WindowsおよびMacOS上のセキュアクライアントのKDFログの収集

内容

はじめに

WindowsおよびMacOSフラグ

- KDFログ、Wireshark、およびDARTバンドルの収集
  - Windows
  - MacOS

関連情報

はじめに

このドキュメントでは、WindowsおよびMacOSでKDFログおよびその他の重要なトラブルシューティングログを収集する方法について説明します。

WindowsおよびMacOSフラグ

DNS関連（OpenDNSが含まれる場合）:	0x20801FF
Web flow(SWG)プロキシおよびDNS関連：	0x70C01FF
ZTA	0x400080152

KDFログ、Wireshark、およびDARTバンドルの収集

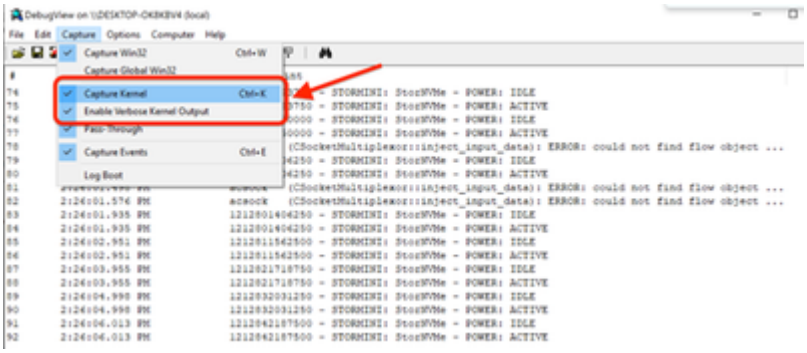
注：結果を送信する際には、使用された設定をTACチームに必ず知らせ、TACの必要に応じて変更できるようにしてください。

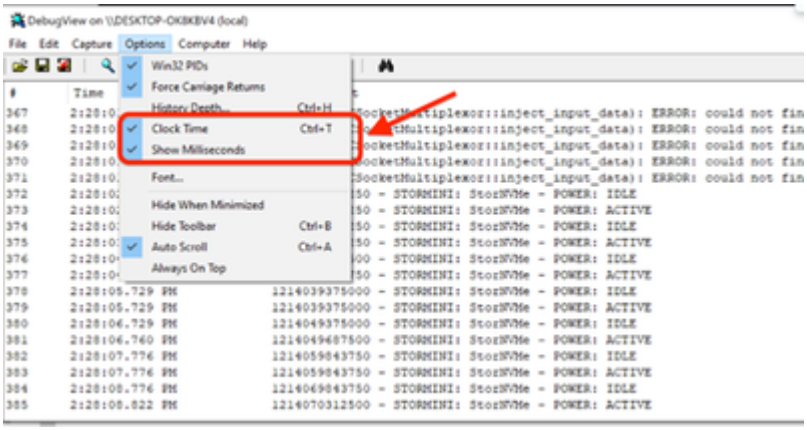
Windows

admin権限でCMDを開き、次のコマンドを実行します。

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

- SysInternalからDebugViewをダウンロードして、KDFログをキャプチャします
- DebugViewを管理者として実行し、次のメニューオプションを有効にします。
- Captureをクリックします
    - キャプチャカーネルのチェックマーク
    - チェックマーク冗長カーネル出力の有効化
- Options
    - クロック時間のチェックマーク
    - チェックマークShow Milliseconds

