Kennzeichnen Sie ein Gerät über die REST-API

Veröffentlicht: 2024-03-20

Mithilfe von Tags können Sie Geräte, die ein gemeinsames Merkmal aufweisen, aus potenziell Hunderten von erkannten Geräten in Ihrem Netzwerk klassifizieren.

Möglicherweise möchten Sie Geräte nach ihrer Rolle in Ihrem Netzwerk kennzeichnen, z. B. die Geräte, aus denen Ihre Entwicklungs- und Produktionsserver bestehen. Wenn Sie beispielsweise mehrere AWS-Instanzen in Ihrer Umgebung ausführen, ist es wichtig, diese entsprechend ihrer Arbeitslast zu dimensionieren. Eine zu kleine Instance kann zu schlechter Leistung führen; eine zu große Instance ist unnötig teuer. Wenn Sie Ihre AWS-Instances taggen, können Sie Gerätegruppen ganz einfach nach Instance-Größe einrichten und anschließend ein Dashboard zur Überwachung von Nutzungs- und Leistungsmetriken erstellen.

In diesem Handbuch erfahren Sie, wie Sie ein Tag erstellen, das Gerät finden, das Sie taggen möchten, und das Tag dann dem Gerät hinzufügen. Am Ende wird ein Beispielskript bereitgestellt, das allen aus einer CSV-Datei gelesenen IP-Adressen ein bestimmtes Geräte-Tag hinzufügt.

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.)

Einen Tag erstellen

Wenn Sie bereits ein Tag auf dem System haben, können Sie diesen Schritt überspringen. Das Beispielskript am Ende dieser Anleitung sucht nach einem Tag und erstellt nur bei Bedarf ein neues Tag.

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 **Schlagwort** und klicken Sie dann **Beitrag/Schlagworte**.
5. Klicken Sie **Probiere es aus**.
   Das JSON-Schema wird automatisch dem hinzugefügt Körper Parameter-Textfeld.
6. In der `name` Feld, ersetzen `string` mit dem neuen Tag-Namen.
7. Klicken Sie **Anfrage senden** um das Tag zu erstellen.

Rufen Sie Geräte ab, die Ihren Kriterien entsprechen

In diesem Schritt suchen Sie nach den Geräten, die Sie taggen möchten, und notieren sich die Geräte-ID. Sie benötigen die Geräte-ID, bevor Sie Geräte taggen können.

1. Scrollen Sie auf der Seite nach oben und klicken Sie auf **Gerät** um Geräteoperationen anzuzeigen.
2. klicken **POST /Geräte/Suche**.
3. klicken **Probiere es aus**.

Das JSON-Schema wird automatisch dem Textfeld für den Body-Parameter hinzugefügt.

4. Geben Sie in das Textfeld die Suchkriterien ein, mit denen die Geräte ausgewählt werden. Die folgenden Suchkriterien geben ein Gerät mit der IP-Adresse 10.10.10.200 zurück:

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

Weitere Informationen zu Gerätesuchfiltern finden Sie unter Operandenwerte für die Gerätesuche.

5. klicken **Anfrage senden**.

In der Antwort des Servers Abschnitt, der Antworttext zeigt Informationen zu jedem Gerät an, das Ihren Suchkriterien entspricht, einschließlich der Geräte-ID.

Weisen Sie das Tag einem Gerät zu

In diesem Schritt weisen Sie einem Gerät anhand der Geräte-ID, die Sie im vorherigen Schritt gefunden haben, ein Tag zu.

1. Scrollen Sie auf der Seite nach unten und klicken Sie **Tag** um Tag-Operationen anzuzeigen.
2. klicken **POST /tags/ {id} /devices/ {child-id}**.
3. klicken **Probiere es aus**.
4. In der Kind-ID Feld, geben Sie die ID des Gerät Sie taggen möchten.
5. In der id Feld, geben Sie die ID des Tags ein, das Sie zuweisen möchten.
6. klicken **Anfrage senden** um das Tag dem Gerät zuzuweisen.

Hinweis: Nachdem du geklickt hast **Anfrage senden**, können Sie auf die Tabs klicken , um Skripte für den Vorgang in Curl, Python 2.7 oder Ruby anzuzeigen.

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

Das ExtraHop GitHub-Repository enthält ein Python-Skript, das ein Geräte-Tag erstellt und das Tag dann allen Geräten mit den in einer CSV-Datei angegebenen IP-Adressen zuweist. Das Skript erstellt nur dann ein neues Tag, wenn das angegebene Tag noch nicht existiert.

1. Gehe zum ExtraHop Codebeispiele GitHub-Repository und laden Sie das herunter `tag_device/tag_device.py` Datei auf Ihrem lokalen Computer.
2. Öffnen Sie in einem Texteditor den `tag_device.py` archivieren und ersetzen Sie die folgenden 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.
     - **ETIKETT:** Der Name des Tags
     - **GERÄTELISTE:** Die Datei, die die Liste der IP-Adressen 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 enthält nicht `/oauth2/token`.

- **ID:** Die ID der Reveal (x) 360-REST-API-Anmeldeinformationen.
- **GEHEIM:** Das Geheimnis der Reveal (x) 360 REST-API-Anmeldeinformationen.
- **ETIKETT:** Der Name des Tags
- **GERÄTELISTE:** Die Datei, die die Liste der IP-Adressen enthält

3. Führen Sie den folgenden Befehl aus:

```
python3 tag_device.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)
```