Deploy the ExtraHop Trace Appliance with VMware

Published: 2018-01-11

This guide explains how to deploy the virtual ExtraHop Trace appliance (EDA 1150v) on the VMware ESXi/ESX platform.

Virtual machine requirements

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

- An existing installation of VMware ESX or ESXi server version 6.0 or later capable of hosting the Trace virtual appliance. The virtual Trace appliance is available in the following configuration:
  - 2 CPUs
  - 16 GB RAM
  - 4 GB boot disk
  - 1 TB packetstore disk. You can reconfigure the disk size between 50 GB and 4 TB before deploying, if necessary.

To ensure proper functionality of the virtual appliance:

- Always choose thick provisioning. The ExtraHop packetstore requires low-level access to the complete drive and is not able to grow dynamically with thin provisioning.
- Do not change the default disk size after the appliance is deployed. Size the virtual disk either smaller or larger than the default 1TB before deploying. We do not support changing the original disk size or adding additional disks after the virtual machine is deployed.
- Do not migrate the virtual machine from one host or storage location to another. Although it is possible to migrate when the datastore is on a remote SAN, ExtraHop does not recommend this configuration.

Important: If you want to deploy more than one virtual Trace appliance, create the new instance with the original deployment package or clone an existing instance that has never been started.

Network requirements

Appliance	Intra-VM	External
ETA 1150v	A one 1-Gbps Ethernet network port is required for management. A dedicated port is not necessary. You can take advantage of the same physical NIC as other VMs in your environment. The management port must be accessible on port 443.	A one 1-Gbps Ethernet network port for the physical port mirror. We recommend that you duplicate the feed of the traffic that is sent to the Discover appliance to take advantage of the ExtraHop workflow.

Deploy the OVA file through the VMware vSphere web client

ExtraHop distributes the virtual Trace appliance package in the open virtual appliance (OVA) format.

Before you begin

If you have not already done so, download the ExtraHop Trace virtual appliance OVA file for VMware from the ExtraHop Customer Portal.

1. Start the VMware vSphere web client and connect to your ESX server.
2. Select the datacenter where you want to deploy the virtual Trace appliance.
3. Select **Deploy OVF Template…** from the Actions menu.
4. Follow the wizard prompts to deploy the virtual machine. For most deployments, the default settings are sufficient.
   a) Select **Local file** and then click **Browse…**.
   b) Select the OVA file on your local machine and then click **Open**.
   c) Click **Next**.
   d) Review the virtual appliance details and then click **Next**.
   e) Specify a name and location for the appliance and then click **Next**.
   f) Select a resource location and then click **Next**.
   g) For disk format, select **Thick Provision Lazy Zeroed** and then click **Next**.
   h) Map the OVF-configured network interface labels with the correct ESX-configured interface labels and then click **Next**.
   i) Verify the configuration and then choose one of the following options:

   - If you want to resize the packetstore disk:
     1. Click **Finish** to begin the deployment. When the deployment is complete, select **Edit Settings** from the Actions menu.
     2. Type a new size in the Hard disk 2 field. The minimum disk size is 50 GB and the maximum is 4 TB.
     3. From the Actions menu, select **Power** > **Power on**.
   - If you do not want to resize the packetstore disk, select the Power on after deployment checkbox and then click **Finish** to begin the deployment.
5. Select the virtual Trace appliance in the ESX Inventory and then select **Open Console** from the Actions menu.
6. Click the console window and then press ENTER to display the IP address. DHCP is enabled by default on the ExtraHop virtual appliance. To configure a static IP address, see the Configure a static IP address through the CLI section.
7. In VMware ESXi, configure the virtual switch to receive traffic and restart to see the changes.

Configure a static IP address through the CLI

The ExtraHop appliance is delivered with DHCP enabled. If your network does not support DHCP, no IP address is acquired, and you must configure a static address manually.

1. Establish a console connection to the ExtraHop appliance.
2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type `default`, and then press ENTER.
4. To configure the static IP address, run the following commands:
   a) Enable privileged commands:

   ```
   enable
   ```

   b) At the password prompt, type `default`, and then press ENTER.
   c) Enter configuration mode:

   ```
   configure
   ```

d) Enter the interface configuration mode:

```
interface
```

e) 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:

```
ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

f) Leave the interface configuration section:

```
exit
```

g) Save the running config file:

