Coletando registros KDF para cliente seguro no Windows e MacOS

Contents

Introdução

Este documento descreve como coletar logs KDF e outros logs de solução de problemas importantes no Windows e MacOS.

SINALIZADORES Windows e MacOS

Relacionado ao DNS (quando o OpenDNS está envolvido):	0x20801FF
Proxy de fluxo da Web (SWG) e DNS relacionados:	0x70C01FF
ZTA	0x400080152

Coletando registros KDF, Wireshark e pacote DART

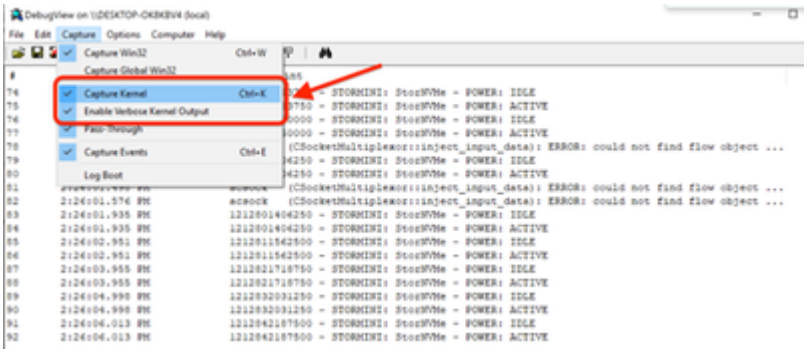
Note: Ao enviar os resultados, sempre informe à Equipe do TAC quais configurações foram usadas e esteja aberto a alterações, conforme exigido pelo TAC.

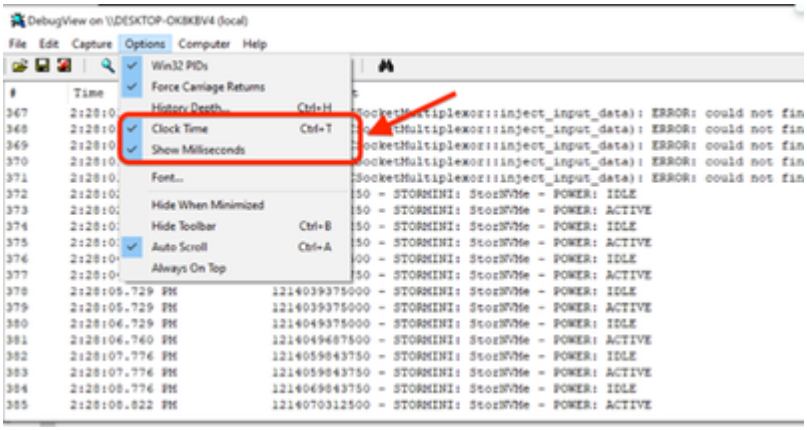
Windows

Abra um CMD com privilégios de administrador e execute o próximo comando:

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

- Baixe DebugView de SysInternal para capturar o log KDF
- Execute DebugView como administrator e ative as próximas opções de menu:
- Clique em Capture
    - Marca de seleção Capture Kernel
    - Marca de seleção Enable Verbose Kernel Output
- Opções
    - Marca de seleção Clock Time
    - Marca de seleção Show Milliseconds

