配置ZTNA日志记录以进行故障排除

目录

简介

背景信息

收集日志

- 在创建TAC支持请求之前进行预检查
- 要收集的日志
- 启用ZTNA调试跟踪模式
- 在事件查看器中增加ZTA日志大小
  - Windows 窗口版本
  - MacOS
- 启用KDF日志记录、数据包捕获、双调试模式和Dart套件
  - Windows 窗口版本
  - 要启用和禁用的Windows Powershell命令，必须作为管理员运行：
  - MacOS

相关信息

简介

本文档介绍如何收集详细的ZTA故障排除日志以及何时逐步启用。

背景信息

随着组织越来越多地采用零信任架构(ZTA)来保护用户、设备和应用，对连接和策略实施问题进行故障排除变得越来越复杂。与传统基于边界的模型不同，ZTA依赖于跨身份、设备状态、网络环境和基于云的策略引擎的多项实时决策。出现问题时，高级日志通常不足以查明根本原因。

收集详细的ZTA级别跟踪对于深入了解客户端行为、策略评估、流量拦截和云服务交互至关重要。这些跟踪使工程师能够超越基于症状的故障排除，分析导致访问故障、性能下降或意外策略结果的事件确切顺序。

收集日志

在创建TAC支持请求之前进行预检查

这些预检查可帮助TAC团队更有效地识别问题。向工程师提供此信息有助于他们尽快解决您的问题：

- 问题出在哪里？有多少用户受到影响？
- 哪些操作系统和版本会受到影响？
- 问题是否持续或间断？如果是间歇性的，它是用户专用还是广泛的？
- 问题是在更改后开始的，还是在部署后一直存在？
- 有什么已知的触发因素吗？
- 是否有可用的变通方法？

要收集的日志

- DART套件
- ZTNA调试跟踪模式日志
- Wireshark捕获（所有接口，包括环回）
- 观察到的错误消息
- 问题的时间戳
- CSC ZTA模块状态屏幕截图
- 受影响用户的用户名

以下各节介绍如何启用和收集每个日志的详细信息。

启用ZTNA调试跟踪模式

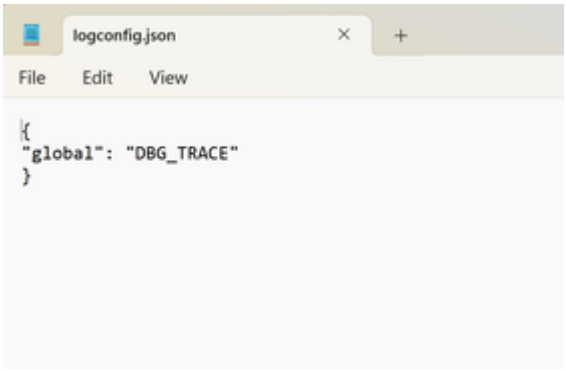
创建名为logconfig.json、具有以下详细信息的文件：

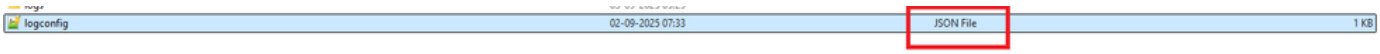
```
{ "global": "DBG_TRACE" }
```

警告：确保使用名称保存您的文件logconfig.json。

创建文件后，根据操作系统将其放置在适当的位置：

- Windows 窗口版本: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS：/opt/cisco/secureclient/zta





