Deploy the ExtraHop Explore Appliance in Azure

Published: 2018-04-20

In this guide, you will learn how to deploy an ExtraHop Explore virtual appliance in a Microsoft Azure 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:

- An Explore appliance product key
- An Azure storage account
- A Linux client with the latest updates installed
- The ExtraHop Explore 5100v virtual hard disk (VHD) file, available on the ExtraHop Customer Portal
- An Azure instance size that most closely matches the Explore appliance VM size, as listed below:

Appliance	Azure Instance Size
EXA 5100v	Basic A4, Standard A7, or Standard DS13

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.

Deploy the EXA 5100v

The following procedure is completed through the Azure classic deployment method. Additional configuration steps might be required for Azure Resource Manager deployments.

Before you begin
If you have not already done so, download the ExtraHop Explore appliance VHD file for Azure from the ExtraHop Customer Portal.

1. On your Linux client, open a terminal application and run the following commands.
   a) Install npm and node.js-legacy:

   ```
   sudo apt-get install npm nodejs-legacy
   ```

   b) Install the Azure command-line interface tools:

   ```
   sudo npm install -g azure-cli@0.9.7
   ```

   Note: Version 0.9.7 is not the most recent version of the Azure command-line tools. However, in order to upload VHD files to Azure, you must install the older version of the tool.

   c) Download your publish settings file from Azure:

   ```
   azure account download
   ```

   Your default browser automatically opens to `http://go.microsoft.com/fwlink/?LinkId=254432`
2. Sign into your Azure account.

3. Save the `.publishsettings` file to your computer.
4. Return to your terminal application and run the following commands:
   a) Import your publish settings file:

```
azure account import <path_to_publishsettings_file>
```

   b) Create a boot image in the Azure blob storage location. The *<azure-EXA5100v.vhd>* file is uploaded to blob storage, and then the new virtual instance is created from this boot image.

```
azure vm image create <boot_image_name> <path_to_extrahop.vhd> -o
 linux -u <storage_account_url>
```

   Where *<boot_image_name>* is the name of your boot image, *<path_to_extrahop_extrahop.vhd>* is the name of the ExtraHop VHD file on your local machine, and *<storage_account_url>* is the location of your storage account in Azure.

   For example:

```
azure vm image create example-image /temp/azure-EXA5100v-5.1.0.983.vhd
 -o linux -u https://exstorage1.blob.core.windows.net/vm-images/
example-vm.vhd
```

   Note: The VHD name in the URL (*example-vm.vhd*, in the example above) must be unique. If you try to overwrite an existing VHD file with the same name, this step will fail and you will need to repeat this step with a new VHD name.

   c) Create and start an Azure VM instance:

```
azure vm create <vm_name> <boot_image_name> --ssh -z <instance_size> -
l '<zone_name>' --userName user --password 'Ignored@Password1'
```

   Where *<vm_name>* is the name of your Explore VM, *<boot_image_name>* is the name of the boot image you created in step 4b, *<instance_size>* is the Azure instance size, and *<zone_name>* is your local time zone.

   Note: Choose an Azure instance size that most closely matches the Explore VM (Basic_A4, Standard_A7, or Standard_DS13).

   For example:

```
azure vm create example-vm example-image --ssh -z Basic_A4 -l 'West
 US' --userName user --password 'Ignored@Password1'
```

   Note: Azure requires that you specify a username and password to create and start the VM instance; however, the username and password are not required for the Discover virtual appliance.

   d) Create HTTP, HTTPS, and EXA endpoints. The HTTP and HTTPS Endpoints are required to direct the inbound network traffic to the Discover virtual appliance. The EXA endpoint enables Explore nodes to communicate with other Explore nodes in the same cluster.

```
azure vm endpoint create -n HTTP <vm_name> 80 80
```

```
azure vm endpoint create -n HTTPS <vm_name> 443 443
```

```
azure vm endpoint create -n EXA <vm_name> 9443 9443
```

Configure the Explore appliance

After the Explore appliance is deployed in Azure, log into the Explore Admin UI through the following URL: `https://<vm_name>.cloudapp.net/`.

Note: The default login username is `setup` and the password is `default`.

After you log into the Explore appliance, 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 the Explore appliance

Complete the following steps to apply a product key.

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

1. In your browser, type the IP address of the Explore appliance (`https://<vm_name>.cloudapp.net/`).
2. Review the license agreement, select **I Agree**, and then click **Submit**.
3. On the login screen, type `setup` for the username and `default` for the password, and then click **Log In**.
4. In the Appliance Settings section, click **License**.
5. Click **Manage License**.
6. Click **Register**.
7. Enter the product key, and then click **Register**.