```
running_config save
```

h) Type `y` and then press ENTER.

Configure the Trace appliance

After you configure an IP address for the Trace appliance, you log into the Admin UI and complete the following procedures.

- Register the ExtraHop appliance
- Connect the Discover and Command appliances to the Trace appliance
- Review the ExtraHop Post-deployment Checklist and configure additional Trace appliance settings.

Register the ExtraHop appliance

Complete the following steps to apply a product key.

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 Admin UI, `https://<extrahop_ip_address>/admin`.
2. Review the license agreement, select **I Agree**, and then click **Submit**.
3. On the login screen, type `setup` for the username.
4. For the password, select from the following options:
   - For 1U and 2U appliances, type the service tag number found on the pullout tab on the front of the appliance.
   - For the EDA 1100, type the serial number displayed in the `Appliance info` section of the LCD menu. The serial number is also printed on the bottom of the appliance.
   - For a virtual appliance, type `default`.

5. Click **Log In**.
6. In the Appliance Settings section, click **License**.
7. Click **Manage License**.
8. Click **Register**.
9. Enter the product key and then click **Register**.
10. Click **Done**.

Connect the Discover and Command appliances to the Trace appliance

After you deploy the Trace appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Trace appliance before you can query for packets.

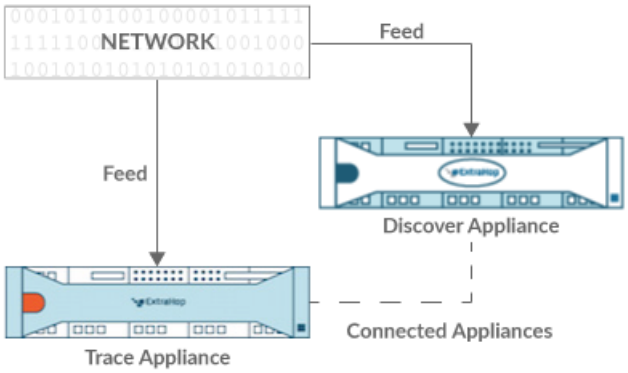


Figure 1: Connected to Discover Appliance

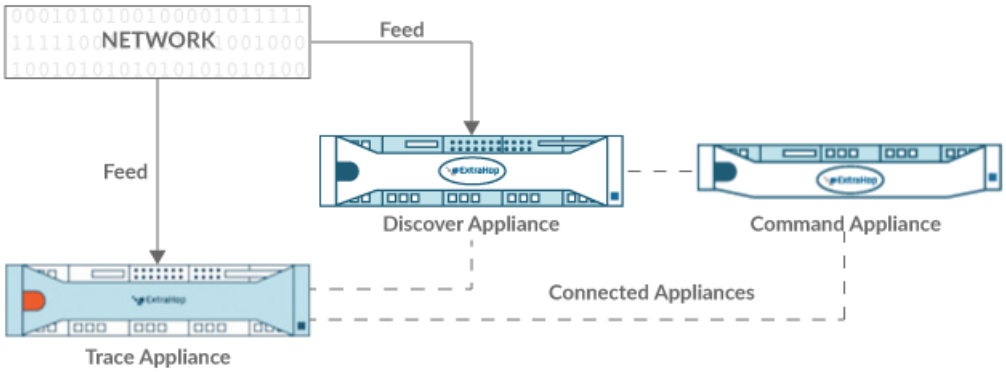


Figure 2: Connected to Discover and Command Appliance

1. Log into the Admin UI of the Discover appliance.
2. In the ExtraHop Trace Settings section, click **Connect Trace Appliances**.
3. Type the hostname or IP address of the Trace appliance in the Appliance hostname field.
4. Click **Pair**.

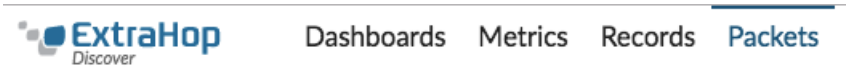
   Note: You can connect a Discover appliance to four or fewer Trace appliances. However, you can connect a Command appliance to an unlimited number of Trace appliances.
5. Note the information listed in the Fingerprint field. Verify that the fingerprint listed on this page matches the fingerprint of the Trace appliance listed on the Fingerprint page in the Admin UI of the Trace appliance.
6. Type the password of the Trace appliance `setup` user in the Trace Setup Password field.
7. Click **Connect**.
8. If you have a Command appliance, log into the Admin UI of the Command appliance and repeat steps 3 through 7.

Verify the configuration

After you have deployed and configured the Trace appliance, verify that the Trace appliance can collect packets through the Discover and Command appliances.

Before you begin
You must have a minimum user privilege of **view and download packets** to perform this procedure.

1. Log into the Web UI on the Discover or Command appliance.
2. Make sure **Packets** appears in the top menu.



3. Click **Packets** to start a new packet query. You should now see a list of the collected packets.

If the Packets menu item does not appear, revisit the Connect the Discover and Command appliances to the Trace appliance section. If no results are returned when you perform a packet query, check your network settings. If either issue persists, contact ExtraHop Support.