Hop supplémentaire

Configurer un flux de données ouvert pour envoyer des données métriques à AWS Cloudwatch

Publié: 2023-09-14

Le système ExtraHop fournit plusieurs outils pour visualiser et surveiller les métriques relatives aux données de votre réseau. Toutefois, vous souhaiterez peut-être stocker ou analyser des données métriques à l'aide d'un outil tiers distant, tel que Splunk, MongoDB ou Amazon Web Services (AWS). Le flux de données ouvert La fonctionnalité (ODS) vous permet de configurer une connexion à un outil tiers via lequel vous pouvez envoyer des données métriques spécifiées.

Dans cette procédure pas à pas, vous allez configurer une cible ODS pour Amazon CloudWatch, écrire un déclencheur qui spécifie les métriques HTTP à envoyer et lancer la transmission des données vers la cible.

Prérequis

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de privilèges d'administration du système et des accès.
- Votre système ExtraHop doit disposer de données réseau avec le trafic du serveur Web.
- Vous devez disposer d'un compte Amazon Web Services et être familiarisé avec le service CloudWatch .
- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant le Flux de données ouverts section du Guide de l'interface utilisateur ExtraHop Admin et le déclencheurs sujet.
- Familiarisez-vous avec les processus de création de déclencheurs en remplissant le Procédure pas à pas du déclencheur.

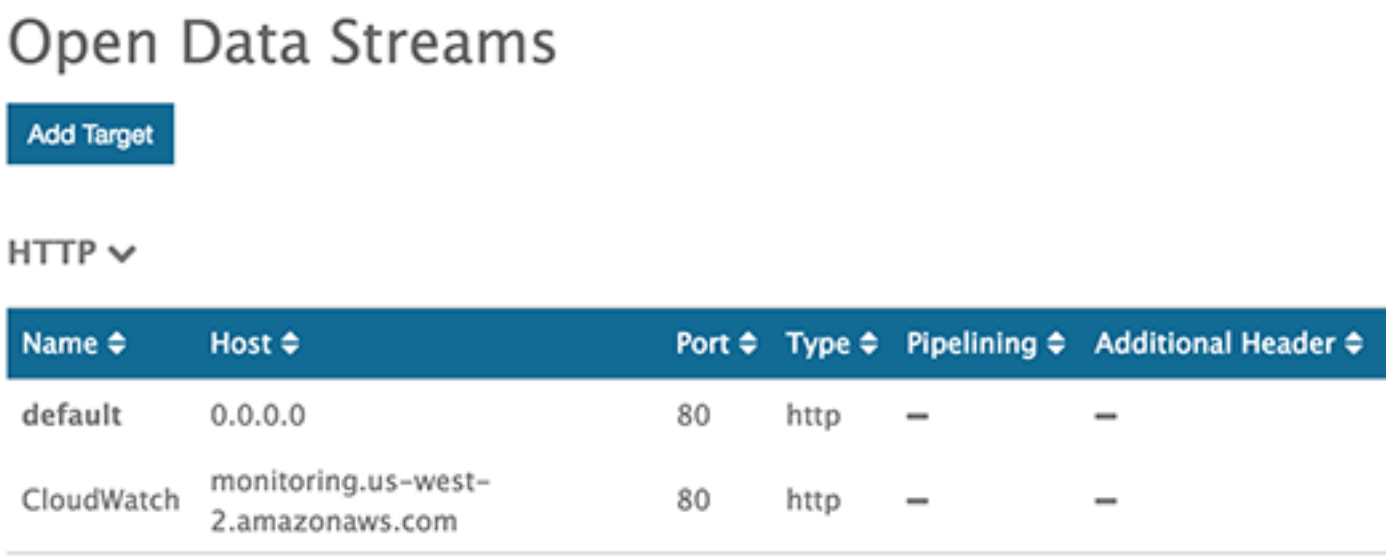
Configuration d'une cible ODS

Dans les étapes suivantes, vous allez configurer l'hôte, le port et la méthode dauthentication pour une cible de flux de données ouvert HTTP.

