。
UntreatedReason	String	物件處理狀態。可能值： • None — 沒有資料。 • NonCurable — 物件無法被清除。 • Locked — 物件被鎖定。 • ReportOnly — 應用程式在*僅報告*模式下。 • NoRights — 無執行該操作的權利。 • Canceled — 處理已取消。 • WriteProtect — 物件受寫入防護。 • TaskStopped — 處理工作中斷。 • Postponed — 操作被延遲。 • NonOverwritable — 物件不能被覆寫。 • CopyFailed — 無法建立物件的副本。 • WriteError — 資料寫入錯誤。 • OutOfSpace — 磁碟空間不足。 • ReadError — 資料讀取錯誤。 • DeviceNotReady — 裝置未準備好。 • ObjectNotFound — 未找到物件。 • WriteNotSupported — 不支援資料寫入。 • CannotBackup — 無法建立物件的備份。 • SystemCriticalObject — 物件對於系統至關重要。 • AlreadyProcessed — 物件已處理。
InteractiveInputText	String	解釋器命令。
ObjectContent	String	被傳送以進行掃描的指令碼內容。
ObjectContentType	integer	指令碼的內容類型。可能值： • 1 – 文字 • 2 – 二進位代碼
FileOperationType	integer	檔案操作的類型。可能值： • 1 – 檔案已建立 • 2 – 檔案已修改 • 3 – 檔案已重命名 • 4 – 檔案屬性被修改 • 5 – 檔案已刪除 • 6 – 檔案已讀取

欄位名稱	類型	敘述
PreviousFileName	String	檔案先前所在目錄的路徑。
PreviousFileFullName	String	檔案的完整名稱，包括檔案先前所在目錄的路徑和/或先前的檔案名稱。
DroppedFileType	integer	被修改檔案的類型。可能值： • 0 – 未知 • 1 – 其他檔案 • 2 – PE 映像 • 3 – PE DLL • 4 – PE 資源 • 5 – .NET 資源檔案 • 6 – ELF 檔案

用於管理威脅回應操作的 API

Kaspersky Anti Targeted Attack Platform 提供執行威脅回應操作的 API。執行操作的命令在 Central Node 伺服器處被接收，然後被轉送到 Endpoint Agent 元件。

您可以使用外部系統在具有 Endpoint Agent 元件的主機上執行下列操作：

- 管理主機網路隔離
- 管理防止規則
- 執行應用程式

上述所有操作均可在使用 Kaspersky Endpoint Agent for Windows 作為 Endpoint Agent 元件的主機上使用。

如果 Kaspersky Endpoint Security for Linux 是作為 Endpoint Agent 元件使用，您可以管理網路隔離並執行應用程式。

請求取得具有 Endpoint Agent 元件的主機清單

若要建立具有 Endpoint Agent 元件的主機的資訊請求，請使用 GET HTTP 方法。

命令語法

GET "<Central Node 伺服器的 URL> :<連接埠，預設為 443>/kata/response_api/v1/<external_system_id> /sensors"

如果請求處理成功，則會顯示具有 Endpoint Agent 元件的主機清單。

您可以建立主機資訊的請求，並按主機的 IP 位址、名稱或 ID 進行篩選。您可以指定一個、多個或所有這些篩選器。

指定主機名稱時，請牢記篩選器區分大小寫。

GET "<Central Node 伺服器的 URL>:<連接埠，預設為 443>/kata/response_api/v1/<external_system_id>/sensors?ip=<主機的 IP 位址>&host=<主機名稱>&sensor_id=<sensor_id >"

如果成功處理要求，將顯示有關具有 Endpoint Agent 元件的選定主機的資訊。

設定

參數	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
ip	string	具有 Endpoint Agent 元件的主機的 IP 位址。
host	string	具有 Endpoint Agent 元件的主機的名稱。

輸入帶有參數的命令的範例

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors"
```

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors?ip=10.16.40.243&host=host4&sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0"
```

回覆

HTTP 代碼：200

格式：JSON

```
type Response Sensors

type Server struct {
Version string `json:"version"`
},

type Sensors struct {
SensorID UUID `json:"sensorId"`
HostIP string `json:"hostIp"`
LastAccessTimestamp `json:"lastAccessTimestamp"`
Version string `json:"version"`
SelfDefenseState boolean `json:"selfDefenseState"`
LicenseStatus string `json:"licenseStatus"`
OSFamily string `json:"osFamily"`
OSName string `json:"osName"`
Capabilities array `json:"capabilities"`

}
```

返回值

返回碼	敘述
400	需要授權。
401	參數不正確。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

請求有關網路隔離以及具有 Kaspersky Endpoint Agent 元件的主機是否存在阻止規則的資訊

HTTP 方法 GET 用於建立請求以顯示網路隔離以及具有 Endpoint Agent 元件的主機是否存在阻止規則的資訊。

命令語法

```
GET "<Central Node 伺服器的 URL> :<連接埠，預設為
443>/kata/response_api/v1/<external_system_id> /settings?sensor_id=<sensor_id>
&settings_type=<network_isolation 或預防> "
```

如果請求成功處理，則會顯示具有 Endpoint Agent 元件的主機清單，其中列出了在處理請求時應用了阻止規則或網路隔離規則的主機。

設定

參數	類型	敘述
`external_system_id`	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
`sensor_id`	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
`settings_type`	enum	規則類型：network_isolation 或預防。

輸入具有開關的命令的範例

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

Response

HTTP 代碼：200

格式：JSON

```
type Response []Settings

type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec int `json:"autoTurnoffTimeoutInSec"`
}
```

返回值

返回碼	敘述
400	需要授權。
401	參數不正確。
404	未找到具有 Endpoint Agent 元件的指定主機。
500, 502, 503, 504	內部錯誤。稍後重複該請求。

