Deploy the ExtraHop Discover Appliance in Azure

Published: 2019-02-08

The following procedures explain how to deploy an ExtraHop Discover 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 Discover appliance in Azure:

- An Azure storage account
- A Linux client with the latest updates installed
- The ExtraHop Discover 1000v or 2000v virtual hard disk (VHD) file, available on the ExtraHop Customer Portal
- A Discover appliance product key
- An Azure instance size that most closely matches the Discover appliance VM size, as follows:

Appliance	Azure Instance Size
EDA 1000v	Basic A3 or Standard DS2
EDA 2000v	Basic A4 or Standard DS4

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 EDA 1000v or 2000v

Before you begin
If you have not already done so, download the ExtraHop Discover 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-EDA2000v.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-EDA2000v-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 Azure subscription region.

   Note: Choose an Azure instance size that most closely matches the Discover VM size. For the EDA 1000v, select Basic_A3 or Standard_DS2. For the EDA 2000v, select Basic_A4 or Standard_DS4.

   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 by the Discover virtual appliance.

   d) Create HTTP and HTTPS endpoints. Endpoints are required to direct the inbound network traffic to the virtual Discover appliance.

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

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

e) Create rpcapd endpoints:

```
azure vm endpoint create -n rpcapd-tcp -o tcp <vm_name> 2003 2003
```

```
azure vm endpoint create -n rpcapd-udp -o udp <vm_name> 2003 2003
```

Note: By default, Access Control Lists (ACLs) do not restrict access to these endpoints.

Configure the Discover appliance

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

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

After you log into the Discover appliance, complete the following recommended procedures:

- Register the ExtraHop appliance
- Configure the system time
- Configure email notifications
- Pair the Discover appliance to any Command or Explore appliances

Register the ExtraHop appliance

Complete the following steps to apply a product key supplied by ExtraHop Support.

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 appliance (`https://<vm_name>.cloudapp.net/admin`).
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.
4. Click **Log In**.
5. In the Appliance Settings section, click **License**.
6. Click **Manage License**.
7. Click **Register**.
8. Enter the product key and then click **Register**.
9. Click **Done**.

Configure the system time

The default time server setting is `pool.ntp.org`. If you want to maintain the default setting, skip this procedure and go to the next section.

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.
4. Click **Save and Continue**.
5. On the Time Setup page, select one of the following options:
   - Set time manually

     Note: You cannot manually set the time if the Discover appliance is managed by a Command appliance.
   - Set time with NTP server
6. Select the **Set time with NTP server** radio button, then click **Select**.

   The `pool.ntp.org` public time server appears in the Time Server #1 field by default.
7. Type the IP address or fully qualified domain name (FQDN) for the time servers in the Time Server fields. You can add a maximum of nine time servers.

   Tip: After adding the fifth time server, click **Add Server** to display up to four additional time server fields.
8. Click **Save**, and then click **Done**.

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

Configure email settings

You must configure an email server and sender before the ExtraHop appliance can send notifications about system alerts by email.

1. In the Network Settings section, click **Notifications**.
2. Click **Email Server and Sender**.
3. Type the IP address or hostname for the outgoing SMTP mail server in the SMTP Server field.

   Note: The SMTP server should be the fully qualified domain name (FQDN) or IP address of an outgoing mail server that is accessible from the ExtraHop management network. If the DNS server is set, then the SMTP server can be a FQDN, otherwise it needs to be an IP address.
4. Type the port number for SMTP communication in the SMTP Port field. The default port number is 25.
5. Select one of the following encryption methods from the Encryption drop-down list:
   - **None**. SMTP communication is not encrypted.
   - **SSL/TLS**. SMTP communication is encrypted through the Secure Socket Layer/Transport Layer Security protocol.
   - **STARTTLS**. SMTP communication is encrypted through STARTTLS.
6. Type the email address for the notification sender in the Sender Address field.

   Note: The displayed sender address might be changed by the SMTP server. When sending through a Google SMTP server, for example, the sender email is changed to the username supplied for authentication, instead of the originally entered sender address.
7. Select Validate SSL Certificates to enable certificate validation. If you select this option, the certificate on the remote endpoint is validated against the root certificate chains specified by the trusted certificates manager. In addition, the host name specified in the certificate presented by the SMTP server must match the host name specified in your SMTP configuration or validation will fail. You must configure which certificates you want to trust on the Trusted Certificates page. For more information, see Add a trusted certificate to your ExtraHop appliance.
8. Type the email address for the report sender in the **Report Sender Address** field.

9. Select the Enable SMTP authentication checkbox and then type the SMTP server setup credentials in the Username and Password fields.
10. Click **Save**.

Add an email notification group

Email notification groups are assigned to alerts to designate who should receive an email when that alert becomes active. Although you can specify individual email addresses to receive emails for alerts, email groups are the most effective way to manage your alert recipient list.

1. In the Network Settings section, click **Notifications**.
2. Click **Email Notification Groups**.
3. Click **Add Group**.
4. In the Group Info section, enter the following information:

   • **Name:** The name of the email group.

   • **System Health Notifications:** Select this checkbox if you want to send system storage alerts to the email group. These alerts are sent under the following conditions:

   - 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 necessary role is missing, such as firmware, datastore, or packet capture.
5. In the Email Addresses text box, type the recipient email addresses for the team members that you want to receive the alert emails for this group. Email addresses can be entered one per line or separated by a comma, semicolon, or space. Email addresses are checked only for [name]@[company].[domain] format validation. There must be at least one email address in this text box for the group to be valid.
6. Click **Save**.

Connect the Discover appliance to any Explore, Trace or Command appliances

If you have any ExtraHop Explore, Trace or Command appliances in your environment, you can connect the Discover appliance to the Command appliance or join the Discover appliance to an Explore or Trace appliance. For more information, see the ExtraHop Admin UI Guide.