收集Windows和MacOS上安全客户端的KDF日志

目录

简介

本文档介绍如何收集Windows和MacOS上的KDF日志和其他重要故障排除日志。

Windows和MacOS标志

与DNS相关（涉及OpenDNS时）：	0x20801FF
Web流(SWG)代理和DNS相关：	0x70C01FF
ZTA	0x400080152

收集KDF日志、Wireshark和DART套件

注意：当您提交结果时，请务必让TAC团队知道使用了哪些设置，并可根据TAC的要求进行更改。

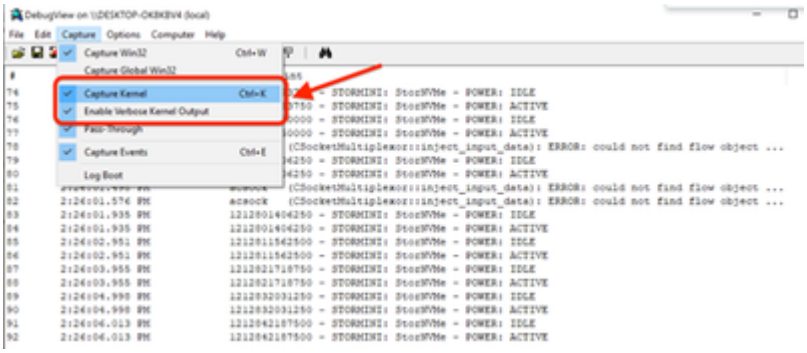
Windows 窗口版本

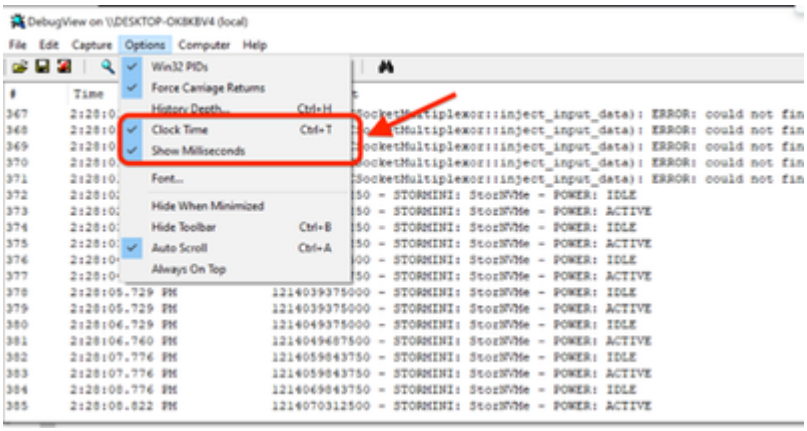
打开具有管理员权限的CMD并运行下一个命令：

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

- 从SysInternal下载DebugView以捕获KDF日志
- 运行DebugViewadministrator 并启用下一个菜单选项：
- 单击Capture（捕获）

    - 复选标记 Capture Kernel
    - 复选标记 Enable Verbose Kernel Output
- 选项
    - 复选标记 Clock Time
    - 复选标记 Show Milliseconds

