收集Windows和MacOS上安全客戶端的KDF日誌

目錄

簡介

Windows和MacOS標誌

收集KDF日誌、Wireshark和DART捆綁包

Windows

MacOS

相關資訊

簡介

本文說明如何收集Windows和MacOS上的KDF日誌和其他重要故障排除日誌。

Windows和MacOS標誌

與DNS相關（涉及OpenDNS時）：	0x20801FF
Web flow(SWG)代理和DNS相關：	0x70C01FF
ZTA	0x400080152

收集KDF日誌、Wireshark和DART捆綁包

附註：當您提交結果時，應始終讓TAC團隊知道使用了哪些設定，並可根據TAC的要求進行更改。

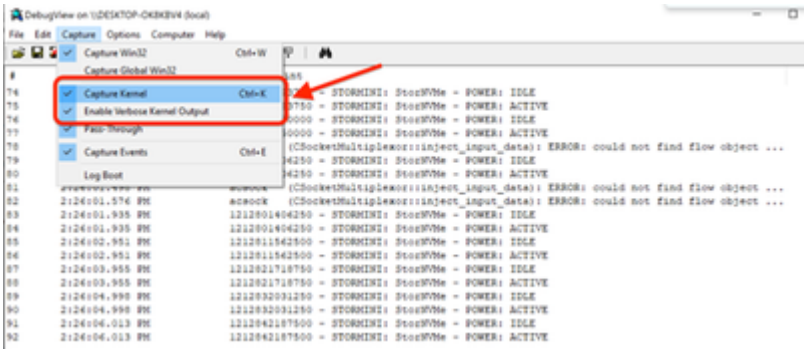
Windows

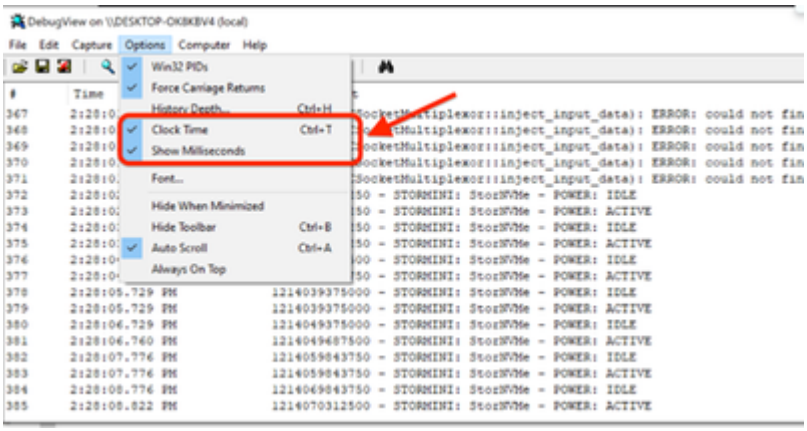
