

Spécifiez les appareils à valeur élevée via l'API REST

Publié: 2024-09-26

L'API REST ExtraHop vous permet de spécifier qu'un équipement a une valeur élevée. Vous pouvez spécifier l'équipement via l'explorateur d'API REST ou automatiser la procédure en lisant les critères de l'équipement à partir d'un fichier CSV ou similaire via un script d'API REST.

Avant de commencer

- 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](#)).
- 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](#)).

Spécifiez un équipement à valeur élevée via l'explorateur d'API REST

Récupérez l'ID de l'équipement

Avant de pouvoir spécifier un équipement à valeur élevée, vous devez récupérer l'ID d'API REST de l'appareil.

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 d'identification d'API dans le **IDENTIFIANT** et **Secret** champs.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **POST /dispositifs/search**.
5. Cliquez **Essayez-le**.

Le schéma JSON est automatiquement ajouté à la zone de texte du paramètre du corps.

6. Dans la zone de texte du corps, saisissez les critères de recherche qui sélectionnent l'équipement. 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](#).

7. Cliquez **Envoyer la demande**.

Dans la section Corps de la réponse, notez `id` champ de l'équipement.

Spécifiez un équipement de valeur élevée

1. Cliquez **PATCH /appareils/ {id}**.
2. Cliquez **Essayez-le**.
3. Dans le **corps** dans le champ, saisissez l'objet JSON suivant :

```
{
  "custom_criticality": "critical"
}
```

4. Dans le **identifiant** dans ce champ, saisissez l'ID de l'équipement qui **que vous avez récupéré lors de la procédure précédente**.
5. Cliquez **Envoyer une demande**.
Si la demande aboutit, un code de réponse 204 apparaît dans la section Réponse du serveur.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui lit une liste d'adresses IP à partir d'un fichier CSV et spécifie tous les appareils dont ces adresses ont une valeur élevée .

1. Accédez au [Référentiel GitHub d'exemples de code ExtraHop](#) et téléchargez le contenu du `specify_high_value` répertoire sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `ip_list.csv` archivez et remplacez les adresses IP par les adresses IP des appareils que vous souhaitez spécifier comme valeur élevée.
3. Dans un éditeur de texte, ouvrez `specify_high_value.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.
 - 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.
4. Exécutez la commande suivante :

```
python3 specify_high_value.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)
```