Extraire des métriques via l'API REST

Publié: 2024-02-13

Vous pouvez extraire des métriques d'un sonde ou console via l'API REST pour visualiser les métriques dans un outil tiers ou comparer les données ExtraHop avec d'autres données que vous avez collectées. Pour extraire une métrique, vous devez d'abord obtenir des identifiants pour les métriques que vous souhaitez extraire et pour les objets pour lesquels vous souhaitez extraire des métriques. Vous pouvez ensuite créer et tester une requête métrique dans l'explorateur d' API REST avant d'intégrer votre demande dans un script capable de lire les métriques dans un format pouvant être importé dans des applications.

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.)

Récupérer les identifiants métriques

Les métriques sont identifiées dans l'API REST ExtraHop grâce à une combinaison des `metric_category`, le `name`, et le `object_type`. Vous pouvez récupérer les trois identifiants via le Metric Explorer.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Catalogue métrique**.
3. Dans le Type pour filtrer un champ, tapez le nom de la métrique que vous souhaitez extraire, puis cliquez sur le nom de la métrique dans les résultats de recherche ci-dessous.
4. Dans le volet droit, faites défiler l'écran jusqu'aux paramètres de l'API REST et enregistrez les valeurs.

   Par exemple, les informations suivantes sont affichées pour la métrique des réponses du serveur HTTP :

REST API Parameters

```
{
    "metric_category": "http_server",
    "object_type": "device",
    "metric_specs": [
        {
            "name": "rsp"
        }
    ]
}
```

Récupérer les identifiants d'objets

Vous devez ensuite trouver l'identifiant unique de l'objet pour lequel vous souhaitez extraire des métriques dans l'API REST. Vous pouvez récupérer cet identifiant via l' explorateur d'API REST.

Important: L'explorateur d'API REST n'est pas disponible sur Reveal (x) 360.

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 sur le type d'objet pour lequel vous souhaitez collecter des métriques, tel que **Appareil**, **Groupe d'appareils**, **Demande**, ou **Appareil**.
5. Cliquez **OBTENEZ/<objects>**.

   Par exemple, si vous extrayez des métriques pour un groupe de déquipements, cliquez sur **Groupes d'obtentions/d'appareils**.
6. Cliquez **Essayez-le**.
7. Optionnel : Dans le Paramètres section, spécifiez les critères de recherche pour l' objet que vous souhaitez localiser.

   Par exemple, vous pouvez rechercher des noms d'objets, des adresses IP ou des adresses MAC. Si vous éprouvez des difficultés à localiser un équipement, voir Trouvez un équipement.
8. Cliquez **Envoyer une demande**.

   Dans le Réponse du serveur section, la Organisme de réponse affiche des informations sur chaque objet correspondant aux critères de recherche.
9. Notez le numéro indiqué dans le champ d'identification de l'objet pour lequel vous souhaitez collecter des métriques .

   Par exemple, l'identifiant du serveur suivant est 1298 :


```
[
  {
    "mod_time": 1516639693474,
    "node_id": null,
    "id": 1298,
    "extrahop_id": "fff4c3090a0a0000",
    "discovery_id": "fff4c3090a0a0000",
    "display_name": "server1",
    "description": null,
    "user_mod_time": 1512688149084,
    "discover_time": 1498685400000,
    "vlanid": 0,
    "parent_id": 140,
    "macaddr": "A1:01:01:01:1A:01",
    "vendor": "Mellanox",
    "is_l3": true,
    "ipaddr4": "10.10.10.200",
    "ipaddr6": null,
    "device_class": "node",
    "default_name": "Mellanox 10.10.10.200",
    "custom_name": "server1",
    "cdp_name": "",
    "dhcp_name": "server1.company.com",
    "netbios_name": "",
    "dns_name": "server1.company.com",
    "custom_type": "",
    "analysis_level": 1,
    "activity": []
  }
]
```

Requête de métriques

Vous pouvez interroger des métriques via l'explorateur d'API REST pour vous assurer que vous avez configuré le bon corps de demande avant de l'ajouter à un script.

Important: L'explorateur d'API REST n'est pas disponible sur Reveal (x) 360.

1. Dans l'explorateur d'API REST, cliquez sur **Actifs**, puis cliquez sur **POST /métriques**.
2. Cliquez **Essayez-le**.
3. Dans le corps champ, spécifiez la métrique que vous souhaitez extraire.

   Par exemple, le corps suivant extrait des métriques de cinq minutes relatives aux réponses HTTP d'un serveur dont l'ID est 1298 :

   ```
   {
     "metric_category": "http_server",
     "metric_specs": [
       {
         "name": "rsp"
       }
     ],
     "object_type": "device",
     "object_ids": [
       1298
     ],
     "cycle": "5min"
   }
   ```

   Le corps doit inclure les paramètres suivants :

   - **type_objet:** Type d'objet pour lequel vous souhaitez collecter des métriques.
   - **identifiant_objets:** L'identifiant de l'objet pour lequel vous souhaitez extraire des métriques.
   - **catégorie_métrique:** Catégorie de la métrique que vous souhaitez collecter.
   - **nom:** Nom de la métrique que vous souhaitez collecter.
   - **cycle:** Période d'agrégation pour les métriques.
4. Cliquez **Envoyer une demande** pour envoyer la demande à votre sonde ou à votre console.

   Dans le Réponse du serveur section, la Organisme de réponse affiche les métriques demandées au format JSON.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait le nombre total de réponses HTTP envoyées par un serveur avec un ID de 1298 sur des intervalles de cinq minutes, puis écrit les valeurs dans un fichier CSV.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `extract_metrics/extract_metrics.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez le `extract_metrics.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 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.

3. Exécutez la commande suivante :

```
python3 extract_metrics.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat SSL a échoué, assurez-vous que un certificat de confiance a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter le `verify=False` possibilité 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 de certificat :

```
requests.get(url, headers=headers, verify=False)
```