開啟具有管理員許可權的CMD並運行下一個命令：

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf [FLAG]
```

- 從SysInternal下載DebugView以捕獲KDF日誌
- 運行DebugViewadministrator 並啟用下一個選單選項：
- 按一下Capture（捕獲）

    - 複選標籤 Capture Kernel
    - 複選標籤 Enable Verbose Kernel Output
- 選項
    - 複選標籤 Clock Time
    - 複選標籤 Show Milliseconds

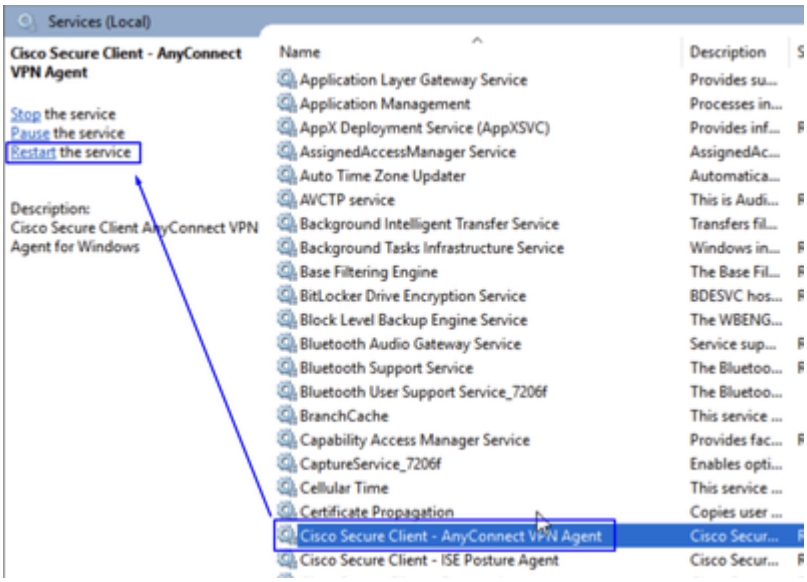




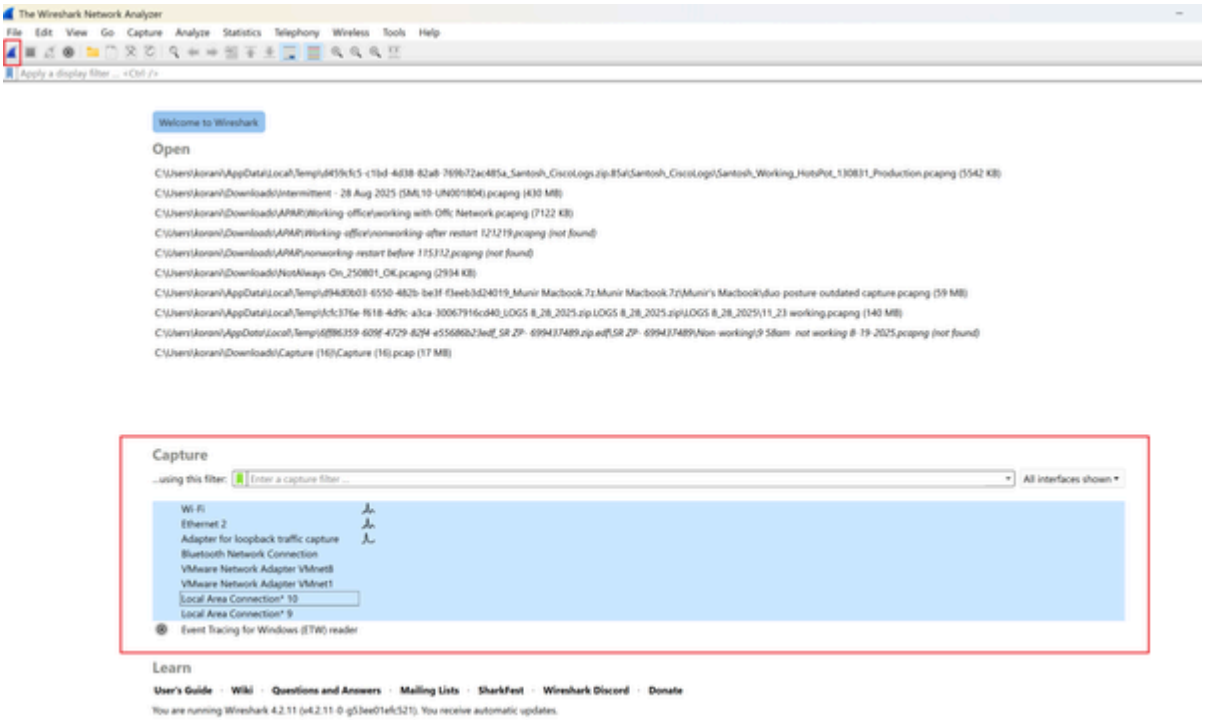
- 通過管理員提示重新啟動客戶端服務：

