Initiate precision packet captures to analyze zero window conditions

Published: 2018-10-27

In TCP metrics, window size specifies the amount of data that a device can receive and process during a flow. When the window size is zero, transmissions are halted until the device signals that it has the space to receive data again.

Zero window conditions that last 1 or 2 seconds are not too unusual, especially during periods of heavy traffic. However, longer-lasting zero window conditions can indicate a more serious problem and cause performance issues.

You can create a dashboard or configure alert notifications to track zero window occurrences, but the cause can be hard to determine. For example, CPU, memory, and NIC usage might be normal, and you don't know if the issue is with the network, the servers, or the application. But you can always find the truth in the packet!

In this walkthrough, you will create a trigger that captures packets with zero window conditions on database response and request flows. Then, you will download the captures so that you can upload the data to a packet analyzer to help you determine the state of the client and server on a flow when zero window conditions occurred.

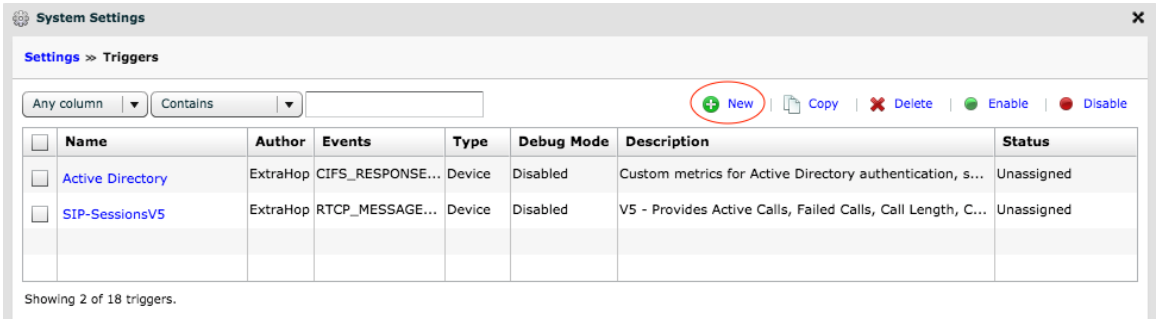
Prerequisites

- You must have access to an ExtraHop Discover appliance with a user account that has full system privileges.
- You must license and enable packet capture through the ExtraHop Admin UI.
- You must have a packet analyzer, such as WireShark or Microsoft Network Monitor.
- Familiarize yourself with Triggers concepts and the procedures in Build a trigger.

Write the precision capture trigger

In the following steps, you will write a trigger that initiates a precision packet capture each time a zero window condition occurs on a database transaction.

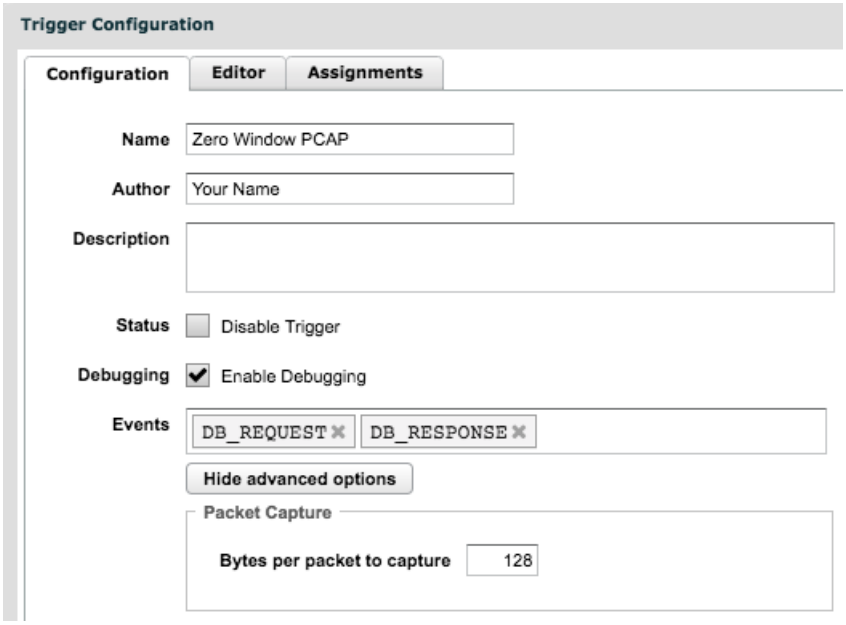
1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon and then click **Triggers**.
3. Click **New** to open the Trigger Configuration window.



