Verzamel gedetailleerde ZTNA-logboeken voor probleemoplossing

Inhoud

Inleiding

In dit document wordt beschreven hoe u gedetailleerde ZTA-logboeken voor probleemoplossing kunt verzamelen, wanneer u deze kunt inschakelen en stap voor stap.

Achtergrondinformatie

Naarmate organisaties steeds meer Zero Trust Architecture (ZTA) gebruiken om gebruikers, apparaten en toepassingen te beveiligen, is het oplossen van problemen met connectiviteit en beleidshandhaving complexer geworden. In tegenstelling tot traditionele perimetergebaseerde modellen, vertrouwt ZTA op meerdere real-time beslissingen over identiteit, apparaathouding, netwerkcontext en cloud-gebaseerde beleidsmotoren. Wanneer zich problemen voordoen, zijn logboeken op hoog niveau vaak onvoldoende om de hoofdoorzaak te achterhalen.

Het verzamelen van gedetailleerde tracering op ZTA-niveau speelt een cruciale rol bij het verkrijgen van diep inzicht in het gedrag van klanten, beleidsevaluatie, verkeersonderschepping en interacties met cloudservices. Deze sporen stellen ingenieurs in staat om verder te gaan dan symptoomgebaseerde probleemoplossing en de exacte volgorde van gebeurtenissen te analyseren die leiden tot toegangsfouten, prestatievermindering of onverwachte beleidsresultaten.

Logbestanden verzamelen

Controles vooraf voordat een TAC-zaak wordt geopend

Deze voorcontroles zullen het TAC-team helpen de kwestie efficiënter te identificeren. Het verstrekken van deze informatie aan de ingenieurs zal hen helpen bij het oplossen van uw probleem zo snel mogelijk:

- Wat is het probleem en hoeveel gebruikers zijn getroffen?
- Welke versies en besturingssystemen worden beïnvloed?
- Is het probleem consistent of intermitterend? Als het intermitterend is, is het dan gebruikersspecifiek of wijdverspreid?
- Is het probleem begonnen na een wijziging of is het al aanwezig sinds de implementatie?
- Zijn er triggers bekend?
- Is er een workaround beschikbaar?

Logbestanden om op te halen

- DART-bundel
- Logboeken voor de ZTNA-foutopsporingsmodus
- Wireshark capture (alle interfaces, inclusief loopback)
- Foutmeldingen waargenomen
- Tijdstempels van de uitgifte
- Schermafbeelding van de status van de CSC ZTA-module
- Gebruikersnaam van de betrokken gebruiker

In de volgende secties wordt uitgelegd hoe u elk van deze logs in kunt schakelen en in detail kunt verzamelen.

ZTNA Debug Trace Mode inschakelen

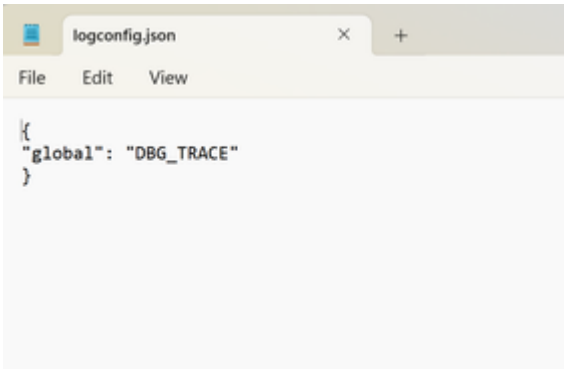
Maak een bestand met de naam logconfig.json met de onderstaande gegevens:

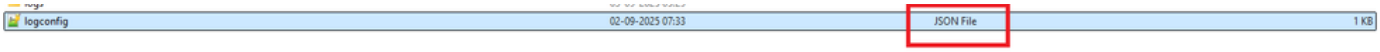
```
{ "global": "DBG_TRACE" }
```

 Waarschuwing: zorg ervoor dat uw bestand is opgeslagen met de naam logconfig.json.

