Configuration de la journalisation ZTNA pour le dépannage

Table des matières

- Introduction
- Informations générales
- Collecte des journaux
  - Vérifications préalables avant l'ouverture d'un dossier TAC
  - Journaux à collecter
  - Activer le mode de suivi de débogage ZTNA
  - Augmenter la taille du journal ZTA dans l'Observateur d'événements
    - Fenêtres
    - MacOS
  - Activer la journalisation KDF, la capture de paquets, le mode de débogage Duo et le bundle Dart
    - Fenêtres
    - Commandes Windows Powershell pour activer et désactiver, il doit être exécuté en tant qu'administrateur :
    - MacOS
- Informations connexes

Introduction

Ce document décrit comment collecter des journaux de dépannage ZTA détaillés et quand activer étape par étape.

Informations générales

À mesure que les entreprises adoptent de plus en plus l'architecture ZTA (Zero Trust Architecture) pour sécuriser les utilisateurs, les périphériques et les applications, le dépannage des problèmes de connectivité et d'application des politiques est devenu plus complexe. Contrairement aux modèles traditionnels basés sur le périmètre, ZTA s'appuie sur plusieurs décisions en temps réel concernant l'identité, la position des périphériques, le contexte réseau et les moteurs de politiques basés sur le cloud. Lorsque des problèmes surviennent, les journaux de haut niveau sont souvent insuffisants pour identifier la cause première.

La collecte d'un suivi détaillé du niveau ZTA joue un rôle essentiel dans l'obtention d'une visibilité approfondie sur le comportement des clients, l'évaluation des politiques, l'interception du trafic et les interactions des services cloud. Ces suivis permettent aux ingénieurs d'aller au-delà du

dépannage basé sur les symptômes et d'analyser la séquence exacte des événements entraînant des défaillances d'accès, une dégradation des performances ou des résultats de stratégie inattendus.

Collecte des journaux

Vérifications préalables avant l'ouverture d'un dossier TAC

Ces vérifications préalables permettent à l'équipe TAC d'identifier le problème plus efficacement. En fournissant ces informations aux ingénieurs, vous les aidez à résoudre votre problème le plus rapidement possible :

- Quel est le problème et combien d'utilisateurs sont concernés ?
- Quels systèmes d'exploitation et versions sont affectés ?
- Le problème est-il constant ou intermittent ? Si elle est intermittente, est-elle spécifique à l'utilisateur ou répandue ?
- Le problème a-t-il commencé après une modification ou a-t-il été présent depuis le déploiement ?
- Existe-t-il des déclencheurs connus ?
- Existe-t-il une solution de contournement ?

Journaux à collecter

- offre groupée DART
- Journaux du mode de suivi du débogage ZTNA
- Capture Wireshark (toutes les interfaces, y compris la boucle)
- Messages d'erreur observés
- Horodatages de l'émission
- Capture d'écran d'état du module CSC ZTA
- Nom de l'utilisateur affecté

Les sections suivantes expliquent en détail comment activer et collecter chacun de ces journaux.

Activer le mode de suivi de débogage ZTNA

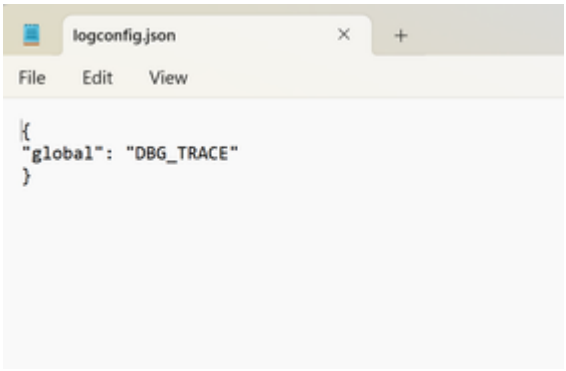
Créez un fichier nommé logconfig.json avec ces détails ci-dessous :

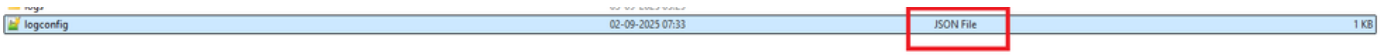
```
{ "global": "DBG_TRACE" }
```

Avertissement : Assurez-vous que votre fichier est enregistré sous le nom logconfig.json.