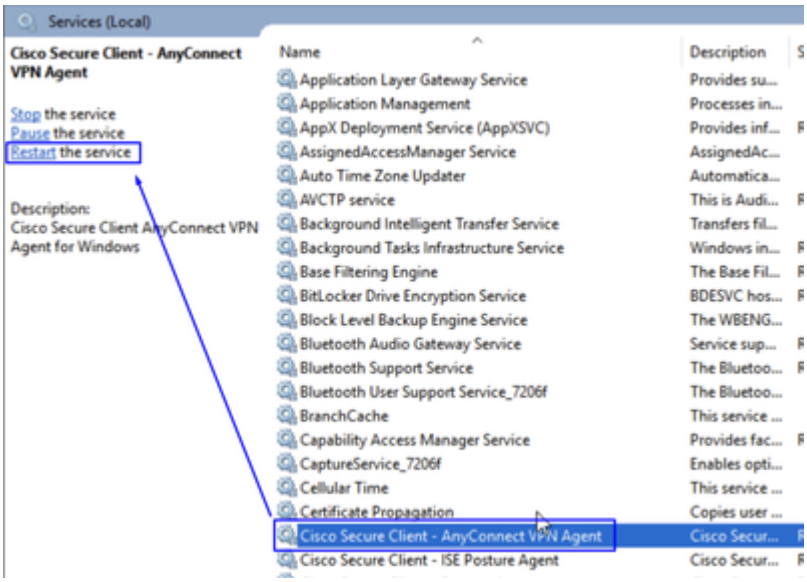




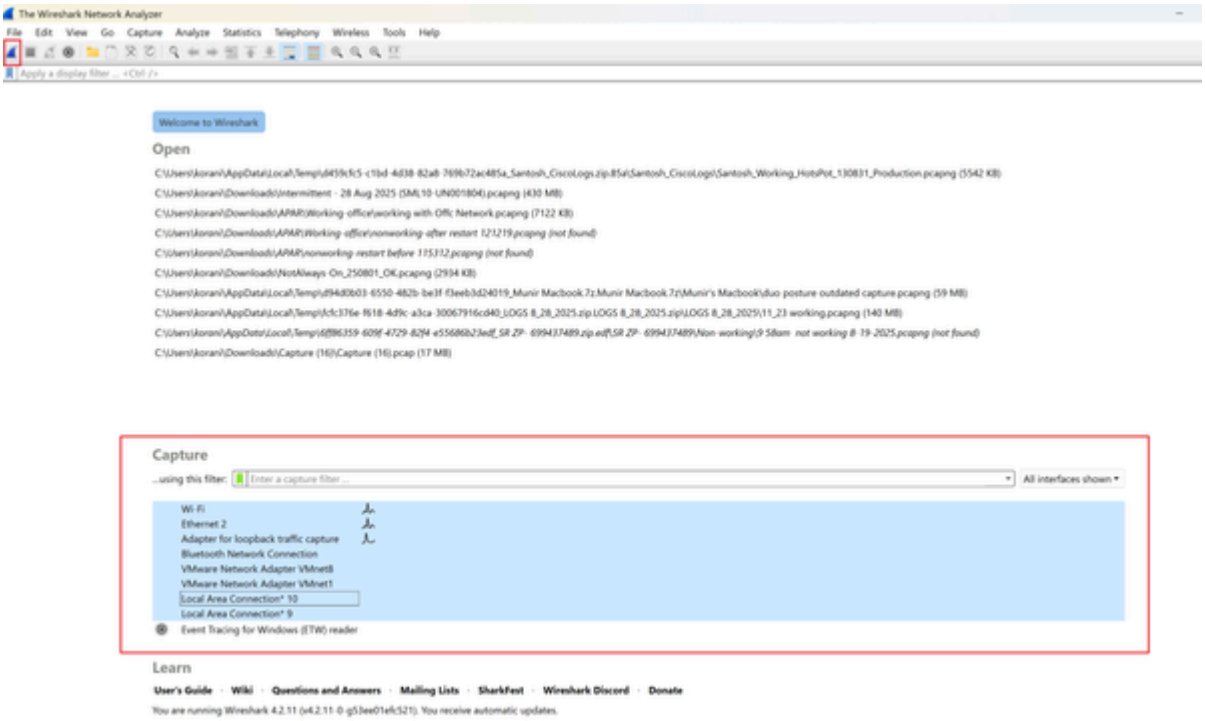
- 通过管理员提示重新启动客户端服务：

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

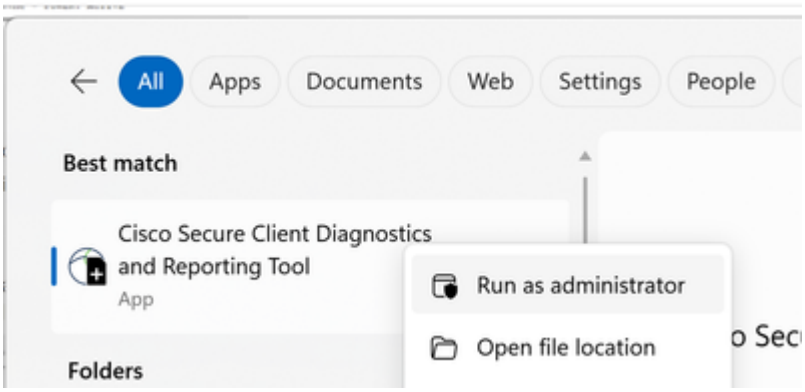
- 如果net stop csc_vpnagent && net start csc_vpnagent不起作用，请从servicesCisco Secure Client.msc重新启动服务



