Création d'un groupe dveloppement d'équipements via l'API REST

Publié: 2024-09-26

Vous pouvez créer un grand nombre de groupes d'équipements complexes via l'API REST en référençant un fichier CSV exporté depuis une application tierce. Dans cette rubrique, nous présentons les méthodes permettant de créer un groupe dveloppements via l'explorateur d'API REST ExtraHop et 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).

Création d'un groupe dveloppement d'équipements 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 par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Entrez les informations d'identification de votre API REST.
   - Pour les capteurs et les machines virtuelles ECA, cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans le **Clé API** champ.
   - Pour RevealX 360, cliquez sur **Entrez les identifiants de l'API** puis collez ou saisissez l'ID et le code secret de vos informations diciatives d'API dans le **IDENTIFIANT** et **Secret** champs.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **Groupe d'appareils** puis cliquez sur **POST /groupes d'appareils**.
5. Cliquez **Essayez-le**.

   Le schéma JSON est automatiquement ajouté à la zone de texte du paramètre du corps.
6. Dans le champ du corps, spécifiez les propriétés du groupe dproximatif d'équipements que vous souhaitez créer.

   Par exemple, le corps suivant crée un groupe dproximatif d'équipements qui inclut des blocs CIDR `192.168.0.0/26`, `192.168.0.64/27`, et `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": "or"
    }
}
```

7. Cliquez **Envoyer la demande**.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui crée des groupes d'équipements en lisant des critères à partir d'un fichier CSV répondant aux spécifications suivantes :

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `create_device_groups/create_device_groups.py` fichier sur votre machine locale.
2. Dans le répertoire où vous avez copié `create_device_groups.py` pour créer un fichier CSV répondant aux spécifications suivantes :
   - Le fichier CSV ne doit pas contenir de ligne d'en-tête.
   - Chaque ligne du fichier CSV doit contenir les trois colonnes suivantes dans l'ordre indiqué :

Nom du groupe d'appareils	Descriptif	adresse IP ou bloc CIDR

   - Chaque colonne située après les trois premières colonnes requises doit spécifier une adresse IP ou un bloc CIDR pour le groupe dproximatif d'équipements.

     Note: Vous ne pouvez pas spécifier plus de 1 000 adresses IP ou blocs CIDR pour un groupe dproximatif d' équipements.

   Note: Pour un exemple de fichier CSV compatible, consultez le fichier create_device_groups/device_group_list.csv dans le référentiel GitHub ExtraHop code-examples.
3. Dans un éditeur de texte, ouvrez `create_device_groups.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.
   - 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.
4. Exécutez la commande suivante :

```
python create_device_groups.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS 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)
```