Raccolta dei log ZTNA dettagliati per la risoluzione dei problemi

Sommario

Introduzione

Questo documento descrive come raccogliere i log dettagliati di risoluzione dei problemi ZTA, quando abilitare e passo dopo passo.

Premesse

Poiché le organizzazioni adottano sempre più spesso l'architettura ZTA (Zero Trust Architecture) per proteggere utenti, dispositivi e applicazioni, la risoluzione dei problemi di connettività e l'applicazione delle policy è diventata più complessa. A differenza dei modelli tradizionali basati sul perimetro, ZTA si basa su più decisioni in tempo reale relative a identità, postura dei dispositivi, contesto di rete e motori di policy basati su cloud. Quando si verificano dei problemi, i log di alto livello sono spesso insufficienti per individuare la root cause.

La raccolta di informazioni dettagliate sul livello ZTA svolge un ruolo critico per ottenere una visibilità completa del comportamento dei client, della valutazione delle policy, dell'intercettazione del traffico e delle interazioni con i servizi cloud. Queste tracce consentono ai tecnici di andare oltre la risoluzione dei problemi basata sui sintomi e di analizzare la sequenza esatta degli eventi che portano ad errori di accesso, peggioramento delle prestazioni o risultati imprevisti delle policy.

Raccolta dei log

Controlli preliminari prima di aprire una richiesta TAC

Questi controlli preliminari consentiranno al team TAC di identificare il problema in modo più efficiente. Fornendo queste informazioni ai tecnici, questi saranno in grado di risolvere il problema il più rapidamente possibile:

- Qual è il problema e quanti utenti ne sono interessati?
- Quali sono i sistemi operativi e le versioni interessati?
- Il problema è coerente o intermittente? Se intermittente, è specifico dell'utente o diffuso?
- Il problema è iniziato dopo una modifica o è presente dopo la distribuzione?
- Ci sono trigger noti?
- È disponibile una soluzione alternativa?

Log da recuperare

- Pacchetto DART
- Registri modalità traccia debug ZTNA
- Wireshark capture (tutte le interfacce, incluso il loopback)
- Messaggi di errore osservati
- Timestamp del problema
- Schermata dello stato del modulo CSC ZTA
- Nome utente dell'utente interessato

Nelle sezioni seguenti viene descritto come attivare e raccogliere questi log in dettaglio.

Abilita modalità di traccia debug ZTNA

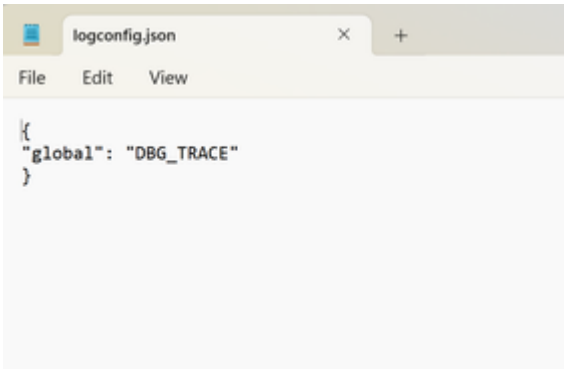
Creare un file denominato `logconfig.json` con i dettagli seguenti:

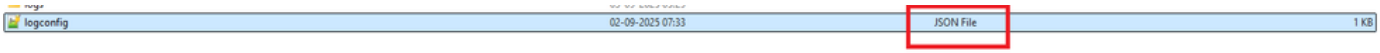
```
{ "global": "DBG_TRACE" }
```

 Avviso: Accertarsi che il file sia stato salvato con il nome `logconfig.json`.

Dopo aver creato il file, posizionarlo nella posizione appropriata in base al sistema operativo:

