Deploy the ExtraHop Explore Appliance in Azure

Published: 2019-02-10

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, Mac, or Windows client with the latest version of Azure CLI 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

Deploy the EXA 5100v

Before you begin
The procedures below assume that you do not have the required resource group, storage account, storage container, and network security group configured. If you already have these parameters configured, you can proceed to step 5 after you log into your Azure account.

1. Open a terminal application on your client and log into to your Azure account.

```
az login
```

2. Open `https://aka.ms/devicelogin` in a web browser and enter the code to authenticate, and then return to the command-line-interface.
3. Create a resource group.

```
az group create --name <name> --location <location>
```

For example, create a new resource group in the West US region.

```
az group create --name exampleRG --location westus
```

4. Create a storage account.

```
az storage account create --resource-group <resource group name> --name
 <storage account name>
```

For example:

```
az storage account create --resource-group exampleRG --name exampleSA
```

5. View the storage account key. The value for `key1` is required for step 5.

```
az storage account keys list --resource-group <resource group name> --
account-name <storage account name>
```

For example:

```
az storage account keys list --resource-group exampleRG --account-name
 exampleSA
```

Output similar to the following appears:

```
[
 {
   "keyName": "key1",
   "permissions": "Full",
   "value":
 "CORuU8mTcxLxq0bbszhZ4RKTB93CqLpjZdAhCrNJugAorAyvJjhGmBSedjYPmnzXPikSRigd
5T5/YGYBoIzxNg=="
 },
 { "keyName": "key2",
   "permissions": "Full",
   "value": "DOlda4+6U3Cf5TUAng8/GKotfX1HHJuc3yljAlU+aktRAf4/
KwVQUuAUnhdrw2yg5Pba5FpZn6oZYvROncnT8Q=="
 }
]
```

6. Set default Azure storage account environment variables. You can have multiple storage accounts in your Azure subscription. To select one of them to apply to all subsequent storage commands, set these environment variables. If you do not set environment variables you will always have to specify `--account-name` and `--account-key` in the commands in the rest of this procedure.

```
export AZURE_STORAGE_ACCOUNT=<storage account_name>
```

```
export AZURE_STORAGE_ACCESS_KEY=<key1>
```

Where <*key1*> is the storage account key value that appears in step 5.

For example:

```
export AZURE_STORAGE_ACCOUNT=exampleSA
```

```
export
 AZURE_STORAGE_ACCESS_KEY=CORuU8mTcxLxq0bbszhZ4RKTB93CqLpjZdAhCrNJugAor
AyvJjhGmBSedjYPmnzXPikSRigd5T5/YGYBoIzxNg==
```

7. Create a storage container.

```
az storage container create --name <storage container name>
```

For example:

```
az storage container create --name exampleSC
```

8. Upload the Discover appliance VHD file to the blob storage.

```
 az storage blob upload --container-name <container> --type page --name
 <blob name> --file <path/to/file> --validate-content
```

For example:

```
az storage blob upload --container-name exampleSC --type page
--name discover_appliance.vhd --file /Users/admin/Downloads/extrahop-
exa-5100v-azure-7.2.0.5000.vhd --validate-content
```

9. Retrieve the blob URI. You need the URI when you create the managed disk in the next step.

```
az storage blob url --container-name <storage container name> --name
 <blob name>
```

For example:

```
az storage blob url --container-name exampleSC --name
 explore_appliance.vhd
```

Output similar to the following appears:

```
https://exampleSA.blob.core.windows.net/exampleSC/explore_appliance.vhd
```

10. Create a managed disk, sourcing the Discover VHD file.

```
az disk create --resource-group <resource group name> --location <Azure
 region>
--name <disk name> --sku Premium_LRS --source <blob uri> --size-gb <size
 gb>
```

Where `sku` specifies the type of disk and desired replication pattern. Managed disks support only Standard_LRS and Premium_LRS. Premium_LRS has a maximum disk size of 1 TB and Standard_LRS has a maximum disk size of 4TB.

