Nexus TDS Insight 使用手冊

SQL Server TDS 封包分析、登入識別與報表匯出

適用產品版本	1.0 (20260527)
手冊版本	1.0
發行日期	2026-06-10

目錄

01 產品概述

02 系統需求與啟動

03 授權與試用模式

04 主畫面導覽

05 快速開始

06 封包與解密設定

07 Session 清單、搜尋與篩選

08 Session 詳細資料

09 通知中心

10 報表匯出

11 疑難排解

12 已知限制

1. 產品概述

Nexus TDS Insight 是 Windows 可攜式 SQL Server TDS 封包分析工具。它會在本機讀取 PCAP/PCAPNG，依 TCP 連線重組 Session，辨識 TDS、TLS、LOGIN7、SSPI、SQL_BATCH 與 RPC，並整理 Client、Server、登入帳號、Database、App、SQL Statement 與執行時間。

主要使用情境

1. 從封包找出哪些用戶端、帳號與應用程式連線到 SQL Server。
2. 在事件調查或變更驗證時，快速檢視 SQL Statement 與 Session 時間範圍。
3. 辨識 TLS Session，判斷登入資料是否因加密而不可見。
4. 將目前篩選結果匯出為 CSV、HTML 或 PDF，或以 JSON 保存完整解析結果。

支援範圍

輸入格式	Classic PCAP、PCAPNG
網路封裝	Ethernet、Linux SLL、Raw IPv4/IPv6、VLAN
主要協定	TCP、SQL Server TDS、TLS 記錄偵測
登入資訊	LOGIN7；部分 NTLM Type 3；Kerberos 通常無法僅由封包還原
一般輸出	Session 清單、詳細資料、CSV、JSON、HTML、PDF

2. 系統需求與啟動

一般使用者應從產品目錄的 dist\NexusTDSInsight.exe 啟動。程式不需要安裝 Python、Node.js 或 IIS；啟動器會將前端檔案解出至本機使用者目錄，並以預設瀏覽器開啟。

作業系統	Windows 10 或 Windows 11（建議使用仍受支援的版本）
執行權限	一般使用者權限即可；讀取受限封包檔時可能需要檔案存取權

作業系統	Windows 10 或 Windows 11（建議使用仍受支援的版本）
瀏覽器	支援現代 JavaScript、File API、WebCrypto 的瀏覽器
記憶體	需求隨封包大小增加；大型封包建議先切割成較小時間區段
網路	分析不需連線；購買授權與聯絡支援連結需要網際網路

啟動步驟

5. 開啟產品資料夾中的 dist 子目錄。
6. 執行 NexusTDSInsight.exe。
7. 若 Windows 顯示「未知發行者」或 SmartScreen 提示，先確認檔案來源與雜湊，再依組織政策決定是否執行。
8. 確認頁首顯示 Nexus TDS Insight 與版本 1.0 (20260527)。

「關於」視窗顯示產品名稱、版本與版權資訊。

3. 授權與試用模式

未輸入有效授權時，產品以試用模式執行。授權狀態儲存在目前瀏覽器的本機儲存空間，因此更換瀏覽器設定檔、清除網站資料或改用不同 Windows 使用者後，可能需要重新啟用。

功能	試用模式	已授權
可見 Session	僅前 10 筆具有 DB user 的 Session	全部解析 Session
無 DB user Session	不顯示	顯示
CSV / JSON / HTML / PDF	停用	啟用
授權識別	頁首顯示「試用版」	頁首顯示授權對象

啟用步驟

9. 按上方「授權」，再選擇「輸入授權金鑰…」。
10. 輸入購買時使用的姓名或組織、Email 與授權金鑰。
11. 按「驗證授權」。成功後，頁首狀態與匯出按鈕會立即更新。
12. 若授權已註銷或 Email 命中黑名單，產品會拒絕啟用；已儲存的授權也可能在下次啟動時被清除。