主機網路隔離管理

若要使用 API 隔離具有 Endpoint Agent 元件的主機，建議依照下列步驟與 Kaspersky Anti Targeted Attack Platform 進行互動：

1. **建立取得具有 Endpoint Agent 元件的主機清單的請求**
2. **建立請求以獲取有關已啟用網路隔離的主機的資訊**
3. **建立下列之一對具有 Endpoint Agent 元件的主機的操作要求：**
   - 啟用網路隔離
   - 停用網路隔離
   - 將排除項目新增至現有網路隔離規則

您可以在應用程式的 Web 介面中管理建立的網路隔離規則。

請求啟用網路隔離

若要為選定的主機啟用網路隔離，您必須新增網路隔離規則。若要建立請求，請使用 HTTP POST 方法。

命令設定以 JSON 格式在請求主體中傳遞。

命令語法

```
curl -k --cert <TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X POST "<Central Node 伺服器的 URL>:
<連接埠，預設為443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=network_isolation" -H 'Content-Type: application/json' -d '

{

"settings": {

"autoTurnoffTimeoutInSec": <網路隔離時段>}

}

'
```

如果請求成功處理，則新增網路隔離規則。新增規則後，所選主機的網路隔離將變為活動狀態。

在建立請求時指定的一段時間後，網路隔離將變為非活動狀態。網路隔離規則本身不會被刪除。如有必要，您可以刪除選定的規則。

若要停用網路隔離，您必須建立請求以停用所選規則。

設定

參數	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
autoTurnoffTimeoutInSec	integer	網路隔離處於活動狀態的時間段。 允許範圍-1 到 9999 小時。網路隔離時間以秒為單位指定。例如，如果要啟用主機網路隔離兩個小時，則必須指定 7200 秒。

輸入具有開關的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": 7200}
}
'
```

Response

HTTP 代碼：200

格式：JSON

```
type Response []Settings

type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec integer `json:"autoTurnoffTimeoutInSec"`
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。
404	未找到具有 Endpoint Agent 元件的指定主機。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

如果要編輯已建立的網路隔離規則的設定，您必須建立新請求以新增具有新設定的規則。

請求停用網路隔離

若要停用選定主機的網路隔離，您必須建立停用網路隔離規則的請求。HTTP 方法 DELETE 用於建立請求。

命令語法

```
curl -k --cert <TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X DELETE "<Central Node 伺服器的URL>:<連接埠，預設為 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id>&settings_type=network_isolation"
```

如果請求處理成功，則網路隔離規則已停用。

設定

參數	類型	敘述
`external_system_id`	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
`sensor_id`	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。

輸入帶有 DELETE 參數的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

若要驗證網路隔離是否已停用，請使用 HTTP GET 方法要求工作資訊。

輸入帶有 GET 參數的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"| python -m json.tool
```

如果網路隔離已停用，Kaspersky Anti Targeted Attack Platform 將以下列格式向外部系統傳回回應：

```
{
"error"："未找到"
}
```

返回值

返回碼	敘述
`400`	參數不正確。
`401`	需要授權。
`404`	未找到具有 Endpoint Agent 元件的指定主機。
`500, 502, 503, 504`	未知伺服器錯誤。稍後重複該請求。

請求將排除項目新增至網路隔離規則

若要將排除項目新增至先前建立的網路隔離規則中，您必須建立新增排除項目的請求。若要建立請求，請使用 HTTP POST 方法。

命令設定以 JSON 格式在請求主體中傳遞。

命令語法

```
curl -k --cert<TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X POST "<Central Node 伺服器的 URL> :
<連接埠，預設為443>/kata/response_api/v1/<external_system_id > /settings?sensor_id=
<sensor_id> &settings_type=network_isolation" -H 'Content-Type：application/json' -d '

{
"settings":
{"excludedRules": [
{
"direction": "<outbound、inbound 或 both>",
"protocol": <IP 協定的編號>,
"remoteIpv4Address": "<具有 Endpoint Agent 元件且其流量不得被封鎖的主機的 IP 位址>",
"localPortRange":
{
"fromPort": <連接埠號碼>,
"toPort": <連接埠號碼>
}
}
,
{
"direction": "<outbound、inbound 或 both>",
"protocol": <IP 協定的編號>,
"remoteIpv4Address": "<具有 Endpoint Agent 元件且其流量不得被封鎖的主機的 IP 位址>",
"remotePortRange":
{
"fromPort": <連接埠號碼>,
"toPort": <連接埠號碼>
}
}
,
{
"direction": "<outbound、inbound 或 both>",
"protocol": <IP 協定的編號>,
"remoteIpv4Address": "<具有 Endpoint Agent 元件且其流量不得被封鎖的主機的 IP 位址>"
}
]
,
"autoTurnoffTimeoutInSec": <網路隔離持續時間>
}
}
'
```

如果請求處理成功，則會新增網路隔離規則的排除項目。

設定

參數	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。

sensor_id	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
direction	array	不得被封鎖的網路流量方向。可能值： • inbound • outbound • both 如果您沒有為此參數指定值，則預設值為“both”，這表示應用程式在兩個方向上傳輸流量。
protocol	integer	由網際網路號碼分配機構 (IANA) 指派的 IP 協定號。 如果不指定此參數的值，則預設情況下，網路隔離將套用於所有協定。
remoteIpv4Address	string	具有 Endpoint Agent 元件的主機的 IP 位址，其流量不得被阻止
remotePortRange	string	目的連接埠。 只有當您選擇了網路流量的傳出方向時，才可以指定目標連接埠。無法為雙向流量指定連接埠範圍。
localPortRange	string	從其發起連線的連接埠。 只有當您選擇了網路流量的傳入方向時，才可以指定目標連接埠。無法為雙向流量指定連接埠範圍。
autoTurnoffTimeoutInSec	integer	網路隔離處於活動狀態的時間段。 允許範圍-1 到 9999 小時。網路隔離時間以秒為單位指定。例如，如果要啟用主機網路隔離兩個小時，則必須指定 7200 秒。

輸入具有開關的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings":
{"excludedRules": [
{
"direction": "inbound",
"protocol": 6,
"remoteIpv4Address": "10.16.41.0",
"localPortRange":
{
"fromPort": 3389,
"toPort": 3389
}
}
,
{
"direction": "outbound",
"remoteIpv4Address": "10.16.41.1",
"remotePortRange":
{
"fromPort": 13957,
"toPort": 55409
}
}
,
{
"direction": "both",
"protocol": 6,
"remoteIpv4Address": "10.16.41.2"
}
]
,
"autoTurnoffTimeoutInSec": 7200
}
}
'
```

