

Problembehandlung bei der Recordstore-Konnektivität

Veröffentlicht: 2023-09-30


Reveal (x) 360 bietet einen vollständig gehosteten, cloudbasierten Recordstore, der Ihnen eine einheitliche Ansicht Ihrer Sensoren bietet. Wenn die Verbindung von einem selbstverwalteten Sensor zum Recordstore deaktiviert ist, finden Sie hier einige Möglichkeiten zur Fehlerbehebung und Wiederherstellung der Verbindung.

Eine Benachrichtigungsregel erstellen

Um etwas über Probleme zu erfahren, wenn sie auftreten, [eine Benachrichtigungsregel erstellen](#) um eine Empfängerliste per E-Mail zu versenden, wenn Systemereignisse auftreten, die mit Verbindungsproblemen im Recordstore zusammenhängen. Die E-Mail-Benachrichtigung enthält die Namen der betroffenen Sensoren, die Sie untersuchen sollten.

Überprüfen Sie die Sensorkonfiguration

Sehen Sie sich die Sensordetails an, um zu überprüfen, ob ein betroffener Sensor deaktiviert ist, eine ungültige Lizenz hat oder eine neuere Firmware benötigt.

1. Loggen Sie sich bei Reveal (x) 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Sensoren**.
3. Klicken Sie auf den Sensor, den Sie untersuchen möchten, und überprüfen Sie die Sensordetails.
 - Wenn der Sensor offline ist, aktivieren Sie den Sensor.
 - Wenn die Lizenz ungültig ist, wenden Sie sich an Ihren ExtraHop-Vertriebsmitarbeiter.
 - Wenn Ihre Firmware veraltet ist, füllen Sie einen [Firmware-Aktualisierung](#).

Testen Sie die Sensorverbindung in den Administrationseinstellungen

Testen Sie die Konnektivität in den Administrationseinstellungen des betroffenen Sensor. Wenn der Sensor keine Verbindung zum Recordstore herstellen kann, zeigt das ExtraHop-System Fehlermeldungen über die Ursache an, z. B. Probleme mit der Firewall oder der BigQuery-Ingest-API.

1. Melden Sie sich über <https://<extrahop-hostname-or-IP-address>/admin> bei den Administrationseinstellungen des betroffenen Sensor an.
2. Klicken Sie im Bereich Aufzeichnungen auf **Plattenladen**.
3. klicken **Verbindung testen**. Das System zeigt eine Erfolgsmeldung oder eine detaillierte Fehlermeldung an, die Ihnen bei der Behebung von Verbindungsproblemen helfen kann.

Überprüfen Sie den Zugriff auf ExtraHop Cloud Services und den Recordstore

Ein Sensor empfängt möglicherweise keine Datensätze, wenn er DNS-Anfragen an Google BigQuery-Domains nicht auflösen kann oder der Datenverkehr zu diesen Domains blockiert ist.

Wenn Ihr ExtraHop-System in einer Umgebung mit einer Firewall eingesetzt wird, müssen Sie den Zugriff auf ExtraHop Cloud Services öffnen. Stellen Sie sicher, dass Ihre Umgebung es Sensoren ermöglicht, DNS-Abfragen für *.extrahop.com aufzulösen, und dass der TCP-443-Zugriff (HTTPS) von der IP-Adresse aus zulässig ist, die Ihrer Sensorlizenz entspricht:

- 35.161.154.247 (Portland, Vereinigte Staaten von Amerika)
- 54.66.242.25 (Sydney, Australien)
- 52.59.110.168 (Frankfurt, Deutschland)

Für Reveal (x) 360-Systeme, die mit selbstverwalteten Sensoren verbunden sind, müssen Sie auch den Zugriff auf den ExtraHop Cloud Recordstore öffnen. Stellen Sie sicher, dass Ihre Umgebung Sensoren den Zugriff auf diese vollqualifizierten Domainnamen über ausgehendes TCP 443 (HTTPS) ermöglicht:

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`
- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Stellen Sie die korrekte Proxykonfiguration sicher

Recordstore-Verbindungen können zu Problemen führen, wenn Ihr ExtraHop-System mit einem falsch konfigurierten Proxyserver verbunden ist. Stellen Sie sicher, dass der Proxy für die Überprüfung von SSL/TLS-Verbindungen zu Google BigQuery-Domains konfiguriert ist und dass das Proxyserver-CA-Zertifikat dem sicheren Zertifikatsspeicher hinzugefügt wurde.

gRPC-Verkehr zulassen

Datensätze können nicht erstellt werden, wenn das gRPC-Protokoll (Remote Procedure Call) auf einem Sensor blockiert ist. Überprüfen Sie Ihre Umgebung, um sicherzustellen, dass gRPC-Verkehr zu Google BigQuery-Domains zulässig ist.