Déclencheurs

Publié: 2023-09-19

Les déclencheurs sont composés d'un code défini par l'utilisateur qui s'exécute automatiquement sur les événements du système par le biais de l'API de déclenchement d'ExtraHop. Vous pouvez écrire un déclencheur, qui est un bloc de JavaScript, par le biais de l'API de déclenchement pour extraire, stocker et visualiser des événements et des mesures de données filaires personnalisés qui sont spécifiques à votre entreprise, votre infrastructure, votre réseau, vos clients et vos applications d'entreprise.

Parmi les flux de travail les plus courants que vous pouvez effectuer à l'aide des déclencheurs, citons les opérations suivantes :

- Créer un conteneur d'application dans lequel les mesures sont collectées pour des périphériques spécifiques. Les conteneurs d'application complètent les vues basées sur les périphériques que le système ExtraHop construit par défaut.
- Créer des mesures personnalisées et les enregistrer dans le magasin de données ExtraHop. Par exemple, les données de l'agent utilisateur générées par une requête HTTP ne sont pas des mesures intégrées au système ExtraHop. Cependant, l'API ExtraHop Trigger fournit une propriété HTTP user agent, qui vous permet d'écrire un trigger qui collecte les données de l'agent utilisateur en tant que métrique personnalisée.
- Générer des enregistrements et les écrire dans un magasin de données pour un stockage et une récupération à long terme.
- Envoyer des données à des consommateurs syslog, tels que Splunk, ou à des bases de données tierces, telles que MongoDB ou Kafka, par l'intermédiaire d'un flux de données ouvert.
- Effectuer une analyse universelle des charges utiles (UPA) pour accéder aux charges utiles TCP et UDP des protocoles non pris en charge et les analyser.
- Initier des captures de paquets pour enregistrer des flux individuels sur la base de critères spécifiés par l'utilisateur. Votre système ExtraHop doit être autorisé à capturer des paquets pour accéder à cette fonctionnalité.

Pour afficher tous les déclencheurs, cliquez sur l'icône **Paramètres système**, puis sur **Déclencheurs**. Sur la page Déclencheurs, vous pouvez créer un déclencheur ou cocher la case en regard d'un déclencheur pour éditer la configuration du déclencheur ou modifier le script du déclencheur.

Planifier un déclencheur

L'écriture d'un déclencheur pour collecter des mesures personnalisées est un moyen puissant de surveiller les performances de votre application et de votre réseau. Cependant, les déclencheurs consomment des ressources système et peuvent affecter les performances du système, et un déclencheur mal écrit peut entraîner une charge système inutile. Avant de créer un déclencheur, évaluez ce que vous voulez qu'il accomplisse, identifiez les événements et les périphériques 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 questions suivantes :
  - Quand mes certificats SSL expireront-ils ?
  - Mon réseau reçoit-il des connexions sur des ports non autorisés ?
  - Combien de transactions lentes mon réseau connaît-il ?
  - Quelles sont les données que je souhaite envoyer à Splunk par le biais d'un flux de données ouvert ?
- Consultez le catalogue de métriques 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 les événements du système qui produisent les données que vous souhaitez collecter. Par exemple, un déclencheur qui surveille l'activité des applications en nuage dans votre environnement peut être exécuté sur les réponses HTTP et sur l'ouverture et la fermeture des connexions SSL. Pour

obtenir une liste complète des événements système, consultez le site Référence API ExtraHop Trigger .

- Familiarisez-vous avec les méthodes et les propriétés de l'API disponibles sur le site Référence 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 afficher les métriques sur un tableau de bord ou, par protocole, envoyer des enregistrements au magasin d'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
  - Forums de la communauté ExtraHop

Création de déclencheurs

Si vous décidez de créer un nouveau déclencheur, familiarisez-vous avec les tâches suivantes :

- Configurer le déclencheur pour fournir des détails tels que le nom du déclencheur et l'activation du débogage. Plus important encore, spécifiez les événements système sur lesquels le déclencheur s'exécutera. 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 produira. Le script de déclenchement peut fournir des instructions pour une tâche simple telle que la création d'une mesure personnalisée du nombre de périphériques appelée "slow_rsp" ou pour une tâche plus complexe telle que la surveillance et la collecte de statistiques sur les applications en nuage auxquelles votre environnement accède.

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

- Consultez le journal de débogage pour connaître les résultats attendus 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 diagrammes de santé du système pour les exceptions de déclenchement, les abandons de la file d'attente de déclenchement et les activités inattendues.
- Vérifiez que le script du déclencheur est conforme au site Guide des meilleures pratiques pour les déclencheurs.

Naviguer dans les déclencheurs

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

Nom
Nom défini par l'utilisateur du déclencheur.

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

Description
La description du déclencheur définie par l'utilisateur.

Affectations
Les appareils ou groupes d'appareils auxquels le déclencheur est affecté.

État

Indique si le déclencheur est activé. Si le déclencheur est activé, le nombre d'affectations de périphériques s'affiche également.

Journal de débogage

Si le débogage est activé. Si le débogage est activé, la sortie des instructions de débogage du script de déclenchement est consignée dans le journal de débogage.

Événements

Les événements système qui provoquent l'exécution du déclencheur, tels que `HTTP_RESPONSE`.

Modifié

La dernière fois que le déclencheur a été modifié.