Deploy the ExtraHop Explore Appliance on a Linux KVM

Published: 2017-11-15

The following procedure guides you through the deployment process of the 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-S	EXA-M	EXA-L
8 CPUs	16 CPUs	32 CPUs
32 GB RAM	64 GB RAM	128 GB RAM
4 GB boot disk (virtio-scsi interface recommended)	4 GB boot disk (virtio-scsi interface recommended)	4 GB boot disk (virtio-scsi interface recommended)
1.2 TB or smaller datastore disk (virtio-scsi interface recommended)	2.5 TB or smaller datastore disk (virtio-scsi interface recommended)	4.1 TB or smaller datastore disk (virtio-scsi interface recommended)

  Note: You must add the second virtual disk to store record data when you deploy the Explore virtual appliance. The minimum datastore disk size for all configurations is 150 GB. Consult with your ExtraHop sales representative to determine the datastore disk size that is best for your needs.
- 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, you can log into the Explore Admin UI through the following URL: `https://<explore_ip_address>/admin`.

Note: The default log in name is `setup` and the password is `default`. You can add and modify additional user names and passwords in the Explore Admin UI.

After you first log into the Explore appliance, complete the following recommended procedures:

- Register an ExtraHop appliance
- 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 log in screen, type `setup` for the user name and `default` for the password.
4. Click **Log In**.
5. In the System Settings section, click **License**.
6. Click **Manage License**.
7. Click **Register**.
8. Enter the product key and then click **Register**.
9. Click **Done**.

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.

Configure the Email Server and Sender settings:

1. In the Network Settings section, click **Notifications**.
2. Click **Email Server and Sender**.
3. On the Email Settings page, enter the following information:

- **SMTP Server:** The IP address for the outgoing SMTP mail server.

  Note: The SMTP server should be the FQDN or IP address of an outgoing mail server that is accessible from the Explore management network. If the DNS server is set, then the SMTP server can be a FQDN, otherwise it needs to be an IP address

- **Sender Address:** The email address for the notification sender.
- **Report Sender Address:** The email address for the report sender.

4. Click **Save**.

Add a recipient email address for notifications:

5. Go to the Network Settings section and click **Notifications**.
6. Under Notifications, click **Email Addresses**.
7. In the Email address text box, type the recipient email address.
8. Click **Save**.

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.

1. Log in to 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