Recopilar registros detallados de ZTNA para la resolución de problemas

Contenido

Introducción

Este documento describe cómo recopilar registros detallados de resolución de problemas de ZTA, cuándo habilitar y paso a paso.

Antecedentes

A medida que las organizaciones adoptan cada vez más la arquitectura Zero Trust Architecture (ZTA) para proteger a los usuarios, los dispositivos y las aplicaciones, la resolución de problemas de conectividad y aplicación de políticas se ha vuelto más compleja. A diferencia de los modelos tradicionales basados en perímetro, ZTA se basa en múltiples decisiones en tiempo real a través de la identidad, el estado del dispositivo, el contexto de la red y los motores de políticas basados en la nube. Cuando surgen problemas, los registros de alto nivel suelen ser insuficientes para identificar la causa raíz.

La recopilación de seguimiento detallado del nivel de ZTA desempeña un papel fundamental a la hora de obtener una mayor visibilidad del comportamiento de los clientes, la evaluación de políticas, la interceptación del tráfico y las interacciones de los servicios en la nube. Estos seguimientos permiten a los ingenieros ir más allá de la resolución de problemas basada en síntomas y analizar la secuencia exacta de eventos que conducen a fallos de acceso, degradación del rendimiento o resultados de políticas inesperados.

Recopilación de registros

Verificaciones previas antes de abrir un caso TAC

Estas comprobaciones previas ayudarán al equipo del TAC a identificar el problema de forma más eficaz. Proporcionar esta información a los ingenieros les ayudará a resolver el problema lo antes posible:

- ¿Cuál es el problema y cuántos usuarios se ven afectados?
- ¿Qué SO y versiones se han visto afectados?
- ¿El problema es constante o intermitente? Si es intermitente, ¿es específico del usuario o está generalizado?
- ¿Se inició el problema después de un cambio o ha estado presente desde la implementación?
- ¿Hay algún desencadenante conocido?
- ¿Hay alguna solución alternativa disponible?

Registros para recopilar

- paquete DART
- Registros del modo ZTNA Debug Trace
- Captura de Wireshark (todas las interfaces, incluido el bucle invertido)
- Mensajes de error observados
- Marcas de tiempo del problema
- Captura de pantalla de estado del módulo CSC ZTA
- Nombre de usuario del usuario afectado

En las siguientes secciones se explica cómo activar y recopilar cada uno de estos registros en detalle.

Activar el modo de seguimiento de depuración ZTNA

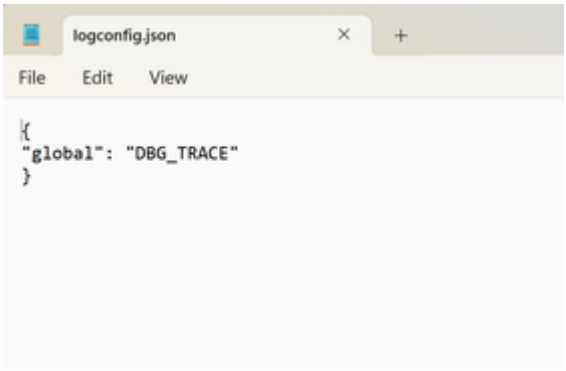
Cree un archivo llamado `logconfig.json` con los detalles a continuación:

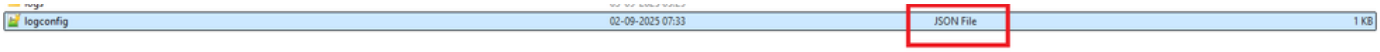
```
{ "global": "DBG_TRACE" }
```

Advertencia: Asegúrese de que el archivo se guarda con el nombre logconfig.json.

