Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren

Veröffentlicht: 2023-10-31

In TCP-Metriken gibt die Fenstergröße die Datenmenge an, die ein Gerät während eines Datenflusses empfangen und verarbeiten kann. Wenn die Fenstergröße Null ist, werden Übertragungen angehalten, bis das Gerät signalisiert, dass es wieder Speicherplatz für den Empfang von Daten hat.

Nullfensterbedingungen, die 1 oder 2 Sekunden andauern, sind nicht allzu ungewöhnlich, insbesondere in Zeiten mit starkem Verkehr. Länger andauernde Nullfensterbedingungen können jedoch auf ein schwerwiegenderes Problem hinweisen und zu Leistungseinbußen führen.

Sie können ein Dashboard erstellen oder Warnmeldungen so konfigurieren, dass keine Fenster auftreten, aber die Ursache kann schwer zu ermitteln sein. Beispielsweise kann die CPU-, Arbeitsspeicher- und NIC-Auslastung normal sein, und Sie wissen nicht, ob das Problem mit dem Netzwerk, den Servern oder der Anwendung zusammenhängt. Aber du kannst immer die Wahrheit in der Paket finden!

In dieser exemplarischen Vorgehensweise erstellen Sie einen Auslöser, der Pakete ohne Fensterbedingungen bei HTTP-Transaktionen erfasst. Anschließend laden Sie die Aufzeichnungen herunter, sodass Sie die Daten in einen Paketanalysator hochladen können, der Ihnen hilft, den Status von Client und Server in einem Fluss zu ermitteln, wenn Nullfensterbedingungen eingetreten sind.

Voraussetzungen

- Sie benötigen entweder System- und Zugriffsadministrationsrechte oder volle Schreibrechte mit aktiviertem Paketzugriff.
- Du musst aktivieren Sie die Paketerfassung über die Administrationsseite.
- Sie benötigen einen Paketanalysator wie WireShark oder Microsoft Network Monitor.
- Machen Sie sich vertraut mit Auslöser Konzepte und Verfahren in Einen Auslöser erstellen.

Schreiben Sie den Precision Capture-Trigger

In den folgenden Schritten schreiben Sie einen Auslöser, der jedes Mal, wenn bei einer HTTP-Transaktion eine Nullfensterbedingung auftritt, eine präzise Paketerfassung initiiert.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Auslöser**.
3. klicken **Erstellen**.
4. Geben Sie die folgenden Einstellungen für die Trigger-Konfiguration an:
   a) Typ `Zero Window PCAP` in die **Name** Feld.
   b) Geben Sie im Feld Zuweisungen Folgendes ein `HTTP Servers`, und wählen Sie dann **HTTP-Server**.
   c) Wählen Sie in der Liste Ereignisse **FLOW_TICK**.
   d) Wählen Sie den **Debug-Log aktivieren** Checkbox.
   e) klicken **Erweiterte Optionen anzeigen** und tippen `128` im Feld Byte pro zu erfassendes Paket.

   Hinweis: Der Standardwert ist 0. Behalten Sie diesen Wert bei, um alle Byte in jedem Paket zu erfassen.

5. Geben Sie im rechten Bereich den folgenden Code ein, um die PCAP zu initiieren, wenn eine Nullfensterbedingung auftritt:

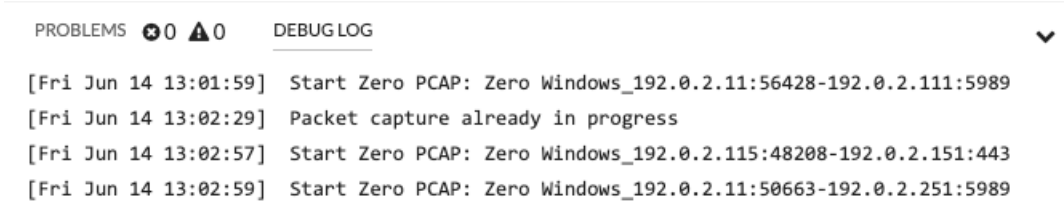
```
// Check to make sure that this is an HTTP transaction
if ( Flow.l7proto !== 'HTTP' ){
    return;
}

//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 debug log
    debug('Start Zero PCAP: ' + pcapName);
}
```

6. klicken **Speichern**.

Debug-Ausgabe im Debug-Log anzeigen

In den folgenden Schritten sehen Sie sich die Trigger-Debug-Ausgabe an, um zu bestätigen, dass der Auslöser ausgeführt wird und Pakete erfasst. Nachdem Sie den Auslöser Ihren Datenquellen zugewiesen haben, führt das System den Auslöser, wenn HTTP-Verkehr stattfindet, und wenn Transaktionen ein Nullfenster enthalten, sendet das System Debug-Ergebnisse an das Debug-Log.

1. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Auslöser**.
2. Klicken Sie auf **Zero Window PCAP** Auslöser, den du gerade erstellt hast.
3. klicken **Trigger-Skript bearbeiten**.
4. Klicken Sie auf **Debug-Protokoll** Registerkarte.
   Das Debug-Log zeigt Ergebnisse, die der folgenden Abbildung ähneln:



Paketerfassungen herunterladen und anzeigen

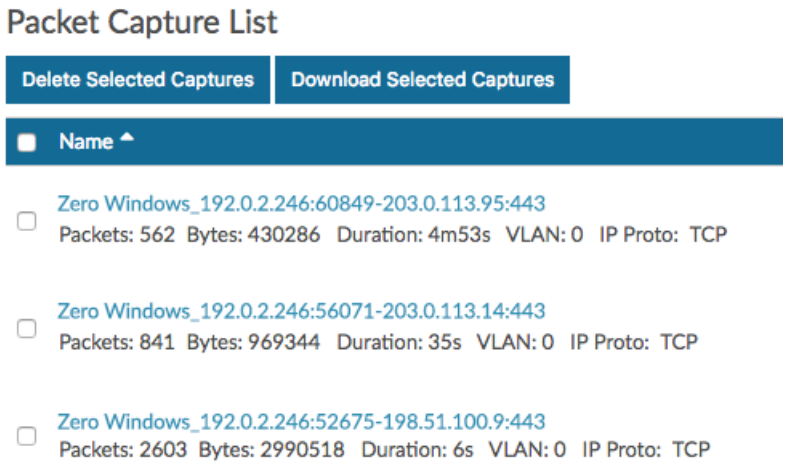
In den folgenden Schritten laden Sie Paketerfassungen herunter.

