Deploy the ExtraHop Trace Appliance

Published: 2018-01-11

This guide explains how to install and configure the rack-mounted ExtraHop Trace appliance.

System requirements

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

Appliance

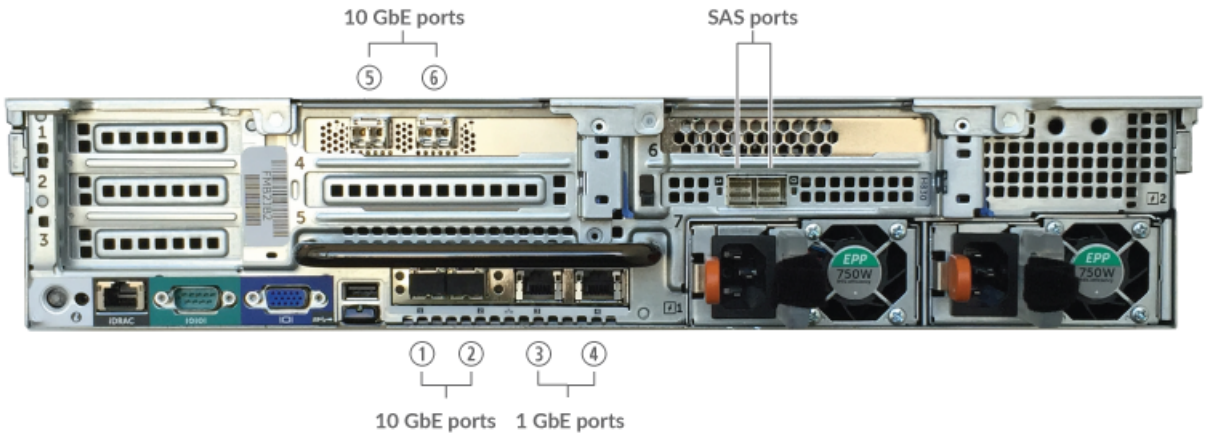
2U of rack space
2x750W of power

Network Access

TCP ports 80 and 443 must be open.

These ports enable you to administer the Trace appliance through the ExtraHop Web UI. Requests sent to port 80 are automatically redirected to HTTPS port 443.

Rear panel ports



- One iDRAC interface port
- One RS-232 serial port to connect a console device
- One VGA port to connect an external display
- Two USB 3.0 ports to connect input devices such as a keyboard and mouse
- Two power ports to connect the appliance to an AC power source
- Two 10/100/1000 BASE-T network ports. Port 3 is the primary management port.
- Four 10G ports. Ports 1 and 2 are reserved for future use and are disabled. Ports 5 and 6 are the monitoring (capture) interfaces.

Set up the appliance

1. Rack mount the Trace appliance.

   Install the Trace appliance in your data center with the included rack-mounting kit. The mounting kit supports most four-post racks with either round or square holes.
2. Connect port 3.

Connect your management network to the 1 GbE interface on port 3.

3. Connect the 10 GbE port.

   Connect your network data feed to the 10 GbE interface on port 5, port 6, or both.

   Important: The Trace appliance requires a duplicate feed of the traffic that is sent to the Discover appliance.

4. Connect the power cords.

   Connect the two supplied power cords to the power supplies on the back of the appliance, and then plug the cords into a power outlet. If the appliance does not power on automatically, press the power button on the front of the appliance.

Configure the management IP address

DHCP is enabled by default on the Trace appliance. When you power on the appliance, interface 3 attempts to acquire an IP address through DHCP. If successful, the IP address appears on the home screen of the LCD. If an IP address has not been configured, the LCD displays `No IP`.

If your network does not support DHCP, you can configure a static IP address through the LCD menu on the front panel or through the command-line interface (CLI). If an IP address has not been configured, the home screen displays `IP:(None)`.

Configure a static IP address through the front panel

Complete the following steps to manually configure an IP address through the front panel LCD controls.