4. On the Configuration tab, specify the following trigger configuration settings:
   a) Type `Zero Window` PCAP into the **Name** field.
   b) Select the **Enable Debugging** checkbox.
   c) From the Events list, select **DB_REQUEST** and **DB_RESPONSE**.

d) Click **Advanced Options** and type 128 in the Bytes per packet to capture field.

Tip: The default value is 0. Keep this value to capture all the bytes in each packet.



5. Click the **Editor** tab.
6. In the **Trigger Script** text box, type the following code to initiate the packet capture when a zero window condition occurs:

```
//The packet capture name, which includes the client and server
//IP addresses and port numbers
var pcapName = 'Zero Windows_'
    + Flow.client.ipaddr + ':' + Flow.client.port
    + '-'
    + Flow.server.ipaddr + ':' + Flow.server.port;

//Initiate packet capture each time a zero window occurs on
//the client or the server
if ( Flow.zeroWnd1 > 0 || Flow.zeroWnd2 > 0 ) {
    var opts = {
        maxPackets: 30,        // Capture up to 30 packets
        maxPacketsLookback: 15 // Capture up to 15 lookback packets
    };
    Flow.captureStart(pcapName, opts);
    //Show capture activity in runtime log
    debug('Start Zero PCAP: ' + pcapName);
}
```

7. Click **Save Changes**.

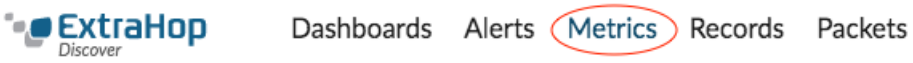
Assign the trigger to a source

In the following steps, you will assign a trigger to a data source. A trigger does not run until it is assigned to a source, and the trigger gathers data only from the sources to which it is assigned.

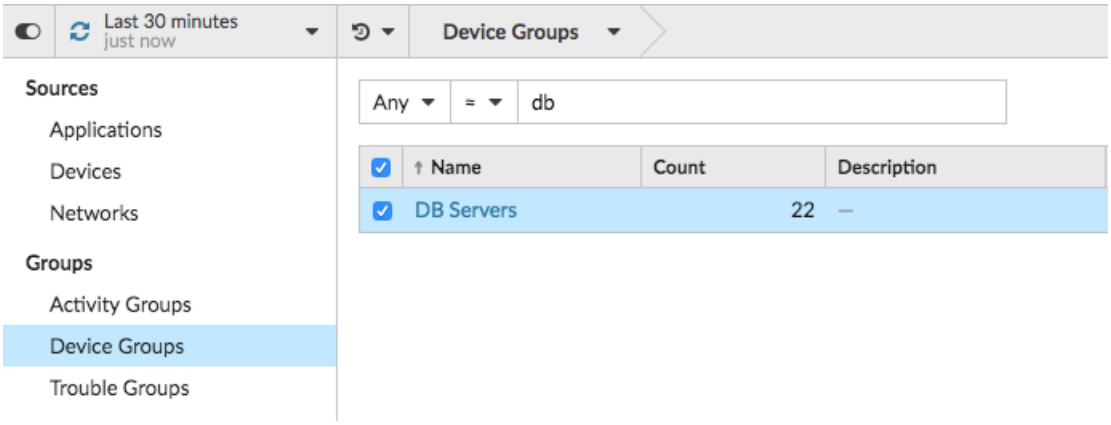
For the purposes of this walkthrough, the following procedure assigns the trigger to a device group called DB Servers. You should assign the triggers to the devices or device groups on your network that you want to monitor for zero window conditions.

Important: Running triggers on unnecessary devices and networks exhausts system resources. Minimize performance impact by assigning a trigger only to the specific sources that you need to collect data from.