For example:

```
az disk create --resource-group exampleRG --location westus
--name exampleDisk --sku Standard_LRS --source https://
exampleSA.blob.core.windows.net/exampleSC/explore_appliance.vhd
--size-gb 60
```

11. Create the VM and attach the managed disk. This command creates the Explore appliance VM with a default network security group and dynamic public IP address.

```
az vm create --resource-group <resource group name> --location <Azure
 region>
--name <vm name> --os-type linux --attach-os-disk <disk name> --size
 <azure machine size>
```

For example:

```
az vm create --resource-group exampleRG --location westus --name
 exampleVM --os-type linux
--attach-os-disk exampleDisk --size Basic_A4
```

12. Log into the Azure portal, https://portal.azure.com, and configure the networking rules for the appliance. The network security group must have the following rules configured:

Table 1: Inbound Port Rules

Name	Port	Protocol
EXA	9443	TCP

Name	Port	Protocol
HTTPS	443	TCP
SSH	22	TCP

Table 2: Outbound Port Rules

Name	Port	Protocol
EXA	9443	ANY
HTTPS	443	TCP
SSH	22	TCP

Next steps
Open a web browser and log into the Admin UI on the Explore appliance through the configured public IP address. The default login name is `setup` and the password is `default`.

Complete the following recommended procedures:

- Register your ExtraHop appliance
- Configure the system time
- Configure email settings for notifications

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:

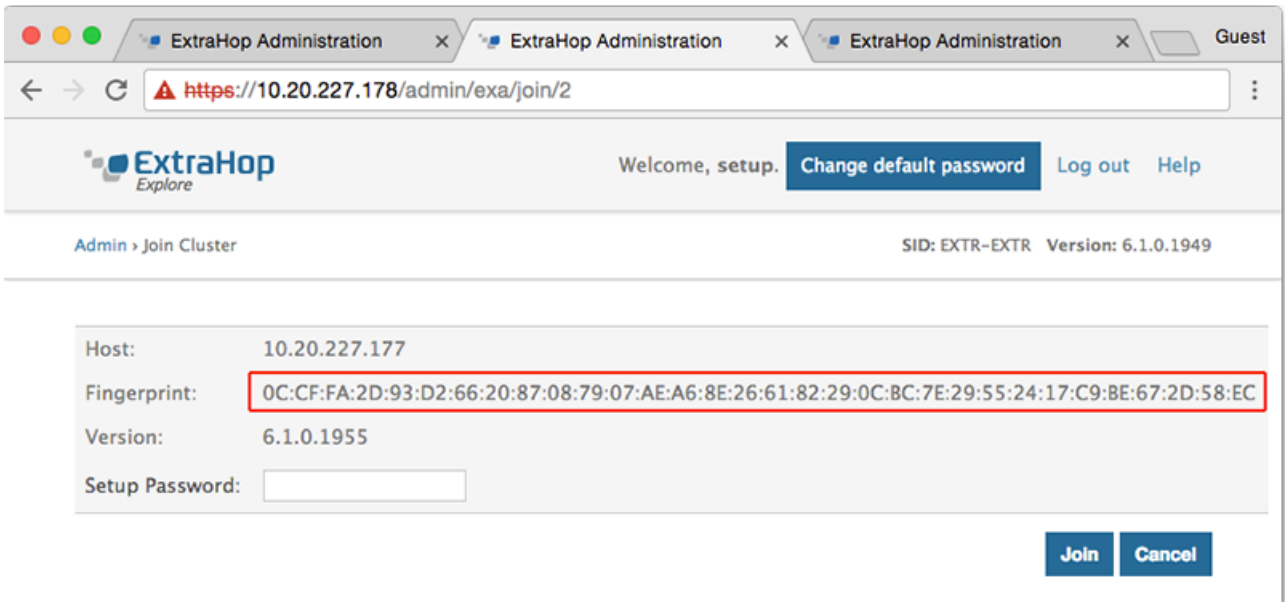
- Node 1: 10.20.227.177
- Node 2: 10.20.227.178
- Node 3: 10.20.227.179

