

# Datensätze von ExtraHop an Google BigQuery senden

Veröffentlicht: 2023-09-13

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-Plattenspeichern laufen nach 90 Tagen ab.

## Bevor Sie beginnen

- 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 ExtraHop Cloud Recordstore benötigen Sie Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) zu diesen vollqualifizierten 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>.

## Datensätze von ExtraHop an BigQuery senden

Führen Sie dieses Verfahren für alle angeschlossenen Sensoren und Konsolen 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 über eine Konsole verfügt, konfigurieren Sie alle Geräte mit denselben Recordstore-Einstellungen oder derselben Übertragungsverwaltung, 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. Klicken Sie im Bereich Datensätze auf **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. Geben Sie im Feld Projekt-ID die ID für Ihr BigQuery-Projekt ein. Die Projekt-ID finden Sie in der BigQuery-API-Konsole.
5. Klicken Sie im Feld JSON-Anmeldeinformationsdatei auf **Datei wählen** und wählen Sie eine der folgenden Dateien aus:
  - Die Anmeldeinformationsdatei wurde von Ihrem [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 Kundenschlüssel**
7. klicken **Verbindung testen** um zu überprüfen, ob Ihr Sensor mit dem BigQuery-Server kommunizieren kann.
8. klicken **Speichern**.

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

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

## Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole verbunden mit Ihren ExtraHop-Sensoren können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen auf den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen über mehrere Sensoren hinweg auf dem neuesten Stand halten.

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

1. Loggen Sie sich in die Administrationseinstellungen auf der Sensor durch `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Bereich Datensätze auf **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Command-Appliance aus und klicken Sie dann auf **Übertragung**.

Wenn Sie sich später entscheiden, die Einstellungen auf dem zu verwalten Sensor, wählen **dieses Discover-Gerät** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Übertragung**.