Après avoir créé le fichier, placez-le à l'emplacement approprié en fonction du système d'exploitation :

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





Remarque : Une fois que vous avez créé le fichier spécifié, vous devez redémarrer le service Zero Trust Access Agent (Veuillez vérifier l'étape Redémarrage du service ZTA). Si le redémarrage du service n'est pas possible, redémarrez l'ordinateur.

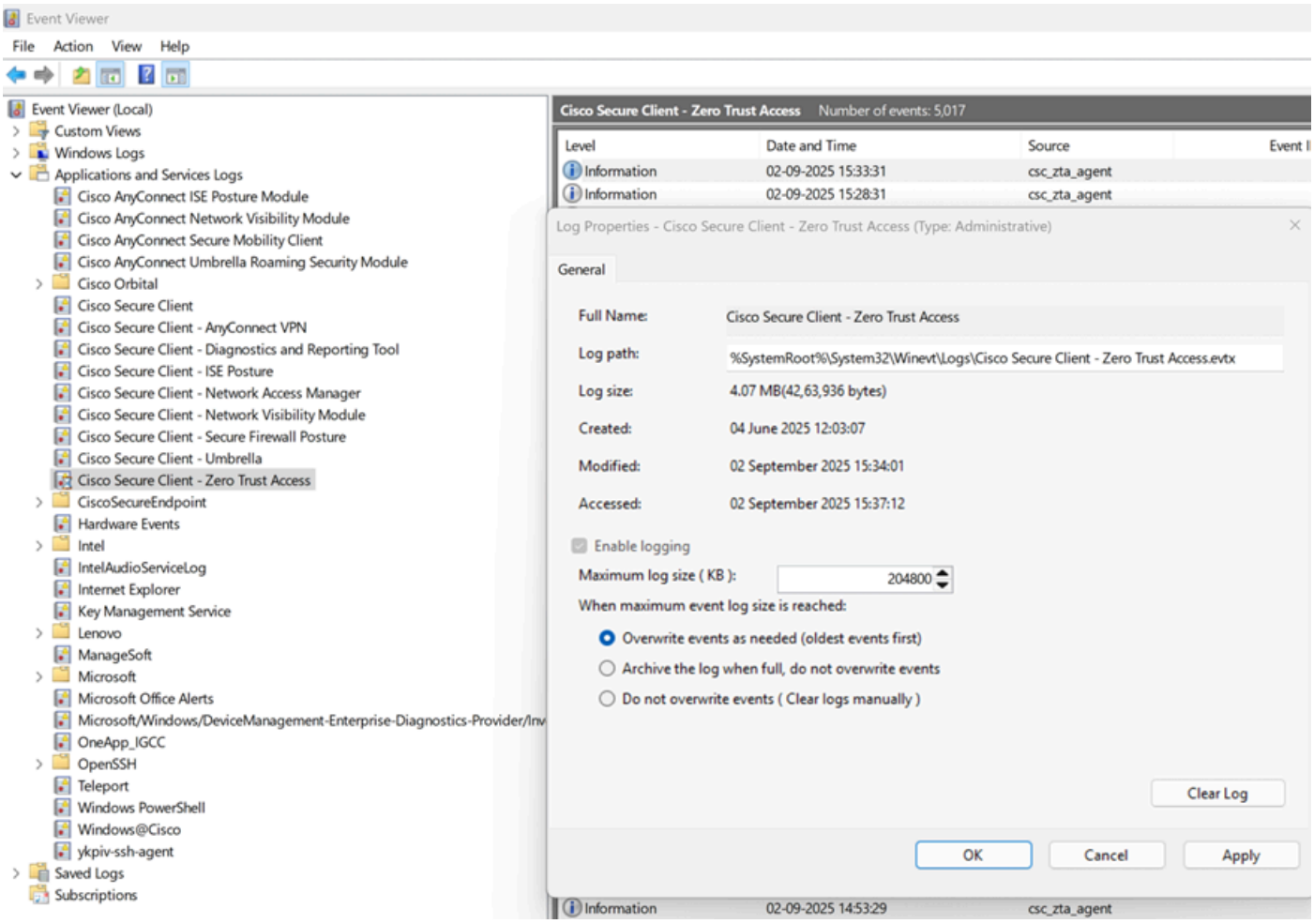
Augmenter la **taille du journal ZTA dans l'Observateur d'événements**

Sur les ordinateurs Windows, après avoir activé la journalisation au niveau du suivi, vous devez

augmenter manuellement la taille du fichier journal ZTA.

