

# Ein Kafka-Target für einen offenen Datenstrom konfigurieren

Veröffentlicht: 2023-09-13

Sie können Daten auf einem ExtraHop-System auf jeden Kafka-Server exportieren, um sie langfristig zu archivieren und mit anderen Quellen zu vergleichen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`  
Wiederholen Sie diese Schritte auf jeder Discover-Appliance in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken **Offene Datenströme**.
3. klicken **Ziel hinzufügen**.
4. Aus dem Typ des Ziels Drop-down-Menü, wählen **Kafka**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. Aus dem Kompression Wählen Sie in der Dropdownliste eine der folgenden Komprimierungsmethoden aus, die auf die übertragenen Daten angewendet werden:
  - **Keine**
  - **GZIP**
  - **Bissig**
7. Aus dem Partitionsstrategie Wählen Sie in der Dropdownliste eine der folgenden Partitionierungsmethoden aus, die auf die übertragenen Daten angewendet werden:
  - **Standard (Hash-Schlüssel)**
  - **Manuell**
  - **Zufällig**
  - **Round Robin**
8. Optional: Konfigurieren Sie die SASL/SCRAM-Authentifizierung.
  - a) Aus dem Authentifizierung Drop-down-Menü, wählen **SASL/SCRAM**.
  - b) In der **Nutzername** Feld, geben Sie den Namen des SASL/SCRAM-Benutzers ein.
  - c) In der **Passwort** Feld, geben Sie das Passwort des SASL/SCRAM-Benutzers ein.
  - d) Aus dem Hash-Algorithmus Wählen Sie im Dropdownmenü den Hash-Algorithmus für die SASL-Authentifizierung aus.
9. Aus dem Protokoll Wählen Sie im Dropdownmenü eines der folgenden Protokolle aus, über das Daten übertragen werden sollen:
  - **TCP**
  - **SSL/TLS**
10. Optional: Wenn Sie das ausgewählt haben **SSL/TLS** Protokoll, geben Sie die Zertifikatsoptionen an.
  - a) Wenn der Kafka-Server eine Client-Authentifizierung erfordert, geben Sie ein TLS-Client-Zertifikat an, das an den Server gesendet werden soll, in der **Client-Zertifikat** Feld.
  - b) Wenn Sie ein Client-Zertifikat angegeben haben, geben Sie den privaten Schlüssel des Zertifikats in der **Kundenschlüssel** Feld.
  - c) Wenn Sie das Zertifikat des Kafka-Servers nicht verifizieren möchten, wählen Sie **Überprüfung Server Serverzertifikats überspringen**.
  - d) Wenn Sie das Zertifikat des Kafka-Servers verifizieren möchten, das Zertifikat aber nicht von einer gültigen Zertifizierungsstelle (CA) signiert wurde, geben Sie vertrauenswürdige Zertifikate an, mit denen das Serverzertifikat verifiziert werden soll, in der **CA-Zertifikate (optional)** Feld. Geben Sie die Zertifikate im PEM-Format an. Wenn diese Option nicht angegeben ist, wird das Serverzertifikat anhand der integrierten Liste gültiger CA-Zertifikate validiert.

11. Geben Sie mindestens einen Kafka-Broker an, der auch als Knoten in einem Kafka-Cluster bezeichnet wird und übertragene Daten empfangen kann.



**Hinweis** Sie können mehrere Broker hinzufügen, die Teil desselben Kafka-Clusters sind, um die Konnektivität sicherzustellen, falls ein einzelner Broker nicht verfügbar ist. Alle Broker müssen Teil desselben Cluster sein.

- a) In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Kafka-Brokers ein.
  - b) In der Hafen Feld, geben Sie die Portnummer des Kafka-Brokers ein.
  - c) Klicken Sie auf das Plus (+) Symbol.
12. Optional: klicken **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-Kafka-Server herzustellen und eine Testnachricht an den Server zu senden.  
Im Dialogfeld wird eine Meldung angezeigt, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Zielkonfiguration und testen Sie die Verbindung erneut.
  13. klicken **Speichern**.

#### Nächste Schritte

Erstellen Sie einen Auslöser, der festlegt, welche Kafka-Nachrichtendaten gesendet werden sollen, und der die Übertragung von Daten an das Ziel initiiert. Weitere Informationen finden Sie in der [Remote.Kafka](#) Klasse in der [ExtraHop Trigger API-Referenz](#).