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





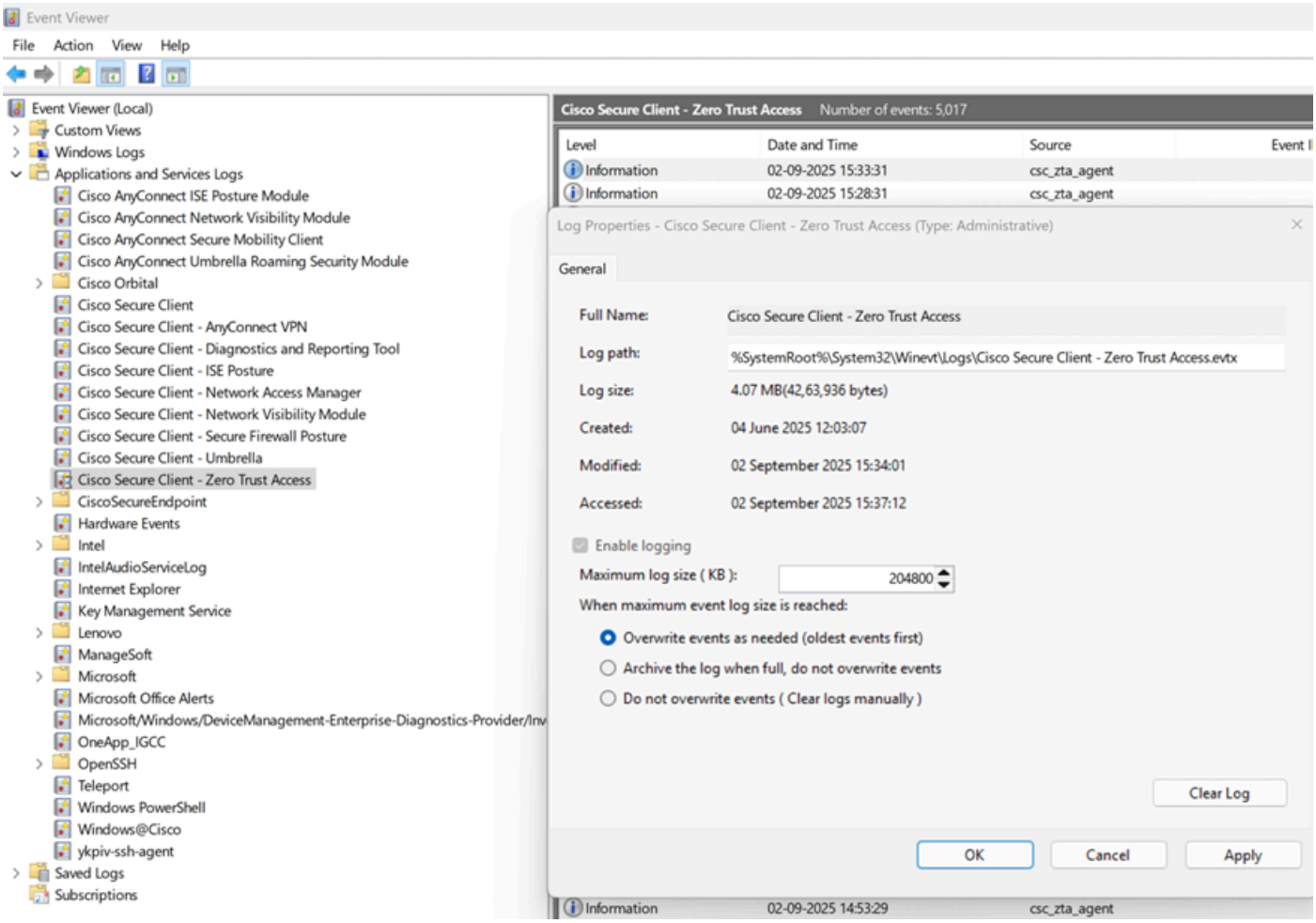
Nota: Dopo aver creato il file specificato, è necessario riavviare il servizio Agente di accesso di protezione zero (vedere il passaggio Riavvio del servizio ZTA). Se non è possibile riavviare il servizio, riavviare il computer.

Aumentare le **dimensioni del registro ZTA nel Visualizzatore eventi**

Nei PC Windows, dopo aver attivato la registrazione a livello di traccia, è necessario aumentare manualmente le dimensioni del file di registro ZTA.

1. Apri Event Viewer.
2. Nel riquadro sinistro espandere Applications and Services Logs.
3. Fare clic con il pulsante destro del mouse Cisco Secure Client – Zero Trust Access e selezionare Properties.
4. In Maximum log size (KB), impostare il valore su 204800 (equivalente a 200 MB).

