Collectez des enregistrements personnalisés

Publié: 2024-04-10

Vous pouvez personnaliser le type de détails d'enregistrement que vous générez et stockez dans un espace de stockage des enregistrements en écrivant un déclencheur. Nous vous recommandons également de créer un format dac.enregistrement pour contrôler la façon dont les enregistrements s'affichent dans le système ExtraHop.

Avant de commencer

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

Dans l'exemple suivant, vous allez apprendre à stocker uniquement les enregistrements pour les transactions HTTP qui génèrent un code dstate 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 allons créer un format d'enregistrement pour afficher les champs d' enregistrement sélectionnés dans la vue tabulaire pour les résultats de nos requêtes d'enregistrement.

Écrire et attribuer un déclencheur

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

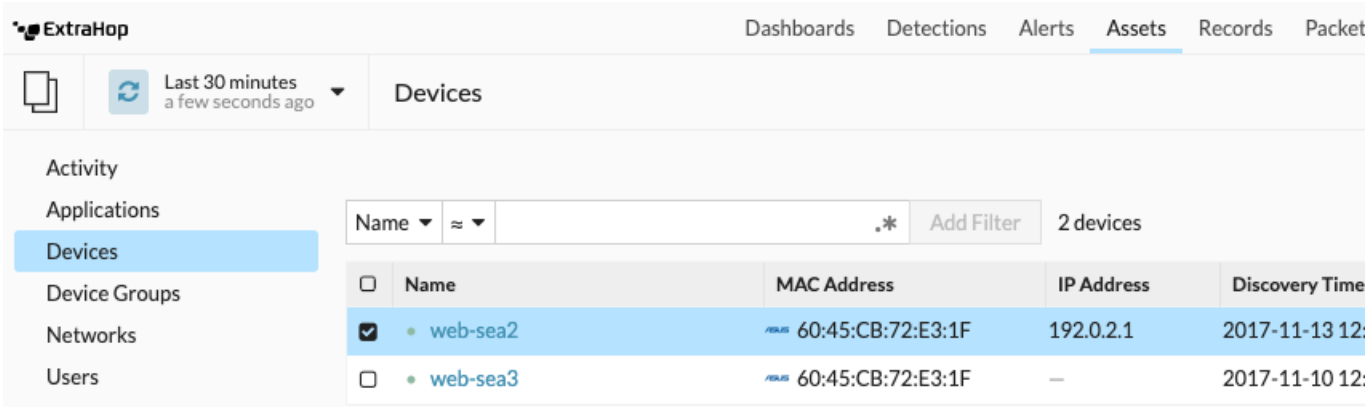
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Dans le Créer un déclencheur volet, complétez vos informations, comme dans l'exemple suivant :
   - **Nom:** `Erreurs HTTP 404`
   - **Descriptif:** `Suivez les erreurs 404 sur le serveur Web principal.`
   - **Activer le journal de débogage:** Cochez la case pour activer le débogage.
   - **Évènements:** `HTTP_RESPONSE`
5. Cliquez sur le **Rédacteur** onglet pour écrire les spécifications du déclencheur.

   La figure suivante montre un exemple de configuration qui collecte des enregistrements uniquement lorsqu'un code ddiligétat 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 d'ajouter des informations d'identification pour le débogage.

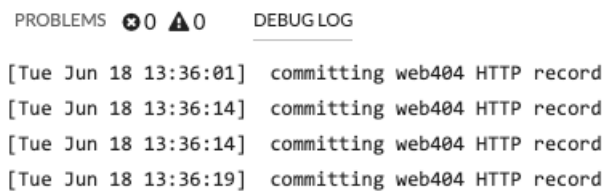
```
1  if (HTTP.statusCode === 404) {
2      commitRecord("web404", HTTP.record);
3      debug("committing web404 HTTP record");
4  }
```

   Dans les étapes suivantes, attribuez le déclencheur à un équipement ou à un groupe d'équipements pour lequel vous souhaitez surveiller les codes d'état 404.
6. Cliquez **Actifs** depuis le menu supérieur.
7. Cliquez **Appareils** puis cliquez sur **Appareils actifs** graphique.

8. Cochez la case correspondant à un équipement 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 lors des étapes précédentes, puis cliquez sur **Assigner des déclencheurs**. Dans la figure suivante, nous avons sélectionné notre serveur Web, `web2-sea`.



