Problembehandlung bei der Recordstore-Konnektivität

Veröffentlicht: 2024-08-09

RevealX 360 mit Standard Investigation bietet einen vollständig gehosteten, cloudbasierten Datenspeicher, der Ihnen eine einheitliche Ansicht Ihrer Sensoren bietet. Wenn die Verbindung von einem selbstverwalteten Sensor zum Recordstore deaktiviert ist, finden Sie hier einige Möglichkeiten, Fehler zu beheben und die Verbindung wiederherzustellen.

Eine Benachrichtigungsregel erstellen

Um mehr über Probleme zu erfahren, wenn sie auftreten, eine Benachrichtigungsregel erstellen um eine Empfängerliste per E-Mail zu senden, wenn Systemereignisse auftreten , die mit Recordstore-Konnektivitätsproblemen 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 in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Fühler**.
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 eine 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 zur 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 Verwaltungseinstellungen des betroffenen Sensor an.
2. Klicken Sie im Abschnitt Aufzeichnungen auf **Plattenladen**.
3. Klicken Sie **Verbindung testen**. Das System zeigt eine Erfolgsmeldung oder eine detaillierte Fehlermeldung an, die Ihnen bei der Behebung der Verbindung helfen kann.

Verifizieren Sie den Zugriff auf ExtraHop Cloud Services und den Recordstore

Ein Sensor empfängt möglicherweise keine Datensätze, wenn er DNS-Abfragen an Google BigQuery-Domains nicht auflösen kann oder der Verkehr 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 zu lösen, und dass der TCP-443-Zugriff (HTTPS) von der IP-Adresse aus ermöglicht wird, 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 RevealX 360-Systeme, die mit selbstverwalteten Sensoren verbunden sind, müssen Sie auch den Zugriff auf den cloudbasierten Recordstore öffnen, der in RevealX 360 mit Standard Investigation enthalten ist. 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

Bei Recordstore-Verbindungen können Probleme auftreten, wenn Ihr ExtraHop-System mit einem falsch konfigurierten Proxyserver verbunden ist. Stellen Sie sicher, dass der Proxy so konfiguriert ist, dass er SSL/TLS-Verbindungen zu Google BigQuery-Domains überprüft, und dass das Proxyserver-CA-Zertifikat zum sicheren Zertifikatsspeicher hinzugefügt wird.

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.