1. Press the checkmark button.
2. Press the arrow buttons to select **Net**.
3. Select **Host**.

   The screen displays the host name. Return to the previous screen by scrolling to the up arrow on the screen and selecting the arrow.
4. Select **DHCP** to see how the IP address is configured. Press the left and right arrow buttons to select an option and then press the **Select** button.
5. On the Net screen, select **IP** and press the left and right arrow buttons to move between the digits. On the selected digit, click the checkmark button. The digit blinks when selected. While the digit is blinking, press the left and right arrow buttons to change the digit value.
6. After you have entered the number, click the checkmark button.
7. Press the left arrow button to navigate to the up arrow on the screen and select the arrow.
8. On the Save screen, select **Yes** and then press the checkmark button.
9. Wait a moment to be redirected to the Net screen. Repeat these steps to set the mask, gateway, and up to two DNS servers.
10. Press the arrow keys to scroll back to the **Home** menu and select **iDRAC**.
11. Configure the iDRAC DHCP, IP, mask, gateway, and DNS in the same manner as the IP address.
12. On the Net screen, select **Errors** to view system events such as CPU errors, undetected hard drives, or missing power supplies. When an error occurs, the LCD turns amber and displays the error immediately.
13. If there are multiple errors, press the left and right arrow buttons to scroll between the error messages. Press the **Select** button to exit the error screen. The **Clear** option removes the list of messages from the error screen.

Configure a static IP address through the CLI

You can access the CLI by connecting a USB keyboard and SVGA monitor to the appliance or through an RS-232 serial cable and a terminal-emulator program. The terminal emulator must be set to 115200 bps with 8 data bits, no parity, 1 stop bit (8N1), and hardware flow control should be disabled.

1. Establish a connection to the ExtraHop appliance.
2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type the service tag number found on the pullout tab on the front of the appliance, and then press ENTER.
4. To configure a static IP address, run the following commands:
   a) Enable privileged commands:

   ```
   enable
   ```

   b) At the password prompt, type the service tag number, and then press ENTER.
   c) Enter configuration mode

   ```
   configure
   ```

   d) Enter the interface configuration mode to configure interface 3:

   ```
   interface 3
   ```

   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.

   After you assign a static IP address, the IP address appears on the LCD at the front of the appliance.

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.

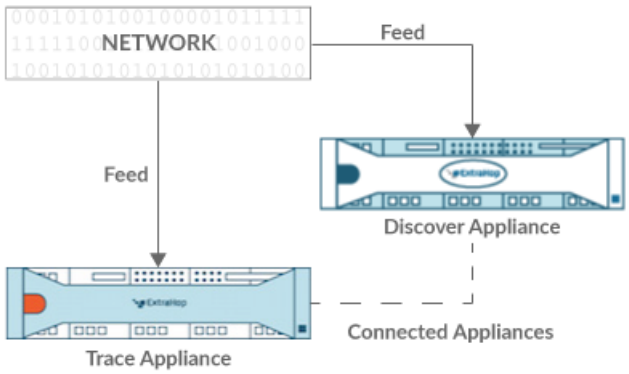


Figure 1: Connected to Discover Appliance

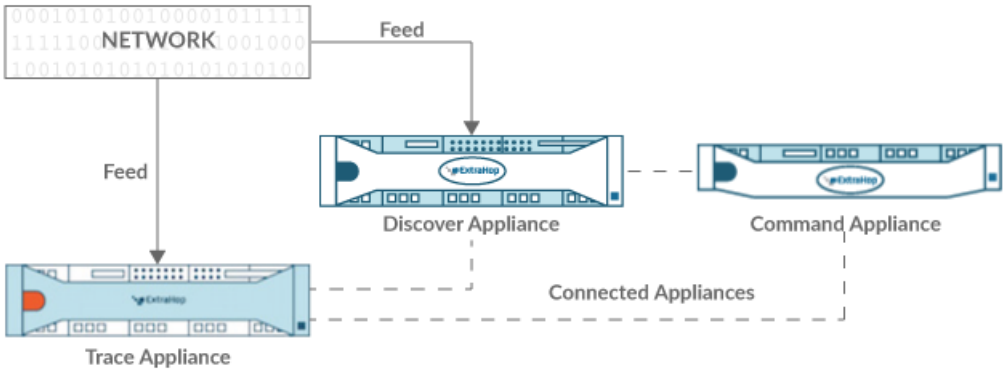


Figure 2: Connected to Discover and Command Appliance

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**.

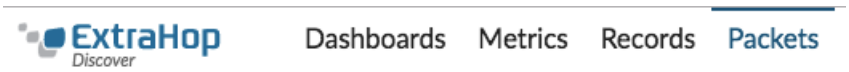
   Note: You can connect a Discover appliance to four or fewer Trace appliances. However, you can connect a Command appliance to an unlimited number of Trace appliances.
5. Note the information listed in the Fingerprint field. Verify that the fingerprint listed on this page matches the fingerprint of the 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.