Créez un déclencheur

Publié: 2023-12-05

Les déclencheurs fournissent des fonctionnalités étendues à votre système ExtraHop. Les déclencheurs vous permettent de créer des métriques personnalisées, de générer et de stocker des enregistrements ou d'envoyer des données à un système tiers. Comme vous écrivez le script de déclenchement, vous contrôlez les actions entreprises par le déclencheur lors d'événements système spécifiés.

Pour créer un déclencheur, vous devez créer une configuration de déclencheur, écrire le script du déclencheur, puis affecter le déclencheur à une ou plusieurs sources métriques. Le déclencheur ne s'exécute pas tant que toutes les actions ne sont pas terminées.

Avant de commencer
Connectez-vous au système ExtraHop avec un compte utilisateur disposant de l'écriture complète privilèges nécessaire pour créer des déclencheurs.

Si vous êtes novice en matière de déclencheurs, familiarisez-vous avec le processus de planification du déclencheur, ce qui vous aidera à affiner le champ de votre déclencheur ou à déterminer s'il est vraiment nécessaire de créer un déclencheur. Ensuite, suivez le processus de création d'un déclencheur en complétant le Procédure pas à pas des déclencheurs.

Configurer les paramètres du déclencheur

La première étape pour créer un déclencheur consiste à fournir un nom de déclencheur, à déterminer si le débogage est activé et, surtout, à identifier les événements système sur lesquels le déclencheur sera exécuté .

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. Spécifiez les paramètres de configuration du déclencheur suivants :

Nom

Nom du déclencheur.

Auteur

Nom de l'utilisateur qui a écrit le déclencheur. Les déclencheurs par défaut affichent ExtraHop.

Descriptif

Description facultative du déclencheur.

Missions

Les appareils ou groupes d'équipements auxquels le déclencheur est attribué. Un déclencheur ne s'exécute pas tant qu'il n'est pas attribué à un équipement, et le déclencheur collecte des données métriques uniquement auprès des appareils auxquels il est attribué.

Avertissement: L'exécution de déclencheurs sur des appareils et des réseaux inutiles épuise les ressources du système. Minimisez l'impact sur les performances en affectant un déclencheur uniquement aux sources spécifiques auprès desquelles vous devez collecter des données.

Important: Les déclencheurs comportant les événements suivants s'exécutent chaque fois que l'événement se produit. Les déclencheurs qui s'exécutent uniquement lors de ces événements ne peuvent pas être attribués à des appareils ou à des groupes d'équipements.

- ALERT_RECORD_COMMIT
- MISE À JOUR DE DÉTECTION

- METRIC_CYCLE_BEGIN
- METRIC_CYCLE_END
- METRIC_RECORD_COMMIT
- NOUVELLE_APPLICATION
- NOUVEL_APPAREIL
- EXPIRATION DE SESSION
- MINUTER_30 SECONDES

Activer le journal de débogage

Case à cocher qui active ou désactive le débogage. Si vous ajoutez des instructions de débogage au script du déclencheur, cette option vous permet de afficher la sortie de débogage dans le journal de débogage lorsque le déclencheur est en cours d'exécution.

Évènements

Les événements sur lesquels le déclencheur s'exécute. Le déclencheur s'exécute chaque fois que l' un des événements spécifiés se produit sur un équipement assigné ; vous devez donc attribuer au moins un événement à votre déclencheur. Vous pouvez cliquer dans le champ ou commencer à saisir le nom d'un événement pour afficher une liste filtrée des événements disponibles.

Options avancées

Options de déclencheur avancées varient en fonction des événements sélectionnés. Par exemple, si vous sélectionnez `HTTP_RESPONSE` événement, vous pouvez définir le nombre d'octets de charge utile à mettre en mémoire tampon sur ces événements.

Écrire un script de déclencheur

Le script de déclenchement spécifie les instructions que le déclencheur exécutera lorsqu' un événement système configuré pour le déclencheur se produit.

