# Requête d'enregistrements via l'API REST

Publié: 2024-06-04

L'API REST ExtraHop vous permet de rechercher des enregistrements stockés sur un espace de stockage des enregistrements. En interrogeant des enregistrements à l'aide d'un script d'API REST, vous pouvez importer des enregistrements dans une application tierce, telle que Microsoft Excel. En outre, si votre requête correspond à un nombre d'enregistrements supérieur au nombre maximal d'enregistrements renvoyés par l'API REST, vous pouvez configurer le script pour qu'il recherche de manière récursive les enregistrements restants. Dans cette rubrique, nous présentons des méthodes permettant d'interroger des enregistrements via l' explorateur d'API REST ExtraHop et un script Python.

**Avant de commencer**

- Vous devez vous connecter au sonde ou console avec un compte disposant de tous les privilèges d'écriture nécessaires pour générer une clé d'API.
- 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.)
- Familiarisez-vous avec Guide de l' API REST ExtraHop pour apprendre à naviguer dans l'explorateur d'API REST d'ExtraHop.

## Interrogez des enregistrements 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 **Journal d'enregistrement** puis cliquez sur **POST /enregistrements/recherche**.
5. Cliquez **Essayez-le**.
   Le schéma JSON est automatiquement ajouté au corps zone de texte des paramètres.
6. Dans la zone de texte du corps, spécifiez les champs pour votre requête d'enregistrement.

   Par exemple, les champs suivants récupèrent les enregistrements des 30 dernières minutes qui incluent une adresse IP, un nom de domaine ou un URI identifié comme suspect selon renseignement sur les menaces:

```
{
    "from": "-30m",
    "filter": {
        "field": "ex.isSuspicious",
        "operator": "=",
        "operand": {
            "type": "boolean",
            "value": "true"
        }
    }
}
```

   Pour une liste complète des champs valides, consultez la section Paramètres du corps sous **POST / enregistrements/recherche** dans l' explorateur d'API REST.

## Exemples de scripts Python

Les scripts Python suivants recherchent des enregistrements contenant une adresse IP, un nom de domaine ou un URI qui ont été identifiés comme suspects selon les renseignements sur les menaces. Les scripts écrivent ensuite les champs d'enregistrement spécifiés dans un fichier CSV qui peut être consulté dans un tableur.

**Note:** Pour en savoir plus sur les renseignements sur les menaces avec ExtraHop, voir Renseignements sur les menaces et Téléchargez des fichiers STIX via l'API REST.

### Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements ExtraHop

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait des enregistrements d'un espace de stockage des enregistrements ExtraHop.

**Important:** Si la requête correspond à un nombre supérieur au nombre maximum d'enregistrements pouvant être récupérés simultanément, le script extrait les enregistrements restants en envoyant un curseur à la sonde ou à la console avec l'opération POST /records/cursor. Cette opération n'est valide qu'avec l'espace de stockage des enregistrements ExtraHop. Si vous avez configuré un espace de stockage des enregistrements tiers ou dans le cloud, voir Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements tiers ou dans le cloud.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `query_records_explore/query_records_explore.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez le `query_records_explore.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :

   • **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console. Notez que ce nom d'hôte n'est pas le nom d'hôte de l'espace de stockage des enregistrements ExtraHop connecté sur lequel les enregistrements sont stockés.

   • **APIKEY:** La clé d'API.

   • **NOM DE FICHIER:** Le fichier dans lequel la sortie est écrite.

   • **TIME_LIMIT:** Si la requête d'enregistrement correspond à plus de 100 enregistrements, délai après la requête initiale pendant lequel les enregistrements restants peuvent être extraits du système.

   • **REQUÊTE:** Les paramètres de requête d'enregistrement.

   • **COLONNES:** Les champs d'enregistrement qui sont écrits dans le fichier de sortie CSV.
3. Exécutez la commande suivante :

```
python3 query_records_explore.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)
```

## Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements tiers ou dans le cloud

Le référentiel GitHub ExtraHop contient un exemple de script Python qui récupère des enregistrements à partir de magasins de disques tiers et dans le cloud.

**Note:** Si la requête correspond à un nombre supérieur au nombre maximum d'enregistrements pouvant être récupérés simultanément, le script récupère les enregistrements restants en envoyant des demandes supplémentaires avec le `offset` paramètre. Le paramètre offset ignore un certain nombre d'enregistrements dans une requête.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `query_records_third_party/query_records_third_party.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `query_records_third_party.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :
   - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console.
   - **APIKEY:** La clé API.
   - **NOM DE FICHIER:** Le fichier dans lequel la sortie est écrite.
   - **LIMITE:** Le nombre maximum d'enregistrements à récupérer à la fois.
   - **REQUÊTE:** Les paramètres de requête d'enregistrement.
   - **COLONNES:** Les champs d'enregistrement qui sont écrits dans le fichier de sortie CSV.
3. Exécutez la commande suivante :

```
python3 query_records_third_party.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)
```