Einen Auslöser erstellen

Veröffentlicht: 2024-07-02

Trigger bieten erweiterte Funktionen Ihres ExtraHop-Systems. Mit Triggern können Sie benutzerdefinierte Metriken erstellen, Datensätze generieren und speichern oder Daten an ein Drittanbietersystem senden. Da Sie das Trigger-Skript schreiben, steuern Sie die Aktionen, die der Auslöser bei bestimmten Systemereignissen ausführt.

Um einen Auslöser zu erstellen, müssen Sie eine Trigger-Konfiguration erstellen, das Trigger-Skript schreiben und den Auslöser dann einer oder mehreren Metrikquellen zuweisen. Der Auslöser wird erst ausgeführt, wenn alle Aktionen abgeschlossen sind.

Bevor Sie beginnen
Melden Sie sich beim ExtraHop-System mit einem Benutzerkonto an, das über die vollständige Schreibberechtigung verfügt Privilegien erforderlich, um Trigger zu erstellen.

Wenn du mit Triggern noch nicht vertraut bist, Machen Sie sich mit dem Trigger-Planungsprozess vertraut, mit deren Hilfe Sie den Fokus Ihres Auslöser eingrenzen oder feststellen können, ob Sie überhaupt einen Auslöser erstellen müssen. Führen Sie dann den Prozess zum Erstellen eines Auslöser durch, indem Sie den Exemplarische Vorgehensweise für Trigger.

Trigger-Einstellungen konfigurieren

Der erste Schritt beim Erstellen eines Auslöser besteht darin, einen Triggernamen anzugeben, festzustellen, ob Debugging aktiviert ist, und vor allem zu identifizieren, bei welchen Systemereignissen der Auslöser ausgeführt wird.

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:

Name

Ein Name für den Auslöser.

Autor

Der Name des Benutzers, der den Auslöser geschrieben hat. Standard-Trigger zeigen ExtraHop an.

Beschreibung

Eine optionale Beschreibung des Auslöser.

Zuweisungen

Die Geräte oder Gerätegruppen, denen der Auslöser zugewiesen ist. Ein Auslöser wird erst ausgeführt, wenn er einem Gerät zugewiesen ist, und der Auslöser sammelt Metrikdaten nur von den Geräten, denen er zugewiesen ist.

Warnung: Das Ausführen von Triggern auf nicht benötigten Geräten und Netzwerken erschöpft die Systemressourcen. Minimiere die Auswirkungen auf die Leistung, indem du einen Auslöser nur den spezifischen Quellen zuweist, aus denen du Daten sammeln musst.

Wichtig: Trigger mit den folgenden Ereignissen werden immer dann ausgeführt, wenn das Ereignis eintritt. Trigger, die nur bei diesen Ereignissen ausgeführt werden, können Geräten oder Gerätegruppen nicht zugewiesen werden.

- ALERT_RECORD_COMMIT
- ERKENNUNGSUPDATE
- METRIC_CYCLE_BEGIN
- ENDE DES METRISCHEN ZYKLUS
- METRIC_RECORD_COMMIT
- NEUE_ANWENDUNG
- NEUES_GERÄT
- SITZUNG ABLAUFEN
- TIMER_30 SEK

Debug-Log aktivieren

Ein Kontrollkästchen, das das Debuggen aktiviert oder deaktiviert. Wenn Sie dem Trigger-Skript Debug-Anweisungen hinzufügen, können Sie mit dieser Option Debug-Ausgabe anzeigen im Debug-Log, wenn der Auslöser ausgeführt wird.

Ereignisse

Die Ereignisse, bei denen der Auslöser ausgeführt wird. Der Auslöser wird immer dann ausgeführt, wenn eines der angegebenen Ereignisse auf einem zugewiesenen Gerät eintritt. Daher müssen Sie Ihrem Auslöser mindestens ein Ereignis zuweisen. Sie können in das Feld klicken oder mit der Eingabe eines Veranstaltungsnamens beginnen, um eine gefilterte Liste der verfügbaren Ereignisse anzuzeigen.