Después de crear el archivo, colóquelo en la ubicación adecuada en función del sistema operativo:

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





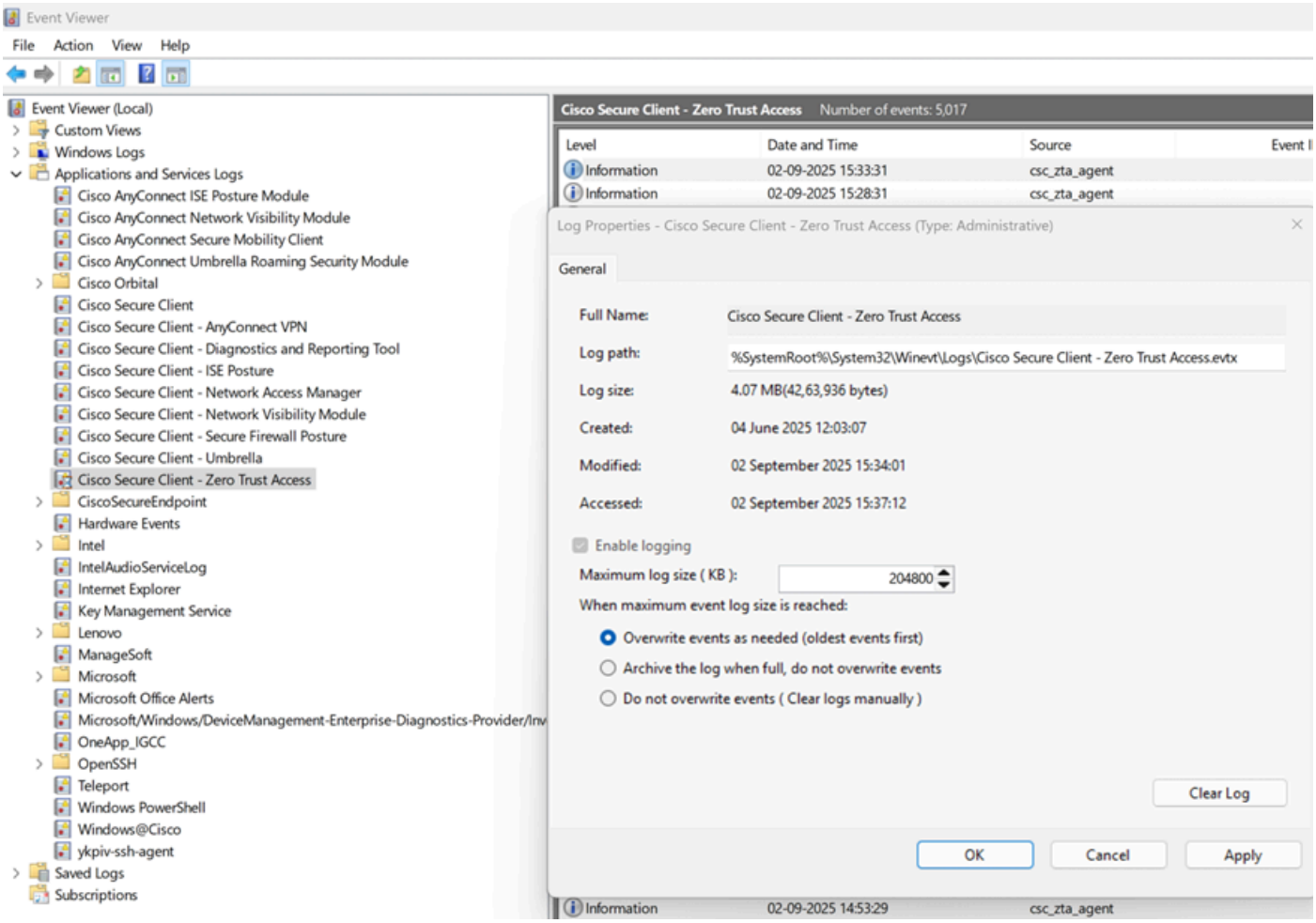
Nota: Una vez que haya creado el archivo especificado, debe reiniciar el servicio Agente de acceso de confianza cero (verifique el paso Reinicio del servicio ZTA). Si no es posible reiniciar el servicio, reinicie el ordenador.

Aumentar el **tamaño del registro ZTA en el Visor de eventos**

En las PC con Windows, después de habilitar el registro de nivel de seguimiento, debe aumentar manualmente el tamaño del archivo de registro ZTA.

1. Abierto.Event Viewer
2. En el panel izquierdo, expanda Applications and Services Logs.
3. Haga clic con el botón derecho Cisco Secure Client – Zero Trust Access y seleccione Properties.
4. En Maximum log size (KB), establezca el valor en 204800 (equivalente a 200 MB).

