# Nexus TDS Insight 用户手册

SQL Server TDS 数据包分析、登录识别与报告导出

| | |
|---|---|
| **适用产品版本** | 1.0 (20260527) |
| **手册版本** | 1.0 |
| **发布日期** | 2026-06-10 |

# 目录

# 1. 产品概述

Nexus TDS Insight 是 Windows 便携式 SQL Server TDS 数据包分析工具。它在本机读取 PCAP/PCAPNG，按 TCP 连接重组 Session，识别 TDS、TLS、LOGIN7、SSPI、SQL_BATCH 与 RPC，并整理 Client、Server、登录账号、Database、App、SQL Statement 与执行时间。

## 主要使用场景

1. 从数据包中找出哪些客户端、账号与应用程序连接到 SQL Server。
2. 在事件调查或变更验证时，快速查看 SQL Statement 与 Session 时间范围。
3. 识别 TLS Session，判断登录数据是否因加密而不可见。
4. 将当前筛选结果导出为 CSV、HTML 或 PDF，或用 JSON 保存完整解析结果。

## 支持范围

| 输入格式 | Classic PCAP、PCAPNG |
| --- | --- |
| 网络封装 | Ethernet、Linux SLL、Raw IPv4/IPv6、VLAN |
| 主要协议 | TCP、SQL Server TDS、TLS 记录检测 |
| 登录信息 | LOGIN7；部分 NTLM Type 3；Kerberos 通常无法仅从数据包还原 |
| 常用输出 | Session 列表、详细信息、CSV、JSON、HTML、PDF |

# 2. 系统要求与启动

普通用户应从产品目录的 dist\NexusTDSInsight.exe 启动。程序不需要安装 Python、Node.js 或 IIS；启动器会把前端文件解压到本地用户目录，并使用默认浏览器打开。

| 操作系统 | Windows 10 或 Windows 11（建议使用仍受支持的版本） |
| --- | --- |
| 运行权限 | 普通用户权限即可；读取受限数据包时可能需要文件访问权限 |

| 操作系统 | Windows 10 或 Windows 11（建议使用仍受支持的版本） |
| --- | --- |
| 浏览器 | 支持现代 JavaScript、File API、WebCrypto 的浏览器 |
| 内存 | 需求随数据包大小增加；大型数据包建议先切分为较小时间段 |
| 网络 | 分析无需联网；购买授权与联系支持链接需要互联网 |

## 启动步骤

5. 打开产品文件夹中的 dist 子目录。
6. 运行 NexusTDSInsight.exe。
7. 如果 Windows 显示“未知发布者”或 SmartScreen 提示，请先确认文件来源与哈希，再按组织策略决定是否运行。
8. 确认页首显示 Nexus TDS Insight 与版本 1.0 (20260527)。


“关于”窗口显示产品名称、版本与版权信息。

# 3. 授权与试用模式

未输入有效授权时，产品以试用模式运行。授权状态保存在当前浏览器的本地存储中，因此更换浏览器配置文件、清除网站数据或使用其他 Windows 用户后，可能需要重新激活。

| 功能 | 试用模式 | 已授权 |
| --- | --- | --- |
| 可见 Session | 仅前 10 条具有 DB user 的 Session | 全部解析 Session |
| 无 DB user Session | 不显示 | 显示 |
| CSV / JSON / HTML / PDF | 禁用 | 启用 |
| 授权标识 | 页首显示“试用版” | 页首显示授权对象 |

## 激活步骤

9. 单击上方“授权”，再选择“输入授权金钥...”。
10. 输入购买时使用的姓名或组织、Email 与授权密钥。
11. 单击“验证授权”。成功后，页首状态与导出按钮会立即更新。
12. 如果授权已注销或 Email 命中黑名单，产品会拒绝激活；已保存的授权也可能在下次启动时被清除。


授权窗口需要姓名/组织、Email 与授权密钥。

## 4. 主界面导览

主界面由顶部菜单、产品标题、输入区、搜索工具栏、通知中心、Session 表格与详细信息区组成。


试用版初始主界面；未授权或没有结果时导出按钮处于禁用状态。

| 区域 | 用途 |
| --- | --- |
| 授权 / 帮助 | 查看授权状态、输入授权、打开购买/支持链接与版本信息 |
| 产品标题 | 显示产品版本、授权状态，以及 CSV/JSON/HTML/PDF 与清除按钮 |
| PCAP / PCAPNG | 选择或拖放数据包；选择后自动解析 |
| SQL Server Port | 默认 1433；可用逗号输入多个 Port |
| PFX / PEM / Key | 提供可用的 RSA 私钥材料；PFX/P12 可配合密码 |
| 统计数字 | 显示数据包数、TCP Streams 与 SQL Sessions |
| 搜索 / 筛选 | 按关键词或“全部 / 有 user / TLS”缩小结果 |
| 通知 | 显示试用限制、TLS 解密与解析警告 |

