Cisco Cyber Vision Sensor VM Installation Guide, Release 5.5.x

Cisco Cyber Vision
Updated September 11, 2026

Topics included

1 Cisco Cyber Vision Sensor VM....4

Sensor VM overview....5
Cisco Cyber Vision sensor overview....6
Deploying Sensor VM on VMware ESXi....7
Deploying Sensor VM on Microsoft Hyper-V....8

2 Set up Cisco Cyber Vision Sensor VM on ESXi....12

Requirements....13
Sensor VM prerequisites....13
Network interface requirements....14
Initial Configurations....16
Sensor VM traffic capture methods....16
Enable Promiscuous Mode to receive mirrored traffic....18
Active Discovery VLAN configuration....19
Sensor VM deployment....21
Configure a Sensor VM in Cisco Cyber Vision Center....21
Deploy Sensor VM on VMware ESXi....24
Verify Sensor VM deployment status and connectivity in Cisco Cyber Vision....25

3 Set up Cisco Cyber Vision Sensor VM on Hyper-V....26

Requirements....27
Sensor VM prerequisites....27
Network interface requirements....28
Initial Configurations....29
Sensor VM traffic capture methods....30
Configure Port Mirroring to receive mirrored traffic....32
Active Discovery VLAN configuration....33
Sensor VM deployment....35
Configure Sensor VM in Cisco Cyber Vision....35
Deploy Sensor VM on Hyper-V....38
Verify Sensor VM deployment status and connectivity in Cisco Cyber Vision....39

4 Sensor configuration....40

Configure Active Discovery....41
Sensor configuration template....41
Templates....41
Create templates....42
Export templates....43

Import templates....43
Capture mode....44
Set a capture mode....44

5 Maintenance....46
Sensor self-update....47
Upgrade sensor....47
Update multiple sensors....47

6 Troubleshooting....50
Troubleshoot sensor update failures....51
Sensor VM deployment issues....52
Sensor VM deployment risks and mitigations....53

1 Cisco Cyber Vision Sensor VM

Topics:

- Sensor VM overview
- Cisco Cyber Vision sensor overview
- Deploying Sensor VM on VMware ESXi
- Deploying Sensor VM on Microsoft Hyper-V

Outlines the Cisco Cyber Vision Sensor VM, describing its purpose and functionality, sensor architecture, and step-by-step deployment procedures for standard environments and for installation within Hyper-V virtualization platforms.

Sensor VM overview

Explains how Sensor VMs operate in Cisco Cyber Vision to simplify sensor deployment, architecture, and network traffic monitoring.

The Cisco Cyber Vision Sensor VM is a virtual-machine-based sensor deployment option that simplifies sensor deployment in Cisco Cyber Vision environments. It enables administrators to deploy sensors, ensure network traffic visibility, and integrate the sensor with Cisco Cyber Vision Center for industrial network security monitoring.

The Sensor VM uses the same deployment image as Cisco Cyber Vision Center. The image is available as an OVA for VMware ESXi and as a VHDX for Microsoft Hyper-V. During setup, the system automatically detects and applies the Sensor VM configuration files from the Sensor VM ISO generated by Cisco Cyber Vision Center.

> **Note**
>
> The QCOW2 image includes the CV Sensor; however, this deployment option has not been validated on all hypervisors, and support may vary depending on the hypervisor used.

This deployment is intended for network administrators, security engineers, and virtualization platform administrators who deploy sensors in Cisco Cyber Vision environments. Administrators should be familiar with virtualization platforms such as VMware ESXi and Microsoft Hyper-V, network concepts such as VLANs and port mirroring, and Cisco Cyber Vision Center access.

Architecture

Sensor VM internally runs multiple sensor containers. Each sensor container is mapped to a dedicated network interface to support traffic capture and Active Discovery. This structure ensures proper visibility into network assets and communication patterns.

Figure 1: Sensor VM architecture

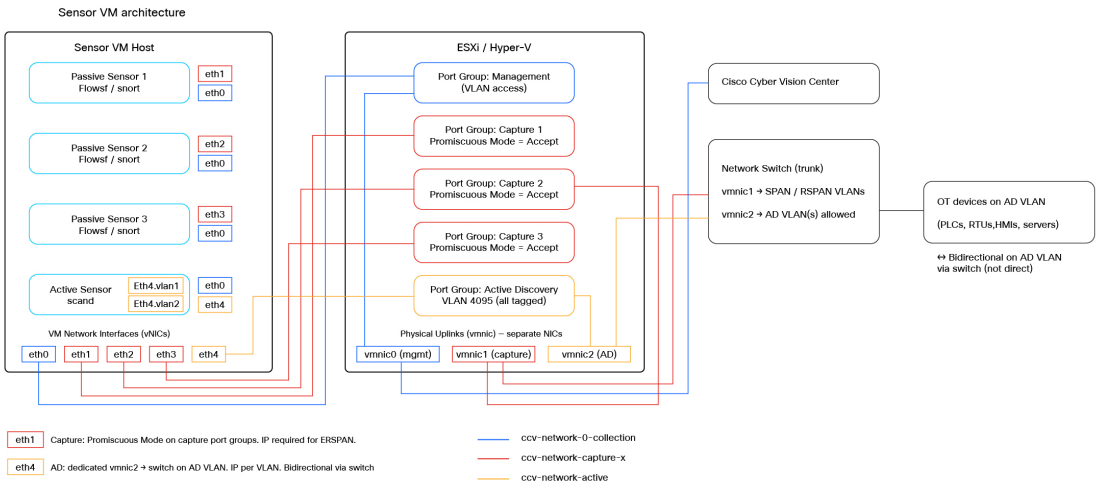


Table 1: Interface roles

Host Interface	Role
eth0 (Management)	Handles communication with the Center (enrollment, image download, telemetry)

Host Interface	Role
eth1 to eth4 (capture)	Each interface receives mirrored traffic (SPAN, RSPAN, or ERSPAN) for passive analysis
eth1 to eth4 (Active Discovery)	Provides bidirectional communication with target subnets for active scanning

Note

Interfaces eth1 to eth4 can be used for either passive capture or Active Discovery. Only one function can be assigned to a single interface at a time. Do not use the same interface for both passive capture and Active Discovery simultaneously.

Multiple containers are deployed to manage distinct capture interfaces and to segment passive and active discovery sensors. These containers are auto-provisioned using the Sensor VM ISO image generated from the Center.

Cisco Cyber Vision sensor overview

Introduces Cisco Cyber Vision sensors by outlining their deployment on Cisco network devices, methods for analyzing OT traffic using deep packet inspection and Active Discovery, identification and transmission of industrial assets and security events, and details on communication protocols between sensors and Cyber Vision Center.

A Cisco Cyber Vision sensor is an application that:

1. Gathers and analyzes industrial network traffic using deep packet inspection.
2. Transmits identified assets, communication flows, and security events to the Cyber Vision Center for further analysis.

Cyber Vision sensors help you analyze industry-specific OT traffic that traditional IT security tools usually cannot interpret.

How does the Cisco Cyber Vision Sensor work?

- The sensors use traffic mirroring methods (such as SPAN, RSPAN, or ERSPAN) to receive copies of OT network traffic for analysis.
- Deep packet inspection (DPI) enables identification of industrial protocols (such as Modbus, S7, EtherNet/IP, and other similar protocols), with configurable templates for targeted protocol recognition.

  Note

  Cyber Vision sensors only inspect TCP and UDP traffic.

  For a list of supported protocols, refer the Cisco Cyber Vision Protocols Data Sheet.

- Capture modes let you define which types of traffic to analyze to optimize performance.
- Beyond passive analysis, sensors can perform Active Discovery by probing the network for device details.
- Processed data is securely sent to Cisco Cyber Vision Center.

Specific ports are used for communication between the deployed sensor and the Cyber Vision Center.

Port	Message type
TCP 5671	AMQP (Advanced Message Queuing Protocol)
TCP 10514	Secure syslogs

Note

From Cyber Vision Release 5.4.0, this port is not used for sensor communications. Secure syslogs are also sent using TCP 5671.

Deploying Sensor VM on VMware ESXi

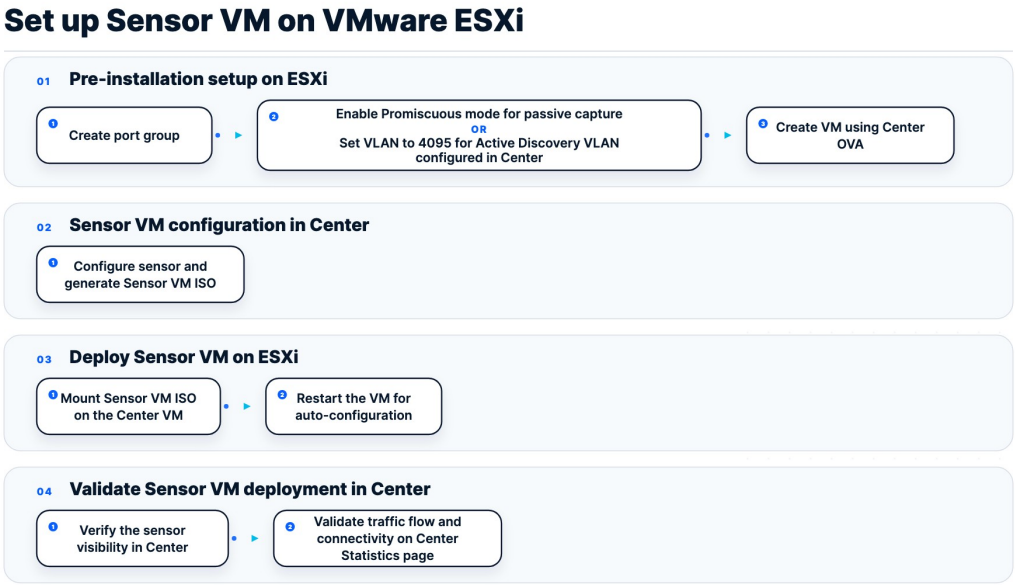
Describes the end-to-end process of deploying Cisco Cyber Vision Sensor VMs on VMware ESXi, including required validations, network configuration, deployment, and verification.