1. Ouvrez Event Viewer.
2. Dans le volet gauche, développez Applications and Services Logs.
3. Cliquez avec le bouton droit Cisco Secure Client – Zero Trust Access et sélectionnez Properties.
4. SousMaximum log size (KB), définissez la valeur sur 204800 (équivalent à 200 Mo).

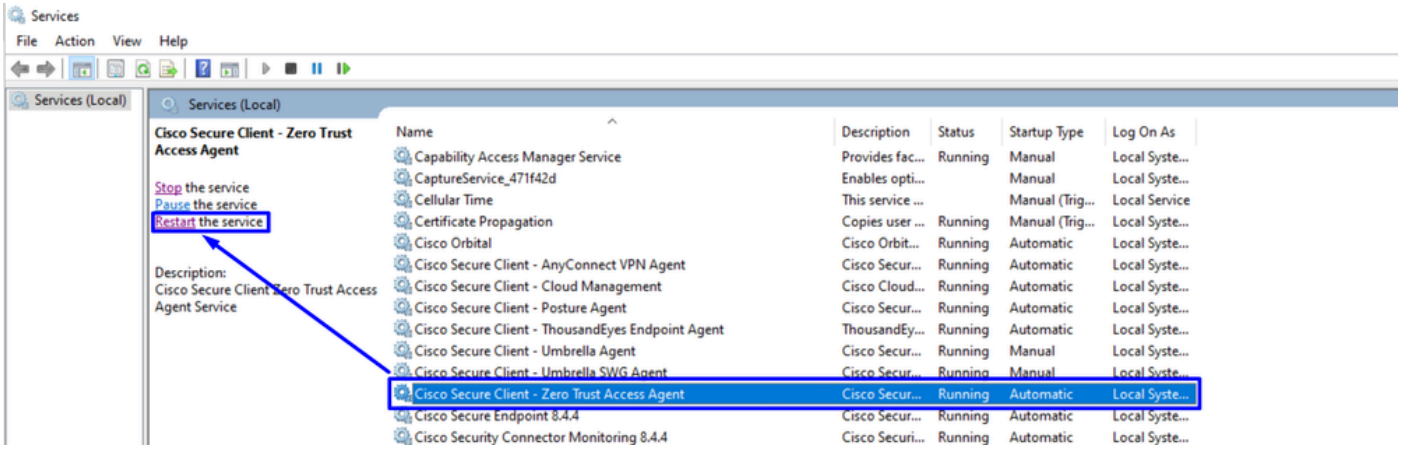
Pour finaliser, cliquez sur **Apply** , puis sur OK.



Redémarrage du service ZTA

Fenêtres

- UtilisezWindows + Rpour ouvrir l' Run Search écriture services.msc et appuyez sur Entrée.
- Recherchez le service Cisco Secure Client - Zero trust Access Agent et cliquez sur Restart. Une fois terminé, vérifiez l'état du module ZTA CSC pour confirmer qu'il est actif.