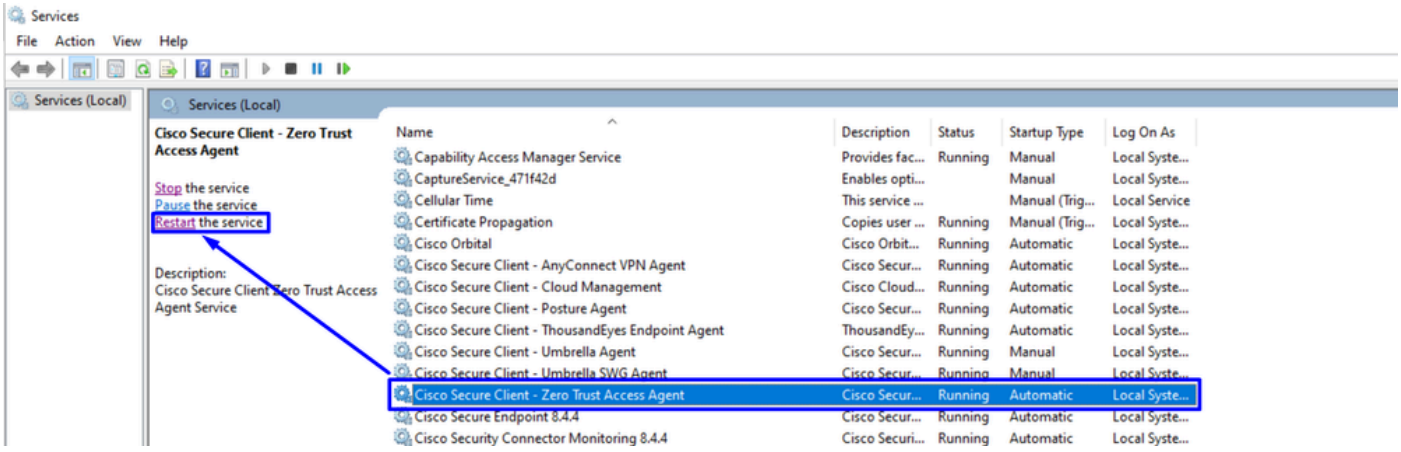
Per finalizzare, fare clic su **Apply** , quindi su OK.



Riavvio del servizio ZTA

Windows

- Utilizzare Windows + R per aprire la finestra di Run Search scrittura services.msc e premere Invio
- Individuare il servizio Cisco Secure Client - Zero trust Access Agent e fare clic su Restart. Al termine, verificare lo stato del modulo CSC ZTA per confermare che è attivo



Nota: Se il servizio ZTA non può essere riavviato a causa di mancanza di accesso

amministrativo, un riavvio completo del sistema è l'opzione successiva.

