


Deploy the ExtraHop Command Appliance on a Linux KVM

Published: 2018-10-27

This document provides information on how to install the ExtraHop Command virtual appliance on a Linux kernel-based virtual machine (KVM). This guide assumes that you are familiar with basic KVM administration.

If you need either the installation package files or a license key for the virtual appliance, contact support@extrahop.com

 **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.

Package contents

The installation package for KVM systems is a `tar.gz` file that contains the following items:

ECA_KVM.xml

The domain XML configuration file

extrahop-boot.qcow2

The boot disk

extrahop-data.qcow2

The datastore disk

Requirements

Before you can install the ExtraHop virtual appliance, make sure that your environment meets the following requirements:

- A KVM hypervisor environment capable of hosting a VM that has:
 - 4 GB RAM
 - Two vCPUs
 - One 4 GB boot disk (virtio-scsi interface recommended)
 - One 40 GB datastore disk (virtio-scsi interface recommended)
- An ExtraHop virtual appliance license key

Determine the best bridge configuration

Identify the bridge through which you will access the management interface of your Command appliance.

1. Make sure the management bridge is accessible to the ExtraHop virtual appliance and to all users who must access the management interface.
2. If you need to access the management interface from an external computer, configure a physical interface on the virtual management bridge.
3. (Recommended) Configure separate bridges for the Command appliance management bridge and any bridge you will capture network traffic through on other ExtraHop appliances.

Edit the domain XML configuration file

After you identify the management bridge, edit the configuration file, and create the ExtraHop virtual appliance.

1. Extract the `tar.gz` file that contains the installation package.
2. Copy the two disks `extrahop-boot.qcow2` and `extrahop-data.qcow2` to your KVM system. Make a note of the location where you store these files.
3. Open the domain XML configuration file. Find and edit the following values:
 - a) Change the VM name (`ExtraHop-ECA`) to the name you want to assign to your ExtraHop virtual appliance.

```
<name>ExtraHop-ECA</name>
```

- b) Change the source file path `[PATH_TO_STORAGE]` with the location where you stored the virtual disk files in step 1.

```
<source file='[PATH_TO_STORAGE]/extrahop-boot.qcow2' />
<source file='[PATH_TO_STORAGE]/extrahop-data.qcow2' />
```

- c) Change the source bridge for the management network (`ovsbr0`) to match the name of your management bridge.

```
<interface type='bridge'>
  <source bridge='ovsbr0' />
  <model type='virtio' />
  <alias name='net0' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
    function='0x0' />
</interface>
```

If you are configuring Open vSwitch virtual switch software for your virtual bridge, add the following `virtualport` type setting to the interface (after the source bridge setting):

```
<virtualport type='openvswitch'>
</virtualport>
```

4. Save the XML file.
5. Log in to the KVM console.
6. Create the new ExtraHop virtual appliance with your revised domain XML configuration file by running the following command:

```
virsh define ECA_KVM.xml
```

7. Start the virtual machine by running the following command:

```
virsh start <vm_name>
```

Where `<vm_name>` is the name of your virtual appliance.

Configure the Command virtual appliance

After you have created your ExtraHop virtual appliance, you can log in to the management interface through a web browser and apply your license key, see network traffic, and customize your ExtraHop virtual appliance.

1. Log into the KVM console and view the IP address for your new ExtraHop virtual appliance by running the following command:

```
sudo virsh console <vm_name>
```

Where `<vm_name>` is the name of your ExtraHop virtual appliance.

2. Open your web browser and type the IP address of your ExtraHop virtual appliance.
3. Log in with the default user name (`setup`) and password (`default`).

Register the ExtraHop appliance

Complete the following steps to apply a product key supplied by ExtraHop Support.

If you do not have a product key, contact support@extrahop.com.



Tip: To verify that your environment can resolve DNS entries for the ExtraHop licensing server, open a terminal application on your Windows, Linux, or Mac OS client and run the following command:

```
nslookup -type=NS d.extrahop.com
```

If the name resolution is successful, output similar to the following appears:

```
Non-authoritative answer:
d.extrahop.com nameserver = ns0.use.d.extrahop.com.
d.extrahop.com nameserver = ns0.usw.d.extrahop.com.
```

1. In your browser, type the URL of the ExtraHop Admin UI, `https://<extrahop_ip_address>/admin`.
2. Review the license agreement, select **I Agree**, and then click **Submit**.
3. On the login screen, type `setup` for the username.
4. For the password, select from the following options:
 - For 1U and 2U appliances, type the service tag number found on the pullout tab on the front of the appliance.
 - For the EDA 1100, type the serial number displayed in the `Appliance info` section of the LCD menu. The serial number is also printed on the bottom of the appliance.
 - For a virtual appliance, type `default`.
5. Click **Log In**.
6. In the System Settings section, click **License**.
7. Click **Manage License**.
8. Click **Register**.
9. Enter the product key and then click **Register**.
10. Click **Done**.