Collecte d'enregistrements personnalisés

Publié: 2023-09-19

Vous pouvez personnaliser le type de détails des enregistrements que vous générez et stockez dans un magasin d'enregistrements en écrivant un déclencheur. Nous vous recommandons de créer également un format d'enregistrement pour contrôler l'affichage des enregistrements dans le système ExtraHop.

Avant de commencer

- Ces instructions supposent une certaine familiarité avec les déclencheurs ExtraHop.
- Si vous êtes connecté à un magasin d'enregistrements Google BigQuery, le nombre de champs d'enregistrements personnalisés est limité à 300.

Dans l'exemple suivant, vous apprendrez à ne stocker que les enregistrements des transactions HTTP qui aboutissent à un code d'état 404. Tout d'abord, nous allons écrire un déclencheur pour collecter des informations à partir du type d'enregistrement HTTP intégré. Ensuite, nous assignerons le déclencheur à un serveur web. Enfin, nous créerons un format d'enregistrement pour afficher les champs d'enregistrement sélectionnés dans la vue tableau des résultats de notre requête d'enregistrement.

Rédiger et attribuer un déclencheur

Notez que le déclencheur doit être créé sur chaque capteur à partir duquel vous souhaitez collecter ces types d'enregistrements. Vous pouvez créer le déclencheur sur une console pour collecter vos enregistrements personnalisés à partir de tous les capteurs connectés.

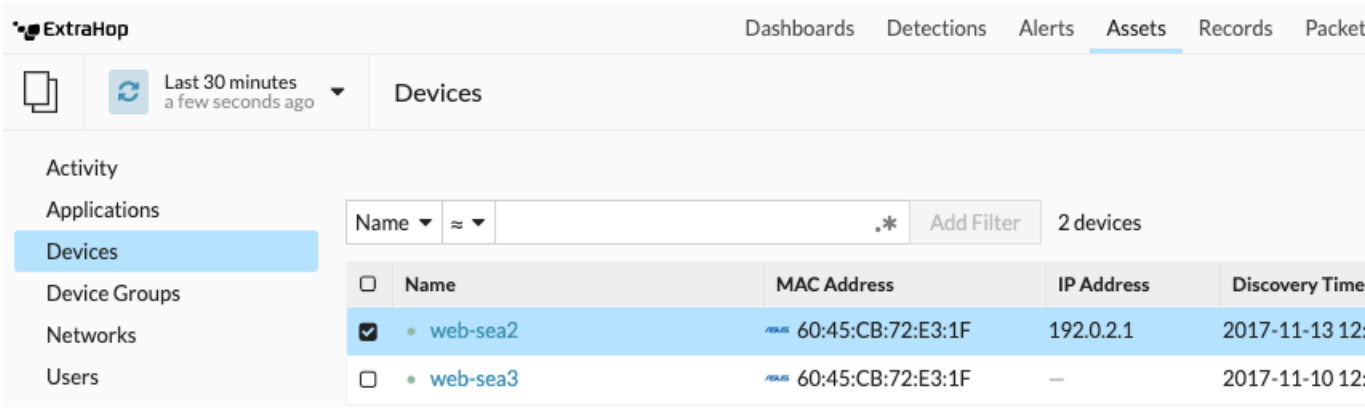
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système, puis sur **Déclencheurs**.
3. Cliquez sur **Créer**.
4. Dans le volet Créer un déclencheur, complétez vos informations, comme dans l'exemple suivant :
   - **Nom:** `Erreurs HTTP 404`
   - **Description:** `Suivre les erreurs 404 sur le serveur web principal.`
   - **Activer le journal de débogage:** Cochez la case pour activer le débogage.
   - **Événements:** `HTTP_RESPONSE`
5. Cliquez sur l'onglet **Éditeur** pour rédiger les spécifications du déclencheur.

   La figure suivante montre un exemple de configuration qui ne collecte des enregistrements que lorsqu'un code d'état 404 est détecté. Nous avons également défini un nom (`web404`) pour ces types d'enregistrements afin de les identifier dans une requête d'enregistrement et nous avons ajouté des informations d'identification pour le débogage.

