Sammeln detaillierter ZTNA-Protokolle zur Fehlerbehebung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie detaillierte ZTA-Fehlerbehebungsprotokolle gesammelt werden, wann diese aktiviert werden müssen und welche Schritte Schritt für Schritt durchzuführen sind.

Hintergrundinformationen

Mit der zunehmenden Einführung der Zero Trust Architecture (ZTA) zum Schutz von Benutzern, Geräten und Anwendungen wird die Fehlerbehebung bei Verbindungs- und Richtliniendurchsetzungsproblemen immer komplexer. Im Gegensatz zu herkömmlichen Perimeter-basierten Modellen beruht ZTA auf mehreren Echtzeitentscheidungen zu Identität, Gerätestatus, Netzwerkkontext und Cloud-basierten Richtlinien-Engines. Wenn Probleme auftreten, reichen allgemeine Protokolle häufig nicht aus, um die Ursache zu bestimmen.

Die detaillierte Verfolgung auf ZTA-Ebene spielt eine wichtige Rolle, wenn es darum geht, umfassende Transparenz in Bezug auf das Client-Verhalten, die Richtlinienauswertung, das Abfangen von Datenverkehr und die Interaktionen mit Cloud-Services zu erhalten. Mithilfe dieser Traces können die Techniker über die symptombasierte Fehlerbehebung hinausgehen und die genaue Abfolge der Ereignisse analysieren, die zu Zugriffsfehlern, Leistungseinbußen oder unerwarteten Richtlinienergebnissen führen.

Protokolle werden gesammelt

Vorabprüfung vor dem Öffnen eines TAC-Tickets

Diese Vorprüfungen werden dem TAC-Team helfen, das Problem effizienter zu identifizieren. Die Bereitstellung dieser Informationen hilft den Technikern dabei, Ihr Problem so schnell wie möglich zu lösen:

- Worum handelt es sich, und wie viele Benutzer sind betroffen?
- Welches Betriebssystem und welche Versionen sind betroffen?
- Besteht ein konsistentes oder zeitweiliges Problem? Wenn unregelmäßig, ist sie benutzerspezifisch oder weit verbreitet?
- Hat das Problem nach einer Änderung begonnen oder ist es seit der Bereitstellung aufgetreten?
- Gibt es bekannte Auslöser?
- Gibt es eine Problemumgehung?

Zu erfassende Protokolle

- DART-Paket
- Protokolle des ZTNA-Debug-Ablaufverfolgungsmodus
- Erfassung von Wireshark (alle Schnittstellen, einschließlich Loopback)
- Fehlermeldungen
- Zeitstempel der Ausgabe
- Statusbildschirm des CSC ZTA-Moduls
- Benutzername des betroffenen Benutzers

In den folgenden Abschnitten wird detailliert erläutert, wie diese Protokolle aktiviert und erfasst werden.

ZTNA Debug Trace-Modus aktivieren

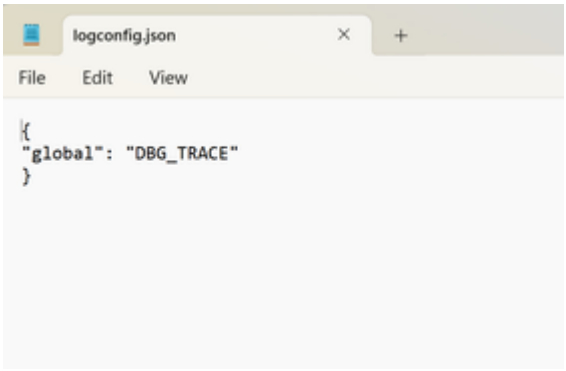
Erstellen Sie eine Datei mit dem Namen `logconfig.json` und den folgenden Details:

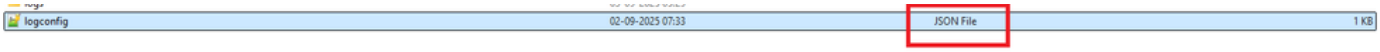
```
{ "global": "DBG_TRACE" }
```

Warnung: Stellen Sie sicher, dass Ihre Datei mit dem Namen logconfig.jsongespeichert wird.

