

Configuration des journaux KDF pour le client sécurisé sous Windows et MacOS

Table des matières

[Introduction](#)

[Indicateurs Windows et MacOS](#)

[Collecte des journaux KDF, offre groupée Wireshark et DART](#)

[Fenêtres](#)

[MacOS](#)

[Informations connexes](#)

Introduction

Ce document décrit comment collecter les journaux KDF et d'autres journaux de dépannage importants sur Windows et MacOS.

Indicateurs Windows et MacOS

DNS Related (Quand OpenDNS est impliqué) :	0x20801FF
Proxy de flux Web (SWG) et DNS associés :	0x70C01FF
ZTA	0x400080152

Collecte des journaux KDF, offre groupée Wireshark et DART



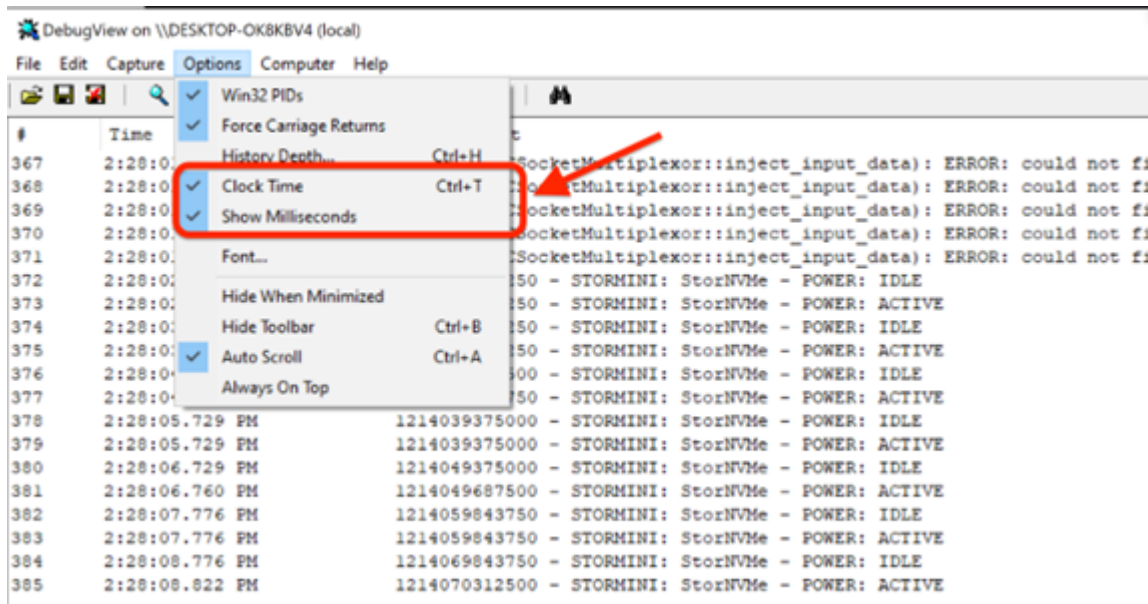
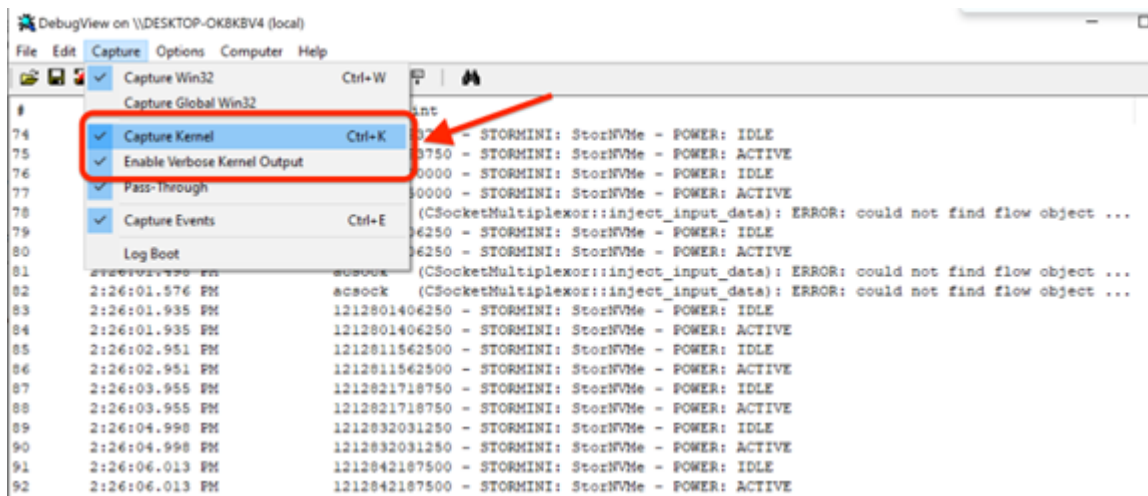
Remarque : Lorsque vous soumettez les résultats, faites toujours savoir à l'équipe TAC quels paramètres ont été utilisés et soyez prêt à les modifier selon les besoins du TAC.

