

déclencheurs

Publié: 2024-04-10

Les déclencheurs sont composés d'un code défini par l'utilisateur qui s'exécute automatiquement en fonction des événements du système via l'API ExtraHop Trigger. Vous pouvez écrire un déclencheur, qui est un bloc de code JavaScript, via l'API de déclenchement pour extraire, stocker et visualiser des événements et des métriques Wire Data personnalisés spécifiques à votre entreprise, à votre infrastructure, à votre réseau, à vos clients et à vos applications professionnelles.

Parmi les flux de travail les plus courants que vous pouvez exécuter via des déclencheurs, citons les opérations suivantes :

- Créez un [application](#) conteneur dans lequel les métriques sont collectées pour des appareils spécifiques. Les conteneurs d'applications augmentent les vues basées sur les appareils que le système ExtraHop construit par défaut.
- Créez [métriques personnalisées](#) et enregistrez-les dans la banque de données ExtraHop. Par exemple, les données d'agent utilisateur générées par un HTTP La requête n'est pas une métrique intégrée au système ExtraHop. Cependant, l'API ExtraHop Trigger fournit une propriété HTTP d'agent utilisateur, qui vous permet d'écrire un déclencheur qui collecte les données de l'agent utilisateur sous forme de métrique personnalisée.
- Générer [disques](#) et écrivez-les dans une banque de données pour les stocker et les récupérer à long terme.
- Envoyez des données à des utilisateurs de Syslog, tels que Splunk, ou à des bases de données tierces, telles que MongoDB ou Kafka, par le biais d'un [flux de données ouvert](#).
- Effectuez une analyse de charge utile universelle (UPA) pour accéder aux charges utiles TCP et UDP et les analyser à partir de données non prises en charge protocoles.
- Lancez des captures de paquets pour enregistrer des flux individuels en fonction de critères spécifiés par l'utilisateur. Votre système ExtraHop doit disposer d'une licence pour la capture de paquets pour accéder à cette fonctionnalité.

Pour afficher tous les déclencheurs, cliquez sur **Réglages du système** icône  puis cliquez sur **déclencheurs**. Sur la page Déclencheurs, vous pouvez [créer un déclencheur](#) ou cochez la case à côté d'un déclencheur pour [modifier la configuration du déclencheur](#) ou [modifier le script du déclencheur](#).

Planifiez un déclencheur

L'écriture d'un déclencheur pour collecter des métriques personnalisées est un moyen puissant de surveiller les performances de votre application et de votre réseau. Cependant, les déclencheurs consomment les ressources du système et peuvent affecter les performances du système, et un déclencheur mal écrit peut entraîner une charge inutile du système. Avant de créer un déclencheur, évaluez ce que vous souhaitez que celui-ci accomplisse, identifiez les événements et les appareils nécessaires pour extraire les données dont vous avez besoin et déterminez s'il existe déjà une solution.

- Identifiez les informations spécifiques que vous devez collecter en posant les types de questions suivants :
 - Quand est-ce que mes certificats SSL expireront ?
 - Mon réseau est-il connecté à des ports non autorisés ?
 - Combien de transactions lentes sont enregistrées sur mon réseau ?
 - Quelles sont les données que je souhaite envoyer à Splunk via un flux de données ouvert ?
- Passez en revue le Catalogue métrique pour déterminer s'il existe déjà une métrique intégrée qui extrait les données dont vous avez besoin. Les métriques intégrées ne créent pas de charge supplémentaire sur le système.
- Identifiez quel système événements produisez les données que vous souhaitez collecter. Par exemple, un déclencheur qui surveille l'activité des applications cloud dans votre environnement peut s'exécuter

sur les réponses HTTP ainsi que sur l'ouverture et la fermeture de connexions SSL. Pour obtenir la liste complète des événements du système, consultez [Référence de l'API ExtraHop Trigger](#) .