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

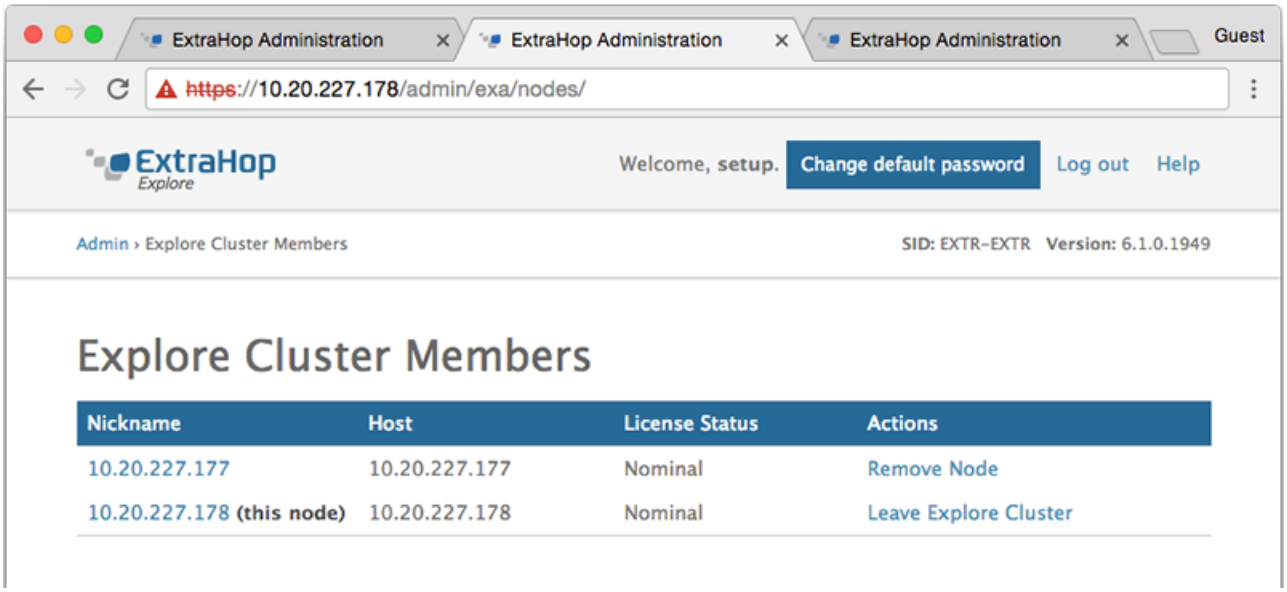
Important: Each node that you join must have the same configuration (physical or virtual) and ExtraHop firmware version.

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**.

   Note: For cloud-based deployments, be sure to type the IP address listed in the Interfaces table on the Connectivity page.
7. Confirm that the fingerprint on this page matches the fingerprint you noted in step 3.