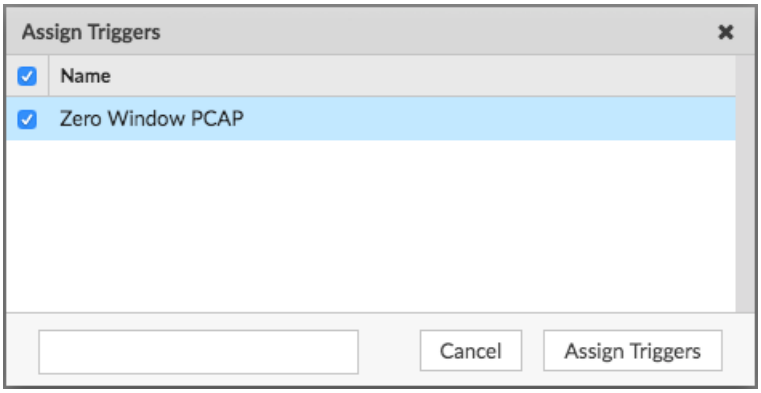
1. Click **Metrics** from the top menu.



2. Click **Device Groups** in the left pane, and then select **DB Servers**.



3. Click the Assign Trigger icon from the top of the page.
4. Select the trigger you just created named **Zero Window PCAP**.

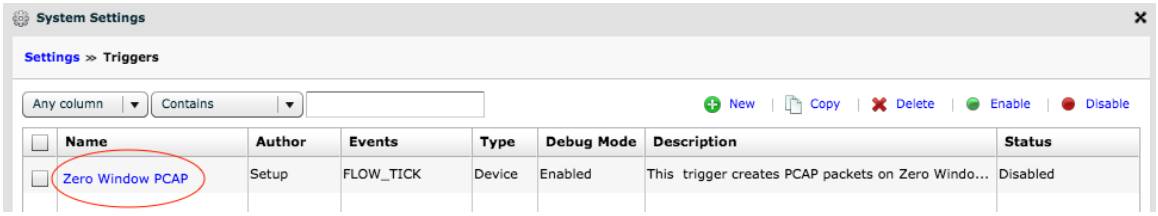


5. Click **Assign Triggers**.

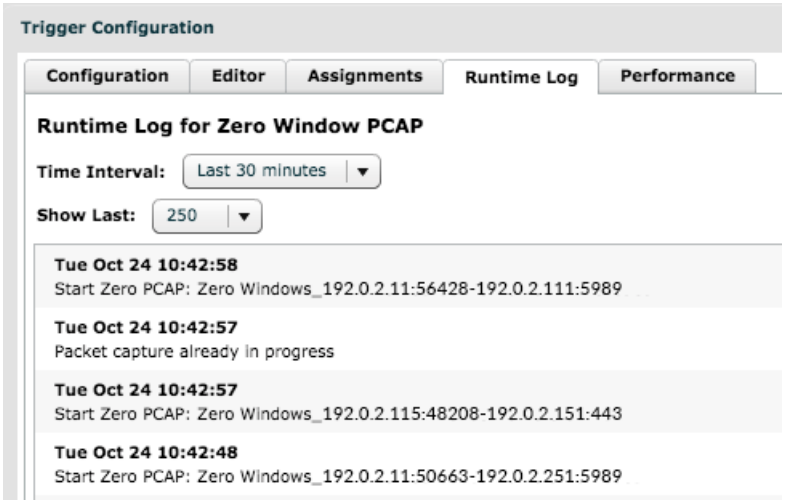
View debug output in the runtime log

In the following steps, you will view the trigger debug output to confirm that the trigger is running and capturing packets. After you assign the trigger to your data sources, the system runs the trigger when database traffic occurs, and if any transactions contain a zero window, the system sends debug results to the runtime log.

1. Click the System Settings icon, and then click **Triggers**.
2. Click the **Zero Window PCAP** trigger you just created.



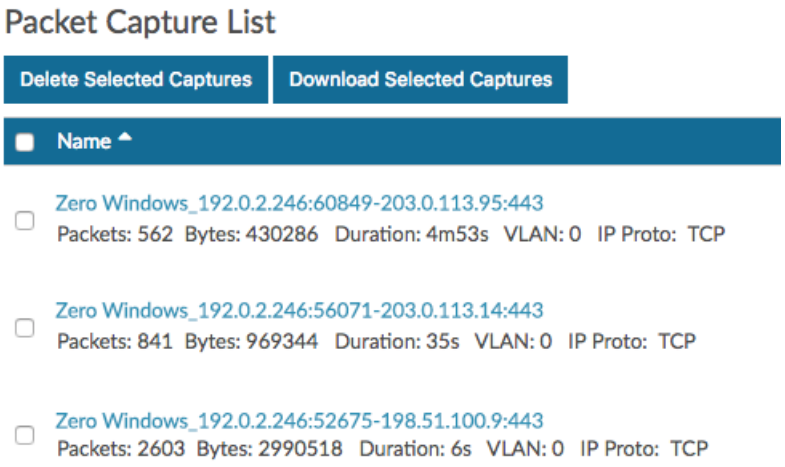
3. Click the **Runtime Log** tab.
   The runtime log displays results similar to the following figure:



