Recopilación de registros KDF para Secure Client en Windows y MacOS

Contenido

Introducción

Este documento describe cómo recopilar registros de KDF y otros registros importantes de solución de problemas en Windows y MacOS.

INDICADORES de Windows y MacOS

DNS relacionado (cuando OpenDNS está involucrado):	0x20801FF
Proxy de flujo web (SWG) y DNS Relacionados:	0x70C01FF
ZTA	0x400080152

Recopilación de registros de KDF, Wireshark y DART Bundle

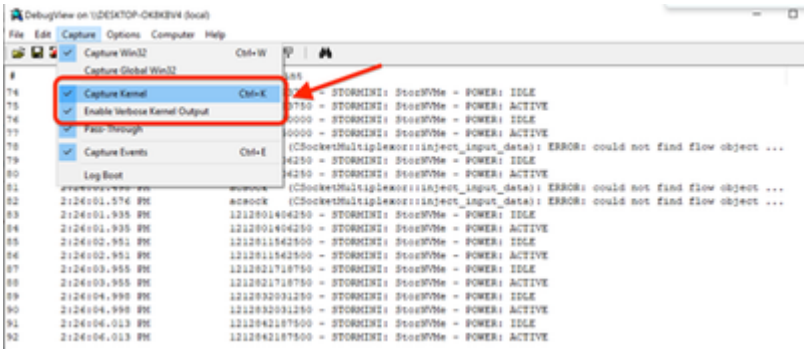
Nota: Cuando envíe los resultados, infórmele siempre al equipo del TAC qué parámetros se han utilizado y esté abierto a cambios según lo requiera el TAC.

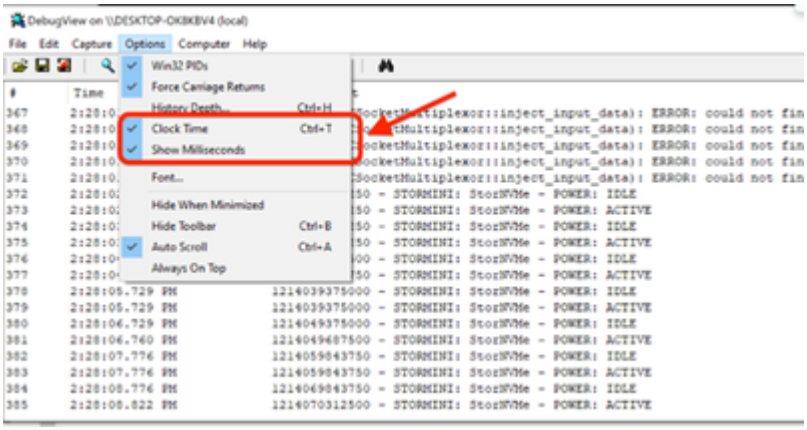
Windows:

Abra un CMD con privilegios de administrador y ejecute el siguiente comando:

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

- Descargue DebugView de SysInternal para capturar el registro KDF
- Ejecutar DebugView como administrator y activar las siguientes opciones de menú:
- Haga clic en Capturar
    - Marca de verificación Capture Kernel
    - Marca de verificación Enable Verbose Kernel Output
- Opciones
    - Marca de verificación Clock Time
    - Marca de verificación Show Milliseconds

