

Cyber Vision 구축의 IoX 센서 문제 해결

목차

[소개](#)

[센서 CLI에 연결](#)

[중요 디렉터리](#)

[Config.yml](#)

[PCAP 캡처](#)

[IoX 센서에서 파일 검색](#)

[로컬 관리자 GUI](#)

[TFTP를 통해 파일 복사](#)

[센서 상태](#)

[상태](#)

[처리 상태](#)

[diag 파일의 중요 정보](#)

소개

이 문서에서는 Cyber Vision 솔루션에서 IoX Sensor를 사용할 때 트러블슈팅에 필요한 필수 사항에 대해 설명합니다.

센서 CLI에 연결

센서 애플리케이션은 직접 액세스할 수 없습니다. 먼저 SSH를 통해 스위치에 연결해야 합니다. 그런 다음 show 명령을 사용하여 실행 중인 애플리케이션을 나열합니다.

```
Show app-hosting list
```

응용 프로그램이 설치되어 있는지 확인하고 이름을 문서화합니다. 그런 다음 (여기서 'ccv_sensor_iox_aarch64'는 이 예의 앱 이름)을 입력합니다

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

중요 디렉터리

Config.yml

플로우, 프로토콜, 포트 정보 컨피그레이션 설정을 문서화하는 중요한 컨피그레이션 파일입니다. 파일은 다음 위치에서 찾을 수 있습니다.

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

PCAP 캡처

GUI에서 실행 및 트리거되는 캡처는

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

IoX 센서에서 파일 검색

로컬 관리자 GUI

Local manager GUI에서 앱으로 이동한 다음 'App-DataDir' 탭에 /iox_data/appdata 디렉토리에 있는 파일이 표시됩니다.

앱 아래의 'Logs' 탭에는 /iox_data/logs의 파일이 표시됩니다.

TFTP를 통해 파일 복사

센서의 CLI에서 아래 명령을 사용하여 원격 TFTP 서버에 파일을 복사할 수 있습니다.

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

센서 상태

Center GUI에서 Administration(관리) → Sensors(센서) → Management(관리)로 이동하여 센서 세부사항을 확인합니다. 사용 가능한 연결 및 처리 상태입니다

상태

- 신규
- 요청 보류 중
- 승인
- 연결 끊김
- 연결됨
- 알 수 없음
- SSH

처리 상태

- 등록되지 않음
- 연결 끊김
- 데이터 대기 중
- 보류 중인 데이터

- 정상 처리 중

diag 파일의 중요 정보

Date - 진단 프로그램이 실행된 시간을 보고합니다.

Ip_addr - 구성된 모든 인터페이스의 IP 주소 및 네트워크 정보를 보고합니다.

Ip_route - 구성된 게이트웨이를 보고합니다.

Journal_errors - 시작하지 못한 서비스를 보고합니다.

Journal_sensorsyncd - TLC 연결 정보를 보고합니다.

메모리 - 사용 중인 메모리의 양을 보고합니다.

sbs-version - 주 버전 및 빌드 날짜를 보고합니다.

sensor-enroll.conf - 등록 패키지에 구성된 IP를 보고합니다.

top - 12초 이내에 CPU별로 정렬된 4개의 "top" 명령을 보고합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.