Nachdem Sie die Datei erstellt haben, legen Sie sie je nach Betriebssystem am entsprechenden Speicherort ab:

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- MacOS:/opt/cisco/secureclient/zta





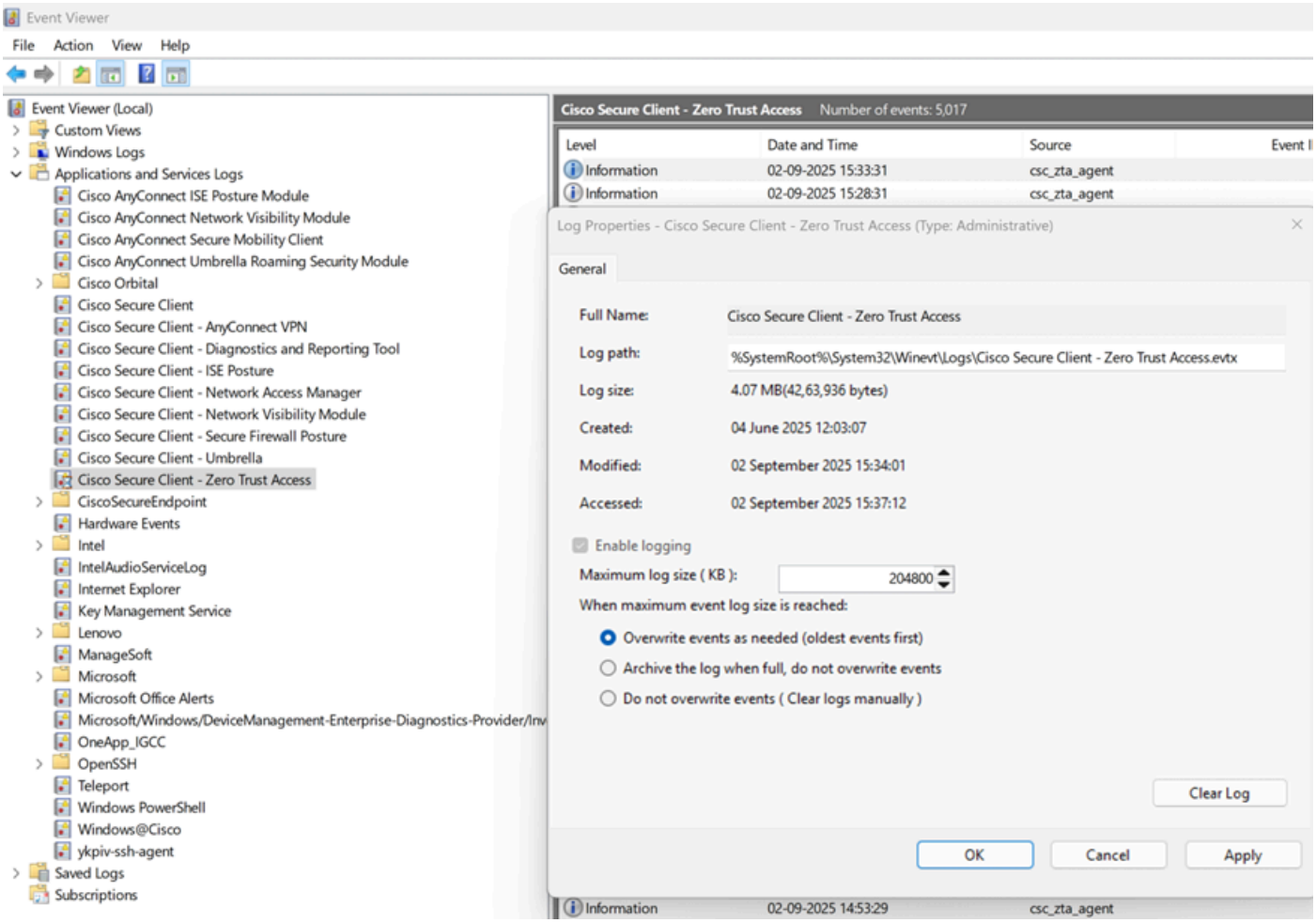
Anmerkung: Nachdem Sie die angegebene Datei erstellt haben, müssen Sie den Zero Trust Access Agent-Dienst neu starten (überprüfen Sie den Schritt ZTA-Dienst neu starten). Wenn ein Neustart des Dienstes nicht möglich ist, starten Sie den Computer neu.

