Sammeln Sie benutzerdefinierte Datensätze

Veröffentlicht: 2024-04-13

Sie können die Art der Datensatzdetails, die Sie generieren und in einem Recordstore speichern, anpassen, indem Sie einen Auslöser schreiben. Wir empfehlen, dass Sie auch ein Datensatzformat erstellen, um zu steuern, wie die Datensätze im ExtraHop-System angezeigt werden.

Bevor Sie beginnen

- Diese Anweisungen setzen eine gewisse Vertrautheit mit ExtraHop voraus Auslöser.
- Wenn Sie mit einem Google BigQuery-Datensatzspeicher verbunden sind, gilt für benutzerdefinierte Datensätze ein Limit von 300.

Im folgenden Beispiel erfahren Sie, wie Sie nur Datensätze für HTTP-Transaktionen speichern, die zu einem 404-Statuscode führen. Zunächst schreiben wir einen Auslöser, um Informationen aus dem integrierten HTTP-Datensatztyp zu sammeln. Dann weisen wir den Auslöser einem Server zu. Schließlich erstellen wir ein Datensatzformat, um ausgewählte Datensatzfelder in der Tabellenansicht für unsere Datensatzabfrageergebnisse anzuzeigen.

Einen Auslöser schreiben und zuweisen

Beachten Sie, dass der Auslöser auf jedem erstellt werden muss Sensor von denen Sie diese Arten von Datensätzen sammeln möchten. Sie können den Auslöser auf einem erstellen Konsole um Ihre benutzerdefinierten Datensätze von allen verbundenen zu sammeln Sensoren.

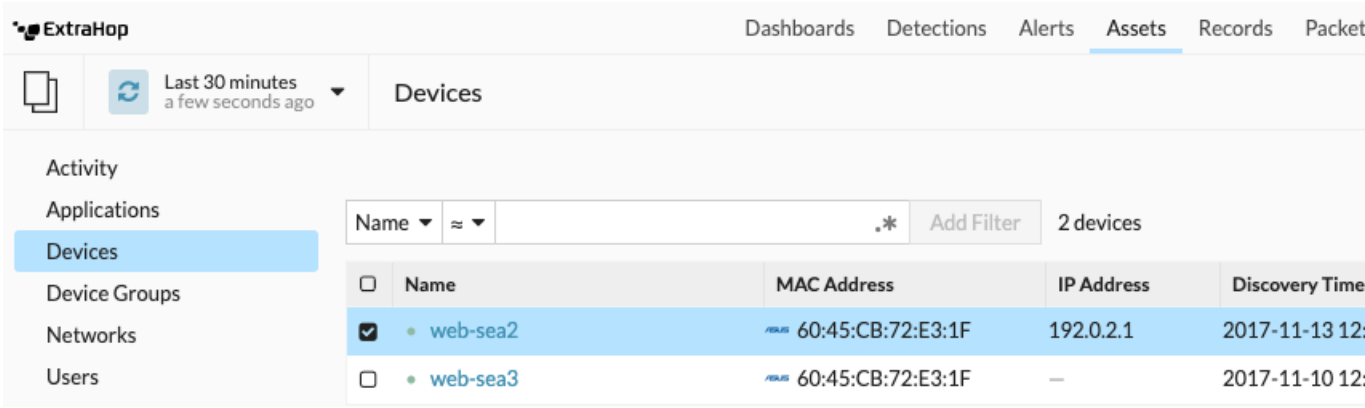
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. klicken **Erstellen**.
4. In der Trigger erstellen Fenster, vervollständigen Sie Ihre Informationen, ähnlich dem folgenden Beispiel:
   - **Name:** `HTTP 404-Fehler`
   - **Beschreibung:** `Verfolgen Sie 404-Fehler auf dem primären Server.`
   - **Debug-Log aktivieren:** Markieren Sie das Kontrollkästchen, um das Debuggen zu aktivieren.
   - **Ereignisse:** `HTTP_RESPONSE`
5. Klicken Sie auf **Herausgeber** Tab, um die Trigger-Spezifikationen zu schreiben.

   Die folgende Abbildung zeigt eine Beispielkonfiguration, die nur Datensätze sammelt, wenn ein 404-Statuscode erkannt wird. Wir haben auch einen Namen festgelegt (`web 404`) für diese Datensatztypen, um sie in einer Datensatzabfrage zu identifizieren, und es wurden identifizierende Informationen für das Debuggen hinzugefügt.