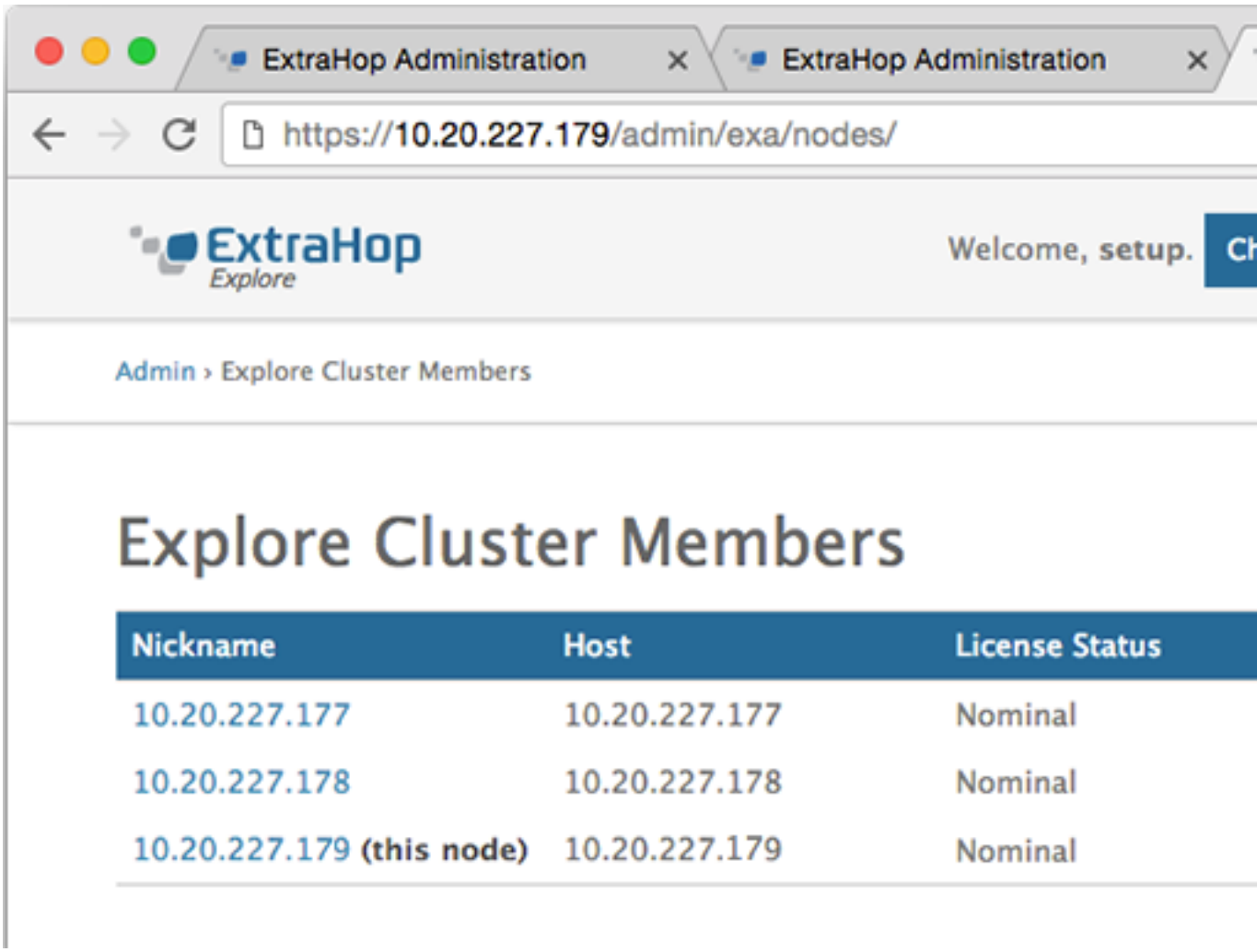
8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**.
   When the join is complete, the Explore Cluster Settings section has two new entries: **Explore Cluster Members** and **Data Management**.
9. Click Explore Cluster Members. You should see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

