Deploy the ExtraHop Explore Appliance with VMware

This guide explains how to deploy the Explore appliance with the vSphere client running on a Windows machine. The guide assumes that you have experience administering VMware ESX and ESXi environments.

The Explore virtual appliance is distributed as an OVA package that includes a preconfigured virtual machine (VM) with a 64-bit, Linux-based OS that is optimized to work with VMware ESX and ESXi version 5.0 and later.

System Requirements

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

- An existing installation of VMware ESX or ESXi server version 5.0 and later capable of hosting the Explore virtual appliance. The Explore virtual appliance is available in the following configurations:
  - **EXA-S**
    - 8 CPUs
    - 32 GB RAM
    - One 4 GB virtual disk
    - One bridged network interface
  - **EXA-M**
    - 16 CPUs
    - 64 GB RAM
    - One 4 GB virtual disk
    - One bridged network interface
  - **EXA-L**
    - 32 CPUs
    - 128 GB RAM
    - One 4 GB virtual disk
    - One bridged network interface

    Note: You must add a second virtual disk to store record data when you deploy the Explore virtual appliance. Consult with your ExtraHop sales representative to determine the disk size that is best for your needs.
- A vSphere client
- The following TCP ports must be open:
  - 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.

Deploy the Explore Virtual Appliance

To deploy the Explore virtual appliance, complete the following steps:

1. Contact ExtraHop Support (support@extrahop.com) to obtain and download the OVA package.
2. Start the VMware vSphere client and connect to your ESX server.
3. Go to the **File** menu and select **Deploy OVF Template**.

4. The steps to deploy the OVF template are described in detail below. For most deployments, the default settings are sufficient.
   a. **Source**: Browse to the location of the downloaded OVA file and then click **Next**.
   b. **OVF Template Details**: Review the details and then click **Next**.
   c. **Name and Location**: Configure the VM name and location. Give the VM a unique and specific name for the ESX Inventory and then click **Next**.
   d. **Disk Format**: Select **Thick Provision Lazy Zeroed** and then click **Next**.
   e. **Network Mapping**: Map the OVF-configured network interface labels with the correct ESX-configured interface labels and then click **Next**.
   f. **Ready to Complete**: Verify the configuration, do not select the **Power on after deployment** checkbox, and then click **Finish** to complete the deployment.

   When the deployment is complete, you can see the unique name you assigned to the Explore VM instance in the inventory tree for the ESX server to which it was deployed.
5. Click the new Explore VM instance in the directory tree.
6. From the **Actions** drop-down list, select **Edit Settings...** to configure the disk where the Explore data is stored.
7. From the **New device** drop-down list, select **New Hard Disk**, and then click **Add**.
8. In the **New Hard disk** field, type the size of your virtual storage disk.
9. Click **OK**.
10. From the **Actions** drop-down list, select **Power On**.
11. From the **Actions** drop-down list, select **Open Console**.
12. Log in with the `shell` user account. Type `default` for the password.
13. Run the `show ipaddr` command to display the IP address of the Explore virtual appliance.
14. Exit the console window.

(Optional) Configure a Static IP Address

The Explore virtual appliance is configured with DHCP enabled. If your network does not support DHCP, you must configure a static address manually.

To configure a static IP address, complete the following steps:

1. Log in to the console with the shell user account. At the password prompt, type `default`, and then press ENTER.
2. Run the following command to enable privileged commands:

   ```
   enable
   ```

3. At the password prompt, type `default`, and then press ENTER.
4. Run the following command to enter configuration mode:

   ```
   configure
   ```

5. Run the following command to enter the interface configuration mode:

   ```
   interface
   ```

6. Run the ip command and specify the IP address and DNS settings in the following format: `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`

   For example:

```
extrahop(config-if)#ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

7. Run the following command to leave the interface configuration section:

   ```
   exit
   ```

8. Run the following command to save the running config file:

   ```
   running_config save
   ```

9. Type `Y` and then press ENTER.

Configure the Explore Appliance

After you configure an IP address for the Explore appliance, you can log into the Explore Admin UI through the following URL: https://<*explore_ip_address*>/admin.

> **Note**: The default username is *setup* and the password is *default*. You can modify user names and passwords in the Explore Admin UI.

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

- Register the Explore appliance.
- 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://<*explore_ip_address*>). If your browser prompts you about security certificates, ignore the warning and proceed.
2. Review the license agreement, select **I Agree**, and then click **Submit**.
3. On the log in screen, type *setup* for the user name 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**.

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

We recommend that you configure email notification settings so that the system can alert you if the following conditions occur:

- The physical disk is in a degraded state.
- The physical disk has an increasing error count.
- A registered Explore appliance node is missing from the cluster. The node might have failed, or is powered off.

Configure the **Email Server and Sender** settings:

1. In the **Network Settings** section, click **Notifications**.
2. Click **Email Server and Sender**.
3. On the **Email Settings** page, enter 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 Explore 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. Go to the **Network Settings** section and click **Notifications**.
2. Under **Notifications**, click **Email Addresses**.
3. In the **Email address** text box, type the recipient email address.
4. Click **Save**.

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.

To pair a Discover or Command appliance to an Explore cluster:

1. Log in to 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 Admin UI Guide*. See the ExtraHop Explore Settings section.
- *ExtraHop Web UI Guide*. See the Records section.
- *ExtraHop Trigger API Reference*