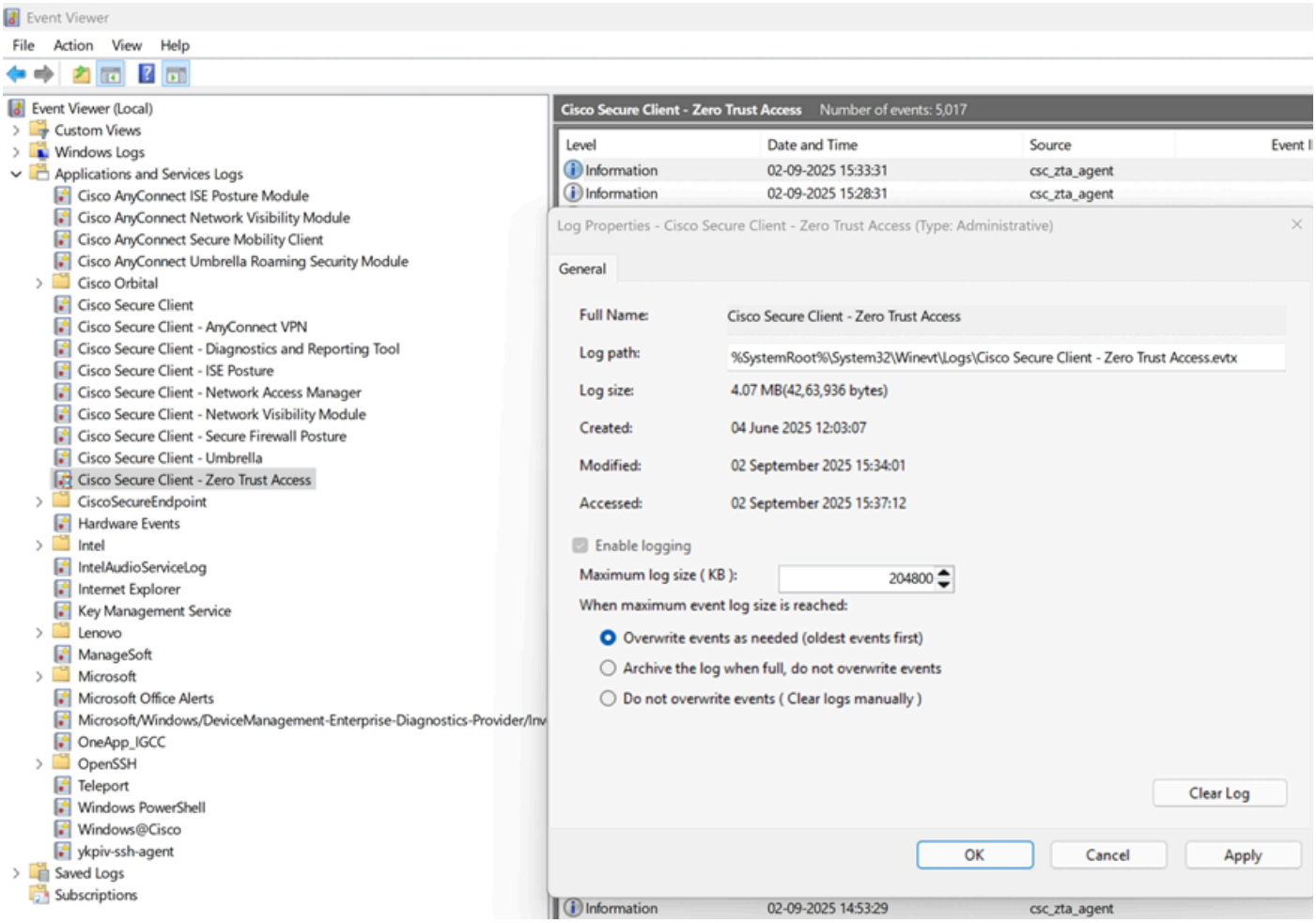
注意：创建指定文件后，必须重新启动零信任访问代理服务(请检查步骤重新启动ZTA服务)。 如果无法重新启动服务，请重新启动计算机。

在事件查看器中增加ZTA日志大小

在Windows PC上，启用跟踪级别日志记录后，必须手动增加ZTA日志文件大小。

1. 打开Event Viewer。
2. 在左侧窗格中，展开Applications and Services Logs。
3. 右键单击Cisco Secure Client – Zero Trust Access，然后选择Properties。
4. 在Maximum log size (KB)下，将值设置为204800（相当于200 MB）。