Nadat u het bestand hebt gemaakt, plaatst u het op de juiste locatie op basis van het besturingssysteem:

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





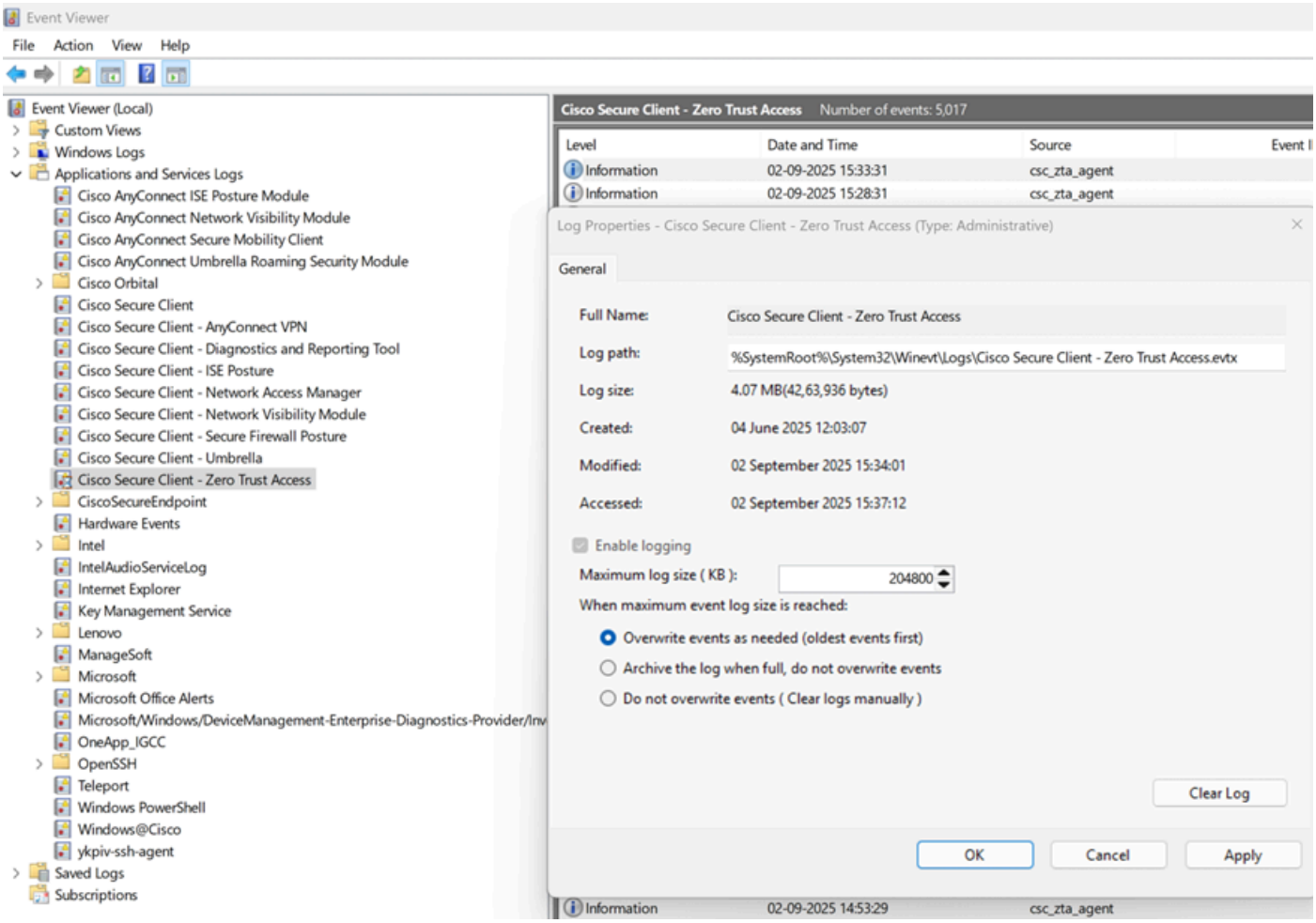
Opmerking: nadat u het opgegeven bestand hebt gemaakt, moet u de service Zero Trust Access Agent opnieuw starten (controleer stap ZTA-service opnieuw starten). Start de computer opnieuw op als het niet mogelijk is de service opnieuw op te starten.

