Extrahieren Sie Metriken über die REST-API

Veröffentlicht: 2024-03-20

Sie können Metriken aus einem extrahieren Sensor oder Konsole über die REST-API, um Metriken in einem Drittanbieter-Tool zu visualisieren oder ExtraHop-Daten mit anderen von Ihnen gesammelten Daten zu vergleichen. Um eine Metrik zu extrahieren, müssen Sie zunächst Identifikatoren sowohl für die Metriken, die Sie extrahieren möchten, als auch für die Objekte, für die Sie Metriken extrahieren möchten, abrufen. Anschließend können Sie eine Metrikabfrage im REST API Explorer erstellen und testen, bevor Sie Ihre Anfrage in ein Skript integrieren, das die Metriken in ein Format lesen kann, das in Anwendungen importiert werden kann.

Bevor Sie beginnen

- Für Sensoren und ECA-VMs benötigen Sie einen gültigen API-Schlüssel, um Änderungen über die REST-API vornehmen und die folgenden Verfahren ausführen zu können. (siehe Generieren Sie einen API-Schlüssel.)
- Für Reveal (x) 360 benötigen Sie gültige REST-API-Anmeldeinformationen, um Änderungen über die REST-API vornehmen und die folgenden Verfahren ausführen zu können. (siehe REST-API-Anmeldeinformationen erstellen.)

Metrik-IDs abrufen

Metriken werden in der ExtraHop REST API durch eine Kombination von identifiziert `metric_category`, der `name`, und die `object_type`. Sie können alle drei Identifikatoren über den Metric Explorer abrufen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Metrischer Katalog**.
3. In der Typ um das Feld zu filtern, geben Sie den Namen der Metrik ein, die Sie extrahieren möchten, und klicken Sie dann in den Suchergebnissen unten auf den Namen der Metrik.
4. Scrollen Sie im rechten Bereich nach unten zu den REST-API-Parametern und Datensatz Sie die Werte auf.

   Beispielsweise werden die folgenden Informationen für die Metrik HTTP-Serverantworten angezeigt:

REST API Parameters

```
{
    "metric_category": "http_server",
    "object_type": "device",
    "metric_specs": [
        {
            "name": "rsp"
        }
    ]
}
```

Objekt-IDs abrufen

Als Nächstes müssen Sie den eindeutigen Bezeichner für das Objekt finden, für das Sie Metriken in der REST-API extrahieren möchten. Sie können diese ID über den REST API Explorer abrufen.

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 Sie **API-Schlüssel eingeben** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das **API-Schlüssel** Feld.
3. Klicken Sie **Autorisieren** und klicken Sie dann **Schliessen**.
4. Klicken Sie auf den Objekttyp, für den Sie Metriken sammeln möchten, z. B. **Gerät**, **Gerätegruppe**, **Bewerbung**, oder **Gerät**.
5. Klicken Sie **HOLEN SIE SICH/<objects>**.

   Wenn Sie beispielsweise Messwerte für eine Gerätegruppe extrahieren, klicken Sie auf **Abrufen/Gerätegruppen**.
6. Klicken Sie **Probiere es aus**.
7. Optional: In der Parameter Abschnitt, geben Sie die Suchkriterien für das Objekt an, das Sie suchen möchten.

   Sie können beispielsweise nach Objektnamen, IP-Adressen oder MAC-Adressen suchen. Wenn Sie Schwierigkeiten haben, ein Gerät zu finden, finden Sie unter Finde ein Gerät.
8. Klicken Sie **Anfrage senden**.

   In der Antwort des Servers Abschnitt, der Antworttext zeigt Informationen zu jedem Objekt an, das den Suchkriterien entspricht.
9. Notieren Sie sich die Zahl im ID-Feld für das Objekt, für das Sie Metriken sammeln möchten.

