

Konfigurieren Sie ein Syslog-Ziel für einen offenen Datenstrom

Veröffentlicht: 2024-09-26

Sie können Daten auf einem ExtraHop-System in jedes System exportieren, das Syslog-Eingaben empfängt (wie Splunk, ArcSight oder Q1 Labs), 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 für jeden Sensor in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Datenströme öffnen**.
3. Klicken Sie **Ziel hinzufügen**.
4. Aus dem Zieltyp Dropdownliste, wählen **Syslog**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Remote-Syslog-Servers ein.
7. In der Hafen Feld, geben Sie die Portnummer des Remote-Syslog-Servers ein.
8. Aus dem Protokoll Wählen Sie in der Dropdownliste eines der folgenden Protokolle aus, über das Daten übertragen werden sollen:
 - **TCP**
 - **UDP**
 - **TLS**
9. Optional: Wählen **Lokale Zeit** um Syslog-Informationen zu senden mit Zeitstempel in der lokalen Zeitzone des ExtraHop-Systems. Wenn diese Option nicht ausgewählt ist, werden Zeitstempel in GMT gesendet.
10. Optional: Wählen **Rahmen für Längenpräfix** um die Anzahl der Byte in einer Nachricht dem Anfang jeder Nachricht voranzustellen. Wenn diese Option nicht ausgewählt ist, wird das Ende jeder Nachricht durch einen abschließenden Zeilenumbruch begrenzt.
11. Optional: In der Mindestanzahl Byte im Stapel Feld, geben Sie die Mindestanzahl an Byte ein, die gleichzeitig an den Syslog-Server gesendet werden sollen.
12. Optional: In der Gleichzeitige Verbindungen Feld, geben Sie die Anzahl der gleichzeitigen Verbindungen ein, über die Nachrichten gesendet werden sollen.
13. Optional: Wenn Sie das ausgewählt haben **TLS** Protokoll, geben Sie die Zertifikatsoptionen an.
 - a) Wenn der Syslog-Server eine Client-Authentifizierung erfordert, finden Sie im **Client-Zertifikat** Feld, geben Sie ein TLS-Client-Zertifikat an, das an den Server gesendet werden soll.
 - b) Wenn Sie ein Client-Zertifikat angegeben haben, in **Kundenschlüssel** Feld, geben Sie den privaten Schlüssel des Zertifikats an.
 - c) Wenn Sie das Zertifikat des Syslog-Servers nicht verifizieren möchten, wählen Sie **Überspringen Sie die Überprüfung Server Serverzertifikats**.
 - d) Wenn Sie das Zertifikat des Kafka-Servers verifizieren möchten, das Zertifikat jedoch nicht von einer gültigen Zertifizierungsstelle (CA) signiert wurde, finden Sie in der **CA-Zertifikate (optional)** Feld, geben Sie vertrauenswürdige Zertifikate im PEM-Format an, mit denen das Serverzertifikat überprüft werden soll. Wenn diese Option nicht angegeben ist, wird das Serverzertifikat mit der integrierten Liste gültiger CA-Zertifikate validiert.
14. Optional: Klicken Sie **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-Syslog-Server herzustellen und eine Testnachricht an den Server zu senden.
Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Zielkonfiguration und testen Sie die Verbindung erneut.

15. Klicken Sie **Speichern**.

Nächste Schritte

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