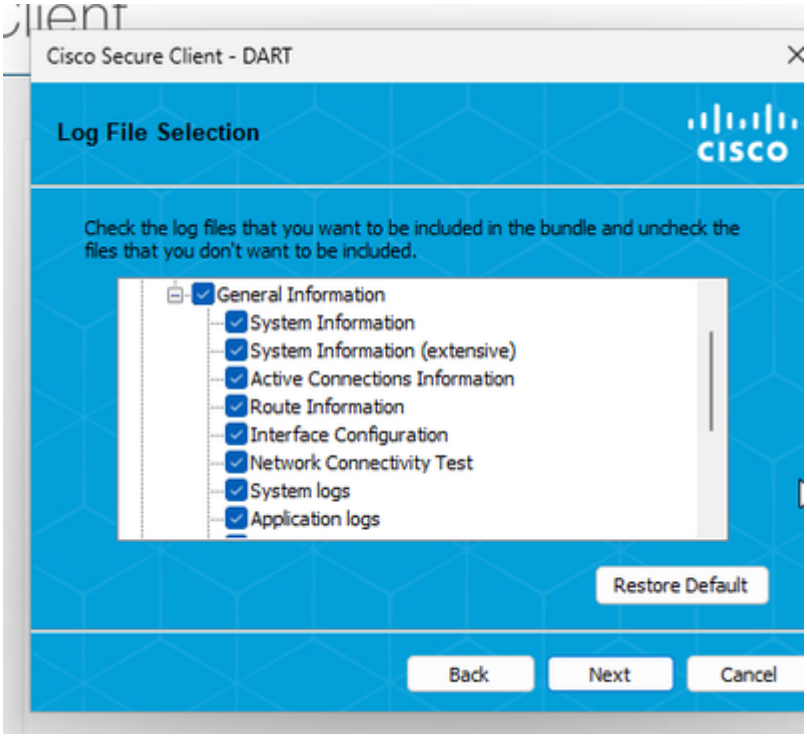
- 开始 Wireshark Capture
- 选择所有接口，然后开始数据包捕获



- 重现问题，然后保存KDF Logs和Wireshark Capture，然后按照步骤进行捕获 DART Bundle
- 以管理员权限打开Cisco Secure Client Diagnostics & Reporting Tool (DART)



