

排除Cyber Vision部署中的IoX传感器故障

目录

[简介](#)

[连接到传感器CLI](#)

[重要目录](#)

[Config.yml](#)

[PCAP捕获](#)

[从IoX传感器检索文件](#)

[本地管理器GUI](#)

[通过TFTP复制文件](#)

[传感器运行状况](#)

[状态](#)

[处理状态](#)

[诊断文件中的重要信息](#)

简介

本文档介绍使用IoX Sensor on Cyber Vision解决方案时进行故障排除所需的要素。

连接到传感器CLI

不能直接访问传感器应用程序。首先，需要通过SSH连接到交换机。然后，使用show命令列出其上运行的应用程序。

```
Show app-hosting list
```

验证是否已安装应用程序并记录其名称。然后，键入（其中“ccv_sensor_iox_aarch64”是本示例中的应用程序名称）

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

重要目录

Config.yml

它是一个重要的配置文件，记录流量、协议和端口信息配置设置。可在以下位置找到该文件：

```
/iox_data/etc/flow
```

PCAP捕获

从GUI运行和触发的捕获位于

```
/iox_data/var/flow/log/pcap
```

从IoX传感器检索文件

本地管理器GUI

从本地管理器GUI导航到应用，然后“App-DataDir”选项卡将显示/iox_data/appdata目录中的文件

应用下的“日志”选项卡将显示/iox_data/logs中的文件。

通过TFTP复制文件

从传感器的CLI中，可以使用以下命令将文件复制到远程TFTP服务器：

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

传感器运行状况

从Center GUI中，导航到Administration → Sensors (管理) → Management (传感器管理) 以查看传感器详细信息。这些是可用的连接和处理状态

状态

- 新
- 请求挂起
- 已授权
- 已断开连接
- 已连接
- 未知
- SSH

处理状态

- 未注册
- 已断开连接
- 正在等待数据
- 待处理数据

- 正常处理

诊断文件中的重要信息

日期 — 报告运行诊断的时间

Ip_addr — 报告所有已配置接口的IP地址和网络信息。

Ip_route — 报告配置的网关

Journal_errors — 报告未能启动的服务

Journal_sensorsyncd — 报告TLC连接信息

内存 — 报告正在使用的内存量

sbs-version — 报告主版本和生成日期

sensor-enroll.conf — 报告注册包上配置的IP

top — 在12秒内报告4个“top”命令，按CPU排序

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。