Fenêtres

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

"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf [FLAG]

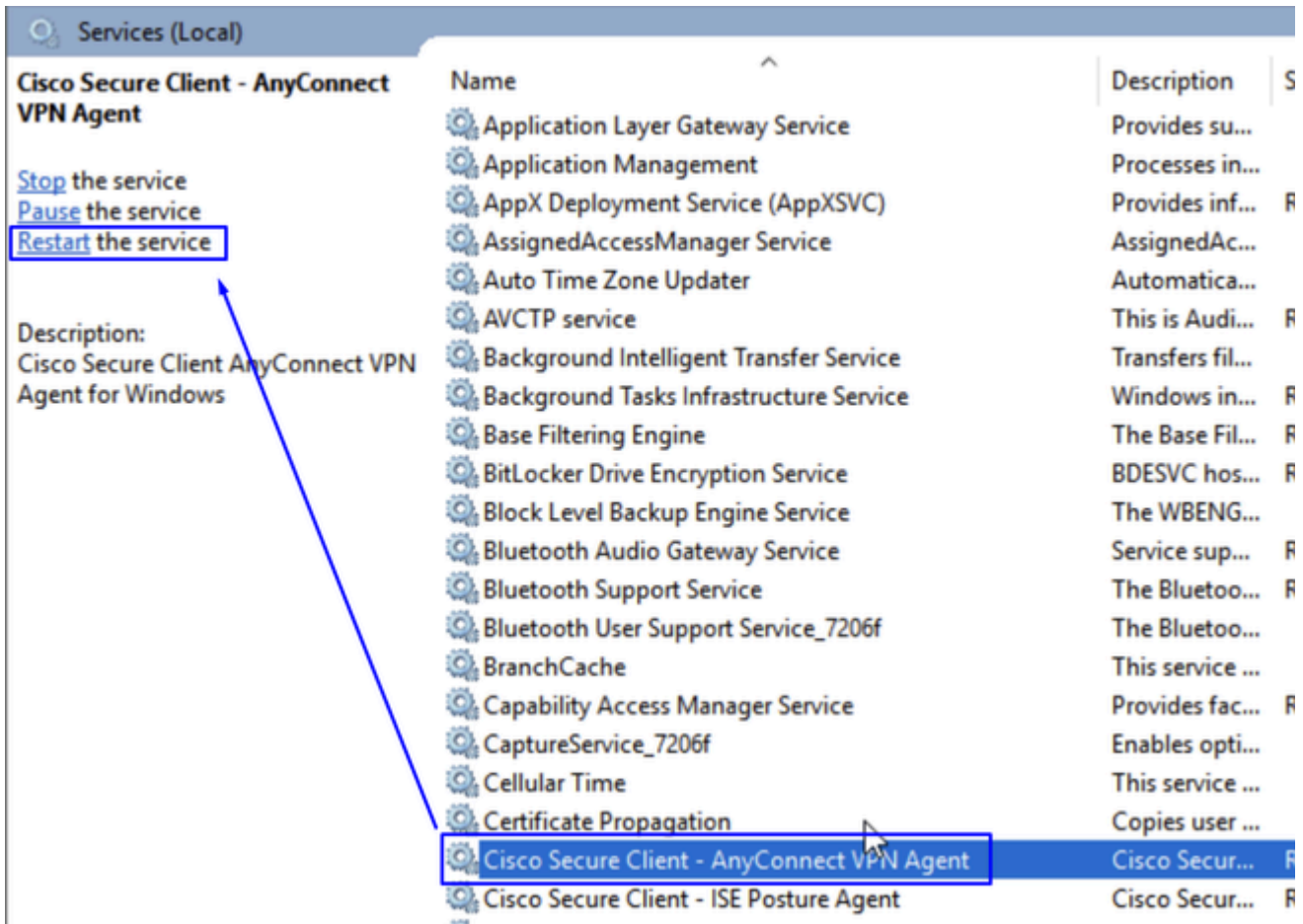
- Téléchargez [DebugView](#) depuis SysInternal pour capturer le journal KDF.
- Exécuter DebugView en tant que administrator et activer les options de menu suivantes.
- Cliquez sur Capture.
 - Coche Capture Kernel.
 - Coche Enable Verbose Kernel Output.
- Options
 - Coche Clock Time.
 - Coche Show Milliseconds.