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: 2018-04-20

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.

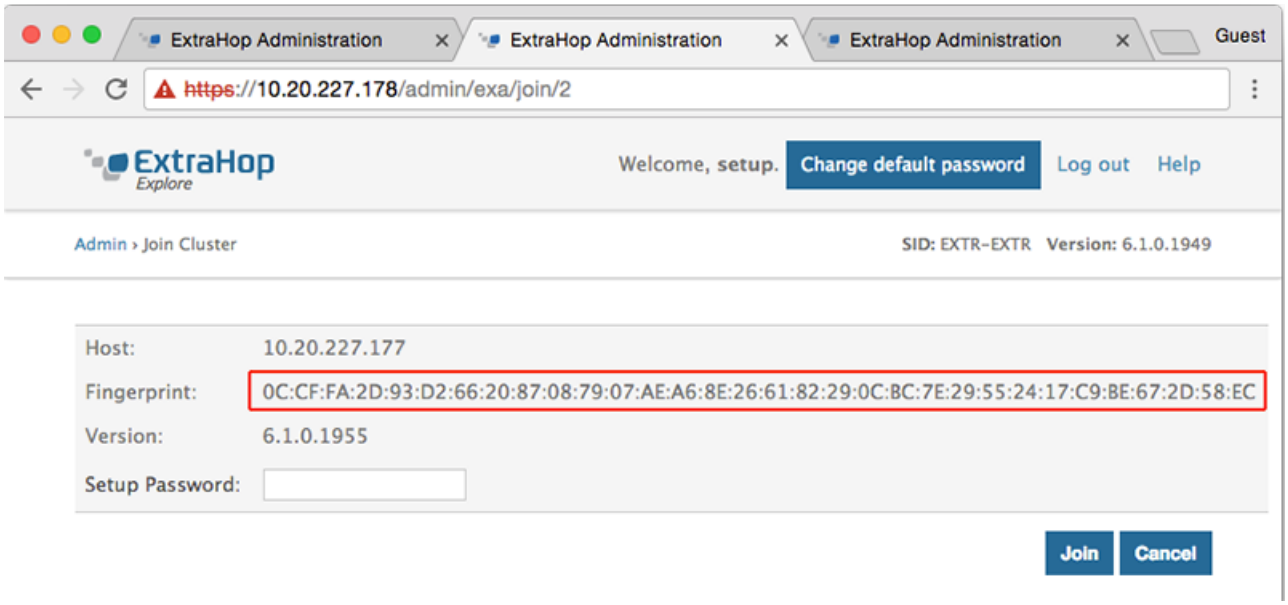
In the following example, the Explore appliances have the following IP addresses:

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

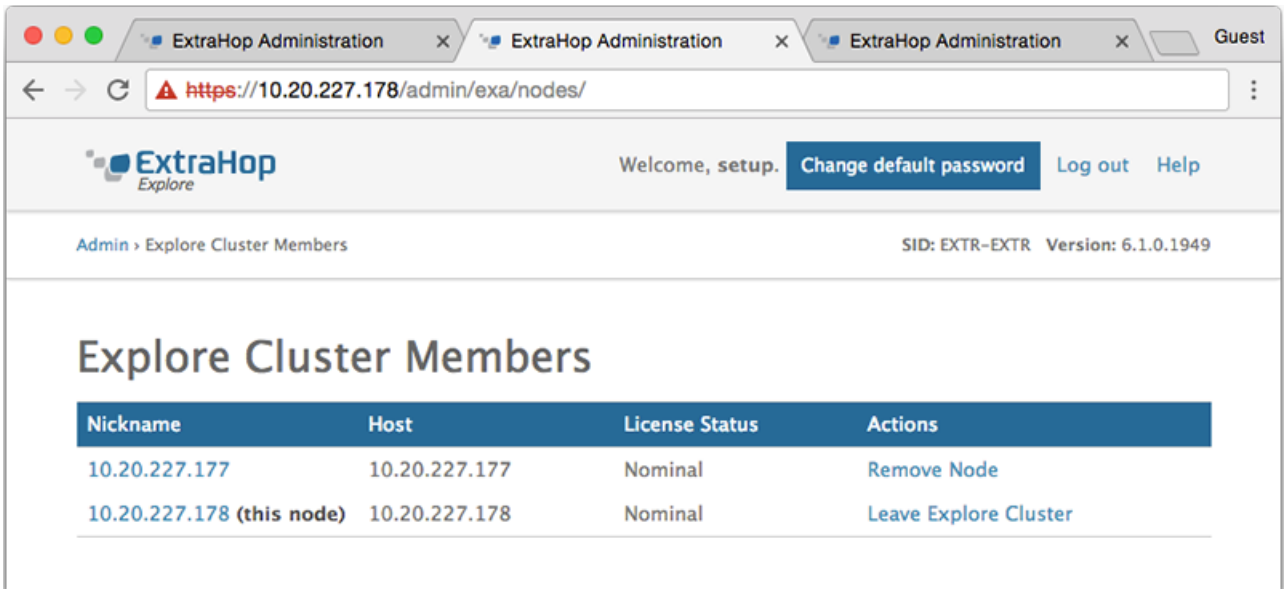
You will join nodes 2 and 3 to node 1 to create the Explore cluster.

