Deploy the ExtraHop sensor on VMware

Published: 2025-01-10

The following procedures explain how to deploy a virtual ExtraHop sensor on a VMware ESXi/ESX platform. You must have experience deploying virtual machines in vSphere within your virtual network infrastructure.

An ExtraHop virtual sensor can help you to monitor the performance of your applications across internal networks, the public internet, or a virtual desktop interface (VDI), including database and storage tiers. The ExtraHop system can monitor application performance across geographically distributed environments, such as branch offices or virtualized environments through inter-VM traffic.

This installation enables you to run network performance monitoring, network detection and response, and intrusion detection on a single sensor.

> ⚠ **Important:** The IDS module requires the NDR module. Before you can enable the IDS module on this sensor, you must upgrade the sensor firmware to version 9.6 or later. When the upgrade completes, you can apply the new license to the sensor.

> 📄 **Note:** Throughput ⧉ might be affected when more than one module is enabled on the sensor.

System requirements

Your environment must meet the following requirements to deploy a virtual ExtraHop sensor in VMware vSphere:

- You must have familiarity with administering VMware vSphere.

  > 📄 **Note:** The images in this guide are examples only, and some of the menu selections might have changed.
- You must have the ExtraHop deployment file, which is available on the ExtraHop Customer Portal ⧉
- You must have an ExtraHop sensor product key.
- You should upgrade to the latest patch for the vSphere environment to avoid any known issues.

Virtual machine requirements

You must provision a VMware vSphere virtual machine that most closely matches the virtual ExtraHop sensor size and meets module requirements.

Sensor	Modules	CPU	RAM	Disk
Reveal(x) EDA 1100v	NDR, NPM	4 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.	8 GB	46 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)
EDA 6100v	NDR, NPM	18 processing cores with hyper-threading support,	64 GB	1 TB or larger disk for data storage (thick-provisioned)

Sensor	Modules	CPU	RAM	Disk
		VT-x or AMD-V technology, and 64-bit architecture. Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.		500 GB or smaller disk for packet captures (thick-provisioned)
EDA 6320v	NDR, NPM, IDS	32 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.	96 GB	1.4 TB or larger disk for data storage (thick-provisioned) 500 GB or smaller disk for packet captures (thick-provisioned)
EDA 8320v	NDR, NPM, IDS	64 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.	192 GB	2 TB or larger disk for data storage (thick-provisioned) 500 GB or smaller disk for packet captures (thick-provisioned)

Hypervisor specifications

Your hypervisor must be able to support the following specifications for the virtual sensor.

- VMware ESX/ESXi server version 6.5 or later
- VMware vSphere client to deploy the OVF file and to manage the virtual machine
- (Optional) If you want to enable packet captures, configure an additional storage disk during deployment

Additional guidelines

To ensure proper functionality of the virtual sensor:

- Make sure that the VMware ESX/ESXi server is configured with the correct date and time.
- Always choose thick provisioning. The ExtraHop datastore requires low-level access to the complete drive and is not able to grow dynamically with thin provisioning. Thin provisioning can cause metric loss, VM lockups, and capture issues.
- Do not change the default disk size on initial installation. The default disk size ensures correct lookback for ExtraHop metrics and proper system functionality. If your configuration requires a different disk size, contact your ExtraHop representative before you make any changes.
- Do not migrate the VM. Although it is possible to migrate when the datastore is on a remote SAN, ExtraHop does not recommend this configuration. If you must migrate the VM to a different host, shut

down the virtual sensor first and then migrate with a tool such as VMware VMotion. Live migration is not supported.

⚠ **Important:** If you want to deploy more than one ExtraHop virtual sensor, create the new instance with the original deployment package or clone an existing instance that has never been started.

Network requirements

The following table provides guidance about configuring network ports for your virtual sensor.

Sensor	Modules	Management	Monitor
EDA 1100v	NDR, NPM	One 1 GbE network port is required (for management). The management interface must be accessible on port 443. The management interface can be configured as an additional ERSPAN/RPCAP target.	A 1 GbE network port is recommended for the physical port mirror. The physical port mirror interface must be connected to the port mirror destination on the switch.
EDA 6100v	NDR, NPM	One 1 GbE network port is required (for management). The management interface must be accessible on port 443. The management interface can be configured as an additional ERSPAN/RPCAP target.	A 10 GbE network port is recommended for the physical port mirror. The physical port mirror interface must be connected to the port mirror destination on the switch. Optionally, you can configure one to three additional network interfaces to receive packet monitor traffic. Adding additional packet monitoring interfaces might reduce overall performance.
EDA 6320v	NDR, NPM, IDS	One 1 GbE network port is required (for management). The management interface must be accessible on port 443. The management interface can be configured as an additional ERSPAN/RPCAP target.	A 10 GbE network port is recommended for the physical port mirror. The physical port mirror interface must be connected to the port mirror destination on the switch.
EDA 8320v	NDR, NPM, IDS	One 1 GbE network port is required (for management). The management interface	A 25 GbE or higher network port is recommended for the physical port mirror.

Sensor	Modules	Management	Monitor
		must be accessible on port 443. The management interface can be configured as an additional ERSPAN/ RPCAP target.	The physical port mirror interface must be connected to the port mirror destination on the switch.

> (!) **Important:** To ensure the best performance for initial device synchronization, connect all sensors to the console and then configure network traffic forwarding to the sensors.

> **Note:** For registration purposes, the virtual sensor requires outbound DNS connectivity on UDP port 53 unless managed by an ExtraHop console.

Deploy the OVA file through the VMware vSphere web client

ExtraHop distributes the virtual sensor package in the open virtual appliance (OVA) format.

