Stellen Sie über die REST-API von selbstverwalteten Sensoren aus eine Verbindung zu Reveal (x) 360 her

Veröffentlicht: 2024-03-27

Die ExtraHop REST-API ermöglicht es Ihnen, Verbindungen für eine große Anzahl selbstverwalteter Sensoren zu Reveal (x) 360 mit einem Skript. Selbstverwaltet Sensoren schließen lokale Discover-Appliances oder Instanzen ein, die auf Cloud-Dienstanbietern wie AWS, Azure und Google Cloud Platform (GCP) bereitgestellt werden.

Dieses Handbuch enthält Anweisungen für den REST API Explorer, damit Sie den REST-Vorgang testen können, sowie ein Python-Skript, das Sie mit Ihren Umgebungsvariablen ändern können.

Hinweis Sie können Trace-Appliances nicht über die REST-API verbinden. Hinweise zum Verbinden von Trace-Appliances finden Sie unter Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu Reveal (x) 360 her.

Bevor Sie beginnen

- Machen Sie sich mit dem vertraut ExtraHop REST-API-Leitfaden um zu erfahren, wie Sie im ExtraHop REST API Explorer navigieren.
- Sie benötigen System- und Zugriffsadministrationsrechte, um Reveal (x) 360 zu konfigurieren. Einzelheiten zur Einrichtung dieses Kontos finden Sie in der Einführungs-E-Mail von ExtraHop Networks.
- Du musst für jedes Token über Reveal (x) 360 generieren Sensor die du verbinden möchtest. Weitere Informationen finden Sie unter Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu Reveal (x) 360 her.
- Du musst dich einloggen im Sensor mit einem Konto, das über System- und Zugriffsadministrationsrechte zum Generieren eines API-Schlüssels verfügt.
- Sie benötigen einen gültigen API-Schlüssel, um Änderungen über die REST-API vorzunehmen und die folgenden Verfahren durchzuführen. (siehe Generieren Sie einen API-Schlüssel.)

Stellen Sie über den REST API Explorer eine Verbindung zu Reveal (x) 360 her

1. Navigieren Sie in einem Browser zum REST API Explorer.

   Die URL ist der Hostname oder die IP-Adresse Ihres Sensor oder Konsole, gefolgt von `/api/v1/explore/`. Wenn Ihr Hostname beispielsweise seattle-eda ist, lautet die URL `https://seattle-eda/api/v1/explore/`.
2. klicken **API-Schlüssel eingeben** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das **API-Schlüssel** Feld.
3. klicken **Autorisieren** und dann klicken **Schliessen**.
4. klicken **Wolke** und dann klicken **POST /cloud/connect**.
5. klicken **Probiere es aus**.
6. Ersetzen Sie im Körperfeld `string` mit dem Token, das Sie aus Reveal (x) 360 generiert haben, wie im folgenden Beispiel gezeigt:

   ```
   {
       "cloud_token": "561b85-e9092a3a-343fcb03-78c72777-8db70bbd"
   }
   ```

   Im Abschnitt Serverantwort wird ein 201-Statuscode angezeigt.

Python-Skriptbeispiel

Das ExtraHop GitHub-Repository enthält ein Python-Python-Skript, das Ihre Sensor zu Reveal (x) 360 durch Lesen von Tokens und API-Schlüsseln aus einer CSV-Datei.

1. Gehe zum GitHub-Repository mit ExtraHop-Codebeispielen und laden Sie die `self-managed-sensor-rx360-connect/self-managed-sensor-rx360-connect.py` Datei auf Ihrem lokalen Computer.
2. In das Verzeichnis, das Sie kopiert haben `self-managed-sensor-rx360-connect.py` um eine CSV-Datei zu erstellen, die die folgenden Spezifikationen erfüllt:
   - Die CSV-Datei darf keine Kopfzeile enthalten.
   - Jede Zeile der CSV-Datei muss die folgenden drei Spalten in der angegebenen Reihenfolge enthalten:

Die Sensor Hostname	Die Sensor API-Schlüssel	Das Token, das Sie mit Reveal (x) 360 generiert haben

   - Die CSV-Datei muss benannt werden `sensors.csv` und im selben Verzeichnis wie das Skript gespeichert.

     Hinweis: Ein Beispiel für eine kompatible CSV-Datei finden Sie in der Datei self-managed-sensor-rx360-connect/sensors.csv im GitHub-Repository ExtraHop code-examples.
3. Führen Sie den folgenden Befehl aus:

```
python self-managed-sensor-rx360-connect.py
```

Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die SSL-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen `verify=False` Option zur Umgehung der Zertifikatsüberprüfung. Diese Methode ist jedoch nicht sicher und wird nicht empfohlen. Der folgende Code sendet eine HTTP GET-Anfrage ohne Zertifikatsüberprüfung:

```
requests.get(url, headers=headers, verify=False)
```