Deploy the ExtraHop Explore Appliance in AWS

Published: 2019-02-09

In this guide, you will learn how to launch the ExtraHop Explore appliance AMI in your Amazon Web Services (AWS) environment, and join multiple Explore appliances to create an Explore cluster.

System requirements

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

- An AWS account
- Access to the Amazon Machine Image of the ExtraHop Explore appliance
- An Explore appliance product key
- A **m4.2xlarge** instance type in AWS
- A datastore size between 186 GiB (200 GB) and 2328 GiB (2.5 TB)

> (!) **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.

Create the Explore instance in AWS

Before you begin

The Amazon Machine Images (AMIs) of ExtraHop appliances are not publicly shared. Before you can start the deployment procedure, you must send your AWS account ID to support@extrahop.com. Your account ID will be linked to the ExtraHop AMIs. Additionally, you must have administrative access to launch a third-party AMI.

1. Sign in to AWS with your user name and password.
2. Click **EC2**.
3. In the left navigation panel, under Images, click **AMIs**.
4. Above the table of AMIs, change the **Filter** from **Owned by Me** to **Private Images**.
5. In the filter box, type `ExtraHop` and then press ENTER.
6. Select the checkbox next to the ExtraHop Explore appliance AMI and click **Launch**.
7. On the Choose an Instance Type page, select **m4.2xlarge**, and then click **Next: Configure Instance Details**.
8. In the **Number of instances** text box, type the number nodes in your Explore cluster.
9. Click the **Network** drop-down list and select the default setting or one of your organization's VPCs.
10. From the **Shutdown behavior** drop-down list, select **Stop**.
11. Click the **Protect against accidental termination** checkbox.
12. Optional: Click the **IAM role** drop-down list and select an IAM role.
13. Optional: If you launched into a VPC and want to add more than one interface, scroll down to the Network Interfaces section and click **Add Device** to add additional interfaces to the instance.

> 📋 **Note:** If you add more than one interface, make sure that each interface is on a different subnet.

14. Click **Next: Add Storage**.
15. In the Size (GiB) field for the root volume, type the size of the storage volume. The minimum datastore size is 186 GiB (200 GB) and the maximum datastore size is 2328 GiB (2.5 TB). If you specify a

storage volume greater than 2047 GiB, you can safely ignore any warning messages stating that root volumes of this size might result in the instance not booting successfully.

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

16. Click **Next: Tag Instance**.
17. In the Value field, type a name for the instance.
18. Click **Next: Configure Security Group**.
19. On the Configure Security Group page, create a new security group or add ports to an existing group.

    If you already have a security group with the required ports for ExtraHop, you can skip this step.

    a) Select either **Create a new security group** or **Select an existing security group**. If you choose to edit an existing group, select the group you want to edit. If you choose to create a new group, type a name for the Security group and type a Description.

    b) Click the **Type** drop-down list, and select a protocol. Type the port number in the **Port Range** field.

    c) For each additional port needed, click the **Add Rule** button. Then click the **Type** drop-down list, select a protocol, and type the port number in the **Port Range** field.

    The following ports must be open for the Explore appliance AWS instance:

    • 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.

20. Click **Review and Launch**.
21. Select **Make General Purpose (SSD)...(recommended)** and click **Next**.

    > **Note:** If you select **Make General Purpose (SSD)...(recommended)**, you will not see this step on subsequent instance launches.

22. Scroll down to review the AMI details, instance type, and security group information, and then click **Launch**.
23. In the pop-up window, click the first drop-down list and select **Proceed without a key pair**.
24. Click the **I acknowledge…** checkbox and then click **Launch Instance**.
25. Click **View Instances** to return to the AWS Management Console.

    From the AWS Management Console, you can view your instance on the Initializing screen.

    Under the table, on the **Description** tab, you can find an IP or hostname for the Explore appliance that is accessible from your environment.

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.

• Register the Explore 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 an ExtraHop system in AWS

Complete the following steps to apply a product key supplied by ExtraHop Support in an AWS environment.

If you do not have a product key, contact support@extrahop.com.

> **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 IP address of the ExtraHop appliance (`https://<extrahop_management_ip>/admin`).
2. Review the license agreement, select **I Agree**, and click **Submit**.
3. On the log in screen, type `setup` for the user name and the instance ID for the password.

   You can find the Instance ID on the Description tab of an instance selected on the Initializing screen. Type the string of characters that follow i- (but not i- itself), and then click **Log In**.
4. Click **Please apply license in Admin UI**.
5. Click **Register**.
6. Enter the product key, and then click **Register**.
7. Click **Done**.

Configure the system time

1. In the **Appliance Settings** section, click **System Time**.
2. Click **Configure Time**.
3. Click to select from the **Select time zone drop-down** list.
4. Click **Save and Continue**.
5. Select the **Use NTP server to set time** radio button, then click **Select**.