Erweiterte Optionen

Erweiterte Trigger-Optionen variieren je nach den ausgewählten Ereignissen. Wenn Sie zum Beispiel die `HTTP_RESPONSE` Ereignis, Sie können die Anzahl der Nutzdatenbytes festlegen, die bei diesen Ereignissen zwischengespeichert werden sollen.

Schreiben Sie ein Trigger-Skript

Das Triggerskript gibt die Anweisungen an, die der Auslöser ausführt, wenn ein für den Auslöser konfiguriertes Systemereignis eintritt.

Bevor Sie beginnen
Wir empfehlen Ihnen, das zu öffnen ExtraHop Trigger API-Referenz, das die Ereignisse, Methoden und Eigenschaften enthält, die Sie für Ihren Auslöser benötigen. Ein Link ist auch im Trigger-Editor-Fenster im ExtraHop-System verfügbar.

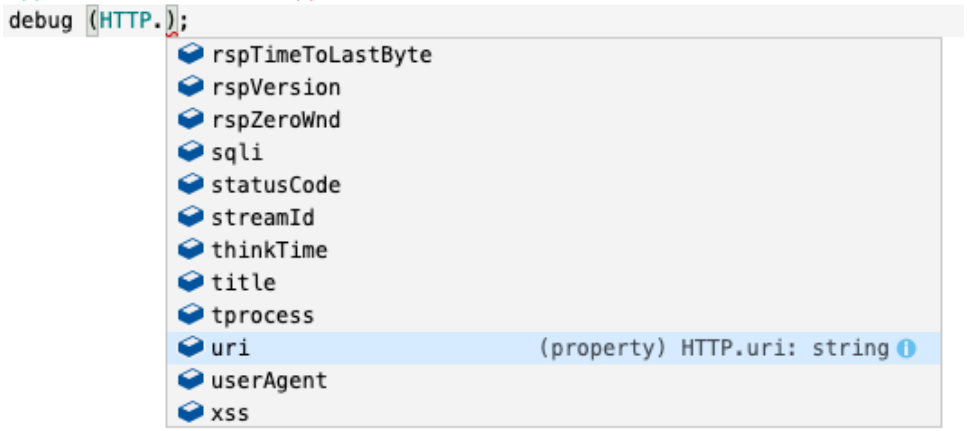
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Auslöser**.
3. klicken **Erstellen**.
4. Geben Sie im rechten Bereich das Triggerskript in JavaScript-ähnlicher Syntax mit Ereignissen, Methoden und Eigenschaften aus dem ExtraHop Trigger API-Referenz.

   Die folgende Abbildung zeigt ein Beispielskript, das auf der Registerkarte Editor eingegeben wurde:

```
1  if (HTTP.uri.match("seattle")){
2      Application("Seattle App").commit();
3      debug (HTTP.uri);
4  }
```

Der Editor bietet eine Autocomplete-Funktion, die eine Liste von Eigenschaften und Methoden anzeigt, die auf dem ausgewählten Klassenobjekt basieren. Geben Sie beispielsweise einen Klassennamen und

dann einen Punkt (.) ein, um eine Liste der verfügbaren Eigenschaften und Methoden anzuzeigen, wie in der folgenden Abbildung dargestellt:

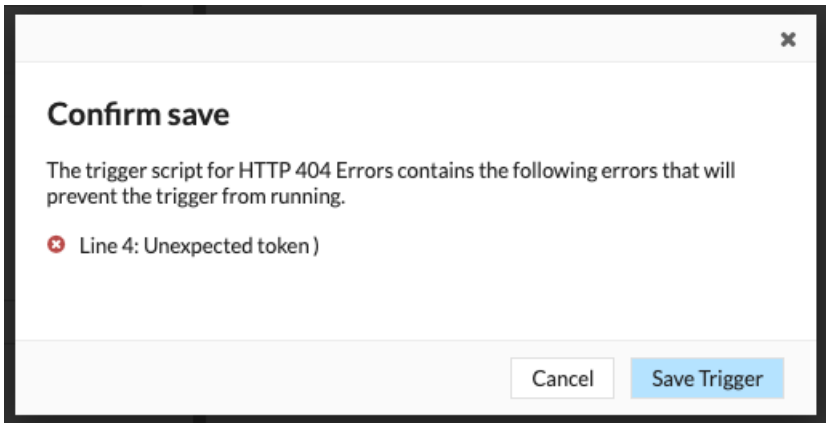


5. klicken **Speichern**.