Erhöhen der **ZTA-Protokollgröße in der Ereignisanzeige**

Auf Windows-PCs müssen Sie nach dem Aktivieren der Protokollierung auf Ablaufverfolgungsebene die Größe der ZTA-Protokolldatei manuell erhöhen.

1. Offen.Event Viewer
2. Erweitern Sie im linken Bereich die Option Applications and Services Logs.
3. Klicken Sie mit der rechten MaustasteCisco Secure Client – Zero Trust Access, und wählen Sie Properties.
4. Setzen Sie den Wert unter Maximum log size (KB)auf (entspricht 200 MB).204800

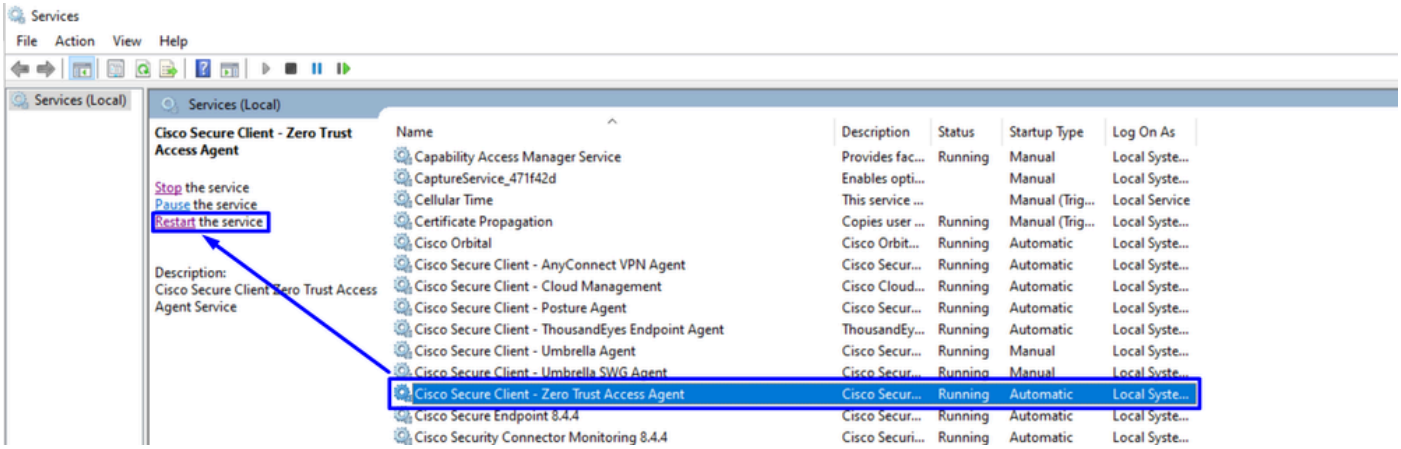
Klicken Sie zum Abschluss auf **Apply** und dann OK.



ZTA-Dienst wird neu gestartet

Windows

- Öffnen SieWindows + Rden Run Search Schreibvorgang services.msc, und drücken Sie die Eingabetaste.
- Suchen Sie den Dienst Cisco Secure Client - Zero trust Access Agent , und klicken Sie auf Restart. Überprüfen Sie anschließend den Status des CSC ZTA-Moduls, um zu bestätigen, dass es aktiv ist.



Anmerkung: Wenn der ZTA-Dienst aufgrund eines fehlenden administrativen Zugriffs nicht neu gestartet werden kann, ist ein vollständiger Systemneustart die nächste Option.

