Deploy the ExtraHop Explore Appliance with VMware

Published: 2018-07-07

In this guide, you will learn how to deploy the ExtraHop Explore virtual appliance with the vSphere client running on a Windows machine and to join multiple Explore appliances to create an Explore cluster. You should be familiar with administrating VMware ESX and ESXi environments before proceeding.

The Explore virtual appliance is distributed as an OVA package that includes a preconfigured virtual machine (VM) with a 64-bit, Linux-based OS that is optimized to work with VMware ESX and ESXi version 5.5 and later.

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:

- An existing installation of VMware ESX or ESXi server version 5.5 or later 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.
- A vSphere client
- 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.

Deploy the Explore virtual appliance

Before you begin

If you have not already done so, download the ExtraHop Explore virtual appliance OVA file for VMware from the ExtraHop Customer Portal.

1. Start the VMware vSphere client and connect to your ESX server.
2. Go to the File menu and select **Deploy OVF Template**.
3. The steps to deploy the OVF template are described in detail below. For most deployments, the default settings are sufficient.
   a) Source: Browse to the location of the downloaded OVA file and then click **Next**.
   b) OVF Template Details: Review the details and then click **Next**.
   c) Name and Location: Configure the VM name and location. Give the VM a unique and specific name for the ESX Inventory and then click **Next**.
   d) Disk Format: Select **Thick Provision Lazy Zeroed** and then click **Next**.
   e) Network Mapping: Map the OVF-configured network interface labels with the correct ESX-configured interface labels and then click **Next**.
   f) Ready to Complete: Verify the configuration, do not select the Power on after deployment checkbox, and then click **Finish** to complete the deployment.

   When the deployment is complete, you can see the unique name you assigned to the Explore appliance VM instance in the inventory tree for the ESX server to which it was deployed.
4. Click the new Explore appliance VM instance in the directory tree.
5. From the Actions drop-down list, select **Edit Settings...** to configure the disk where the Explore appliance data is stored.
6. From the New device drop-down list, select **New Hard Disk**, and then click **Add**.
7. In the New Hard disk field, type the size of your virtual storage disk and then click **OK**.
8. From the Actions drop-down list, select **Power On**.
9. From the Actions drop-down list, select **Open Console**.
10. Log in with the `shell` user account. Type `default` for the password.
11. Run the `show ipaddr` command to display the IP address of the Explore virtual appliance.
12. Exit the console window.

Configure a static IP address through the CLI

The ExtraHop appliance is delivered with DHCP enabled. If your network does not support DHCP, no IP address is acquired, and you must configure a static address manually.

1. Establish a console connection to the ExtraHop appliance.
2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type `default`, and then press ENTER.
4. 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

If you are deploying more than one Explore appliance, join the appliances together to create a cluster. For the best performance, data redundancy, and stability, you must configure at least three Explore appliances in an Explore cluster.

