Deploy the ExtraHop Explore Appliance on a Linux KVM

Published: 2018-07-17

In this guide, you will learn how to deploy an ExtraHop Explore virtual appliance on a Linux kernel-based virtual machine (KVM) and to join multiple Explore appliances to create an Explore cluster. You should be familiar with basic KVM administration before proceeding.

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.

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
8 GB 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 port 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:

```
virsh console <vm_name>
```

Configure a static IP address

By default, ExtraHop appliances ship with DHCP enabled. If your network does not support DHCP, you must configure a static address manually.

1. Log into the KVM host.
2. Run the following command to connect to the ExtraHop appliance 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 appliance login prompt.

```
ExtraHop Discover Appliance Version 6.2.6.3385
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.

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 login username 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.

If you do not have a product key, contact your ExtraHop account team.

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 Appliance Settings section, click **License**.
7. Click **Manage License**.
8. Click **Register**.
9. Enter the product key and then click **Register**.
10. 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 Appliance 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 **Set time with NTP server** radio button and then click **Select**.
5. Type the IP address or hostname for the time server, and then click **Save**.

   Note: You can configure up to 9 time servers.

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.

Create an Explore cluster

Published: 2018-07-17

If you are deploying more than one Explore appliance, join the appliances together to create a cluster. For optimal performance, we recommend that you set up three or more Explore appliances in a cluster to take advantage of data redundancy.

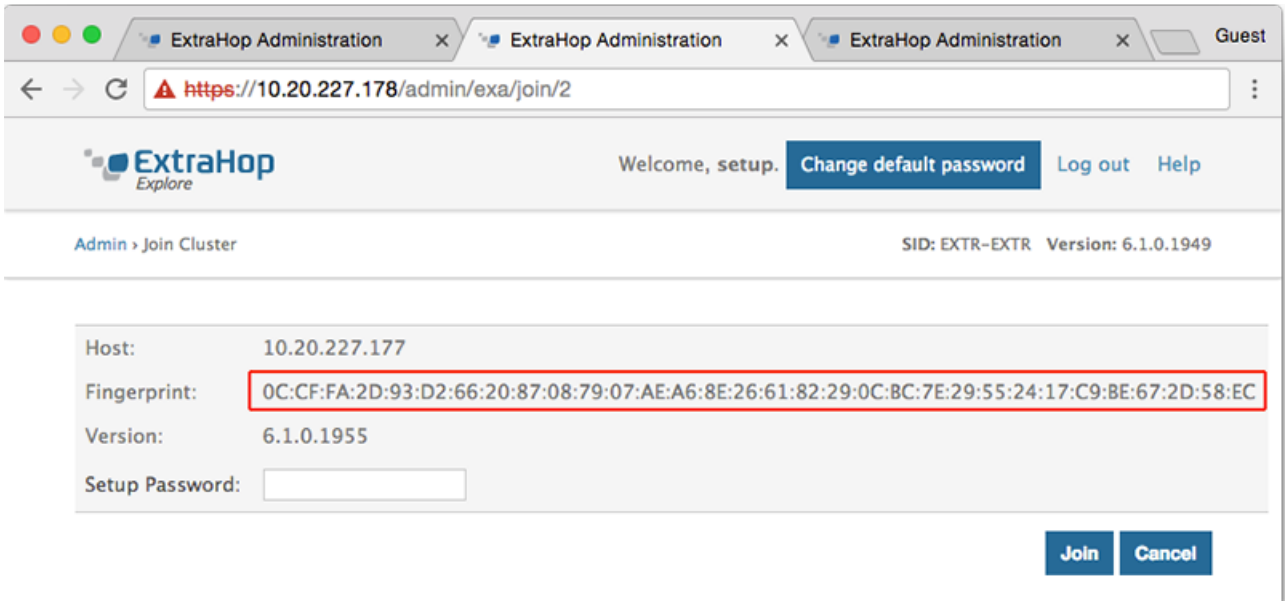
In the following example, the Explore appliances have the following IP addresses:

- Node 1: 10.20.227.177
- Node 2: 10.20.227.178
- Node 3: 10.20.227.179

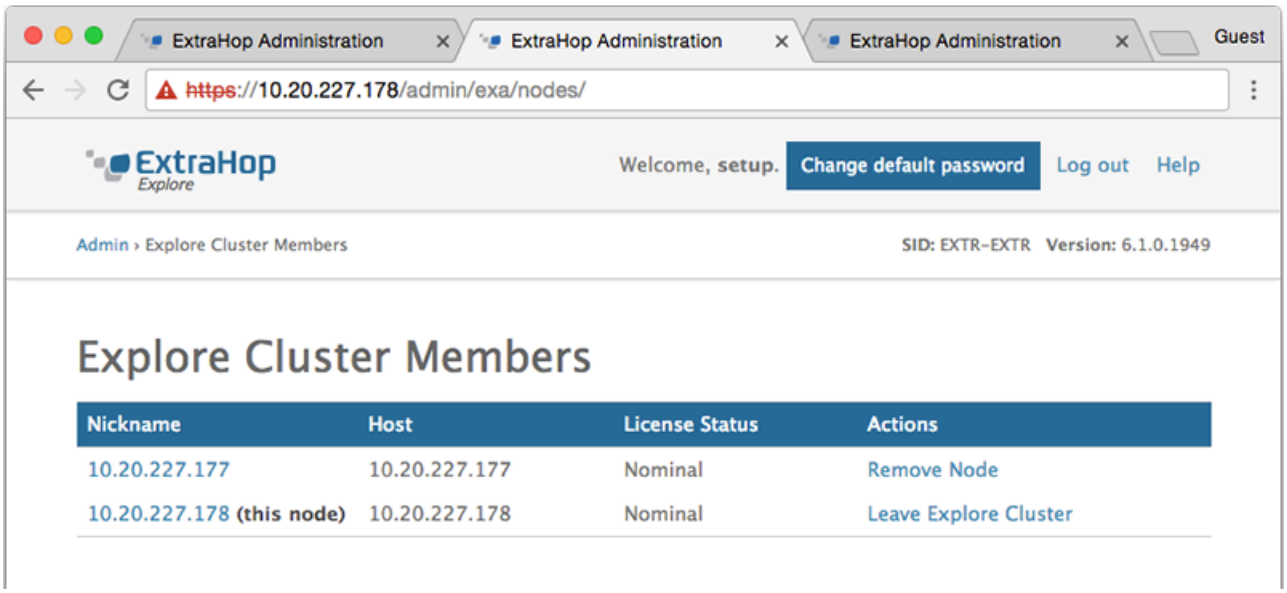
You will join nodes 2 and 3 to node 1 to create the Explore cluster.

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 all three Explore appliances with the setup user account in three separate browser windows or tabs.
2. Select the browser window of node 1.
3. In the Status and Diagnostics section, click **Fingerprint** and note the fingerprint value. You will later confirm that the fingerprint for node 1 matches when you join the remaining two nodes.
4. Select the browser window of node 2.