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"
```

Anmerkung: Wenn Befehle nicht ausgeführt werden können oder der ZTA-Dienst aufgrund eines fehlenden administrativen Zugriffs nicht neu gestartet werden kann, ist ein vollständiger Systemneustart die nächste Option.

KDF-Protokollierung, Paketerfassung, Duo-Debugmodus und DART-Paket aktivieren

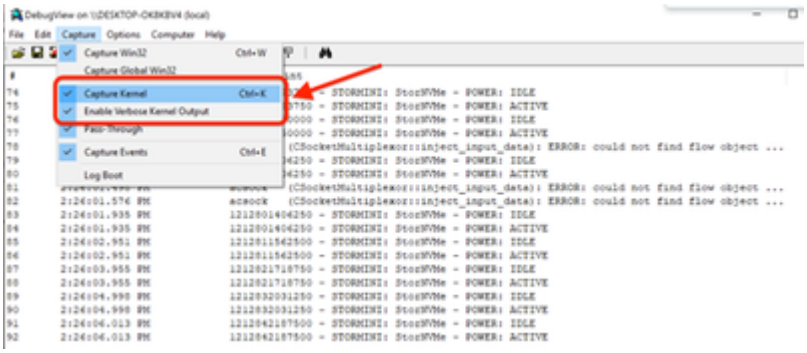
Windows

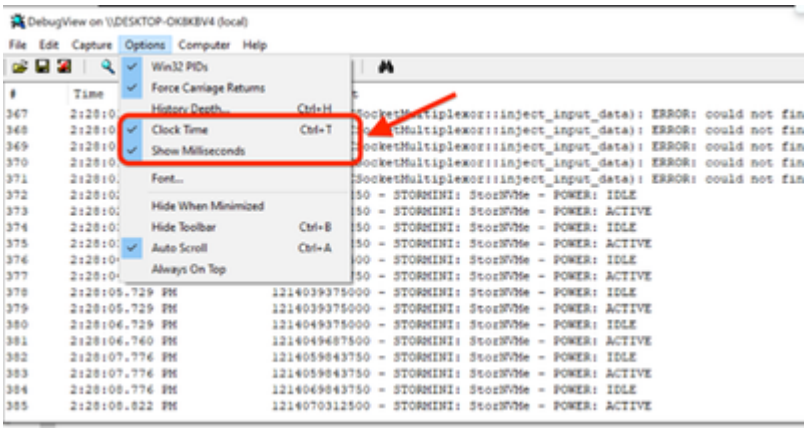
Öffnen Sie einen CMD mit Administratorberechtigungen, und führen Sie den folgenden Befehl aus:

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

- DebugView von SysInternal herunterladen, um das KDF-Protokoll zu erfassen
- Führen Sie DebugViewals aus, administratorund aktivieren Sie die nächsten Menüoptionen:
- Auf Erfassung klicken
  - Markierung Capture Kernel
  - Markierung Enable Verbose Kernel Output