Before you begin
If you have not already done so, download the ExtraHop virtual sensor OVA file for VMware from the ExtraHop Customer Portal ⧉.

1. Start the VMware vSphere web client and connect to your ESX server.
2. Select the data center where you want to deploy the virtual sensor.
3. From the Actions menu, select **Deploy OVF Template...**.
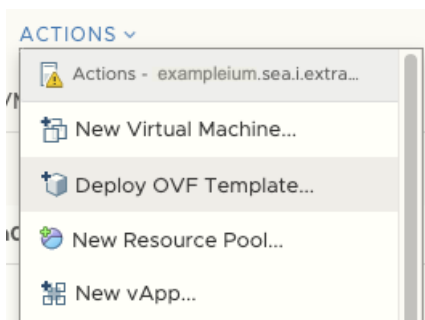
4. Follow the wizard prompts to deploy the virtual machine.
   For most deployments, the default settings are sufficient.
   a) Select Local file and then click **Choose Files**.
   b) Select the OVA file on your local machine and then click **Open**.
   c) Click **Next**.
   d) Specify a name and location for the sensor and then click **Next**.
   e) Select the destination compute resource location, verify that the compatibility checks are successful, and then click **Next**.
   f) Review the template details and then click **Next**.
   g) For Disk Format, select **Thick Provision Lazy Zeroed** and then click **Next**.
   h) Map the OVF-configured network interface labels with the correct ESXi-configured interface labels and then click **Next**.
   i) Verify the configuration and then click **Finish** to begin the deployment.
      When the deployment is complete, you can see the unique name you assigned to the ExtraHop VM instance in the inventory tree for the ESX server to which it was deployed.
5. Configure the network adapter on the virtual sensor, if necessary.

The sensor contains a preconfigured bridged virtual interface with the network label, VM Network. So if your ESX has a different interface label, you must reconfigure the virtual sensor network adapter before starting the sensor.

    a)   Select the Summary tab.

    b)   Click **Edit Settings** and select **Network adapter 1**.

    c)   From the **Network label** drop-down menu, select the correct network label, and then click **OK**.

6.   Select the virtual sensor in the ESX Inventory, and then from the Actions menu, select **Open Console**.

7.   Click the console window and then press ENTER to display the IP address.

> **Note:** DHCP is enabled by default on the ExtraHop virtual sensor. To configure a static IP address, see Configure a static IP address through the CLI.

8.   In VMware ESXi, configure the virtual switch to receive traffic and restart to see the changes.

Add a packet capture disk in VMware vSphere

If your sensor is licensed for packet capture you must configure an additional disk to store the packet capture files.

1.   Select your sensor virtual machine in the Virtual Machines inventory list.

2.   From the **Actions** drop-down menu, select **Edit Settings**.

3.   Click **Add New Device** and then click **Hard Disk**.

4.   In the New Hard disk field, type a disk size, based on the sensor you are deploying:

- 250 GB for the EDA 1100v
- 500 GB for the EDA 6100v
- 500 GB for the EDA 6320v
- 500 GB for the EDA 8320v

5.   Expand the New Hard disk settings and confirm that **Thick Provision Lazy Zeroed** is selected for Disk Provisioning.

     The remaining disk settings do not need to be changed.

6.   Click **OK**.

Configure a static IP address through the CLI

The ExtraHop system is configured by default with DHCP enabled. If your network does not support DHCP, no IP address is acquired, and you must configure a static address manually.

You can manually configure a static IP address for the ExtraHop system from the CLI.

> **⚠ Important:** We strongly recommend configuring a unique hostname ⤢. If the system IP address changes, the ExtraHop console can re-establish connection easily to the system by hostname.

1. Access the CLI through an SSH connection, by connecting a USB keyboard and SVGA monitor to the physical ExtraHop appliance, or through an RS-232 serial (null modem) cable and a terminal emulator program. Set the terminal emulator to 115200 baud with 8 data bits, no parity, 1 stop bit (8N1), and hardware flow control disabled.
2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type `default`, and then press ENTER.
4. To configure the static IP address, run the following commands:

   a) Enable privileged commands:

   ```
   enable
   ```

   b) At the password prompt, type `default`, and then press ENTER.
   c) Enter configuration mode:

   ```
   configure
   ```

   d) Enter interface configuration mode:

   ```
   interface
   ```

   e) Specify the IP address and DNS settings in the following format:
   `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`
   For example:

   ```
   ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
   ```

   f) Leave interface configuration mode:

   ```
   exit
   ```

   g) Save the running configuration file:

   ```
   running_config save
   ```

   h) Type `y` and then press ENTER.

Configure the sensor

Before you begin
Before you can configure the sensor, you must have already configured a management IP address.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

   The default login name is `setup` and the password is the VM instance ID.The default login name is `setup` and the password is `default`.

2. Accept the license agreement and then log in.

3. Follow the prompts to enter the product key, change the default setup and shell user account passwords, connect to ExtraHop Cloud Services, and connect to an ExtraHop console.

Next steps
After the system is licensed, and you have verified that traffic is detected, complete the recommended procedures in the post-deployment checklist ⧉.

Related documentation

For information about configuring RSPAN, ERSPAN, and RPCAP to monitor remote devices, see the following topics.

- Configure RSPAN with VMware ⧉
- Configure ERSPAN with VMware ⧉
- Configure ERSPAN with the Nexus 1000V ⧉
- Packet Forwarding with RPCAP ⧉

For information about mirroring traffic with VMware, see Mirror Wire Data with VMware ⧉.