Download and view packet captures

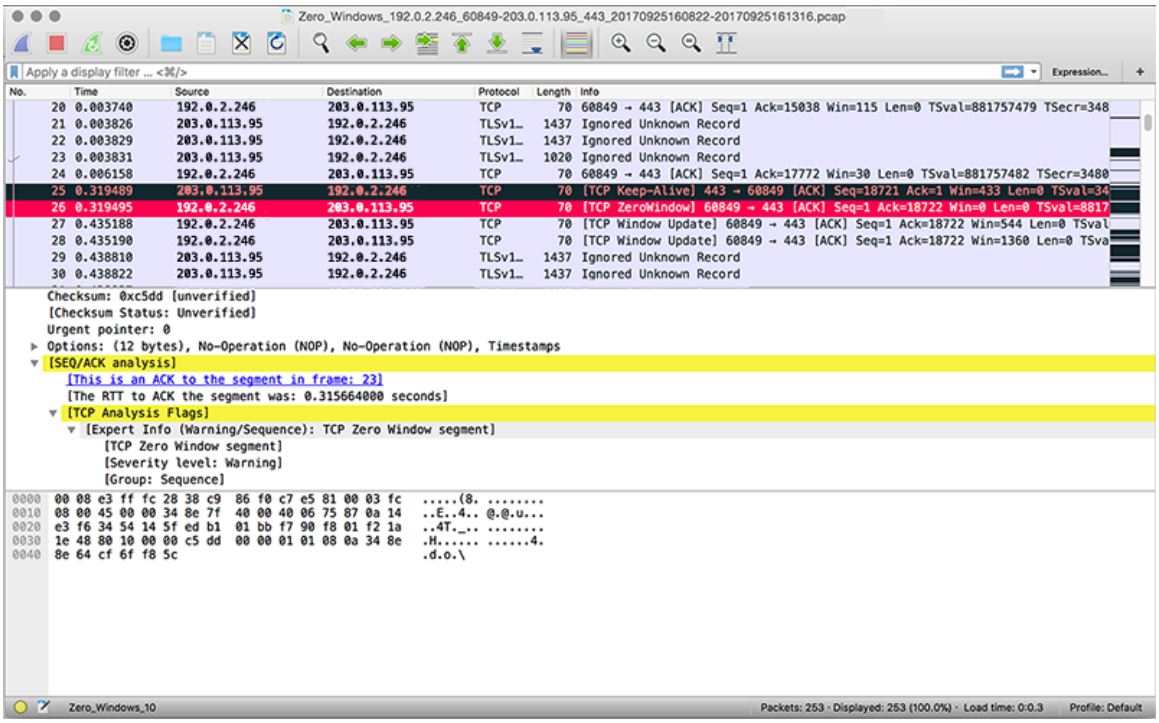
In the following steps, you will download packet captures from the ExtraHop Admin UI.

1. Click the System Settings icon, and then click **Administration**.
2. From the Packet Captures section, click **View and Download Packet Captures**.
   The Packet Capture List displays results similar to the following figure:



   Each packet capture in the list represents a flow of data between devices, and provides information about the devices, ports, and time range to help you narrow down which captures to download.
3. Select any capture named **Zero Windows_** and click **Download Selected Captures**.
   The capture is saved to your local machine with the `.pcap` file extension.
4. Open the capture file with a packet analyzer, such as Wireshark.

The output will look similar to the following figure:



5. Open packets that indicate a zero window occurrence.

   You will see details such as TCP flags, when zero window conditions occurred, the length of each occurrence, and which devices were involved.

   Look for patterns in the data and investigate the state of the client and server devices to help you narrow down and resolve the cause.