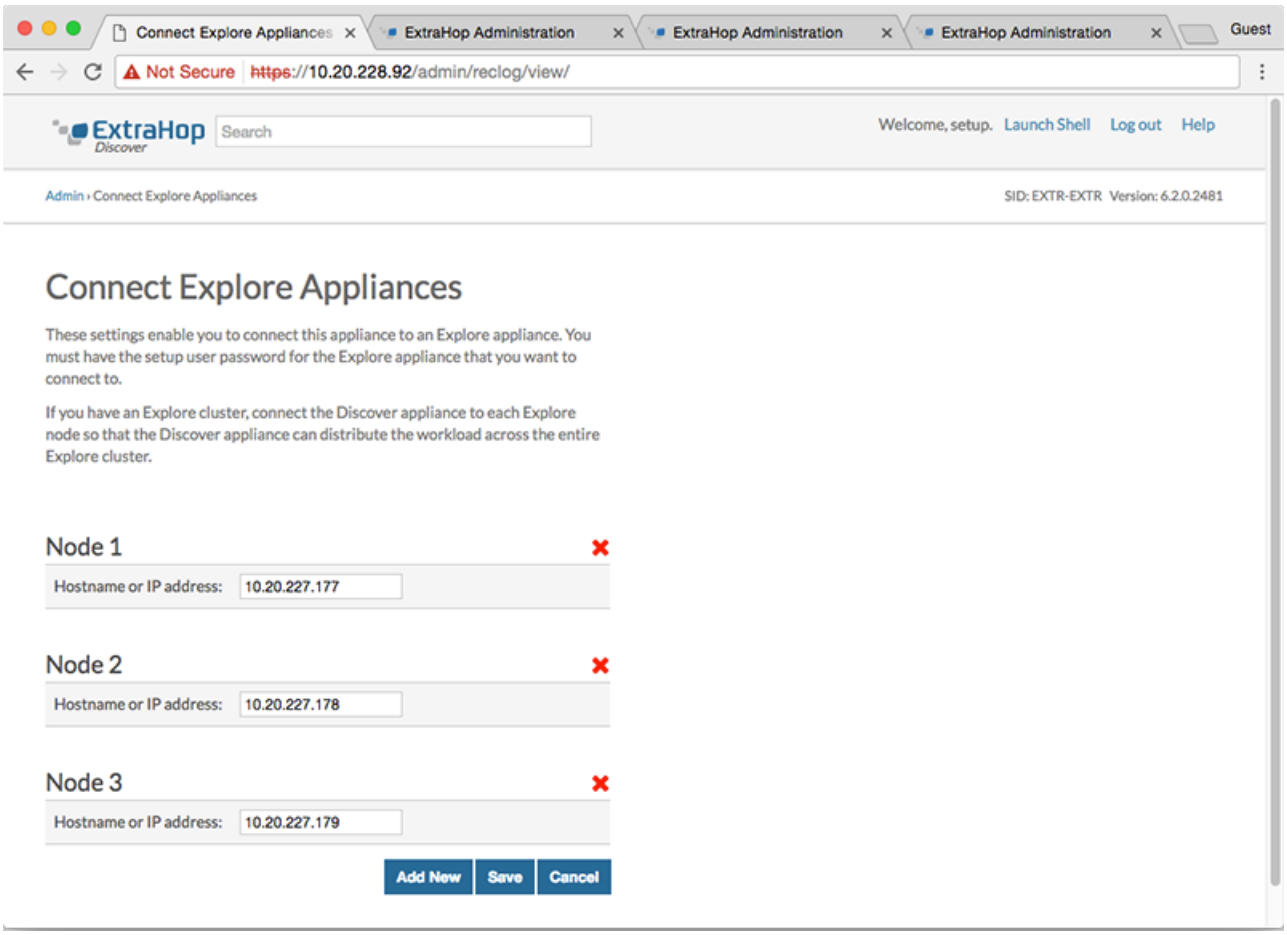
Connect the Explore appliance to Discover and Command appliances

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.

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:

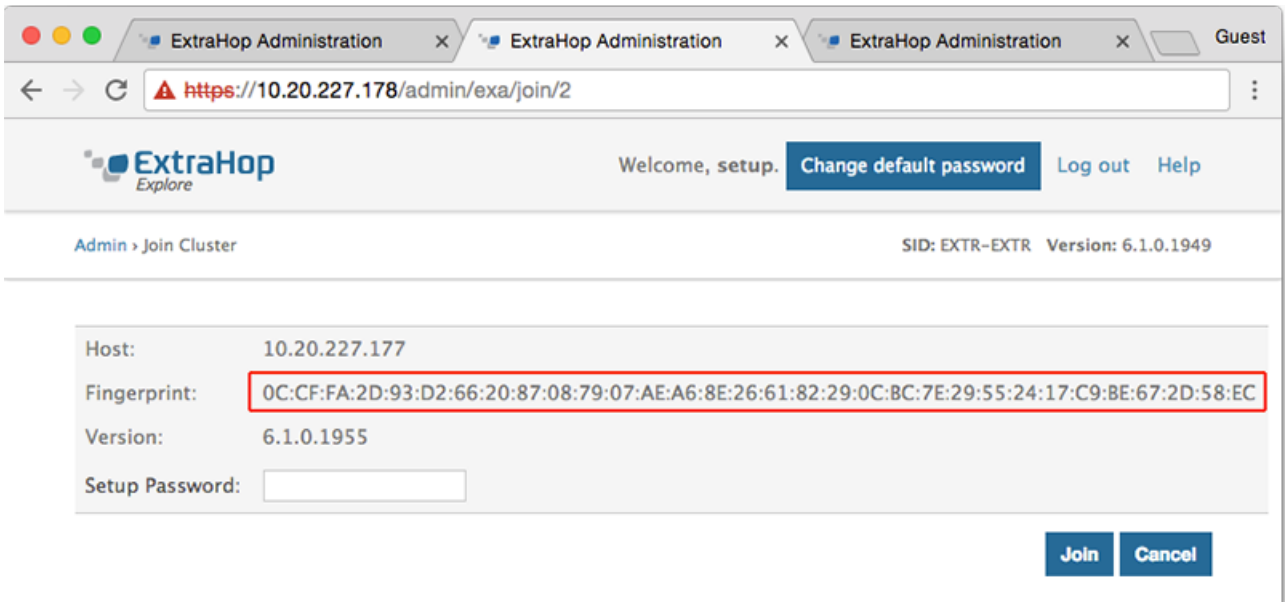
- Node 1: 10.20.227.177
- Node 2: 10.20.227.178
- Node 3: 10.20.227.179