1. Connectez-vous au système ExtraHop à partir duquel vous souhaitez envoyer des données avec un compte doté de privilèges d'administration du système et des accès.
2. Cliquez sur Réglages du système icône, puis cliquez sur **Toute l'administration**.
3. À partir du Configuration du système section, cliquez **Flux de données ouverts**.
4. Cliquez **Ajouter une cible**.
5. Sélectionnez **HTTP** à partir du Type de cible liste déroulante.
6. Dans le Nom champ, type `Cloud Watch`.
7. Dans le Hôte dans ce champ, saisissez l'adresse IP ou le nom d'hôte du serveur Web Amazon auquel vous souhaitez envoyer des données.
8. Dans le Port champ, type 443 pour le numéro de port par lequel vous souhaitez envoyer des données.
9. Dans le Type champ, sélectionnez **HTTPS** comme transfert protocole vous souhaitez envoyer des données.
10. Dans le Authentification champ, sélectionnez **Amazon AWS**.
11. Dans le ID de clé d'accès dans ce champ, saisissez la clé d'accès à votre compte AWS.

12. Dans le Clé secrète dans ce champ, saisissez la clé secrète de votre compte AWS.
13. Dans le Service champ, saisissez le point d'entrée pour le service CloudWatch, tel que la surveillance.
14. Dans le Région dans ce champ, saisissez la région du service CloudWatch, par exemple us-west-2.
15. Dans le Méthode champ, sélectionnez **POSTE** comme méthode REST que le déclencheur appellera lors de l'envoi de données.
16. Cliquez **Enregistrer**.

La cible est ajoutée à la table HTTP sur la page Open Data Stream, comme dans la figure suivante :



Testez la configuration ODS

Dans les étapes suivantes, vous allez écrire une requête HTTP REST pour tester la transmission de données du système ExtraHop vers le compte AWS.

Comme configuré dans la section précédente, la demande de test applique la méthode POST.

1. Dans le HTTP tableau, cliquez **Modifier** pour ouvrir la cible CloudWatch.
2. Dans le Options dans ce champ, copiez et collez le code de requête HTTP REST suivant pour envoyer une métrique appelée « Test » d'une valeur de 4 octets au service CloudWatch :

```
{
    "path": "/",
        "payload":
 "Action=PutMetricData&Version=2010-08-01&Namespace=test&MetricData.member.1.MetricN
           "headers": {
               "Content-Type": [
                   "application/x-www-form-urlencoded"
               ]
           }
}
```

Conseil Pour en savoir plus sur la syntaxe de la requête HTTP REST, consultez le Remote.HTTP section du Référence de l'API ExtraHop Trigger.

3. Cliquez **Enregistrer**.
4. Dans le HTTP table, passez le curseur sur l'état de la cible pour afficher l'activité de connexion.

Si le test est réussi, la fenêtre affiche le nombre de messages et d'octets envoyés et reçus ainsi que le nombre de tentatives de connexion, comme dans la figure suivante :

Écrire le déclencheur ODS

Dans les étapes suivantes, vous allez écrire un déclencheur qui spécifie les métriques à envoyer au service CloudWatch et qui contient la commande permettant d'envoyer des données métriques via le flux de données ouvert.

Conseil: Lorsque vous créez le déclencheur dans cette procédure, ajoutez des commentaires décrivant l'objectif d'un extrait de code, les restrictions ou les meilleures pratiques.

1. Cliquez sur le logo ExtraHop dans le coin supérieur gauche pour revenir au système ExtraHop .
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Dans le Nom champ, type `Métriques pour CloudWatch`.
5. Cliquez **Activer le journal de débogage**.
6. Dans le Évènements champ, sélectionnez **HTTP_RESPONSE**.
7. Dans le volet droit, ajoutez le code déclencheur suivant à l'éditeur pour spécifier « ExtraHop » comme espace de noms personnalisé pour les données métriques qui seront affichées par le service CloudWatch :

```
let namespace = 'ExtraHop';
```

Note: La valeur de l'espace de noms ne peut pas être « AWS ».