   Der Editor bietet eine Syntaxvalidierung Ihres Skripts. Wenn Sie den Auslöser speichern, ruft der Validator alle ungültigen Aktionen, Syntaxfehler oder veralteten Elemente im Skript auf. Falls verfügbar, zeigt der Validator Ersetzungen für veraltete Elemente an.

   Warnung: Um eine schlechte Triggerleistung, falsche Ergebnisse oder einen Auslöser zu vermeiden, der nicht funktioniert, wird dringend empfohlen, den Code zu korrigieren oder das veraltete Element zu ersetzen.

   Die folgende Abbildung zeigt ein Beispiel für eine vom Syntaxvalidator generierte Fehlermeldung:



Erweiterte Trigger-Optionen

Sie müssen Trigger so konfigurieren, dass sie bei mindestens einem Ereignis ausgeführt werden. Je nach ausgewähltem Ereignis werden im Bereich „Trigger erstellen“ erweiterte Konfigurationsoptionen angezeigt. Wählen Sie zum Beispiel die HTTP_RESPONSE Ereignis ermöglicht es Ihnen, die Anzahl der Payload-Bytes festzulegen, die bei jedem Auftreten dieses Ereignis im System zwischengespeichert werden sollen.

In der folgenden Tabelle werden die verfügbaren erweiterten Optionen und die Ereignisse beschrieben, die jede Option unterstützen.

Option	Beschreibung	Unterstützte Ereignisse
Zu erfassende Byte pro Paket	Gibt die Anzahl der Byte an, die pro Paket erfasst werden sollen. Die Erfassung beginnt mit dem ersten Byte im Paket. Geben Sie diese Option nur an , wenn das Trigger-Skript die PCAP durchführt. Ein Wert von 0 gibt an, dass die Erfassung alle Byte in jedem Paket sammeln soll.	Alle Ereignisse außer der folgenden Liste werden unterstützt: • `ALERT_RECORD_COMMIT` • `METRIC_CYCLE_BEGIN` • `METRIC_CYCLE_END` • `FLOW_REPORT` • `NEW_APPLICATION` • `NEW_DEVICE` • `SESSION_EXPIRE`
L7-Nutzdaten-Bytes in den Puffer	Gibt die maximale Anzahl von Nutzdatenbytes an, die gepuffert werden sollen. **Hinweis:** Wenn mehrere Trigger für dasselbe Ereignis ausgeführt werden, bestimmt der Auslöser mi dem höchsten Wert für L Payload Bytes to Buffer die maximale Nutzlast für dieses Ereignis für jeden Auslöser.	• `CIFS_REQUEST` • `CIFS_RESPONSE` • `HTTP_REQUEST` • `HTTP_RESPONSE` • `ICA_TICK` • `LDAP_RESPONSE`
Byte aus der Zwischenablage	Gibt die Anzahl der Byte an, die bei einer Übertragung in die Citrix-Zwischenablage gepuffert werden sollen.	• `ICA_TICK`
Metrischer Zyklus	Gibt die Länge des Metrik Zyklus an, ausgedrückt in Sekunden. Der einzig gültige Wert ist `30sec`.	• `METRIC_CYCLE_BEGIN` • `METRIC_CYCLE_END` • `METRIC_RECORD_COMMIT`
Metrische Typen	Gibt den Metriktyp anhand des Rohmetriknamens an, z. B. `extrahop.device.http_server`. Geben Sie mehrere Metriktypen in einer kommagetrennten Liste an.	• `ALERT_RECORD_COMMIT` • `METRIC_RECORD_COMMIT`
Auslöser bei jedem Flow-Turn ausführen	Aktiviert die PCAP auf jedem Fluss drehen. Die Per-Turn-Analyse analysiert kontinuierlich die Kommunikation	• `SSL_PAYLOAD` • `TCP_PAYLOAD`