Summary

Deploying sensor VMs on VMware ESXi involves several coordinated steps to ensure proper installation, connectivity, and operation. This process requires careful preparation, configuration, deployment, and validation tasks.

Workflow

Figure 2: Sensor VM deployment process flow



These stages provides a high-level view of deploying Sensor VM on VMware ESXi. Refer to the official VMware ESXi installation guide and the Set up Cisco Cyber Vision Sensor VM on ESXi on page 12 sections in this document for step-by-step configuration.

1. Pre-installation setup on ESXi
    - Perform the initial validation of hypervisor versions and resources for deployment readiness.
        - Validate ESXi version compatibility and ensure that the hardware resources meet the minimum requirements specified for the Cisco Cyber Vision Center OVA.
        - Synchronize time using an NTP server to keep the sensor and Center clocks aligned.
        - Ensure that the Center's Fully Qualified Domain Name (FQDN) is resolvable via DNS or static mapping to maintain connectivity during deployment.
        - Generate a deployment token from the Cisco Cyber Vision Center.
    - Create the required vSwitches and port groups for management, capture traffic, and Active Discovery within VMware ESXi.
    - Connect the sensor management interface (eth0) to a VLAN or port group that can reach Cisco Cyber Vision Center collection interface on TCP port 443 and AMQP 5671.
    - Configure the sensor's capture interfaces (eth1-eth4), assigning them to port groups with Promiscuous Mode enabled. Configure the physical switch SPAN or RSPAN session toward the ESXi capture uplink.
    - If using Active Discovery with VLAN tagging, set the Active Discovery VLAN ID to 4095; otherwise, use an access port group for untagged traffic.
    - Map dedicated physical network interfaces (vmnics) as needed, especially where traffic separation is required.
    - Create the Sensor VM using the Cisco Cyber Vision OVA and attach the required virtual network interfaces.
2. Sensor VM configuration in Center
    - In Cisco Cyber Vision Center, configure the sensor details, including sensor mode, capture mode, Center connection details, NTP, and any Active Discovery options.
    - Generate and download the Sensor VM configuration ISO file from the Center.
3. Deploy Sensor VM on ESXi
    - On the ESXi host, upload and mount the generated Sensor VM configuration ISO file on the Sensor VM, and power on or restart the VM.
    - The ISO will automatically apply the necessary network settings, certificates, time sync configuration, Center registration, and trigger a final VM reboot.
4. Validate Sensor VM deployment in Center
    - Confirm that the sensor registers with Cyber Vision Center (over eth0) and is visible in the Sensor Explorer in Center Webapp.
    - Verify that mirrored network traffic appears on the capture interfaces.
    - If Active Discovery is enabled, ensure VLAN or network reachability and that bidirectional probes to operational technology (OT) target devices are successful.

Deploying Sensor VM on Microsoft Hyper-V

Describes the process of deploying Cisco Cyber Vision Sensor VMs on Microsoft Hyper-V, including prerequisites, network setup, VM configuration, and verification stages.

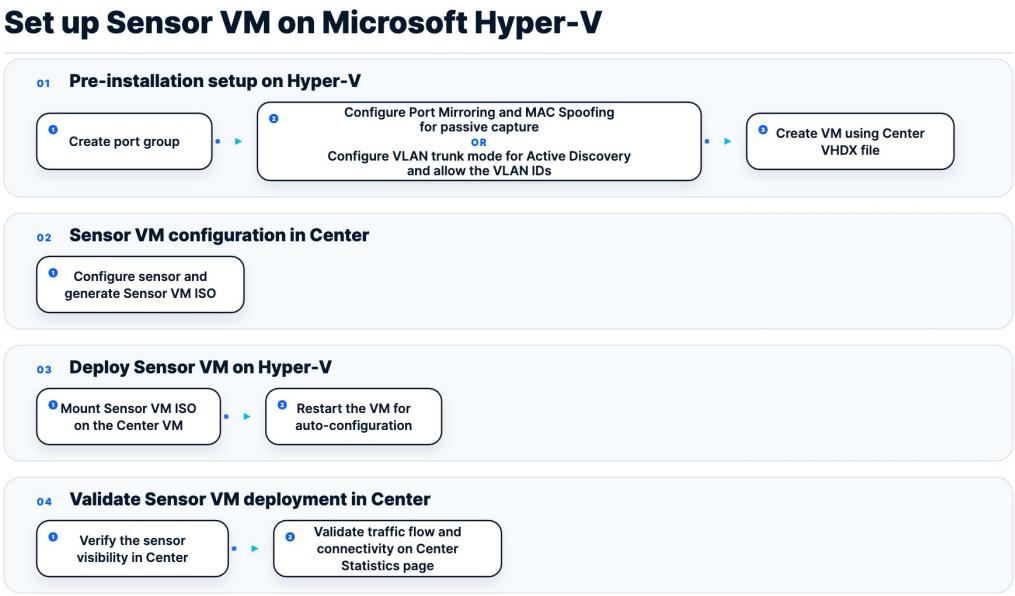
Summary

Deploying Sensor VMs on Microsoft Hyper-V requires careful preparation, network configuration, VM setup, and post-deployment validation to ensure secure and effective monitoring in your environment.

Validate Hyper-V port mirroring, MAC address spoofing, and VLAN trunk settings with the virtualization administrator before implementation to avoid any disruption in the network traffic.

Workflow

Figure 3: Sensor VM deployment process flow



These stages provides a high-level view of deploying Sensor VM on Microsoft Hyper-V. Refer to the official Microsoft Hyper-V installation guide and the Set up Cisco Cyber Vision Sensor VM on Hyper-V on page 26 sections in this document for step-by-step configuration.

1. Pre-installation setup on Hyper-V
   - Perform initial validation of hypervisor versions and resources for deployment readiness.
     - Validate that the Hyper-V host runs Windows Server 2019 or 2022.
     - Allocate the required CPU, memory, and network resources for the Sensor VM.
     - Obtain the Cisco Cyber Vision VHDX file for Hyper-V deployments.
     - Use an NTP server to synchronize sensor and Center clocks for accurate reporting.
     - Ensure the Cyber Vision Center FQDN is resolvable via DNS or static entry to maintain the connectivity with the Cisco Cyber Vision Center during deployment.
     - Generate a deployment token from Cisco Cyber Vision Center.
   - Create virtual switches for management, capture, and Active Discovery interfaces as required.
   - Connect the management interface (eth0) to a VLAN or access port that can reach Cisco Cyber Vision Center collection interface on TCP port 443 and AMQP 5671.
   - Configure port mirroring and enable MAC address spoofing on capture interfaces to ensure traffic is delivered to the Sensor VM.
     - Configure Hyper-V port mirroring so that monitored traffic is sent to the Sensor VM capture vNIC. Set the capture vNIC as the destination for mirrored traffic and enable MAC Address Spoofing on that vNIC.

    - Configure the physical switch SPAN or RSPAN session, or the Hyper-V port mirroring source, as required.
- If Active Discovery uses VLANs, set the relevant vNIC to trunk mode and allow required VLAN IDs; otherwise, connect to an access or untagged network.
- Map dedicated adapters for capture and Active Discovery if traffic separation is required. Use PowerShell in Hyper-V to configure VLAN trunking as needed.
- Confirm port mirroring, MAC address spoofing, and network trunking with the virtualization administrator before proceeding.
- Create the Virtual Machine in Hyper-V using the VHDX file. Attach the vNICs in the required order.

2. Sensor VM configuration in Center

- In Cisco Cyber Vision Center, configure Sensor VM details: mode, capture settings, Center connection, NTP, and Active Discovery options.
- Generate and download the configuration ISO from Cyber Vision Center.

3. Deploy Sensor VM on Hyper-V

- Mount the Sensor VM configuration ISO file on the Sensor VM. Power on or restart the Sensor VM.
- The ISO applies the network configuration, certificates, time synchronization, Center registration, and trigger a final reboot.

4. Validate Sensor VM deployment in Center

- Verify that the Sensor registers over the management interface (eth0) and appears in Cyber Vision Center.
- Confirm that port mirroring delivers traffic to the Sensor's capture interfaces and passive sensors process flows.
- Ensure the trunked interface allows the required VLANs for Active Discovery and that bidirectional connectivity to OT targets via switch.

2 Set up Cisco Cyber Vision Sensor VM on ESXi

Topics:

- Requirements
- Initial Configurations
- Sensor VM deployment
- Verify Sensor VM deployment status and connectivity in Cisco Cyber Vision

Introduces the end-to-end deployment process for Cisco Cyber Vision Sensor VM on ESXi, detailing requirements, initial configurations such as traffic capture and VLAN settings, sensor installation procedures, and verification steps for connectivity and operation.

Requirements

Details hardware and software prerequisites for Sensor VM deployment on ESXi, including sensor-specific requirements and network interface considerations necessary for successful installation and operation.

Sensor VM prerequisites

Defines the hardware and software requirements necessary for deploying a sensor virtual machine. These specifications ensure optimal performance and connectivity within the network environment.

Ensure your environment meets the following hardware specifications and prerequisites prior to deploying a Sensor VM.

Supported hypervisors

Deploy the Sensor VM only on VMware vSphere ESXi 7.0 or VMware vSphere ESXi 8.0.

> **Note**
>
> Create a virtual machine on your VMware ESXi by deploying the Cisco Cyber Vision OVA. For detailed steps, refer to the Install the Virtual Center topic in Cisco Cyber Vision Center VM Installation Guide.

Sensor VM resource requirements

For optimal performance and stability, the Sensor VM requires the same minimum hardware resources as the Cisco Cyber Vision Center OVA. For further details on resource allocation requirements, refer to the Cisco Cyber Vision Center VM Installation Guide.

