Connectez-vous à Reveal (x) 360 à partir de capteurs autogérés via l'API REST

Publié: 2024-03-27

L'API REST ExtraHop vous permet d'automatiser les connexions pour un grand nombre de sites autogérés capteurs pour Reveal (x) 360 à l'aide d'un script. Autogéré capteurs inclure des appliances ou des instances Discover sur site déployées sur des fournisseurs de services cloud tels qu' AWS, Azure et Google Cloud Platform (GCP).

Ce guide fournit des instructions pour l'explorateur d'API REST, afin que vous puissiez tester l' opération REST, ainsi qu'un exemple de script Python que vous pouvez modifier avec vos variables d'environnement.

Note: Vous ne pouvez pas connecter les appliances Trace via l'API REST. Pour plus d'informations sur la connexion des appliances Trace, voir Connectez-vous à Reveal (x) 360 à partir de capteurs autogérés.

Avant de commencer

- Familiarisez-vous avec les Guide de l'API REST ExtraHop pour savoir comment naviguer dans l' explorateur d'API REST ExtraHop.
- Vous devez disposer des privilèges d'administration du système et des accès pour configurer Reveal (x) 360. Les détails relatifs à la configuration de ce compte se trouvent dans l'e-mail d'introduction envoyé par ExtraHop Networks.
- Vous devez générer des jetons via Reveal (x) 360 pour chaque sonde que vous souhaitez connecter. Pour plus d'informations, voir Connectez-vous à Reveal (x) 360 à partir de capteurs autogérés.
- Vous devez vous connecter au sonde avec un compte doté des privilèges d'administration du système et des accès pour générer une clé API.
- Vous devez disposer d'une clé API valide pour apporter des modifications via l'API REST et suivre les procédures ci-dessous. (Voir Génération d'une clé d'API).

Connectez-vous à Reveal (x) 360 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 d'API** puis collez ou saisissez votre clé d'API dans **Clé d'API** champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **Nuage** puis cliquez sur **POST/cloud/connect**.
5. Cliquez **Essayez-le**.
6. Dans le champ dédié au corps, remplacez `string` avec le jeton que vous avez généré à partir de Reveal (x) 360, comme illustré dans l'exemple suivant :

   ```
   {
       "cloud_token": "561b85-e9092a3a-343fcb03-78c72777-8db70bbd"
   }
   ```

   La section Réponse du serveur affiche le code dstatus 201.

Exemple de script Python

Le dépôt GitHub d'ExtraHop contient un exemple de script Python qui connecte votre sonde vers Reveal (x) 360 en lisant des jetons et des clés d'API à partir d'un fichier CSV.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `self-managed-sensor-rx360-connect/self-managed-sensor-rx360-connect.py` fichier sur votre machine locale.
2. Dans le répertoire où vous avez copié `self-managed-sensor-rx360-connect.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 :

Le sonde nom d'hôte	Le sonde Clé d'API	Le jeton que vous avez généré à partir de Reveal (x) 360

   - Le fichier CSV doit être nommé `sensors.csv` et stockées dans le même répertoire que le script.

   Note: Pour un exemple de fichier CSV compatible, consultez le fichier self-managed-sensor-rx360-connect/sensors.csv dans le référentiel GitHub d' exemples de code ExtraHop.
3. Exécutez la commande suivante :

```
python self-managed-sensor-rx360-connect.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)
```