Envoi d'enregistrements d'ExtraHop vers Google BigQuery

Publié: 2023-09-19

Vous pouvez configurer votre système ExtraHop pour qu'il envoie des enregistrements de niveau transactionnel à un serveur Google BigQuery pour un stockage à long terme, puis qu'il interroge ces enregistrements à partir du système ExtraHop et de l'API REST ExtraHop. Les enregistrements sur les magasins d'enregistrements BigQuery expirent au bout de 90 jours.

Avant de commencer

- Vous avez besoin de l'ID du projet BigQuery
- Vous avez besoin du fichier d'identification (JSON) de votre compte de service BigQuery. Le compte de service nécessite les rôles d'éditeur de données BigQuery, de visualiseur de données BigQuery et d'utilisateur BigQuery.
- Pour accéder à l'ExtraHop Cloud Recordstore, vos capteurs doivent pouvoir accéder à la sortie TCP 443 (HTTPS) vers ces noms de domaine pleinement qualifiés :
  - `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 concernant les plages d'adresses IP possibles pour googleapis.com.
- Si vous souhaitez configurer les paramètres du magasin d'enregistrements BigQuery avec l'authentification de fédération d'identité de charge de travail Google Cloud, vous avez besoin du fichier de configuration de votre pool d'identité 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 Client Credentials. Pour plus d'informations sur la fédération d'identité de charge de travail, voir https://cloud.google.com/iam/docs/workload-identity-federation.

Envoi d'enregistrements d'ExtraHop vers BigQuery

Note: Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` à un magasin d'enregistrements ExtraHop sont automatiquement redirigés vers BigQuery

.

Important: Si votre système ExtraHop comprend une console, configurez tous les appareils avec les mêmes paramètres de magasin d'enregistrement ou transférez la gestion pour gérer les paramètres à partir de la console

.

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 **Magasin d'enregistrements**.
3. Sélectionnez **Activer BigQuery en tant que magasin d'enregistrements**.

Important: Si vous migrez vers BigQuery à partir d'un magasin d'enregistrements ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements stockés sur le magasin d'enregistrements.

4. Dans le champ ID du projet, saisissez l'ID de votre projet BigQuery. L'ID du projet se trouve dans la console API BigQuery.
5. Dans le champ JSON Credential File, cliquez sur **Choose File** et sélectionnez l'un des fichiers suivants :
   - Le fichier d'informations d'identification enregistré à partir de votre compte de service BigQuery

     . Consultez la documentation de 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
     - Visualisateur de données BigQuery
     - Utilisateur BigQuery
   - Le fichier de configuration de votre pool d'identité de charge de travail.
6. Optionnel : Si vous avez choisi le fichier de configuration de votre pool d'identité de charge de travail à l'étape précédente, sélectionnez **Authentifier via le fournisseur d'identité local pour la fédération d'identité de charge de travail** et entrez les informations d'identification de votre fournisseur d'identité dans les champs suivants :
   - **Token URL**
   - **ID du client**
   - **Secret du client**
7. Cliquez sur **Tester la connexion** pour vérifier que votre capteur peut communiquer avec le serveur BigQuery.
8. Cliquez sur **Enregistrer**.

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

Important: Ne modifiez pas et ne supprimez pas la table de BigQuery dans laquelle les enregistrements sont stockés. La suppression de la table supprime tous les enregistrements stockés.

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**.