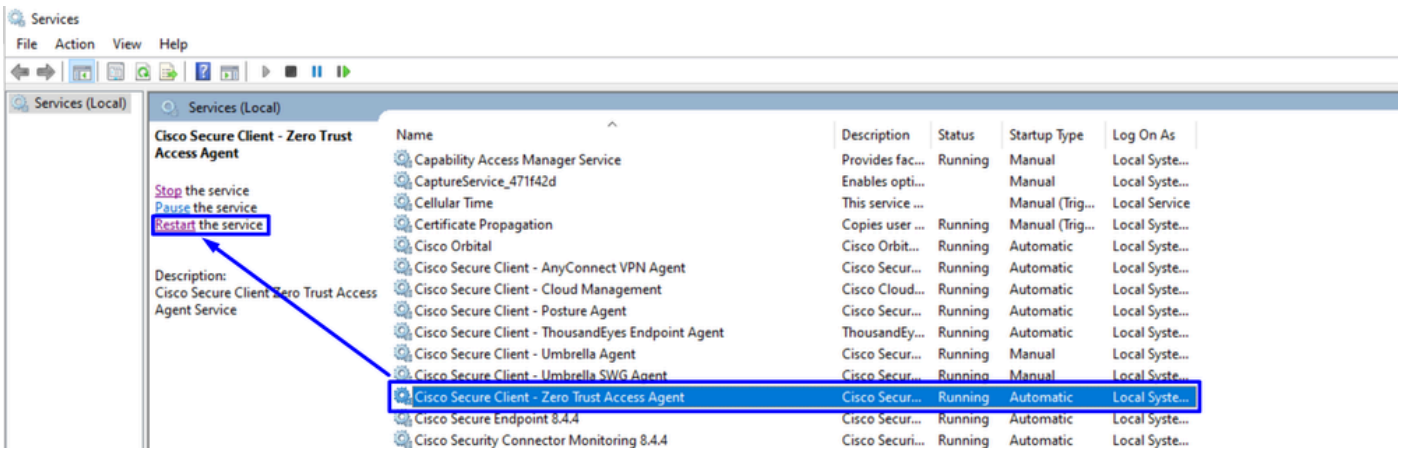
要最终确定，请**Apply**单击，然后OK。



重新启动ZTA服务

Windows 窗口版本

- 使Windows + R用打开Run Search writeservices.msc ，然后按enter。
- 找到服务Cisco Secure Client - Zero trust Access Agent ，然后单击Restart。完成后，请验证CSC ZTA模块状态以确认其处于活动状态。



注意：如果由于缺少管理访问权限而无法重新启动ZTA服务，则下一个选项是完整系统重新启动。

MacOS

Stop Service.

```
sudo "/opt/cisco/secureclient/zta/bin/Cisco Secure Client - Zero Trust Access.app/Contents/MacOS/Cisco
```

Start Service.

```
open -a "/opt/cisco/secureclient/zta/bin/Cisco Secure Client - Zero Trust Access.app"
```

