Configure global packet capture

Published: 2018-04-20

When you enable the global packet capture feature on the Discover appliance, you start collecting packets for every flow to an SSD installed on your Discover appliance or, in the case of a virtual machine, to a regular disk drive.

Before you begin
Make sure you are licensed for the packet capture feature and that you have added the packet capture disk (an SSD on a physical appliance or an additional drive on a virtual machine). Note that the Packet Captures section in the Admin UI does not appear if your Discover appliance is not licensed for the feature. For information about adding an SSD drive, see Install an SSD for Packet Capture on the ExtraHop Discover Appliance.

For Discover virtual appliances, refer to your hypervisor manual for configuring an additional 500 GB disk.

1. Log into the Admin UI on the Discover appliance.
2. In the Packet Captures section, click **Global Packet Capture**.
3. In the Start Global Packet Capture section, type the following information:

   • **Name:** The name for the capture.

   • **Max Packets:** The maximum number of packets to capture. This value cannot be a negative number.

   • **Max Bytes:** The maximum number of bytes to captures. This value cannot be a negative number.

   • **Max Duration (milliseconds):** The maximum duration that the global capture should run. If this value is set to 0, this field is ignored and the duration runs for an unlimited time.

   • **Snaplen:** The maximum number of bytes copied per frame. By default, this value is 96 bytes, but you can set this value to a number between 1 and 65535.
4. Click **Start**.
5. Click **Stop** to stop the packet capture before any of the maximum limits are reached.

Download your packet capture from the View Packet Captures page and open the file in a packet analyzer such as Wireshark.

© 2018 ExtraHop Networks, Inc. All rights reserved.