Deploy the ExtraHop ECA VM console on Linux KVM

Published: 2024-07-22

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

If you have not already done so, download the ExtraHop virtual console file for KVM from the ExtraHop Customer Portal.

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.

Requirements

Before you can install the ExtraHop virtual console, 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 or larger datastore disk (virtio-scsi interface recommended)

  The hypervisor CPU should provide Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.
- An ExtraHop virtual console license key

Performance guidelines

The performance of the ECA VM console depends on the number of sensors you are deploying in combination with the number of devices you expect the system to discover in your environment. To determine the appropriate sizing, see the ECA VM Console Performance Guidelines.

Package contents

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

eca.xml
: The domain XML configuration file

eca.xml.md5
: An MD5 checksum file to verify the integrity of the eca.xml file.

extrahop-boot.qcow2
: The boot disk

extrahop-boot.qcow2.md5
: An MD5 checksum file to verify the integrity of the extrahop-boot.qcow2 file.

extrahop-data.qcow2
: The datastore disk

extrahop-data.qcow2.md5

An MD5 checksum file to verify the integrity of the extrahop-data.qcow2 file.

Edit the domain XML configuration file

Edit the configuration file and create the ExtraHop virtual console.

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 console.

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

   ```
   virsh define eca.xml
   ```
7. Start the virtual machine by running the following command:

   ```
   virsh start <vm_name>
   ```

   Where *<vm_name>* is the name of the virtual console you configured in step 3.

(Optional) Configure a static IP address

By default, the ExtraHop system is configured with DHCP enabled. If your network does not support DHCP, you must configure a static address manually.

1. Log in to the KVM host.
2. Run the following command to connect to the ExtraHop system through the virtual serial console:

   ```
   virsh console <vm_name>
   ```

   Where *<vm_name>* is the name of your virtual machine.
3. Press ENTER twice to get to the system login prompt.

   ```
   ExtraHop Discover Appliance Version 7.8.2.2116
   IP: 192.0.2.81
   exampleium login:
   ```
4. At the login prompt, type `shell`, and then press ENTER.
5. At the password prompt, type `default`, and then press ENTER.
6. 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 the 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 the interface configuration section:

```
exit
```

g) Save the running config file:

```
running_config save
```

h) Type `y` and then press ENTER.

Post-deployment actions

Open a web browser and type the IP address of the ExtraHop system in the address bar and then press **ENTER**. Accept the EULA and enter the product key to license the console.

Log in to the ExtraHop system with the `setup` user account and type `default` for the password.

- Review the Discover and Command Post-deployment Checklist and configure additional settings.
- Connect an ExtraHop console to an ExtraHop sensor
- Connect the console and sensors to ExtraHop recordstores
- Connect sensors and console to the packetstore