Deploy the ExtraHop Explore Appliance on a Linux KVM

Published: 2018-07-16

The following procedures explain how to deploy an ExtraHop Explore virtual appliance on a Linux kernel-based virtual machine (KVM). You should be familiar with basic KVM administration before proceeding.

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, do not clone an existing instance. Always start with the original deployment package when deploying additional instances.

System requirements

Your environment must meet the following requirements to deploy a virtual Explore appliance:

- A KVM hypervisor environment capable of hosting the Explore virtual appliance. The Explore virtual appliance is available in the following configurations:

EXA-XS	EXA-S	EXA-M	EXA-L
4 CPUs	8 CPUs	16 CPUs	32 CPUs
8GB RAM	16 GB RAM	32 GB RAM	64 GB RAM
4 GB boot disk	4 GB boot disk	4 GB boot disk	4 GB boot disk
500 GB or smaller datastore disk	1.2 TB or smaller datastore disk	2.5 TB or smaller datastore disk	4.1 TB or smaller datastore disk

Note: When you deploy an Explore appliance, a second virtual disk is required to store record data. The EXA-XS is preconfigured with a 500 GB datastore disk; however, you must manually add a second virtual disk to the other available EXA configurations. The minimum datastore disk size for all configurations is 150 GB.

Consult with your ExtraHop sales representative or Technical Support to determine the datastore disk size that is best for your needs.

Note: For KVM deployments, virtio-scsi interface is recommended for the boot and datastore disks.

- An Explore virtual appliance license key.
- The following TCP ports must be open:
  - TCP ports 80 and 443: Enables you to administer the Explore appliance through the Web UI. Requests sent to port 80 are automatically redirected to HTTPS port 443.
  - TCP port 9443: Enables Explore nodes to communicate with other Explore nodes in the same cluster.

Package contents

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

`EXA_KVM-<x>.xml`

The domain XML configuration file

`extrahop-boot.qcow2`

The boot disk

`extrahop-data.qcow2`

The datastore disk

Deploy the Explore virtual appliance

To deploy the Explore virtual appliance, complete the following procedures:

- Determine the best virtual bridge configuration for your network
- Edit the domain XML configuration file and create your virtual appliance
- Resize the datastore disk
- Start the VM
- Configure the Explore appliance

Determine the best bridge configuration

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

1. Make sure the management bridge is accessible to the Explore 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 management bridge.

Edit the domain XML configuration file

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

1. Contact ExtraHop Support (support@extrahop.com) to obtain and download the Explore KVM package.
2. Extract the tar.gz file that contains the installation package.
3. 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.
4. Open the domain XML configuration file in a text editor and edit the following values:

   a) Change the VM name to a name for your ExtraHop virtual appliance.

   For example:

   ```
   <name>ExtraHop-EXA-S</name>
   ```

   b) Change the source file path (`[PATH_TO_STORAGE]`) to the location where you stored the virtual disk files in step 3.

   ```
   <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>
```

d) (Optional) If your virtual bridge is configured through Open vSwitch virtual switch software, add the following virtualport type setting to the interface (after the source bridge setting):

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

5. Save the XML file.
6. Create the new Explore virtual appliance with your revised domain XML configuration file by running the following command:

   ```
   virsh define <EXA_KVM_x.xml>
   ```

   Where `<EXA_KVM_x.xml>` is the name of your domain XML configuration file.

Resize the datastore disk

Resize the datastore disk so that the allotted space is large enough to store the type of records you want to store for the amount of lookback desired.

Resize the datastore disk by running the following command:

```
qemu-img resize extrahop-data.qcow2 <+nGB>
```

Where <+*nGB*> is the size of the disk.

For example:

```
qemu-img resize extrahop-data.qcow2 +100GB
```

Start the VM

1. Start the VM by running the following command:

   virsh start `<vm_name>`

   Where `<vm_name>` is the name of your ExtraHop virtual appliance you configured in step 4 of the Edit the domain XML file section.
2. Log in to the KVM console and view the IP address for your new ExtraHop virtual appliance by running the following command:

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

Configure the Explore appliance

After you obtain the IP address for the Explore appliance, log into the Explore Admin UI through the following URL: `https://<explore_ip_address>/admin` and complete the following recommended procedures.