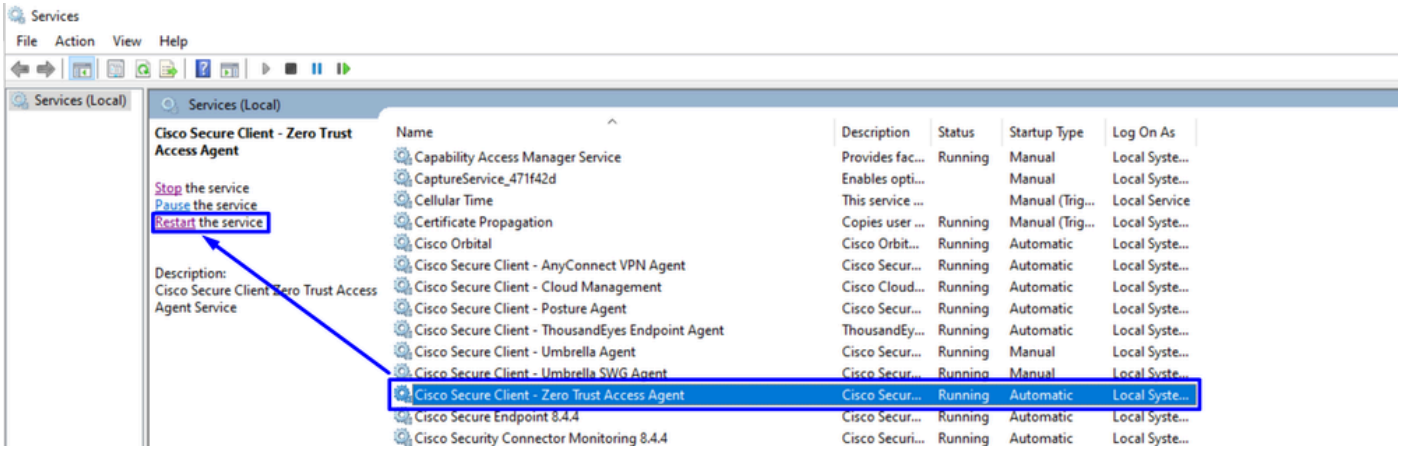
Para finalizar, haga clic en **Apply** y, a continuación OK.



Reiniciando el servicio ZTA

Windows:

- Utilícelo Windows + R para abrir la Run Search escritura services.msc y presione Intro
- Localice el servicio Cisco Secure Client - Zero trust Access Agent y haga clic en Restart. Una vez hecho esto , verifique el estado del módulo CSC ZTA para confirmar que está activo



Nota: Si el servicio ZTA no se puede reiniciar debido a la falta de acceso administrativo,

un reinicio completo del sistema es su siguiente opción.

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: Si los comandos no se pueden ejecutar o el servicio ZTA no se puede reiniciar debido a la falta de acceso administrativo, un reinicio completo del sistema es su siguiente opción.

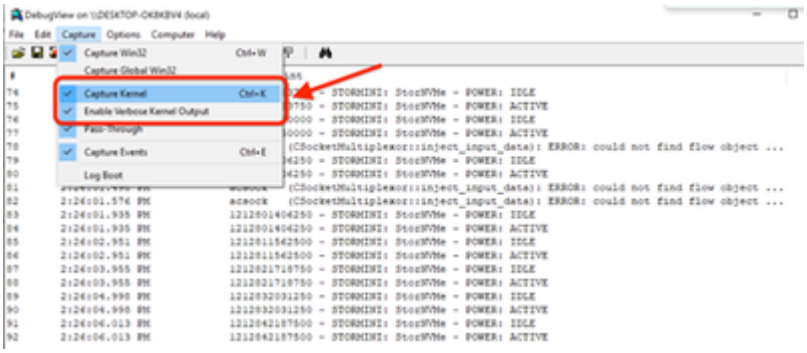
Activar el registro de KDF, la captura de paquetes, el modo de depuración Duo y el paquete Dart