回覆

HTTP 代碼：200

格式：JSON

```
type Response []Settings
type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec integer `json:"autoTurnoffTimeoutInSec"`
}
type ExcludedRules struct {
Direction array `json:"direction"`
Protocol integer `json:"autoTurnoffTimeoutInSec"`
RemotePortRange string `json:"remotePortRange"`
LocalPortRange string `json:"localPortRange"`
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。
404	未找到具有 Endpoint Agent 元件的指定主機。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

如果要編輯已建立的排除項目的設定，您必須建立一個新請求以新增具有新設定的排除項目。

管理防止規則

您可以使用阻止規則來阻止檔案或處理程序在具有 Endpoint Agent 元件的選定主機或所有主機上執行。例如，您可以阻止某些您認為不安全的應用程式。該應用程式透過使用 MD5 和 SHA256 雜湊演算法基於檔案雜湊識別檔案。透過外部系統建立的阻止規則可以包含多個檔案雜湊。

您可以使用外部系統來管理為單個主機或同時為所有主機建立的所有阻止規則。當您透過外部系統為選定主機建立阻止規則時，Kaspersky Anti Targeted Attack Platform 會將套用於該主機的所有阻止規則替代為具有新參數的阻止規則。例如，如果您透過應用程式的 Web 介面為選定主機新增了多個阻止規則，隨後透過外部系統新增了一條阻止規則，則在 Web 介面中新增的所有阻止規則都會替代為透過外部系統新增的規則。

當透過外部系統建立的阻止規則的參數被修改時，應用程式僅儲存新參數。例如，如果您新增了一條包含多個檔案的雜湊值的阻止規則，並且想要向該規則新增另一個雜湊值，則必須建立一個請求來新增阻止規則並指定您先前有防禦的所有雜湊值，加上新的雜湊值。

所描述的場景也與套用於所有主機的阻止規則相關。

若要使用 API 建立阻止規則，建議依照下列步驟與 Kaspersky Anti Targeted Attack Platform 互動：

1. **建立取得具有 Endpoint Agent 元件的主機清單的請求**
2. **建立請求以取得已具有阻止規則的主機的資訊。**
3. **建立請求執行下列阻止規則操作之一：**
   - 建立規則
   - 刪除規則

新增的阻止規則顯示在應用程式的 Web 介面中的**阻止**部分，**阻止規則**子部分。

如果要透過外部系統為所有主機建立阻止規則，您必須先確保伺服器上不存在相同檔案的阻止規則，或者規則沒有套用於一台或多台主機。如果您想要透過外部系統為選定的主機建立阻止規則，則此先決條件也很重要：您必須確保伺服器上不存在相同檔案的阻止規則，並且沒有套用於所有主機。否則，伺服器將向外部系統傳回錯誤，其中包含已套用阻止規則的主機清單。

如果透過外部系統建立的阻止規則包含多個檔案雜湊，則錯誤資訊僅提及導致錯誤的第一個檔案。其他防重複規則的資訊不顯示。

> 若要修改先前透過 Web 介面或外部系統建立的阻止規則，您必須建立請求以新增具有更新參數的阻止規則。

請求建立阻止規則

若要建立請求，請使用 HTTP POST 方法。命令設定以 JSON 格式在請求主體中傳遞。

命令語法

```
curl -k --cert<TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X POST "<Central Node 伺服器的 URL>:<連接埠，預設為 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id 或全部，如果要为所有主機建立阻止規則>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": [

{

"file": {

"<sha256 or md5> ": "<要阻止啟動的檔案的 SHA256 或 MD5 雜湊>"

}

},

{

"file": {

"<sha256 or md5> ": "<要阻止啟動的檔案的 SHA256 或 MD5 雜湊>"

}

}

]

}

}
```

'

如果請求處理成功，則阻止規則被新增。阻止規則在新增後立即生效。

如有必要，您可以刪除阻止規則。

設定

參數	類型	敘述
`external_system_id`	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
`sensor_id`	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
`objects`	string	您想要阻止運行的物件的類型。 參數的可能值：file。
`sha256 or md5`	string	SHA256 或 MD5 具有您想要阻止運行的物件。

輸入具有開關的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{
"settings": {
"objects": [
{
"file": {
"sha256": "830195824b742ee59390bc5b9302688c778fc95a64e7d597e28a74c03a04dd63"
}
},
{
"file": {
"md5": "d8e577bf078c45954f4531885478d5a9"
}
}
]
}
}
'
```

Response

HTTP 代碼：200

格式：JSON

```
type Response []Objects

type Objects struct {
type file struct {
SHA256 string `json:"sha256"`
},
type file struct {
MD5 string `json:"md5"`
}
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。
404	未找到具有 Endpoint Agent 元件的指定主機。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

請求刪除阻止規則

您可以使用具有空白值的新請求或具有 DELETE 參數的請求來刪除阻止規則。POST 和 DELETE HTTP 方法用於建立請求。

新請求的命令語法

命令設定以 JSON 格式在請求主體中傳遞。

