Rechercher un équipement via l'API REST

Publié: 2024-04-10

Vous pouvez effectuer une recherche parmi tous les appareils découverts sur votre sonde ou console en spécifiant vos critères (tels que l'adresse IP ou l'identifiant de découverte), puis en exportant la liste des appareils et leurs métadonnées associées dans un format de fichier lisible via une application tierce telle que Microsoft Excel ou un lecteur CSV. Par exemple, vous souhaiterez peut-être consulter et exporter les adresses IP de chaque équipement VMware de votre réseau.

Vous pouvez tester les requêtes de recherche sur les équipements avant de les intégrer dans un script en les exécutant dans l' explorateur d'API REST ExtraHop. Ce guide inclut des méthodes pour l'explorateur d' API REST et un exemple de script Python.

Avant de commencer

- Pour les capteurs et les machines virtuelles ECA, vous devez disposer d'une clé d'API valide pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Génération d'une clé d'API.)
- Pour Reveal (x) 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.)

Rechercher un équipement via l'explorateur d'API REST

1. Dans un navigateur, accédez à l'explorateur d'API REST.
   L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi de `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans le Clé API champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **Appareil** pour afficher le fonctionnement de l'équipement.
5. Cliquez **POST /dispositifs/search**.
6. Cliquez **Essayez-le**.
   Le schéma JSON est automatiquement ajouté à la zone de texte du paramètre du corps.
7. Dans le corps du texte, saisissez vos critères de recherche.
   Les critères de recherche suivants renvoient un équipement dont l'adresse IP est 10.10.10.200 :

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

   Pour plus d'informations sur les filtres de recherche d'équipements, voir Valeurs d'opérandes pour la recherche d'équipements.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui recherche une liste d'appareils par adresse IP. Le script génère ensuite l'ID de découverte ExtraHop pour chaque adresse IP.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `search_device/search_device.py` fichier sur votre machine locale.

2. Dans un éditeur de texte, ouvrez `search_device.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.
     - **LISTE_ADRESSES IP:** Tableau d'adresses IP.
   - Pour Reveal (x) 360, spécifiez les variables de configuration suivantes :
     - **HÔTE:** Le nom d'hôte de l'API Reveal (x) 360. Ce nom d'hôte est affiché sur la page d'accès à l'API Reveal (x) 360 sous API Endpoint. Le nom d'hôte n'inclut pas `/oauth2/token`.
     - **IDENTIFIANT:** L'ID des informations d'identification de l'API REST Reveal (x) 360.
     - **SECRET:** Le secret des informations d'identification de l'API REST Reveal (x) 360.
     - **LISTE_ADRESSES IP:** Tableau d'adresses IP.
3. Exécutez la commande suivante :

```
python3 search_device.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 le `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)
```