Avant de commencer

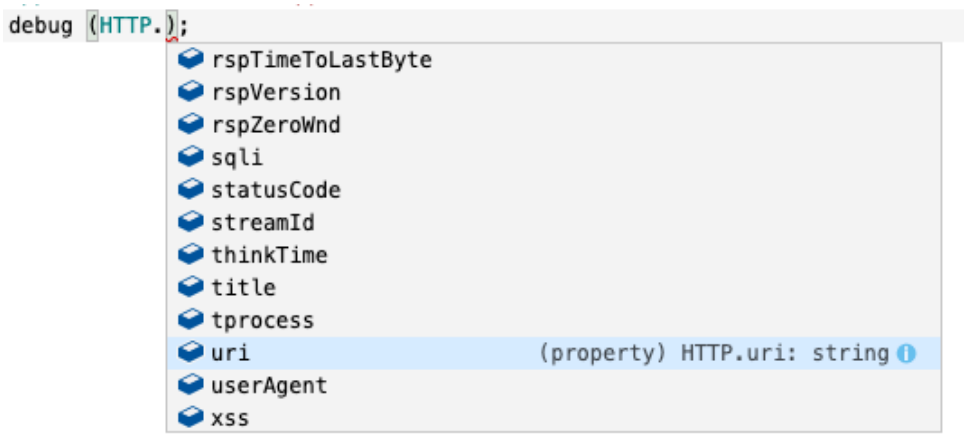
Nous vous recommandons d'ouvrir Référence de l'API ExtraHop Trigger , qui contient les événements, les méthodes et les propriétés dont vous avez besoin pour votre déclencheur. Un lien est également disponible depuis la fenêtre de l'éditeur du déclencheur du système ExtraHop.

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 volet droit, tapez le script du déclencheur dans une syntaxe de type JavaScript avec les événements, les méthodes et les propriétés du Référence de l'API ExtraHop Trigger .

   La figure suivante montre un exemple de script saisi dans l'onglet Editeur :

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

L'éditeur fournit une fonction de saisie semi-automatique qui affiche une liste de propriétés et de méthodes en fonction de l' objet de classe sélectionné. Par exemple, tapez le nom d'une classe, puis tapez un point (.) pour afficher la liste des propriétés et méthodes disponibles, comme illustré dans la figure suivante :

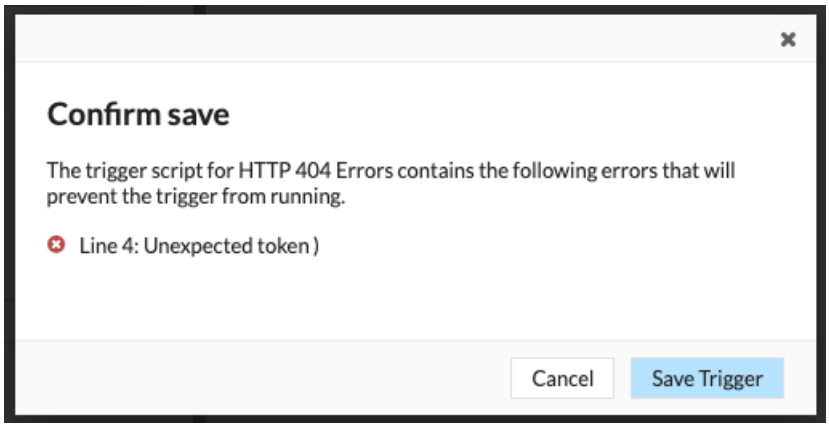


5. Cliquez **Enregistrer**.

   L'éditeur permet de valider la syntaxe de votre script. Lorsque vous enregistrez le déclencheur, le validateur signale les actions non valides, les erreurs de syntaxe ou les éléments obsolètes du script. S'il est disponible, le validateur affiche les remplacements des éléments obsolètes.

   Avertissement Pour éviter de mauvaises performances du déclencheur, des résultats incorrects ou un dysfonctionnement du déclencheur , nous vous recommandons vivement de corriger le code ou de remplacer l'élément obsolète.

   La figure suivante montre un exemple de message d'erreur généré par le validateur de syntaxe :



Options de déclencheur avancées

Vous devez configurer les déclencheurs pour qu'ils s'exécutent sur au moins un événement. En fonction de l' événement sélectionné, le volet Create Trigger affiche des options de configuration avancées. Par exemple, en sélectionnant le HTTP_RESPONSE cet événement vous permet de définir le nombre d'octets de charge utile à mettre en mémoire tampon chaque fois qu'un événement se produit sur le système.

Le tableau suivant décrit les options avancées disponibles et les événements qui prennent en charge chaque option.