```
curl -k --cert <TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X POST "<Central Node 伺服器的 URL>:<連接埠，預設為 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id 或全部，如果要刪除所有主機的阻止規則>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": []
```

```
}

}

'
```

帶有 DELETE 參數的命令語法

```
curl -k --cert <TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X DELETE "<Central Node 伺服器的URL>:<連接埠，預設為 443>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id 或全部，如果要刪除所有主機的阻止規則>&settings_type=prevention"
```

設定

參數	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。

新請求的命令範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{

"settings": {

"objects": []

}

}

'
```

輸入帶有DELETE 參數的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"
```

如果請求成功處理，則阻止規則被刪除。

若要驗證阻止規則是否已被刪除，請使用 HTTP GET 方法要求有關阻止規則的資訊。

輸入帶有 GET 參數的命令的範例

```
curl -k --cert <TLS 憑證檔案路徑> --key <私密金鑰檔案路徑> -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"| python -m json.tool
```

如果阻止規則被刪除，Kaspersky Anti Targeted Attack Platform 將以以下格式向外部系統傳回回應：

```
{
"error"："未找到"
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。
404	未找到具有 Endpoint Agent 元件的指定主機。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

管理應用程式運行工作

若要使用 API 管理應用程式執行工作，建議依照下列步驟與 Kaspersky Anti Targeted Attack Platform 互動：

1. **建立有關工作設定、建立時間和完成狀態資訊的請求**
2. **建立請求執行下列工作操作之一：**
   - 建立工作
   - 刪除工作

新增的工作顯示在應用程式的 Web 介面中的**工作**部分。

請求獲取有關工作的資訊

若要建立獲取有關工作的資訊的請求，請使用 HTTP GET 方法。

命令語法

```
GET "<Central Node 伺服器的 URL>:<連接埠，預設為
443>/kata/response_api/v1/<external_system_id>/tasks/<task_id>?settings=<true 或 false>"
```

如果請求處理成功，則會顯示有關工作的設定、建立時間和完成狀態的資訊。

設定

設定	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
task_id	UUID	工作的唯一 ID。
settings	boolean	可能值： • true。 如果輸入此值，將顯示有關工作的設定、建立時間和完成狀態的資訊。 • false。 如果輸入此值，將顯示有關工作的建立時間和完成狀態的資訊。

輸入具有開關的命令的範例

```
GET https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=<true 或 false>
```

回覆

HTTP 代碼：200

格式：JSON

```
type Response struct {
State `json:"state"`
LatestStartDateTime `json:"latestStartDateTime"`
type Task struct {
type Schedule struct {
StartNow boolean `json:"startNow"`
ExecCommand string `json:"execCommand"`
}
}
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。

返回碼	敘述
409	指定 ID 的工作已經存在。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

請求建立工作

HTTP POST 方法用於要求執行 Kaspersky Anti Targeted Attack Platform 應用程式。命令設定以 JSON 格式在請求主體中傳遞。

命令語法

```
curl -k --<TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X POST "<Central Node 伺服器的 URL>:<連接埠，預設 443>/kata/response_api/v1/<external_system_id>/tasks/<task_id>?sensor_id=<sensor_id>&task_type=run_process" -H 'Content-Type：application/json' -d '

{

"task": {

"shedule": {"startNow":<true 或 false> },

"execCommand": "<要執行的應用程式的名稱>",

"cmdLineParameters": "<執行檔案或命令的其他選項>",

"workingDirectory": "<工作目錄>"

}

}

'
```

如果成功處理請求，則會建立執行應用程式工作。

設定

參數	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
sensor_id	UUID	具有 Endpoint Agent 元件的主機的唯一 ID。
task_id	UUID	工作的唯一 ID。

輸入具有開關的命令的範例

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&task_type=run_process" -H 'Content-Type: application/json' -d '
{

"task": {

"schedule": {"startNow": true},

"execCommand": "Example.exe",

"cmdLineParameters": "C:\Windows\System32\",

"workingDirectory": "/all"

}

}

'
```

Response

HTTP 代碼：200

格式：JSON

```
type Response struct {
State `json:"state"`
LatestStartDateTime `json:"latestStartDateTime"`
type Task struct {
type Schedule struct {
StartNow boolean `json:"startNow"`
ExecCommand string `json:"execCommand"`
}
}
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。

返回碼	敘述
404	未找到具有指定 ID 的工作。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

如果要編輯已建立工作的設定，則必須建立新請求以新增具有新設定的工作。

請求刪除工作

若要建立刪除 Kaspersky Anti Targeted Attack Platform 工作的請求，請使用 HTTP DELETE 方法。

命令語法

curl -k --<TLS 憑證檔案路徑> --key <私鑰檔案路徑> -X DELETE "<Central Node 伺服器的 URL>:<連接埠，預設為443>/kata/response_api/v1/<external_system_id>/tasks/<task_id>"

如果成功處理請求，則會刪除應用程式執行工作。

設定

參數	類型	敘述
external_system_id	UUID	用於 Kaspersky Anti Targeted Attack Platform 授權的外部系統的唯一 ID。
task_id	UUID	工作的唯一 ID。

輸入帶有DELETE 參數的命令的範例

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8"
```

如果請求成功處理，則阻止規則被刪除。

若要驗證工作是否已刪除，請使用 HTTP GET 方法要求有關工作的資訊。

輸入帶有 GET 參數的命令的範例

```
curl -k --example.cert --example.key -X GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=false"| python -m json.tool
```

如果工作被刪除，Kaspersky Anti Targeted Attack Platform 將以以下格式向外部系統返回回應：

```
{
"error"："未找到"
}
```