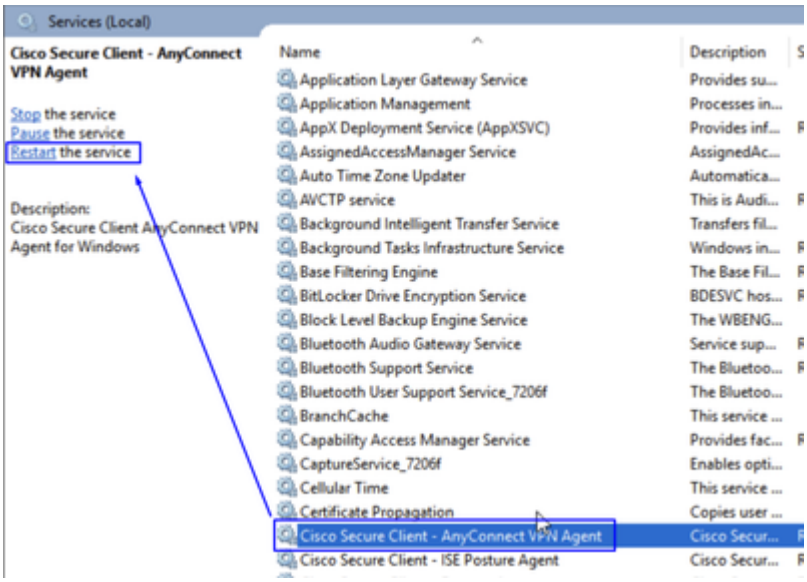




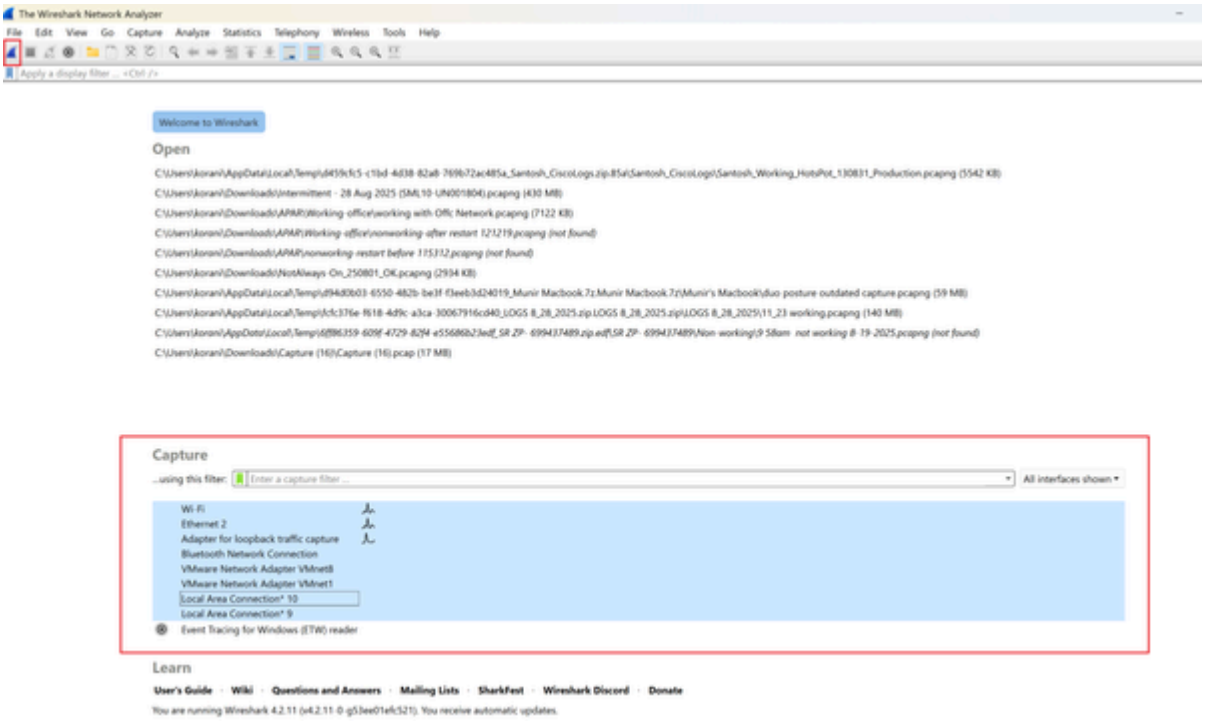
- Reinicie o serviço do cliente através do prompt do administrador:

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

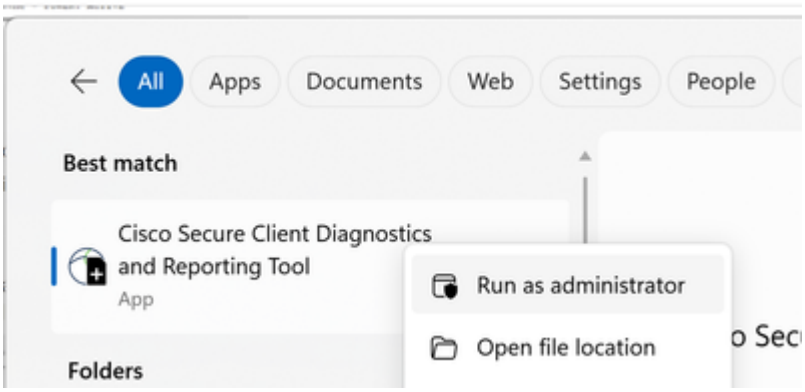
- Se net stop csc_vpnagent && net start csc_vpnagent não funcionar, reinicie Cisco Secure Client o serviço do services.msc