- vCPU: 4
- RAM: 8 GB
- Disk: 60 GB

> **Note**
>
> Scale the hypervisor resources based on the number of sensors deployed and the network traffic rate to ensure optimal allocation.

Sensor VM deployment prerequisites

The table details the requirements that must be met to successfully deploy and connect the Sensor VM to the Cisco Cyber Vision Center.

Table 2: Sensor VM deployment prerequisites

Category	Requirements
Deployment Token	A pre-created deployment token from the Cisco Cyber Vision Center (**Admin** > **Deployment**).

Category	Requirements
Center FQDN	The Center FQDN (e.g., `center.example.com`) must be resolvable to an IP address through DNS or a static hostname entry. This ensures the Sensor VM can locate and communicate with the Cisco Cyber Vision Center during deployment. **Note** If DNS is unavailable, check the **Add a static DNS entry for the Center FQDN** check box in the Sensor VM deployment wizard.
NTP	Time synchronization is mandatory. The Sensor VM and the Cisco Cyber Vision Center must have accurate, synchronized system time. Refer Synchronize the Center and the sensors to NTP servers. **Note** During Sensor VM deployment, you can specify an NTP server (e.g., `ntp.ubuntu.com` or your internal NTP server). If you leave this field blank, the Sensor VM will automatically inherit the Center's NTP configuration.

Network interface requirements

Defines the maximum network interface configuration for the Sensor VM. This ensures proper connectivity for management, capture, and Active Discovery functions.

The Sensor VM supports up to five network interfaces: one dedicated management interface (eth0) and a maximum of four interfaces for capture and Active Discovery.

Use the table to map Sensor VM networking requirements to the equivalent configuration on VMware ESXi. Apply these settings only to the relevant Sensor VM interfaces. Keep eth0 dedicated to management and Center connectivity.

> **Note**
>
> Consult your virtualization platform administrator to ensure these settings are applied correctly to avoid network disruption.

Table 3: Network interface requirements

Interface	Purpose	Hypervisor Configuration
eth0	Management communication with the Cisco Cyber Vision Center **Note** eth0 is reserved for Center connectivity. It cannot be used for capture or Active Discovery.	Connect to a management VLAN or access port group with reachability to the Center on TCP ports 443 and 8443.
eth1 to eth4	Passive traffic capture from a SPAN or RSPAN source.	Assign each capture interface to a dedicated VLAN port group. Enable **Promiscuous Mode** = **Accept** on the capture port group. **Note** VLAN 4095 is not required for standard passive capture.
eth1 to eth4	Passing VLAN-tagged traffic to the Sensor VM (multi-VLAN / Active Discovery with VLAN).	Set the port group VLAN ID to 4095 to pass tagged frames to the guest VM.
eth1 to eth4	Active Discovery with VLAN tag configured in Cisco Cyber Vision Center. Bidirectional communication with target devices.	Configure the Active Discovery port group with VLAN ID 4095 so VLAN-tagged traffic is passed to the Sensor VM. Use a dedicated uplink (vmnic) for Active Discovery traffic.
eth1 to eth4	Active Discovery without VLAN tag configured in Cisco Cyber Vision Center. Bidirectional communication with target devices.	Connect the interface to an access port group on the target network.

Initial Configurations

Explains essential Sensor VM configuration steps, including supported traffic capture methods, enabling promiscuous mode in the hypervisor, and configuring Active Discovery VLANs, with guidance for setting communication paths and enabling VLAN trunking mode.

Sensor VM traffic capture methods

Describes the available traffic capture modes for the Sensor VM. This information helps administrators select the appropriate method based on network topology and configuration requirements.

This reference provides a summary of traffic capture modes, including SPAN, RSPAN, ERSPAN, and Direct trunk, to facilitate effective network monitoring and sensor deployment.

The table shows the available traffic capture modes for the Sensor VM. Use this information to determine the best method for your network environment, based on sensor location and configuration requirements.

Table 4: Capture modes

Mode	Description	Use When	Key Requirement
SPAN	Local port mirroring on the same switch.	Sensor is on the same switch as monitored traffic.	Promiscuous Mode on port group. The maximum number of supported SPAN sessions is platform-dependent; refer to your specific switch documentation for limitations. **Note** A port configured as a SPAN destination is dedicated solely to mirrored traffic. It cannot simultaneously carry standard VLAN traffic or be used for Active Discovery.
RSPAN	Mirrored traffic in a dedicated VLAN across trunks.	Sensor is on a different switch, or single cable is used for capture and Active Discovery.	RSPAN VLAN configured with remote-span on all switches. The maximum number of supported RSPAN sessions is platform-dependent; refer to your specific switch documentation for limitations. **Note** Mirrored frames within an RSPAN VLAN do not retain the original 802.1Q tags. If tag preservation is required for your analysis, use ERSPAN instead.
ERSPAN	Mirrored traffic encapsulated in GRE over IP (Layer 3).	Traffic crosses routed boundaries or VLAN preservation is needed.	Requires IP address on capture interface and IP reachability to source. Preserves VLAN tags.

Mode	Description	Use When	Key Requirement
Direct trunk	Normal L2 forwarding (no mirroring).	Lab replay from a test machine.	Trunk with allowed VLANs; no SPAN needed.

Capture mode features

The table evaluates key technical features of the capture modes, such as VLAN tag preservation, switch traversal capabilities, and interface requirements. This information helps you select the capture method most suitable for your architecture.

Table 5: Capture mode feature comparison

Feature	SPAN	RSPAN	ERSPAN
Mirror across switches	No	Yes (Layer 2)	Yes (Layer 3)
VLAN tag preservation	Yes	No	Yes
Share trunk with AD	No	Yes	Yes
Dedicated port	Yes	No	No
Capture interface IP	No	No	Yes
Promiscuous Mode on port group	Yes	Yes	No

Enable Promiscuous Mode to receive mirrored traffic

Enables Promiscuous Mode on the capture port group to allow the sensor to receive mirrored traffic. This configuration ensures that ESXi does not drop frames with destination MAC addresses that do not belong to the sensor virtual NIC.

When receiving SPAN or RSPAN traffic, the mirrored frames have destination MAC addresses that do not belong to the sensor virtual NIC. By default, ESXi drops such frames. To allow the sensor to receive this traffic, Promiscuous Mode must be enabled on the capture port group.

For ERSPAN, Promiscuous Mode is not required because traffic is encapsulated in IP packets and delivered directly to the sensor's interface.

Important

Enable Promiscuous Mode only on capture port groups. Do not enable it on management port groups.

Before you begin

Create a port group in the VMware vSphere Client. For detailed steps to create a port group in ESXi, refer to the VMware official documentation: Add a Virtual Machine Port Group.

Follow these steps to enable Promiscuous Mode the capture port group.

Procedure

1. Log in to the VMware vSphere Client.

2. From the inventory, click the ESXi host where the sensor VM is deployed.
3. Go to **Networking** and click the vSwitch that is associated with the sensor VM capture network.
4. Select the port group used for traffic capture (sensor interface).
5. Click the edit icon (or right-click the port group) and select **Edit Settings**).
6. In the **Edit port group** page, navigate to **Security** section and set **Promiscuous Mode** to **Accept**.
7. (Optional) Set **Forged Transmits** to **Accept** if you want to enable Active Discovery on the same port group.
8. Click **Save**.

Active Discovery VLAN configuration

Describes the requirements for configuring Active Discovery with a VLAN. This ensures the sensor successfully communicates with the target subnet by maintaining VLAN-tagged frames.

When Active Discovery is configured with a VLAN, the sensor creates a corresponding VLAN subinterface to communicate with the target subnet. VMware ESXi must pass 802.1Q-tagged frames to the guest operating system so the Sensor VM can send probes and receive replies on that VLAN.

VLAN Configuration Requirements

When configuring a VLAN for Active Discovery in Cisco Cyber Vision Center, map the Active Discovery vNIC to an ESXi port group with VLAN ID 4095.

Important

If the port group uses the specific Active Discovery (AD) VLAN ID instead, ESXi strips the VLAN tag before traffic reaches the sensor VM and Active Discovery can fail, typically resulting in ARP timeouts. If no VLAN is configured for Active Discovery, use a standard access port group; VLAN 4095 is not required.

Note

Consult your virtualization platform administrator before implementation to avoid disruption in network traffic.

Table 6: Use case to use VLAN 4095 on ESXi

Use Case	VLAN 4095 Required?	Notes
Active Discovery with a VLAN configured in Center	Yes	Set the Active Discovery port group VLAN ID to 4095. Use this setting only on the Active Discovery vNIC that expects tagged traffic. Ensure the physical switch trunk allows the Active Discovery VLAN. Assign an IP address to the Sensor VM for that Active Discovery VLAN.
Active Discovery without a VLAN configured in Center(flat network)	No	Use an access port group on the target network. VLAN 4095 is not required. The Active Discovery interface sends and receives untagged traffic on the target network.

Use Case	VLAN 4095 Required?	Notes
Standard passive capture with SPAN or RSPAN	No	Use the capture port group design for the capture interface, with Promiscuous Mode set to Accept. VLAN 4095 is not required for the standard passive-capture layout.
Passive capture with multiple VLANs on one vNIC	Yes	Advanced only; not the default Sensor VM layout.
Management on eth0	No	Use the management VLAN or an access port group that can reach Cisco Cyber Vision Center. Never use eth0 for capture or Active Discovery purposes.
ERSPAN capture	No	Use an access port group with IP on the capture interface.

Setting communication path for Active Discovery

Describes how to configure communication paths for the Active Discovery feature, the required network components, and the sequence to ensure bidirectional traffic between the Sensor VM and OT devices.

Summary

Active Discovery is a bidirectional process that does not use eth0 for traffic. Discovery traffic must flow from the active sensor process through the Sensor VM's Active Discovery interface, then continue through the ESXi port group, dedicated physical uplink, and the network switch trunk to reach OT devices on the same Active Discovery VLAN. The Sensor VM sends ARP, ICMP, and protocol probes. Replies from OT devices return via the same path. The switch trunk must include the Active Discovery VLAN for proper connectivity.