授權視窗需要姓名/組織、Email 與授權金鑰。

4. 主畫面導覽

主畫面由上方選單、產品標頭、輸入區、搜尋工具列、通知中心、Session 表格與詳細資料區組成。

試用版初始主畫面；匯出按鈕在未授權或尚無結果時停用。

區域	用途
授權 / 幫助	查看授權狀態、輸入授權、開啟購買/支援連結與版本資訊
產品標頭	顯示產品版本、授權狀態，以及 CSV/JSON/HTML/PDF 與清除按鈕
PCAP / PCAPNG	選擇或拖曳封包檔；選取後自動解析
SQL Server Port	預設 1433；可用逗號輸入多個 Port
PFX / PEM / Key	提供可用的 RSA 私鑰材料；PFX/P12 可搭配密碼
統計數字	顯示封包數、TCP Streams 與 SQL Sessions
搜尋 / 篩選	依關鍵字或「全部 / 有 user / TLS」縮小結果
通知	顯示試用限制、TLS 解密與解析警告

5. 快速開始

以下流程適合第一次分析一份 SQL Server 封包。

13. 確認授權狀態。若需查看全部 Session 或匯出報表，請先完成授權。
14. 在「SQL Server Port」輸入伺服器 Port；多個 Port 以逗號分隔，例如 1433,14330。
15. 如需嘗試 TLS 1.2 RSA 解密，先輸入 PFX/P12 密碼，再選擇 PFX/P12/PFXA；或選擇 PEM/KEY 私鑰。
16. 按 PCAP/PCAPNG 的「選擇檔案」，或將封包拖曳至虛線區域。
17. 等待計數器與 Session 表格更新。解析在瀏覽器本機進行，時間取決於封包大小。
18. 使用搜尋、篩選與欄位排序找到目標 Session。
19. 按 Session 列查看詳細資料與 SQL Statements。
20. 確認篩選結果後，選擇所需的報表格式。

重要: 成功時，封包、TCP streams 與 SQL sessions 計數會更新，Session 表格至少顯示一列。若只有 TLS Session 而沒有 user，請先閱讀通知中心，不要將空白 user 誤判為沒有連線。

6. 封包與解密設定

設定	操作與影響
PCAP / PCAPNG	支援單一封包檔；重新選取檔案會取代目前結果
SQL Server Port	預設 1433；輸入 1 到 65535 的整數，可用逗號分隔
包含只符合 port 的 TCP session	啟用後，即使未辨識為 TDS/TLS，只要端點符合指定 Port 也會列出
PFX / P12 密碼	輸入後按 Enter 或變更欄位可重新解析目前封包
清除	清除目前封包、金鑰檔、密碼、搜尋、篩選、通知與詳細資料