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"
```

Nota: Se non è possibile eseguire i comandi o riavviare il servizio ZTA a causa di mancanza di accesso amministrativo, il riavvio completo del sistema rappresenta l'opzione successiva.

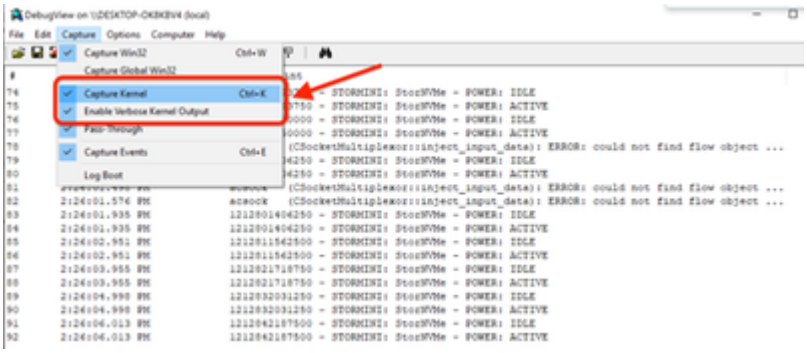
Abilita registrazione KDF, acquisizione pacchetti, modalità di debug Duo e bundle Dart

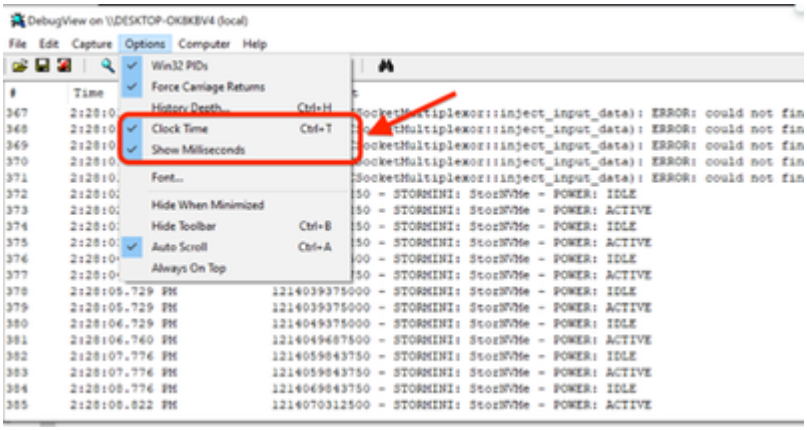
Windows

Aprire un CMD con privilegi di amministratore ed eseguire il comando successivo:

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

- Scaricare DebugView da SysInternal per acquisire il log KDF
- Esegui DebugViewcome administratore abilita le opzioni di menu successive:
- Fare clic su Cattura
  - Segno Di Spunta Capture Kernel
  - Segno Di Spunta Enable Verbose Kernel Output
- Options
  - Segno Di Spunta Clock Time
  - Segno Di Spunta Show Milliseconds

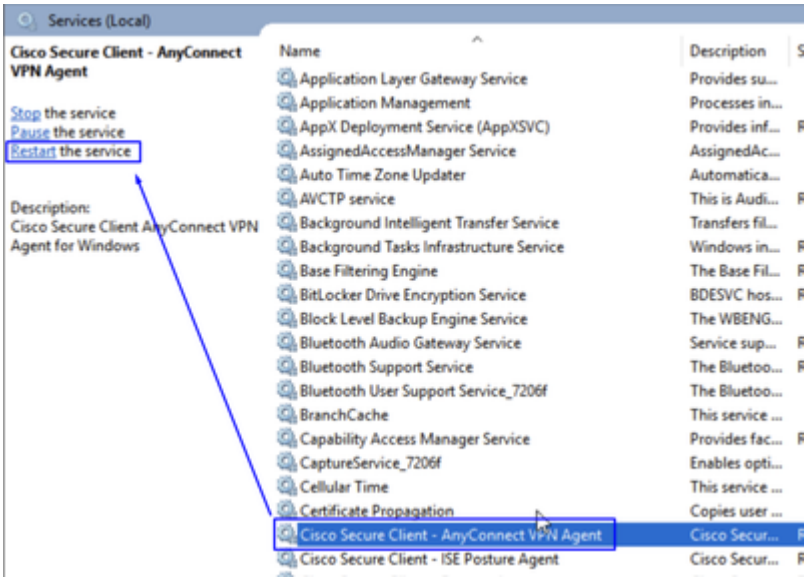




- Riavviare il servizio client tramite il prompt dell'amministratore:

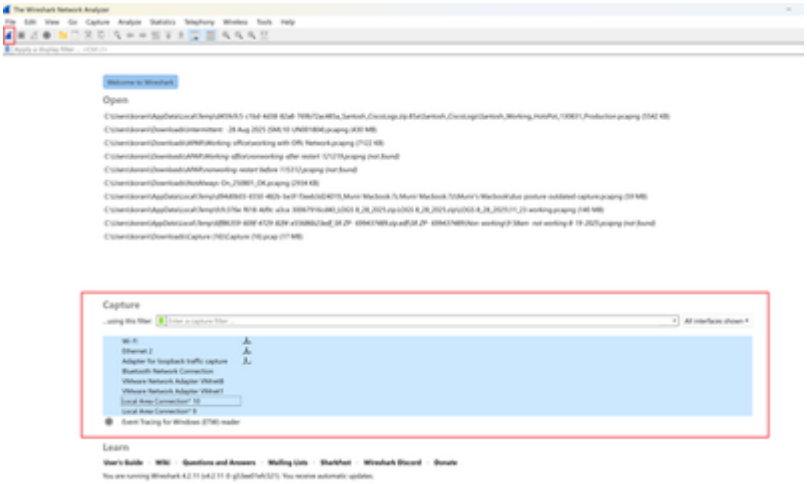
```
net stop csc_vpnagent && net start csc_vpnagent