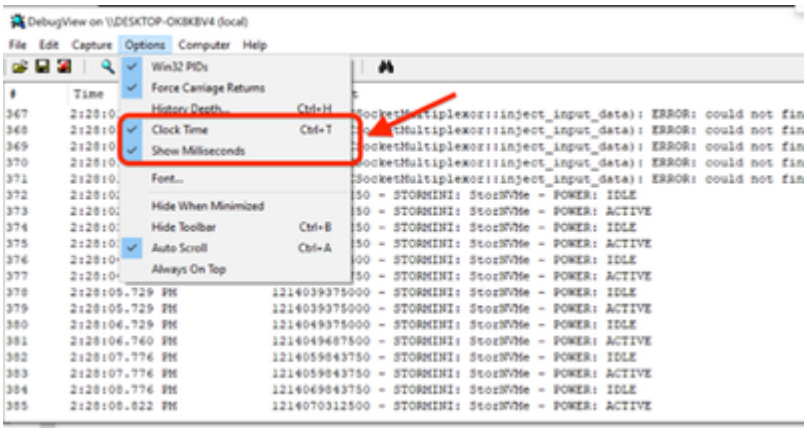
Windows:

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

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

- Descargue DebugView de SysInternal para capturar el registro KDF
- Ejecute DebugViewas administratory habilite 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

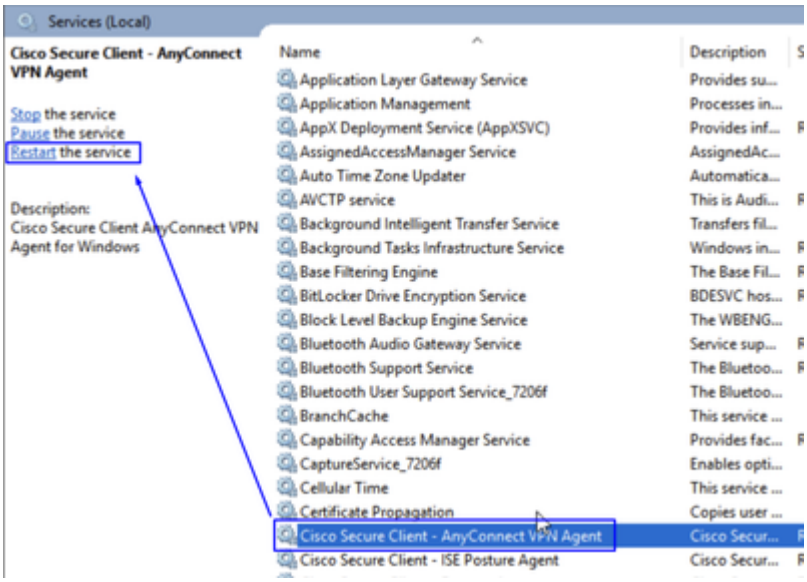




- Reinicie el servicio de cliente a través del prompt admin:

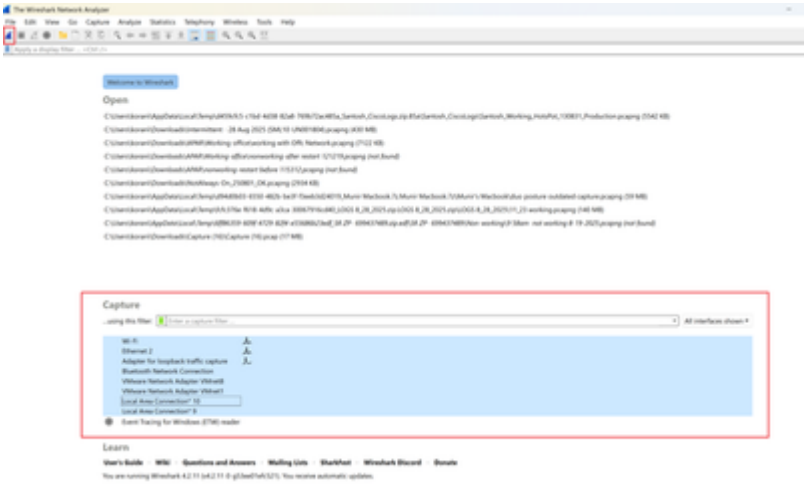
```
net stop csc_vpnagent && net start csc_vpnagent
```