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

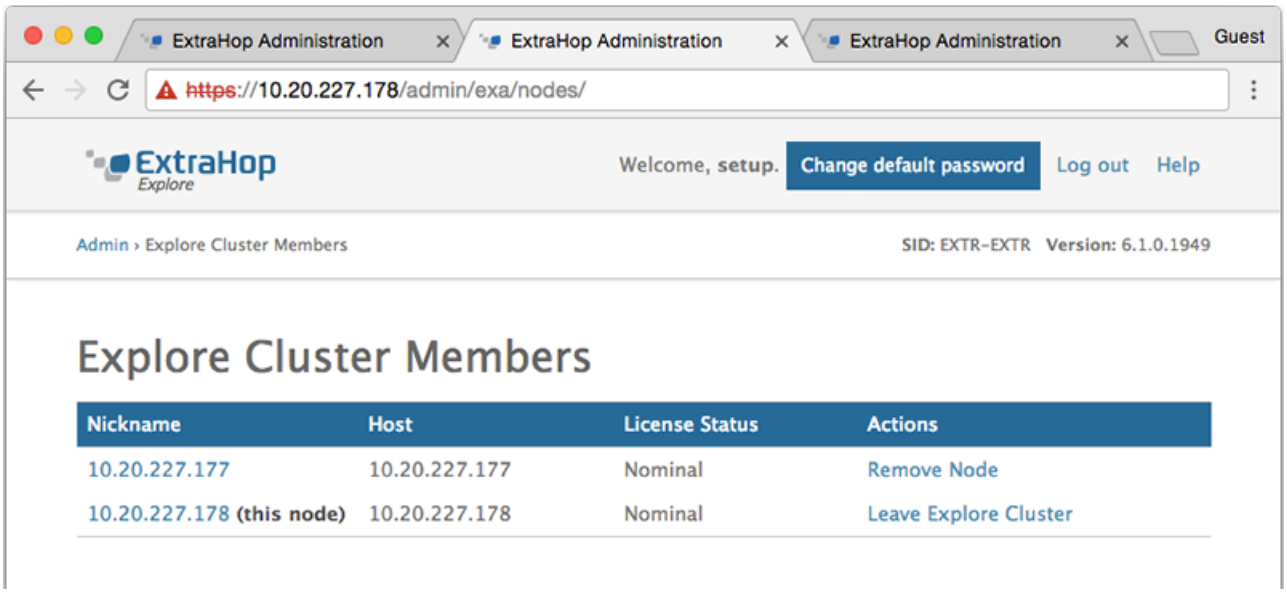
Important: Each node that you join must have the same configuration (physical or virtual) and ExtraHop firmware version.

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**.

   Note: For cloud-based deployments, be sure to type the IP address listed in the Interfaces table on the Connectivity page.
7. Confirm that the fingerprint on this page matches the fingerprint you noted in step 3.