注意：如果命令无法执行，或由于缺少管理访问权限而无法重新启动ZTA服务，则下一个选项是完整系统重新启动。

启用KDF日志记录、数据包捕获、双调试模式和Dart套件

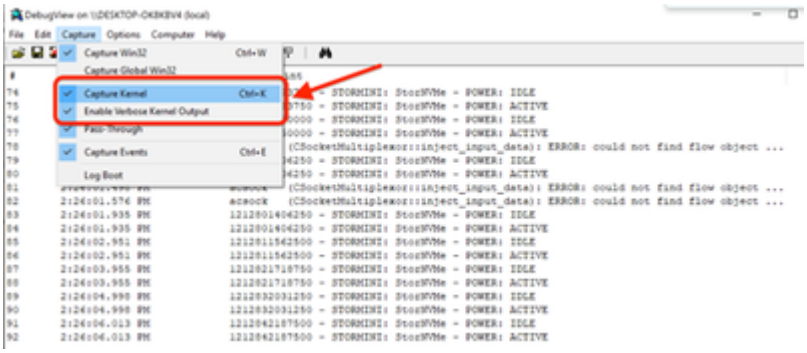
Windows 窗口版本

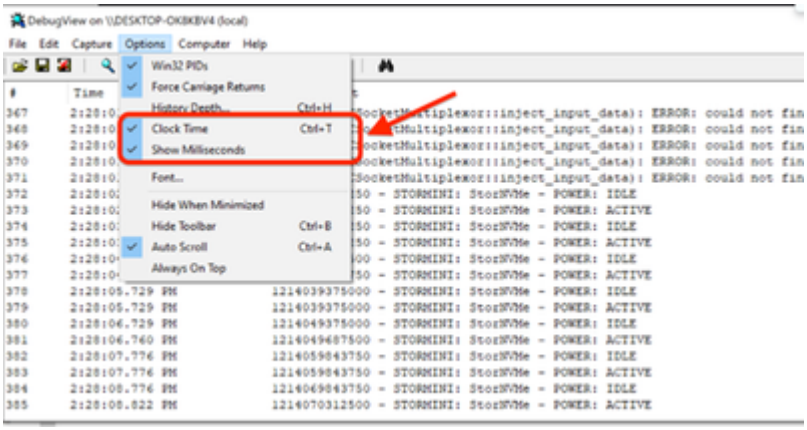
打开具有管理员权限的CMD，然后运行下一个命令：

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x400080152
```

- 从SysInternal下载DebugView以捕获KDF日志。
- 运行asDebugViewadministrator并启用下一个菜单选项：
- 点击Capture。
  - 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.

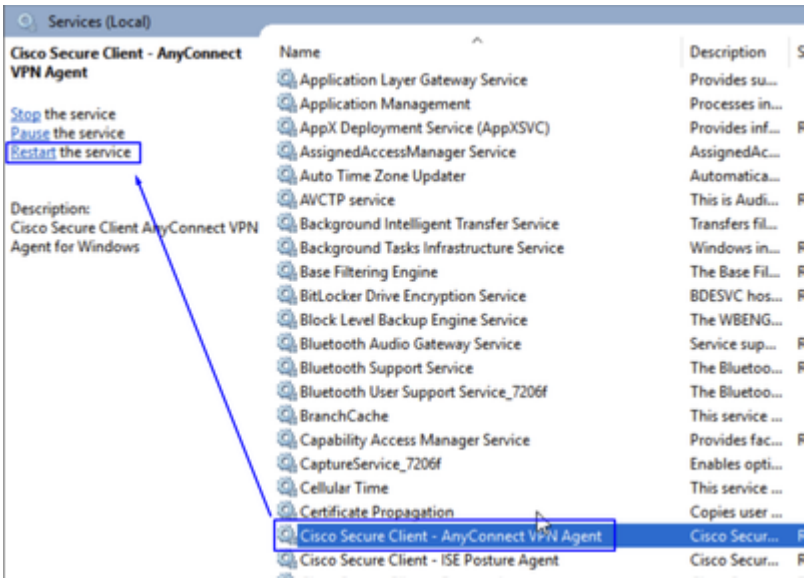




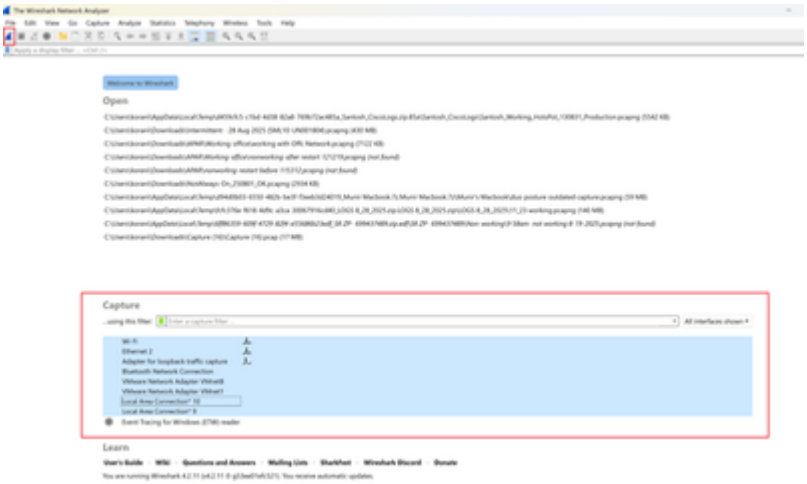
- 通过管理员提示重新启动客户端服务：