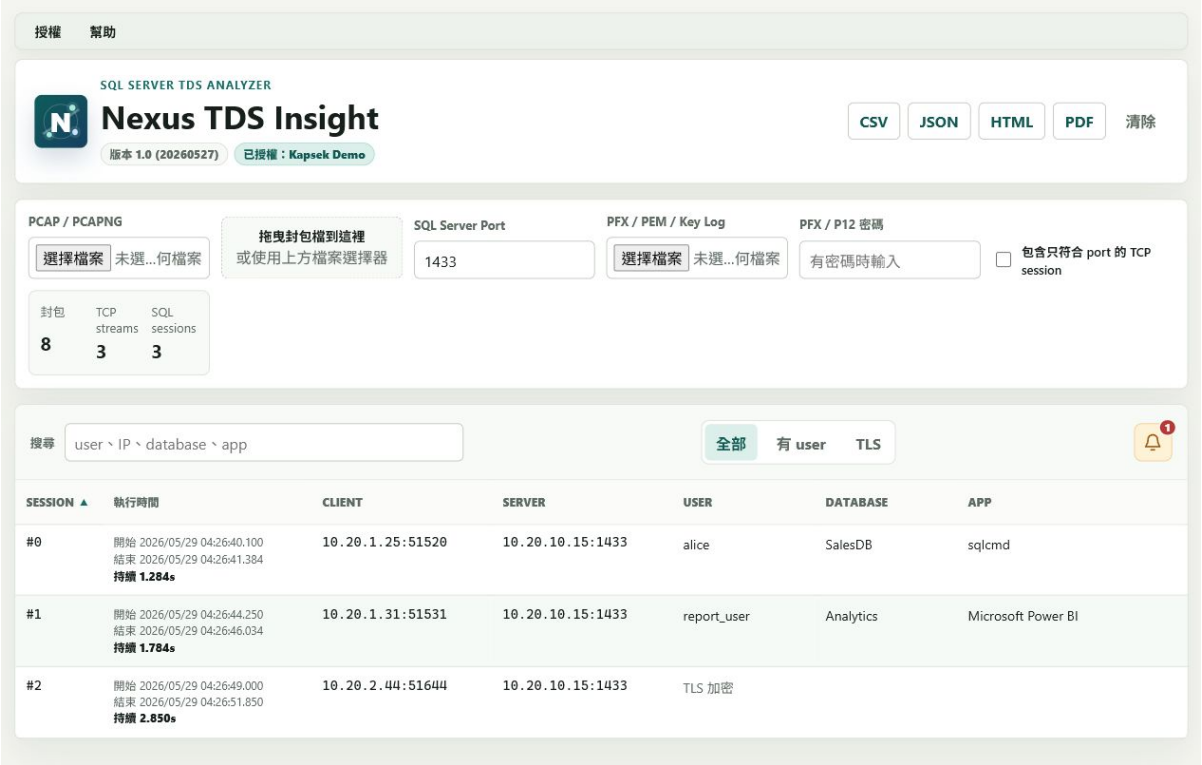
TLS 解密能力與限制

21. 目前瀏覽器版會從 PEM、KEY、TXT 或 PFX/P12/PFXA 嘗試讀取 RSA 私鑰。

22. 僅適用於封包中含完整交握、且使用受支援 TLS 1.2 RSA key exchange 的情況。
23. TLS 1.2 ECDHE、TLS 1.3，以及缺少 full handshake/master secret 的 resumed TLS，無法只靠伺服器私鑰解密。
24. 檔案選擇器雖顯示 Key Log/.log，但目前瀏覽器實作不會以 key log 解密；需要使用具 TShark/key log 支援的進階工作流程。
25. 金鑰檔與密碼屬敏感資料。只應在受控端點使用，並遵循組織的憑證與私鑰管理政策。