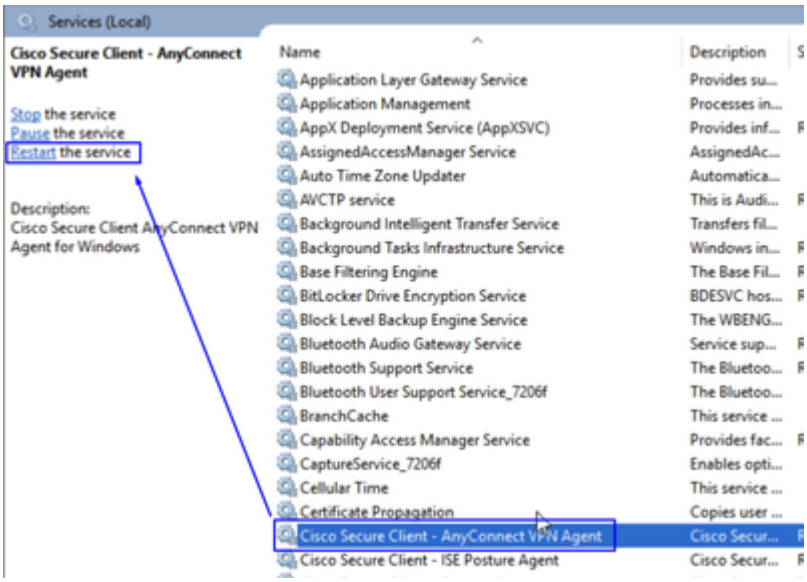




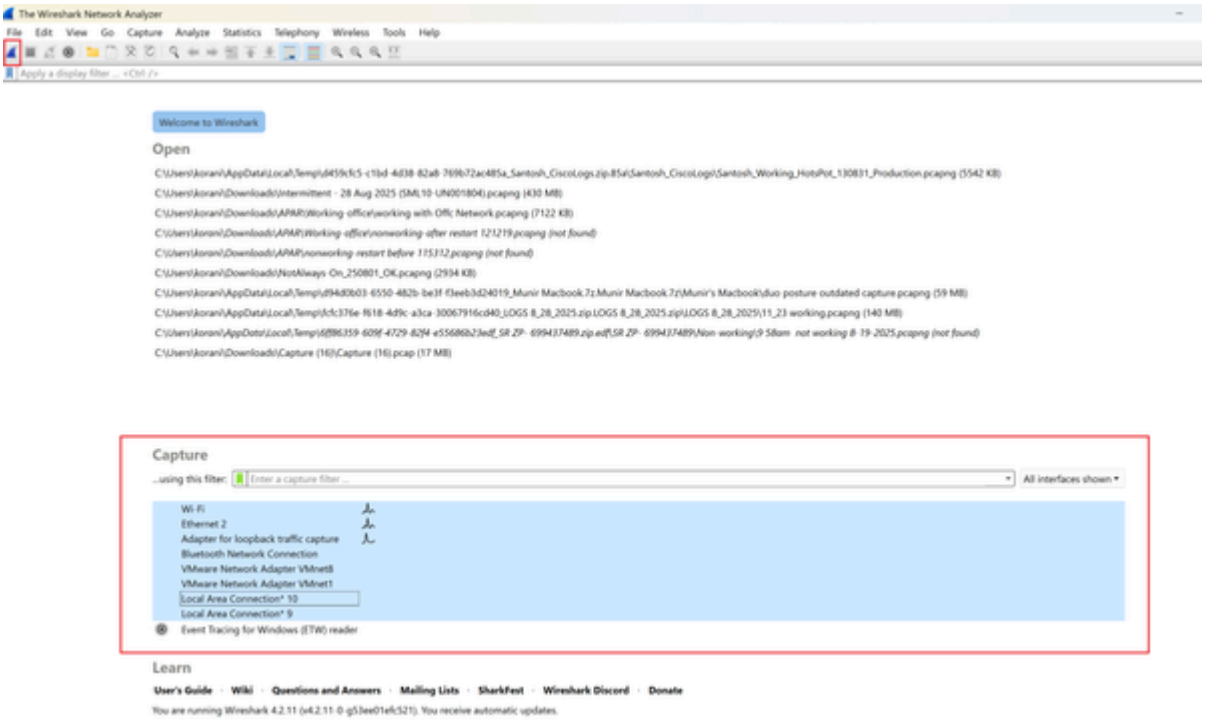
- 管理プロンプトでクライアントサービスを再起動します。

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

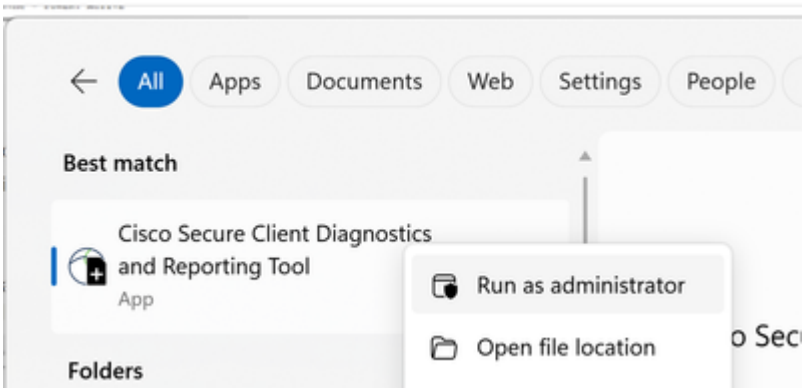
- net stop csc_vpnagent && net start csc_vpnagentが機能しない場合は、services.mscからCisco Secure Clientサービスを再起動します



