Extraire la liste des équipements via l'API REST

Publié: 2024-07-18

L'API REST ExtraHop vous permet d'extraire la liste des appareils découverts par sonde ou console. En extrayant la liste à l'aide d'un script d'API REST, vous pouvez exporter la liste dans un format lisible par des applications tierces, comme une base de données de gestion des configurations (CMDB). Dans cette rubrique, nous montrons les méthodes permettant d'extraire une liste à la fois par le biais de la commande cURL et d'un script Python.

Avant de commencer

- Pour les capteurs et les machines virtuelles ECA, vous devez disposer d'une clé API valide pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Générer une clé API).
- Pour RevealX 360, vous devez disposer d'informations d'identification d'API REST valides pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Création d'informations d'identification pour l'API REST).

Récupérez la liste des équipements à l'aide de la commande cURL

La liste des appareils inclut toutes les métadonnées de l'équipement, telles que les adresses MAC et les identifiants des appareils. Cependant, vous pouvez filtrer la liste des appareils à l'aide d'un analyseur JSON pour extraire les informations spécifiques que vous souhaitez exporter. Dans cet exemple, la liste des équipements est récupérée puis filtrée avec l'analyseur jq pour extraire uniquement le nom d'affichage de chaque appareil.

Note: La procédure suivante n'est pas compatible avec l'API REST RevealX 360. Pour récupérer la liste des équipements depuis RevealX 360, voir Récupérez la liste des équipements depuis RevealX 360 à l'aide de la commande cURL.

Avant de commencer

- L'outil cURL doit être installé sur votre machine.
- L'analyseur jq doit être installé sur votre machine. Pour plus d'informations, voir https://stedolan.github.io/jq/.

Ouvrez une application de terminal et exécutez la commande suivante, où `YOUR_KEY` est l'API de votre compte utilisateur, `HOSTNAME` est le nom d'hôte de votre sonde ou console, et `MAX_DEVICES` est un nombre suffisamment élevé pour être supérieur au nombre total de périphériques découverts par votre système :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --header
 "accept: application/json" --header "Authorization: ExtraHop
 apikey=YOUR_KEY" --header "Content-Type: application/json" -d
 "{ \"active_from\": 1, \"active_until\": 0, \"limit\": MAX_DEVICES}" |
 jq -r '.[] | .display_name'
```

Note: Si la commande ne renvoie aucun résultat, assurez-vous que un certificat fiable a été ajouté à votre système ExtraHop. Vous pouvez également ajouter `--insecure` option pour récupérer la liste des équipements à partir d'un système ExtraHop sans certificat fiable ; cependant, cette méthode n'est pas sécurisée et n'est pas recommandée.

Conseil Vous pouvez ajouter `select(.analysis == "LEVEL")` option pour filtrer les résultats par niveau d'analyse. Par exemple, la commande suivante limite les résultats afin d'inclure uniquement les appareils sélectionnés pour une analyse avancée :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --
header "accept: application/json" --header "Authorization:
 ExtraHop apikey=YOUR_KEY" --header "Content-Type: application/
json" -d "{ \"active_from\": 1, \"active_until\": 0, \"limit\":
 1000000000}" | jq -r '.[] | select(.analysis == "advanced")
 | .display_name'
```

Conseil Vous pouvez ajouter `select(.critical == BOOLEAN)` option pour filtrer les résultats en fonction du champ critique. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils identifiés comme critiques par le système ExtraHop :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --
header "accept: application/json" --header "Authorization:
 ExtraHop apikey=YOUR_KEY" --header "Content-Type: application/
json" -d "{ \"active_from\": 1, \"active_until\": 0, \"limit
\": 1000000000}" | jq -r '.[] | select(.critical == true)
 | .display_name'
```

Conseil Vous pouvez ajouter `select(.cloud_instance_name != null)` option pour filtrer les résultats en fonction du champ de nom de l'instance cloud. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils dotés d'un nom d'instance cloud :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --
header "accept: application/json" --header "Authorization:
 ExtraHop apikey=YOUR_KEY" --header "Content-Type: application/
json" -d "{ \"active_from\": 1, \"active_until\": 0, \"limit
\": 1000000000}" | jq -r '.[] | select(.cloud_instance_name !=
 null) | .cloud_instance_name'
```

Récupérez la liste des équipements depuis RevealX 360 à l'aide de la commande cURL

La liste des appareils inclut toutes les métadonnées de l'équipement, telles que les adresses MAC et les identifiants des appareils. Cependant, vous pouvez filtrer la liste des appareils à l'aide d'un analyseur JSON pour extraire les informations spécifiques que vous souhaitez exporter. Dans cet exemple, la liste des équipements est récupérée puis filtrée avec l'analyseur jq pour extraire uniquement le nom d'affichage de chaque appareil.

Note: La procédure suivante est uniquement compatible avec l'API REST RevealX 360. Pour récupérer la liste des équipements à partir des capteurs et des machines virtuelles ECA, voir Récupérez la liste des équipements à l'aide de la commande cURL.

Avant de commencer

- L'outil cURL doit être installé sur votre machine.
- L'analyseur jq doit être installé sur votre machine. Pour plus d'informations, voir https://stedolan.github.io/jq/.