Remarque : Si le service ZTA ne peut pas être redémarré en raison d'un manque d'accès administratif, un redémarrage complet du système est votre prochaine 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"
```

Remarque : Si les commandes ne peuvent pas être exécutées ou si le service ZTA ne peut pas être redémarré en raison d'un manque d'accès administratif, un redémarrage complet du système est votre prochaine option.

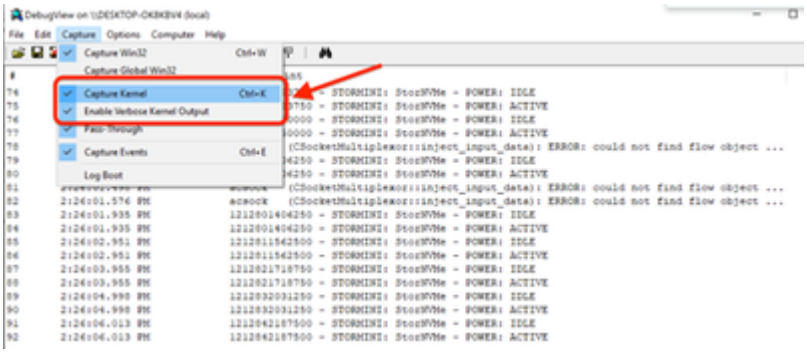
Activer la journalisation KDF, la capture de paquets, le mode de débogage Duo et le bundle Dart

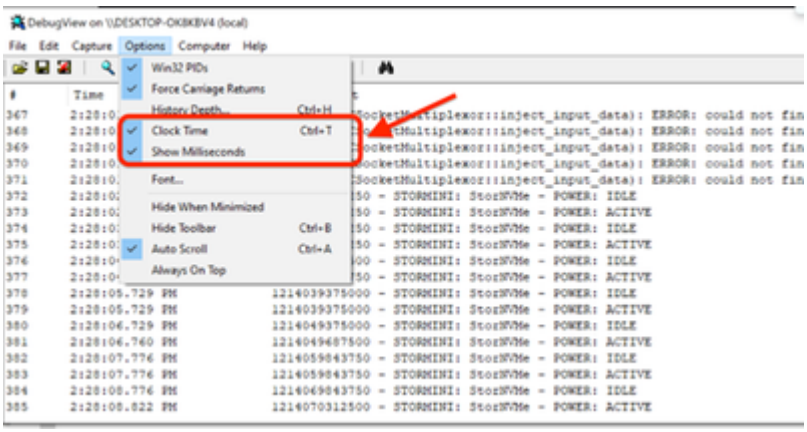
Fenêtres

Ouvrez un CMD avec des privilèges d'administrateur et exécutez la commande suivante :

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

- Téléchargez DebugView depuis SysInternal pour capturer le journal KDF.
- Exécuter DebugViewen tant que administratoret activer les options de menu suivantes :
- Cliquez sur Capture.
  - Coche Capture Kernel.
  - Coche Enable Verbose Kernel Output.
- Options
  - Coche Clock Time.
  - Coche Show Milliseconds.

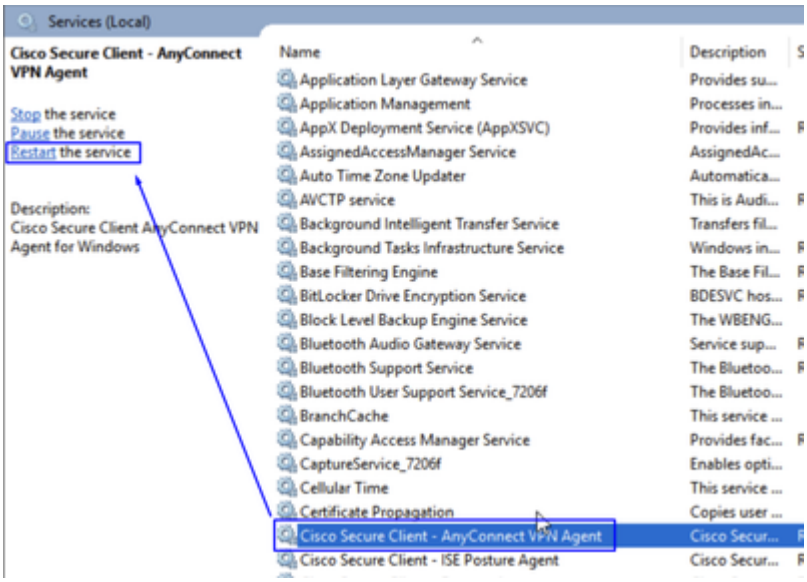




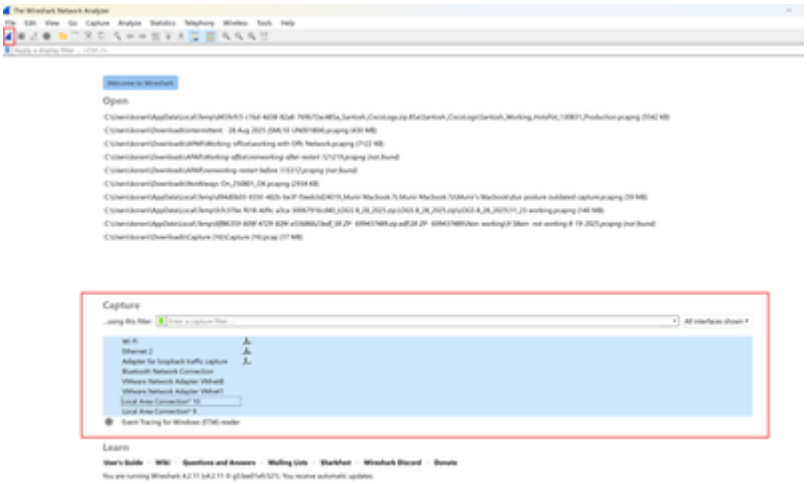
