Risoluzione dei problemi dei sensori IoX su un'implementazione Cyber Vision

Sommario

Introduzione

Questo documento descrive le caratteristiche essenziali necessarie per risolvere i problemi quando si lavora con il sensore IoX sulla soluzione Cyber Vision.

Collegamento alla CLI del sensore

Non è possibile accedere direttamente alle applicazioni dei sensori. In primo luogo, è necessario collegarsi allo switch tramite SSH. Utilizzare quindi il comando show per elencare l'applicazione in esecuzione su di essa.

```
Show app-hosting list
```

Verificare se l'applicazione è installata e documentarne il nome. Quindi, digitare (dove 'ccv_sensor_iox_arch64' è il nome dell'applicazione in questo esempio)

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

Directory importanti

Simbolo.config

È un file di configurazione importante che documenta le impostazioni di configurazione delle informazioni su flusso, protocollo e porta. Il file è disponibile in:

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

Acquisizioni PCAP

Le clip eseguite e attivate dalla GUI si trovano

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

Recupero di file dal sensore IoX

GUI di Local Manager

Dalla GUI di Gestione locale, passare all'app, quindi la scheda â€˜App-DataDirâ€™ mostrerà i file presenti nella directory/iox_data/appdata

La scheda â€˜Logâ€™ sotto l'app mostrerà i file in /iox_data/logs.

Copia dei file tramite TFTP

Dalla CLI del sensore, i file possono essere copiati su un server TFTP remoto usando il comando seguente:

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

```
      -r
```

Integrità sensore

Dalla GUI di Center, selezionare Amministrazione â†’ Sensori â†’ Gestione per esaminare i dettagli del sensore. Questi sono gli stati di connessione ed elaborazione disponibili

Stato

-Nuovo
-Richiesta in sospeso
-Autorizzato
-Disconnesso
-Connesso
-Sconosciuto
-SSH

Stato elaborazione

-Non registrato
-Disconnesso
-In attesa di dati
-Dati in sospeso

-Elaborazione normale

Informazioni critiche nel file diag

Data: riporta l'ora di esecuzione della diagnostica.

Ip_addr - Riporta l'indirizzo IP e le informazioni di rete di tutte le interfacce configurate.

Ip_route - Segnala il gateway configurato

Journal_errors: segnala i servizi che non sono stati avviati

Journal_sensorsyncd: segnala le informazioni sulla connessione TLC

Memoria: indica la quantità di memoria in uso.

sbs-version - Riporta la versione principale e la data di creazione

sensor-enroll.conf - Segnala l'indirizzo IP configurato nel pacchetto di registrazione

top - Riporta 4 comandi "top" entro 12 secondi ordinati per CPU

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).