Dépannage des capteurs IoX sur un déploiement Cyber Vision

Table des matières

Introduction

Ce document décrit les éléments essentiels à dépanner lors de l'utilisation de la solution IoX Sensor on Cyber Vision.

Connexion à la CLI du capteur

Les applications de détection ne sont pas accessibles directement. Tout d'abord, vous devez vous connecter au commutateur via SSH. Ensuite, utilisez la commande show pour répertorier l'application qui s'exécute dessus.

```
Show app-hosting list
```

Vérifiez si l'application est installée et documentez son nom. Ensuite, tapez (où « ccv_sensor_iox_aarch64 » est le nom de l'application dans cet exemple)

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

Répertoires importants

Config.yml

Il s'agit d'un fichier de configuration important qui documente les paramètres de configuration des informations de flux, de protocole et de port. Le fichier se trouve sous :

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

Captures PCAP

Les captures qui sont exécutées et déclenchées à partir de l'interface utilisateur graphique sont sous

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

<u>Récupération de fichiers à partir du capteur IoX</u>

Interface graphique du gestionnaire local

À partir de l'interface graphique du gestionnaire local, accédez à l'application, puis l'onglet « App-DataDir » affiche les fichiers présents dans le répertoire /iox_data/appdata

L'onglet « Logs » sous l'application affiche les fichiers dans /iox_data/logs.

Copie de fichiers via TFTP

À partir de l'interface de ligne de commande du capteur, les fichiers peuvent être copiés sur un serveur TFTP distant à l'aide de la commande ci-dessous :

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

```
      -r
```

Santé du capteur

À partir de l'interface utilisateur graphique du Centre, accédez à Administration → Capteurs → Gestion pour consulter les détails du capteur. Il s'agit des états de connexion et de traitement disponibles

Status (état)

-Nouveau
- Demande en attente
-Autorisé
- Déconnecté
- Connecté
-Inconnu
-SSH

État du traitement

- Non inscrit
- Déconnecté
- Attente des données
- Données en attente

- Traitement normal

Informations critiques dans le fichier diag

Date : indique l'heure d'exécution des diagnostics

Ip_addr : indique l'adresse IP et les informations réseau de toutes les interfaces configurées.

Ip_route : signale la passerelle configurée

Journal_errors - Signale les services qui n'ont pas pu démarrer

Journal_sensorsyncd - Signale les informations de connexion TLC

Mémoire : indique la quantité de mémoire utilisée.

sbs-version : indique la version principale et la date de génération

sensor-enroll.conf : indique l'adresse IP configurée sur le package d'inscription

top : affiche 4 commandes « top » en 12 secondes, triées par CPU

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.