返回值

返回碼	敘述
400	參數不正確。
401	需要授權。
404	未找到具有指定 ID 的工作。
500, 502, 503, 504	未知伺服器錯誤。稍後重複該請求。

使用 NDR API

REST API 伺服器為外部系統提供對 NDR 功能的存取，它在 Central Node 伺服器上運行並使用 REST (Representational State Transfer) 架構風格處理請求。使用 HTTPS 向 REST API 伺服器發出請求。您可以在**設定 → 連線伺服器**下設定 REST API 伺服器（包括以受信任憑證取代預設的自簽章憑證）。

JSON 格式用於表示請求和回應中的資料。

包含基於 REST 架構風格的請求描述的文件作為"線上說明指南"發佈在"卡巴斯基線上說明"頁面上。本文件是英文版的開發者指南。開發人員指南還提供了被傳送到 REST API 伺服器的請求中可用的可呼叫元素的範例程式碼和詳細描述。

開啟描述對 REST API 伺服器的請求的文件，版本 4

外部系統可以使用 Kaspersky Anti Targeted Attack Platform API 來：

- 接收有關應用程式已知裝置的資訊。
- 新增、修改和刪除裝置。
- 接收已註冊的網路流量事件（NDR 事件）的資訊。
- 將 NDR 事件傳送至 Kaspersky Anti Targeted Attack Platform（代碼為 4000005400 的系統事件類型用於註冊事件）。
- 接收有關偵測到的弱點的資訊。
- 接收應用程式訊息和稽核記錄。
- 接收有關允許規則的資訊。
- 啟用、停用和刪除允許規則。
- 接收與裝置相關的風險資訊。
- 接收有關位址空間的資訊。
- 將網路拓撲圖報告傳送至 Kaspersky Anti Targeted Attack Platform。
- 傳送、接收和刪除有關裝置上使用者的資訊。
- 傳送和接收有關裝置上的應用程式和修補程式的資訊。
- 傳送和刪除有關裝置上的可執行檔的資訊。
- 傳送裝置日誌的內容。
- 接收以下應用程式資料：
  - 包含應用程式元件的伺服器清單
  - 監控點及其參數清單

- 支援的協定堆棧及其參數清單
- NDR 事件類型及其參數清單
- 技術現況及運作模式
- 應用程式版本和已安裝更新的發布日期
- 有關新增的產品授權金鑰的資訊
- 應用程式本地化語言

使用 Kaspersky Anti Targeted Attack Platform API 的外部系統透過連線器連線到 Central Node 元件。連線器使用憑證來建立安全連線。對於您想要向 REST API 伺服器傳送請求的每個外部系統，您需要在 Kaspersky Anti Targeted Attack Platform 中建立一個單獨的連線器。

外部系統必須使用驗證權杖才能連線到 Kaspersky Anti Targeted Attack Platform。Kaspersky Anti Targeted Attack Platform 會根據外部系統的請求頒發驗證權杖，權杖使用為該系統建立的連線器的憑證。身分驗證權杖的有效期限為 10 小時。外部系統可以透過特殊請求更新身分驗證權杖。

包含身分驗證權杖操作查詢描述的文件作為線上說明指南發佈在“卡巴斯基線上說明”頁面上。本文件是英文版的開發者指南。

開啟描述身分驗證權杖操作查詢的文件，版本 4

Kaspersky Anti Targeted Attack Platform API 允許透過以下方式與外部系統進行互動：

- 基於 REST 架構風格的互動
- 透過 WebSocket 協定進行互動

外部系統可以使用 WebSocket 協定在 Kaspersky Anti Targeted Attack Platform API 中進行互動，以建立對應用程式收到的修改值的訂購。

確保使用 Kaspersky Anti Targeted Attack Platform API 時的安全性

外部系統透過建立加密的 HTTPS 連線，使用 Kaspersky Anti Targeted Attack Platform API 存取應用程式的功能。Kaspersky Anti Targeted Attack Platform 的 Central Node 元件所頒發的憑證用於保護連線的安全。此元件為外部系統用於連線伺服器的連線器頒發憑證。

必須在 Kaspersky Anti Targeted Attack Platform 中為每個外部系統建立單獨的連線器。只有使用由 Central Node 元件頒發並保存在該連線器的通訊封包中的特定憑證才能透過連線器建立連線。如果外部系統提供來自不同連線器、Kaspersky Anti Targeted Attack Platform 的不同 Central Node 元件或用於其他連線的憑證（例如，Sensor 元件的憑證），則無法建立連線。

建立加密連線後，外部系統必須為連線器請求一個*身分驗證權杖*，外部系統將在傳送至 Central Node REST API 伺服器的請求中使用該權杖。

身分驗證權杖在簽發後 10 小時內有效。如果權杖需要使用更長時間，則外部系統必須在權杖過期之前請求延長時間。

有關 Kaspersky Anti Targeted Attack Platform API 支援的請求和方法的資訊，請參閱 Kaspersky Anti Targeted Attack Platform API 的文件。

在處理來自外部系統的請求時，Kaspersky Anti Targeted Attack Platform 使用稽核日誌記錄有關嘗試執行以下操作的資訊：

- 接收身分驗證權杖。
- 延伸身分驗證權杖的有效期限。
- 將裝置新增至裝置表中。
- 編輯裝置資訊。
- 刪除裝置。
- 查詢稽核日誌（載入Web 伺服器後第一次透過連線器讀取稽核條目時）。

建立並使用 Kaspersky Anti Targeted Attack Platform API 的連線器

為了實現外部系統與 Kaspersky Anti Targeted Attack Platform API 之間的互動，您需要為該系統新增一個連線器。建立連線器時，您必須指明連線器的**一般**系統類型。