7. Session 清單、搜尋與篩選

解析完成後，表格以 TCP Stream 為單位顯示結果。表格可水平捲動；點選欄名可切換升冪/降冪，拖曳欄位右側邊界可調整欄寬。排序與欄寬會保存在目前瀏覽器。



已授權的範例結果，包含兩個可辨識登入與一個 TLS Session。

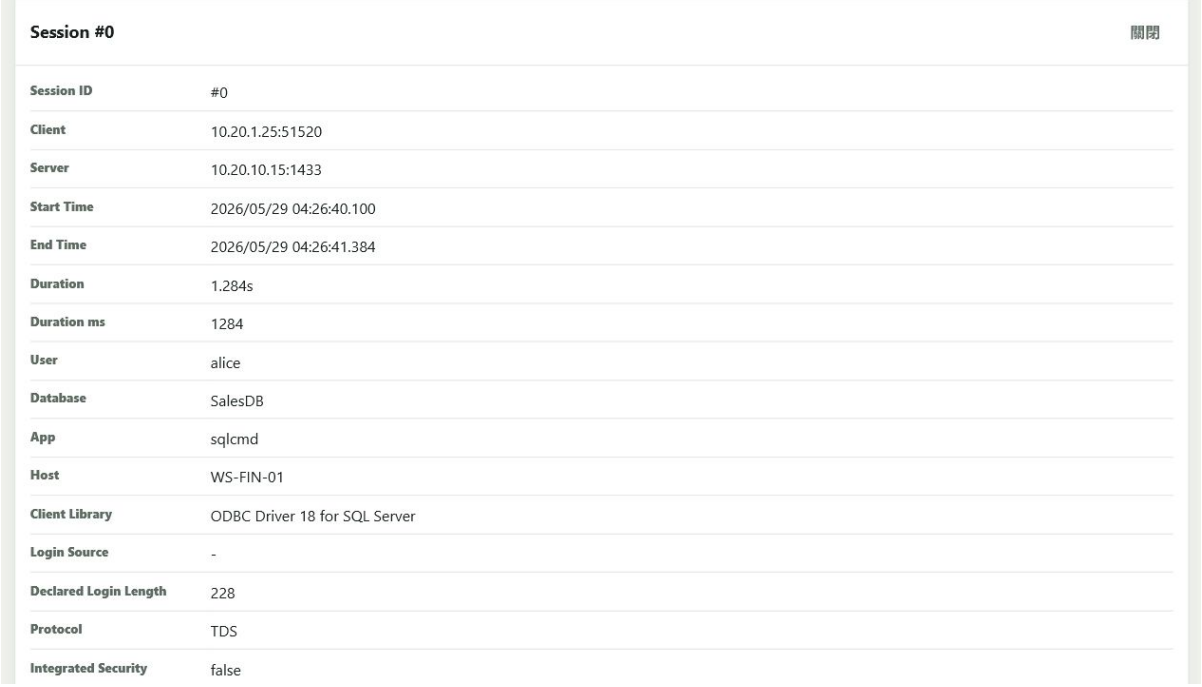
26. 搜尋會比對 Session ID、Client/Server IP、user、database、app、host、SQL、加密資訊與 notes。

27. 「有 user」只保留已解析 display user 的 Session。
28. 「TLS」只保留偵測到 TLS 的 Session。
29. 匯出 CSV、HTML 與 PDF 時，會使用目前授權可見且經過搜尋/篩選後的 Session。

欄位	說明
Session	產品內部 TCP Stream 編號
執行時間	開始、結束與兩者差值；代表封包內可觀察的 Session 時間範圍
Client / Server	推定的用戶端與 SQL Server IP:Port
User	LOGIN7 user 或可見的 NTLM 使用者；TLS 加密時可能空白
Database	LOGIN7 所要求的 Database，不一定等同登入後有效資料庫主體
App	LOGIN7 App Name，例如 sqlcmd、Power BI 或自訂應用程式名稱
SQL	第一筆 SQL Statement 預覽；完整內容位於詳細資料
Protocol	TDS、TLS、TDS + TLS 或 TCP
狀態	USER、TLS、TDS 或 PORT

8. Session 詳細資料

按任一 Session 列會展開詳細資料。再次選擇其他列可切換內容；按右上角「關閉」可收合。



Session #0 關閉

Session ID	#0
Client	10.20.1.25:51520
Server	10.20.10.15:1433
Start Time	2026/05/29 04:26:40.100
End Time	2026/05/29 04:26:41.384
Duration	1.284s
Duration ms	1284
User	alice
Database	SalesDB
App	sqlcmd
Host	WS-FIN-01
Client Library	ODBC Driver 18 for SQL Server
Login Source	-
Declared Login Length	228
Protocol	TDS
Integrated Security	false

Session 詳細資料上半部：端點、時間、使用者、Database、App 與 Client Library。

Login Source	-
Declared Login Length	228
Protocol	TDS
Integrated Security	false
TLS Detected	false
TDS Detected	true
TDS Types	LOGIN7, SQL_BATCH, TABULAR_RESULT
Encryption	-
Prelogin Details	{ "client": [], "server": [] }
Bytes C->S	426
Bytes S->C	9
TCP Segments	3
SQL Count	1
SQL Statements	-- #1 SELECT TOP (20) OrderId, CustomerName, TotalAmount FROM dbo.Orders ORDER BY OrderDate DESC;
Notes	-