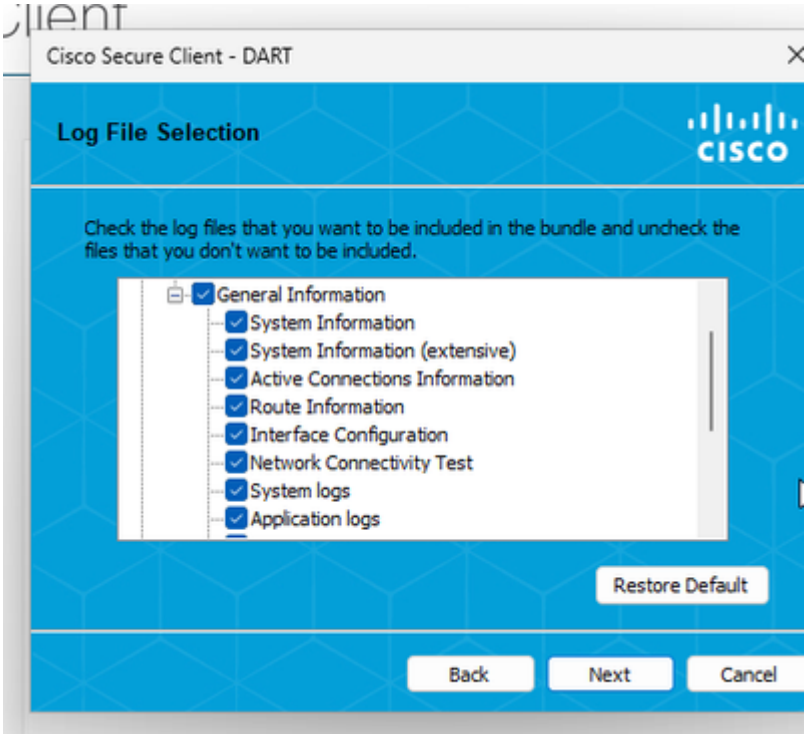
- Iniciar Wireshark Capture
- Selecione todas as interfaces e inicie a captura de pacotes



- Reproduza o problema e salve KDF Logs e Wireshark Capturee siga as etapas para capturar DART Bundle
- Abrir o Cisco Secure Client Diagnostics & Reporting Tool (DART) com privilégios de administrador



- Clique em Custom
  - Incluir System Information Extensive e Network Connectivity Test



Note: Colete todos os registros, registros KDF, captura do Wireshark e pacote DART no caso TAC.

- Para parar o registro KDF no Windows, use o próximo comando:

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

MacOS

Abra o terminal e siga a próxima cadeia de comandos para ativar o registro KDF no MacOS:

- Stop Service

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

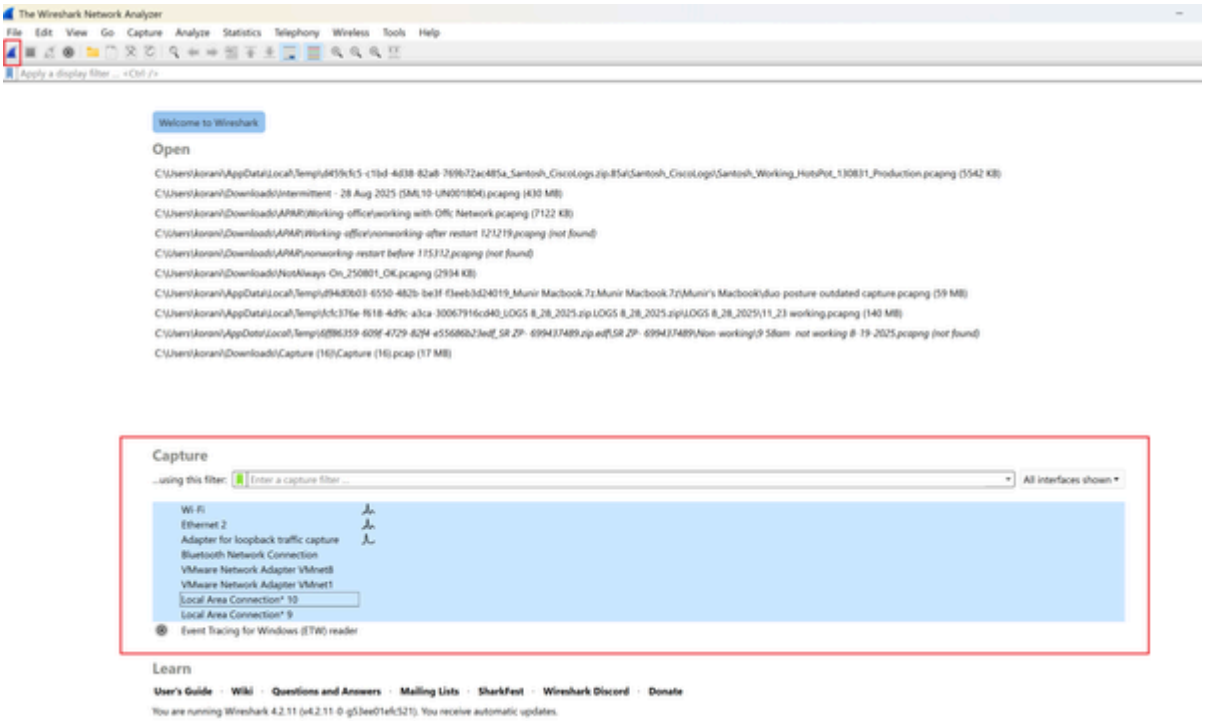
- Enable Flag

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

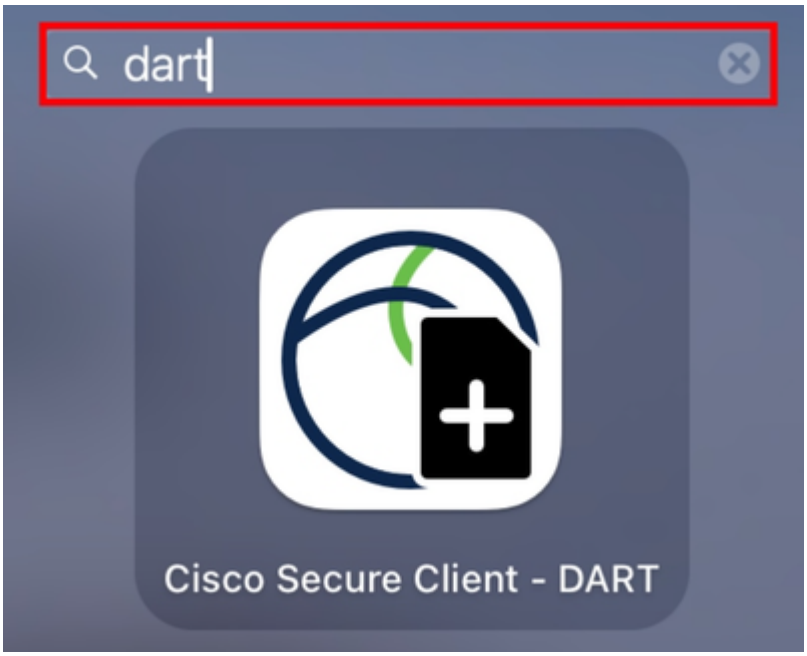
- Start Service

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

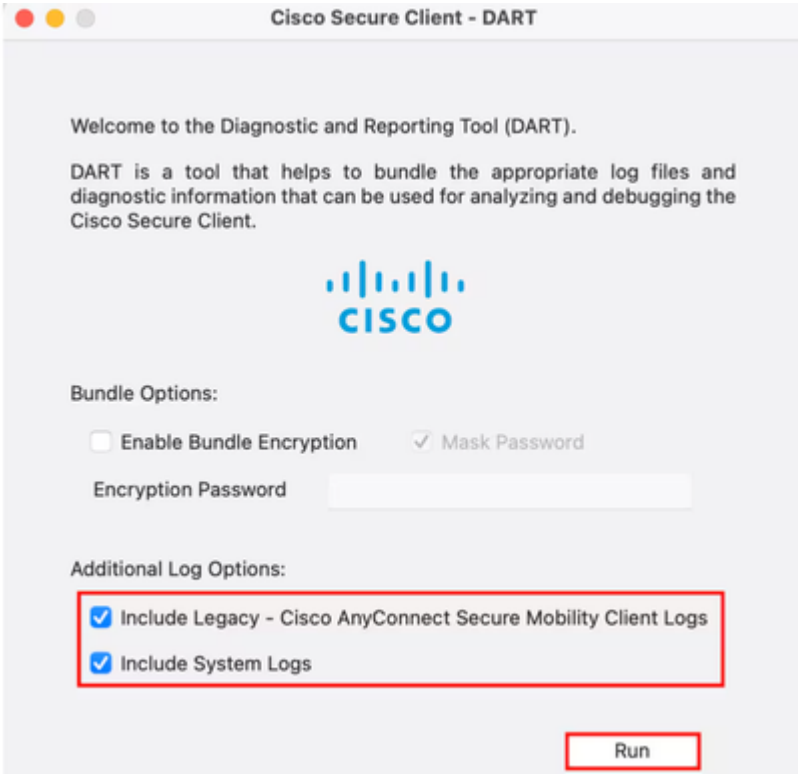
- Iniciar Wireshark Capture
- Selecione todas as interfaces e inicie a captura de pacotes



- Reproduza o problema e salve KDF Logs e Wireshark Capturee siga as etapas para capturar DART Bundle
- Abra o Cisco Secure Client - DART



- Marque as próximas opções:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- Clique em Run



Note: Colete todos os registros, registros KDF, captura do Wireshark e pacote DART no caso TAC.

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Central de ajuda do Cisco Secure Access
- Guia de design do Cisco SASE

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.