當新增連線器並為此連線器建立新的通訊封包時，Central Node 會產生一個通訊封包，您需要使用該封包使連線器運作。

通訊封包是一個包含以下檔案的壓縮檔案：

- certificates.pfx 檔案包含 Central Node 憑證的加密公鑰和 Central Node 為連線器所頒發的憑證（有私鑰）。檔案內容使用新增連線器時或為此連線器建立新的通訊封包時所設定的密碼加密。
- metadata.json 檔案包含連線器的配置資料。資料以 JSON 格式呈現。

必須使用列出的檔案透過連線器連線外部系統。要解密 certificates.pfx 檔案並套用其包含的憑證和金鑰，您可以使用處理此格式的檔案的標準方法（例如，`openss1` 命令）。連線器工作以及向 REST API 伺服器傳送請求需要 metadata.json 檔案中指定的位址。

通訊封包中的憑證和設定資料一直有效，直到建立新的通訊封包或從應用程式移除連線器為止。

有關應用程式的資訊來源

本節列出了有關程式的資訊來源。

您可依據問題的緊急性或重要性等級，來選取最適宜的來源。

卡巴斯基網站上的 Kaspersky Anti Targeted Attack Platform 網頁

在 Kaspersky Anti Targeted Attack Platform 頁面 上，您可以找到有關該應用程式、其功能和特點的一般資訊。

Kaspersky Anti Targeted Attack Platform 網頁中包含線上商店的連結。在線上商店中，您可以購買應用程式或續約產品授權。

知識庫中的 Kaspersky Anti Targeted Attack Platform 網頁

*知識庫*是技術支援網站的一部分。

在知識庫中的 Kaspersky Anti Targeted Attack Platform 頁面 上，您可以閱讀文章，這些文章提供有關購買，安裝和使用該程式的常見問題的有用資訊，建議和解答。

知識庫文章不僅可以回答與 Kaspersky Anti Targeted Attack Platform 相關的問題，還可以回答與卡巴斯基其他應用程式相關的問題。知識庫文章也可能包含技術支援的新聞。

在論壇上討論卡巴斯基軟體

如果您的問題不需要立即回答，您可以在我們的論壇 上與卡巴斯基專家和其他使用者一起討論。

在論壇上，您可以檢視現有主旨、發表評論以及建立新的討論主旨。

聯絡技術支援服務

本節介紹獲取技術支援的途徑和提供技術支援的條件。

如何獲得技術支援

如果您無法在程式檔案或其中一個 Kaspersky Anti Targeted Attack Platform 資訊來源中找到問題的解決方案，建議您聯絡技術支援。技術支援人員將解答您有關安裝和使用 Kaspersky Anti Targeted Attack Platform 的問題。

卡巴斯基在 Kaspersky Anti Targeted Attack Platform 的整個生命週期內提供支援（請參閱產品生命週期頁面）。與技術支援聯繫之前，請閱讀技術支援規則。

您可以透過以下方式之一聯絡技術支援：

- 造訪技術支援網站
- 透過 Kaspersky CompanyAccount 入口網站向技術支援傳送請求。

透過 Kaspersky CompanyAccount 獲得技術支援

Kaspersky CompanyAccount 是一個為使用卡巴斯基軟體的公司提供的入口網站。Kaspersky CompanyAccount 入口網站是為了透過網路請求方便使用者和卡巴斯基專家之間的互動。Kaspersky CompanyAccount 入口網站允許監控卡巴斯基員工在線上請求處理的進度並保留電子請求的歷史記錄。

您可以讓您的組織機構中所有的員工在 Kaspersky CompanyAccount 註冊一個帳戶。單個帳戶可讓您集中管理註冊員工傳送給卡巴斯基的電子要求，也可以透過 Kaspersky CompanyAccount 管理這些員工的權限。

Kaspersky CompanyAccount 入口網站支援以下語言：

- 英語
- 西班牙語
- 義大利語
- 德文
- 波蘭語
- 葡萄牙語
- 俄語
- 法語
- 日語

有關 Kaspersky CompanyAccount 操作的更多資訊，請造訪技術支援網站。

術語表

Central Node

應用程式元件。掃描資料、分析物件的行為，並將分析結果發佈到應用程式的 Web 介面上。

CSRF 攻擊

跨站請求偽造（也稱為“XSRF 攻擊”）。利用 HTTP 協定的弱點攻擊網站使用者。這種攻擊使得駭客能夠打著授權使用者的幌子在易受攻擊的網站中執行操作。例如，在易受攻擊的網站中，駭客可以打著授權使用者的幌子秘密地向外部支付系統的伺服器傳送請求，以便將資金轉移到駭客的帳戶。

Endpoint Agent 元件

應用程式元件。安裝在執行Microsoft Windows、Linux 和 MacOS 作業系統的企業 IT 基礎架構的工作站和伺服器上。持續監控在這些電腦上執行的處理程序、活動的網路連線和被修改的檔案。

ICAP 用戶端

Kaspersky Anti Targeted Attack Platform 透過其接收流量的系統。

ICAP 資料

由 ICAP 協定（網際網路內容適配協定）接收的資料。該協定允許篩選和修改 HTTP 請求和 HTTP 回應的資料。例如，它允許掃描資料中的病毒、封鎖垃圾郵件以及拒絕存取個人資源。ICAP 用戶端通常是透過 ICAP 協定與 ICAP 伺服器互動的代理伺服器。在 ICAP 伺服器上處理完此資料後，Kaspersky Anti Targeted Attack Platform 會從組織的代理伺服器接收資料。

IOA

攻擊指標。對公司 IT 基礎架構內物件可疑行為的描述，可能表示該組織受到有針對性的攻擊。

IOC

入侵指標。有關惡意物件或惡意活動的一組資料。

IOC 檔案

IOC 檔案包含一組與事件指標進行比較的指標。如果比較的指標匹配，應用程式將該事件視為偵測並建立警示。如果掃描偵測到物件資料與多個 IOC 檔案之間的精確匹配，則警示的可能性會增加。