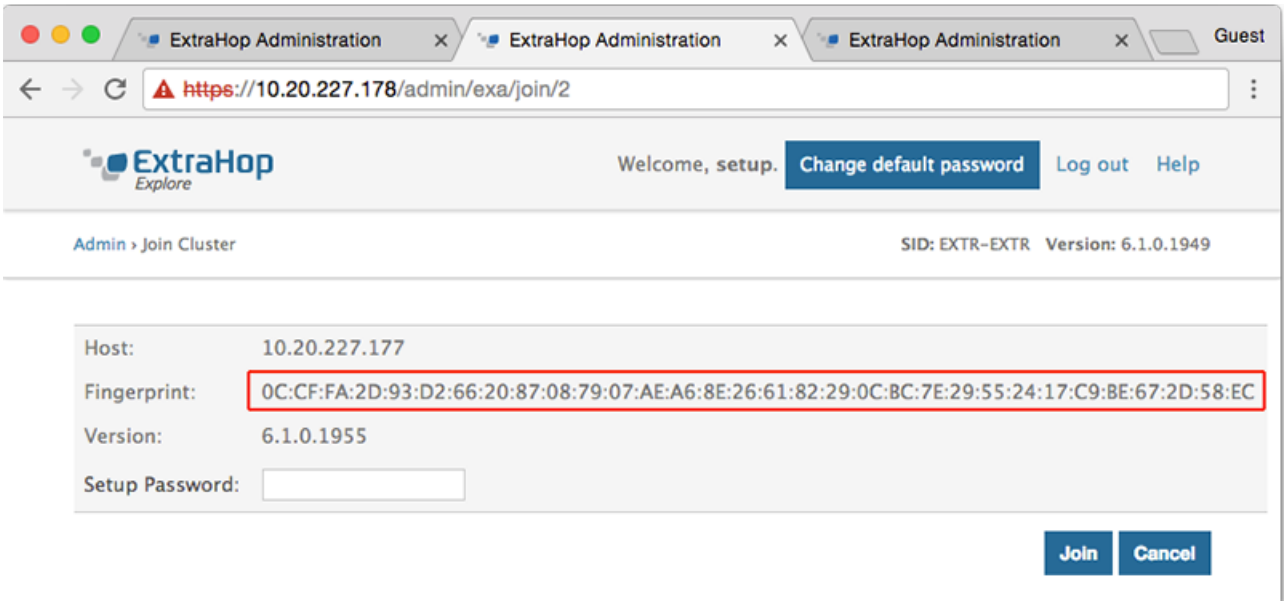
In the following example, the Explore appliances have the following IP addresses:

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

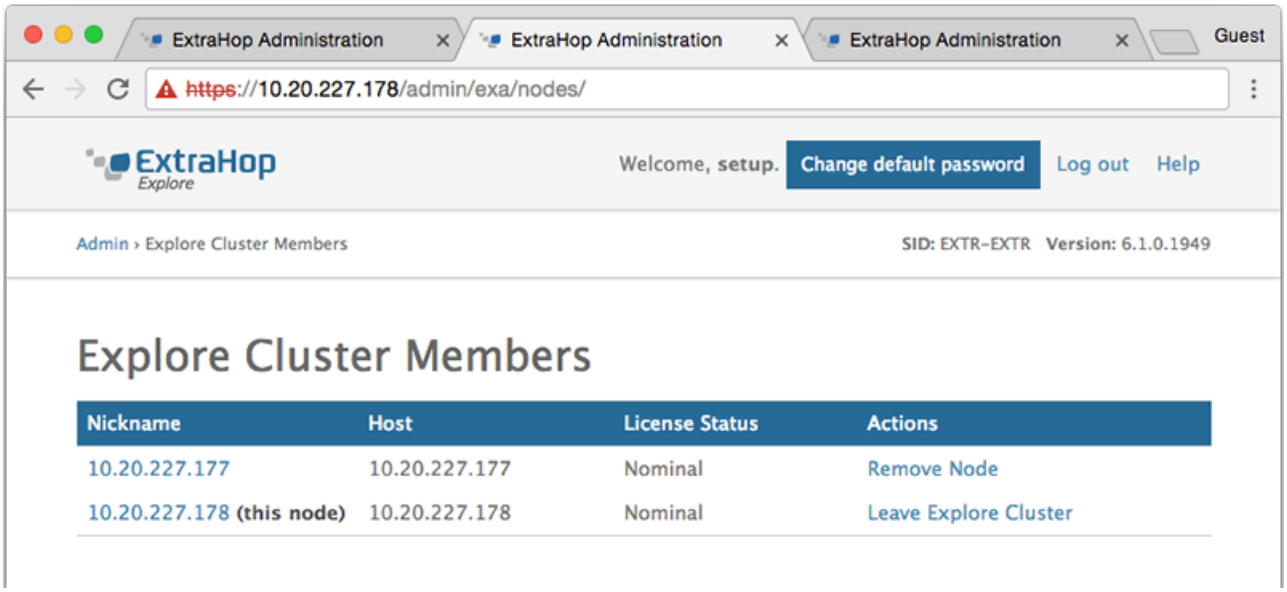
You will join nodes 2 and 3 to node 1 to create the Explore cluster.

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.