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

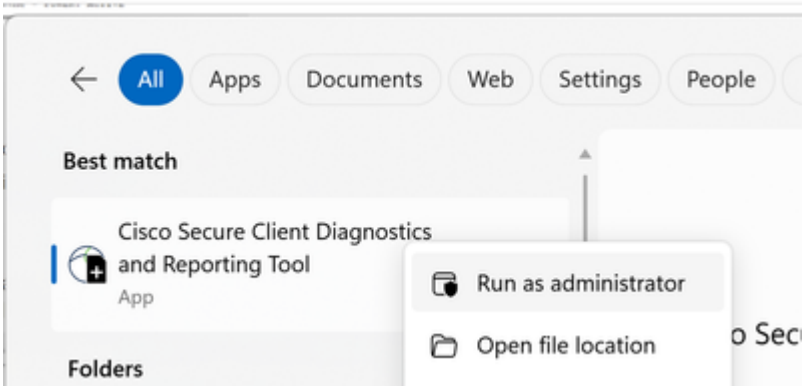
- 如果net stop csc_vpnagent && net start csc_vpnagent不起作用，请从Cisco Secure Clientservices.msc重新启动服务。



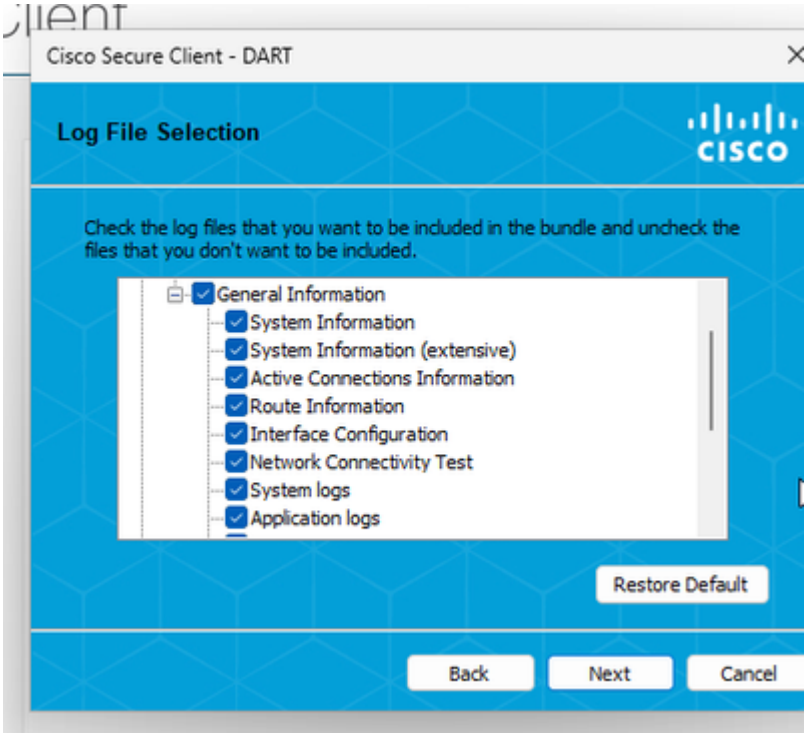
- 在调[试模式下启用Duo](#)
- 开始 Wireshark Capture.
- 选择所有接口，然后开始数据包捕获。



- 重现问题，保存并KDF LogsWireshark Capture按照步骤进行捕获 DART Bundle.
- 以管理员Cisco Secure Client Diagnostics & Reporting Tool (DART)权限打开。



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



- 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
```

