Fehlerbehebung bei IoX-Sensoren in einer Cyber Vision-Bereitstellung

Inhalt

Einleitung

In diesem Dokument werden die wesentlichen Punkte beschrieben, die bei der Arbeit mit der IoX Sensor on Cyber Vision-Lösung zur Fehlerbehebung erforderlich sind.

Herstellen einer Verbindung zur Sensor-CLI

Auf Sensoranwendungen kann nicht direkt zugegriffen werden. Zunächst muss über SSH eine Verbindung zum Switch hergestellt werden. Verwenden Sie dann den Befehl show, um die darauf ausgeführte Anwendung aufzulisten.

```
Show app-hosting list
```

Überprüfen Sie, ob die Anwendung installiert ist, und dokumentieren Sie ihren Namen. Geben Sie dann ein (wobei "ccv_sensor_iox_aarch64" der Name der App in diesem Beispiel ist).

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

Wichtige Verzeichnisse

Konfig.yml

Es handelt sich um eine wichtige Konfigurationsdatei, die Einstellungen für Datenfluss-, Protokoll- und Portinformationen dokumentiert. Die Datei ist zu finden unter:

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

PCAP erfasst

Die von der GUI ausgeführten und ausgelösten Erfassungen befinden sich unter

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

Abrufen von Dateien vom IoX-Sensor

Benutzeroberfläche für lokalen Manager

Navigieren Sie über die lokale Manager-GUI zur App, und zeigen Sie auf der Registerkarte "App-DataDir" die Dateien im Verzeichnis "/iox_data/appdata" an.

Auf der Registerkarte "Logs" (Protokolle) unter der App werden die Dateien in "/iox_data/logs" angezeigt.

Kopieren von Dateien über TFTP

Über die CLI des Sensors können Dateien mit dem folgenden Befehl auf einen Remote-TFTP-Server kopiert werden:

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

```
      -r
```

Sensorzustand

Navigieren Sie in der mittleren GUI zu Administration â†’ Sensors â†’ Management (Administration

Sensoren Management), um die Sensordetails anzuzeigen. Verfügbare Verbindungs- und Verarbeitungsstatus

Status

- Neu
-Anfrage ausstehend
Autorisiert
- Getrennt
- Verbunden
- Unbekannt
SSH

Verarbeitungsstatus

- Nicht angemeldet
- Getrennt
- Warten auf Daten
- Ausstehende Daten

- Normalerweise Verarbeitung

Kritische Informationen in der Diagnosedatei

Datum - Gibt die Zeit an, zu der die Diagnose ausgeführt wurde.

Ip_addr - Meldet die IP-Adresse und Netzwerkinformationen aller konfigurierten Schnittstellen.

IP_route - Konfiguriertes Gateway melden

Journal_errors - Meldet die Dienste, die nicht gestartet werden konnten.

Journal_sensorsyncd - meldet TLC-Verbindungsinformationen

Arbeitsspeicher - meldet den belegten Arbeitsspeicher

sbs-version - Meldet die Hauptversion und das Erstellungsdatum

sensor-enroll.conf - Meldet die im Registrierungspaket konfigurierte IP

top - meldet 4 "top"-Befehle innerhalb von 12 Sekunden sortiert nach CPU

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.