Discovery traffic goes through the network switch on the configured VLAN. It is not sent directly to an abstract OT network, and the switch trunk must allow the Active Discovery VLAN.

Before you begin configuring Active Discovery VLANs,

- configure an IP address for each Active Discovery VLAN in Cisco Cyber Vision Center.
- reserve one Sensor VM interface (from eth1 through eth4) for Active Discovery. Use eth0 only for management and Cisco Cyber Vision Center connectivity.
- use a dedicated physical uplink for Active Discovery in standard deployments. This uplink should be separate from the capture uplink. For example, use vmnic1 for capture and vmnic2 for Active Discovery
- configure the physical switch port connected to the Active Discovery uplink as a trunk. Allow the required Active Discovery VLANs on this trunk port.

Workflow

1. Create or select the ESXi vSwitch and port group that will carry Active Discovery traffic.
2. If Active Discovery uses a VLAN configured in Cisco Cyber Vision Center, set the port group VLAN ID to 4095.
3. Attach the Sensor VM Active Discovery vNIC (for example eth4) to the Active Discovery port group. Do not attach eth0 to this port group.
4. Map the Active Discovery port group to the dedicated physical uplink that connects to the network switch trunk.
5. If Active Discovery does not use a VLAN, connect the Active Discovery vNIC to a standard access port group on the target network instead of using VLAN 4095.
6. Validate that the Sensor VM can reach OT devices on the Active Discovery VLAN and that OT devices can send replies back through the same VLAN path.

Enable VLAN trunking mode

Configures a port group to VLAN 4095 in VMware ESXi to enable VLAN trunking mode. This setting allows all VLAN-tagged traffic to pass through to the virtual machine.

In ESXi, setting the VLAN ID to 4095 enables VLAN trunking mode on a port group, allowing all VLAN-tagged traffic to pass through to the virtual machine.

Before you begin

Create a port group in the VMware vSphere Client. Port groups enable configuration of the VLAN ID and security settings required for the Sensor VM. For detailed steps to create a port group in ESXi, refer to the VMware official documentation: Add a Virtual Machine Port Group.

Follow these steps to enable VLAN trunking mode on a port group.

Procedure

1. Log in to the vSphere Client.
2. Select the ESXi host where the sensor VM is deployed.
3. From the left pane, click **Networking**.
4. Under **Port Group**, locate the port group configured for Active Discovery (AD traffic).
5. Right-click the port group and click **Edit Settings**. Alternatively, click **Actions**, then select **Edit Settings**.
6. In the **General** section, set **VLAN ID** to 4095.
7. Click **OK** to save the changes.
   The port group is now in trunk mode. All tagged frames will be passed to the Sensor VM.

Sensor VM deployment

Describes the Sensor VM deployment process, providing instructions to configure the Sensor VM in Cisco Cyber Vision and to deploy the Sensor VM in ESXi for operational readiness.

Configure a Sensor VM in Cisco Cyber Vision Center

Configures a Sensor VM within the Cisco Cyber Vision environment by defining application, capture, and network settings. This procedure generates the necessary configuration files for sensor deployment.

In Cisco Cyber Vision Center, you can configure a Sensor VM and generate an ISO file for sensor deployment.

The Sensor VM ISO file contains

- ca-cert.pem (Center public certificate for authentication, such as downloading sensor images)

> **Note**
>
> If the Center CA certificate changes, manually update the Sensor VM certificate to maintain connectivity.

- compose.yaml (Compose file for Sensor VM setup), and
- sbs-config.json (OS configuration).

Before you begin

Create deployment tokens. Refer to the Create Deployment Tokens topic of the Cisco Cyber Vision Administration Guide for instructions.

Follow these steps to configure Sensor VM in Center

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click **New sensor** and select **Sensor VM** from the drop-down list.
3. Fill in the details in the **Sensor Application** page.
   a) Enter the **Name** of your sensors.

   > **Note**
   >
   > The name of your sensors must be unique for each center.

   b) Click the **Deployment token** drop-down list and select your deployment token name.
   c) Click the **Sensor Mode** drop-down list and select your Sensor Mode: **Passive only**, **Active Discovery only**, **Passive or Active Discovery**.
   d) If the Center's FQDN is not resolvable via DNS, check the **Add a static DNS entry for the Center FQDN** check box to add the Center FQDN to the VM's /etc/hosts file.
   e) If NAT is used for sensor and Cisco Cyber Vision Center IP connectivity, check the **Center is behind NAT** check box and enter the **Center Collection IP**.
   f) Click **Next**.
4. Fill in the details in the **Capture Configuration** page.

   If **Sensor Mode** is set to **Active Discovery only**, then proceed with step 5.

   > **Note**
   >
   > The mirrored traffic type determines the form: SPAN, RSPAN, ERSPAN2, or ERSPAN3.

   a) Configure SPAN mode.
      - Click the **Mirrored traffic type** drop-down field and select SPAN from the list.
      - Click the **Capture Interface** drop-down field and select the host interface that will receive the capture (for example, eth2, eth3).
      - Click the **Capture Mode** drop-down field and select sensor filter (for example, **Optimal (default)** , **All** , **Industrial** , **Custom**).

   b) Configure RSPAN mode.
      - Click the **Mirrored traffic type** drop-down field and select RSPAN from the list.
      - Click the **Capture Interface** drop-down field and select the host interface that will receive the capture (for example, eth2, eth3).
      - Click the **Capture Mode** drop-down field and select sensor filter (for example, **Optimal (default)** , **All** , **Industrial** , **Custom**).

- Add a VLAN ID configured for the RSPAN destination.

c) Configure ERSPAN mode.

- Click the **Mirrored traffic type** drop-down field and select ERSPAN from the list.
- Click the **Capture Interface** drop-down field and select the host interface that will receive the capture (for example, eth2, eth3).
- Click the **Capture Mode** drop-down field and select sensor filter (for example, **Optimal (default)** , **All** , **Industrial** , **Custom**).
- Enter the Capture IP address of the interface in the **Capture IP** field that will receive the spanned traffic.
- Add a **VLAN** ID if needed.

d) Click **Save Interface**.
e) Click **Continue with interfaces**.

The **Active Discovery** page appears.

5. Fill in the details on the **Active Discovery** page.
   a) Click the **Active Discovery Interface** drop-down field and select the host interface that will be used for active discovery (for example, eth2, eth3).
   b) Enter an IP address for active discovery in the **IP** field.
   c) If needed, add a **VLAN**.

> **Note**
>
> When a VLAN is specified for Active Discovery, the hypervisor must be configured to pass VLAN-tagged frames to the Sensor VM. For more information on Active Discovery VLAN configuration, refer to Active Discovery VLAN configuration on page 19.

   d) To add a new target, click **Add a new target** and enter the target details.
   e) Click **Continue with target interface**.

   The **Sensor VM Specific** page appears.

6. Enter the details on the **Sensor VM Specific** page.
   a) Check the **DHCP** check box to configure the Sensor VM to use the IP address assigned to the eth0 interface.

   Or,

   Uncheck the **DHCP** check box.

   - Enter a static **IP** address in CIDR notation. For example, 192.168.1.10/24.
   - Enter a **Gateway** if needed.

   b) Click the **Keymap** drop-down field and select a Virtual monitor and keyboard VGA console keymap.
   c) Enter the admin **Password** and **Confirm Password**.
   d) In **DNS Server**, enter the DNS configuration of the Sensor VM. If left blank, the system automatically inherits the Center's DNS settings when in single-interface mode. This setting is not applicable in dual-interface mode.

   To add more DNS servers, click the **+** icon.

e) In **NTP**, enter the NTP settings for the Sensor VM. If this field is left blank in single interface mode, the configuration is inherited from the Center. In dual interface mode, if left blank, the Center's eth1 IP address is used as the NTP server.

To add more NTP, click the **+** icon.

f) In **Firewall Allowed,** enter the firewall configuration for the Sensor VM. If left blank, the configuration is inherited from the Center.

To add more firewall configurations, click the **+** icon.

g) In **Authorized Keys**, enter the SSH authorized keys for the cv-admin user. If left blank, the keys are inherited from the Center.

To add more SSH authorized keys, click the **+** icon.

h) Click **Next**.
The **Configure Sensor VM** page appears.

7. Click **Download image**.
The Sensor VM ISO file is downloaded to your local machine.

Deploy Sensor VM on VMware ESXi

Deploys the sensor VM by uploading the ISO file to the datastore and mounting it to the Cisco Cyber Vision Center VM. This process enables the VM to automatically configure its network, synchronize time, and initialize reboot.

This procedure describes how to upload and mount the Sensor VM ISO file on a VMware ESXi host. After you mount the ISO and reboot, the VM automatically configures its management and capture network settings. It synchronizes system time, registers with the Cyber Vision Center, and completes initial provisioning.

Before you begin

- Create a virtual machine on VMware ESXi by deploying the Cisco Cyber Vision OVA. For detailed deployment steps, refer to the Install the Virtual Center topic of the Cisco Cyber Vision Center VM Installation Guide.
- Confirm that the virtual machine is configured with one management interface (eth0) and one or more capture interfaces (eth1–eth4).
- Ensure the Sensor VM ISO file has been generated from the Cyber Vision Center.

> **Note**
>
> A virtual machine can operate either as a Center or a Sensor. If the ISO is mounted and contains valid configuration files, the host is auto-provisioned as a Sensor VM.

Follow these steps to deploy the Sensor VM.

Procedure

1. Upload the Sensor VM ISO to a Datastore.
   a) In VMware ESXi, click **Storage** from the left pane, and select the Datastore where you want to store the ISO file.
   b) Click **Datastore browser**.
   c) (Optional) Create a dedicated folder.
   d) Click **Upload** and upload the ISO file from your local machine.