Note: The default log in name is `setup` and the password is `default`.

- Register an ExtraHop appliance
- Create an Explore cluster

- Configure the system time
- Configure email notifications
- Pair the Explore appliance to all Discover and Command appliances
- Send record data to the Explore appliance

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.

1. In your browser, type the IP address of the ExtraHop appliance (`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 a physical appliance, type the service tag number found on the pullout tab on the front of the appliance.

     Note: The serial number for the EDA 1100 is located on the bottom of the appliance, and displayed in the `Appliance info` section of the LCD menu.
   - 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**.

Create an Explore cluster

Before you begin
Log into the Admin UI of each Explore node, click **Fingerprint** in the Status section, and note the value listed in the Fingerprint field. The fingerprint of each node should be verified during the join process.

If you are deploying three or more Explore nodes, join the nodes to create a cluster.

Important: Each node that you join must have the same configuration (physical or virtual) and ExtraHop firmware version.

1. Log into the Admin UI of any new Explore node.
2. In the Cluster Settings section, click **Join Cluster**.
3. In the Host text box, type the hostname or IP address of any of the other new nodes and then click **Continue**.
4. Verify that the fingerprint displayed on the page matches the fingerprint of the Explore node that you are joining. If these fingerprints do not match, communication between the nodes might have been intercepted and altered.
5. In the Setup Password field, type the password for the `setup` user.
6. Click **Join**.
7. In the Status section, click **Cluster Status**.
8. Wait for the Status field to change to `green`.
9. Repeat steps 1 - 8 to join each additional node to the new cluster.

Note: Always join a new node to the existing cluster and not another unjoined node, or you will create multiple clusters.

10. Click **Cluster Members** in the Cluster Settings section to confirm that all of the nodes are listed on the page.

Configure the system time

By default, the Explore appliance synchronizes the system time through the pool.ntp.org network time protocol (NTP) server. If your network environment prevents the Explore appliance from communicating with this time server, you must configure an alternate time server source.

Note: Time synchronization is critical to ensuring proper cluster operations and maintaining consistent views of data across both Discover and Explore appliances. We strongly recommend that you either keep the default system time setting or configure settings for a different NTP server.

1. In the System Settings section, click **System Time**.
2. Click **Configure Time**.
3. Click the Time Zone drop-down list and select a time zone. Click **Save and Continue**.
4. Select the Use NTP server to set time radio button and then click **Select**.
5. Type the IP addresses for the time server, and then click **Save**.
6. Click **Done**.
7. Click **Sync Now** to sync system time on the Explore appliance with the remote time server.

Configure email notifications

You must configure an email server and sender before the ExtraHop appliance can send notifications about system alerts by email.

You can receive the following alerts from the system:

- A virtual disk is in a degraded state.
- A physical disk is in a degraded state.
- A physical disk has an increasing error count.
- A registered Explore node is missing from the cluster. The node might have failed, or is powered off.

Pair the Explore appliance to Discover and Command appliances

After you deploy the Explore cluster, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore cluster before you can query records. If you manage all of your Discover appliances from a Command appliance, you only need to perform this procedure from the Command appliance.

1. Log into the Discover or Command appliance Admin UI.
2. In the ExtraHop Explore Settings section, click **Configure Explore Cluster**.
3. Click **Add New**.
4. In the Host #1 Host field, type the hostname or IP address of any Explore appliance in the Explore cluster.
5. For each additional Explore appliance in the cluster, click **Add New** and enter the individual hostname or IP address in the corresponding Host field.
6. Click **Save**.

7. Note the information listed for Fingerprint. Verify that the fingerprint listed on this page matches the fingerprint of the Explore appliance (**Host #1**) listed on the Fingerprint page in the Explore Admin UI.
8. In the Explore Setup Password field, type the password of the Explore appliance.
9. Click **Join**, and then click **Done**.

Send record data to the Explore appliance

After your Explore appliance is paired with all of your Discover and Command appliances, you must configure the type of records you want to store. See the following documentation for more information about Explore configuration settings, how to generate and store records, and how to create record queries.

- ExtraHop Explore Admin UI Guide
- ExtraHop Explore Settings section in the *ExtraHop Admin UI Guide*.
- Records section in the *ExtraHop Web UI Guide*.
- ExtraHop Trigger API Reference