Envoyer des enregistrements depuis ExtraHop vers Splunk

Publié: 2024-09-26

Vous pouvez configurer le système ExtraHop pour envoyer des enregistrements au niveau des transactions à un serveur Splunk pour un stockage à long terme, puis interroger ces enregistrements depuis le système ExtraHop et l'API REST ExtraHop.

Voici quelques considérations concernant l'envoi d'enregistrements depuis ExtraHop vers Splunk :

- Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` vers un espace de stockage des enregistrements sont automatiquement redirigés vers le serveur Splunk. Aucune autre configuration n'est requise.
- Si vous migrez vers Splunk depuis un espace de stockage ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements qui y sont stockés.
- Si vous souhaitez consulter et analyser des données ExtraHop telles que des métriques et des détections dans une interface Splunk, configurez un Splunk ou Splunk SOAR intégration.

Activer Splunk comme espace de stockage des enregistrements

Effectuez cette procédure sur tous les systèmes ExtraHop connectés.

Important: Si votre système ExtraHop inclut une console ou RevealX 360, configurez tous les capteurs avec les mêmes paramètres d'espace de stockage des enregistrements ou gérez les transferts pour gérer les paramètres depuis la console ou RevealX 360.

Avant de commencer

- Toutes les consoles et tous les capteurs connectés doivent exécuter la même version du firmware ExtraHop.
- Vous devez disposer de la version 7.0.3 ou ultérieure de Splunk Enterprise et d'un compte utilisateur doté de privilèges dcessant d'être administrateur.
- Vous devez configurer le collecteur d'événements HTTP Splunk pour que votre serveur Splunk puisse recevoir des enregistrements ExtraHop . Consultez les Collecteur d'événements HTTP Splunk documentation pour les instructions.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Disques section, cliquez sur **Disquaire**.
3. Sélectionnez **Activer Splunk comme espace de stockage des enregistrements**.
4. Dans le Objectif d'ingestion record section, renseignez les champs suivants :

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

   • **Port du collecteur d'événements HTTP:** Port par lequel le collecteur d'événements HTTP doit envoyer les enregistrements.

   • **Jeton de collecte d'événements HTTP:** Le jeton d'authentification que vous créé dans Splunk pour le collecteur d'événements HTTP.
5. Dans le Enregistrer la cible de la requête section, renseignez les champs suivants :

   • **Hôte de requêtes 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 **Authentifiez-vous avec un jeton**, puis collez votre jeton d'authentification Splunk. Pour obtenir des instructions sur la création d'un jeton d'authentification, consultez Documentation Splunk.

Pour les versions de Splunk antérieures à 7.3.0, sélectionnez **Authentifiez-vous avec nom d'utilisateur et mot de passe**, puis saisissez vos informations dcessaires d'identification Splunk.

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

   Note: Les connexions sécurisées au serveur Splunk peuvent être vérifiées via certificats fiables que vous téléchargez sur le système ExtraHop.

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

   L'index par défaut de Splunk s'appelle `main`, nous vous recommandons toutefois 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 Documentation Splunk.

8. (ExtraHop) sonde uniquement) Cliquez **Connexion de test** pour vérifier que le système ExtraHop peut atteindre votre serveur Splunk.
9. Cliquez **Enregistrer**.

Une fois votre configuration terminée, vous pouvez rechercher des enregistrements stockés dans le système ExtraHop en cliquant **Disques** depuis le menu du haut.

Transférer les paramètres de l'espace de stockage des enregistrements

Si vous avez un ExtraHop console connecté à vos capteurs ExtraHop, vous pouvez configurer et gérer les paramètres de l'espace de stockage des enregistrements sur le capteur, ou transférer la gestion des paramètres au console. Le transfert et la gestion des paramètres de l'espace de stockage des enregistrements sur la console vous permettent de maintenir les paramètres de l'espace de stockage à jour sur plusieurs capteurs.

Les paramètres de Recordstore sont configurés pour les magasins d'enregistrements tiers connectés et ne s'appliquent pas à l'espace de stockage des enregistrements ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Disques section, cliquez sur **Disquaire**.
3. À partir du **Paramètres du Recordstore** liste déroulante, sélectionnez la console, puis cliquez sur **Transférer la propriété**.

   Si vous décidez ultérieurement de gérer les paramètres du sonde, sélectionnez **cette sonde** dans la liste déroulante des paramètres de Recordstore , puis cliquez sur **Transférer la propriété**.