   Die ID des folgenden Server lautet beispielsweise 1298:


```
[
  {
    "mod_time": 1516639693474,
    "node_id": null,
    "id": 1298,
    "extrahop_id": "fff4c3090a0a0000",
    "discovery_id": "fff4c3090a0a0000",
    "display_name": "server1",
    "description": null,
    "user_mod_time": 1512688149084,
    "discover_time": 1498685400000,
    "vlanid": 0,
    "parent_id": 140,
    "macaddr": "A1:01:01:01:1A:01",
    "vendor": "Mellanox",
    "is_l3": true,
    "ipaddr4": "10.10.10.200",
    "ipaddr6": null,
    "device_class": "node",
    "default_name": "Mellanox 10.10.10.200",
    "custom_name": "server1",
    "cdp_name": "",
    "dhcp_name": "server1.company.com",
    "netbios_name": "",
    "dns_name": "server1.company.com",
    "custom_type": "",
    "analysis_level": 1,
    "activity": []
  }
]
```

Abfrage nach Metriken

Sie können Metriken über den REST API Explorer abfragen, um sicherzustellen, dass Sie den richtigen Anforderungstext konfiguriert haben, bevor Sie die Anfrage zu einem Skript hinzufügen.

1. Klicken Sie im REST API Explorer auf **Vermögenswerte**, und klicken Sie dann auf **POST /Metriken**.
2. klicken **Probiere es aus**.
3. In der Körper Feld, geben Sie die Metrik an, die Sie extrahieren möchten.

   Der folgende Text extrahiert beispielsweise Fünf-Minuten-Metriken zu HTTP-Antworten für einen Server mit der ID 1298:

   ```
   {
     "metric_category": "http_server",
     "metric_specs": [
       {
         "name": "rsp"
       }
     ],
     "object_type": "device",
     "object_ids": [
       1298
     ],
     "cycle": "5min"
   }
   ```

   Der Körper muss die folgenden Parameter enthalten:

   - **Objekttyp:** Der Objekttyp, für den Sie Metriken sammeln möchten.
   - **Objekt-IDs:** Die ID des Objekts, für das Sie Metriken extrahieren möchten.
   - **metrische_Kategorie:** Die Kategorie der Metrik, die Sie erfassen möchten.
   - **Name:** Der Name der Metrik, die Sie erfassen möchten.
   - **Zyklus:** Der Aggregationszeitraum für Metriken.
4. klicken **Anfrage senden** um die Anfrage an Ihren Sensor oder Ihre Konsole zu senden.

   In der Antwort des Servers Abschnitt, der Antworttext zeigt die angeforderten Metriken im JSON-Format an.

Rufen Sie das Python-Beispielskript ab und führen Sie es aus

Das ExtraHop GitHub-Repository enthält ein Python-Skript, das die Gesamtzahl der HTTP-Antworten extrahiert, die ein Server mit der ID 1298 in Zeitintervallen von fünf Minuten gesendet hat, und die Werte dann in eine CSV-Datei schreibt.

1. Gehe zum ExtraHop Codebeispiele GitHub-Repository und laden Sie das herunter `extract_metrics/extract_metrics.py` Datei auf Ihrem lokalen Computer.
2. Öffnen Sie in einem Texteditor den `extract_metrics.py` archivieren und ersetzen Sie die Konfigurationsvariablen durch Informationen aus Ihrer Umgebung.
   - Geben Sie für Sensoren und ECA-VMs die folgenden Konfigurationsvariablen an:
     - **GASTGEBER:** Die IP-Adresse oder der Hostname des Sensor oder der ECA-VM.
     - **API-SCHLÜSSEL:** Der API-Schlüssel.
   - Geben Sie für Reveal (x) 360 die folgenden Konfigurationsvariablen an:

- **GASTGEBER:** Der Hostname der Reveal (x) 360-API. Dieser Hostname wird auf der Reveal (x) 360 API Access-Seite unter API-Endpunkt angezeigt. Der Hostname beinhaltet nicht `/oauth2/token`.
- **ID:** Die ID der Reveal (x) 360-REST-API-Anmeldeinformationen.
- **GEHEIM:** Das Geheimnis der Reveal (x) 360 REST-API-Anmeldeinformationen.

3. Führen Sie den folgenden Befehl aus:

```
python3 extract_metrics.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)
```