# Configure Packet Capture on the ExtraHop Discover Appliance with VMware

Published: 2018-04-20

This guide describes how to configure the packet capture feature on the EDA 1000v, EDA 2000v, and EDA 6100v virtual ExtraHop Discover appliance with VMware. When packet capture is enabled through the Admin UI on the Discover appliance, you can write triggers to specify and deploy targeted packet captures from the Discover appliance to a disk drive on your VMware server.

## License packet capture

Ensure that your ExtraHop license has packet capture enabled.

**Before you begin**
The Discover appliance requires a product key and a license to configure packet capture. Contact ExtraHop Support to obtain your product key.

1. Log into the Admin UI on the Discover appliance .
2. In the System Settings section, click **License**.
3. In the Features section, verify if Packet Capture is already enabled.
   - If packet capture is enabled, proceed to step 7.
   - If your license does not have packet capture enabled, continue to the next step.
4. Click **Manage License** and then click **Register**.
5. Enter the product key, and then click **Register**. The ExtraHop system contacts the license server and validates the product key. After the product key is validated, the license is downloaded and applied to your appliance.
6. Refresh your browser to see the updated license.
7. Return to the main Admin UI page.
8. In the System Settings section, click **Disk**.
   The packet capture status displays `No Packet Capture Disk`. You will configure the packet capture disk in the next section.

## Configure a packet capture disk in VMware

The following settings are configured through the VMware vSphere Web Client.

1. Log into the VMware vSphere Web Client.
2. Select your Discover appliance virtual machine in the Virtual Machines inventory list.
3. From the Actions drop-down list , select **Edit Settings**.
4. From the New device drop-down list, select **New Hard Disk**, and then click **Add**.
5. Set the size of the disk to `500` GB.
6. Expand the New Hard disk settings and confirm that **Thick Provision Lazy Zeroed** is selected for Disk Provisioning. The remaining disk settings do not need to be changed.
7. Click **OK**.

## Enable the packet capture disk

1. In the ExtraHop Admin UI, refresh the Disk page. The packet capture disk should display a status of `running` and the size should display `500.0GB`. The drive is now allocated for packet capture.

2. In the Actions column for the packet capture disk, next to Triggered Packet Capture, click **Enable**.
3. Click **OK** to add the packet capture disk.

## Configure triggers to define the packet capture

The ExtraHop system gathers custom metrics through Application Inspection Triggers. These metrics are stored internally and can be accessed by the packet capture feature. The system will automatically process packet captures encountered in the trigger script.

For information about writing triggers, see the following documentation:

- Get started with triggers in the ExtraHop Web UI Guide.
- ExtraHop Trigger API Reference

1. In the ExtraHop Web UI, click the System Settings icon, and then click **Triggers**.
2. On the Triggers page, click **New**.
3. Type a name for the trigger in the Name field.
4. Select the **Enable Debugging** checkbox to help you validate that the script is running correctly.

   **Note:** Deselect **Enable Debugging** after you verify your script to avoid excessive debug messages in the Runtime Log.
5. Click in the Events field and select the events that will activate the trigger.
6. Click the **Editor** tab, type your trigger script, and then click **Save and Close**.

### Assign trigger to devices

After you create a trigger, the trigger must be assigned to one or more devices before the trigger can begin collecting data.

You also can assign the trigger to a device group, which assigns the trigger to each device in the group.

**Warning:** Avoid assigning any trigger to all devices. Running triggers on unnecessary devices exhausts system resources. Minimize performance impact by assigning a trigger only to the specific devices that you need to collect data from.

1. In the ExtraHop Web UI, click **Metrics** in the top menu, then click **Sources** > **Devices** in the left pane.
2. Select the checkbox for each device you want to assign the trigger to.
3. From the Select Action drop-down list, select **Assign to Trigger**.
4. Select the checkbox for the trigger you want to assign to the selected devices.
5. Click **OK**.

The trigger will execute on the selected devices whenever the trigger event occurs.

## View the packet capture results

1. In the ExtraHop Admin UI, in the Packet Captures section, click **View and Download Packet Captures**.
2. Select a packet capture and then click **Download Selected Captures** to download the pcap file to your workstation.
3. Open the downloaded packet capture in a packet analyzer, such as Wireshark.