- Redémarrez le service client via l'invite admin :

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

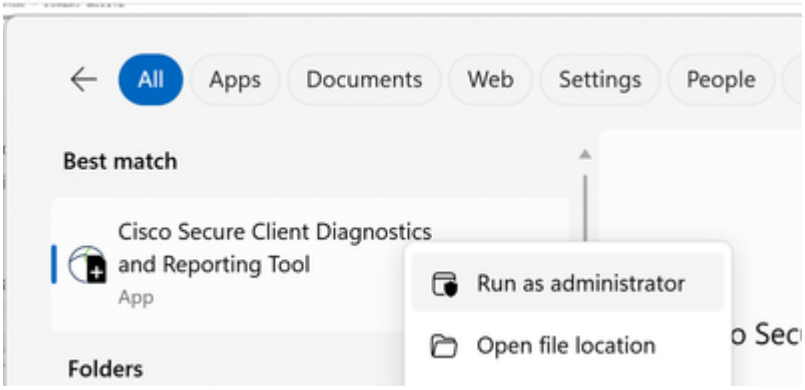
- Si net stop csc_vpnagent && net start csc_vpnagentne fonctionne pas, redémarrez le Cisco Secure Clientservice à partir de services.msc.



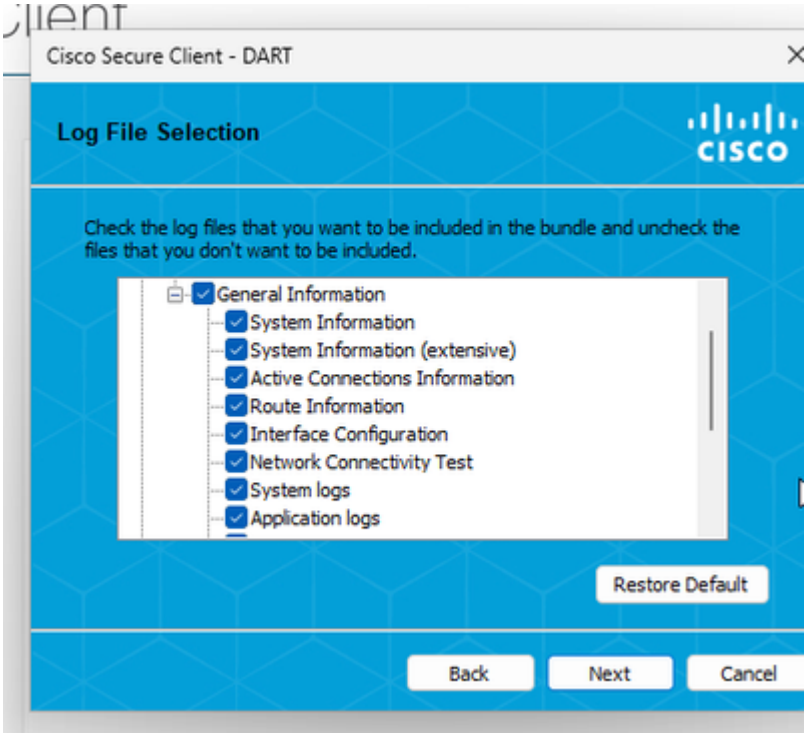
- Activer Duo en mode débogage
- Début Wireshark Capture.
- Sélectionnez toutes les interfaces et lancez la capture de paquets.



- Reproduisez le problème, enregistrez-le KDF LogsWireshark Captureet suivez les étapes de capture DART Bundle.
- Ouvrez l' Cisco Secure Client Diagnostics & Reporting Tool (DART)avec des privilèges d'administrateur.



- Cliquer Custom.
  - Inclure System Information Extensive et Network Connectivity Test.



- Pour arrêter la journalisation du fichier KDF sous Windows, utilisez la commande suivante :

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

Remarque : Collectez tous les journaux : Journaux KDF, offre groupée de capture Wireshark et DART au dossier TAC.

Commandes Windows Powershell pour activer et désactiver, il doit être exécuté en tant qu'administrateur :