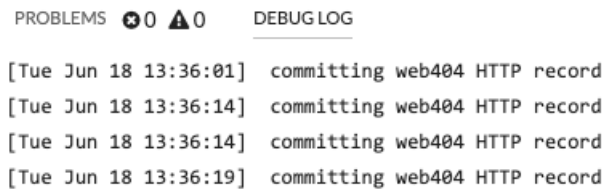
```
1  if (HTTP.statusCode === 404) {
2      commitRecord("web404", HTTP.record);
3      debug("committing web404 HTTP record");
4  }
```

   Dans les étapes suivantes, affectez le déclencheur à un dispositif ou à un groupe de dispositifs pour lequel vous souhaitez surveiller les codes d'état 404.
6. Cliquez sur **Assets** dans le menu supérieur.
7. Cliquez sur **Dispositifs**, puis sur le tableau **Dispositifs actifs**.
8. Cochez la case d'un dispositif dans la liste. Pour notre exemple, nous allons sélectionner un serveur web appelé `web2-sea`.

9. Cliquez sur l'icône Attribuer des déclencheurs, sélectionnez le déclencheur que vous avez créé dans les étapes précédentes, puis cliquez sur **Attribuer des déclencheurs**. Dans la figure suivante, nous avons sélectionné notre serveur web, `web2-sea`.



Après avoir assigné le déclencheur, retournez à l'écran **Paramètres du système > Déclencheur** et sélectionnez le déclencheur que vous avez créé. Tout d'abord, assurez-vous que votre appareil est actif. Ensuite, cliquez sur l'onglet **Debug Log** pour voir si le déclencheur engage vos enregistrements. Dans l'exemple suivant, nous avons intentionnellement visité des pages web indisponibles pour générer des erreurs 404.



Créer un format d'enregistrement personnalisé pour afficher les résultats de vos enregistrements dans un tableau

Les formats d'enregistrement sont le moyen recommandé pour afficher vos enregistrements avec uniquement les champs que vous souhaitez voir. Sans format d'enregistrement personnalisé, les rubriques de votre enregistrement personnalisé n'apparaîtront pas dans les listes sélectionnables, telles que la liste Grouper par.

Le moyen le plus rapide de créer un format d'enregistrement personnalisé consiste à copier et à coller le schéma lu à partir d'un format d'enregistrement intégré dans un nouveau format d'enregistrement. Si vous disposez de plusieurs capteurs, vous devez créer le format d'enregistrement personnalisé sur chaque appareil où les résultats de l'enregistrement sont visualisés. Vous pouvez créer le format d'enregistrement sur une console pour formater un enregistrement personnalisé sur tous les capteurs connectés.