8. Ajoutez le code déclencheur suivant au script existant pour spécifier le nom de la cible ODS que vous avez configurée précédemment :

```
let target = 'CloudWatch';
```

9. Ajoutez le code déclencheur suivant au script existant pour spécifier les métriques à transmettre au service CloudWatch :

```
let metrics = [
    {
        'MetricName': 'processingTime',
        'Unit': 'Milliseconds',
        'Value' : HTTP.processingTime
    },
    {
        'MetricName': 'rspSize',
        'Unit': 'Bytes',
        'Value' : HTTP.rspSize
    }
];
```

10. Ajoutez le code déclencheur suivant au script existant pour spécifier la structure de la charge utile, qui est définie par `PutMetricData` méthode dans le API Amazon CloudWatch :

```
let payload = 'Action=PutMetricData&Version=2010-08-01&Namespace=' +
 namespace;

let i,
    count = 0;

for (i = 0; i < metrics.length; i++) {
    let idx = i + 1,
        metric = metrics[i],
        val = metric.Value,
        attr;

    // If the metric value is NaN, do not publish.
    if (Number.isNaN(val)) {
        continue;
    }

    for (attr in metric) {
        payload += '&MetricData.member.' + idx + '.' +
            encodeURIComponent(attr) + '=' +
            encodeURIComponent(metric[attr]);
    }
    count++;
}

if (count == 0) {
    // No metrics to publish.
    return;
}
```

11. Ajoutez le code déclencheur suivant au script existant pour définir la requête HTTP REST qui spécifie le chemin de la demande, les en-têtes et la charge utile :

```
let req = {
    'path': '/',
    'headers': {
        'Content-Type': 'application/x-www-form-urlencoded'
    },
    'payload': payload
};
```

Ce code est similaire à la demande de test que vous avez effectuée dans la procédure précédente.

12. Ajoutez le code déclencheur suivant au script existant pour spécifier la cible ODS et lancer la demande de transmission de données métriques vers cette cible :

```
Remote.HTTP(target).post(req);
```

13. Cliquez **Enregistrer**.

Attribuer le déclencheur ODS à un équipement

Avant que le déclencheur puisse envoyer des données métriques au service CloudWatch, vous devez attribuer le déclencheur à au moins un équipement. Pour cette procédure pas à pas, vous allez attribuer le déclencheur à un seul serveur HTTP dans un groupe d'équipements.

Lorsque vous créez vos propres déclencheurs, attribuez des déclencheurs uniquement aux appareils spécifiques à partir desquels vous devez collecter des métriques afin de minimiser l'impact de vos déclencheurs sur les performances du système ExtraHop.

1. Cliquez **Actifs** depuis le menu supérieur.
2. Dans le volet de gauche, cliquez sur **Appareils**.
3. Dans le tableau, cochez la case correspondant à un seul équipement dont vous savez qu'il y a du trafic Web.
4. Dans le menu des icônes en haut de la page, cliquez sur l'icône Attribuer un déclencheur.
5. Cliquez sur la case à cocher à côté du **Métriques pour CloudWatch** déclencheur, puis cliquez sur **Assigner des déclencheurs**.

Une fois le déclencheur attribué, le système exécute le déclencheur en continu jusqu'à ce qu'il soit désactivé.

Vérifier la transmission des données vers la cible ODS

Une fois le déclencheur exécuté, vérifiez que les données ont été reçues par la cible ODS, puis désactivez le déclencheur.

Important: Amazon Web Services est une solution à plusieurs niveaux ; le premier niveau est gratuit, sauf si l'utilisation est dépassée. Exécutez ce déclencheur pendant une courte période pour éviter de dépasser la quantité de données autorisée. Si vous ne désactivez pas le déclencheur et que l'utilisation dépasse le délai imparti, des frais supplémentaires peuvent vous être facturés.