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.

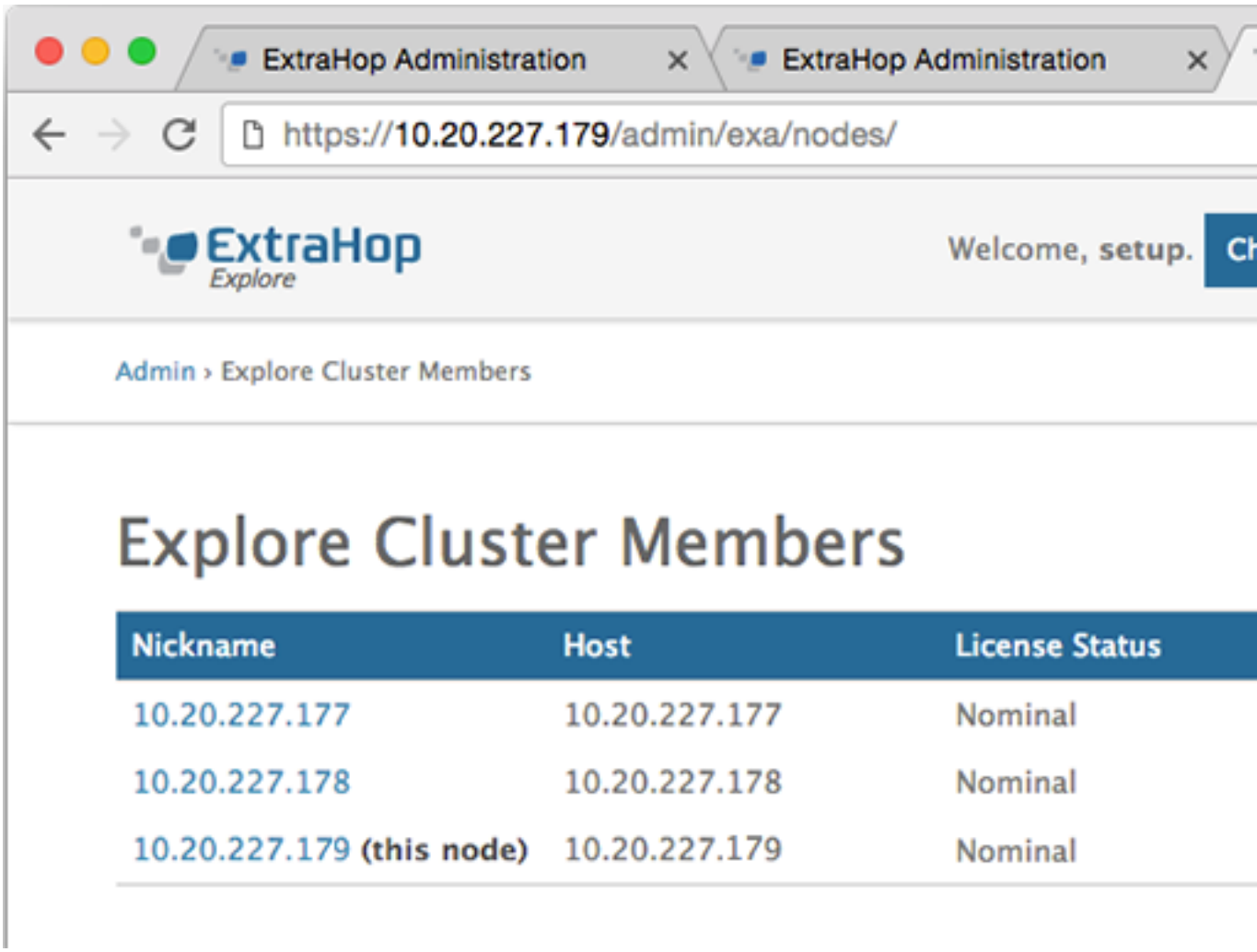


8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**.
   When the join is complete, the Explore Cluster Settings section has two new entries: **Explore Cluster Members** and **Data Management**.
9. Click Explore Cluster Members. You should see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