- Optionen
  - Markierung Clock Time

- Markierung Show Milliseconds

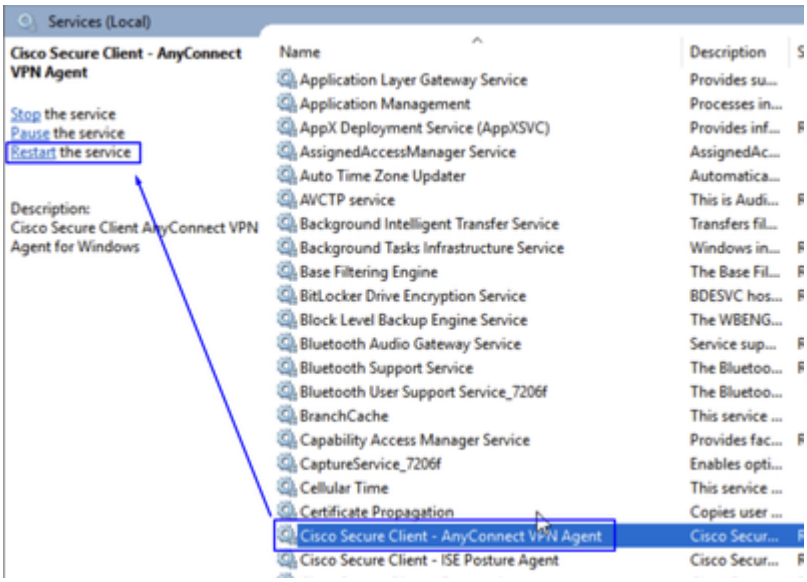




- Starten Sie den Client-Dienst über die Admin-Eingabeaufforderung neu:

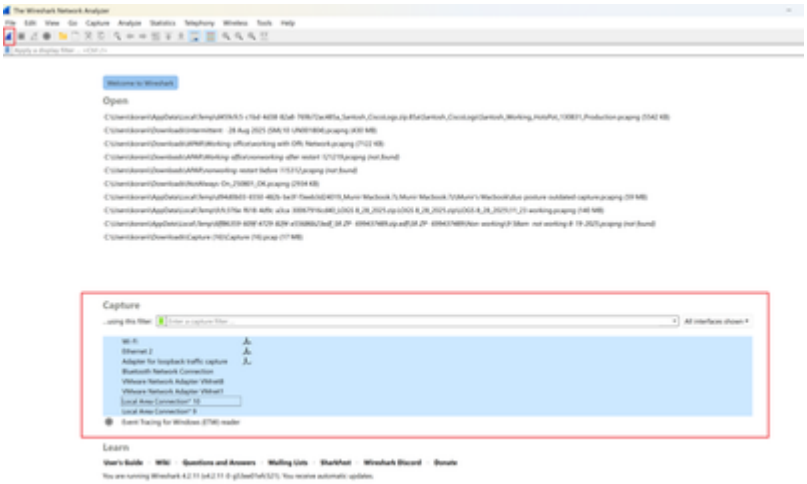
```
net stop csc_vpnagent && net start csc_vpnagent
```

- Wenn net stop csc_vpnagent && net start csc_vpnagentnicht funktioniert, starten Sie den Cisco Secure ClientDienst von services.msc neu.

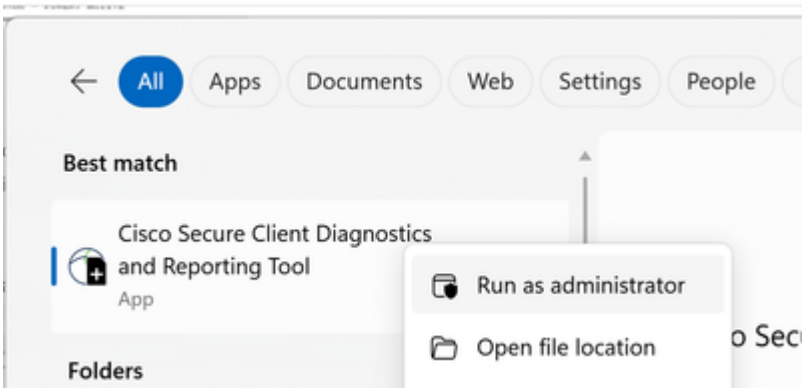


- Duo im Debugmodus aktivieren

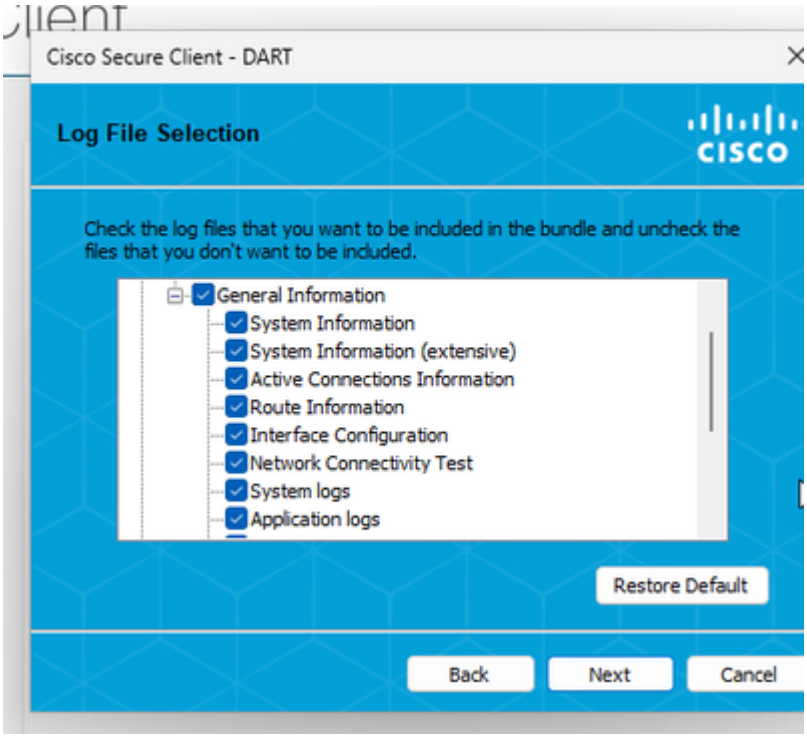
- Start Wireshark Capture
- Wählen Sie alle Schnittstellen aus, und starten Sie die Paketerfassung.



- Reproduzieren Sie das Problem, speichern Sie es KDF Logsund Wireshark Captureund befolgen Sie dann die Schritte zur Erfassung DART Bundle