```

- Se net stop csc_vpnagent && net start csc_vpnagentnon funziona, riavviare il Cisco Secure Clientservizio da services.msc

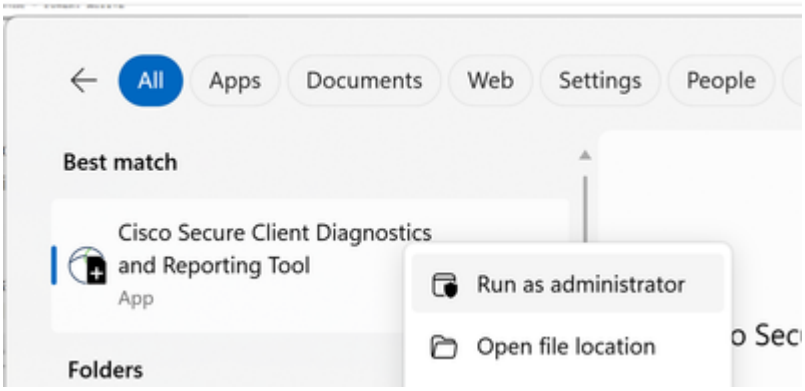


- Abilitare Duo in modalità di debug
- Inizio Wireshark Capture

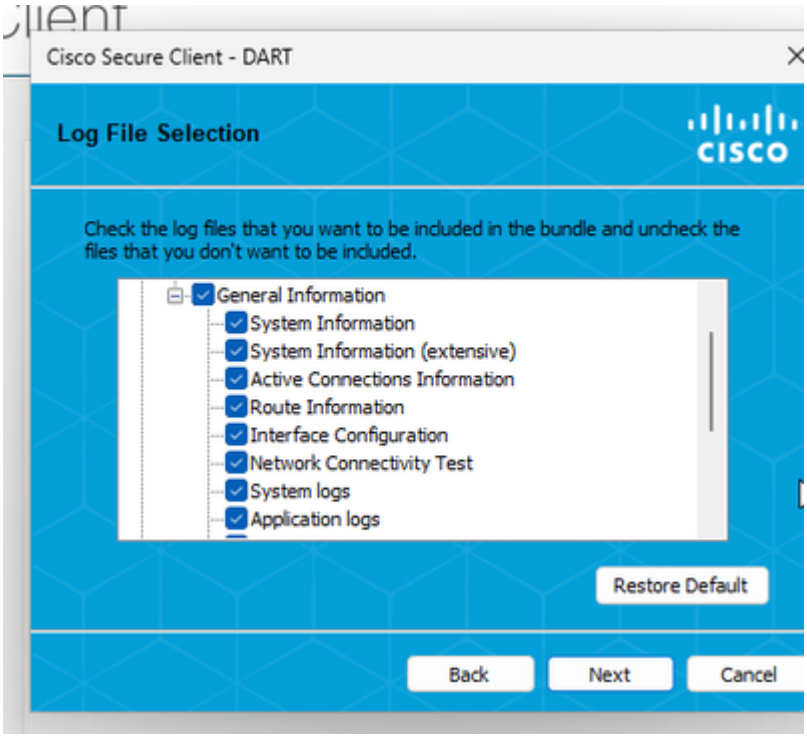
- Selezionare tutte le interfacce e avviare l'acquisizione del pacchetto



- Riprodurre il problema, salvare KDF LogseWireshark Capture, quindi seguire i passaggi per acquisire DART Bundle
- Aprire Cisco Secure Client Diagnostics & Reporting Tool (DART)con privilegi di amministratore



- Fare clic su Custom
  - Includi System Information Extensivee Network Connectivity Test



- Per interrompere la registrazione KDF in Windows, utilizzare il comando seguente:

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

Nota: Raccogliere tutti i registri, i registri KDF, Wireshark Capture e il pacchetto DART nella richiesta TAC.

MacOS

Aprire il terminale e seguire la catena di comandi successiva per abilitare la registrazione KDF su MacOS:

- Stop Service