## 5. 快速开始

以下流程适合第一次分析 SQL Server 数据包。

13. 确认授权状态。如需查看全部 Session 或导出报告，请先完成授权。
14. 在“SQL Server Port”输入服务器 Port；多个 Port 用逗号分隔，例如 1433,14330。
15. 如需尝试 TLS 1.2 RSA 解密，先输入 PFX/P12 密码，再选择 PFX/P12/PFXA；或选择 PEM/KEY 私钥。
16. 单击 PCAP/PCAPNG 的“选择文件”，或把数据包拖到虚线区域。
17. 等待计数器与 Session 表格更新。解析在浏览器本地进行，耗时取决于数据包大小。
18. 使用搜索、筛选与字段排序找到目标 Session。
19. 单击 Session 行查看详细信息与 SQL Statements。
20. 确认筛选结果后，选择需要的报告格式。

**重要:** 成功时，数据包、TCP streams 与 SQL sessions 计数会更新，Session 表格至少显示一行。如果只有 TLS Session 而没有 user，请先阅读通知中心，不要把空白 user 误判为没有连接。

## 6. 数据包与解密设置

| 设置 | 操作与影响 |
| --- | --- |
| PCAP / PCAPNG | 支持单个数据包；重新选择会替换当前结果 |
| SQL Server Port | 默认 1433；输入 1 到 65535 的整数，可用逗号分隔 |
| 包含只符合 port 的 TCP session | 启用后，即使未识别为 TDS/TLS，只要端点符合指定 Port 也会列出 |
| PFX / P12 密码 | 输入后按 Enter 或更改字段可重新解析当前数据包 |
| 清除 | 清除当前数据包、密钥文件、密码、搜索、筛选、通知与详细信息 |

