

Datensätze von ExtraHop an Google BigQuery senden

Veröffentlicht: 2024-08-09

Sie können Ihr ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Google BigQuery-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen. Datensätze in BigQuery-Datensatzspeichern laufen nach 90 Tagen ab.

Bevor Sie beginnen

- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Sie benötigen die BigQuery-Projekt-ID
- Sie benötigen die Anmeldeinformationsdatei (JSON) von Ihrem BigQuery-Dienstkonto. Für das Dienstkonto sind die Rollen BigQuery Data Editor, BigQuery Data Viewer und BigQuery User erforderlich.
- Für den Zugriff auf den cloudbasierten Recordstore, der in RevealX Standard Investigation enthalten ist, benötigen Sie Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) auf diese vollständig qualifizierten Domainnamen zuzugreifen:
 - `bigquery.googleapis.com`
 - `bigquerystorage.googleapis.com`
 - `oauth2.googleapis.com`
 - `www.googleapis.com`
 - `www.mtls.googleapis.com`
 - `iamcredentials.googleapis.com`

Sie können auch die öffentlichen Leitlinien von Google zu folgenden Themen lesen [Berechnung möglicher IP-Adressbereiche](#) für `googleapis.com`.

- Wenn Sie die BigQuery-Recordstore-Einstellungen mit der Google Cloud-Workload-Identitätsverbundauthentifizierung konfigurieren möchten, benötigen Sie die Konfigurationsdatei aus Ihrem Workload-Identitätspool.



Hinweis Der Workload-Identitätsanbieter muss so eingerichtet sein, dass er als Antwort auf eine Anfrage mit Client-Anmeldeinformationen ein vollständig gültiges OIDC-ID-Token bereitstellt. Weitere Informationen zum Workload-Identitätsverbund finden Sie unter <https://cloud.google.com/iam/docs/workload-identity-federation>.

BigQuery als Recordstore aktivieren

Führen Sie diesen Vorgang an allen angeschlossenen ExtraHop-Sensoren und der Konsole durch.



Hinweis Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem ExtraHop-Recordstore werden automatisch zu BigQuery umgeleitet. Es ist keine weitere Konfiguration erforderlich.



Wichtig: Wenn Ihr ExtraHop-System eine Konsole enthält, konfigurieren Sie alle Appliances mit denselben Recordstore-Einstellungen oder übertragen Sie die Verwaltung, um die Einstellungen von der Konsole aus zu verwalten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Plattenladen**.
3. Wählen **BigQuery als Recordstore aktivieren**.

- ! **Wichtig:** Wenn Sie von einem verbundenen ExtraHop-Recordstore zu BigQuery migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
- 4. In der Projekt-ID Feld, geben Sie die ID für Ihr BigQuery-Projekt ein.
Sie finden die Projekt-ID in der BigQuery API-Konsole.
- 5. In der JSON-Anmeldeinformationsdatei Feld, klicken **Wählen Sie Datei** und wählen Sie eine der folgenden Dateien aus:
 - Die Anmeldeinformationsdatei, die von Ihrem gespeichert wurde [BigQuery-Dienstkonto](#).

Informationen zum Erstellen eines Dienstkontos und zum Generieren eines Dienstkontoschlüssels finden Sie in der Google Cloud-Dokumentation.

 - ! **Wichtig:** Erstellen Sie Ihr Dienstkonto mit den folgenden BigQuery-Rollen:
 - BigQuery-Dateneditor
 - BigQuery-Datenviewer
 - BigQuery-Benutzer
 - Die Konfigurationsdatei aus Ihrem Workload-Identitätspool.
- 6. Optional: Wenn Sie im vorherigen Schritt die Konfigurationsdatei aus Ihrem Workload-Identitätspool ausgewählt haben, wählen Sie **Authentifizieren Sie sich über den lokalen Identitätsanbieter für Workload Identity Federation** und geben Sie die Anmeldedaten Ihres Identitätsanbieters in die folgenden Felder ein:
 - **Token-URL**
 - **Kunden-ID**
 - **Geheimer Kunde**
- 7. Klicken Sie **Verbindung testen** um zu überprüfen, ob Ihr Sensor mit dem BigQuery-Server kommunizieren kann.
- 8. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie im ExtraHop-System nach gespeicherten Datensätzen abfragen, indem Sie auf **Rekorde**.

- ! **Wichtig:** Ändern oder löschen Sie die Tabelle in BigQuery, in der die Datensätze gespeichert sind, nicht. Durch das Löschen der Tabelle werden alle gespeicherten Datensätze gelöscht.

Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores von Drittanbietern konfiguriert und gelten nicht für den ExtraHop-Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.