注意：收集所有日志：KDF日志、Wireshark捕获和DART捆绑包到TAC案例。

要启用和禁用的Windows Powershell命令，必须作为管理员运行：

```
#Enable ZTNA Logs
New-Item -Path "C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logconfig.json" -ItemType "file" -Value '{
Limit-EventLog -LogName "Cisco Secure Client - Zero Trust Access" -MaximumSize 2240000KB
& "C:\Program Files (x86)\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x400080152
Restart-Service csc_vpnagent
Restart-Service csc_zta_agent

#Disable ZTNA Logs
Remove-Item -Path "C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logconfig.json"
Limit-EventLog -LogName "Cisco Secure Client - Zero Trust Access" -MaximumSize 6400KB
& "C:\Program Files (x86)\Cisco\Cisco Secure Client\acsocktool.exe" -cdf 0x400080152
Restart-Service csc_vpnagent
Restart-Service csc_zta_agent
```

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.

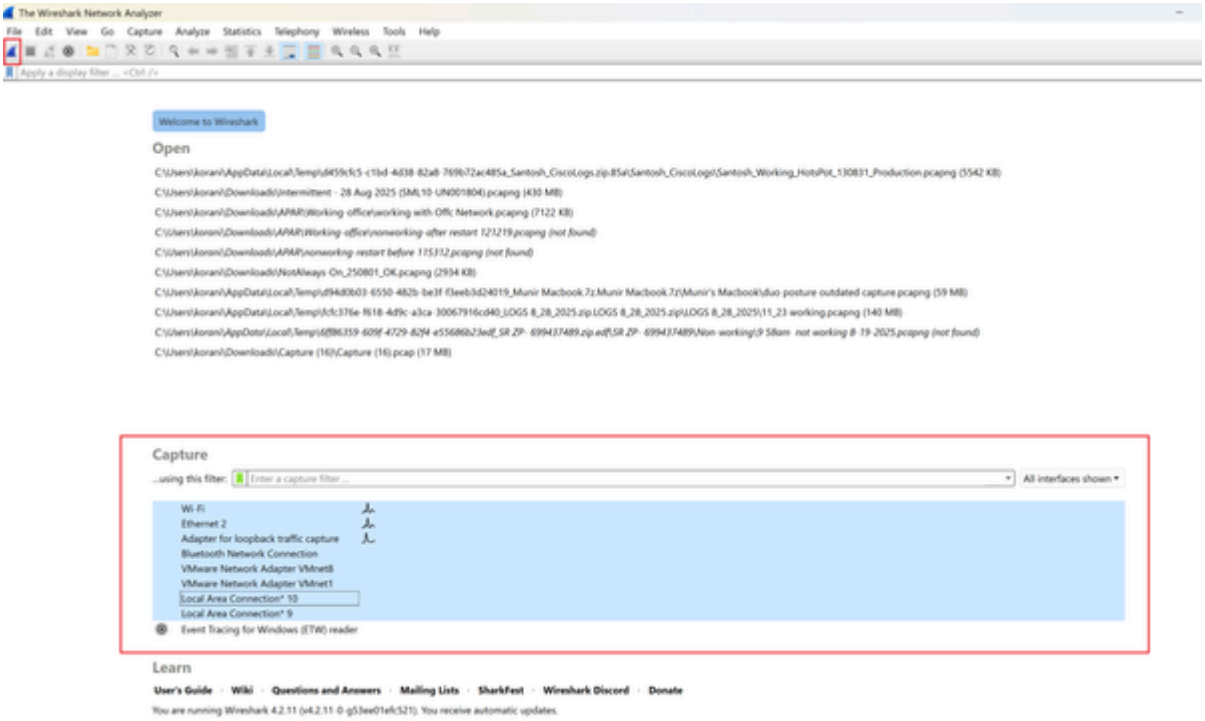
```
echo debug=0x400080152 | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

- Start Service.

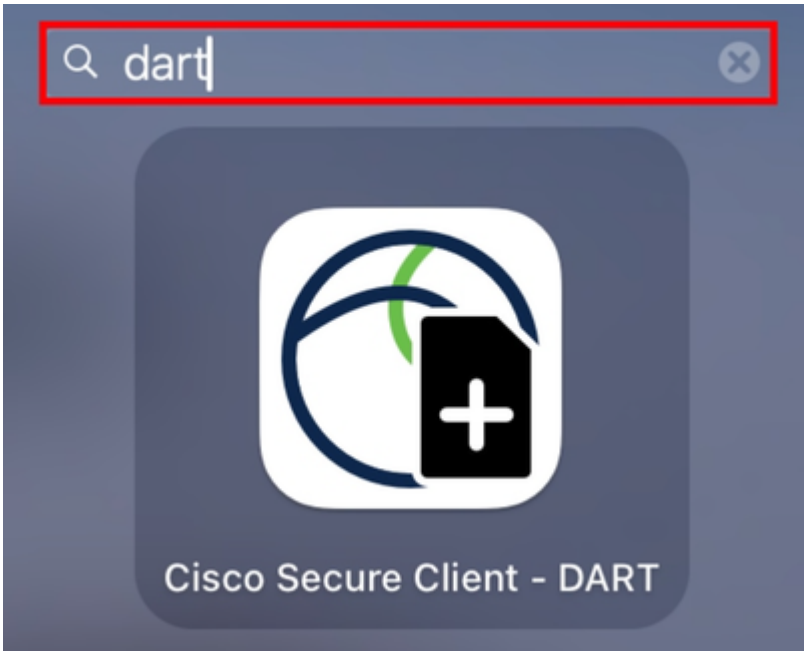
```
open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