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

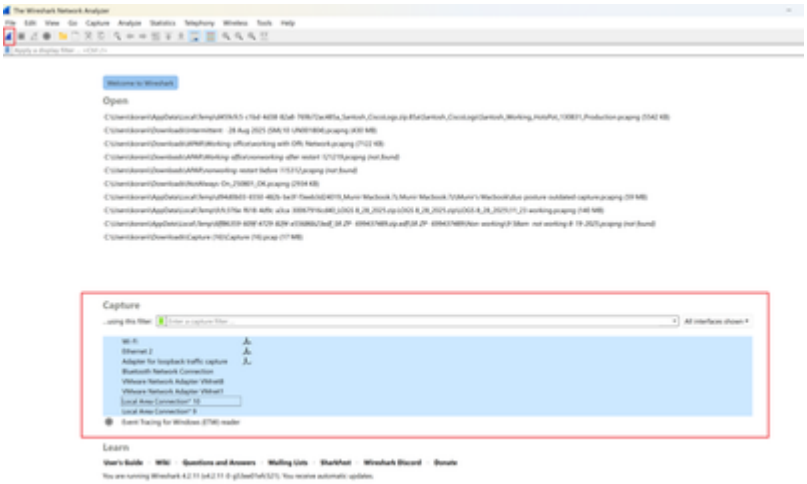
- Enable Flag

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

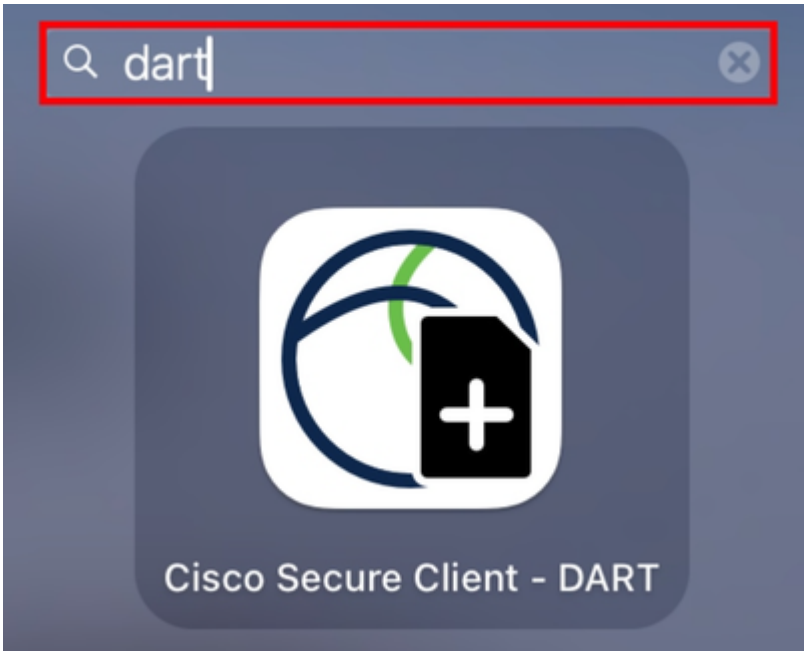
- Start Service

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

- Abilitare Duo in modalità di debug
- Inizio Wireshark Capture
- Selezionare tutte le interfacce e avviare l'acquisizione del pacchetto

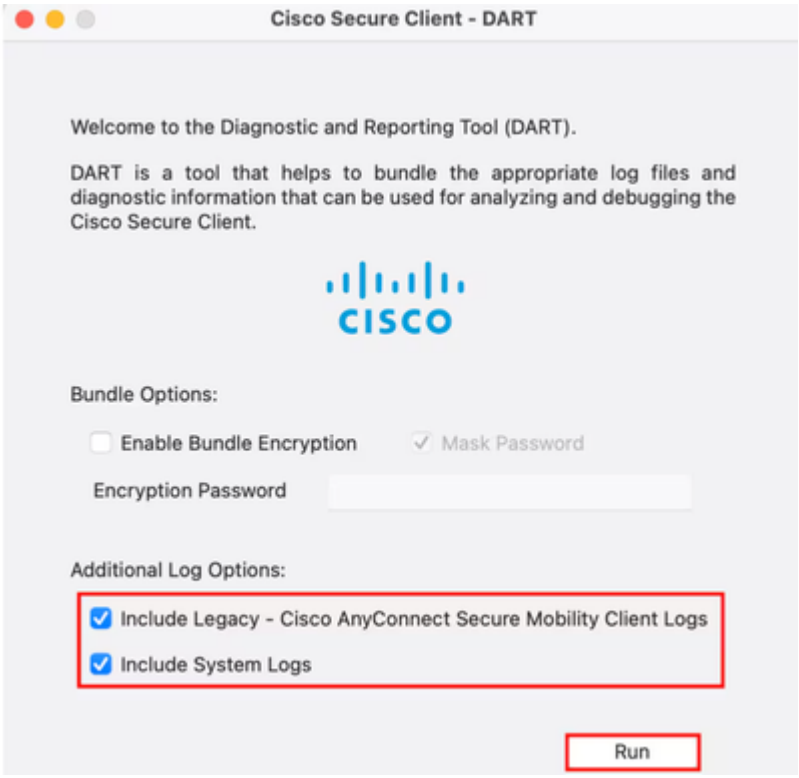


- Riprodurre il problema, salvare KDF LogseWireshark Capture, quindi seguire i passaggi per acquisire DART Bundle
- Aprire il Cisco Secure Client - DART



- Selezionare le opzioni successive:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs

- Fare clic su Run



Nota: Raccogliere tutti i registri, i registri KDF, Wireshark Capture e il pacchetto DART nella richiesta TAC.

Informazioni correlate

- Supporto tecnico Cisco e download
- Cisco Secure Access Help Center
- Guida alla progettazione di Cisco BASE
- Raccolta dei log KDF per Secure Client su Windows e MacOS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).