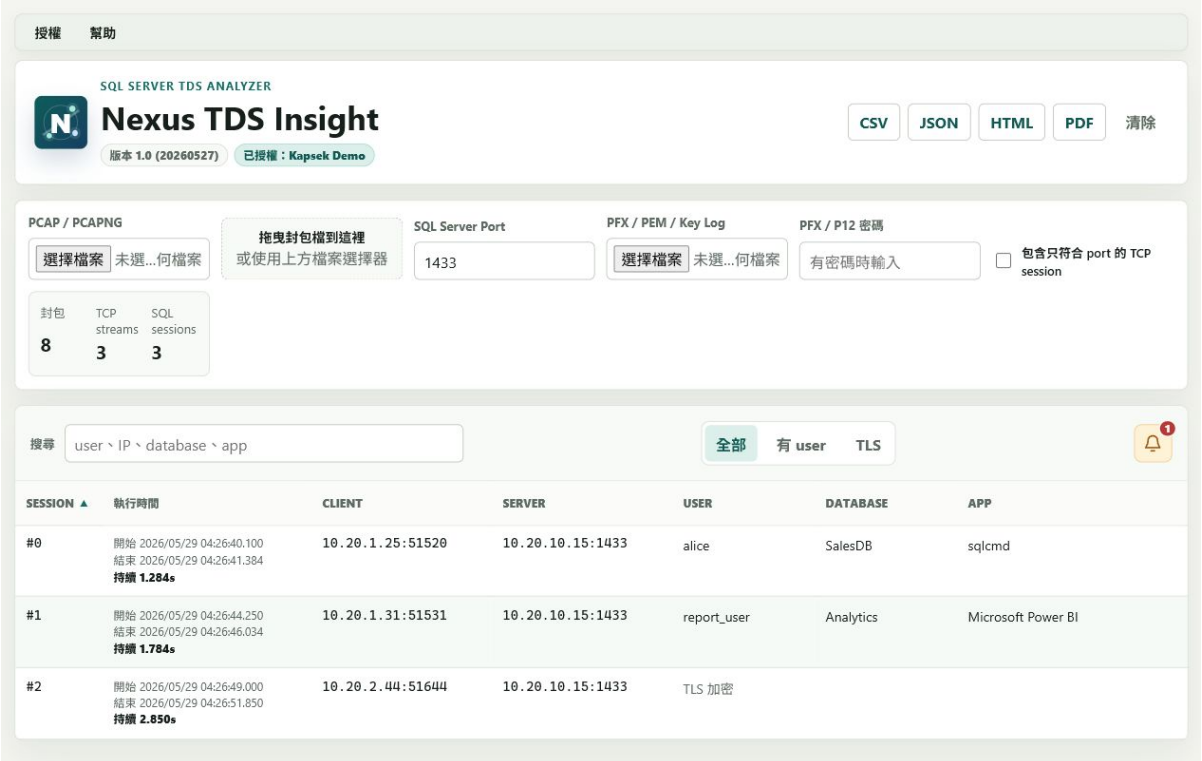
### TLS 解密能力与限制

21. 当前浏览器版会从 PEM、KEY、TXT 或 PFX/P12/PFXA 尝试读取 RSA 私钥。

22. 仅适用于数据包包含完整握手且使用受支持 TLS 1.2 RSA key exchange 的情况。
23. TLS 1.2 ECDHE、TLS 1.3，以及缺少 full handshake/master secret 的 resumed TLS，无法仅靠服务器私钥解密。
24. 文件选择器虽然显示 Key Log/.log，但当前浏览器实现不会用 key log 解密；需要使用支持 TShark/key log 的高级流程。
25. 密钥文件与密码属于敏感数据，只应在受控终端使用，并遵循组织的证书与私钥管理策略。

## 7. Session 列表、搜索与筛选

解析完成后，表格按 TCP Stream 显示结果。表格可水平滚动；单击列名可切换升序/降序，拖动列右侧边界可调整列宽。排序与列宽会保存在当前浏览器。




已授权的示例结果，包含两个可识别登录与一个 TLS Session。

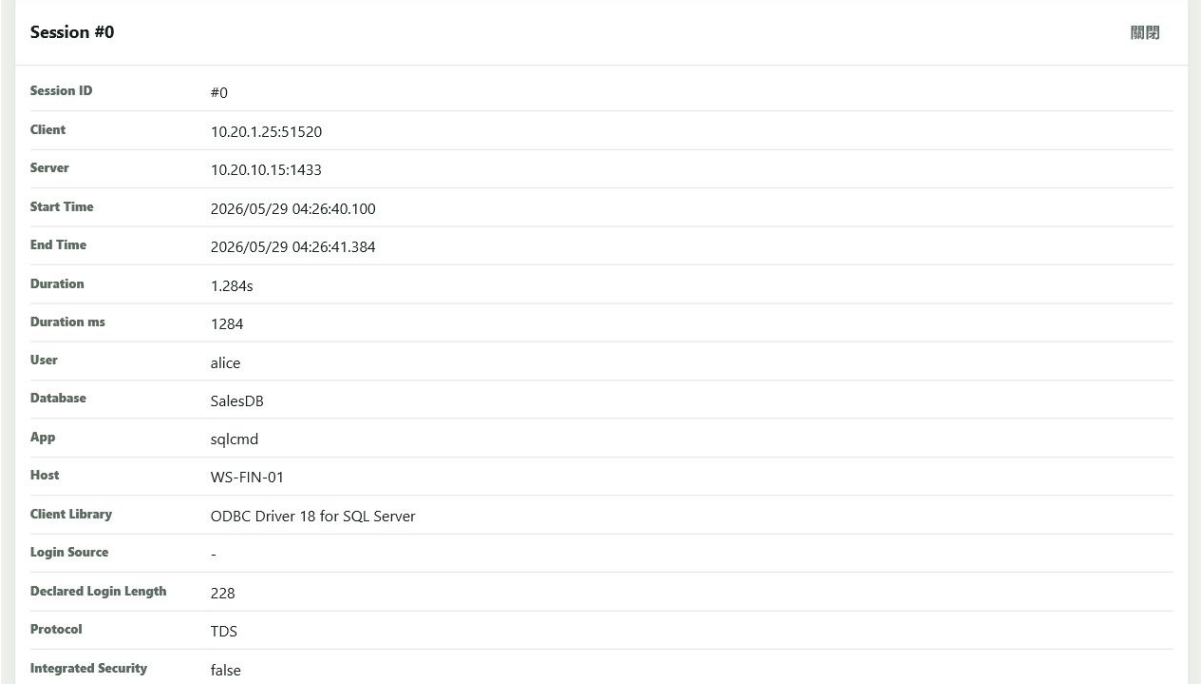
26. 搜索会匹配 Session ID、Client/Server IP、user、database、app、host、SQL、加密信息与 notes。