Après avoir assigné le déclencheur, revenez au **Paramètres système > Déclencheur** page et sélectionnez le déclencheur que vous avez créé. Tout d'abord, assurez-vous que votre équipement est actif. Cliquez ensuite sur le **Journal de débogage** onglet pour voir si le déclencheur est en train de valider vos enregistrements. Dans l'exemple suivant, nous avons visité intentionnellement des pages Web non disponibles pour générer des erreurs 404.



Créez un format d'enregistrement personnalisé pour afficher les résultats de votre enregistrement dans un tableau

Les formats d'enregistrement sont la méthode recommandée pour afficher vos enregistrements avec uniquement les champs que vous souhaitez voir. Sans format d'enregistrement personnalisé, les champs de votre enregistrement personnalisé n'apparaîtront dans aucune liste sélectionnable, telle que la liste Grouper par.

Le moyen le plus rapide de créer un format d'enregistrement personnalisé consiste à copier-coller le schéma lors de la lecture à partir d'un format d'enregistrement intégré dans un nouveau format d'enregistrement. Si vous avez plusieurs capteurs, vous devez créer le format d'enregistrement personnalisé sur chaque appliance sur laquelle les résultats des enregistrements 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 des paramètres système puis cliquez 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 dans la zone de texte ci-dessous Schéma en cours de lecture.
5. Cliquez **Nouveau format d'enregistrement**.

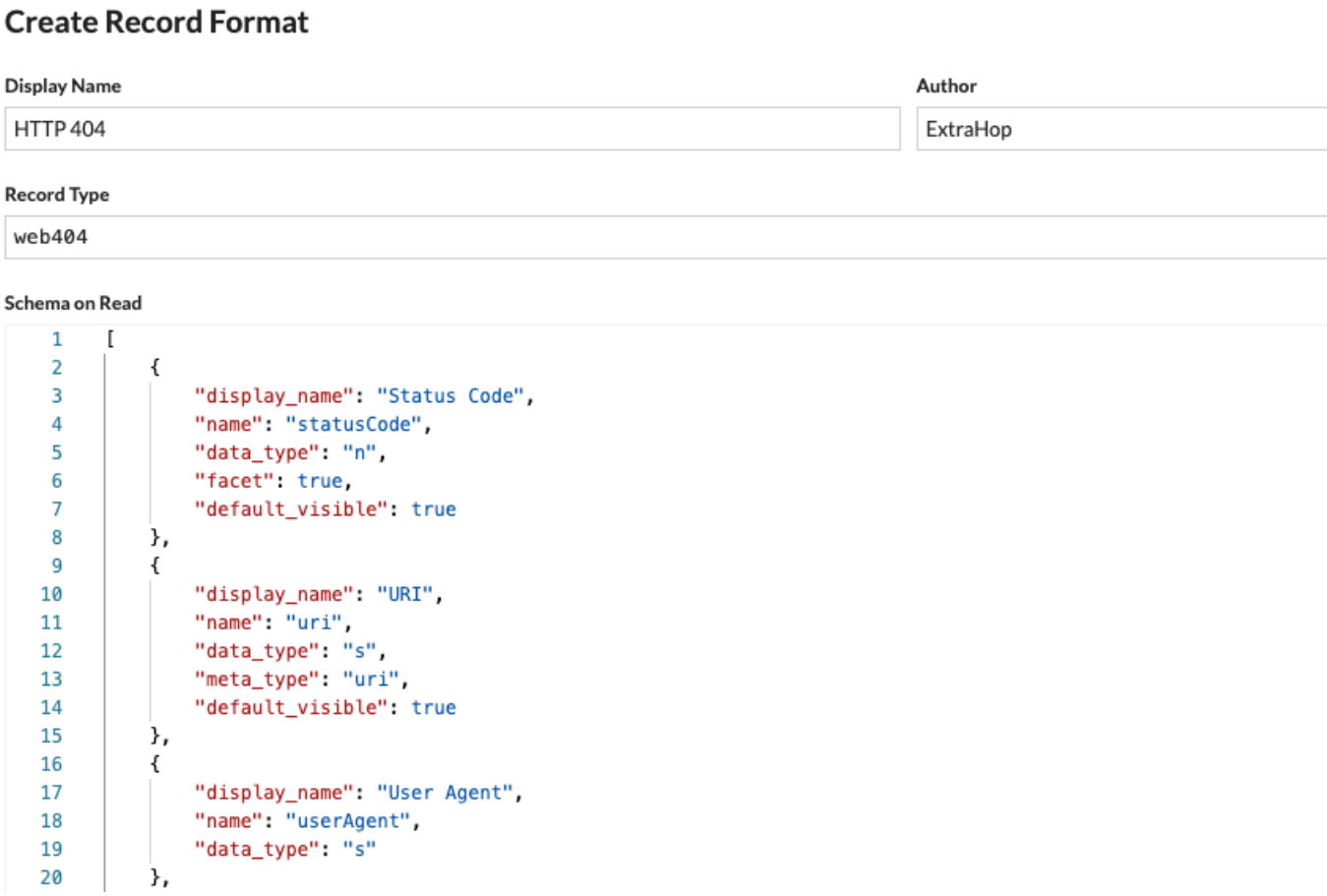
6. Renseignez les champs suivants :