Hinweis: Die folgenden Schritte zeigen, wie Pakete von Reveal (x) Enterprise-Systemen heruntergeladen werden. Hinweise zum Herunterladen von Paketen von ExtraHop Performance-Systemen finden Sie unter Pakete auf ExtraHop Performance-Systemen herunterladen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Rekorde**.
3. Klicken **Aufzeichnungen anzeigen**.
4. Wählen Sie in der Dropdownliste Datensatztyp **Paketerfassung**.
5. Nachdem die mit Ihrer PCAP verknüpften Datensätze angezeigt werden, klicken Sie auf das Paketsymbol, und klicken Sie dann auf **PCAP herunterladen**.

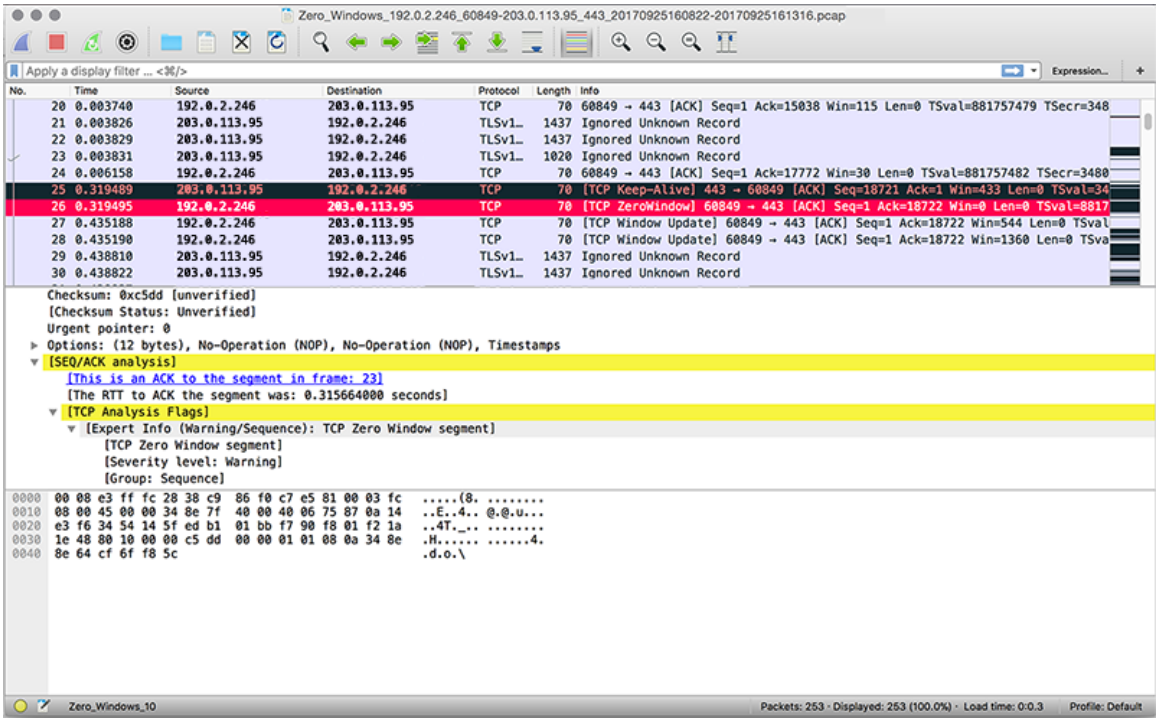
Pakete auf ExtraHop Performance-Systemen herunterladen

1. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Gesamte Verwaltung**.
2. Aus dem Paketerfassungen Abschnitt, klicken **Paketerfassungen anzeigen und herunterladen**.
   Die Liste der Paketerfassung zeigt Ergebnisse an, die der folgenden Abbildung ähneln:



   Jede PCAP in der Liste stellt einen Datenfluss zwischen Geräten dar und bietet Informationen zu den Geräten, Anschlüssen und dem Zeitbereich, sodass Sie eingrenzen können, welche Aufzeichnungen heruntergeladen werden sollen.
3. Wählen Sie eine Aufnahme mit dem Namen **Null Windows_** und klicken **Ausgewählte Aufnahmen herunterladen**.
   Die Aufnahme wird auf Ihrem lokalen Computer mit dem gespeichert `.pcap` Dateierweiterung.
4. Öffnen Sie die Capture-Datei mit einem Paketanalysator wie Wireshark.

Die Ausgabe sieht in etwa wie in der folgenden Abbildung aus:



5. Öffnet Pakete, die auf ein Nullfenstervorkommen hinweisen.

   Sie sehen Details wie TCP-Flags, wann Nullfensterbedingungen aufgetreten sind, die Dauer jedes Vorfalls und welche Geräte beteiligt waren.

   Suchen Sie nach Mustern in den Daten und untersuchen Sie den Zustand der Client- und Servergeräte, um die Ursache einzugrenzen und zu beheben.