2. Mount the Sensor VM ISO.
   a) From the left pane, click **Virtual Machines** and select the Center VM.
   b) From the top menu, click **Edit**.
   The **Edit setting** window appears.
   c) From the **CD/DVD Drive 1** drop-down field, select **Datastore ISO files**.
   d) Navigate to your datastore, select the uploaded ISO file, and click **Select**.
   e) Check the **Connect** check box.
   f) Check the **Connect at power on** check box.
   g) Click **Save**.
3. Restart the VM.
   The VM detects the ISO, automatically configures network settings, synchronizes time (via NTP), registers with the Cyber Vision Center, and performs an automatic reboot to complete setup.

Verify Sensor VM deployment status and connectivity in Cisco Cyber Vision

Confirms the successful deployment and connectivity of the sensor VM within the Cisco Cyber Vision environment. This procedure ensures that the sensor is actively capturing and processing network traffic data.

After Sensor VM is deployed, ensure that the sensor VM is operational, connected, and actively monitoring network traffic in the Cisco Cyber Vision environment.

Follow these steps to verify the sensor VM deployment and connectivity.

Procedure

1. Log in to Cisco Cyber Vision Center and choose **Admin** > **Sensors** > **Sensor Explorer** .
2. Confirm that the newly deployed sensor appears in the sensor list.
3. Select the sensor from the list and click **Go to statistic** from the right pane.
4. Verify that the sensor is connected.

   The Captured Packets section displays new data on dropped and processed packets.
5. Alternatively, choose **Explore** > **All Data** > **Map** to view the network traffic data and components that are connected.

3 Set up Cisco Cyber Vision Sensor VM on Hyper-V

Topics:

- Requirements
- Initial Configurations
- Sensor VM deployment
- Verify Sensor VM deployment status and connectivity in Cisco Cyber Vision

Guides you through setting up the Cisco Cyber Vision Sensor VM on Hyper-V, covering requirements, prerequisites, network interface needs, initial configuration tasks, traffic capture methods, VLAN and trunking setup, deployment workflows, and connectivity verification in Cisco Cyber Vision.

Requirements

Details hardware and software prerequisites for Sensor VM deployment on Hyper-V, including sensor-specific requirements and network interface considerations necessary for successful installation and operation.

Sensor VM prerequisites

Defines the hardware and software requirements necessary for deploying a sensor virtual machine. These specifications ensure optimal performance and connectivity within the network environment.

Before deploying the Sensor VM, ensure your environment meets the necessary prerequisites and hardware specifications.

Supported hypervisors

Deploy the Sensor VM only on Microsoft Hyper-V Windows Server 2019 or Microsoft Hyper-V Windows Server 2022.

> **Note**
>
> Create a virtual machine on your Hyper-V) by deploying the Cisco Cyber Vision VHDX file. For detailed steps, refer to the Install the Virtual Center topic in Cisco Cyber Vision Center VM Installation Guide.

Sensor VM resource requirements

For optimal performance and stability, the Sensor VM requires the same minimum hardware resources as the Cisco Cyber Vision Center VM. For further details on resource allocation requirements, refer to the Cisco Cyber Vision Center VM Installation Guide.

- vCPU: 4
- RAM: 8 GB
- Disk: 60 GB

> **Note**
>
> Scale the hypervisor resources based on the number of sensors deployed and the network traffic rate.

Sensor VM deployment prerequisites

The table details the requirements that must be met to successfully deploy and connect the Sensor VM to the Cisco Cyber Vision Center.

Table 7: Sensor VM deployment prerequisites

Category	Requirements
Deployment Token	A pre-created deployment token from the Cisco Cyber Vision Center (**Admin** > **Deployment**).

Category	Requirements
Center FQDN	The Center FQDN (e.g., `center.example.com`) must be resolvable to an IP address through DNS or a static hostname entry. This ensures the Sensor VM can locate and communicate with the Cisco Cyber Vision Center during deployment. **Note** If DNS is unavailable, check the **Add a static DNS entry for the Center FQDN** check box in the Sensor VM deployment wizard.
NTP	Time synchronization is mandatory. The Sensor VM and the Cisco Cyber Vision Center must have accurate, synchronized system time. Refer Synchronize the Center and the sensors to NTP servers. **Note** During Sensor VM deployment, you can specify an NTP server (e.g., `ntp.ubuntu.com` or your internal NTP server). If you leave this field blank, the Sensor VM will automatically inherit the Center's NTP configuration.

Network interface requirements

Defines the maximum network interface configuration for the Sensor VM. This ensures proper connectivity for management, capture, and Active Discovery functions.

The Sensor VM supports up to five network interfaces: one dedicated management interface (eth0) and a maximum of four interfaces for capture and Active Discovery.

Use the table to map Sensor VM networking requirements to the equivalent configuration on Microsoft Hyper-V. Apply these settings only to the relevant Sensor VM interfaces. Keep eth0 dedicated to management and Center connectivity.

> **Note**
>
> Consult your virtualization platform administrator to ensure these settings are applied correctly to avoid network disruption.

Table 8: Network interface requirements

Interface	Purpose	Hypervisor Configuration
eth0	Management communication with the Cisco Cyber Vision Center **Note** eth0 is reserved for Center connectivity. It cannot be used for capture or Active Discovery.	Connect to a management VLAN or access port on the virtual switch with reachability to the Center on TCP ports 443 and 8443.
eth1 to eth4	Passive traffic capture from a SPAN or RSPAN source.	Configure port mirroring. Set the monitored interface as the source and the Sensor VM capture vNIC as the destination. Enable MAC Address Spoofing on the capture vNIC.
eth1 to eth4	Passing VLAN-tagged traffic to the Sensor VM (multi-VLAN / Active Discovery with VLAN).	Configure the vSwitch port or vNIC in trunk mode and allow the required VLAN IDs.
eth1 to eth4	Active Discovery with VLAN tag configured in Cisco Cyber Vision Center. Bidirectional communication with target devices.	Configure the Active Discovery vNIC in trunk mode and allow the required VLAN IDs. A dedicated uplink is recommended where network separation is required.
eth1 to eth4	Active Discovery without VLAN tag configured in Cisco Cyber Vision Center. Bidirectional communication with target devices.	Connect the interface to an access or untagged port on the target network.

Initial Configurations

Explains essential Sensor VM configuration steps, including supported traffic capture methods, enabling promiscuous mode in the hypervisor, and configuring Active Discovery VLANs, with guidance for setting communication paths and enabling VLAN trunking mode.

Sensor VM traffic capture methods

Describes the available traffic capture modes for the Sensor VM. This information helps administrators select the appropriate method based on network topology and configuration requirements.

This reference provides a summary of traffic capture modes, including SPAN, RSPAN, ERSPAN, and Direct trunk, to facilitate effective network monitoring and sensor deployment.

The table shows the available traffic capture modes for the Sensor VM. Use this information to determine the best method for your network environment, based on sensor location and configuration requirements.

Table 9: Capture modes

Mode	Description	Use When	Key Requirement
SPAN	Local port mirroring on the same switch.	Sensor is on the same switch as monitored traffic.	Promiscuous Mode on port group. The maximum number of supported SPAN sessions is platform-dependent; refer to your specific switch documentation for limitations. **Note** A port configured as a SPAN destination is dedicated solely to mirrored traffic. It cannot simultaneously carry standard VLAN traffic or be used for Active Discovery.
RSPAN	Mirrored traffic in a dedicated VLAN across trunks.	Sensor is on a different switch, or single cable is used for capture and Active Discovery.	RSPAN VLAN configured with remote-span on all switches. The maximum number of supported RSPAN sessions is platform-dependent; refer to your specific switch documentation for limitations. **Note** Mirrored frames within an RSPAN VLAN do not retain the original 802.1Q tags. If tag preservation is required for your analysis, use ERSPAN instead.
ERSPAN	Mirrored traffic encapsulated in GRE over IP (Layer 3).	Traffic crosses routed boundaries or VLAN preservation is needed.	Requires IP address on capture interface and IP reachability to source. Preserves VLAN tags.

Mode	Description	Use When	Key Requirement
Direct trunk	Normal L2 forwarding (no mirroring).	Lab replay from a test machine.	Trunk with allowed VLANs; no SPAN needed.

Capture mode features

The table evaluates key technical features of the capture modes, such as VLAN tag preservation, switch traversal capabilities, and interface requirements. This information helps you select the capture method most suitable for your architecture.

Table 10: Capture mode feature comparison

Feature	SPAN	RSPAN	ERSPAN
Mirror across switches	No	Yes (Layer 2)	Yes (Layer 3)
VLAN tag preservation	Yes	No	Yes
Share trunk with AD	No	Yes	Yes
Dedicated port	Yes	No	No
Capture interface IP	No	No	Yes
Promiscuous Mode on port group	Yes	Yes	No

Configure Port Mirroring to receive mirrored traffic

Enables traffic capture on a Sensor VM by configuring port mirroring and MAC address spoofing settings within the Hyper-V Manager. These settings allow the capture interface to receive mirrored traffic from the source adapter.

In Hyper-V, Promiscuous Mode is not exposed as a direct setting. To allow a sensor VM to receive mirrored traffic, you must configure port mirroring and enable MAC address spoofing on the capture interface.

Follow these steps to configure port mirroring and MAC address spoofing in Hyper-V.

Procedure

1. Open Hyper-V Manager.
2. Configure port mirroring on the source adapter (adapter where traffic originates - VM or external network interface).
   a) Right-click on source VM and select **Settings**.
   b) In the left-hand pane, locate the source adapter and expand its settings.
   c) Select **Advanced Features**.
   d) Under **Port mirroring**, select **Source**.
   e) Click **Apply**, and then click **OK**.
3. Configure port mirroring and MAC address spoofing on the sensor capture adapter (adapter on the sensor VM that captures traffic).
   a) Right-click on the Sensor VM and select **Settings**.
   b) In the left-hand pane, locate the adapter you are using for traffic capture and expand its settings.
   c) Select **Advanced Features**.
   d) Under **Port mirroring**, select **Destination**.

e) Under **MAC address**, check the **Enable MAC address spoofing** check box.
f) Click **Apply**, and then click **OK**.

