Solucionar problemas de sensores de IoX em uma implantação do Cyber Vision

Contents

Introdução

Este documento descreve os elementos essenciais necessários para solucionar problemas ao trabalhar com o sensor IoX na solução Cyber Vision.

Conectando ao Sensor CLI

Os aplicativos de sensor não podem ser acessados diretamente. Primeiro, é necessário conectar-se ao switch através do SSH. Em seguida, use o comando show para listar o aplicativo em execução nele.

```
Show app-hosting list
```

Valide se o aplicativo está instalado e documente seu nome. Em seguida, digite (onde 'ccv_sensor_iox_arch64' é o nome do aplicativo neste exemplo)

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

Diretórios Importantes

Config.yml

É um arquivo de configuração importante que documenta as definições de configuração de fluxo, protocolo e informações de porta. O arquivo pode ser encontrado em:

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

Capturas PCAP

As capturas que são executadas e disparadas a partir da GUI estão sob

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

Recuperando arquivos do sensor IoX

GUI do Gerenciador Local

Na GUI do gerente local, navegue até o aplicativo e a guia "App-DataDir" mostrará os arquivos presentes no diretório /iox_data/appdata

A guia â€˜Logsâ€™ abaixo do aplicativo mostrará os arquivos em /iox_data/logs.

Copiando arquivos através do TFTP

A partir do CLI do sensor, os arquivos podem ser copiados para um servidor TFTP remoto usando o comando abaixo:

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

```
      -r
```

Integridade do sensor

Na GUI do Centro, navegue até Administração â†’ Sensores â†’ Gerenciamento para examinar os detalhes do Sensor. Estes são os status de conexão e processamento que estão disponíveis

Status

-Novo
- Solicitação pendente
-Autorizado
- Desconectado
-Conectado
-Desconhecido
-SSH

Status do Processamento

-Não inscrito
- Desconectado
- Aguardando dados
- Dados pendentes

- Processando normalmente

Informações críticas no arquivo de diagnóstico

Data - Informa a hora em que o diagnóstico foi executado

Ip_addr - Relata o endereço IP e as informações de rede de todas as interfaces configuradas.

Ip_route - Relata o gateway configurado

Journal_errors - Informa os serviços que falharam ao iniciar

Journal_sensorsyncd - Relata as informações de conexão do TLC

Memória - Informa a quantidade de memória que está em uso

sbs-version - Informa a versão principal e a data de compilação

sensor-enroll.conf - Relata o IP configurado no pacote Enrollment

top - Informa 4 comandos "top" em 12 segundos classificados pela CPU

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.