- 点击 Custom
  - 包括System Information Extensive和 Network Connectivity Test



注意：将所有日志、KDF日志、Wireshark捕获和DART捆绑包收集到TAC案例。

- 要停止Windows上的KDF日志记录，请使用以下命令：

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

MacOS

打开terminal，然后按照下一个命令链在MacOS上启用KDF日志记录：

- Stop Service

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

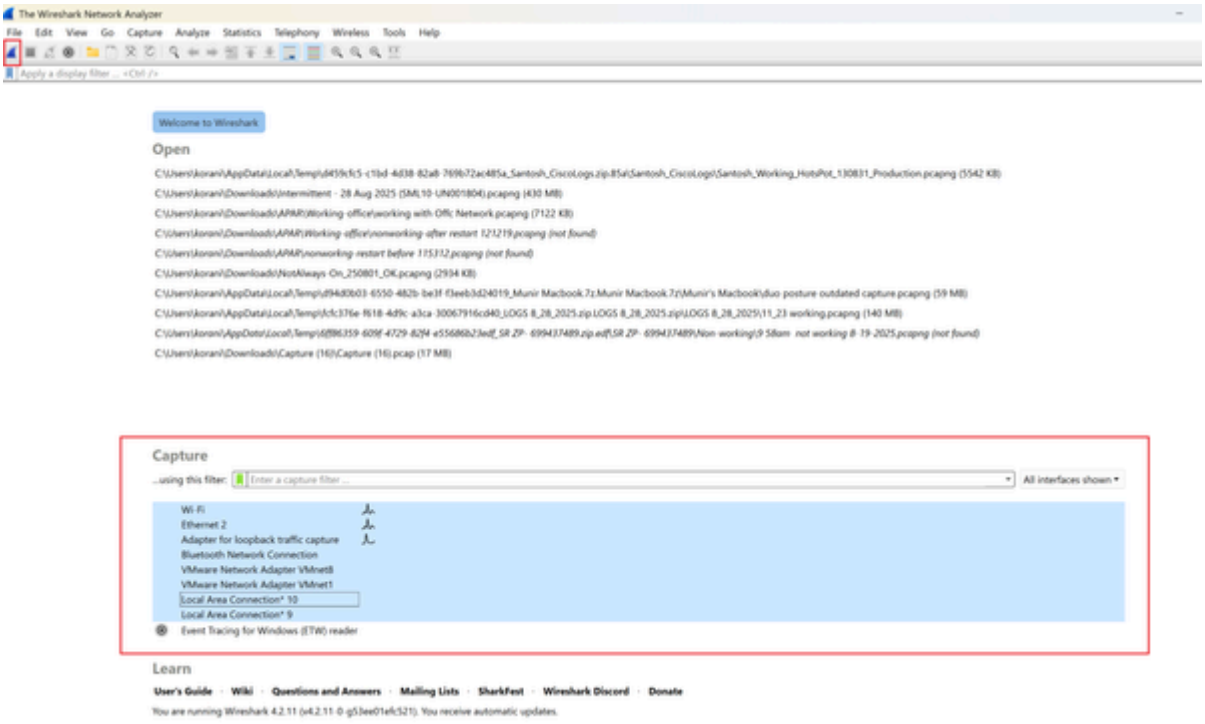
- Enable Flag

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

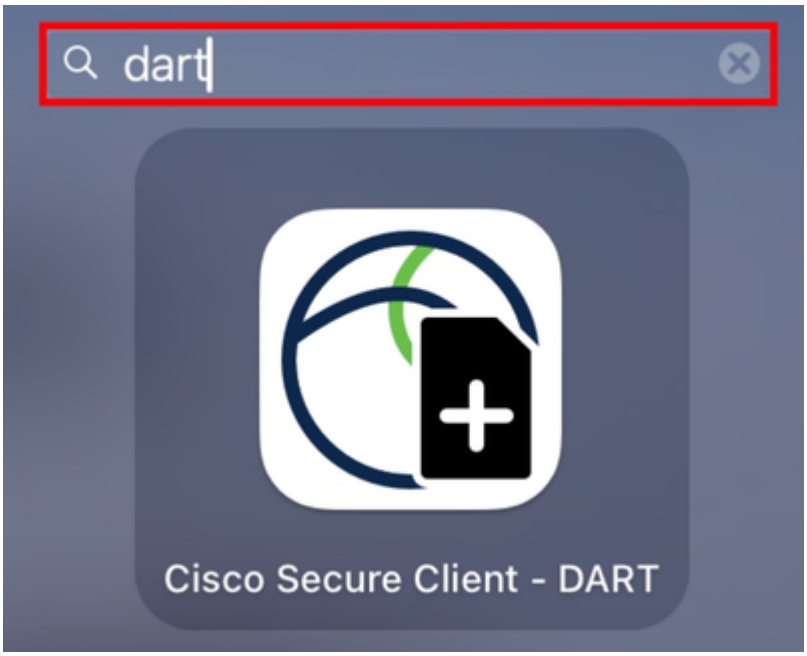
- Start Service

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

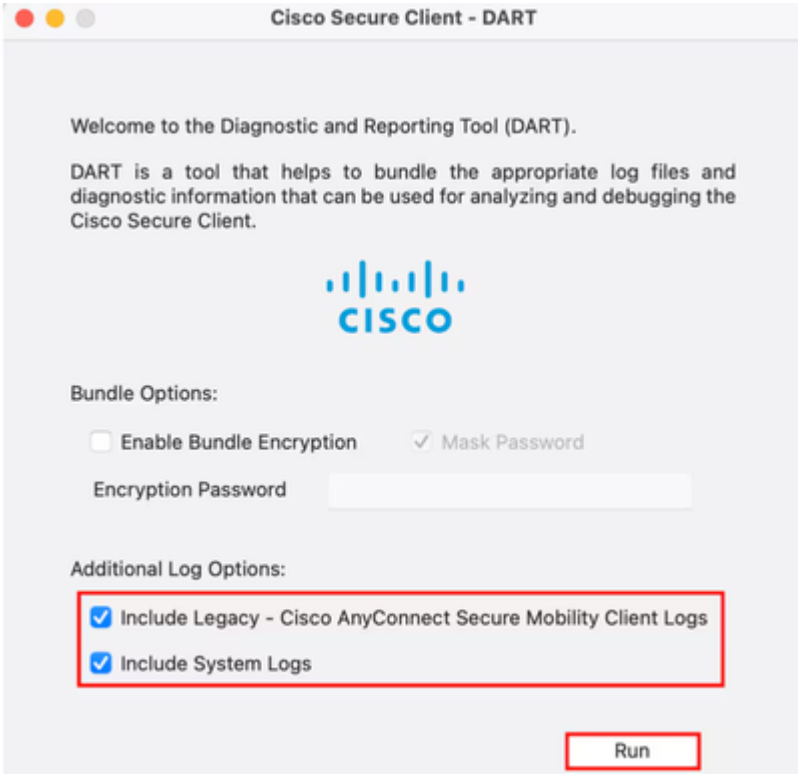
- 开始 Wireshark Capture
- 选择所有接口，然后开始数据包捕获



- 重现问题，然后保存KDF Logs和Wireshark Capture，然后按照步骤进行捕获 DART Bundle
- 打开 Cisco Secure Client - DART



- 选中下一个选项：
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- 点击 Run



注意：将所有日志、KDF日志、Wireshark捕获和DART捆绑包收集到TAC案例。

相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- Cisco SASE设计指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。