

Deploy the ExtraHop sensor with VMware

Published: 2022-06-30

Published: 2022-06-30

The 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 intra-VM traffic.

Before you begin

- You must have familiarity with administering VMware. The images in this guide are from VMware version 6.7, and some of the menu selections might have changed.
- We recommend that you upgrade to the latest patch for the vSphere environment to avoid any known issues.

This guide explains how to deploy the following ExtraHop virtual sensors on the VMware ESXi/ESX platform:

- EDA 1000v (Monitors up to 250 devices)
- Reveal(x) EDA 1100v (Monitors up to 250 devices)
- EDA 2000v (Monitors up to 1000 devices)
- EDA 6100v (Monitors up to 3000 devices)

Virtual machine requirements

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


- VMware ESX/ESXi server version 5.5 or later
- 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
- The following table provides the server hardware requirements for each Discover appliance model:

Sensor	CPU	RAM	Disk
EDA 1000v	2 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support. If you want to enable SSL decryption, 3 CPUs are required. For more information, see Add a CPU Core to the EDA 1000v with VMware .	4 GB	46 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)
Reveal(x) EDA 1100v	4 processing cores with hyper-threading support, VT-x or AMD-V technology, and	8 GB	46 GB or larger disk for data storage (thick-provisioned)

Sensor	CPU	RAM	Disk
	64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support.		250 GB or smaller disk for packet captures (thick-provisioned)
EDA 2000v	6 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support.	6 GB	255 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)
EDA 6100v	16 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support.	64 GB	1 TB or larger disk for data storage (thick-provisioned) 500 GB or smaller disk for packet captures (thick-provisioned)

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 Discover appliance.

Sensor	Management	Monitor
EDA 1000v	One 1-Gbps Ethernet network port is required (for management). The management port must be accessible on port 443.	Two 1-Gbps Ethernet network ports are required. One for the physical port mirror and one for management. The physical port mirror interface must be connected to the port mirror of the switch.

Sensor	Management	Monitor
		While it is possible to configure a 10-Gbps Ethernet network port for the port mirror interface, it is not recommended as the virtual sensor cannot process more than 1 Gbps of traffic.
EDA 2000v	One 1-Gbps Ethernet network port is required (for management). The management interface must be accessible on port 443.	Two to four 1-Gbps Ethernet network ports are required for the physical port mirror and management. The physical port mirror interface must be connected to the port mirror of the switch. The VMware ESX server must support network interface drivers. While it is possible to configure a 10-Gbps Ethernet network port for the port mirror interface, it is not recommended as the virtual sensor cannot process more than 3 Gbps of traffic.
EDA 6100v	One 1-Gbps Ethernet 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-Gbps Ethernet 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. The VMware ESX server must support network interface drivers. Optionally, you can configure 1-3 1-Gbps Ethernet network ports to receive packet monitor traffic.

 **Important:** If your deployment includes a console, the following workflow ensures the best performance for initial device synchronization. First, connect all sensors to the console, 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.

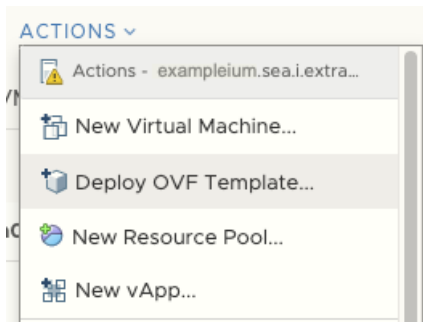
Deploy the OVA file through the VMware vSphere web client

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. Select **Deploy OVF Template...** from the Actions menu.



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 ESX-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. The sensor contains a preconfigured bridged virtual interface with the network label, VM Network. If your ESX has a different interface label, you must reconfigure the network adapter on the virtual sensor before starting the sensor.
 - a) Select the Summary tab.
 - b) Click **Edit Settings**, select **Network adapter 1**, select the correct network label from the Network label drop-down list, and then click **OK**.
6. Select the virtual sensor in the ESX Inventory and then select **Open Console** from the Actions menu.
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 the [Configure a Static IP Address](#) section.
8. In VMware ESXi, configure the virtual switch to receive traffic and restart to see the changes.

Add a packet capture disk in VMware

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 list, select **Edit Settings**.
3. Click **Add New Device** and then click **Hard Disk**.
4. In the New Hard disk field, type the following disk size, based on the sensor you are deploying:
 - 250 GB for the EDA 1000v, EDA 1100v, and EDA 2000v
 - 500 GB for the EDA 6100v

Edit Settings | example-eda-1000v



Virtual Hardware

VM Options

ADD NEW DEVICE

> CPU	2		
> Memory	4	GB	
> Hard disk 1	4	GB	
> Hard disk 2	20	GB	
> New Hard disk *	250	GB	
> SCSI controller 0	VMware Paravirtual		

- 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.
- 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.

Important: For deployments that include a sensor that is connected to an ECA VM console, we strongly recommend [configuring a unique hostname](#). If the IP address on the sensor is changed, the console can re-establish connection easily to the sensor by hostname.

- 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.
- At the login prompt, type `shell` and then press ENTER.
- At the password prompt, type `default`, and then press ENTER.
- To configure the static IP address, run the following commands:
 - Enable privileged commands:

```
enable
```

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

```
configure
```

- Enter the interface configuration mode:

```
interface
```

- Run the `ip` command and 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 the interface configuration section:

```
exit
```

- g) Save the running config file:

```
running_config save
```

- h) Type `y` and then press ENTER.

Configure the sensor

After you configure an IP address for the sensor, open a web browser and navigate to the ExtraHop system through the configured IP address. Accept the license agreement and then log in. The default login name is `setup` and the password is `default`. 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.

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](#)