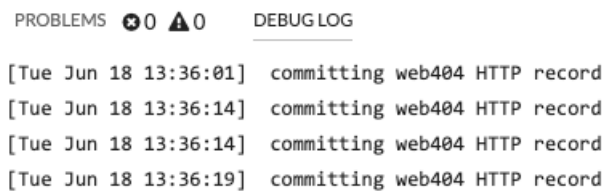
```
1  if (HTTP.statusCode === 404) {
2      commitRecord("web404", HTTP.record);
3      debug("committing web404 HTTP record");
4  }
```

   Weisen Sie den Auslöser in den nächsten Schritten einem Gerät oder einer Gerätegruppe zu, für die Sie 404-Statuscodes überwachen möchten.
6. klicken **Vermögenswerte** aus dem oberen Menü.
7. klicken **Geräte** und klicken Sie dann auf **Aktive Geräte** Diagramm.

8. Wählen Sie das Kontrollkästchen für ein Gerät aus der Liste aus. Für unser Beispiel wählen wir einen Server namens `web2-sea`.
9. Klicken Sie auf das Symbol „Auslöser zuweisen“, wählen Sie den Trigger aus, den Sie in den vorherigen Schritten erstellt haben, und klicken Sie dann auf **Trigger zuweisen**. In der folgenden Abbildung haben wir unseren Server ausgewählt, `web2-sea`.



Nachdem Sie den Auslöser zugewiesen haben, kehren Sie zurück zum **Systemeinstellungen > Trigger** Seite und wählen Sie den Auslöser aus, den Sie erstellt haben. Stellen Sie zunächst sicher, dass Ihr Gerät aktiv ist. Klicken Sie dann auf **Debug-Protokoll** Klicken Sie auf die Registerkarte, um zu sehen, ob der Auslöser Ihre Datensätze festschreibt. Im folgenden Beispiel haben wir bewusst nicht verfügbare Webseiten besucht, um 404-Fehler zu generieren.



Erstellen Sie ein benutzerdefiniertes Datensatzformat, um Ihre Datensatzergebnisse in einer Tabelle anzuzeigen

Datensatzformate sind die empfohlene Methode, um Ihre Datensätze nur mit den Feldern anzuzeigen, die Sie sehen möchten. Ohne ein benutzerdefiniertes Datensatzformat werden die Felder für Ihren benutzerdefinierten Datensatz in keiner auswählbaren Liste angezeigt, z. B. in der Liste Gruppieren nach.

Der schnellste Weg, ein benutzerdefiniertes Datensatzformat zu erstellen, besteht darin, das Schema beim Lesen aus einem integrierten Datensatzformat zu kopieren und in ein neues Datensatzformat einzufügen. Wenn Sie über mehrere Sensoren verfügen, müssen Sie das benutzerdefinierte Datensatzformat auf jeder Appliance erstellen, auf der die Aufzeichnungsergebnisse angezeigt werden. Sie können das Datensatzformat auf einer Konsole erstellen, um einen benutzerdefinierten Datensatz auf allen angeschlossenen Sensoren zu formatieren.

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 **Formate aufzeichnen**.
3. Klicken Sie auf den Datensatztyp, den Sie kopieren möchten. In unserem Beispiel kopieren wir das HTTP-Datensatzformat.
4. Kopieren Sie den Inhalt in das Textfeld unten Schema beim Lesen.
5. klicken **Neues Datensatzformat**.

