Cisco: IOS

Cisco IOS is an instance of network device log data. IOS is Cisco’s network operating system that runs mainly on their switches and routers. The IOS log data contains information about the operational state of the device and the network functions served by the device.

This data is used for troubleshooting the operations of Cisco devices running IOS. It can be used to confirm configuration settings that influence the functionality the device is expected to deliver. Examples include mismatched duplex settings, up and down state of ports, routing, and operating conditions, such as temperature and power. In the Common Information Model, Cisco IOS can be mapped to any of the following data models, depending on the field: Network Traffic and Change.

Configuration

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Source type: syslog
- Input type: Monitor and HTTP Event Collector
- Add-on or app: Cisco Networks Add-on for Splunk Enterprise
- Sizing estimate: The amount of data ingestion will depend on the number of devices involved and how busy a device is. Estimates at the low end are 5MB/day per device. The best way to know is to test and measure directly in Splunk or at the syslog server.

Validation

If collection is working correctly, the add-on reassigns the cisco:ios source type. Therefore, begin validation with a search for sourcetype=cisco:ios. If data is returned, further validation can be done by inspecting the fields that are extracted.

Application

When your Splunk deployment is ingesting Cisco IOS, you can use the data to achieve the following:

- Managing Cisco devices