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

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

   • **Type d'enregistrement:** Entrez le même identifiant de type d'enregistrement que celui que vous avez créé dans le déclencheur. Dans notre exemple, cette valeur est `web404`.

   • **Schéma en cours de lecture:** Collez le contenu copié de l'étape 4 dans la zone de texte. Modifiez la case pour supprimer tous les champs indésirables. 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.



Recherchez votre type d'enregistrement personnalisé

1. Cliquez **Enregistrements** depuis le menu supérieur.
2. Cliquez sur **N'importe quel type d'enregistrement** dans une liste déroulante, sélectionnez le format d'enregistrement que vous venez de créer.
3. Cliquez **Afficher les enregistrements**.
4. Cliquez sur **Vue verbeuse** icône.
5. Cliquez **Champs** puis cliquez sur **Tout sélectionner**.
   Toutes les informations collectées par le déclencheur concernant ces enregistrements sont affichées dans les résultats de la requête.

Paramètres du format d'enregistrement

Le Paramètres du format d'enregistrement cette page 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-coller le schéma lors de la lecture des informations à partir d'un format d'enregistrement intégré. Les utilisateurs expérimentés souhaiteront peut-être créer un format d'enregistrement personnalisé avec leurs propres paires champ-valeur et devraient appliquer le matériel de référence fourni dans cette section.

Les formats d'enregistrement comprennent les paramètres suivants :

Nom d'affichage

Le nom affiché pour le format dac.enregistrement dans le système ExtraHop. S'il n'existe aucun format d'enregistrement pour l'enregistrement, le type d'enregistrement est affiché.

Auteur

(Facultatif) Auteur du format dac.enregistrement. Tous les formats d'enregistrement intégrés s'affichent `ExtraHop` en tant qu'auteur.

Type d'enregistrement

Nom alphanumérique unique qui identifie le type d'information contenu dans le format dac.enregistrement associé. Le type d'enregistrement lie le format d'enregistrement aux enregistrements envoyés à l'espace de stockage des 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 commençant par un tilde (~) ou un symbole arobase (@).

Schéma en cours de lecture

Tableau au format JSON contenant au moins un objet, constitué d'une paire nom de champ et valeur. 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

Nom d'affichage du champ. Si le `display_name` le champ est vide, le `name` le champ s'affiche.

description

(Facultatif) Informations descriptives sur le format dac.enregistrement. Ce champ est limité à la page Paramètres du format d'enregistrement et n'apparaît dans aucune requête d'enregistrement.

visible par défaut

(Facultatif) Si défini sur `true`, ce champ s'affiche dans le système ExtraHop sous forme d'en-tête de colonne par défaut dans l'affichage sous forme de tableau.

facette

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

type_données

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

Type de données	Abréviation	Descriptif
application	`app`	ID de l'application ExtraHop (chaîne)
booléen	`b`	Valeur booléenne
équipement	`dev`	ID de l'équipement ExtraHop (chaîne)
interface de flux	`fint`	ID de l'interface Flow
réseau de flux	`fnet`	ID du réseau Flow
IPv4	`addr4`	Adresse IPv4 au format quadrilatère. Plus ou moins que les filtres pris en charge.
IPv6	`addr6`	Une adresse IPv6. Seuls les filtres orientés chaîne sont pris en charge.
nombre	`n`	Nombre (entier ou virgule flottante)
chaîne	`s`	Chaîne générique

méta-type

Sous-classification du type de données qui détermine en outre 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
Corde	• `domain` • `uri` • `user`
Numéro	• `bytes` • `count` • `expiration` • `milliseconds` • `packets` • `timestamp`