Search for a device through the REST API

Published: 2020-06-08

You can search through all discovered devices on your ExtraHop system by specifying your criteria (such as IP address or discovery ID) and then export the list of devices and their associated metadata to a file format that is readable through a third-party application like Microsoft Excel or any CSV reader. For example, you might want to view and export the IP addresses of each VMware device on your network.

You can test device search queries before incorporating them into a script by running the queries in the ExtraHop REST API Explorer. This guide includes methods for both the REST API Explorer and a sample Python script.

Search for a device through the REST API Explorer

1. In a browser, navigate to the REST API Explorer.
   The URL is the hostname or IP address of your ExtraHop Discover or Command appliance, followed by `/api/v1/explore/`. For example, if your hostname is seattle-eda, the URL is `https://seattle-eda/api/v1/explore/`.
2. Click **Enter API Key** and then paste or type your API key into the API Key field.
3. Click **Authorize** and then click **Close**.
4. Click **Device** to display device operations.
5. Click **POST /devices/search**.
6. Click **Try it out**.
   The JSON schema is automatically added to the body parameter text box.
7. In the body text box, type your search criteria.
   The following search criteria returns a device with an IP address of 10.10.10.200:

```
{
  "filter": {
    "field": "ipaddr",
    "operand": "10.10.10.200",
    "operator": "="
  }
}
```

Python script example

The following example Python script searches for a list of devices by IP address. The script then outputs the ExtraHop discovery ID for each IP address.

The script includes the following configuration variables that you must replace with information from your environment:

HOST

The IP address or hostname of the Discover or Command appliance.

APIKEY

The API key generated from the Discover or Command appliance.

IP_ADDR_LIST

An array of IP addresses.

```
#!/usr/bin/python3

import json
```

```
import requests

HOST = 'https://extrahop.example.com'
APIKEY = '123456789abcdefghijklmnop'
IP_ADDR_LIST = [
                '10.10.10.200',
                '10.10.10.201',
                '10.10.10.202',
                '10.10.10.203'
                ]

def searchDevice(search):
    url = HOST + '/api/v1/devices/search'
    headers = {'Authorization': 'ExtraHop apikey=%s' % APIKEY}
    r = requests.post(url, headers=headers, verify=False,
 data=json.dumps(search))
    return r.json()[0]

for ip in IP_ADDR_LIST:
    search_filter = {
                      "filter": {
                        "field": "ipaddr",
                        "operand": ip,
                        "operator": "="
                      }
                    }
    device = searchDevice(search_filter)
    print(ip)
    print('    ' + device['discovery_id'])
```