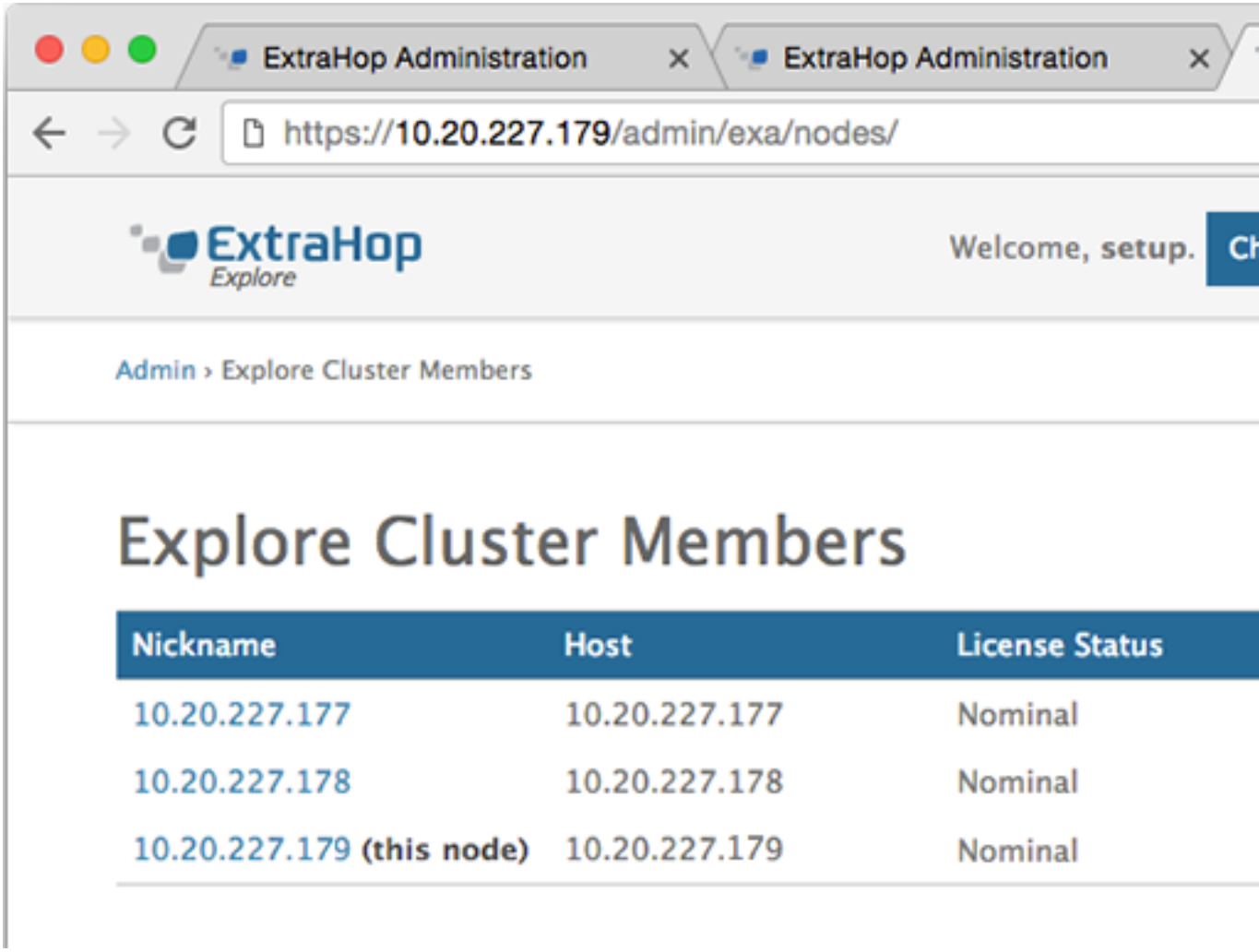


10. In the Status and Diagnostics section, click **Explore Cluster Status**. Wait for the Status field to change to `Green` before adding the next node.