Session 詳細資料下半部：協定、TDS 類型、流量統計與完整 SQL Statements。

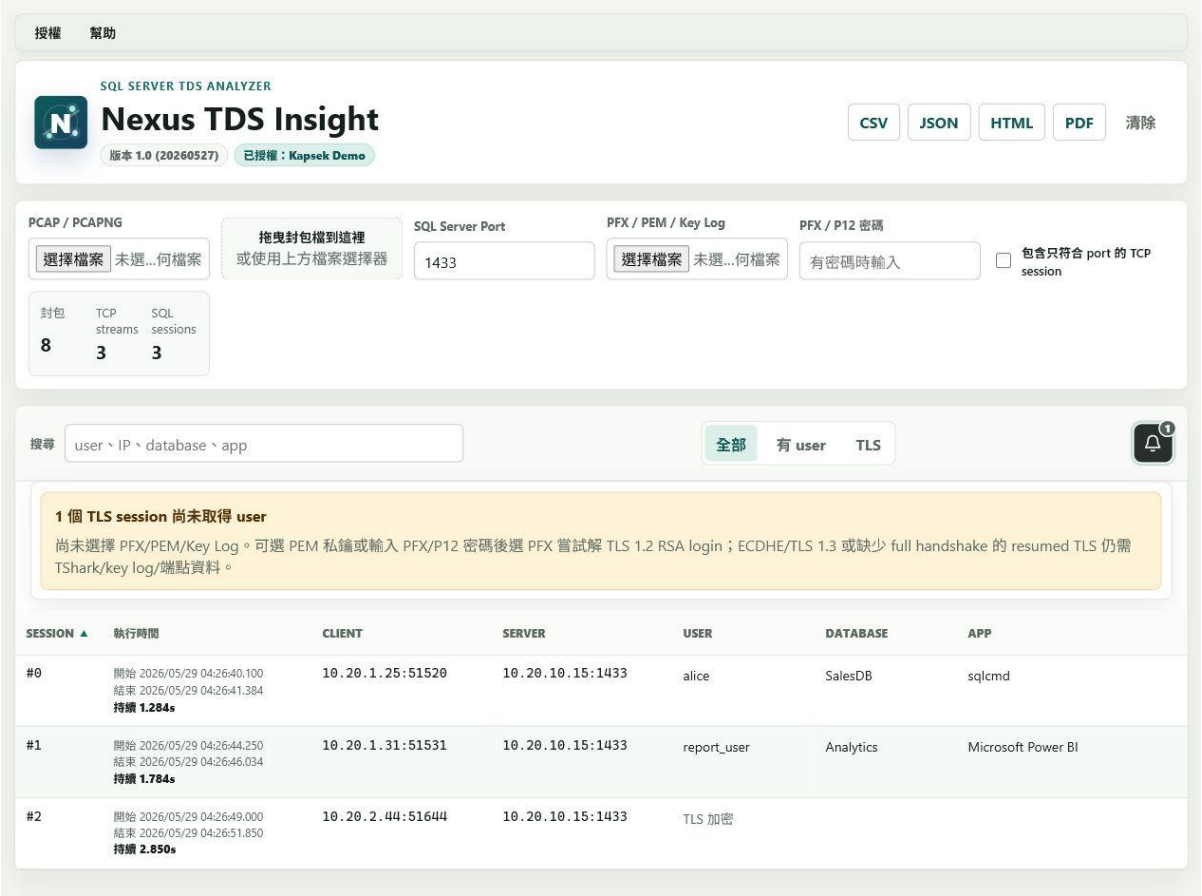
群組	重點欄位
識別與時間	Session ID、Client、Server、Start Time、End Time、Duration、Duration

群組	重點欄位
	ms
登入	User、Database、App、Host、Client Library、Login Source、Declared Login Length
協定	Protocol、Integrated Security、TLS Detected、TDS Detected、TDS Types、Encryption
流量	Bytes C->S、Bytes S->C、TCP Segments
SQL 與備註	SQL Count、SQL Statements、Notes