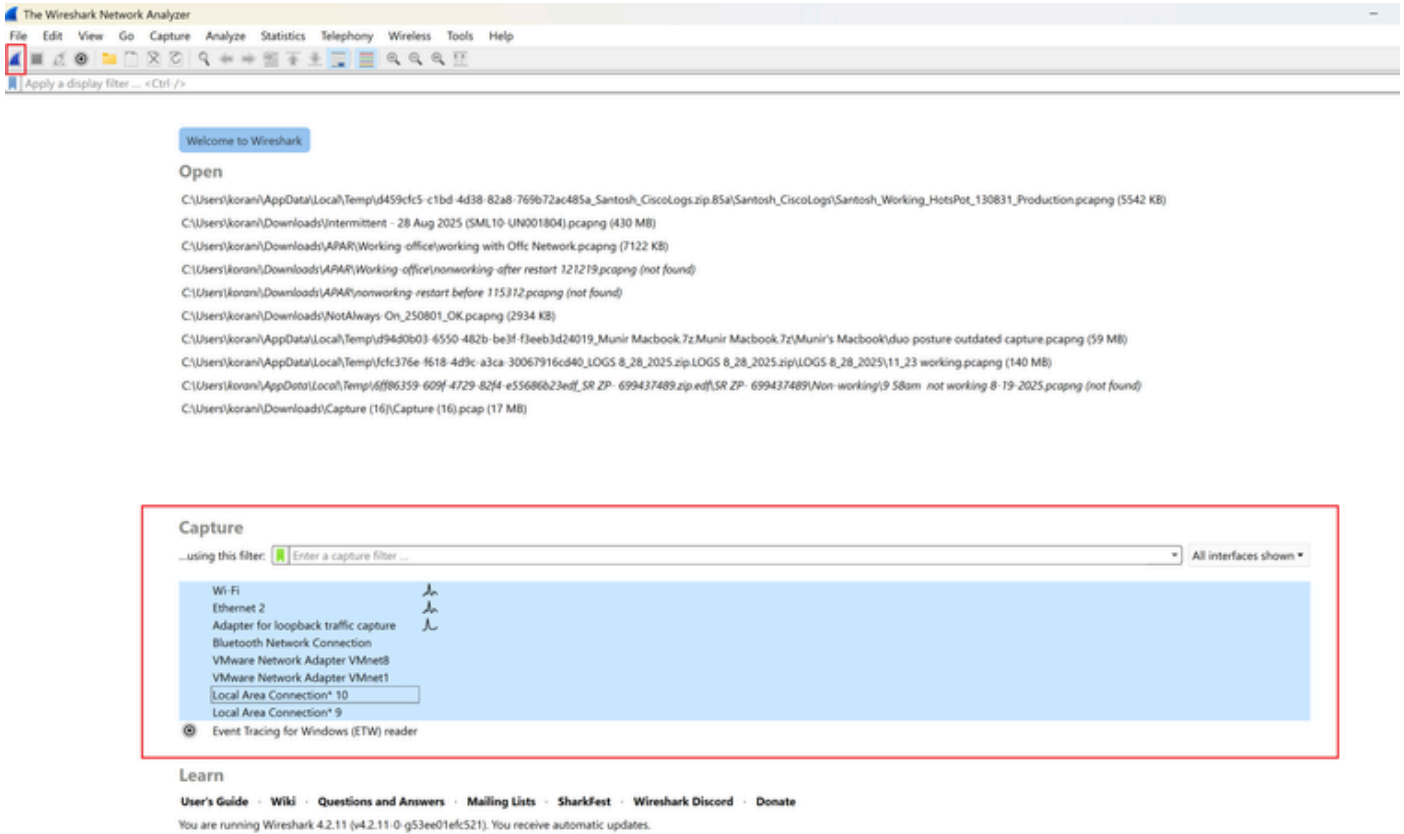
- Redémarrez le service client via l'invite admin :

