éléments déclencheurs

Publié: 2024-09-26

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

Parmi les flux de travail les plus courants que vous pouvez exécuter à l'aide de 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 des agents utilisateurs générées par un HTTP request 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.
- Générez disques et écrivez-les dans une banque de données pour un stockage et une extraction à long terme.
- Envoyez des données à des utilisateurs 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 universelle de la charge utile (UPA) pour accéder aux charges utiles TCP et UDP non prises en charge et les analyser 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 **Paramètres du système** icône puis cliquez sur **éléments déclencheurs**. À partir de 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.

Planifier un déclencheur

La création 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 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 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 TLS expireront ?
  - Mon réseau est-il connecté à des ports non autorisés ?
  - Combien de transactions sont lentes sur mon réseau ?
  - Quelles données dois-je 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.
- Identifier 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 et lors de l'ouverture et de la fermeture de connexions TLS. Pour obtenir la liste complète des événements du système, consultez le Référence de l'API ExtraHop Trigger.

- Familiarisez-vous avec les méthodes et 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 SMB par défaut.
- Déterminez comment vous souhaitez visualiser ou stocker les données collectées par le déclencheur. Par exemple, vous pouvez consulter les statistiques d'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 pourrait 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

Créer des déclencheurs

Si vous déterminez que vous devez créer un nouveau déclencheur, familiarisez-vous avec les tâches suivantes à effectuer :

- Configurer le déclencheur pour fournir des informations telles que le nom du déclencheur et indiquer si le débogage est activé. 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.
- Écrivez 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 du script de déclencheur. Le journal affiche également toutes 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.
- Consultez les graphiques de santé du système pour les exceptions liées aux déclencheurs, les sorties de la file d'attente des déclencheurs et les activités inattendues.
- Vérifiez que le script du déclencheur est conforme à Guide des meilleures pratiques relatives aux déclencheurs.

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

Descriptif
Description du déclencheur définie par l'utilisateur.

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

État

Si le déclencheur est activé. Si le déclencheur est activé, le nombre d'attributions d' équipements s'affiche également.

Journal de débogage

Indique si le débogage est activé. Si le débogage est activé, les résultats des instructions de débogage du script de déclencheur sont enregistrés dans le sortie du journal de débogage.

Évènements

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

Modifié

La dernière fois que le déclencheur a été modifié.