Requirement

Docker Sensor Prerequisites

Cisco Cyber Vision 5.1.x and above provides a new way to host sensors. Cyber Vision supports Docker sensors. Docker sensor containers run on a Linux operating system. This guide lists the supported operating systems and software.

- Hardware
  - x86-64 and aarm64 devices
  - Memory: Ensure 4G of memory is available for the container.
  - Network Interface Card (NIC): The Cisco Cyber Vision Docker sensor uses promiscuous mode based on a Docker macvlan interface (passthru mode). Not all adapters are compatible. Cisco supports only Intel network adapters.
- Supported host operating systems: Ubuntu Desktop or Server versions 20.04, 22.04, and 24.04
- Docker version: 27.0 and above
- Cisco Cyber Vision release: 5.1.x and above.
- Configure the host Linux operating system with access to the CLI (ssh).
- To deploy the Docker sensor, the Linux host must have access to the center (collection interface).

Docker Sensor Definitions

- **Cisco Cyber Vision Center**: The Center receives metadata from sensors and stores it in an internal database (PostgreSQL). The Center manages all sensors.

- **Docker**: It is an open platform for developing, shipping, and running applications. It allows you to package and run an application in a loosely isolated environment called a container. Cyber Vision supports Docker.
- **Host / Linux Host**: Cyber Vision supports Docker running on Linux OS (Ubuntu V20.04, 22.04 and 24.04).
- **Docker Container**: A container is a runnable instance of an image. You can create, start, stop, move, or delete a container using the Docker API or CLI.
- **Docker Images**: An image is a read-only template with instructions for creating a Docker container.
- **Docker Compose**: Docker Compose uses a YAML configuration file, called the Compose file, to configure application services. Use the Compose CLI to create and start all services from your configuration.
- **Compose File**: The Compose file, or compose.yaml file, follows the Compose Specification rules to define multicontainer applications.
- **Docker Image Registry**: A registry centralizes the storage and management of container images. A repository collects related container images within a registry. It functions like a folder organizing images based on projects. Each repository contains one or more container images.

Cisco Cyber Vision Docker Sensor Characteristics

The Cisco Cyber Vision 5.1.x Docker sensor has specific characteristics compared to other Cisco Cyber Vision sensor types:

- There are two different Docker images:
  - A passive image includes flow, DPI service, and Snort (NIDS).
  - An active image contains only the Active Discovery service.
- Deploy multiple Docker images on the same host to support both active and passive sensors or to manage multiple capture interfaces. For example, use this setup to receive several ERSPANs. Each passive container has one capture interface.
- Each container consumes one deployment token, even if they run on the same host.
- The persistent directory is /data instead of /iox_data.
- eth0 is behind NAT.
- Use eth1 for Active Discovery (instead of eth2 on IOx).
- The deliverable is in the form of a Docker Compose file, which specifies a Docker image that is hosted on the Center. It comes with the correct networks, environment variables, volume, and so on.
- Containers have no default resource limitations and can consume all host resources. Use the commented lines in the compose.yml file to limit CPU and RAM usage.
- Active and Capture Interfaces that declared in the compose file must exist.
- Disk usage grows if there is a Center communication issue.

Cyber Vision Docker Sensor Architecture and Network Settings Recommendations

The Docker host must be able to communicate with the Cisco Cyber Vision Center on interface eth0. The Docker sensor must be able to communicate with the Cisco Cyber Vision Center:

- For a single interface, use eth0.
- For a dual interface, use eth1.

The host interface that reaches the center allows the sensor container to communicate with it.

The Cyber Vision Docker sensor deployment uses Docker Compose and leverages the Cyber Vision sensor ZTP feature. A Docker application pull requests a connection with the center. The first sensor connection that is established through the ZTP feature also requests a connection with the center.

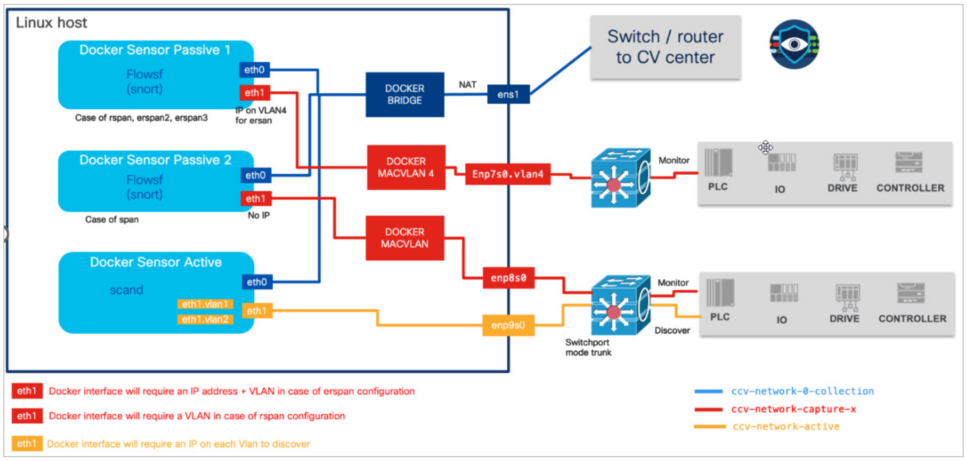
The sensor, once deployed, regularly sends results of DPI, NIDS, or Active Discovery to the center. It requires a valid communication path to the center.

The sensor has other interfaces that are described below:

- The passive container includes an extra interface connected to a Docker macvlan network in passthru mode, making it promiscuous with a host interface. This interface is used for data collection (SPAN, RSPAN, ERSPAN).
- The active container includes one or several extra interfaces, all connected to a Docker macvlan network in passthru mode, making them promiscuous with a host interface. These interfaces are used for the active discovery of OT networks.

The host networking equipment must handle "promiscuous mode," where one physical interface can have multiple MAC addresses. Not all physical network interfaces support this mode.

Basic schema of the network connections used by CV sensor docker container:



This is an example of a host with two passive Docker sensors (to monitor two different sources of traffic) and one active Docker sensor that can discover two VLANs.