```
net stop csc_vpnagent && net start csc_vpnagent
```

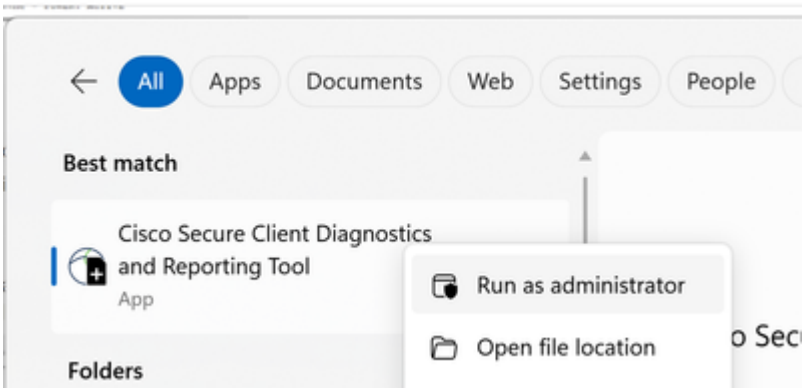
- 如果net stop csc_vpnagent && net start csc_vpnagent不起作用，請從servicesCisco Secure Client.msc重新啟動服務



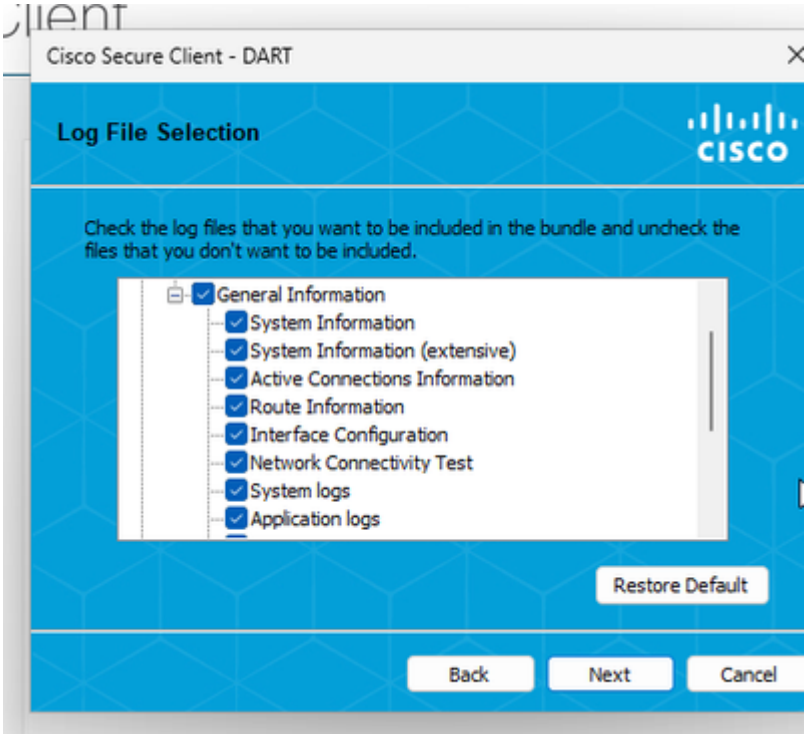
- 開始 Wireshark Capture
- 選擇所有介面，然後開始資料包捕獲



- 重現問題，然後儲存KDF LogsWireshark Capture，然後按照步驟進行捕獲 DART Bundle
- 以管理員許可權開啟Cisco Secure Client Diagnostics & Reporting Tool (DART)



- 按一下 Custom
  - 包括System Information Extensive和 Network Connectivity Test



附註：將所有日誌、KDF日誌、Wireshark捕獲和DART捆綁包收集到TAC案例。

- 要停止Windows上的KDF日誌記錄，請使用以下命令：

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

MacOS

開啟terminal，然後按照下一個命令鏈在MacOS上啟用KDF日誌記錄：

- Stop Service

```
sudo "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app/Contents/MacOS/Cisco
```

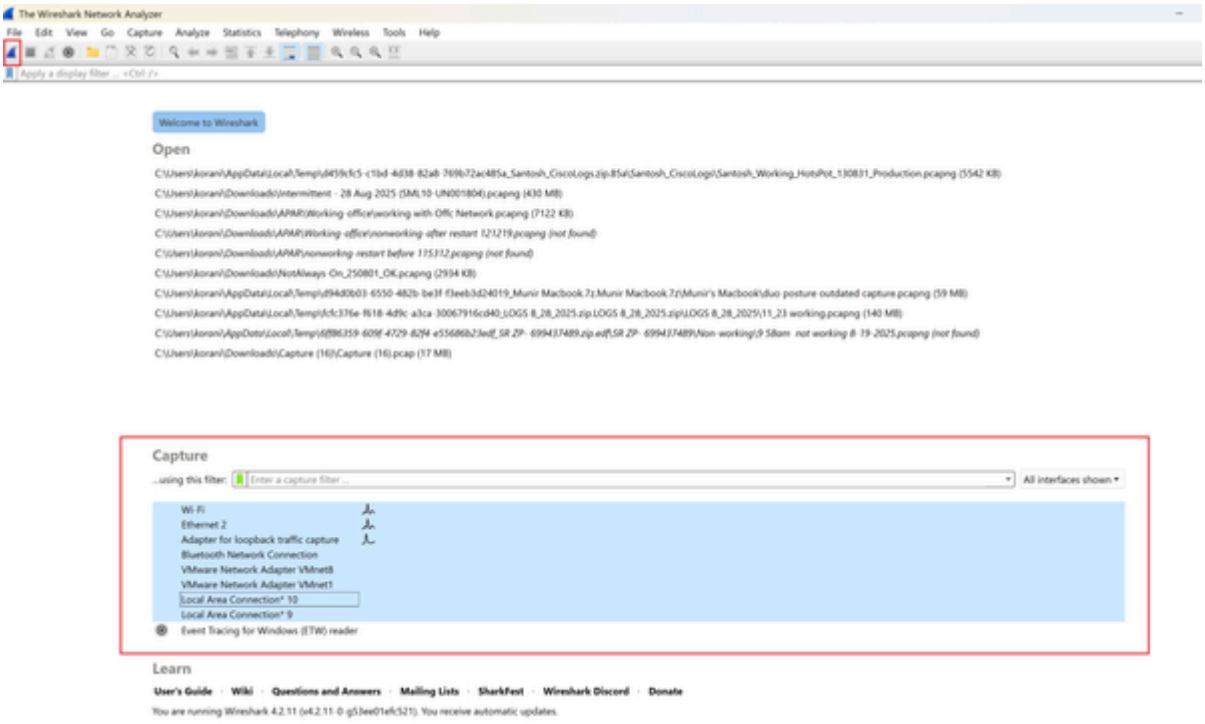
- Enable Flag