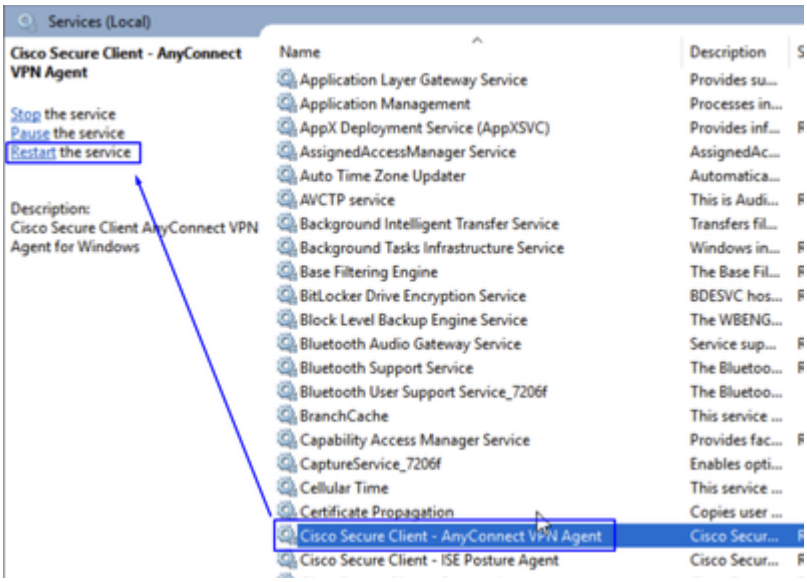




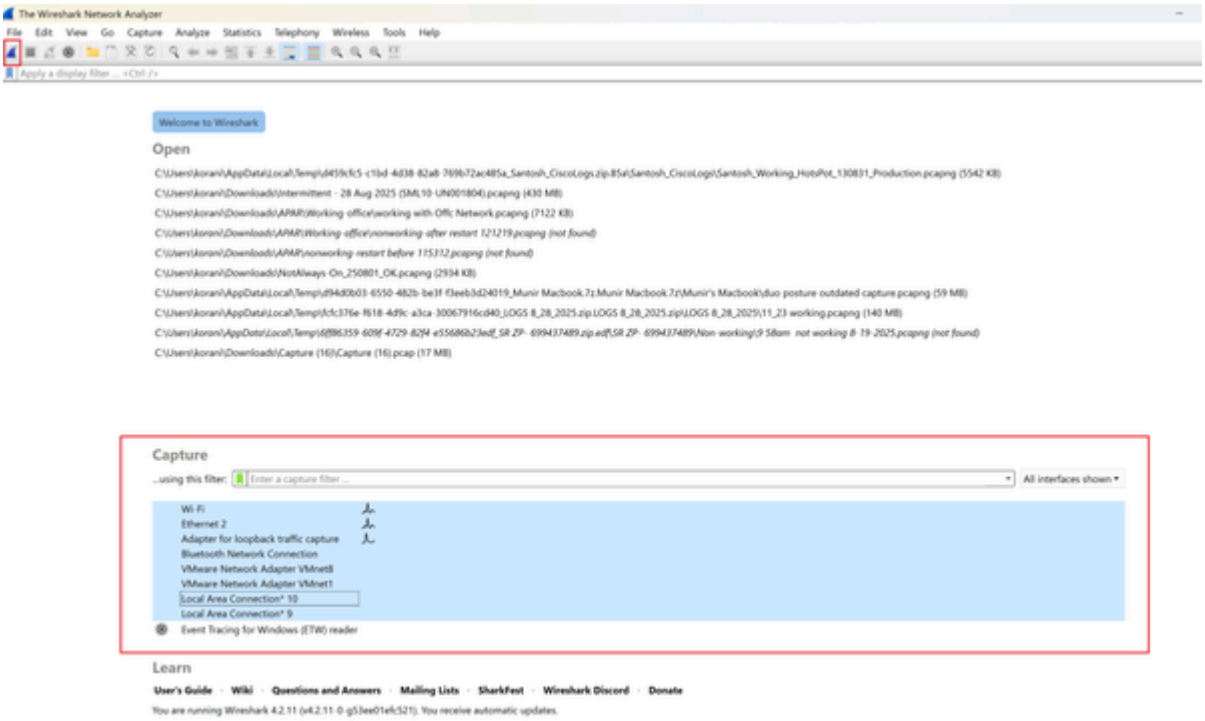
- Reinicie el servicio de cliente a través del prompt admin:

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

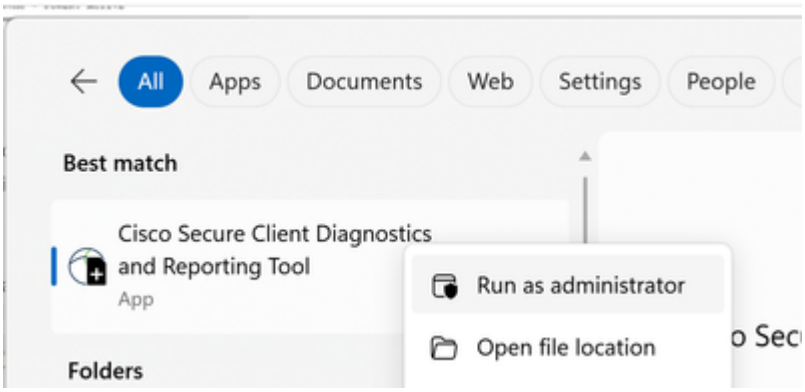
- Si net stop csc_vpnagent && net start csc_vpnagent no funciona, reinicie el Cisco Secure Client servicio desde services.msc