- Öffnen Sie Cisco Secure Client Diagnostics & Reporting Tool (DART)mit Administratorrechten.



- Klicken Sie Custom
  - Einschließen System Information Extensiveund Network Connectivity Test



- Um die KDF-Protokollierung unter Windows zu beenden, verwenden Sie den folgenden Befehl:

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

Anmerkung: Sammeln Sie alle Protokolle, KDF-Protokolle, Wireshark Capture und DART-Pakete bis zum TAC-Gehäuse.

MacOS

Öffnen Sie Terminal und folgen Sie der nächsten Befehlskette, um KDF Logging unter MacOS zu aktivieren:

- Stop Service

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

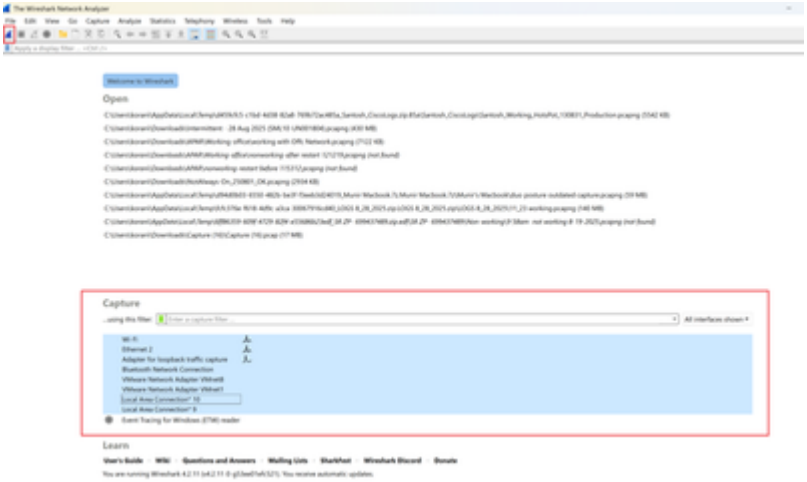
- Enable Flag

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

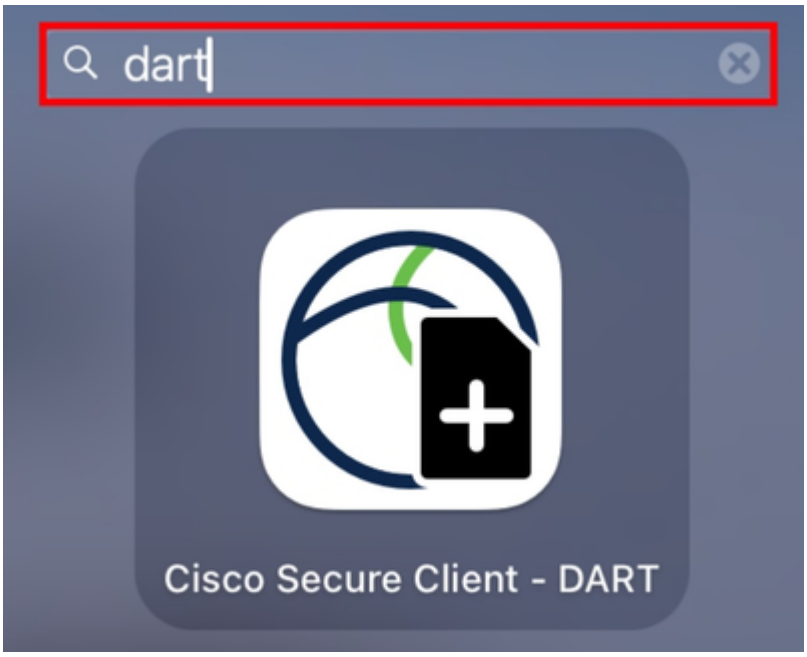
- Start Service

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