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

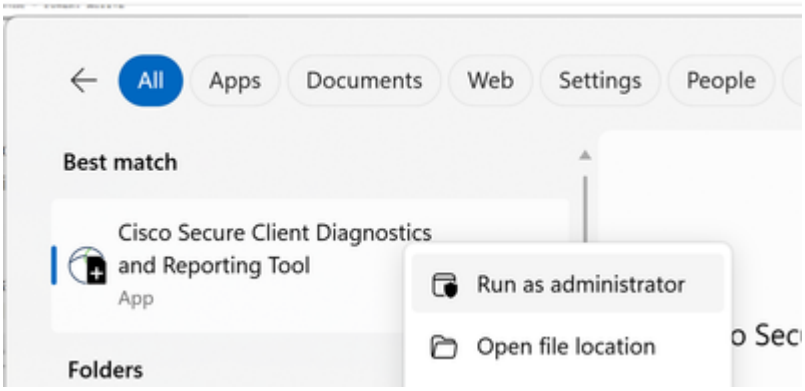


- Activar Duo en modo de depuración
- Inicio Wireshark Capture

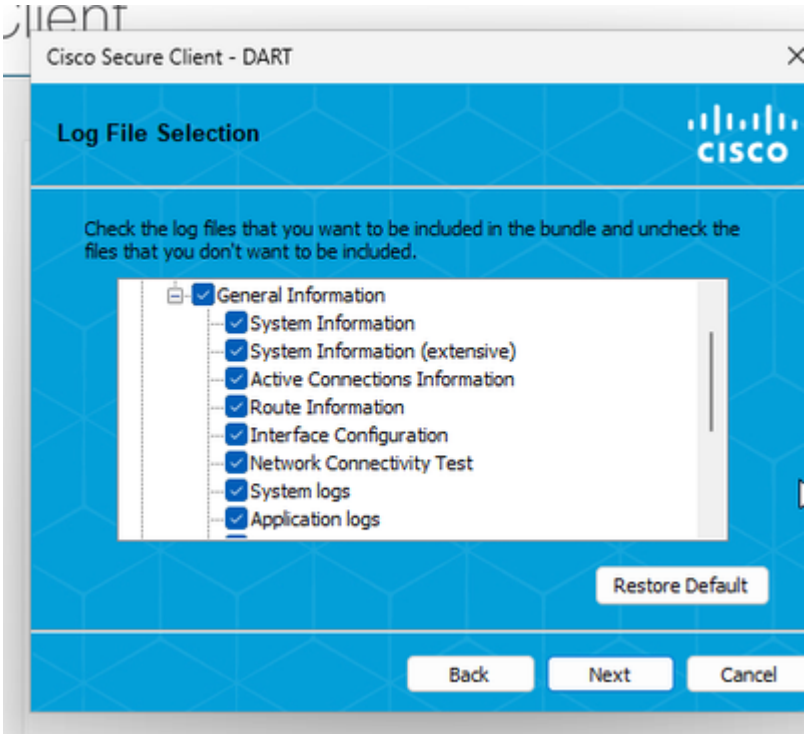
- Seleccione todas las interfaces e inicie la captura de paquetes



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



- Haga clic en Custom
  - Incluir System Information Extensivey Network Connectivity Test



