

# Resolución de problemas de sensores IoX en una implementación de Cyber Vision

## Contenido

[Introducción](#)

[Conexión a la CLI del sensor](#)

[Directorios importantes](#)

[Config.yml](#)

[Capturas PCAP](#)

[Recuperación de archivos del sensor de IoX](#)

[GUI del administrador local](#)

[Copiando archivos a través de TFTP](#)

[Estado del sensor](#)

[Estado](#)

[Estado de procesamiento](#)

[Información crítica en el archivo diag](#)

## Introducción

En este documento se describen los elementos esenciales para solucionar problemas relacionados con la solución IoX Sensor on Cyber Vision.

## Conexión a la CLI del sensor

No se puede acceder directamente a las aplicaciones de los sensores. En primer lugar, debe conectarse al switch a través de SSH. A continuación, utilice el comando show para mostrar la aplicación que se ejecuta en él.

```
Show app-hosting list
```

Valide si la aplicación está instalada y documente su nombre. A continuación, escriba (donde 'ccv\_sensor\_iox\_arch64' es el nombre de la aplicación en este ejemplo)

```
app-hosting connect appid ccv_sensor_iox_aarch64 session
```

## Directorios importantes

### Config.yml

Se trata de un archivo de configuración importante que documenta los parámetros de configuración de flujo, protocolo y puerto. El archivo se puede encontrar en:

/iox\_data/etc/flow

## **Capturas PCAP**

Las capturas que se ejecutan y desencadenan desde la GUI se encuentran en

/iox\_data/var/flow/log/pcap

## **Recuperación de archivos del sensor de IoX**

### **GUI del administrador local**

Desde la GUI del administrador local, navegue hasta la aplicación y, a continuación, la ficha **App-DataDir**™ mostrará los archivos presentes en el directorio /iox\_data/appdata

La pestaña **Registros**™ debajo de la aplicación mostrará los archivos en /iox\_data/logs.

### **Copiando archivos a través de TFTP**

Desde la CLI del sensor, los archivos se pueden copiar a un servidor TFTP remoto mediante el siguiente comando:

```
tftp -p -l /iox_data/appdata/
```

-r

## **Estado del sensor**

En la GUI del centro, vaya a Administration **Sensors** Management (Administración Sensores

Gestión) para ver los detalles del sensor. Éstos son los estados de conexión y procesamiento disponibles

### **Estado**

- Nuevo
- Solicitud pendiente
- Autorizado
- Desconectado
- Conectado
- Desconocido
- SSH

### **Estado de procesamiento**

- No inscrito
- Desconectado
- Esperando datos
- Datos pendientes
  
- Procesamiento normal

### **Información crítica en el archivo diag**

Fecha: informa de la hora a la que se ejecutaron los diagnósticos

Ip\_addr - Informa la dirección IP y la información de red de todas las interfaces configuradas.

Ip\_route - Informa sobre el gateway configurado

Journal\_errors - Informa sobre los servicios que no han podido iniciarse

Journal\_sensorsyncd - Informa sobre la información de conexión TLC

Memoria: informa de la cantidad de memoria que está en uso

sbs-version - Informa sobre la versión principal y la fecha de compilación

sensor-enroll.conf - Informa sobre la IP configurada en el paquete Enrollment

top: informa de 4 comandos "top" en un plazo de 12 segundos ordenados por CPU

## 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).