```
echo debug=[Flag Value] | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

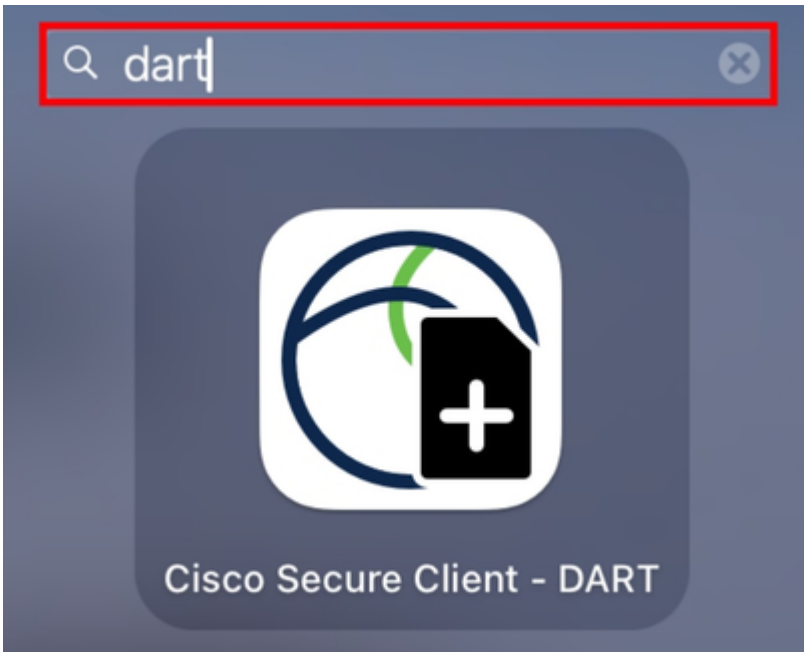
- Start Service

```
open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

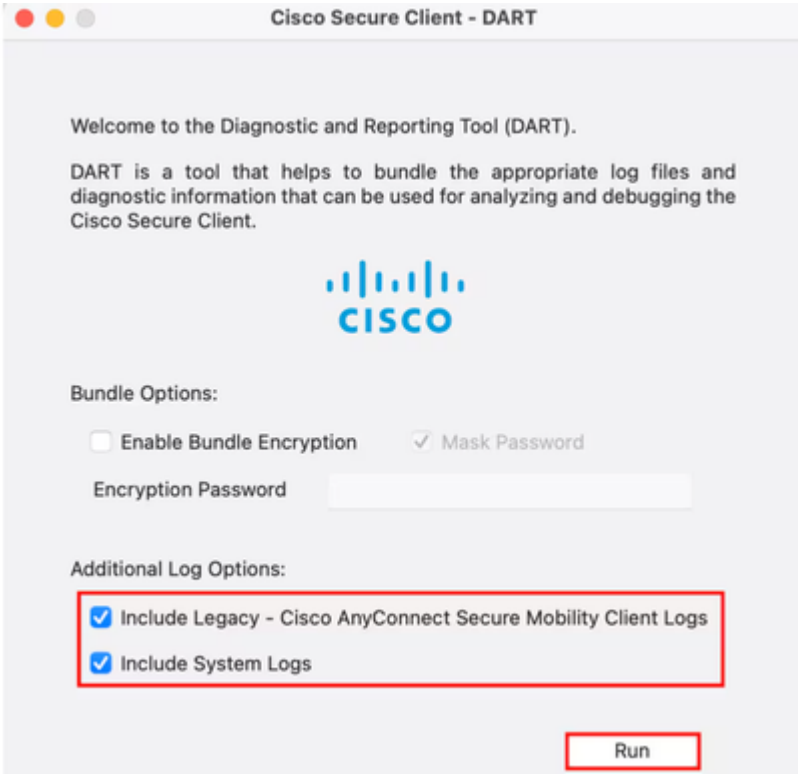
- 開始 Wireshark Capture
- 選擇所有介面，然後開始資料包捕獲



- 重現問題，然後儲存KDF LogsWireshark Capture，然後按照步驟進行捕獲 DART Bundle
- 開啟 Cisco Secure Client - DART



- 選中下一個選項：
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- 按一下 Run



附註：將所有日誌、KDF日誌、Wireshark捕獲和DART捆綁包收集到TAC案例。

相關資訊

- 思科技術支援與下載
- Cisco Secure Access幫助中心
- Cisco SASE設計手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。