注意:「執行時間」是目前 TCP Stream 中第一個與最後一個可見封包的時間差，不一定等同 SQL Server 端真正的查詢 CPU 時間或伺服器執行計畫耗時。

9. 通知中心

當產品有試用限制、TLS 尚未取得 user、金鑰讀取失敗、封包格式異常或其他解析警告時，工具列右側會顯示通知鈴鐺與數量。按鈴鐺可展開訊息；已讀狀態會保存在目前瀏覽器。



通知中心說明 TLS Session 為何尚未取得 user，並提供下一步建議。

30. 先閱讀完整訊息；通知通常包含缺少的資料、密碼錯誤或不支援的 TLS 類型。
31. 若訊息指出沒有 SQL Server Session，確認 Port、封包方向與封包是否包含登入階段。
32. 若訊息指出 TLS Session 無 user，檢查是否有完整交握與合適的 RSA 私鑰；否則改用端點或 TShark/key log 工作流程。

10. 報表匯出

匯出只在已授權且目前有可見 Session 時啟用。匯出前應先確認搜尋與篩選條件，避免把不相關 Session 放入報表。

格式	內容與適用情境
CSV	目前篩選 Session；適合 Excel、SIEM 匯入或後續資料整理

格式	內容與適用情境
JSON	完整 results 物件，包含 counters、全部 Sessions、warnings 與解析欄位
HTML	獨立離線報表，包含摘要、Session overview、詳細資料與 SQL
PDF	以 jsPDF 產生文字型多頁報表；包含摘要、Session overview、詳細資料、SQL 與頁碼

33. CSV 使用 UTF-8，欄位包含端點、user、database、app、host、SQL、時間、Protocol 與 notes。
34. PDF 直接產生失敗時，產品會開啟或下載 HTML 報表，供使用者以瀏覽器列印成 PDF。
35. 瀏覽器若阻擋新視窗，產品可能改為下載 HTML；請檢查下載列與彈出式視窗設定。
36. 報表可能包含帳號、IP、Database 與 SQL 文字，分享前應依資料分級政策審查。

11. 疑難排解

問題	可能原因	處理方式
沒有任何 Session	Port 錯誤、非 TCP、封包不含 SQL 流量	確認 SQL Server Port；必要時啟用「包含只符合 port」
有 Session 但沒有 user	缺少 LOGIN7、TLS 加密、從連線中途開始擷取	重新擷取登入階段；檢查通知與 Protocol
TLS 私鑰無法取得 user	ECDHE/TLS 1.3、resumed TLS、PFX 密碼錯誤、私鑰不匹配	確認交握與 Cipher；改用端點或 TShark/key log
Port 欄位錯誤	輸入非整數或超出 1-65535	使用逗號分隔有效 Port，例如 1433,14330
匯出按鈕停用	試用模式、沒有結果、目前篩選為空	完成授權並調整搜尋/篩選
PDF 未直接下載	瀏覽器限制或 jsPDF 失敗	使用產品提供的 HTML fallback，再列印為 PDF
大型封包反應慢	瀏覽器記憶體與單執行緒解析負荷	先用 Wireshark/tshark 依時間或主機切割封包

問題	可能原因	處理方式
重新啟動後授權消失	清除網站資料、換瀏覽器設定檔、授權被註銷	重新輸入有效授權；仍失敗時聯絡支援

12. 已知限制

37. 無法使用伺服器私鑰解密 TLS 1.2 ECDHE 或 TLS 1.3。
38. Resumed TLS 若封包中沒有完整交握/master secret，無法僅靠私鑰還原。
39. Kerberos 使用者通常無法只由封包內容可靠還原。
40. 若封包未包含 LOGIN7，TDS Session 可能存在但 user、database、app 仍為空白。
41. SQL 擷取屬封包解析與文字啟發式；截斷、重組缺口或非典型 RPC 可能造成不完整結果。
42. 超長 SQL 會在 PDF 中換行與分頁；仍應在交付前目視檢查報表。