11. Repeat steps 5 - 11 to join each additional node to the new cluster.

    Tip: 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

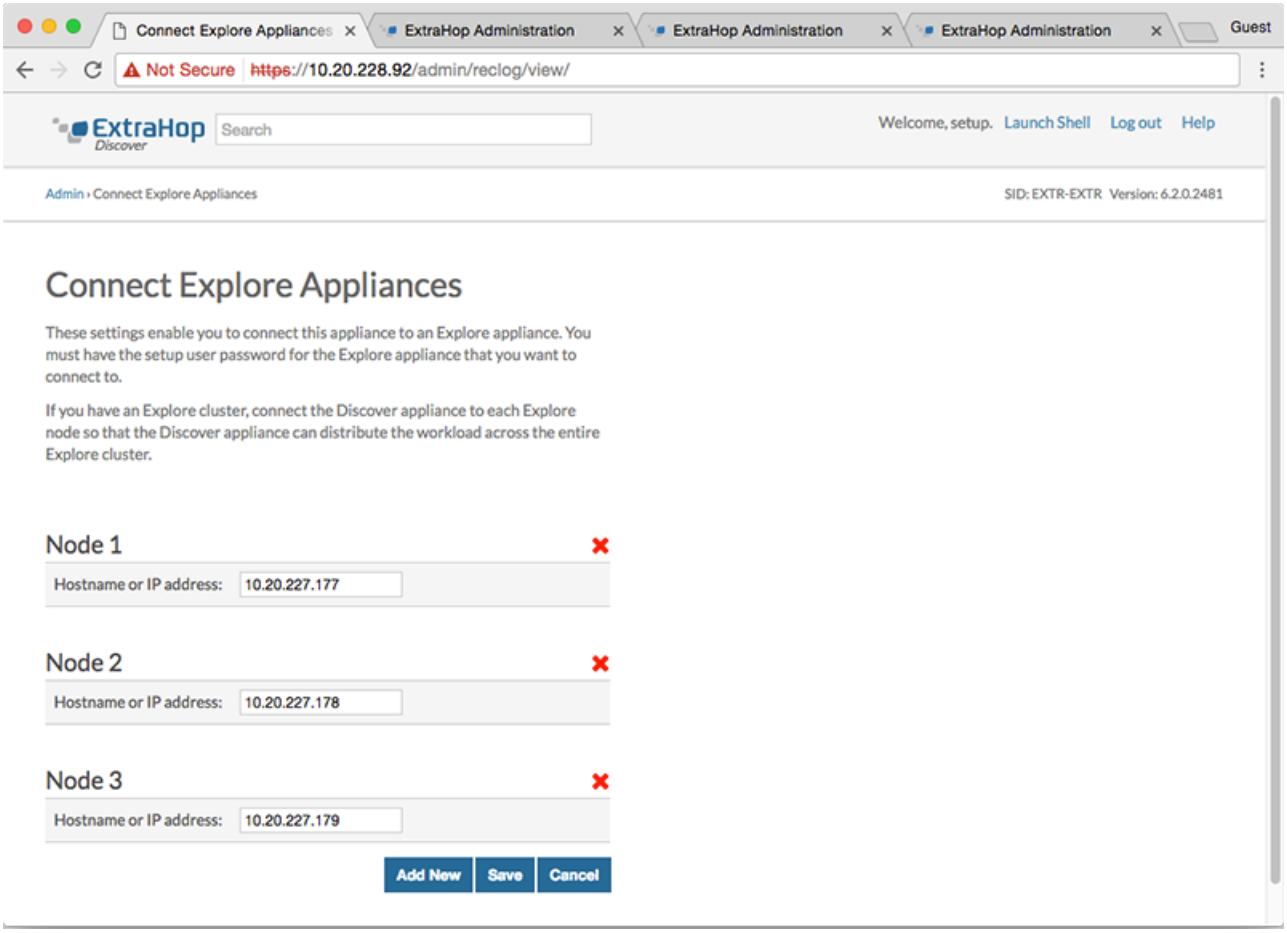
After you deploy the Explore appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore appliance before you can query records.

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

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 Records concepts for more information about Explore configuration settings, how to generate and store records, and how to create record queries.