net stop csc_vpnagent && net start csc_vpnagent

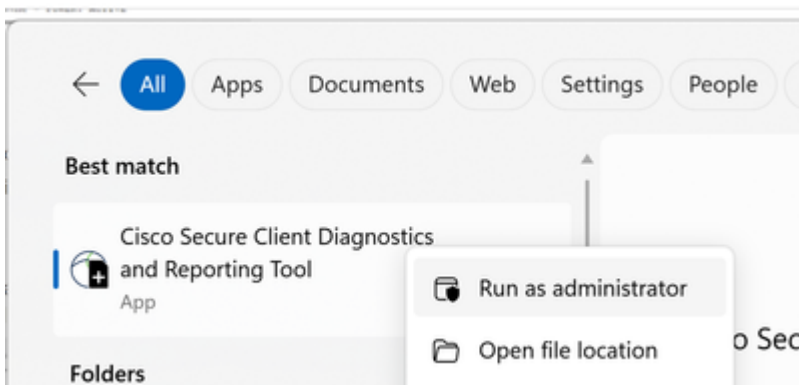
- Si `net stop csc_vpnagent && net start csc_vpnagent` ne fonctionne pas, redémarrez Cisco Secure Client le service à partir de `services.msc`.



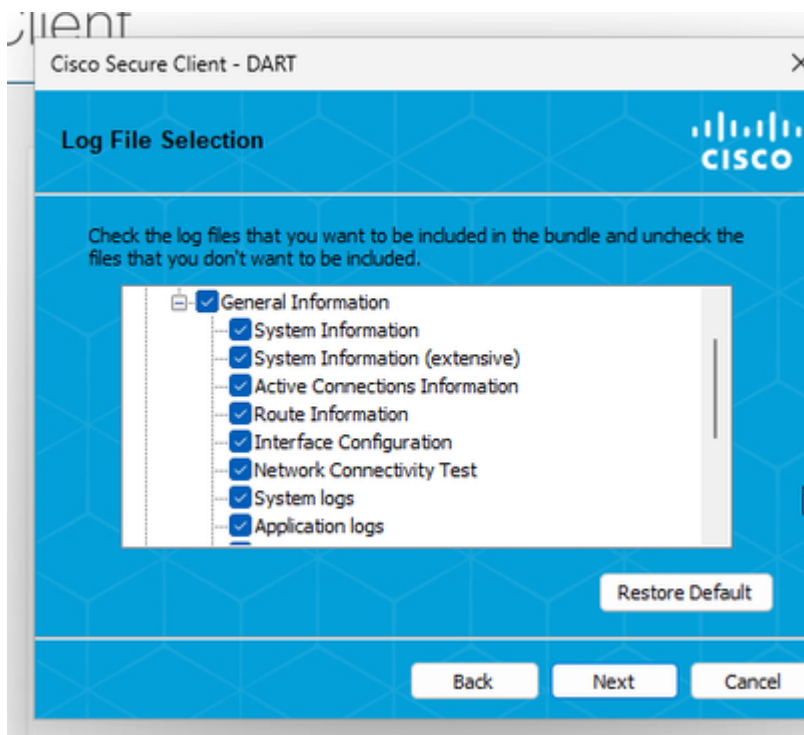
- Début Wireshark Capture.
- Sélectionnez toutes les interfaces et lancez la capture de paquets.



- Reproduisez le problème, enregistrez KDF Logs et Wireshark Capture, puis 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.