1. Ouvrez une application de terminal et exécutez la commande suivante, où REVEAL_X_360_REST_API est le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché dans RevealX 360 sur l'accès à l'API page sous API Endpoint. Le nom d'hôte n'inclut pas /oauth2/token:

```
HOST="https://REVEAL_X_360_REST_API"
```

2. Exécutez la commande suivante, où YOUR_ID est l'ID des informations dcessatives d'identification de l'API REST :

```
ID="YOUR_ID"
```

3. Exécutez la commande suivante, où YOUR_SECRET est le secret des informations dcessaires d'identification de l'API REST :

```
SECRET="YOUR_SECRET"
```

4. Exécutez la commande suivante :

```
AUTH=$(printf "$ID:$SECRET" | base64 --wrap=0)
```

5. Exécutez la commande suivante :

```
ACCESS_TOKEN=$(curl -s \
    -H "Authorization: Basic ${AUTH}" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    --request POST \
     ${HOST}/oauth2/token \
    -d "grant_type=client_credentials" \
    | jq -r '.access_token')
```

6. Exécutez la commande suivante, où MAX_DEVICES est un nombre suffisamment élevé pour être supérieur au nombre total de périphériques découverts par votre système :

```
curl -s -X GET -H "Authorization: Bearer ${ACCESS_TOKEN}"  "$HOST/api/
v1/devices?active_from=1&active_until=0&limit=MAX_DEVICES" | jq -r '.[]
 | .display_name'
```

Conseil Vous pouvez ajouter `select(.analysis == "LEVEL")` option pour filtrer les résultats par niveau d'analyse. Par exemple, la commande suivante limite les résultats afin d' inclure uniquement les appareils sélectionnés pour une analyse avancée :

```
curl -s -X GET -H "Authorization: Bearer
 ${ACCESS_TOKEN}"  "$HOST/api/v1/devices?
active_from=1&active_until=0&limit=10000000000" | jq -r '.[] |
 select(.analysis == "advanced") | .display_name'
```

Conseil Vous pouvez ajouter `select(.critical == BOOLEAN)` option pour filtrer les résultats en fonction du champ critique. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils identifiés comme critiques par le système ExtraHop :

```
curl -s -X GET -H "Authorization: Bearer
 ${ACCESS_TOKEN}"  "$HOST/api/v1/devices?
active_from=1&active_until=0&limit=10000000000"  | jq -r '.[] |
 select(.critical == true) | .display_name'
```

Conseil Vous pouvez ajouter `select(.cloud_instance_name != null)` option pour filtrer les résultats en fonction du champ de nom de l'instance cloud. Par exemple, la

commande suivante limite les résultats pour inclure uniquement les appareils dotés d'un nom d'instance cloud :

```
curl -s -X GET -H "Authorization: Bearer
 ${ACCESS_TOKEN}"  "$HOST/api/v1/devices?
active_from=1&active_until=0&limit=10000000000"  | jq -r '.[] |
 select(.cloud_instance_name != null) | .cloud_instance_name'
```

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait la liste des équipements, y compris toutes les métadonnées de l'équipement, et écrit la liste dans un fichier CSV situé dans le même répertoire que le script.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `extract_device_list/extract_device_list.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez le `extract_device_list.py` archivez et remplacez les variables de configuration par des informations provenant de votre environnement.
   - Pour les capteurs et les machines virtuelles ECA, spécifiez les variables de configuration suivantes :
     - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la machine virtuelle ECA.
     - **CLÉ_API:** La clé API.
     - **FICHIER_CSV:** Fichier contenant la liste des groupes d'équipements.
     - **NOM DE FICHIER:** Le fichier dans lequel la sortie sera écrite
     - **LIMITE:** Le nombre maximum d'appareils à récupérer avec chaque requête GET
     - **SAVEL2:** Récupère les appareils parents L2. Cette variable n'est valide que si vous avez activé le système ExtraHop pour détecter les appareils par adresse IP.
     - **AVANCÉ_UNIQUEMENT:** Récupère uniquement les appareils qui font actuellement l'objet d'une analyse avancée
     - **HAUTE_VALEUR_UNIQUEMENT:** Récupère uniquement les appareils considérés comme ayant une valeur élevée
   - Pour RevealX 360, spécifiez les variables de configuration suivantes :
     - **HÔTE:** Le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché sur la page d'accès à l'API RevealX 360 sous API Endpoint. Le nom d'hôte n'inclut pas `/oauth2/token`.
     - **IDENTIFIANT:** L'ID des informations d'identification de l'API REST RevealX 360.
     - **SECRET:** Le secret des informations d'identification de l'API REST RevealX 360.
     - **FICHIER_CSV:** Fichier contenant la liste des groupes d'équipements.
     - **NOM DE FICHIER:** Le fichier dans lequel la sortie sera écrite
     - **LIMITE:** Le nombre maximum d'appareils à récupérer avec chaque requête GET
     - **SAVEL2:** Récupère les appareils parents L2. Cette variable n'est valide que si vous avez activé le système ExtraHop pour détecter les appareils par adresse IP.
     - **AVANCÉ_UNIQUEMENT:** Récupère uniquement les appareils qui font actuellement l'objet d'une analyse avancée
     - **HAUTE_VALEUR_UNIQUEMENT:** Récupère uniquement les appareils considérés comme ayant une valeur élevée
3. Exécutez la commande suivante :

```
python3 extract_device_list.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat SSL a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

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