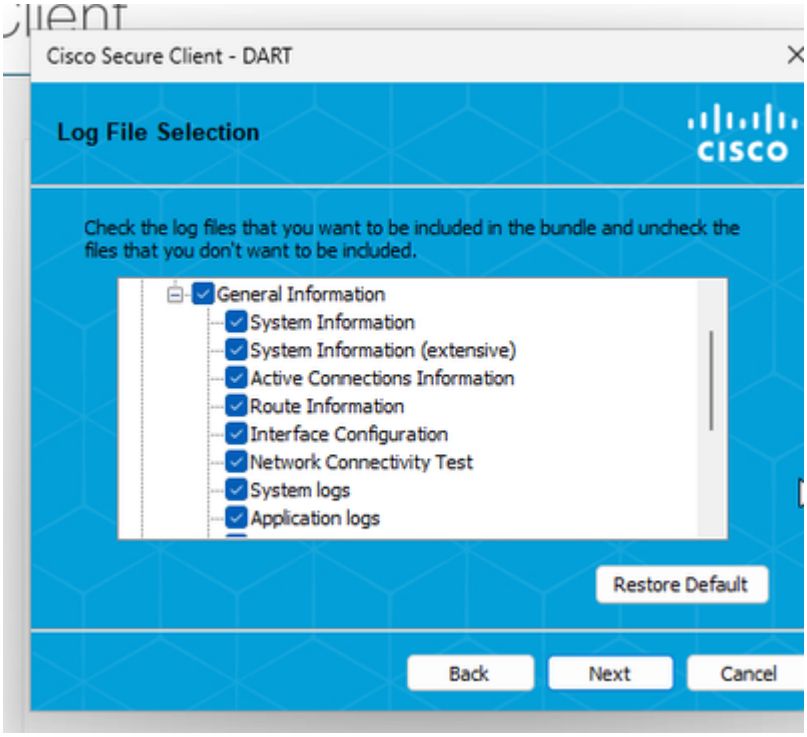
- Wiresharkキャプチャの開始
- すべてのインターフェイスを選択し、パケットキャプチャを開始します



- 問題を再現し、KDFログとWiresharkキャプチャを保存して、次にDARTバンドルをキャプチャする手順に従います
- 管理者権限でCisco Secure Client Diagnostics & Reporting Tool(DART)を開きます