Active Discovery VLAN configuration

Describes the requirements for configuring Active Discovery with a VLAN. This ensures the sensor successfully communicates with the target subnet by maintaining VLAN-tagged frames.

When Active Discovery is configured with a VLAN, the sensor creates a corresponding VLAN subinterface to communicate with the target subnet. Microsoft Hyper-V must pass 802.1Q-tagged frames to the guest operating system so the Sensor VM can send probes and receive replies on that VLAN.

VLAN Configuration Requirements

Important

On Microsoft Hyper-V, configure the Active Discovery network adapter in trunk mode and allow the required Active Discovery VLAN IDs. If the adapter is configured only as an access VLAN while the Sensor VM expects tagged Active Discovery traffic, Hyper-V does not pass the VLAN tags required by the Sensor VM.

Note

Consult with your virtualization platform administrators before implementation to avoid disruptions in network traffic.

Table 11: Use Case to use Hyper-V trunk mode

Use case	Trunk Mode Required?	Notes
Active Discovery with a VLAN configured in Center	Yes	Tagged frames reach the Sensor VM. The virtual switch and the physical switch trunk must allow the Active Discovery VLANs.
Active Discovery without a VLAN configured in Center (flat network)	No	Trunk mode is not required. The Active Discovery interface sends and receives untagged traffic on the target network.
Standard passive capture with SPAN or RSPAN	No	Use Hyper-V port mirroring for the capture vNIC. Enable MAC Address Spoofing on that capture vNIC.
Passive capture with multiple VLANs on one vNIC	Yes	Configure the Active Discovery network adapter in trunk mode and allow the required AD VLAN IDs. This configuration is advanced only; it is not the default Sensor VM layout.
Management on eth0	No	Use the management VLAN or an access port group that can reach Cisco Cyber Vision Center. Do not use eth0 for capture or Active Discovery.
ERSPAN capture	No	Use Access port group with IP on capture interface.

Setting communication path for Activity Discovery

Guides you through configuring the network communication path for Activity Discovery in Cisco Cyber Vision, including VLAN setup, Sensor VM interface assignments, Hyper-V virtual switch configuration, and validation of bidirectional connectivity with OT devices.

Summary

Active Discovery is bidirectional and does not use eth0. Traffic flows from the active sensor process through the Sensor VM Active Discovery network adapter, through the Hyper-V trunk configuration, through the virtual switch and dedicated uplink, and then through the network switch trunk to OT devices on the same Active Discovery VLAN. The Sensor VM sends ARP, ICMP, and protocol probes, and OT devices must be able to reply on that VLAN through the switch.

Discovery traffic goes through the network switch on the configured VLAN. It is not sent directly to an abstract OT network, and the switch trunk must allow the Active Discovery VLAN.

Before you begin configuring Active Discovery VLANs,

- configure an IP address for each Active Discovery VLAN in Cisco Cyber Vision Center.
- reserve one Sensor VM interface from eth1 through eth4 for Active Discovery. Keep eth0 for management and Cisco Cyber Vision Center connectivity only.
- identify the Hyper-V network adapter name that maps to the Sensor VM Active Discovery interface.
- use a dedicated virtual switch or uplink for Active Discovery where traffic separation is required.
- ensure that the Hyper-V virtual switch path and the physical network switch trunk allow the required Active Discovery VLANs.

Workflow

1. Create or select the Hyper-V virtual switch that will carry Active Discovery traffic, and connect it to the physical uplink that reaches the OT network switch trunk.
2. Attach the Sensor VM Active Discovery network adapter, for example the adapter mapped to eth4, to the Active Discovery virtual switch. Do not attach eth0 to this virtual switch for Active Discovery.
3. If Active Discovery uses a VLAN configured in Cisco Cyber Vision Center, configure the Active Discovery network adapter in trunk mode and allow the required VLAN IDs.
4. If Active Discovery does not use a VLAN, connect the Active Discovery network adapter to an untagged or access network instead of using trunk mode.
5. Validate that the Sensor VM can reach OT devices on the Active Discovery VLAN and that OT devices can send replies back through the same VLAN path.

Enable VLAN trunking mode

Configures a virtual network adapter to receive VLAN-tagged traffic using Windows PowerShell. This procedure enables trunk mode in a Hyper-V host where a standard UI option is unavailable.

Hyper-V does not provide a simple UI option for trunking. This configuration must be performed using Windows PowerShell to enable the virtual network adapter to receive VLAN-tagged traffic.

Before you begin

In Hyper-V, create a virtual switch using Virtual Switch Manager and configure VLAN settings on the virtual network adapters as required. For detailed steps to create and configure a virtual switch, refer to the Microsoft documentation: Create and configure a virtual switch with Hyper-V and Configure virtual local area networks (VLANs) for Hyper-V.

Follow these steps to enable trunking mode in Hyper-V.

Procedure

1. Open PowerShell as an administrator on the Hyper-V host.
2. Run the following command to enable trunk mode on the specific virtual network adapter.

```
Set-VMNetworkAdapterVlan -VMName "<VM_Name>" -VMNetworkAdapterName
"<Adapter_Name>" -Trunk -AllowedVlanIdList 1-4094 -NativeVlanId 0
```

You need to replace `<VM_Name>` and `<Adapter_Name>` with your actual VM and adapter names.

`<Adapter_Name>` must match the Hyper-V network adapter name mapped to the Sensor VM eth1-eth4 interface used for Active Discovery.

Note

`-AllowedVlanIdList 1-4094` is a lab sample. For production deployments, Cisco recommends restricting the allowed VLAN list to the specific Active Discovery (AD) VLAN(s) and any required RSPAN VLANs. For example:

```
Set-VMNetworkAdapterVlan -VMName "<VM_Name>" -VMNetworkAdapterName
"<Adapter_Name>" -Trunk -AllowedVlanIdList 100,200,900 -NativeVlanId 0
```

3. To verify the settings were applied correctly, run

```
Get-VMNetworkAdapterVlan -VMName "<VM_Name>"
```

The adapter is now configured to pass tagged frames to the guest, allowing the Sensor VM to handle VLAN tagging internally.

Sensor VM deployment

Describes the Sensor VM deployment process, providing instructions to configure the Sensor VM in Cisco Cyber Vision and to deploy the Sensor VM in Hyper-V for operational readiness.

Configure Sensor VM in Cisco Cyber Vision

Configures a Sensor VM within the Cisco Cyber Vision environment by defining application, capture, and network settings. This procedure generates the necessary configuration files for sensor deployment.

In Cisco Cyber Vision, you can configure a Sensor VM and generate an ISO file for sensor deployment.

The Sensor VM ISO file contains:

- ca-cert.pem: The center public certificate, in order to trust the center (for example, to download the sensor images).

> **Note**
>
> If the Center CA certificate is regenerated, you must manually update the Sensor VM with the new certificate to maintain connectivity.

- compose.yaml: The compose file to setup the Sensor VM.
- sbs-config.json: The OS configuration.

Before you begin

Create deployment tokens. Refer to the Create Deployment Tokens topic in the Cisco Cyber Vision Administration Guide.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click **New sensor** and select **Sensor VM** from the drop-down list.
3. Fill in the details in the **Sensor Application** page.
   a) Enter the **Name** of your sensors.

   > **Note**
   >
   > The name of your sensors must be unique for each center.

   b) Click the **Deployment token** drop-down list and select your deployment token name.
   c) Click the **Sensor Mode** drop-down list and select your Sensor Mode: **Passive only**, **Active Discovery only**, **Passive or Active Discovery**.
   d) If the Center's FQDN is not resolvable via DNS, check the **Add a static DNS entry for the Center FQDN** check box to add the Center FQDN to the VM's /etc/hosts file.
   e) If NAT is used for sensor and Cisco Cyber Vision Center IP connectivity, check the **Center is behind NAT** check box and enter the **Center Collection IP**.
   f) Click **Next**.
4. Fill in the details in the **Capture Configuration** page.

   If **Sensor Mode** is **Active Discovery only**, then proceed with step 5.

   > **Note**
   >
   > The form changes based on the mirrored traffic type: SPAN, RSPAN, ERSPAN2, or ERSPAN3.

   a) For SPAN configuration:
      - Click the **Mirrored traffic type** drop-down field and select SPAN from the list.
      - Click the **Capture Interface** drop-down field and select the host interface that will receive the capture (for example, eth2, eth3).

- Click the **Capture Mode** drop-down field and select sensor filter (for example, **Optimal (default)** , **All** , **Industrial** , **Custom**).

b) For RSPAN configuration:

- Click the **Mirrored traffic type** drop-down field and select RSPAN from the list.
- Click the **Capture Interface** drop-down field and select the host interface that will receive the capture (for example, eth2, eth3).
- Click the **Capture Mode** drop-down field and select sensor filter (for example, **Optimal (default)** , **All** , **Industrial** , **Custom**).
- Add a VLAN ID configured for the RSPAN destination.

c) For ERSPAN configuration:

- Click the **Mirrored traffic type** drop-down field and select ERSPAN from the list.
- Click the **Capture Interface** drop-down field and select the host interface that will receive the capture (for example, eth2, eth3).
- Click the **Capture Mode** drop-down field and select sensor filter (for example, **Optimal (default)** , **All** , **Industrial** , **Custom**).
- Enter the Capture IP address of the interface in the **Capture IP** field that will receive the spanned traffic.
- Add a **VLAN** ID if needed.

d) Click **Save Interface**.
e) Click **Continue with interfaces**.

The **Active Discovery** page appears.

5. Fill in the details on the **Active Discovery** page.
   a) Click the **Active Discovery Interface** drop-down field and select the host interface that will be used for active discovery (for example, eth2, eth3).
   b) Enter an IP address for active discovery in the **IP** field.
   c) If needed, add a **VLAN**.

