Envoyer des enregistrements depuis ExtraHop vers Google BigQuery

Publié: 2024-08-09

Vous pouvez configurer votre système ExtraHop pour envoyer des enregistrements au niveau des transactions à un serveur Google BigQuery pour un stockage à long terme, puis interroger ces enregistrements depuis le système ExtraHop et l'API REST ExtraHop. Les enregistrements des librairies BigQuery expirent au bout de 90 jours.

Avant de commencer

- Toutes les consoles et tous les capteurs connectés doivent exécuter la même version du firmware ExtraHop.
- Vous avez besoin de l'ID de projet BigQuery
- Vous avez besoin du fichier d'identification (JSON) de votre compte de service BigQuery. Le compte de service nécessite les rôles BigQuery Data Editor, BigQuery Data Viewer et BigQuery User.
- Pour accéder à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation, votre capteurs doit pouvoir accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :
  - `bigquery.googleapis.com`
  - `bigquerystorage.googleapis.com`
  - `oauth2.googleapis.com`
  - `www.googleapis.com`
  - `www.mtls.googleapis.com`
  - `iamcredentials.googleapis.com`

  Vous pouvez également consulter les conseils publics de Google sur calcul des plages d'adresses IP possibles pour googleapis.com.
- Si vous souhaitez configurer les paramètres de l'espace de stockage des enregistrements BigQuery avec l'authentification par fédération d'identité de charge de travail Google Cloud, vous avez besoin du fichier de configuration provenant de votre pool d'identités de charge de travail.

  Note: Le fournisseur d'identité de charge de travail doit être configuré pour fournir un jeton d'identification OIDC entièrement valide en réponse à une demande d'informations d'identification du client. Pour plus d'informations sur la fédération des identités de charge de travail, voir https://cloud.google.com/iam/docs/workload-identity-federation.

Activer BigQuery comme espace de stockage des enregistrements

Effectuez cette procédure sur tous les capteurs et la console ExtraHop connectés.

Note: Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` vers un espace de stockage des enregistrements ExtraHop sont automatiquement redirigés vers BigQuery. Aucune autre configuration n'est requise.

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

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 BigQuery comme espace de stockage des enregistrements**.

Important: Si vous migrez vers BigQuery depuis un espace de stockage ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements stockés dans cet espace de stockage.

4. Dans le ID du projet dans ce champ, saisissez l'ID de votre projet BigQuery.

   L'ID du projet se trouve dans la console de l'API BigQuery.
5. Dans le Fichier d'identification JSON champ, cliquez sur **Choisissez un fichier** et sélectionnez l'un des fichiers suivants :

   - Le fichier d'informations d'identification enregistré depuis votre Compte de service BigQuery.

     Consultez la documentation Google Cloud pour savoir comment créer un compte de service et générer une clé de compte de service.

     Important: Créez votre compte de service avec les rôles BigQuery suivants :

     - Éditeur de données BigQuery
     - Visionneuse de données BigQuery
     - Utilisateur BigQuery
   - Le fichier de configuration de votre pool d'identités de charge de travail.
6. Optionnel : Si vous avez choisi le fichier de configuration dans votre pool d'identités de charge de travail à l'étape précédente, sélectionnez **Authentifiez-vous via le fournisseur d'identité local pour Workload Identity Federation** et saisissez les informations d'identification de votre fournisseur d'identité dans les champs suivants :

   - **URL du jeton**
   - **Identifiant du client**
   - **Secret du client**
7. Cliquez **Connexion de test** pour vérifier que votre sonde peut communiquer avec le serveur BigQuery.
8. Cliquez **Enregistrer**.

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

Important: Ne modifiez ni ne supprimez la table dans BigQuery dans laquelle les enregistrements sont stockés. La suppression de la table entraîne la suppression de tous les enregistrements enregistrés.

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**.