De **grootte van het ZTA-logboek in Event Viewer** vergroten

Op Windows-pc's moet u, nadat u logboekregistratie op traceringsniveau hebt ingeschakeld, de grootte van het ZTA-logboekbestand handmatig vergroten.

1. Open Event Viewerdeuren.
2. Vouw uit in het linkerdeelvenster Applications and Services Logs.
3. Klik met de rechtermuisknop Cisco Secure Client – Zero Trust Access en selecteer PropertiesBewerken.
4. Stel onder Maximum log size (KB)de waarde in op 204800 (gelijk aan 200 MB).

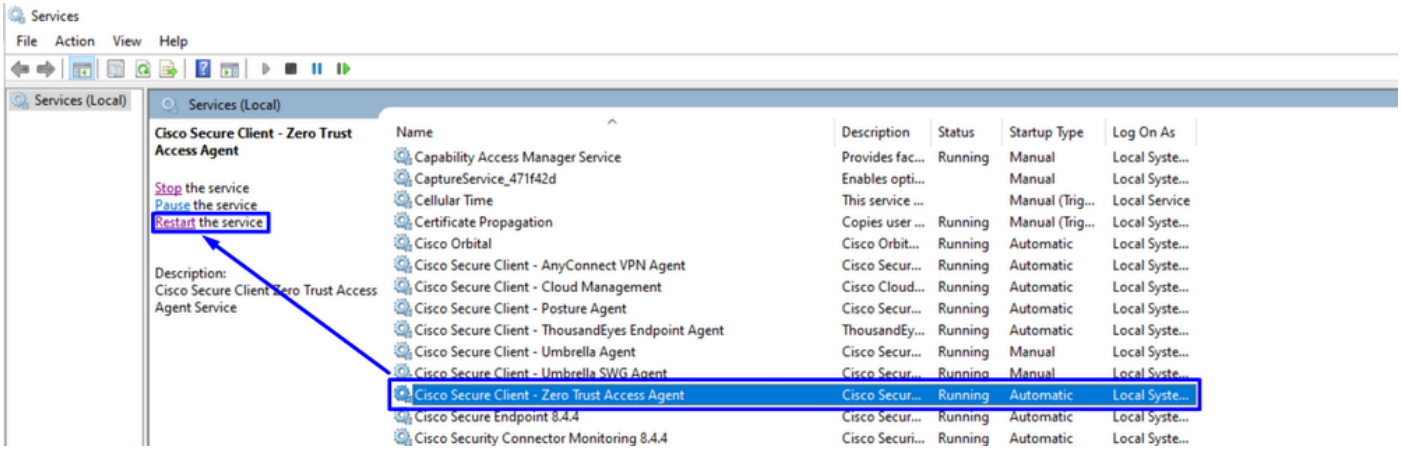
Om te voltooien klik op **Apply** en dan OK.



ZTA-service opnieuw starten

Windows

- GebruikWindows + Rom het Run Search schrijfvenster te openen services.msc en druk op enter
- Zoek de service Cisco Secure Client - Zero trust Access Agent en klik op Restart. Controleer de status van de CSC ZTA-module om te bevestigen dat deze actief is



Opmerking: als de ZTA-service niet opnieuw kan worden gestart vanwege een gebrek aan

beheerderstoegang, is een volledige systeemreboot de volgende optie.

