Envoyer des enregistrements de ExtraHop à CrowdStrike Falçon LogScale

Publié: 2024-01-31

Vous pouvez configurer votre système ExtraHop Reveal (x) Enterprise pour envoyer des enregistrements au niveau des transactions à un référentiel CrowdStrike FalconLogScale pour un stockage à long terme, puis interroger ces enregistrements depuis le système ExtraHop et l'API REST ExtraHop.

Voici quelques considérations importantes concernant l'activation d'un référentiel LogScale en tant qu'espace de stockage des enregistrements :

- La quantité de recherche dans l'espace de stockage des enregistrements qui peut être interrogée est déterminée par paramètres de conservation des données configuré pour votre système LogScale.
- Vous pouvez activer un référentiel LogScale distinct pour chaque sonde ExtraHop.
- À partir d'une console ExtraHop, vous pouvez interroger les enregistrements des référentiels LogScale sur tous les capteurs ExtraHop connectés si ces référentiels sont associés à la même vue LogScale.
- Si tous les capteurs ExtraHop envoient des enregistrements vers le même référentiel, vous pouvez transférer les paramètres de l'espace de stockage des enregistrements et gérez tous les capteurs depuis la console ExtraHop.
- Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` vers un espace de stockage des enregistrements sont automatiquement redirigés vers le référentiel LogScale. Aucune autre configuration n'est requise.

Activer LogScale en tant qu'espace de stockage des enregistrements

Avant de commencer

- Votre système ExtraHop doit disposer d'une licence pour l'espace de stockage des enregistrements LogScale .
- Votre système ExtraHop doit exécuter le firmware Reveal (x) Enterprise version 9.5 ou ultérieure.
- Toutes les consoles et tous les capteurs connectés doivent exécuter la même version du firmware ExtraHop.
- Votre compte utilisateur ExtraHop doit avoir Privilèges d'administration du système et des accès.
- Votre système LogScale doit disposer de la version 1.111.0 ou ultérieure.
- Votre compte utilisateur LogScale doit disposer de privilèges d'administrateur.
- Vous devez disposer d'un jeton d'ingestion LogScale associé à un référentiel ou à un jeton d'organisation qui autorise l'ingestion sur tous les référentiels de l'organisation.
- Vous devez disposer d'un jeton d'affichage LogScale qui inclut l' autorisation d'accès à la lecture des données.

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 **Disquaire**.
3. Sélectionnez **Activer LogScale en tant qu'espace de stockage des enregistrements**.

   Important: Si vous migrez vers LogScale depuis un espace de stockage ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements stockés sur cet espace de stockage ExtraHop.
4. Dans le Ingérer section, spécifiez les informations suivantes concernant le référentiel LogScale qui va ingérer et stocker les enregistrements du système ExtraHop :
   - **Nom d'hôte d'ingestion:** Le nom d'hôte du référentiel LogScale.
   - **Port d'ingestion:** Port par lequel les enregistrements sont envoyés au référentiel.

- **Jeton d'ingestion du référentiel:** Le jeton d'authentification pour l'ingestion de données dans LogScale.

5. Dans le Requête section, spécifiez les informations suivantes concernant le serveur API LogScale qui traitera les requêtes d'enregistrement provenant du système ExtraHop .
   - **Nom d'hôte de l'API:** Le nom d'hôte du serveur d'API.
   - **Port de l'API:** Port par lequel les requêtes d'enregistrement sont envoyées à l'API.
   - **Afficher le nom:** Nom de la vue LogScale connectée au référentiel.
   - **Afficher le jeton:** Le jeton d'authentification pour les requêtes adressées au référentiel LogScale.
6. Optionnel : Sélectionnez **Compressez les charges utiles des enregistrements sortants avec GZip** pour réduire la taille des fichiers ingérés.
7. Cliquez **Connexion de test** pour vérifier que votre sonde peut communiquer avec le référentiel LogScale.
8. Cliquez **Enregistrer**.

Une fois votre configuration terminée, vous pouvez requête pour les enregistrements stockés dans le système ExtraHop en cliquant **Disques** depuis le menu de navigation supérieur ou depuis le API REST ExtraHop.

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 sonde à travers `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Enregistrements, 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**.