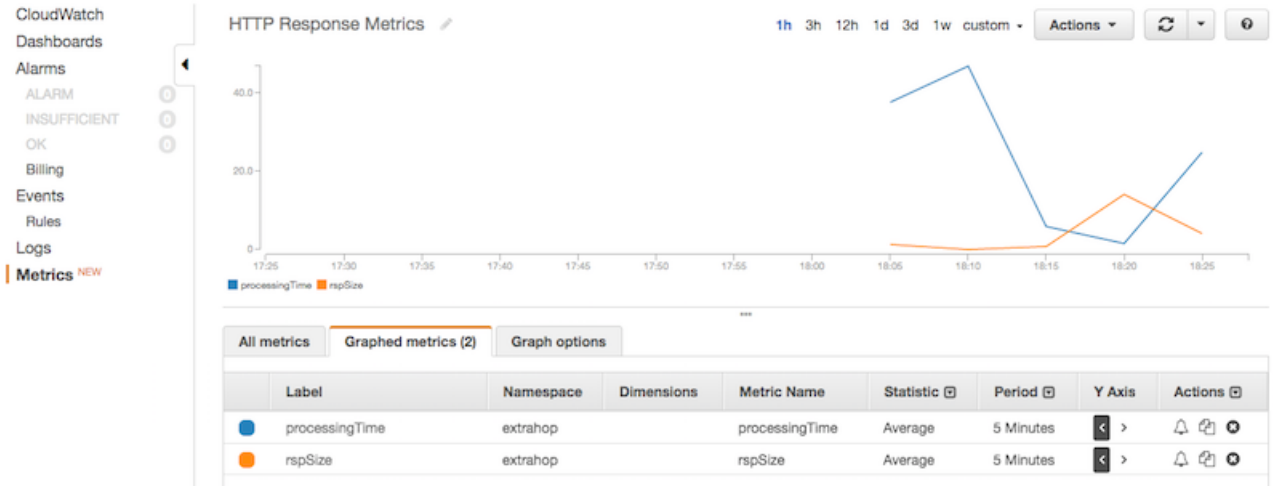
1. Laissez le déclencheur fonctionner pendant 10 à 15 minutes.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **Toute l'administration**.
3. À partir du Configuration du système section, cliquez **Flux de données ouverts**.
4. Dans le HTTP table, passez le curseur sur l'état de la cible CloudWatch pour afficher l'activité sur la connexion.

   Si le déclencheur réussit, la fenêtre affiche le nombre de messages et d'octets envoyés et reçus, ainsi que le nombre de tentatives de connexion.
5. Fermez la fenêtre des paramètres d'administration.
6. Cliquez sur l'icône des paramètres système, puis cliquez sur **déclencheurs**.
7. Dans le **DÉCLENCHEURS** tableau, cliquez **Métriques pour CloudWatch**.
8. Cliquez **Désactiver le déclencheur**.
9. Cliquez **Enregistrer et fermer**.

Afficher les résultats dans AWS CloudWatch

Après avoir vérifié que les données métriques ont été envoyées à la cible ODS, vous pouvez les consulter avec le service CloudWatch. Dans les étapes suivantes, vous trouverez les métriques dans CloudWatch et visualiserez les données métriques sur un graphique.

1. Accédez au Amazon Web Services site.
2. Cliquez **Connectez-vous à la console** et entrez vos informations daccréditations de connexion AWS.
3. Dans la liste des services AWS, cliquez sur **Cloud Watch**.
4. Dans le menu de gauche, cliquez sur **Actifs**.
   L'onglet Toutes les métriques affiche l'espace de noms « ExtraHop » créé par le déclencheur et l'espace de noms « test » créé par la demande de test.
5. Cliquez **Hop supplémentaire**, puis cliquez sur **Métriques sans dimensions**.
   L'onglet affiche les deux métriques spécifiées dans le déclencheur , « ProcessingTime » et « RSPSize ».
6. Cochez la case à côté de chaque métrique pour afficher les données métriques sur le graphique, comme dans la figure suivante :



Prochaines étapes

Maintenant que vous avez correctement envoyé des données métriques de votre système ExtraHop à AWS CloudWatch, essayez de modifier le déclencheur pour envoyer des métriques supplémentaires ou créez une nouvelle cible ODS pour envoyer des données à d'autres outils tiers.