- 在Debug模式下启用Duo。
- 开始 Wireshark Capture.

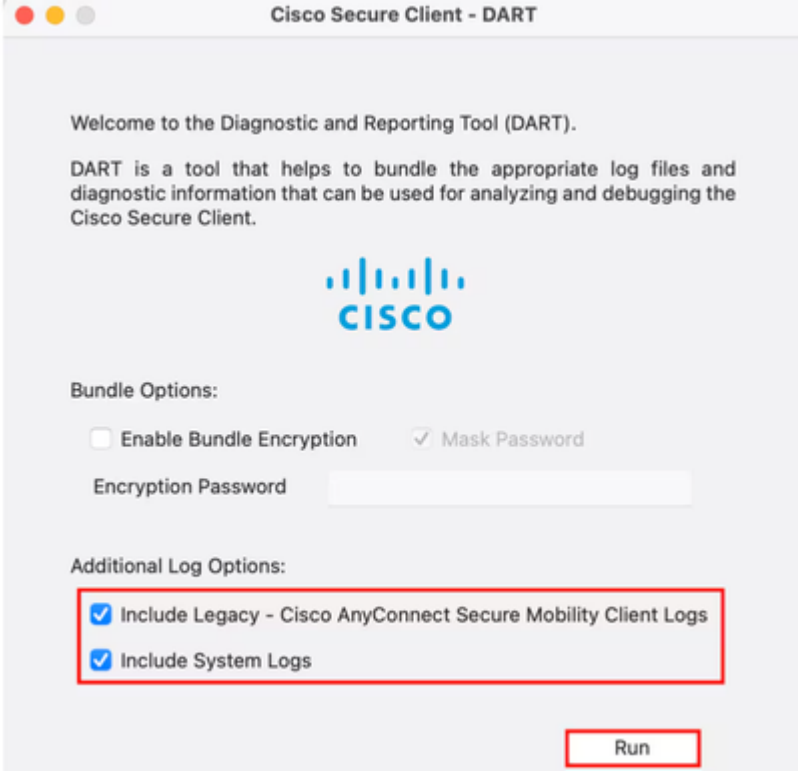
- 选择所有接口，然后开始数据包捕获。



- 重现问题，保存并KDF LogsWireshark Capture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：收集所有日志：KDF日志、Wireshark捕获和DART捆绑包到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
- 收集Windows和MacOS上安全客户端的KDF日志

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）。