

Erstellen Sie eine Gerätegruppe über die REST-API


Veröffentlicht: 2024-02-12

Sie können über die REST-API eine große Anzahl komplexer Gerätegruppen erstellen, indem Sie auf eine CSV-Datei verweisen, die aus einer Drittanwendung exportiert wurde. In diesem Thema zeigen wir Methoden zum Erstellen einer Gerätegruppe sowohl über den ExtraHop REST API Explorer als auch über ein Python-Skript.

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](#).)

Erstellen Sie eine Gerätegruppe über den REST API Explorer

 **Wichtig:** Der REST-API-Explorer ist auf Reveal (x) 360 nicht verfügbar.

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 **Gerätegruppe** und dann klicken **POST /Gerätegruppen**.
5. klicken **Probieren es aus**.
Das JSON-Schema wird automatisch dem Textfeld für den Body-Parameter hinzugefügt.
6. Geben Sie im Feld **Eigenschaften** für die Gerätegruppe an, die Sie erstellen möchten.
Der folgende Text erstellt beispielsweise eine Gerätegruppe, die CIDR-Blöcke enthält `192.168.0.0/26`, `192.168.0.64/27`, und `192.168.0.96/30`:

```
{
  "name": "New group",
  "description": "A newly created group",
  "filter": {
    "rules": [
      {
        "field": "ipaddr",
        "operand": "192.168.0.0/26",
        "operator": "="
      },
      {
        "field": "ipaddr",
        "operand": "192.168.0.64/27",
        "operator": "="
      },
      {
        "field": "ipaddr",
        "operand": "192.168.0.96/30",
        "operator": "="
      }
    ]
  }
}
```

```

        "operator": "="
    },
    "operator": "or"
}

```

7. klicken **Anfrage senden**.

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

Das ExtraHop GitHub-Repository enthält ein Python-Skript, das Gerätegruppen erstellt, indem es Kriterien aus einer CSV-Datei liest, die die folgenden Spezifikationen erfüllt:

1. Gehe zum [ExtraHop Codebeispiele GitHub-Repository](#) und laden Sie das herunter `create_device_groups/create_device_groups.py` Datei auf Ihrem lokalen Computer.
2. In dem Verzeichnis, das Sie kopiert haben `create_device_groups.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:

Name der Gerätegruppe	Beschreibung	IP-Adresse oder CIDR-Block
-----------------------	--------------	----------------------------

- Jede Spalte nach den ersten erforderlichen drei Spalten muss eine IP-Adresse oder einen CIDR-Block für die Gerätegruppe angeben.



Hinweis Sie können nicht mehr als 1000 IP-Adressen oder CIDR-Blöcke für eine Gerätegruppe angeben.



Hinweis Ein Beispiel für eine kompatible CSV-Datei finden Sie in der Datei `create_device_groups/device_group_list.csv` im GitHub-Repository für ExtraHop-Codebeispiele.

3. Öffnen Sie in einem Texteditor den `create_device_groups.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.
 - **CSV_DATEI**: Die Datei, die die Liste der Gerätegruppen enthält.
 - 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.
 - **CSV_DATEI**: Die Datei, die die Liste der Gerätegruppen enthält.
4. Führen Sie den folgenden Befehl aus:

```
python create_device_groups.py
```



Hinweis Wenn das Skript eine Fehlermeldung zurückgibt, dass die Überprüfung des SSL-Zertifikats 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)
```