- Duo im Debugmodus aktivieren
- Start Wireshark Capture
- Wählen Sie alle Schnittstellen aus, und starten Sie die Paketerfassung.



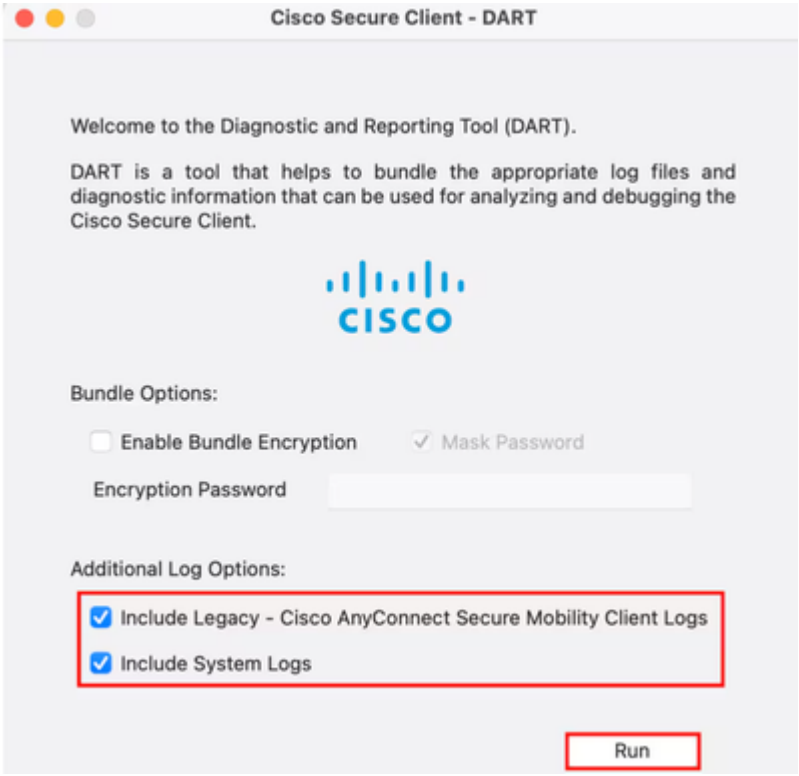
- Reproduzieren Sie das Problem, speichern Sie es KDF Logsund Wireshark Captureund befolgen Sie dann die Schritte zur Erfassung DART Bundle
- Öffnen Sie Cisco Secure Client - DART



- Markieren Sie die nächsten Optionen:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs

- Include System Logs

- Klicken Sie auf Run



Anmerkung: Sammeln Sie alle Protokolle, KDF-Protokolle, Wireshark Capture und DART-Pakete bis zum TAC-Gehäuse.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Cisco Secure Access-Hilfecenter
- Cisco SASE Designleitfaden
- Sammeln von KDF-Protokollen für Secure Client unter Windows und MacOS

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.