```
#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

Ouvrez le terminal et suivez la chaîne de commandes suivante pour activer la journalisation KDF sur MacOS :

- Stop Service.

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

- Enable Flag.

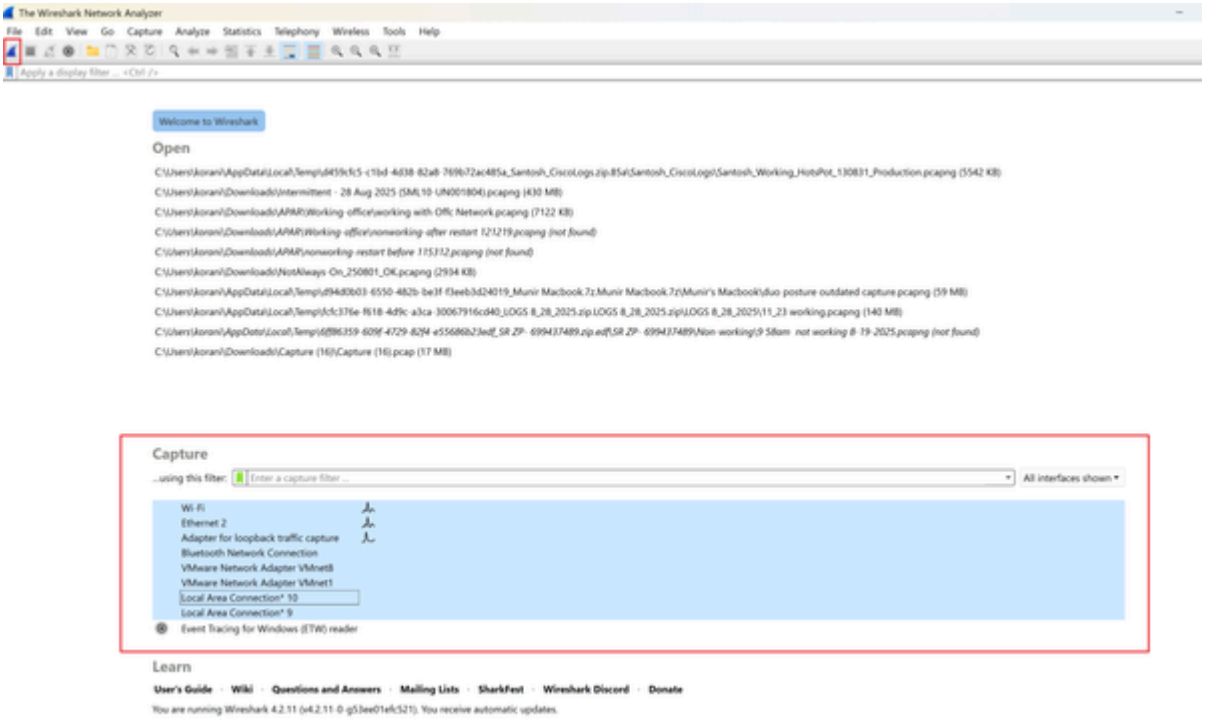
```
echo debug=0x400080152 | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

- Start Service.

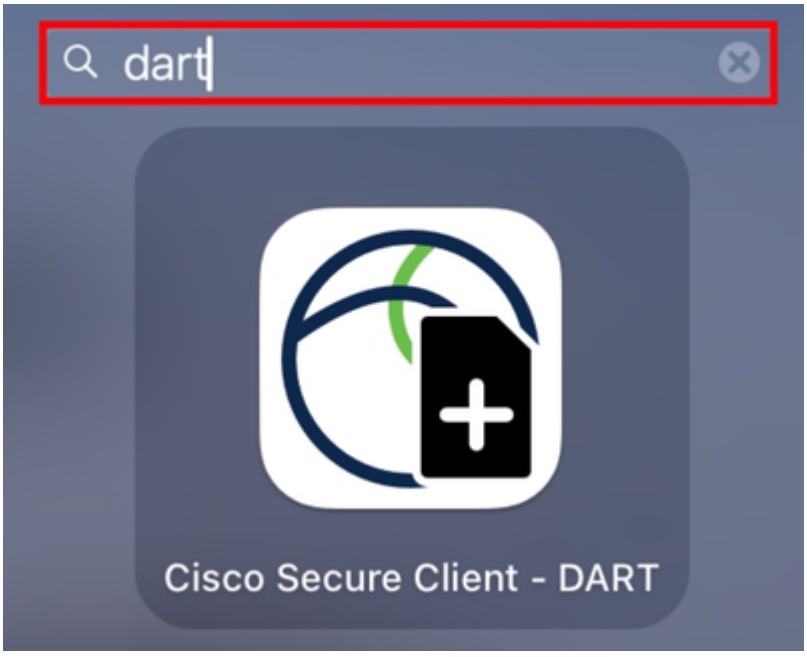
```
open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