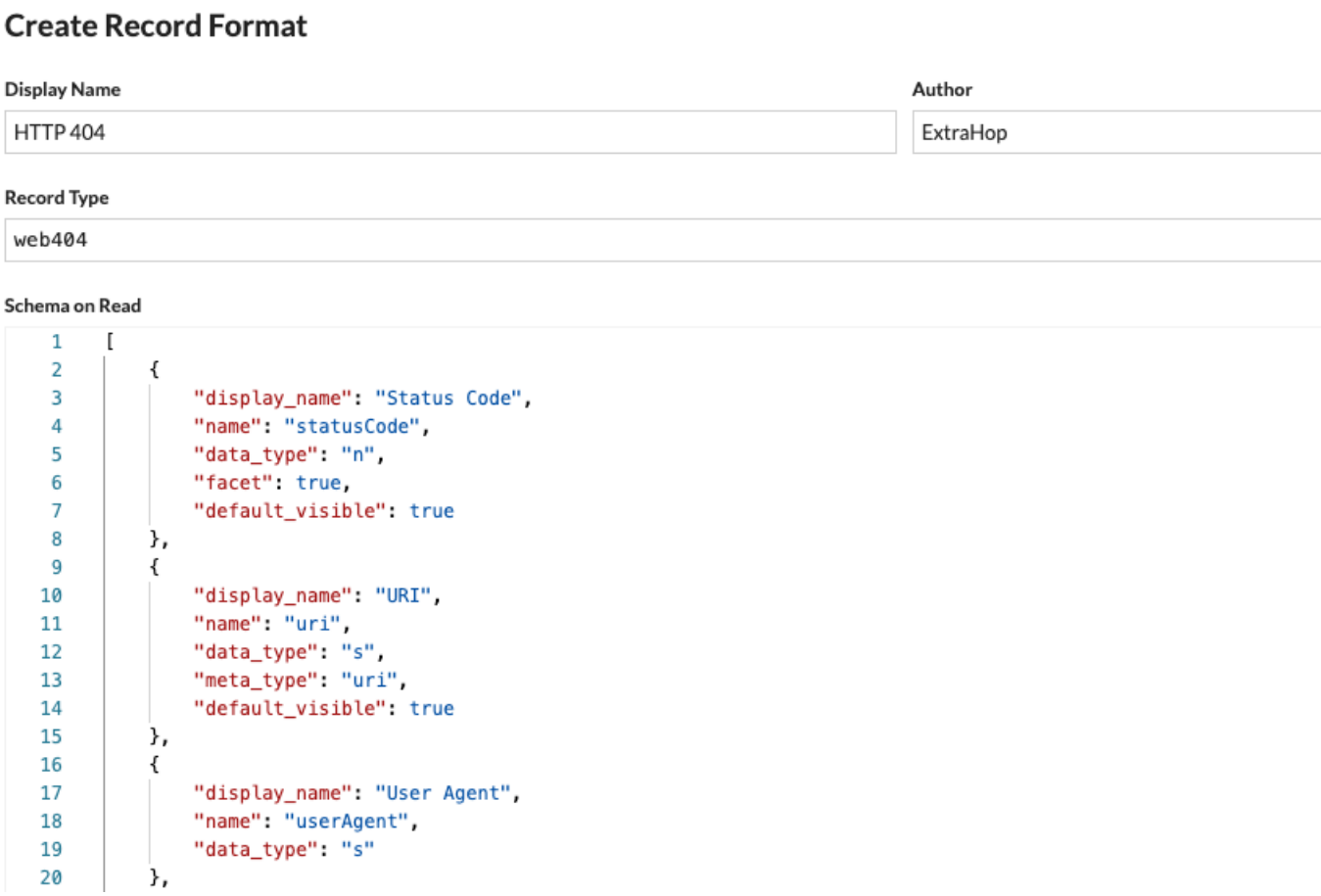
6. Füllen Sie die folgenden Felder aus:

   • **Name anzeigen:** Geben Sie einen eindeutigen Namen für Ihr Datensatzformat ein.

   • **Autor:** Identifizieren Sie den Autor für das Datensatzformat.

   • **Art des Datensatzes:** Geben Sie dieselbe Datensatztyp-ID ein, die Sie im Auslöser erstellt haben. In unserem Beispiel ist dieser Wert `web404`.

   • **Schema beim Lesen:** Fügen Sie den kopierten Inhalt aus Schritt 4 in das Textfeld ein. Bearbeiten Sie das Feld, um alle unerwünschten Felder zu löschen. Für unser Beispiel in der Abbildung unten haben wir nur die folgenden Felder beibehalten: Client, Server, Methode, Statuscode, URI und Verarbeitungszeit.



Fragen Sie nach Ihrem benutzerdefinierten Datensatztyp ab

1. klicken **Rekorde** aus dem oberen Menü.
2. Klicken Sie auf **Beliebiger Datensatztyp** Drop-down-Liste und wählen Sie Ihr neu erstelltes Datensatzformat aus.
3. klicken **Aufzeichnungen ansehen**.
4. Klicken Sie auf **Ausführliche Ansicht**  Ikone.
5. klicken **Felder** und dann klicken **Alles auswählen**.
   Alle vom Auslöser gesammelten Informationen zu diesen Datensätzen werden in den Abfrageergebnissen angezeigt.