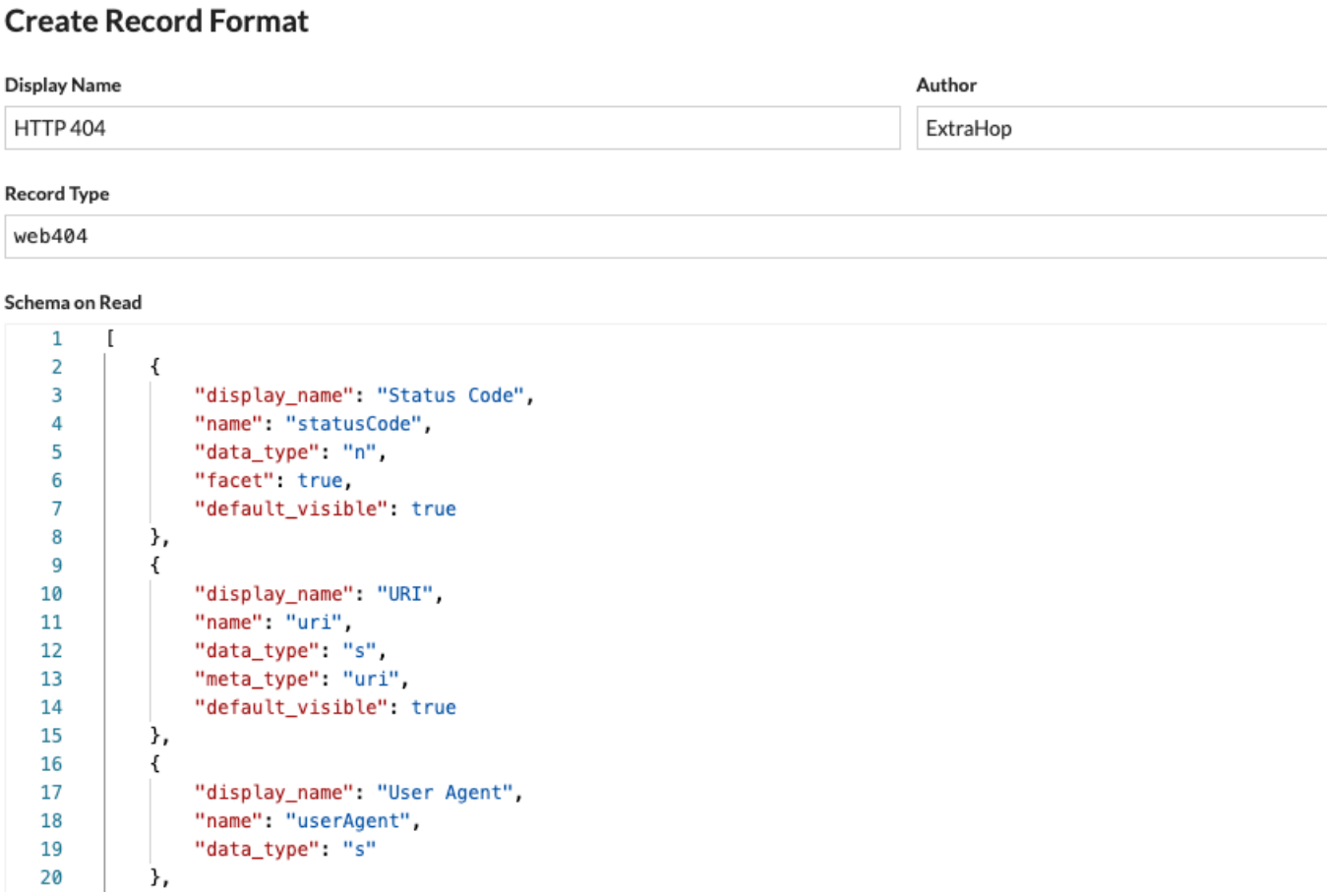
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système, puis sur **Formats d'enregistrement**.
3. Cliquez sur le type d'enregistrement que vous souhaitez copier. Pour notre exemple, nous allons copier le format d'enregistrement HTTP.
4. Copiez le contenu de la zone de texte située sous Schema on Read.
5. Cliquez sur **Nouveau format d'enregistrement**.
6. Complétez les champs suivants :

   • **Nom d'affichage:** Saisissez un nom unique pour votre format d'enregistrement.

• **Auteur:** Identifiez l'auteur du format d'enregistrement.

• **Type d'enregistrement:** Saisissez l'identifiant du type d'enregistrement que vous avez créé dans le déclencheur. Dans notre exemple, cette valeur est `web404`.

• **Schéma en lecture:** Collez le contenu copié de l'étape 4 dans la zone de texte. Modifiez la zone pour supprimer les champs non souhaités. Dans l'exemple de la figure ci-dessous, nous n'avons conservé que les champs suivants : Client, Serveur, Méthode, Code d'état, URI et Temps de traitement.



Recherche d'un type d'enregistrement personnalisé

1. Cliquez sur **Enregistrements** dans le menu supérieur.
2. Cliquez sur la liste déroulante **Tout type d'enregistrement** et sélectionnez le format d'enregistrement que vous venez de créer.
3. Cliquez sur **Afficher les enregistrements**.
4. Cliquez sur l'icône **Affichage détaillé** .
5. Cliquez sur **Champs**, puis sur **Sélectionner tout**.
   Toutes les informations collectées à partir du déclencheur sur ces enregistrements sont affichées dans les résultats de la requête.