> **Note**
>
> When a VLAN is specified for Active Discovery, the hypervisor must be configured to pass VLAN-tagged frames to the Sensor VM. For more information on Active Discovery VLAN configuration, refer to Active Discovery VLAN configuration on page 33.

   d) To add a new target, click **Add a new target** and target details.
   e) Click **Continue with target interface**.

The **Sensor VM Specific** page appears.

6. Fill in the details on the **Sensor VM Specific** page.
   a) Check the **DHCP** check box to configure the Sensor VM to use the IP address assigned to the eth0 interface.

Or,

Uncheck the **DHCP** check box.

- Enter a static **IP** address in CIDR notation. For example, 192.168.1.10/24.
- Enter a **Gateway** if needed.

b) Click the **Keymap** drop-down field and select a Virtual monitor and keyboard VGA console keymap.
c) Enter the admin **Password** and **Confirm Password**.
d) In **DNS Server**, enter the DNS configuration of the Sensor VM. If left blank, the system automatically inherits the Center's DNS settings when in single-interface mode. This setting is not applicable in dual-interface mode.

To add more DNS servers, click the **+** icon.

e) In **NTP**, enter the NTP settings for the Sensor VM. If this field is left blank in single interface mode, the configuration is inherited from the Center. In dual interface mode, if left blank, the Center's eth1 IP address is used as the NTP server.

To add more NTP, click the **+** icon.

f) In **Firewall Allowed,** enter the firewall configuration for the Sensor VM. If left blank, the configuration is inherited from the Center.

To add more firewall configurations, click the **+** icon.

g) In **Authorized Keys**, enter the SSH authorized keys for the cv-admin user. If left blank, the keys are inherited from the Center.

To add more SSH authorized keys, click the **+** icon.

h) Click **Next**.
The **Configure Sensor VM** page appears.

7. Click **Download image**.
The Sensor VM ISO file is downloaded to your local machine.

Deploy Sensor VM on Hyper-V

Deploy a Sensor VM using an ISO file on a Hyper-V virtual machine for automatic network configuration and sensor registration.

This procedure describes how to mount the Sensor VM ISO file on a Microsoft Hyper-V host. After you mount the ISO and reboot, the VM automatically configures its management and capture network settings. It synchronizes system time, registers with the Cyber Vision Center, and completes initial provisioning.

Before you begin

- Create a virtual machine on your Hyper-V environment using Cisco Cyber Vision VHDX file. For detailed deployment steps, refer to the Install the Virtual Center topic in Cisco Cyber Vision Center VM Installation Guide.
- Configure the VM with one management interface (eth0) and one or more capture interfaces (eth1-eth4).
- Ensure the Sensor VM ISO file has been generated from the Cyber Vision Center.

> **Note**
>
> A virtual machine can operate either as a Center or a Sensor. If the ISO is mounted and contains valid configuration files, the host is auto-provisioned as a Sensor VM.

Follow these steps to deploy a Sensor VM on Hyper-V.

Procedure

1. Copy the Sensor VM ISO file to a location accessible by the Hyper-V host, such as local disk or shared storage.
2. Open Hyper-V Manager.
3. Right-click the Center VM and select **Settings**.
4. Under **IDE Controller** (DVD Drive), select **Image file (.iso)**.
5. Browse for and select the Sensor VM ISO file.
6. Click **Apply**, and then click **OK**.
7. Power on the VM.
   The VM detects the ISO, automatically configure its network, synchronizes time (NTP), registers the sensor with the Cyber Vision Center, and performs an automatic reboot to complete the setup.

Verify Sensor VM deployment status and connectivity in Cisco Cyber Vision

Confirms the successful deployment and connectivity of the sensor VM within the Cisco Cyber Vision environment. This procedure ensures that the sensor is actively capturing and processing network traffic data.

After Sensor VM is deployed, ensure that the sensor VM is operational, connected, and actively monitoring network traffic in the Cisco Cyber Vision environment.

Follow these steps to verify the sensor VM deployment and connectivity.

Procedure

1. Log in to Cisco Cyber Vision Center and choose **Admin** > **Sensors** > **Sensor Explorer** .
2. Confirm that the newly deployed sensor appears in the sensor list.
3. Select the sensor from the list and click **Go to statistic** from the right pane.
4. Verify that the sensor is connected.

   The Captured Packets section displays new data on dropped and processed packets.
5. Alternatively, choose **Explore** > **All Data** > **Map** to view the network traffic data and components that are connected.

4 Sensor configuration

Topics:

- Configure Active Discovery
- Sensor configuration template
- Capture mode

Outlines sensor configuration workflows, including instructions for active discovery setup, management of sensor configuration templates with creation, export, and import tasks, and capture mode configuration to tailor sensor operation.

Configure Active Discovery

Provides instructions for configuring Active Discovery, including setting parameters such as IP address, prefix length, and VLAN number for simultaneous subnetworks scanning.

Once the sensor connects, you can modify the Active Discovery network interface configuration to:

- Add multiple network interfaces for the sensor to perform Active Discovery on several subnetworks simultaneously.
- Delete an Active Discovery network interface.
- Change the configuration of an Active Discovery network interface.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the sensor to configure and click the **Active Discovery** button on its right side panel.

   The ACTIVE DISCOVERY CONFIGURATION appears with the interface currently set.
3. To add a new network interface, click **New network interface**.
4. Enter the following parameters to set dedicated network interfaces:
   - IP address
   - Prefix length
   - VLAN number
5. Click **Add**.

   You can add as many network interfaces as needed.
6. Click **Configure**.

   A message indicates that the configuration applies successfully.

Sensor configuration template

Provides instructions for setting up sensor configuration templates to ensure consistent monitoring across the network. This process helps administrators standardize sensor settings for improved operational efficiency.

This reference defines the parameters and configuration steps required to deploy sensor templates effectively.

Templates

Describes the functionality of sensor templates for managing protocol configurations and DPI engine settings. These templates ensure accurate packet analysis and protocol representation within the user interface.

In Cisco Cyber Vision, the Template page allows you to create and set templates with protocol configurations and assign them to specific sensors.

- Enables or disables protocol DPI engines to control analysis scope.
- Maps UDP and TCP ports to ensure packets reach the correct DPI engine.

- Associates a single template with each sensor for consistent deployment.

Template Configuration and Deployment

Enable or disable a protocol DPI engine to choose which protocols to analyze. Disable a protocol DPI engine to avoid false positives in Cisco Cyber Vision. This occurs when a protocol appears on the user interface but is not present because the same UDP/TCP ports can be used by other non-standardized protocols.

Although UDP/TCP port configurations are mostly standardized, conflicts still occur with field-specific or with limited usage. Map UDP/TCP port numbers to ensure packets are sent to the correct DPI engine for accurate analysis and representation in the user interface. Sending the protocol's packet to the wrong port results in related information appearing in Security Insights/Flows without a tag.

The Default template disables some protocols because they are not commonly used or are specific to fields like transportation. The Default template applies to all compatible sensors.

Template deployment fails under the following conditions:

- The sensor is disconnected.
- There are connection issues.
- The sensor version is too old.

Create templates

Configures sensor templates to define protocol DPI engine settings and assign them to specific sensors. This process ensures consistent monitoring configurations across the network environment.

Cisco Cyber Vision enables you to create sensor templates and assign them to specific sensors.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Templates**, click **Add sensor template** button.

   The **CREATE SENSOR TEMPLATE** window appears.

2. Add a name to the template.

   (Optional) You can add a description.

3. Click **Next** .

   The list of protocol DPI engines with their basic configurations appears.

4. In the search bar, type the protocol you want to configure.
5. To edit its settings, click the **pen** icon under the **Port Mapping** column.

   The protocol's port mapping window appears.

   a) Enter the port numbers you want to add.

   > **Note**
   >
   > If you have continuous port numbers, you can enter a port range. For example, type 15000-15003 for ports 15000, 15001, 15002, and 15003.

   b) Click **OK** .

The port number is added to the protocol's default settings.

6. Enable the toggle button **Displayed modified only** to quickly find the protocol.
7. Click **Next** .
8. Select the check boxes for the sensors to which you want to apply the template and click **Next** .
9. Check the template configurations and click **Confirm** .

   The configuration is sent to the sensors. Configuration deployment will take a few moments.

   The OPCUA template appears in the template list with its two assigned sensors.

Export templates

Exports a template from one center to migrate it to another location. This process allows for the efficient transfer of configuration settings between systems.

You can use this feature to define the template at one center and then migrate it to another.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Templates**.
2. Locate the template and hover over the ellipsis (...) in the **Actions** column.
3. Click **Export** from the drop-down list.

   Your system downloads the template to its local location.

Import templates

Imports sensor templates into the system to apply configuration settings to selected sensors. This process involves uploading a template file and mapping it to specific sensors within the administration interface.

To import the sensor templates:

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Templates**.
2. Click **Import sensor template**.

   The system's local folder will opens.

3. Select the template and click **Open**.

   The system displays the imported template on the **Configuration Template** page.

4. Locate the template and hover over the ellipsis (...) in the **Actions** column.
5. Click **Edit** from the dropdown list.
6. From the **Select sensors** tab, check the check boxes of the sensors to which you want to apply the template.
7. Click **Next**.
8. Check the details and click **Update**.

The template recovers all the changes made in the previous center, and will be applied to the selected sensors.

Capture mode

Describes the capture mode feature, which enables users to select specific network communications for sensor analysis. This process optimizes monitoring efficiency and reduces the load on the Center by filtering relevant traffic.

Capture mode is a filtering mechanism applied to sensors to define which incoming packets are analyzed and recorded in the Center database.

- Focuses monitoring on relevant traffic.
- Reduces the load on the Center.
- Improves performance on large networks.