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"
```

Opmerking: als opdrachten niet kunnen worden uitgevoerd of als de ZTA-service niet opnieuw kan worden gestart vanwege een gebrek aan beheerderstoegang, is een volledige systeemreboot de volgende optie.

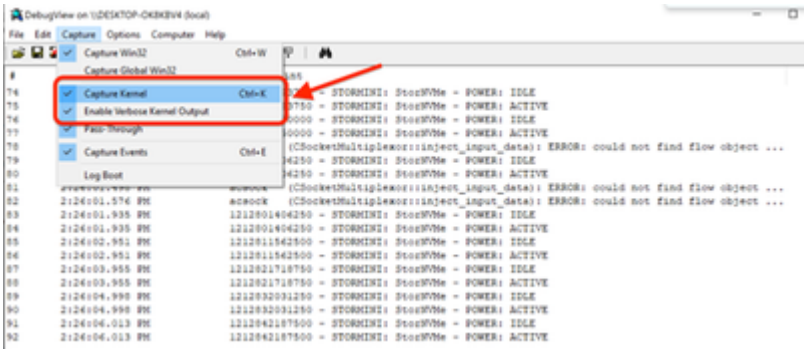
KDF-logboekregistratie, pakketopname, Duo-debugmodus en Dart-bundel inschakelen

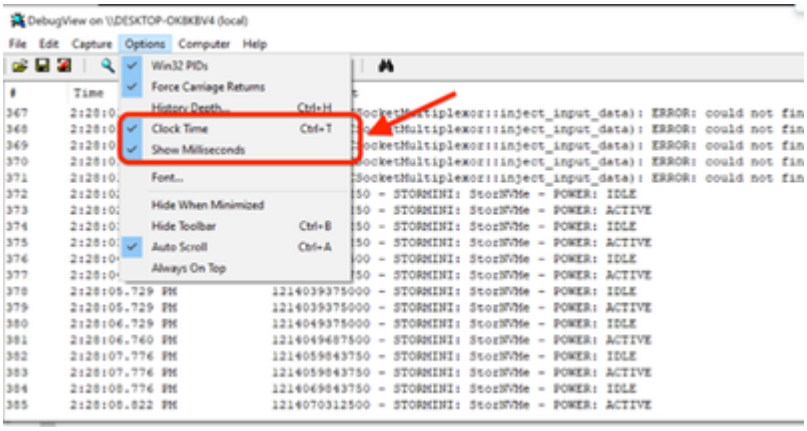
Windows

Open een CMD met beheerdersbevoegdheden en voer de volgende opdracht uit:

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

- Download DebugView van SysInternal om het KDF-log vast te leggen
- Uitvoeren DebugViewals administratoren de volgende menuopties inschakelen:
- Klik op Capture
  - vinkje Capture Kernel