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

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

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

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
```

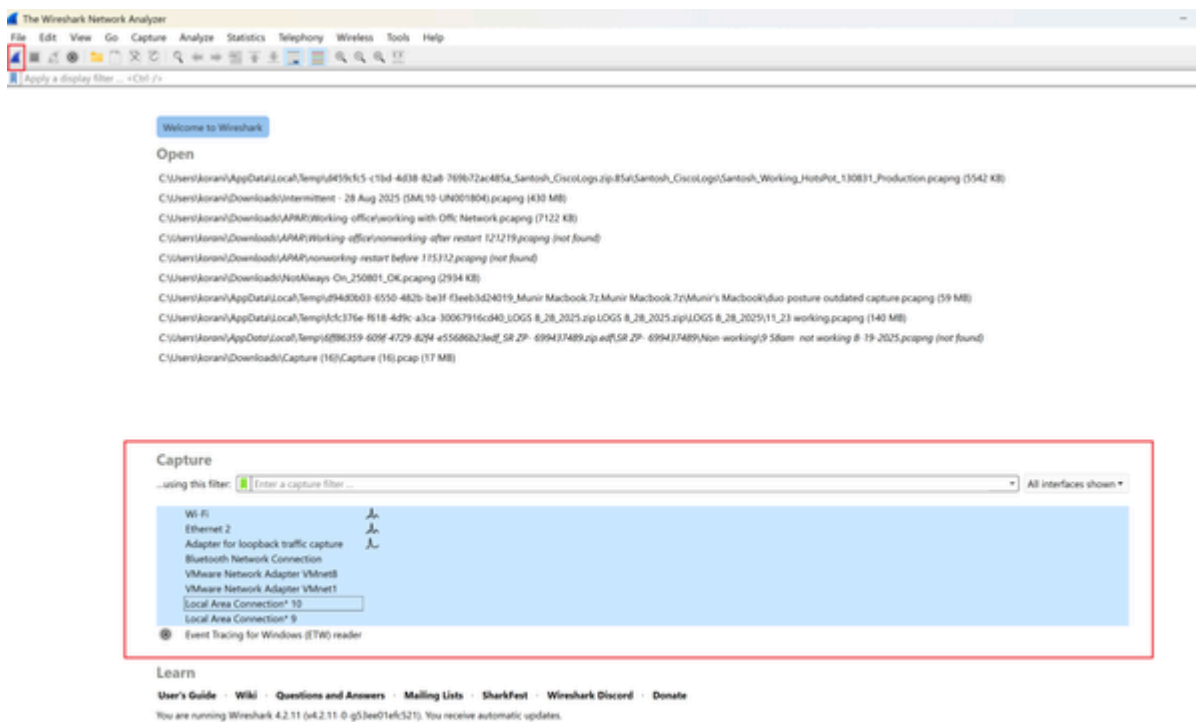
- Enable Flag.

```
echo debug=[Flag Value] | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

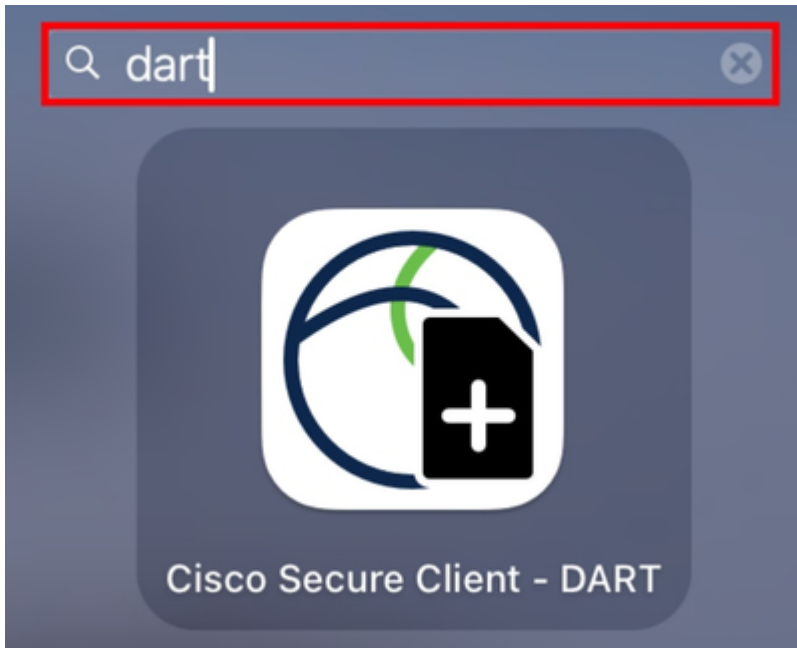
- Start Service.

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

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



- Reproduisez le problème, enregistrez KDF Logs et Wireshark Capture, puis 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](#)

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.