Kaspersky Anti Targeted Attack Platform

防護企業 IT 基礎架構和及時偵測諸如*零時差攻擊*、*針對性攻擊*，以及被稱為*進階持續性威脅*（以下也稱為 "*APT*"）的複雜針對性攻擊等威脅的解決方案。

Kaspersky Secure Mail Gateway

用於防護傳入和傳出的電子郵件免受惡意物件和垃圾郵件的影響，以及用於郵件內容篩選的一種解決方案。此解決方案可讓您部署虛擬郵件閘道並將其整合到現有的企業郵件基礎架構中。虛擬郵件閘道上預先安裝了作業系統、郵件伺服器和卡巴斯基病毒防護應用程式。

Kaspersky Threat Intelligence Portal

卡巴斯基資訊系統 包含並顯示檔案和 URL 位址的信譽資訊。

KATA

Kaspersky Anti Targeted Attack。Kaspersky Anti Targeted Attack Platform 的功能區塊，用於偵測企業 IT 基礎架構週邊的威脅。

KEDR

Kaspersky Endpoint Detection and Response。Kaspersky Anti Targeted Attack Platform 的功能區塊，為組織的區域網路提供防護。

Kerberos 身分驗證

在用戶端和伺服器之間建立連線之前進行相互驗證的機制，允許透過不受防護的網路進行通訊。此機制是基於使用受信任的身分驗證中心向使用者頒發的票證。

Keytab 檔案

一個包含被允許使用 Kerberos 驗證的用戶端對的唯一名稱（主體）和從使用者密碼派生的加密金鑰的檔案。支援 Kerberos 的系統使用 keytab 檔案來驗證使用者身分，而無需輸入密碼。

KPSN 的本機信譽資料庫

儲存在卡巴斯基私人安全網路伺服器上但不儲存在卡巴斯基安全網路伺服器上的物件（檔案或 URL）的信譽資料庫。本機信譽資料庫由 KPSN 管理員管理。

MIB（管理資訊庫）

用於管理透過 SNMP 協定傳輸的物件的虛擬資料庫。

MITRE 技術

MITRE ATT&CK（對抗政策、技術和常識）資料庫包含基於真實攻擊分析的駭客行為描述。它是以表格形式表示的已知駭客技術的結構化清單。

NTP 伺服器

使用網路時間協定的精確時間伺服器。

OpenIOC

一種基於 XML 的開放性標準，用於描述包含超過500 種不同入侵指標的入侵指標。

Sandbox

應用程式元件。啟動作業系統的虛擬映像。在這些作業系統中啟動檔案並追蹤每個作業系統中檔案的行為，以偵測惡意活動以及針對企業 IT 基礎架構的針對性攻擊的跡象。

Sensor

應用程式元件。接收資料。

SIEM 系統

安全資訊和事件管理系統。用於管理組織安全系統中的資訊和事件的解決方案。

SPAN

交換埠分析器。用於將流量從一個連接埠映像到另一個連接埠的技術。

Syslog

傳送和記錄 UNIX™ 和 GNU/Linux 平台上使用的系統中發生的事件相關訊息的標準。

TAA (IOA) 規則

企業 IT 基礎架構中物件的可疑行為的一種跡象，會導致 Kaspersky Anti Targeted Attack Platform 將事件視為偵測並建立警示。TAA (IOA) 規則包含攻擊跡象的描述和建議的對策。

TLS 加密

兩台伺服器之間連線的加密，可確保網際網路伺服器之間資料的安全傳輸。

VIP 身分

具有特殊存取權限的偵測的狀態。例如，具有**安全官**角色的使用者無法檢視 VIP 身分的警示。

YARA

應用程式模組。使用由 Kaspersky Anti Targeted Attack Platform 使用者建立的 YARA 規則資料庫掃描檔案和物件，以發現對企業 IT 基礎架構的針對性攻擊的跡象。

YARA 規則

一種公開可用的惡意軟體分類，其中包含對企業 IT 基礎架構的針對性攻擊和入侵的跡象的簽章，由 Kaspersky Anti Targeted Attack Platform 用於掃描檔案和物件。

中間人攻擊

中間人。對組織的 IT 基礎結構的攻擊，其中駭客劫持兩個接入點之間的通訊鏈路，將其進行傳輸，並在必要時修改這些接入點之間的連線。

偵測

應用程式的單個模組或元件掃描物件的結果。

備用資料流

NTFS 檔案系統的資料流（備用資料流）用於檔案的其他屬性或資訊。

NTFS 檔案系統中的每個檔案都包含一組流。主流包含檔案內容。其他（備用）流用於中繼資料。可以建立、刪除、單獨儲存、重新命名流，甚至可以作為一個處理程序運行。

駭客可以使用替代流來隱藏傳輸或從電腦接收資料。

傾印

在指定時刻處理程序的工作記憶體或系統整個RAM 的內容。

入侵偵測系統

應用程式模組。掃描 Internet 流量是否有入侵企業 IT 基礎架構的跡象。

最終使用者產品授權協議

您與 AO卡巴斯基之間達成的有約束力的協議，其中明確了使用者使用該應用程式的條款。

分佈式解決方案

安裝有 Central Node 元件的伺服器的兩層架構。此架構分配主控制伺服器*（主 Central Node (PCN)）*和從屬伺服器*（從屬 Central Node (SCN)）*。

卡巴斯基安全網路（KSN）

雲端服務基礎架構，可供存取卡巴斯基線上知識庫，其中包含持續更新的檔案、網路資源和軟體信譽資訊。使用來自卡巴斯基安全網路的資料可確保卡巴斯基應用程式能夠更快地回應威脅，提高某些防護元件的效能，並降低誤報的可能性。