  - vinkje Enable Verbose Kernel Output
- Opties
  - vinkje Clock Time
  - vinkje Show Milliseconds

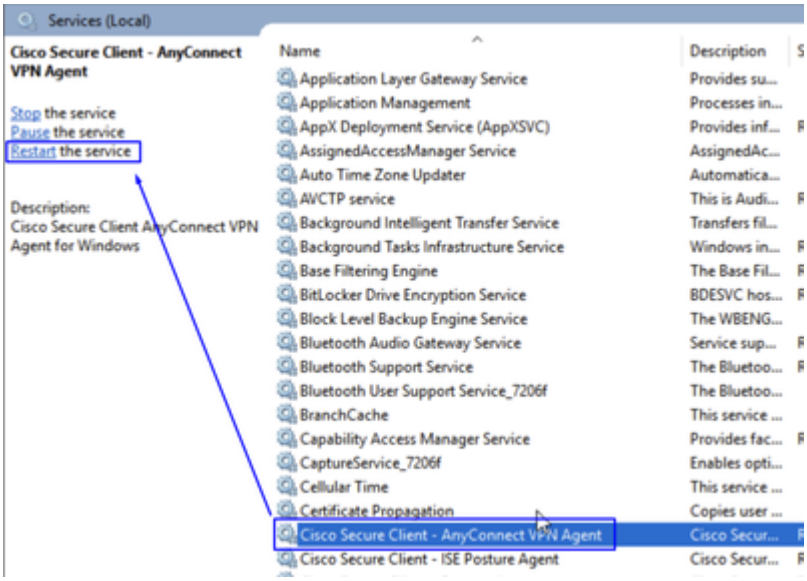




- Start de clientservice opnieuw op via de beheerdersprompt:

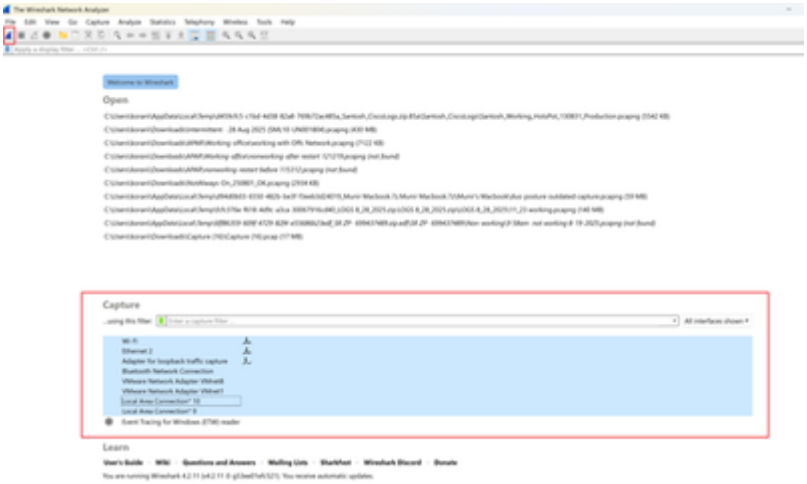
```
net stop csc_vpnagent && net start csc_vpnagent
```

- Als net stop csc_vpnagent && net start csc_vpnagentdit niet werkt, start u de Cisco Secure Clientservice opnieuw op vanaf services.msc

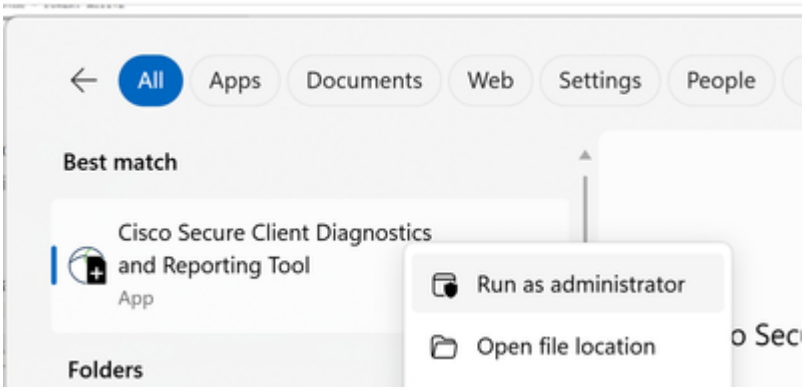


- Duo inschakelen in foutopsporingsmodus
- starten Wireshark Capture

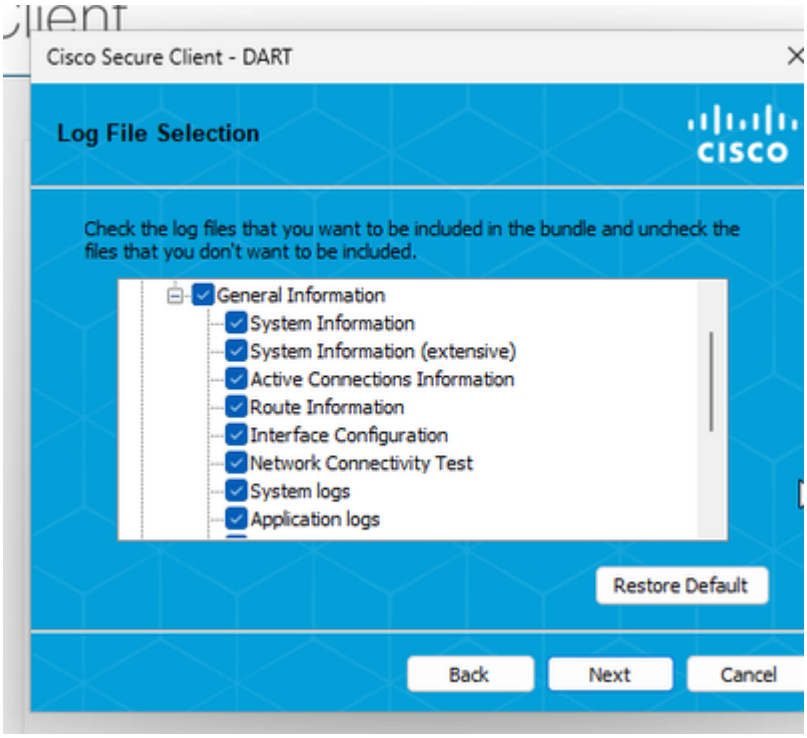
- Selecteer alle interfaces en start de pakketopname



- Reproduceer het probleem en sla KDF Logsen Wireshark Captureop en volg de stappen om vast te leggen DART Bundle