27. “有 user”只保留已解析 display user 的 Session。
28. “TLS”只保留检测到 TLS 的 Session。
29. 导出 CSV、HTML 与 PDF 时，会使用当前授权可见且经过搜索/筛选后的 Session。

| 字段 | 说明 |
| --- | --- |
| Session | 产品内部 TCP Stream 编号 |
| 执行时间 | 开始、结束与差值；表示数据包内可观察的 Session 时间范围 |
| Client / Server | 推断的客户端与 SQL Server IP:Port |
| User | LOGIN7 user 或可见 NTLM 用户；TLS 加密时可能为空 |
| Database | LOGIN7 请求的 Database，不一定等于登录后的有效数据库主体 |
| App | LOGIN7 App Name，例如 sqlcmd、Power BI 或自定义应用名称 |
| SQL | 第一条 SQL Statement 预览；完整内容位于详细信息 |
| Protocol | TDS、TLS、TDS + TLS 或 TCP |
| 状态 | USER、TLS、TDS 或 PORT |

## 8. Session 详细信息

单击任一 Session 行会展开详细信息。再次选择其他行可切换内容；单击右上角“关闭”可收起。



**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 详细信息上半部分：端点、时间、用户、Database、App 与 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<br>SELECT TOP (20) OrderId, CustomerName, TotalAmount FROM dbo.Orders ORDER BY OrderDate DESC; |
| Notes | - |

Session 详细信息下半部分：协议、TDS 类型、流量统计与完整 SQL Statements。

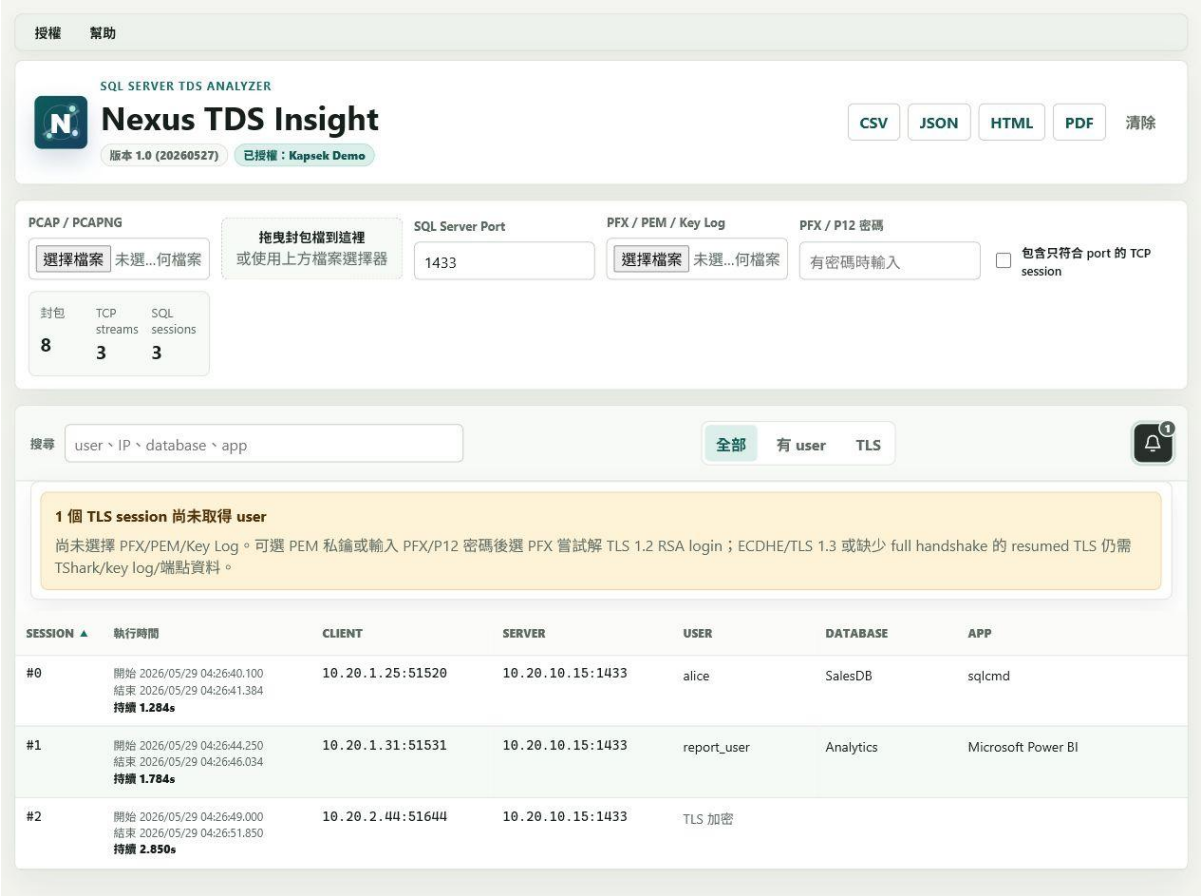
| 分组 | 重点字段 |
|---|---|
| 标识与时间 | Session ID、Client、Server、Start Time、End Time、Duration、 |

| 分组 | 重点字段 |
| --- | --- |
| | Duration ms |
| 登录 | User、Database、App、Host、Client Library、Login Source、Declared Login Length |
| 协议 | Protocol、Integrated Security、TLS Detected、TDS Detected、TDS Types、Encryption |
| 流量 | Bytes C->S、Bytes S->C、TCP Segments |
| SQL 与备注 | SQL Count、SQL Statements、Notes |