Capture mode types

The capture modes available for sensor configuration are:

- **ALL** : The sensor analyzes all incoming flows without applying a filter and stores all flows in the Center database.
- **OPTIMAL (Default)** : The filter selects the most relevant flows based on Cisco Cyber Vision expertise and excludes multicast flows for long-term capture and monitoring.
- **INDUSTRIAL ONLY** : The filter selects only industrial protocols like Modbus, S7, and EtherNet/IP. This means that the sensor does not analyze IT flows of the monitored network, and they do not appear in the GUI.
- **CUSTOM (advanced users)** : Allows full customization of the filter using tcpdump syntax to define specific filtering rules.

Capture Mode Configuration

You can set the capture mode during the initial installation wizard or modify it at any time via the Sensor Explorer page in the GUI, provided SSH access is enabled. For example, a common filter can remove network management flows like SNMP by applying a rule such as "not (port 161 and host 10.10.10.10)".

Set a capture mode

Selects the network communications analyzed by the sensors using the capture mode feature. This configuration ensures that the system monitors the appropriate traffic for analysis.

The capture mode feature allows you to select which network communications will be analyzed by the sensors.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the name of the sensor from the label column.

   The right side panel appears with the sensor details.
3. Click **Capture mode**.

   The **CAPTURE MODE** window appears.

4. Click the radio button to select **Capture mode**.

5 Maintenance

Topics:

- Sensor self-update

Details maintenance activities for sensors, including sensor self-update processes and step-by-step instructions for updating both single and multiple sensors to support efficient sensor management and continued operational accuracy.

Sensor self-update

Describes the sensor update process in Cisco Cyber Vision. This feature enables automated sensor updates and provides the foundation for future self-update capabilities.

Cisco Cyber Vision allows sensor updates regardless of the installation method and provides the foundation for sensor self-updates.

The sensor update process follows these steps:

- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

Upgrade sensor

Updates a sensor when an alert appears on the Sensor Explorer page in the Cisco Cyber Vision Center. This process ensures the sensor runs the latest available software version.

On the Sensor Explorer page in the Cisco Cyber Vision Center, an alert appears when a sensor update is available. In the Version column, the latest version number is emphasized, and an upward arrow icon with a tooltip indicates that the sensor can be upgraded

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the sensor that is upgradeable from the **Label** column.
   The right side panel appears with sensor details.
3. Click **Update**.

Update multiple sensors

Updates multiple sensors simultaneously using the Sensor Explorer interface. This procedure ensures that selected devices receive the latest configuration or firmware version.

Cisco Cyber Vision enables you to update multiple sensors simultaneously using the Sensor Explorer interface.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Check the check boxes to select multiple sensors.
3. Click the drop-down arrow of the **More Actions** button.
4. Select **Update sensors** from the drop-down list.

   The **UPDATE SENSORS** pop-up appears.
5. Click **OK**.

During the update, an in-progress indicator appears in the **Update Status** column to show that the update is underway. After the update is complete, the version number is displayed in its standard format, and a check mark icon appears in the same column to confirm that the update was successful.

6 Troubleshooting

Topics:

- Troubleshoot sensor update failures
- Sensor VM deployment issues
- Sensor VM deployment risks and mitigations

Explains troubleshooting steps for resolving sensor update failures, addresses typical deployment issues encountered in sensor VMs, and describes mitigations for sensor VM deployment risks to ensure effective problem identification and remediation in sensor environments.

Troubleshoot sensor update failures

Identifies the cause of an unsuccessful update by reviewing the status details in the Sensor Explorer. This procedure helps isolate network connectivity issues, software state inconsistencies, or resource constraints.

When a Sensor VM update fails, it is typically due to network connectivity issues, software state inconsistencies, or resource constraints. The following troubleshooting steps allow you to systematically isolate the cause of the failure.

Follow these steps to view and verify update status.

Procedure

1. Verify version mismatch in Sensor Explorer. An update may fail if the Sensor VM is in an unexpected state or if there is a version conflict between the Center and the sensor.
   a) Log in to the Cyber Vision Center web interface.
   b) From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
   c) Locate your Sensor VM in the list and check the current version and Center-supported version.
   d) If the sensor version differs from the Center-supported version, ensure the update package is available on the Center and re-trigger the update.

   Or,

2. Verify Center reachability (Port 443). The Sensor VM must maintain a stable HTTPS connection to the Center to pull update packages.
   a) Access the Sensor VM command line via SSH or the hypervisor console.
   b) Test the connection to the Center using the curl command.

   ```
   curl -v https://<Center_IP_or_FQDN>:443
   ```

   c) If the connection fails, verify the firewall rules (host, network, and Center) and ensure the Center is reachable on the network..

   Or,

3. Verify available disk space. Insufficient disk space on the Sensor VM will prevent the download and extraction of update files.
   a) Access the Sensor VM command line.
   b) Run the following command to check disk usage:

   ```
   df -h
   ```

   c) Review the output for the root partition (/) or partitions where update logs/files are stored (e.g., /var) .

   > **Note**
   >
   > Sufficient free space should be available (typically at least 10–20% free)

   d) If disk space is low, remove unnecessary files (logs, old captures, temporary files) or expand the disk if required.

Sensor VM deployment issues

Describes common diagnostic checks and resolution steps for sensor deployment and operational issues. This guide assists in isolating connectivity, traffic, and discovery problems within virtual environments.

This section provides a structured approach to diagnosing and resolving common issues encountered during sensor deployment and operation. The checks below are grouped by symptom, along with corresponding actions and expected outcomes to help isolate and resolve problems efficiently.

Sensor does not appear in Center

If the sensor is not visible in the Center, perform these checks:

Check	Action	Expected Result
Console banner	Check VM console after boot	Displays **Sensor VM instance** in console
ISO mounted	Verify VM settings - CD/DVD	**Connected** and **Connect at power on** are enabled
eth0 connectivity	Run `ping <Center_IP>` from sensor	Successful response
FQDN resolution	Run `nslookup <Center_FQDN>`	Resolves to correct Center IP
Ports open	Run `curl -k https://<Center_IP>:443`	Returns HTTP response
Time synchronization	Run `timedatectl`	Time is in sync with Center (within a few seconds)

Sensor connected but no traffic observed

If the sensor is connected to the Center but not receiving traffic:

Check	Action	Expected Result
Traffic on host NIC	Run `tcpdump -ni eth1 -c 50` on sensor	Captured frames are visible
Promiscuous Mode	Verify port group security settings	Set to **Accept**
VLAN allowed on trunk	Switch: `show interfaces switchport`	Required VLAN is in allowed list
RSPAN configuration	Switch: `show vlan id <id>`	VLAN includes **remote-span** keyword
Port group VLAN	Check ESXi port group configuration	Correct VLAN ID configured
Monitor session	Switch: `show monitor session all`	Source and destination configured correctly

Active Discovery failures

If Active Discovery is not discovering devices or is timing out

Table 12: Common root cause

Issue / Symptom	Root Cause	Corrective Action
ESXi Active Discovery Failure	Active Discovery port group set to a specific VLAN ID instead of 4095.	Set the Active Discovery port group to VLAN 4095 to enable transparent trunking.
Hyper-V Active Discovery Failure	Active Discovery adapter missing Trunk mode or allowed VLAN list.	Enable Trunk mode and explicitly add the Active Discovery VLAN to the Allowed VLAN list.
Switch Trunk Block	The network switch trunk does not allow the Active Discovery VLAN.	Update the switch trunk configuration to allow the Active Discovery VLAN.
Traffic Path Failure	Active Discovery traffic is not reaching OT devices via the switch.	Ensure bidirectional reachability; verify the sensor can ping the OT target and vice versa via the switch.

Table 13: Additional checks

Check	Action	Expected Result
Ping from sensor	Run `ping <target_IP>` from sensor VM	Receives replies
ARP resolution	Check ARP table on sensor	Valid MAC address entry exists
Port group VLAN mode (when VLAN configured in Center)	Verify Active Discovery port group in hypervisor	ESXi - set the Active Discovery port group VLAN ID to 4095. Hyper-V - configure the Active Discovery network adapter in trunk mode and allow the required Active Discovery VLAN IDs.
Switch allows Active Discovery VLAN on trunk	Switch: `show interfaces switchport` or allowed VLAN list	Active Discovery VLAN is present in the allowed VLAN list on the trunk connected to the sensor Active Discovery uplink.
Bidirectional reachability on Active Discovery VLAN	Ping tests (Sensor to OT target; Switch SVI to Sensor)	Successful replies; traffic must route through the switch (Active Discovery does not bypass the switch).
Forged Transmits	Check ESXi port group security	Set to **Accept** (if Active Discovery uses different source MAC)

Sensor VM deployment risks and mitigations

Identifies common risks associated with Sensor VM deployments and provides recommended mitigations to ensure system stability. Addressing these configuration pitfalls helps prevent packet loss, connectivity failures, and security misconfigurations before they impact network visibility.

Review these risks and mitigations to ensure your Sensor VM deployment maintains optimal system stability and performance.

Risk	Impact	Mitigation
Oversubscribed capture link	Packet loss on mirrored traffic.	Size link; mirror only needed VLANs; use higher-speed uplinks.
Promiscuous Mode on wrong port group	Exposes traffic to all VMs on that group.	Only enable on dedicated capture port groups.
SPAN destination port misconfiguration	Loss of Active Discovery if sharing same port.	Use RSPAN when Active Discovery shares the link.
Missing remote-span keyword	Mirrored traffic not delivered.	Verify all switches in path.
Wrong VLAN mode on AD port group (VLAN set in Center)	ARP failure - sensor cannot reach OT targets on Active Discovery VLAN.	For ESXi, set the Active Discovery port group VLAN ID to 4095. Ensure the physical switch trunk allows the Active Discovery VLAN. For Hyper-V, configure the Active Discovery network adapter in trunk mode and allow the required Active Discovery VLAN IDs.
Single point of failure	All capture or Active Discovery lost if link down.	NIC teaming or redundant uplinks.