Troubleshoot IoX Sensors on a Cyber Vision deployment

Contents

Introduction

This document describes the essentials needed to troubleshoot when working with the IoX Sensor on Cyber Vision solution.

Connecting to the Sensor CLI

Sensor applications canâ€™t be accessed directly. First, need to connect to the switch through SSH. Then, use the show command to list the application running on it.

```
Show app-hosting list
```

Validate if the application is installed and document its name. Then, type (where 'ccv_sensor_iox_aarch64' is the app name in this example)

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

Important Directories

Config.yml

Itâ€™s an important config file that documents flow, protocol, and port information configuration settings. The file can be found under:

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

PCAP Captures

The captures that are run and triggered from the GUI are under

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

Retrieving files from the IoX Sensor

Local Manager GUI

From the Local manager GUI, navigate to the app, then the â€˜App-DataDirâ€™ tab will show the files present in the/iox_data/appdata directory

The â€˜Logsâ€™ tab under the app will show the files in /iox_data/logs.

Copying Files through TFTP

From the CLI of the sensor, files can be copied to a remote TFTP server using the command below:

```
tftp -p -l /iox_data/appdata/<local-filename> -r <remote-filename> <tftp-server-IP>
```

Sensor Health

From the Center GUI, navigate to Administration â†’ Sensors â†’ Management to look at the Sensor details. These are the connection and processing statuses that are available

Status

-New
-Request pending
-Authorized
-Disconnected
-Connected
-Unknown
-SSH

Processing Status

-Not enrolled
-Disconnected

-Waiting for data
-Pending data

-Normally processing

Critical Information in the diag file

Date â€“ Reports the time when the diagnostics were run

Ip_addr â€“ Reports the IP address & network information of all interfaces configured.

Ip_route â€“ Report the configured gateway

Journal_errors â€“ Reports the services which have failed to start

Journal_sensorsyncd â€“ Reports the TLC connection info

Memory â€“ Reports the amount of memory thatâ€™s in use

sbs-version â€“ Reports the main version and the build date

sensor-enroll.conf â€“ Reports the IP configured on the Enrollment package

top â€“ Reports 4 â€œtopâ€ commands within 12 seconds sorted by CPU