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

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

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

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
```

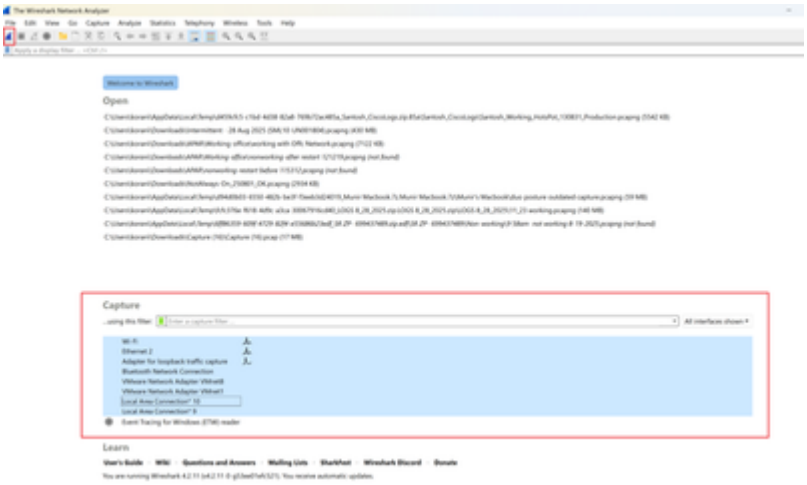
- Enable Flag

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

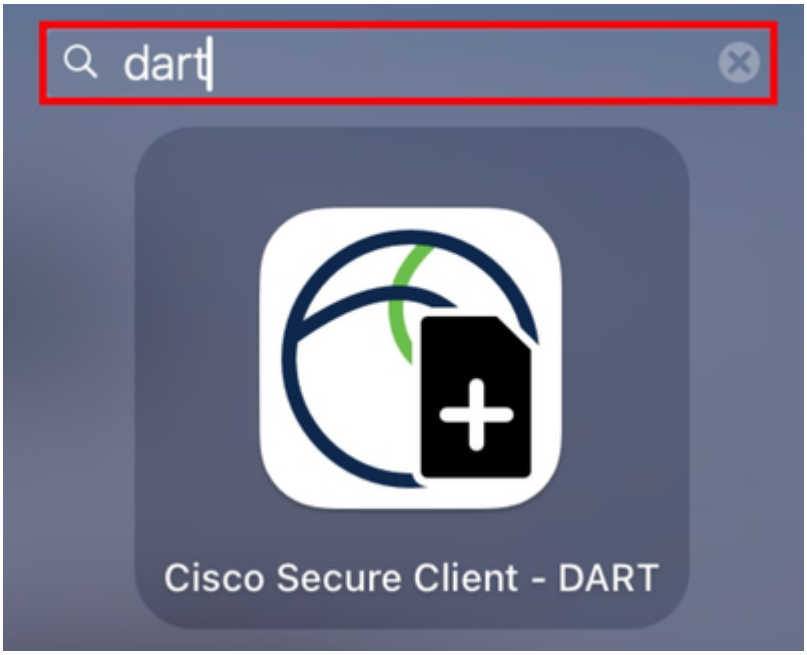
- Start Service

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

- Activar Duo en modo de depuración
- Inicio Wireshark Capture
- Seleccione todas las interfaces e inicie la captura de paquetes

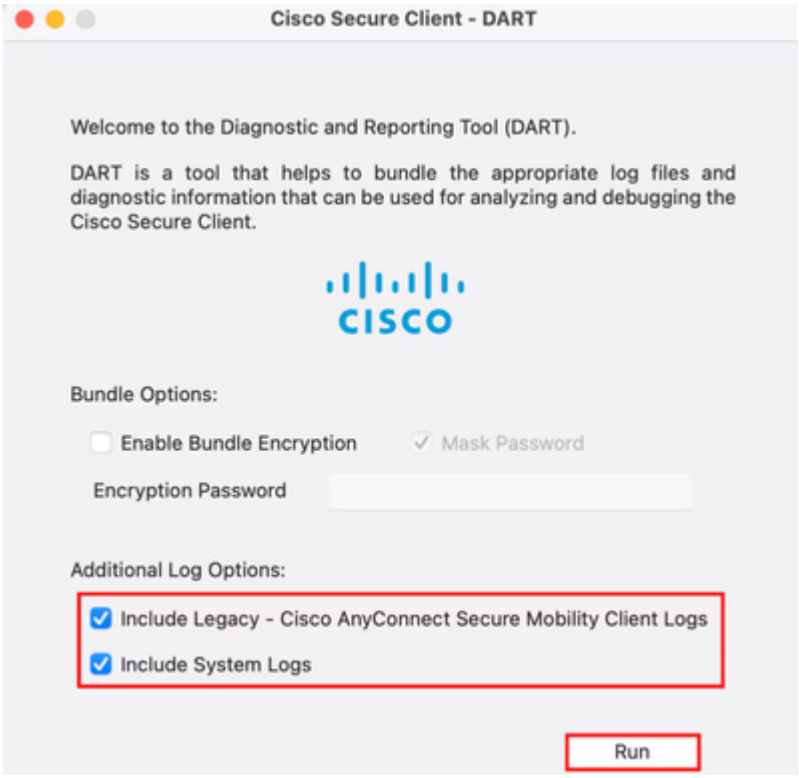


- Reproduzca el problema, guarde KDF LogsyWireshark Capture, y siga los pasos para capturar DART Bundle
- Abra el Cisco Secure Client - DART



- 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
- Recopilación de registros KDF para Secure Client en Windows y MacOS

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).