- Customをクリックします。
  - システム情報の広範囲にわたるテストとネットワーク接続テストを含めます。



注：すべてのログ、KDFログ、Wiresharkキャプチャ、およびDARTバンドルをTACケースに収集してください。

- WindowsでKDFロギングを停止するには、次のコマンドを使用します。

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

MacOS

ターミナルを開き、次のコマンドチェーンに従ってMacOSでKDFロギングを有効にします。

- サービスの停止

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

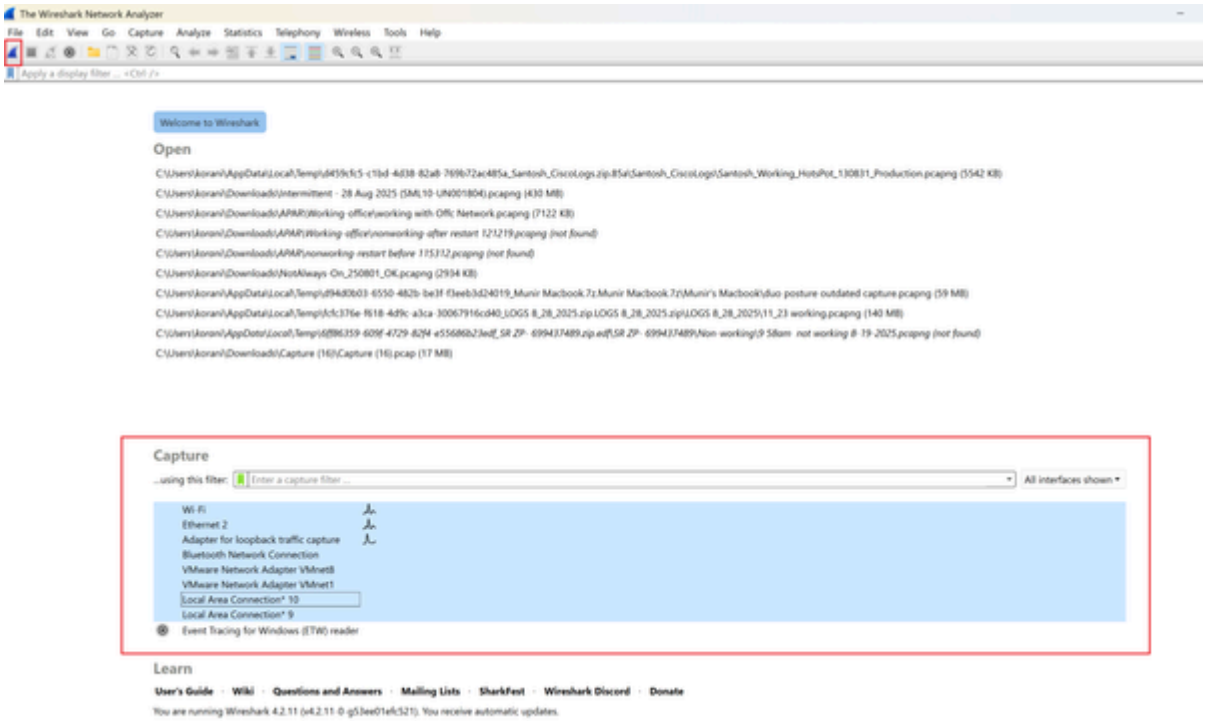
- フラグの有効化

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

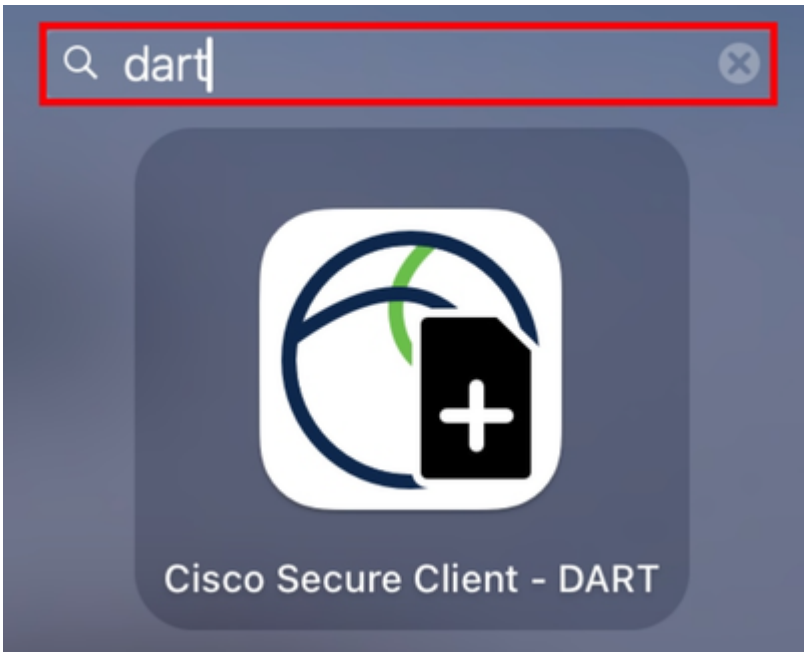
- サービスの開始

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

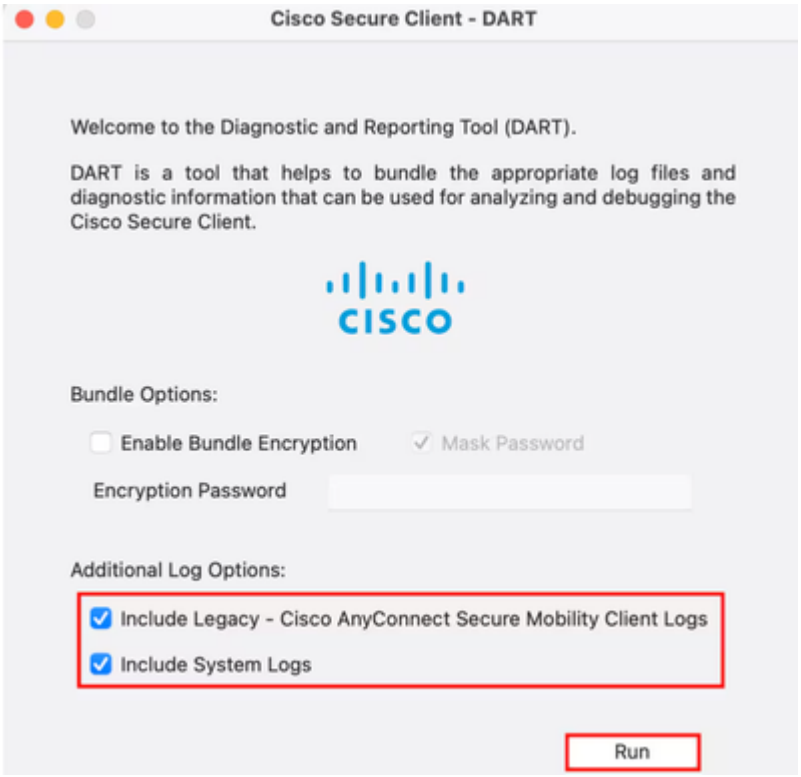
- Wiresharkキャプチャの開始
- すべてのインターフェイスを選択し、パケットキャプチャを開始します



- 問題を再現し、KDFログとWiresharkキャプチャを保存して、次にDARTバンドルをキャプチャする手順に従います
- Cisco Secure Client - DARTを開きます。



- 次のオプションにチェックマークを付けます。
  - レガシーを含める：Cisco AnyConnectセキュアモビリティクライアントログ
  - システムログを含める
- Runをクリックします。



注：すべてのログ、KDFログ、Wiresharkキャプチャ、およびDARTバンドルをTACケースに収集してください。

関連情報

- シスコのテクニカルサポートとダウンロード
- Cisco Secure Accessヘルプセンター
- Cisco SASE設計ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。