- Activez Duo en mode débogage.

- Début Wireshark Capture.
- Sélectionnez toutes les interfaces et lancez la capture de paquets.

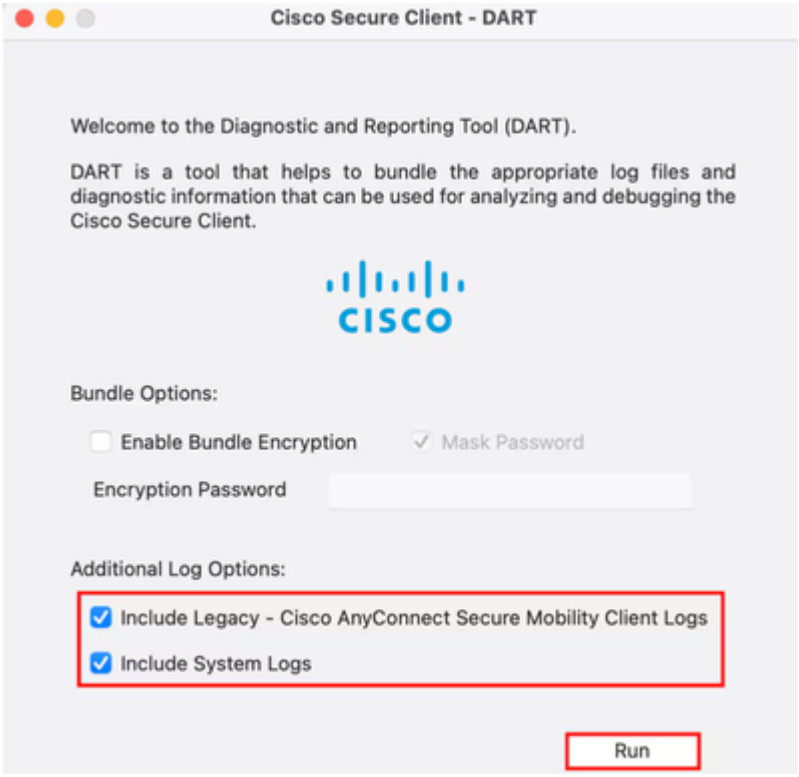


- Reproduisez le problème, enregistrez-le KDF LogsWireshark Captureet suivez les étapes de capture DART Bundle.
- Ouvrez le Cisco Secure Client - DART.



- Cochez les options suivantes :
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs.

    - Include System Logs.
- Cliquer Run.



Remarque : Collectez tous les journaux : Journaux KDF, offre groupée de capture Wireshark et DART au dossier TAC.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Centre d'aide Cisco Secure Access
- Guide de conception Cisco SASE
- Collecte des journaux KDF pour le client sécurisé sous Windows et MacOS

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.