Deploy the ExtraHop Flow Collector with VMware

Published: 2024-01-19

This guide explains how to deploy the ExtraHop Flow Collector virtual appliance (EFC 1290v) on the VMware ESXi/ESX platform.

The EFC 1290v is designed to connect to Reveal(x) 360 and collect flow-based traffic from your network. Features available on packet sensors, such as machine learning, rules-based detections, threat intelligence, packet analysis, and activity maps, are not available on the EFC 1290v. Triggers and Open Data Streams are supported.

The EFC 1290v supports the following flow technologies: Cisco NetFlow v5 and v9, AppFlow, IPFIX, and sFlow. For more information on collecting traffic from Netflow and sFlow devices, see Collect traffic from NetFlow and sFlow devices ⤤.

Virtual machine requirements

Your hypervisor must be able to support the following virtual machine requirements for the virtual Flow Collector appliance.

- An existing installation of VMware ESX or ESXi server version 6.5 or later capable of hosting the virtual Flow Collector appliance.
- The virtual Flow Collector appliance has the following resource requirements:

Appliance	CPU	RAM	Disk
Reveal(x) EFC 1290v	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)

The following configuration settings are required to ensure proper functionality of the virtual appliance:

- 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 appliance 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 appliance, 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 Flow Collector appliance.

Appliance	Management	Flow Network
Reveal(x) EFC 1290v	One 1-Gbps Ethernet network port is required (for management). The management port must be accessible on port 443.	One 1-Gbps Ethernet network port or virtual interface is required. The flow target interface must be connected to the source of the NetFlow traffic.

> **Note:** For registration purposes, the Flow Collector appliance requires outbound connectivity on TCP port 443.

Deploy the OVA file through the VMware vSphere web client

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

Before you begin
Download the 1100v Reveal(x) virtual Discover appliance OVA file for VMware from the ExtraHop Customer Portal ☑. The EDA 1100v appliance is automatically converted to the EFC 1290v after you register the appliance with the 1290v product key.

1. Start the VMware vSphere web client and connect to your ESX server.
2. Select the data center where you want to deploy the Flow Collector virtual appliance.
3. Select **Deploy OVF Template...** from the Actions menu.
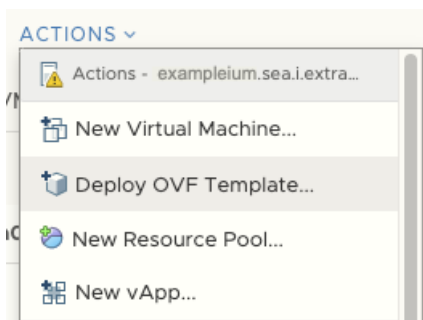
4. Follow the wizard prompts to deploy the virtual machine. For most deployments, the default settings are sufficient.
   a) Select **Local file** and then click **Choose Files**.
   b) Select the OVA file on your local machine and then click **Open**.
   c) Click **Next**.
   d) Specify a name and location for the appliance 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 to 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 Flow Collector appliance 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 Flow Collector virtual appliance before starting the appliance.

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 Flow Collector virtual appliance 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 appliance. 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 the appliance to see the changes.

Configure a static IP address through the CLI

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

1. Access the CLI through an SSH connection to the configured IP address, vSphere web console, or VMware Remote Console.

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) 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 interface configuration mode:

```
exit
```

g)   Save the running configuration file:

```
running_config save
```

h)   Type y, and then press ENTER.