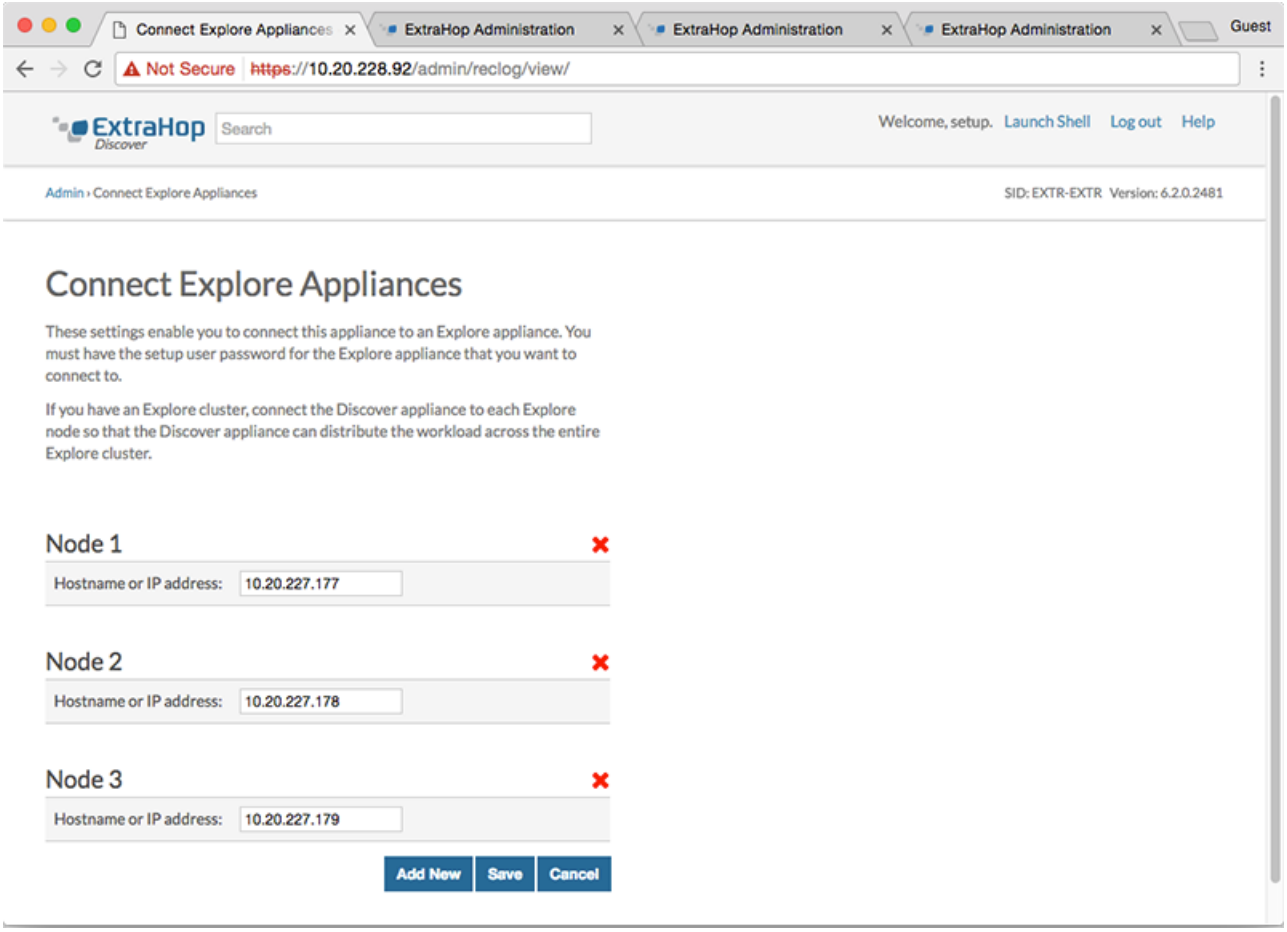
Published: 2018-04-20

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: 2018-04-20

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