Paramètres du format d'enregistrement

La page Paramètres du format d'enregistrement affiche une liste de tous les formats d'enregistrement intégrés et personnalisés disponibles sur vos capteurs ou votre console ExtraHop. Si vous devez créer un format d'enregistrement personnalisé, nous vous recommandons de copier et de coller le schéma sur les

informations lues à partir d'un format d'enregistrement intégré. Les utilisateurs avancés peuvent vouloir créer un format d'enregistrement personnalisé avec leurs propres paires champ-valeur, et doivent appliquer le matériel de référence fourni dans cette section.

Les formats d'enregistrement se composent des paramètres suivants :

Nom d'affichage

Nom affiché pour le format d'enregistrement dans le système ExtraHop. S'il n'y a pas de format d'enregistrement pour la fiche, le type d'enregistrement est affiché.

Auteur

(Facultatif) L'auteur du format d'enregistrement. Tous les formats d'enregistrement intégrés affichent `ExtraHop` comme auteur.

Type d'enregistrement

Un nom alphanumérique unique qui identifie le type d'informations contenues dans le format d'enregistrement associé. Le type d'enregistrement relie le format d'enregistrement aux enregistrements qui sont envoyés au magasin d'enregistrements. Les formats d'enregistrement intégrés ont un type d'enregistrement qui commence par un tilde (~). Les formats d'enregistrement personnalisés ne peuvent pas avoir un type d'enregistrement qui commence par un tilde (~) ou un symbole at (@).

Schéma en lecture

Un tableau au format JSON avec au moins un objet, qui consiste en une paire de noms de champs et de valeurs. Chaque objet décrit un champ de l'enregistrement et chaque objet doit avoir une combinaison unique de nom et de type de données pour ce format d'enregistrement. Vous pouvez créer les objets suivants pour un format d'enregistrement personnalisé :

nom

Le nom du champ.

nom_affichage

Le nom d'affichage du champ. Si le champ `display_name` est vide, le champ `name` est affiché.

description

(Facultatif) Informations descriptives sur le format d'enregistrement. Ce champ est limité à la page Paramètres du format d'enregistrement et n'est pas affiché dans les requêtes d'enregistrement.

default_visible

(Facultatif) S'il a pour valeur `true`, ce champ s'affiche par défaut dans le système ExtraHop en tant qu'en-tête de colonne dans la vue tableau.

facette

(Facultatif) S'il est défini sur `true`, les facettes de ce champ s'affichent dans le système ExtraHop. Les facettes sont une courte liste des valeurs les plus courantes du champ sur lesquelles on peut cliquer pour ajouter un filtre.

data_type

L'abréviation qui identifie le type de données stockées dans ce champ. Les types de données suivants sont pris en charge :

Type de données	Abréviation	Description du type de données
application	`app`	ID de l'application ExtraHop (chaîne)
booléen	`b`	Valeur booléenne
dispositif	`dev`	ID de l'appareil ExtraHop (chaîne)

Type de données	Abréviation	Description du type de données
interface de flux	`fint`	ID de l'interface de flux
réseau de flux	`fnet`	ID du réseau de flux
IPv4	`addr4`	Une adresse IPv4 au format quadratique pointé. Les filtres supérieurs ou inférieurs sont pris en charge.
IPv6	`addr6`	Une adresse IPv6. Seuls les filtres orientés chaîne de caractères sont pris en charge.
nombre	`n`	Nombre (entier ou virgule flottante)
chaîne	`s`	Chaîne générique

meta_type

Sous-classification du type de données qui détermine la manière dont les informations sont affichées dans le système ExtraHop. Les méta-types suivants sont pris en charge pour chacun des types de données associés :

Type de données	Méta type
Chaîne	• `domain` • `uri` • `user`
Nombre	• `bytes` • `count` • `expiration` • `milliseconds` • `packets` • `timestamp`