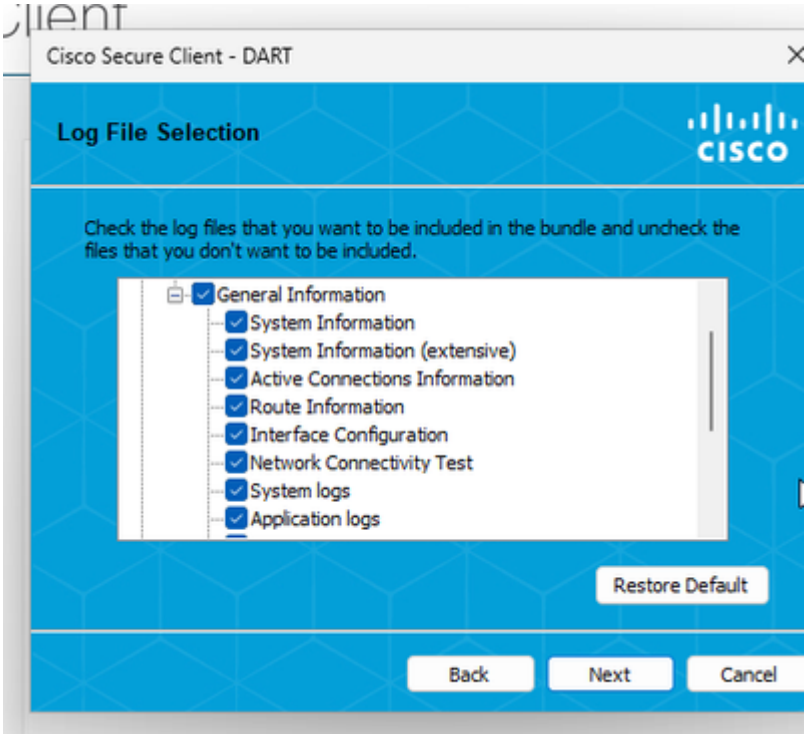
- Inicio Wireshark Capture
- Seleccione todas las interfaces e inicie la captura de paquetes



- Reproduzca el problema y guarde KDF Logs y Wireshark Capturedespués siga los pasos para capturar DART Bundle
- Abra el con Cisco Secure Client Diagnostics & Reporting Tool (DART) privilegios de administrador



- Haga clic en Custom
  - Incluir System Information Extensive y Network Connectivity Test



Nota: Recopile todos los registros, registros KDF, captura Wireshark y paquete DART en el caso TAC.

- Para detener el registro de KDF en Windows, utilice el siguiente comando:

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

MacOS

Abra el terminal y siga la siguiente cadena de comandos para habilitar el registro de KDF en

MacOS:

- Stop Service

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

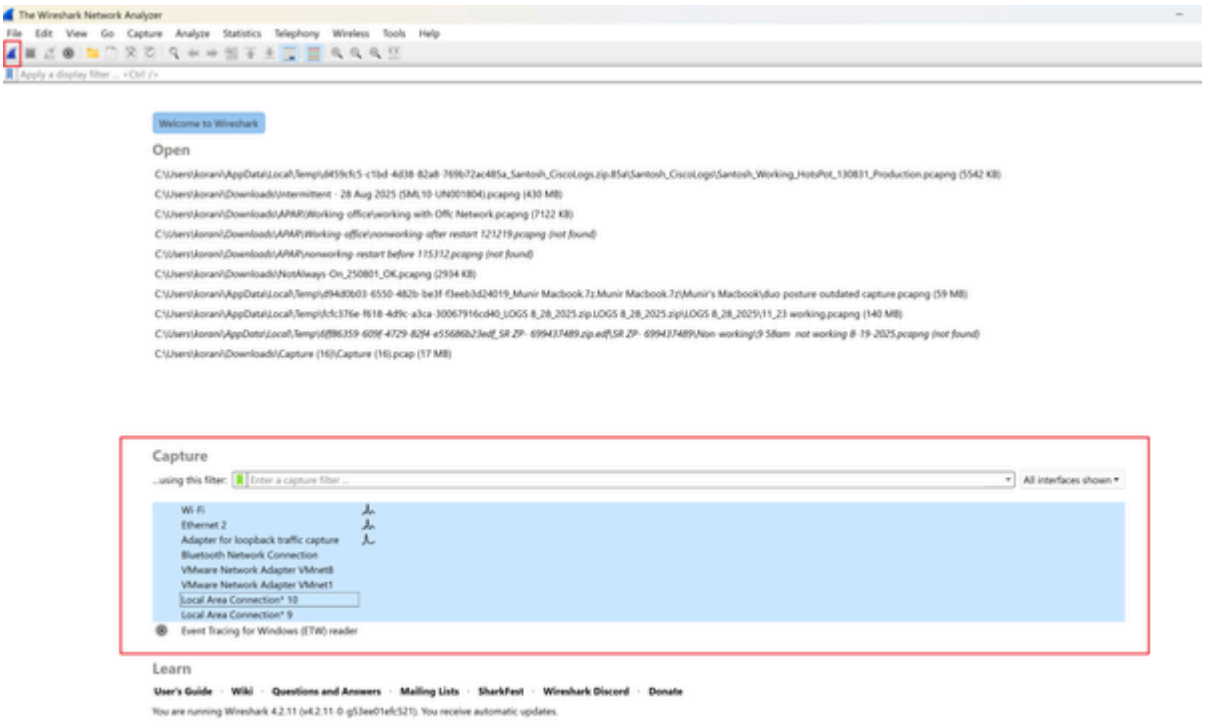
- Enable Flag

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

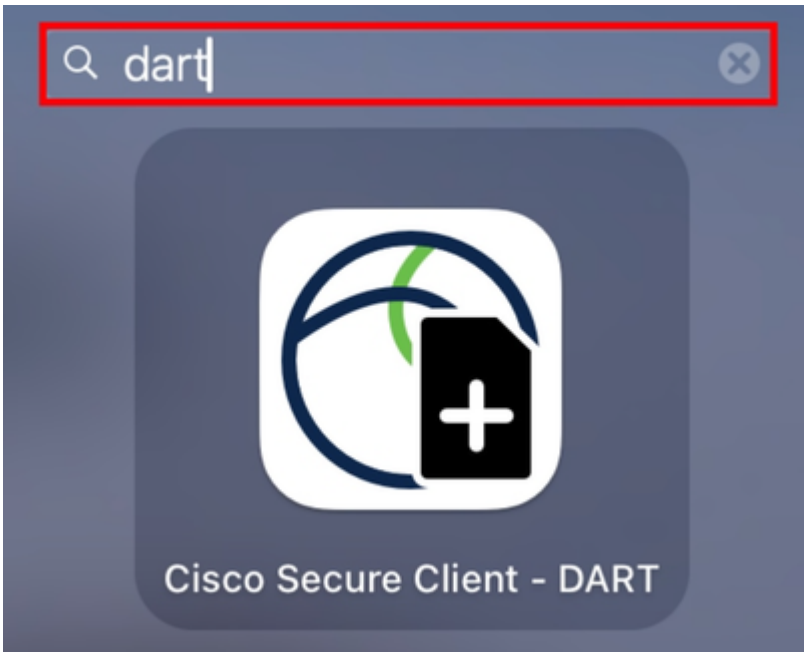
- Start Service

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

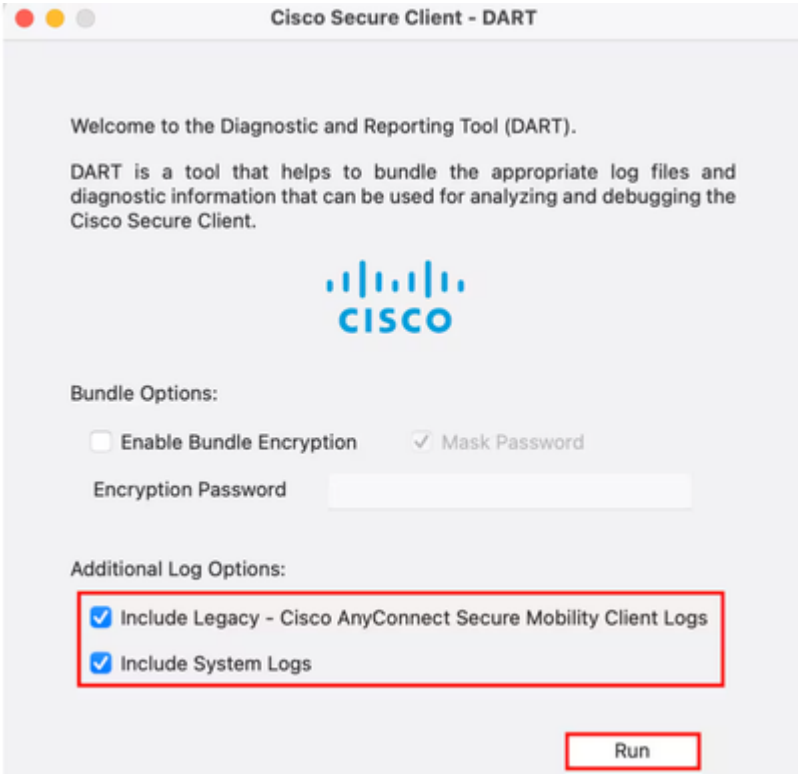
- Inicio Wireshark Capture
- Seleccione todas las interfaces e inicie la captura de paquetes



- Reproduzca el problema y guarde KDF Logs y Wireshark Capturedespués siga los pasos para capturar DART Bundle
- Abra el Cisco Secure Client - DART



- Marque las siguientes opciones:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- Haga clic en Run



Nota: Recopile todos los registros, registros KDF, captura Wireshark y paquete DART en el caso TAC.

Información Relacionada

- Soporte técnico y descargas de Cisco
- Centro de ayuda de Cisco Secure Access
- Guía de diseño de Cisco SASE

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).