Einstellungen für das Aufzeichnungsformat

Die Einstellungen für das Aufzeichnungsformat Auf dieser Seite wird eine Liste aller integrierten und benutzerdefinierten Aufzeichnungsformate angezeigt, die auf Ihren ExtraHop-Sensoren oder Ihrer Konsole verfügbar sind. Wenn Sie ein benutzerdefiniertes Datensatzformat erstellen müssen, empfehlen wir Ihnen, das Schema zu kopieren und in gelesene Informationen aus einem integrierten Datensatzformat einzufügen. Fortgeschrittene Benutzer möchten möglicherweise ein benutzerdefiniertes Datensatzformat mit ihren eigenen Feld-Wert-Paaren erstellen und sollten das in diesem Abschnitt bereitgestellte Referenzmaterial verwenden.

Aufzeichnungsformate bestehen aus den folgenden Einstellungen:

Name anzeigen

Der Name, der für das Datensatzformat im ExtraHop-System angezeigt wird. Wenn es kein Datensatzformat für den Datensatz gibt, wird der Datensatztyp angezeigt.

Autor

(Optional) Der Autor des Datensatzformat. Alle integrierten Aufzeichnungsformate werden angezeigt `ExtraHop` als Autor.

Art des Datensatzes

Ein eindeutiger alphanumerischer Name, der den Informationstyp identifiziert, der im zugehörigen Datensatzformat enthalten ist. Der Datensatztyp verknüpft das Datensatzformat mit den Datensätzen, die an den Recordstore gesendet werden. Integrierte Aufzeichnungsformate haben einen Datensatztyp, der mit einer Tilde (~) beginnt. Benutzerdefinierte Datensatzformate können keinen Datensatztyp haben, der mit einer Tilde (~) oder einem AT-Symbol (@) beginnt.

Schema beim Lesen

Ein Array im JSON-Format mit mindestens einem Objekt, das aus einem Feldnamen- und Wertepaar besteht. Jedes Objekt beschreibt ein Feld im Datensatz, und jedes Objekt muss eine eindeutige Kombination aus Name und Datentyp für dieses Datensatzformat haben. Sie können die folgenden Objekte für ein benutzerdefiniertes Datensatzformat erstellen:

Name

Der Name des Feldes.

Anzeigename

Der Anzeigename für das Feld. Wenn der `display_name` Feld ist leer, das `name` Feld wird angezeigt.

Beschreibung

(Optional) Beschreibende Informationen zum Datensatzformat. Dieses Feld ist auf die Seite mit den Einstellungen für das Datensatzformat beschränkt und wird in keiner Datensatzabfrage angezeigt.

default_visible

(Optional) Wenn gesetzt auf `true`, wird dieses Feld im ExtraHop-System standardmäßig als Spaltenüberschrift in der Tabellenansicht angezeigt.

Facette

(Optional) Wenn gesetzt auf `true`, Facetten für dieses Feld werden im ExtraHop-System angezeigt. Facetten sind eine kurze Liste der häufigsten Werte für das Feld, auf die Sie klicken können, um einen Filter hinzuzufügen.

Datentyp

Die Abkürzung, die den Typ der in diesem Feld gespeicherten Daten identifiziert. Die folgenden Datentypen werden unterstützt:

Art der Daten	Abkürzung	Beschreibung
Anwendung	`app`	ExtraHop-Anwendungs-ID (Zeichenfolge)
boolesch	`b`	Boolescher Wert
Gerät	`dev`	ExtraHop-Geräte-ID (Zeichenfolge)
Flussschnittstelle	`fint`	Flow-Schnittstellen-ID
Flussnetz	`fnet`	Flow-Netzwerk-ID
IPv4	`addr4`	Eine IPv4-Adresse im Dotted-Quad-Format. Filter, die größer oder kleiner als sind, werden unterstützt.
IPv6	`addr6`	Eine IPv6-Adresse. Es werden nur string-orientierte Filter unterstützt.
Nummer	`n`	Zahl (Ganzzahl oder Fließkomma)
Schnur	`s`	Generische Zeichenfolge

metatyp

Die Unterklassifizierung des Datentyps, die weiter bestimmt, wie die Informationen im ExtraHop-System angezeigt werden. Die folgenden Metatypen werden für jeden der zugehörigen Datentypen unterstützt:

Art der Daten	Metatyp
Schnur	• `domain` • `uri` • `user`
Zahl	• `bytes` • `count` • `expiration` • `milliseconds` • `packets` • `timestamp`