   The `pool.ntp.org` public time server is entered by default.
6. Change the default server address or add a second server address in the two available time server fields, and then click **Save**.
7. Click **Done**.

The NTP Status table displays a list of NTP servers that keep the system clock in sync. To sync a remote server to the current system time, click the **Sync Now** button.

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

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

4. Click **Save**.

Add a recipient email address for notifications

1. In the Network Settings section, click **Notifications**.
2. Under Notifications, click **Email Addresses**.
3. In the Email address text box, type the recipient email address.
4. Click **Save**.

Create an Explore cluster

Published: 2019-02-09

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.
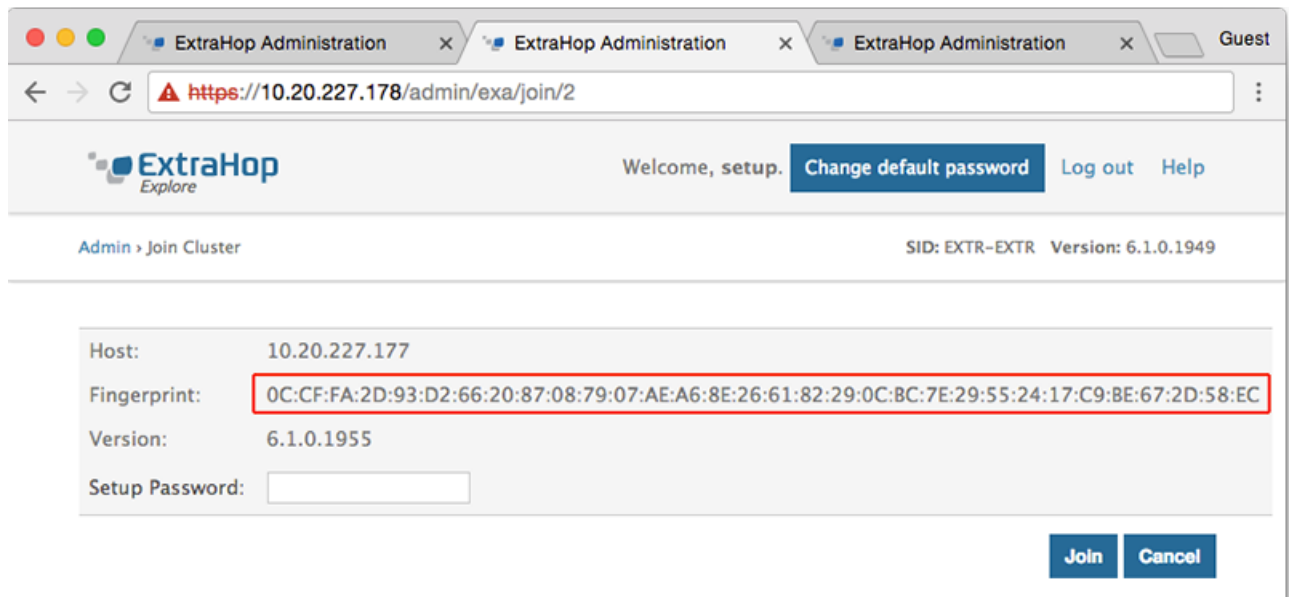
8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**.
9. When the join is complete, notice that the Explore Cluster Settings section has two new entries; **Explore Cluster Members** and **Data Management**.
10. Click Explore Cluster Members. You should see node 1 and node 2 in the list.
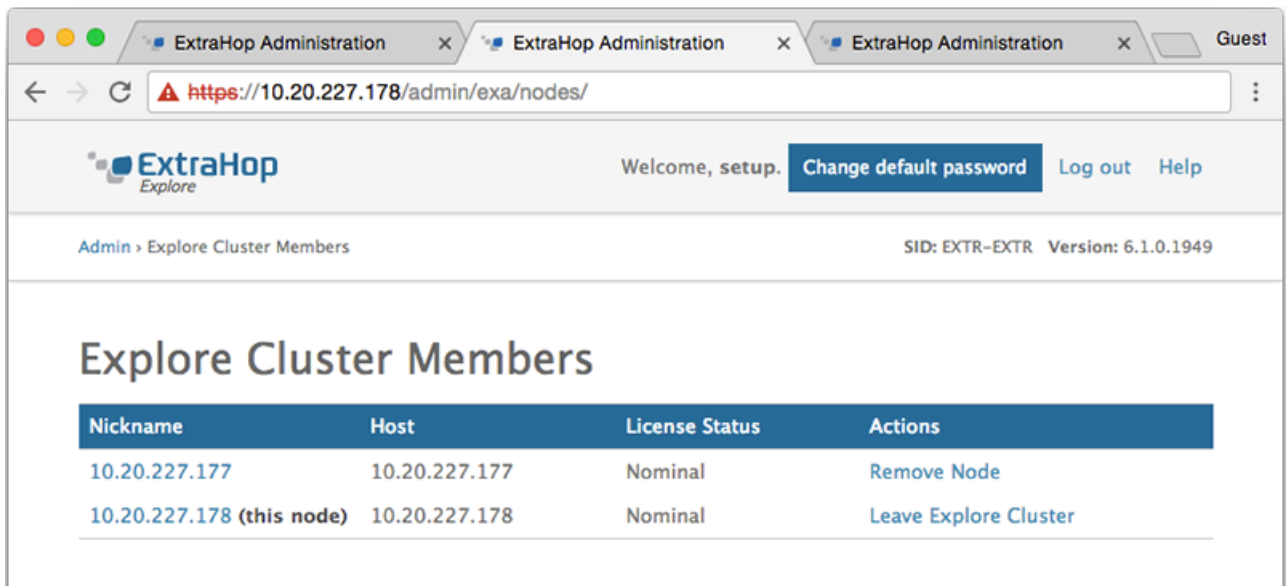
11. In the Status and Diagnostics section, click **Explore Cluster Status**. Wait for the Status field to change to `green` before adding the next node.