- Open de Cisco Secure Client Diagnostics & Reporting Tool (DART)met beheerdersbevoegdheden



- Klik op Custom
  - Inclusief System Information Extensiveen Network Connectivity Test



- Als u de KDF-aanmelding in Windows wilt stoppen, gebruikt u de volgende opdracht:

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

Opmerking: Verzamel alle logs, KDF-logs, Wireshark Capture en DART-bundel voor de TAC-case.

MacOS

Open terminal en volg de volgende opdrachtketen om KDF Logging op MacOS in te schakelen:

- Stop Service

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

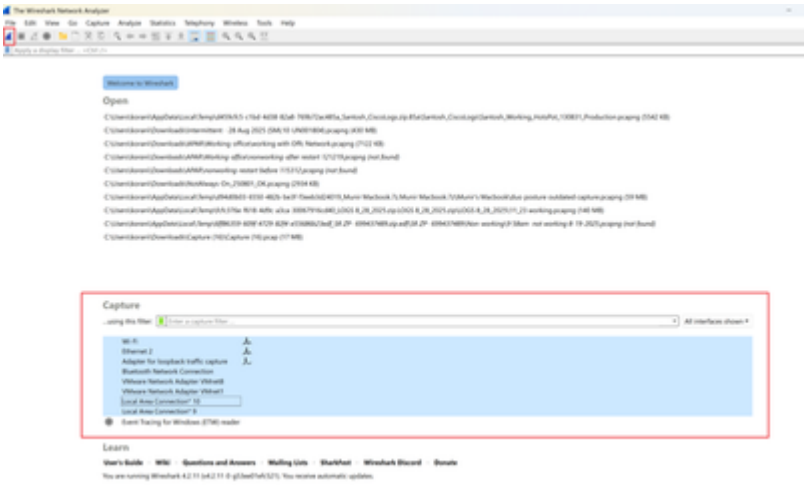
- Enable Flag

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

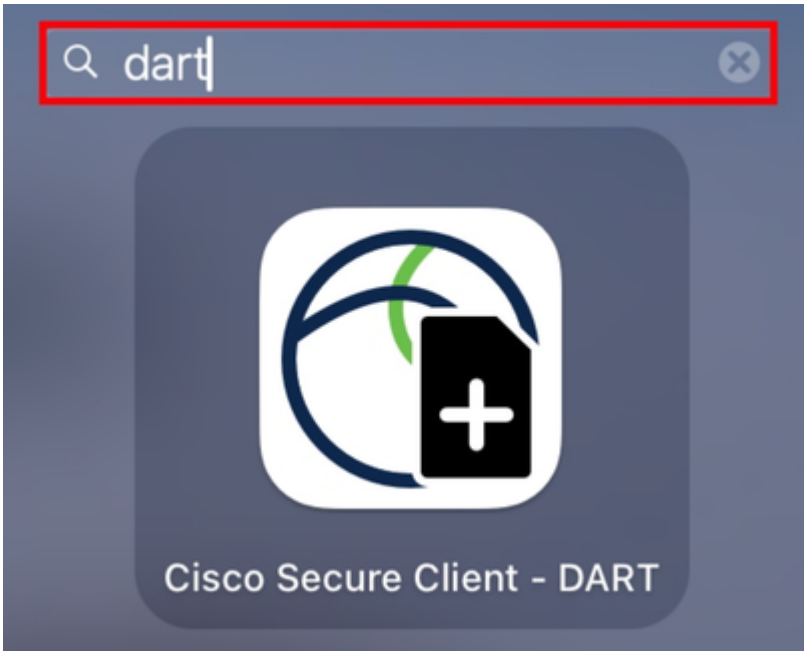
- Start Service