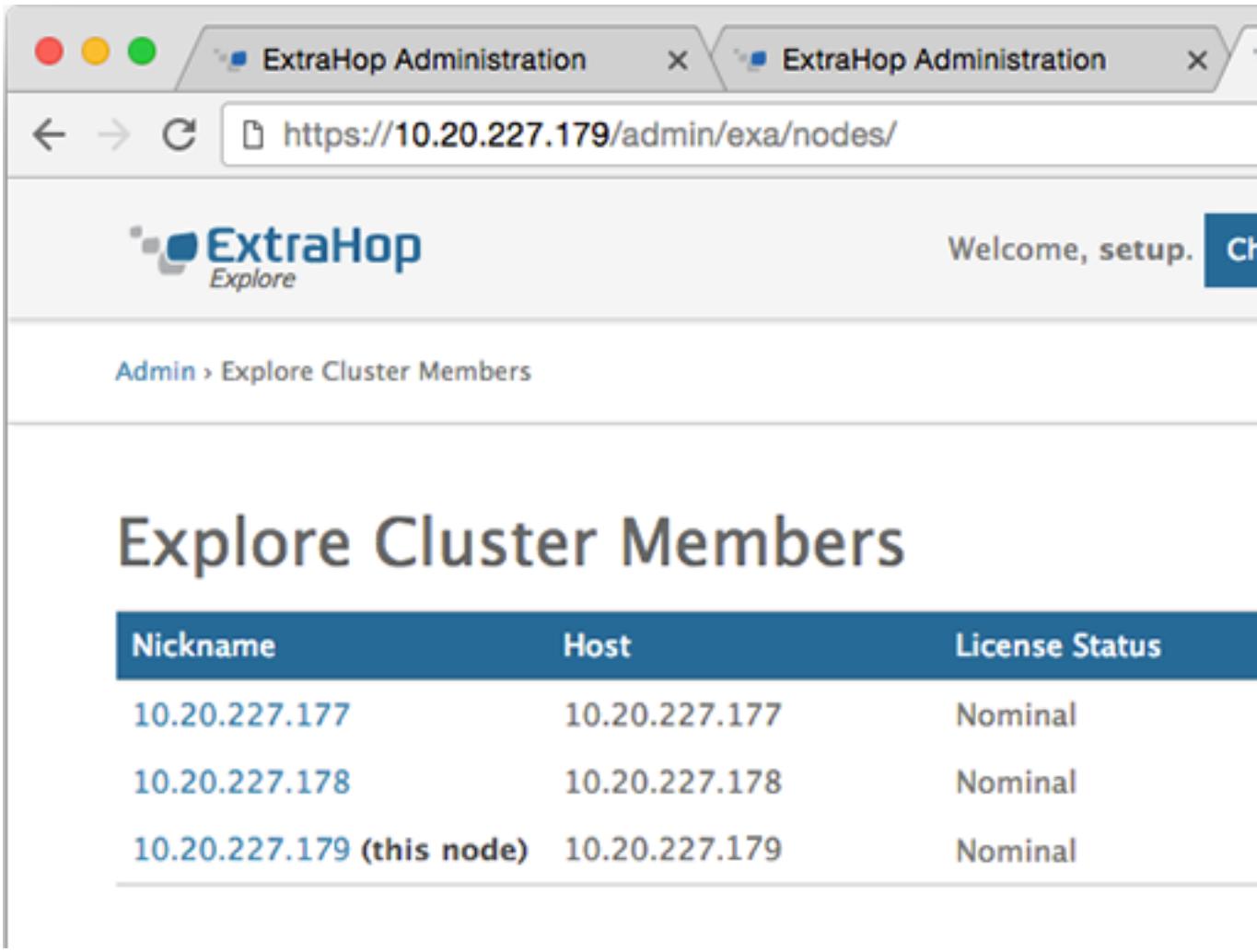


8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**.
   When the join is complete, the Explore Cluster Settings section has two new entries: **Explore Cluster Members** and **Data Management**.
9. Click Explore Cluster Members. You should see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