Option	Beschreibung	Unterstützte Ereignisse
	zwischen zwei Endpunkten, um einen einzelnen Nutzdatenpunkt aus dem Datenfluss zu extrahieren. Wenn diese Option aktiviert ist, werden alle angegebenen Werte für **Übereinstimmende Zeichenfolge für den Client** und **Passende Zeichenfolge für den Server** Optionen werden ignoriert.	
Portbereich des Clients	Gibt den Portbereich des Client an. Gültige Werte liegen zwischen 0 und 65535.	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD
Client-Bytes in den Puffer	Gibt die Anzahl der Client-Bytes an, die gepuffert werden sollen. Der Wert dieser Option kann nicht auf 0 gesetzt werden, wenn der Wert von **Server-Bytes zum Puffer** Die Option ist ebenfalls auf 0 gesetzt.	• SSL_PAYLOAD • TCP_PAYLOAD
Suchzeichenfolge für den Client-Puffer	Gibt die Formatzeichenfolge an, die angibt, wann mit dem Puffern der Client-Daten begonnen werden soll. Gibt bei einer Zeichenkettenübereinstimmung das gesamte Paket zurück. Sie können die Zeichenfolge als Text oder Hexadezimalzahlen angeben. Zum Beispiel beide `ExtraHop` und `\x45\x78\x74\x72\x61\x48\x6F\x70` sind gleichwertig. Hexadezimalzahlen unterscheiden nicht zwischen Groß- und Kleinschreibung. Jeder für diese Option angegebene Wert wird ignoriert , wenn **Pro Spielzug** oder **Auslöser**	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD

Option	Beschreibung	Unterstützte Ereignisse
	auf allen UDPs ausführen Die Option Pakete ist aktiviert.	
Server-Port-Bereich	Gibt den Serverportbereich an. Gültige Werte liegen zwischen 0 und 65535.	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD
Server-Bytes in Puffer	Gibt die Anzahl der Server-Bytes an, die gepuffert werden sollen. Der Wert dieser Option kann nicht auf 0 gesetzt werden, wenn der Wert von **Client-Bytes zum Puffer** Die Option ist ebenfalls auf 0 gesetzt.	• SSL_PAYLOAD • TCP_PAYLOAD
Suchzeichenfolge für Serverpuffer	Gibt die Formatzeichenfolge an, die angibt, wann mit dem Puffern der Serverdaten begonnen werden soll. Sie können die Zeichenfolge als Text oder Hexadezimalzahlen angeben. Zum Beispiel beide `ExtraHop` und `\x45\x78\x74\x72\x61\x48\x6F\x70` sind gleichwertig. Hexadezimalzahlen unterscheiden nicht zwischen Groß- und Kleinschreibung. Jeder für diese Option angegebene Wert wird ignoriert , wenn **Pro Spielzug** oder **Auslöser auf allen UDPs ausführen** Option ist aktiviert.	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD
Auslöser für alle UDP-Pakete ausführen	Ermöglicht die Erfassung aller UDP-Datagramme.	• UDP_PAYLOAD
FLOW_CLASSIFY für ablaufende, nicht klassifizierte Flows ausführen	Ermöglicht die Ausführung des Ereignis nach Ablauf, um Metriken zu sammeln für Flüsse die vor Ablauf nicht klassifiziert wurden.	• FLOW_CLASSIFY
Externe Typen	Gibt die Typen von externen Daten an, die der Auslöser verarbeitet. Der Auslöser wird nur ausgeführt, wenn die Payload ein Typfeld mit einem der angegebenen Werte enthält. Geben Sie mehrere Typen in einer kommagetrennten Liste an.	1. EXTERNAL_DATA