Deploy the ExtraHop Explore Appliance in Azure

Published: 2018-01-10

The following procedures explain how to deploy an ExtraHop Explore virtual appliance in a Microsoft Azure environment. You must have experience administering in an Azure environment to complete these procedures.

System requirements

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

- An Azure storage account
- A Linux client with the latest updates installed
- The ExtraHop Explore 5100v virtual hard disk (VHD) file
- An Explore appliance product key

Important: If you want to deploy more than one ExtraHop virtual appliance, do not clone an existing instance. Always start with the original deployment package when deploying additional instances.

Deploy the EXA 5100v

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 and HTTPS endpoints. Endpoints are required to direct the inbound network traffic to the Discover VM.

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

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

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 log in name 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 the product key supplied by ExtraHop Customer Support. If you do not have a product key, contact support@extrahop.com.

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 System Settings section, click **License**.
5. Click **Manage License**.
6. Click **Register**.
7. Enter the product key, and then click **Register**.

Create an Explore cluster

Before you begin
Log into the Admin UI of each Explore node, click **Fingerprint** in the Status section, and note the value listed in the Fingerprint field. The fingerprint of each node should be verified during the join process.

If you are deploying three or more Explore nodes, join the nodes to create a 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 any new Explore node.
2. In the Cluster Settings section, click **Join Cluster**.
3. In the Host text box, type the hostname or IP address of any of the other new nodes and then click **Continue**.
4. Verify that the fingerprint displayed on the page matches the fingerprint of the Explore node that you are joining. If these fingerprints do not match, communication between the nodes might have been intercepted and altered.
5. In the Setup Password field, type the password for the `setup` user.
6. Click **Join**.
7. In the Status section, click **Cluster Status**.
8. Wait for the Status field to change to `green`.
9. Repeat steps 1 - 8 to join each additional node to the new cluster.

   Note: Always join a new node to the existing cluster and not another unjoined node, or you will create multiple clusters.
10. Click **Cluster Members** in the Cluster Settings section to confirm that all of the nodes are listed on the page.

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 System 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 Use NTP server to set time radio button and then click **Select**.
5. Type the IP addresses for the time server, and then click **Save**.
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.

Pair the Explore appliance to Discover and Command appliances

After you deploy the Explore cluster, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore cluster before you can query records. 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 Discover or Command appliance Admin UI.
2. In the ExtraHop Explore Settings section, click **Configure Explore Cluster**.
3. Click **Add New**.
4. In the Host #1 Host 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 Host field.
6. Click **Save**.
7. Note the information listed for Fingerprint. Verify that the fingerprint listed on this page matches the fingerprint of the Explore appliance (**Host #1**) listed on the Fingerprint page in the Explore Admin UI.
8. In the Explore Setup Password field, type the password of the Explore appliance.
9. Click **Join**, and then click **Done**.

Send record data to the Explore appliance

After your Explore appliance is paired with 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