12. 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.

13. When you have added all of your Explore appliances to the cluster, click **Cluster Members** in the Explore Cluster Settings section. You should see all of the joined nodes in the list, similar to the following figure.
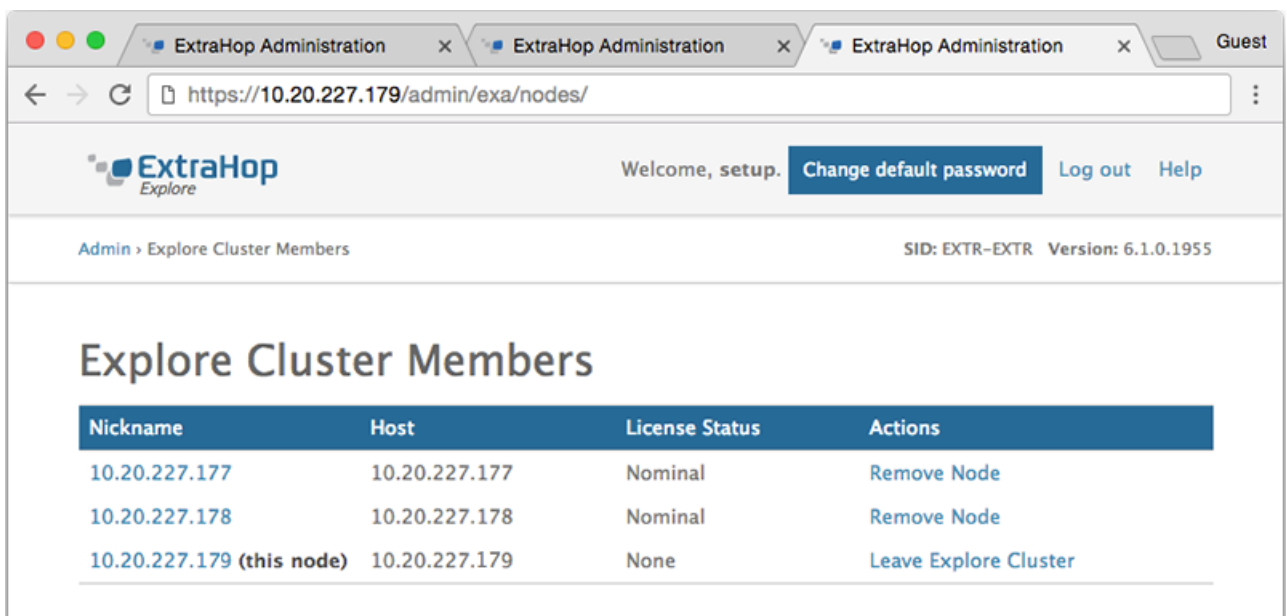
You have now created an Explore cluster.

Connect the Explore appliance to Discover and Command appliances

Published: 2019-02-09

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, 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.

ExtraHop Administ × | **ExtraHop** Administ × | **ExtraHop** Admin

← → C ⚠ **https**://10.20.227.162/admin/reclog/view/

ExtraHop
Discover

Search

Welcome, **setup.** | **Change default pass**

Admin > Connect Explore Appliances

Connect Explore Appliances

Configure an Explore appliance to store and retrieve
records. You must have the setup password for Explore
Node #1 to join with the Explore cluster.

Explore Node #1 ✖

Explore node: | 10.20.227.177 |

Explore Node #2 ✖

Explore node: | 10.20.227.178 |

Explore Node #3 ✖

Explore node: | 10.20.227.179 |

Add New | **Save** | **Cancel**

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**.

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 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 ☒