Option	Descriptif	Événements soutenus
Nombre d'octets par paquet à capturer	Spécifie le nombre d'octets à capturer par paquet. La capture commence par le premier octet du paquet. Spécifiez cette option uniquement si le script déclencheur effectue une capture de paquets. Une valeur de 0 spécifie que la capture doit collecter tous les octets de chaque paquet.	Tous les événements sont pris en charge à l'exception de la liste suivante : • `ALERT_RECORD_COMMIT` • `METRIC_CYCLE_BEGIN` • `METRIC_CYCLE_END` • `FLOW_REPORT` • `NEW_APPLICATION` • `NEW_DEVICE` • `SESSION_EXPIRE`
Octets de charge utile L7 à mettre en mémoire tampon	Spécifie le nombre maximum d'octets de charge utile à mettre en mémoire tampon. **Note:** Si plusieurs déclencheurs s'exécutent sur le même événement, le déclencheu... avec la valeur L7 d'octets charge utile par rapport à la mémoire tampon la plus élevée détermine la valeu... maximale charge utile pou... cet événement pour chaq... déclencheur.	• `CIFS_REQUEST` • `CIFS_RESPONSE` • `HTTP_REQUEST` • `HTTP_RESPONSE` • `ICA_TICK` • `LDAP_RESPONSE`
Clipboard Bytes	Spécifie le nombre d'octets à mettre en mémoire tampon dans un presse-papiers Citrix transfert.	• `ICA_TICK`
Cycle métrique	Spécifie la durée du cycle métrique, exprimée en secondes. Les valeurs suivantes sont valides : • `30sec` • `5min` • `1hr` • `24hr`	• `METRIC_CYCLE_BEGIN` • `METRIC_CYCLE_END` • `METRIC_RECORD_COMMIT`
Types de métriques	Spécifie le type de métrique par le nom brut de la métrique, tel que `extrahop.device.http_server`. Spécifiez plusieurs types de	• `ALERT_RECORD_COMMIT` • `METRIC_RECORD_COMMIT`

Option	Descriptif	Événements soutenus
	métriques dans une liste délimitée par des virgules.	
Exécutez le déclencheur à chaque tour de flux	Permet la capture de paquets sur chaque flux tourner. L'analyse par tour analyse en permanence la communication entre deux terminaux pour extraire un seul point de données de charge utile à partir du flux. Si cette option est activée, toutes les valeurs spécifié pour **Chaîne correspondante au client** et **Chaîne correspondante au serveur** les options sont ignoré.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Gamme de ports client	Spécifie la plage de ports client. Les valeurs valides sont comprises entre 0 et 65535.	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`
Nombre d'octets client à mettre en mémoire tampon	Spécifie le nombre d'octets client à mettre en mémoire tampon. La valeur de cette option ne peut pas être définie sur 0 si la valeur de **Octets du serveur à mettre en mémoire tampon** l'option est également défini sur 0.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Chaîne de recherche dans la mémoire tampon du client	Spécifie la chaîne de format qui indique quand commencer mise en mémoire tampon des données des clients. Renvoie le paquet entier sur une chaîne match. Vous pouvez spécifier la chaîne sous forme de texte ou de nombres hexadécimaux. Par exemple, les deux `ExtraHop` et `\x45\x78\x74\x72\x61\x48\x6F\x70` sont équivalent. Les nombres hexadécimaux ne sont pas majuscules sensible. Toute valeur spécifiée pour cette option est ignorée si le **Par tour** ou **Exécuter le déclencheur sur**	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`

Option	Descriptif	Événements soutenus
	tous les UDP l'option packets est activé.	
Plage de ports du serveur	Spécifie la plage de ports du serveur. Les valeurs valides sont comprises entre 0 et 65535.	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`
Octets du serveur à mettre en mémoire tampon	Spécifie le nombre d'octets du serveur à mettre en mémoire tampon. La valeur de cette option ne peut pas être définie sur 0 si la valeur de **Nombre d'octets client à mettre en mémoire tampon** l'option est également défini sur 0.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Chaîne de recherche de la mémoire tampon du serveur	Spécifie la chaîne de format qui indique quand commencer mise en mémoire tampon des données du serveur. Vous pouvez spécifier la chaîne sous forme de texte ou nombres hexadécimaux. Par exemple, les deux `ExtraHop` et `\x45\x78\x74\x72\x61\x48\x6F \x70` sont équivalent. Les nombres hexadécimaux ne sont pas majuscules sensible. Toute valeur spécifiée pour cette option est ignorée si le **Par tour** ou **Exécuter le déclencheur sur tous les UDP** l'option est activée.	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`
Exécuter le déclencheur sur tous les paquets UDP	Permet la capture de tous les datagrammes UDP.	• `UDP_PAYLOAD`
Exécutez FLOW_CLASSIFY sur des flux non classifiés arrivant à expiration	Permet d'exécuter l'événement à son expiration pour accumuler des métriques pour flux qui n'étaient pas classifiés auparavant expirant.	• `FLOW_CLASSIFY`
Types externes	Spécifie les types de données externes que le déclencheur traite. Le le déclencheur ne s'exécute que si la charge utile contient un champ de type avec l'un des les valeurs spécifiées. Spécifiez plusieurs types séparés par des virgules liste.	1. `EXTERNAL_DATA`