卡巴斯基私有安全網路

允許卡巴斯基病毒防護應用程式使用者存取卡巴斯基安全網路資料庫、而無需不從他們的電腦傳送資料到卡巴斯基安全網路伺服器的解決方案。

多租戶

Kaspersky Anti Targeted Attack Platform 被用來同時防護多個組織或同一組織分支機構的基礎架構的運作模式。

後門程式

駭客在受感染電腦上植入的程序，目的是將來能夠存取該電腦。

惡意 Web 位址

分發惡意軟體的資源的 URL。

惡意軟體防護引擎

應用程式核心。使用防毒資料庫掃描檔案和物件以尋找企業 IT 基礎架構中的病毒和其他威脅。

新一代威脅

企業 IT 基礎架構威脅，能夠覆寫、修改、加密或扭曲其代碼，以至於安全系統無法再偵測到與簽章相符的位置。

映像流量

從一個交換機連接埠重新導向到同一交換機（本機映像）或遠端交換機（遠端映像）的另一個連接埠的流量副本。網路管理員可以配置應該映像哪部分流量以傳輸到 Kaspersky Anti Targeted Attack Platform。

Kaspersky Anti Targeted Attack Platform 支援從聚合裝置接收映像流量：網路封包代理程式或網路輕觸。如果要對來自聚合裝置的流量套用篩選，則必須調整 Kaspersky Anti Targeted Attack Platform 的硬體需求。為了確定解決方案的實際硬體需求，我們建議先進行試點部署。

服務主要名稱（SPN）

網路上用於 Kerberos 驗證的服務的唯一 ID。

租戶

為其提供 Kaspersky Anti Targeted Attack Platform 解決方案的單個組織或組織的分支機構。

簽章

包含已知威脅描述的資訊防護資料庫中的代碼。

網路釣魚 URL 位址

資源的 URL 位址，旨在取得對使用者機密資料的未授權存取。網路釣魚的目的通常是竊取各種財務資料。

警示

使用 Kaspersky Anti Targeted Attack Platform 模組和技術掃描物件後進行的一次或一組偵測的記錄。顯示在警示表中。

追蹤

應用程式以調試模式運行；執行每個命令後，應用程式停止並顯示該步驟的結果。

通訊頻道頻寬

特定通訊頻道中資訊傳輸的最高速度。

進階持續性威脅（APT）

針對企業 IT 基礎架構的進階針對性攻擊，可同時使用不同的方法滲透網路，隱藏於網路並獲得對機密資料的無障礙存取。

針對性攻擊

針對特定個人或組織的攻擊。與旨在感染盡可能多台電腦的電腦病毒的大規模攻擊不同，針對性攻擊的目的是感染特定組織的網路，甚至是企業 IT 基礎架構內的單獨伺服器。可以編寫專門的木馬程式來分階段進行針對性攻擊。

針對性攻擊分析器

應用程式模組。使用 TAA (IOA) 規則分析並監控公司 LAN 電腦上安裝的軟體的網路活動。搜尋 Kaspersky Anti Targeted Attack Platform 的使用者應注意的網路活動的跡象，以及對企業 IT 基礎架構的針對性攻擊的跡象。

零時差弱點

駭客在軟體供應商有機會發布包含修補程式代碼的修補程式之前發現並利用的軟體弱點。

零時差攻擊

一種利用軟體零時差弱點攻擊企業 IT 基礎架構的攻擊。這些是駭客在軟體供應商發布修補程式之前發現和利用的軟體弱點。

有關協力廠商代碼的資訊

有關協力廠商代碼的資訊包含在應用程式安裝資料夾中的 legal_notices.txt 檔案內。

商標聲明

註冊商標和服務標誌分別屬於其各自的所有者。

Adobe、Flash 是 Adobe 公司在美國和/或其他國家的註冊商標或商標。

AMD 是 Advanced Micro Devices, Inc. 的商標或註冊商標。

Apple、Mac、Macintosh、macOS 和 Safari 是 Apple Inc. 的商標。

Ubuntu 是 Canonical Ltd. 的註冊商標。

Cisco 是 Cisco Systems, Inc. 和/或其附屬公司在美國和某些其他國家/地區的註冊商標或商標。

Citrix 是Cloud Software Group, Inc. 和/或其子公司在美國和/或其他國家的註冊商標或商標。

Docker 和 Docker 標誌是Docker, Inc. 在美國和/或其他國家的商標或註冊商標。Docker, Inc. 和其他方也可能擁有本文所使用的其他術語中所述的商標的權利。

Google、Google Chrome、Android 是Google LLC 的商標。

Intel、Core 和 Xeon 是 Intel Corporation 或其子公司的商標。

Linux 是 Linus Torvalds 在美國和其他國家的註冊商標。

Microsoft、Active Directory、Excel、Internet Explorer、PowerPoint、PowerShell、Win32、Windows、Windows PowerShell、Windows Server 和 Windows XP 是 Microsoft 集團公司的商標。

Mozilla 和 Firefox 是 Mozilla 基金會在美國和其他國家的商標。

NVIDIA 是 NVIDIA 公司的註冊商標。

OpenSSL 是 OpenSSL 軟體基金會的商標。

Java 是 Oracle 和/或其附屬公司的註冊商標。

Python 是 Python 軟體基金會的商標或註冊商標。

CentOS 是 Red Hat, Inc. 或其子公司在美國和其他國家的商標或註冊商標。

Schneider Electric 是 Schneider Electric 的商標。

Siemens 是 Siemens AG 的註冊商標。

Debian 是 Software in the Public Interest, Inc. 的注冊商標。

UNIX 是在美國和其他國家/地區註冊的商標，X/Open Company Limited 根據產品授權使用該商標。