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

- Duo inschakelen [in foutopsporingsmodus](#)
- starten Wireshark Capture
- Selecteer alle interfaces en start de pakketopname

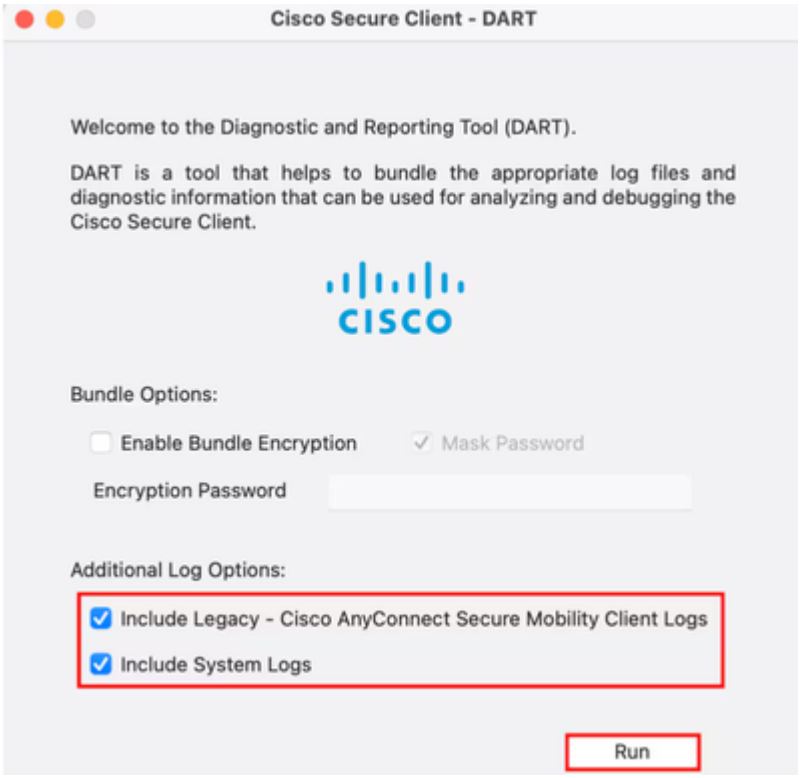


- Reproduceer het probleem en sla KDF Logsen Wireshark Captureop en volg de stappen om vast te leggen DART Bundle
- Open de Cisco Secure Client - DART



- Selecteer de volgende opties:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs

- Klik op de knop Run



Opmerking: Verzamel alle logs, KDF-logs, Wireshark Capture en DART-bundel voor de TAC-case.

Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Cisco SASE-ontwerphandleiding
- KDF-logboeken verzamelen voor beveiligde client op Windows en MacOS

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.