Envoi d'enregistrements d'ExtraHop à Splunk

Publié: 2023-09-19

Vous pouvez configurer le système ExtraHop pour qu'il envoie des enregistrements de niveau transactionnel à un serveur Splunk pour un stockage à long terme, puis interroger ces enregistrements à partir du système ExtraHop et de l'API REST ExtraHop.

Avant de commencer

- Vous devez disposer de la version 7.0.3 ou ultérieure de Splunk Enterprise et d'un compte utilisateur disposant de privilèges d'administrateur.
- Vous devez configurer le collecteur d'événements HTTP Splunk avant que votre serveur Splunk ne puisse recevoir les enregistrements ExtraHop. Consultez la documentation de Splunk HTTP Event Collector pour obtenir des instructions.

Note: Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` à un magasin d'enregistrements sont automatiquement redirigés vers le serveur Splunk. Aucune autre configuration n'est nécessaire.

Envoyer des enregistrements d'ExtraHop à Splunk

Important: Si votre système ExtraHop comprend une console ou Reveal(x) 360, configurez tous les capteurs avec les mêmes paramètres d'enregistrement ou transférez la gestion pour gérer les paramètres depuis la console ou Reveal(x) 360

.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Enregistrements, cliquez sur **Recordstore**.
3. Sélectionnez **Activer Splunk en tant que magasin d'enregistrements**.

   Note: Si vous migrez vers Splunk à partir d'un magasin d'enregistrements ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements stockés sur le magasin d'enregistrements.
4. Dans la section Record Ingest Target, remplissez les champs suivants :

   • **Hôte d'ingestion Splunk:** Le nom d'hôte ou l'adresse IP de votre serveur Splunk.

   • **Port du collecteur d'événements HTTP:** Le port sur lequel le collecteur d'événements HTTP enverra les enregistrements.

   • **Jeton du collecteur d'événements HTTP:** Le jeton d'authentification que vous avez créé dans Splunk pour le collecteur d'événements HTTP.
5. Dans la section Record Query Target, remplissez les champs suivants :

   • **Hôte de la requête Splunk:** Le nom d'hôte ou l'adresse IP de votre serveur Splunk.

   • **Port de l'API REST:** Le port sur lequel envoyer les requêtes d'enregistrement.

   • **Méthode d'authentification:** La méthode d'authentification, qui dépend de votre version de Splunk.

   Pour les versions de Splunk ultérieures à 7.3.0, sélectionnez **Authentifier avec jeton**, puis collez votre jeton d'authentification Splunk
   . Pour

   savoir comment créer un jeton d'authentification, consultez la documentation Splunk.

   Pour les versions de Splunk antérieures à
   7.3.

0, sélectionnez **Authentifier avec le nom d'utilisateur et le mot de passe**, puis saisissez vos informations d'identification Splunk
.

6. Désactivez la case à cocher **Exiger la vérification du certificat** si votre connexion ne nécessite pas de certificat SSL/TLS valide.

   Note: Les connexions sécurisées au serveur Splunk peuvent être vérifiées à l'aide de certificats fiables que vous téléchargez sur le système ExtraHop.

7. Dans le champ Nom de l'index, saisissez le nom de l'index Splunk dans lequel vous souhaitez stocker les enregistrements.

   L'index par défaut de Splunk s'appelle `main`, mais nous vous recommandons de créer un index distinct pour vos enregistrements ExtraHop et de saisir le nom de cet index. Pour obtenir des instructions sur la création d'un index, consultez la documentation Splunk.

8. (Capteur ExtraHop uniquement) Cliquez sur **Tester la connexion** pour vérifier que le système ExtraHop peut atteindre votre serveur Splunk.
9. Cliquez sur **Enregistrer**.

Une fois la configuration terminée, vous pouvez interroger les enregistrements stockés dans le système ExtraHop en cliquant sur **Enregistrements** dans le menu supérieur.

Transférer les paramètres du magasin d'enregistrement

Si une console ExtraHop est connectée à vos capteurs ExtraHop, vous pouvez configurer et gérer les paramètres de stockage d'enregistrements sur le capteur ou transférer la gestion des paramètres vers la console. Le transfert et la gestion des paramètres d'enregistrement sur la console vous permettent de maintenir les paramètres d'enregistrement à jour sur plusieurs capteurs.

Les paramètres des magasins d'enregistrement sont configurés pour les magasins d'enregistrement tiers connectés et ne s'appliquent pas au magasin d'enregistrement ExtraHop.

1. Connectez-vous aux paramètres d'administration du capteur via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Enregistrements, cliquez sur **Magasin d'enregistrements**.
3. Dans la liste déroulante **Paramètres du magasin d'enregistrements**, sélectionnez l'appliance de commande, puis cliquez sur **Transférer**.

   Si vous décidez ultérieurement de gérer les paramètres du capteur, sélectionnez l **'appliance Discover** dans la liste déroulante Paramètres du magasin d'enregistrements, puis cliquez sur **Transférer**.