Configurer une cible Kafka pour un flux de données ouvert

Publié: 2024-11-04

Vous pouvez exporter les données d'un système ExtraHop vers n'importe quel serveur Kafka pour un archivage à long terme et une comparaison avec d'autres sources.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

   Répétez ces étapes pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible liste déroulante, sélectionnez **Kafka**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. À partir du Compression dans la liste déroulante, sélectionnez l'une des méthodes de compression suivantes qui sera appliquée aux données transmises :
   - **Aucune**
   - **GZIP**
   - **Snappy**
7. À partir du Stratégie de partition dans la liste déroulante, sélectionnez l'une des méthodes de partitionnement suivantes qui sera appliquée aux données transmises :
   - **Par défaut (clé de hachage)**
   - **Manuel**
   - **Aléatoire**
   - **Tournoi à la ronde**
8. Optionnel : Configurez l'authentification SASL/SCRAM.
   a) À partir du Authentification liste déroulante, sélectionnez **SASL/SCRAM**.
   b) Dans le Nom d'utilisateur dans ce champ, saisissez le nom de l'utilisateur SASL/SCRAM.
   c) Dans le Mot de passe dans ce champ, saisissez le mot de passe de l'utilisateur SASL/SCRAM.
   d) À partir du **Algorithme de hachage** dans la liste déroulante, sélectionnez l'algorithme de hachage pour l'authentification SASL.
9. À partir du **Protocole** dans la liste déroulante, sélectionnez l'un des protocoles suivants pour transmettre les données :
   - **TCP**
   - **TLS**
10. Optionnel : Si vous avez sélectionné **TLS** protocole, spécifiez les options de certificat.
    a) Si le serveur Kafka nécessite l'authentification du client, dans **Certificat client** champ, spécifiez un certificat client TLS à envoyer au serveur.
    b) Si vous avez spécifié un certificat client, dans **Clé client** champ, spécifiez la clé privée du certificat.
    c) Si vous ne souhaitez pas vérifier le certificat du serveur Kafka, sélectionnez **Ignorer la vérification des certificats de serveur**.
    d) Si vous souhaitez vérifier le certificat du serveur Kafka, mais que celui-ci n'a pas été signé par une autorité de certification (CA) valide, dans **Certificats CA (en option)** champ, spécifiez les certificats sécurisés, au format PEM, à l'aide desquels vérifier le certificat du serveur. Si cette option n'est pas spécifiée, le certificat de serveur est validé à l'aide de la liste intégrée des certificats CA valides.
11. Spécifiez au moins un courtier Kafka, également appelé nœud dans un cluster Kafka, qui peut recevoir les données transmises.

Note: Vous pouvez ajouter plusieurs courtiers faisant partie du même cluster Kafka pour garantir la connectivité au cas où un seul courtier ne serait pas disponible. Tous les courtiers doivent faire partie du même cluster.

a) Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du courtier Kafka.
b) Dans le Port dans ce champ, saisissez le numéro de port du courtier Kafka.
c) Cliquez sur le signe plus (**+**) icône.

12. Optionnel : Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur Kafka distant et envoyer un message de test au serveur.
La boîte de dialogue affiche un message qui indique si la connexion a réussi ou échoué.

Conseil: Si le test échoue, consultez les journaux de votre serveur Kafka pour obtenir des informations plus détaillées sur l'erreur, puis modifiez la configuration cible et testez à nouveau la connexion.

13. Cliquez **Enregistrer**.

Prochaines étapes

Créez un déclencheur qui spécifie les données de message Kafka à envoyer et initie la transmission des données à la cible. Pour plus d'informations, consultez Remote.Kafka classe dans le Référence de l'API ExtraHop Trigger .