5. In the Explore Cluster Settings section, click **Join Cluster**.
6. In the Host field, type the hostname or IP address of node 1 and then click **Continue**.
7. Confirm that the fingerprint on this page matches the fingerprint you noted in step 3.

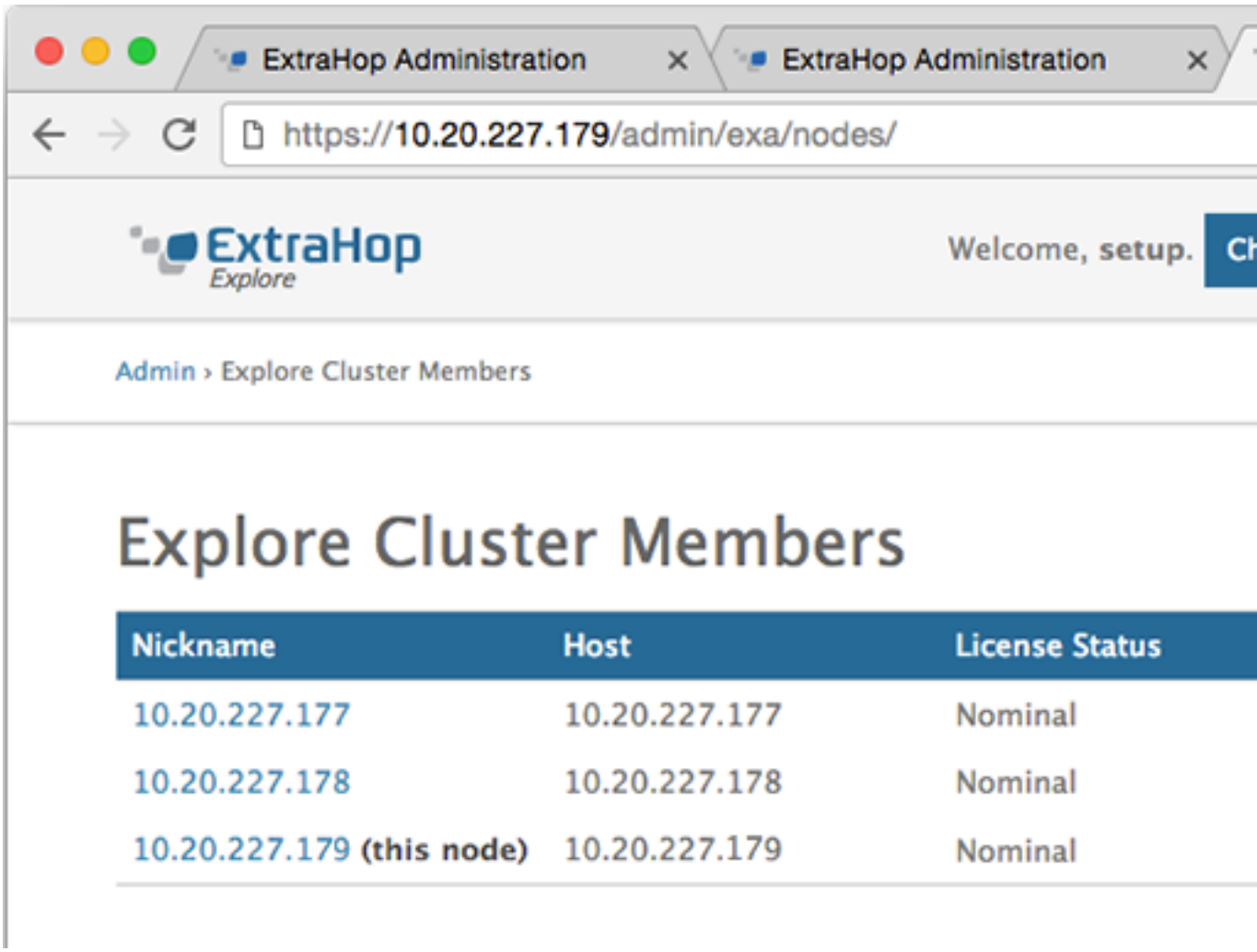


8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**.
   When the join is complete, the Explore Cluster Settings section has two new entries: **Explore Cluster Members** and **Data Management**.
9. Click Explore Cluster Members. You should see node 1 and node 2 in the list.



10. In the Status and Diagnostics section, click **Explore Cluster Status**. Wait for the Status field to change to `Green` before adding the next node.
11. Repeat steps 5 - 11 to join each additional node to the new cluster.

    Note: To avoid creating multiple clusters, always join a new node to the existing cluster and not to another single appliance.
12. When you have added all of your Explore appliances to the cluster, click **Explore Cluster Members** in the Explore Cluster Settings section. You should see all of the joined nodes in the list, similar to the following figure.



13. In the Explore Cluster Settings section, click **Data Management** and make sure that **Replication Level** is set to **1** and **Shard Reallocation** is **ON**.

Connect the Explore appliance to Discover and Command appliances

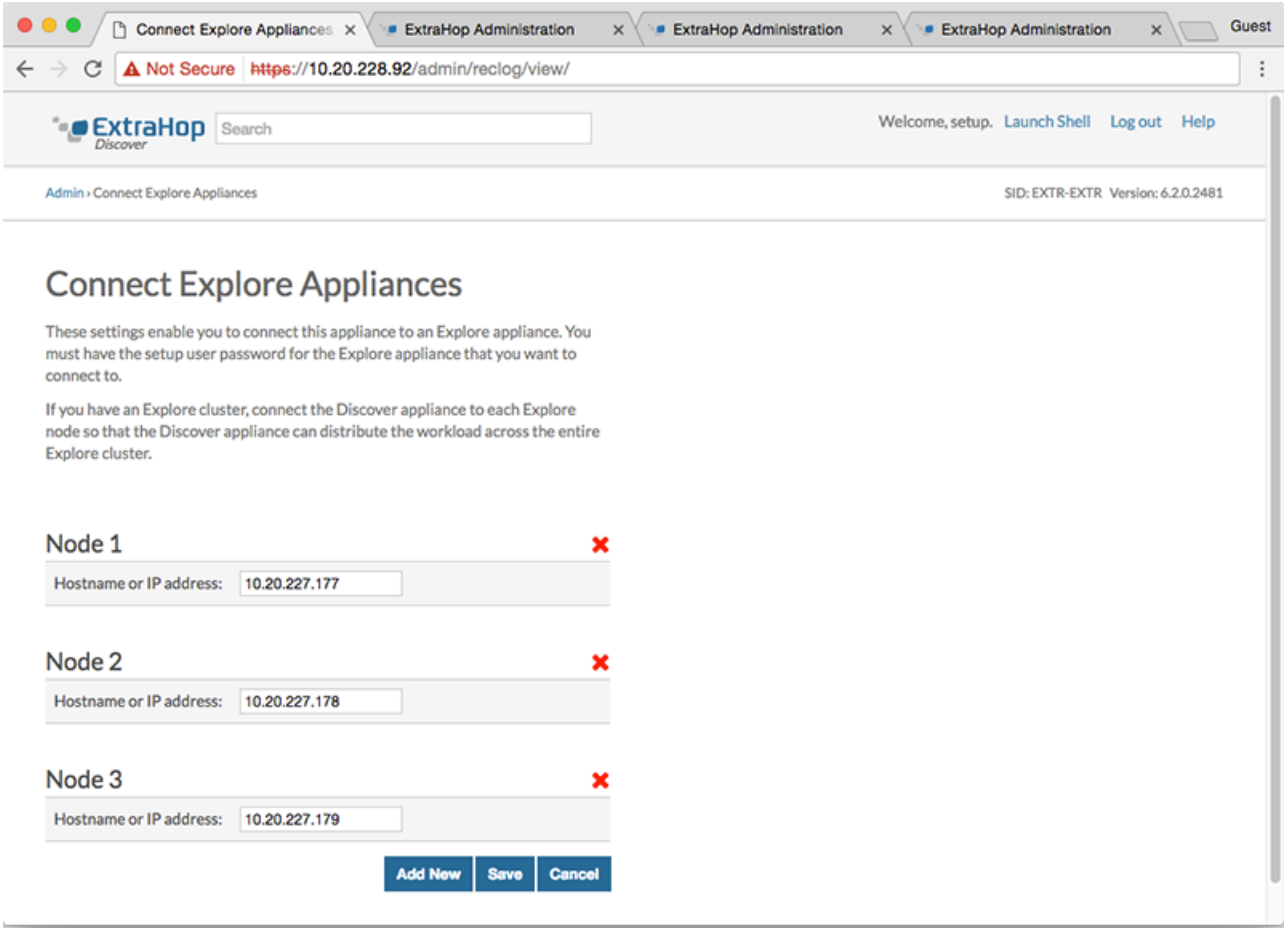
Published: 2018-07-17

After you deploy the Explore appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore appliance before you can query records.

Important: If you have an Explore cluster of three or more Explore nodes, connect the Discover appliance to each Explore node so that the Discover appliance can distribute the workload across the entire Explore cluster.

Note: 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 Admin UI of the Discover or Command appliance .
2. In the ExtraHop Explore Settings section, click **Connect Explore Appliances**.
3. Click **Add New**.
4. In the Explore node 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 Explore node field.



6. Click **Save**.

7. Confirm that the fingerprint on this page matches the fingerprint of node 1 of the Explore cluster.
8. In the Explore Setup Password field, type the password for the Explore node 1 `setup` user account and then click **Connect**.
9. When the Explore Cluster settings are saved, click **Done**.

Next steps

Important: If you only deployed a single Explore appliance, after you connect to your Discover or Command appliance, you must log into the Admin UI on the Explore appliance and set the **Explore Cluster Settings** > **Data Management** > **Replication Level** to **0**.

Send record data to the Explore appliance

Published: 2018-07-17

After your Explore appliance is connected to 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