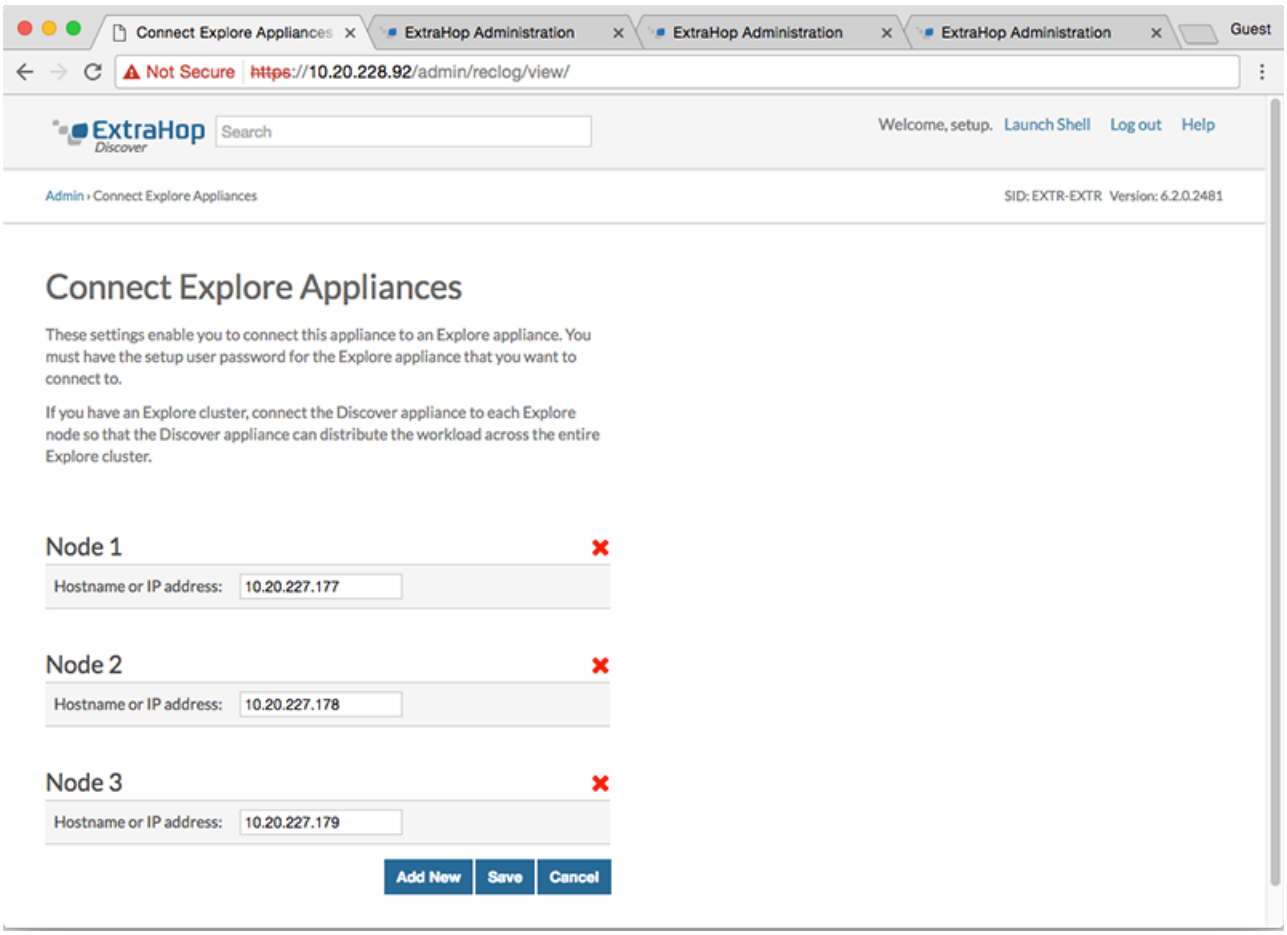
Connect the Explore appliance to Discover and Command appliances

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.