- Familiarisez-vous avec les méthodes et les propriétés de l'API disponibles dans [Référence de l'API ExtraHop Trigger](#) . Par exemple, avant d' aller trop loin dans la planification de votre déclencheur, vérifiez la référence pour vous assurer que la propriété que vous souhaitez extraire est disponible ou pour savoir quelles propriétés sont collectées dans un enregistrement CIFS par défaut.
- Déterminez comment vous souhaitez visualiser ou stocker les données collectées par le déclencheur. Par exemple, vous pouvez consulter les statistiques sur un tableau de bord ou par protocole, vous pouvez envoyer des enregistrements vers l'espace de stockage des enregistrements.
- Déterminez s'il existe déjà un déclencheur qui répond à vos besoins ou qui peut être facilement modifié ; commencez toujours par un déclencheur préexistant dans la mesure du possible. Recherchez un déclencheur existant dans les ressources suivantes :
 - [Déclencheurs existants sur la page Déclencheurs](#)
 - [Les forums de la communauté ExtraHop](#)

Bâtir des déclencheurs

Si vous déterminez que vous devez créer un nouveau déclencheur, familiarisez-vous avec les tâches suivantes qui doivent être effectuées :

- [Configuration du déclencheur](#) pour fournir des détails tels que le nom du déclencheur et si le débogage est activé. Plus important encore, spécifiez les événements système sur lesquels le déclencheur sera exécuté. Par exemple, si vous souhaitez que votre déclencheur s'exécute chaque fois qu'une connexion SSH est ouverte, vous devez spécifier `SSH_OPEN` comme événement déclencheur.
- [Rédigez le script du déclencheur](#), qui spécifie les instructions que le déclencheur exécutera lorsqu'un événement système configuré pour le déclencheur se produit. Le script déclencheur peut fournir des instructions pour une tâche simple, telle que la création d'une métrique personnalisée du nombre d'équipements appelée « `slow_rsp` », ou pour une tâche plus complexe telle que la surveillance et la collecte de statistiques sur les applications cloud accessibles dans votre environnement.

Une fois le déclencheur terminé et en cours d'exécution, il est important de vérifier qu'il fonctionne comme prévu.

- [Afficher le journal de débogage](#) pour le résultat attendu des instructions de débogage dans le script du déclencheur. Le journal affiche également les erreurs d'exécution et les exceptions que vous devez corriger.
- [Surveillez le coût des performances](#) en suivant le nombre de cycles consommés par le déclencheur.
- [Vérifiez les tableaux de santé du système](#) pour les exceptions relatives aux déclencheurs, les suppressions de la file d'attente des déclencheurs et les activités inattendues.
- Vérifiez que le script du déclencheur est conforme au [Guide des meilleures pratiques en matière de déclencheurs](#) .

Parcourir les déclencheurs

La page Déclencheurs contient une liste des déclencheurs actuels avec les informations suivantes :

Nom

Le nom du déclencheur défini par l'utilisateur.

Auteur

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

Description

Description du déclencheur définie par l'utilisateur.

Missions

Les appareils ou groupes d'équipements auxquels le déclencheur est attribué.

État

Si le déclencheur est activé. Si le déclencheur est activé, le nombre d'assignments d' équipement s'affiche également.

Journal de débogage

Si le débogage est activé. Si le débogage est activé, les résultats des instructions de débogage du script déclencheur sont enregistrés dans [sortie du journal de débogage](#).

Évènements

Les événements système à l'origine de l'exécution du déclencheur, tels que HTTP_RESPONSE.

Modifié

La dernière fois que le déclencheur a été modifié.

Triggers

<input type="checkbox"/>	Name ↑	Author	Description	Assignments	Status	Debug Log	Events	Modified
<input type="checkbox"/>	Active Direct...	ExtraHop	Custom metrics for Active Direct...	0	■ ENABLED	■ DISABLED	CIFS_RESPONSE, ...	2017-11-2
<input type="checkbox"/>	AD: DNS Ser...	ExtraHop	DNS service (SRV) resource reco...	0	■ DISABLED	■ DISABLED	DNS_REQUEST, D...	2018-08-2
<input type="checkbox"/>	AD: Group Po...	ExtraHop	Group Policy custom metrics for ...	0	■ DISABLED	■ DISABLED	CIFS_RESPONSE	2018-08-2