**注意：** “执行时间”是当前 TCP Stream 中第一个与最后一个可见数据包的时间差，不一定等于 SQL Server 端真实查询 CPU 时间或执行计划耗时。

## 9. 通知中心

当产品存在试用限制、TLS 尚未取得 user、密钥读取失败、数据包格式异常或其他解析警告时，工具栏右侧会显示通知铃铛与数量。单击铃铛可展开消息；已读状态会保存在当前浏览器。




通知中心说明 TLS Session 为什么尚未取得 user，并给出下一步建议。

30. 先阅读完整消息；通知通常包含缺少的数据、密码错误或不支持的 TLS 类型。
31. 如果消息指出没有 SQL Server Session，请确认 Port、数据包方向以及是否包含登录阶段。
32. 如果 TLS Session 无 user，请检查是否有完整握手与匹配的 RSA 私钥；否则改用端点或 TShark/key log 流程。

## 10. 报告导出

导出仅在已授权且当前存在可见 Session 时启用。导出前应先确认搜索与筛选条件。

| 格式 | 内容与适用场景 |
| --- | --- |
| CSV | 当前筛选 Session；适合 Excel、SIEM 导入或后续整理 |

| 格式 | 内容与适用场景 |
| --- | --- |
| JSON | 完整 results 对象，包含 counters、全部 Sessions、warnings 与解析字段 |
| HTML | 独立离线报告，包含摘要、Session overview、详细信息与 SQL |
| PDF | 使用 jsPDF 生成文本型多页报告；包含摘要、Session overview、详细信息、SQL 与页码 |

33. CSV 使用 UTF-8，字段包含端点、user、database、app、host、SQL、时间、Protocol 与 notes。
34. PDF 直接生成失败时，产品会打开或下载 HTML 报告，供用户用浏览器打印为 PDF。
35. 浏览器阻止新窗口时，产品可能改为下载 HTML；请检查下载栏与弹窗设置。
36. 报告可能包含账号、IP、Database 与 SQL 文本，分享前应按数据分级策略审查。

## 11. 故障排除

| 问题 | 可能原因 | 处理方法 |
| --- | --- | --- |
| 没有任何 Session | Port 错误、非 TCP、数据包不含 SQL 流量 | 确认 SQL Server Port；必要时启用“包含只符合 port” |
| 有 Session 但没有 user | 缺少 LOGIN7、TLS 加密、从连接中途开始抓包 | 重新捕获登录阶段；检查通知与 Protocol |
| TLS 私钥无法取得 user | ECDHE/TLS 1.3、resumed TLS、PFX 密码错误、私钥不匹配 | 确认握手与 Cipher；改用端点或 TShark/key log |
| Port 字段错误 | 输入非整数或超出 1-65535 | 用逗号分隔有效 Port，例如 1433,14330 |
| 导出按钮禁用 | 试用模式、没有结果、当前筛选为空 | 完成授权并调整搜索/筛选 |
| PDF 未直接下载 | 浏览器限制或 jsPDF 失败 | 使用产品提供的 HTML fallback，再打印为 PDF |
| 大型数据包响应慢 | 浏览器内存与单线程解析负荷 | 先用 Wireshark/tshark 按时间或主机切分 |
| 重启后授权消失 | 清除网站数据、换浏览器配置、授权被 | 重新输入有效授权；仍失败时联系支持 |

| 问题 | 可能原因 | 处理方法 |
| --- | --- | --- |
| | 注销 | |

## 12. 已知限制

37. 无法使用服务器私钥解密 TLS 1.2 ECDHE 或 TLS 1.3。
38. Resumed TLS 若数据包中没有完整握手/master secret，无法仅靠私钥还原。
39. Kerberos 用户通常无法仅从数据包可靠还原。
40. 如果数据包不含 LOGIN7，TDS Session 可能存在，但 user、database、app 仍为空。
41. SQL 提取属于数据包解析与文本启发式；截断、重组缺口或非典型 RPC 可能导致不完整。
42. 超长 SQL 会在 PDF 中换行与分页；交付前仍应目视检查报告。