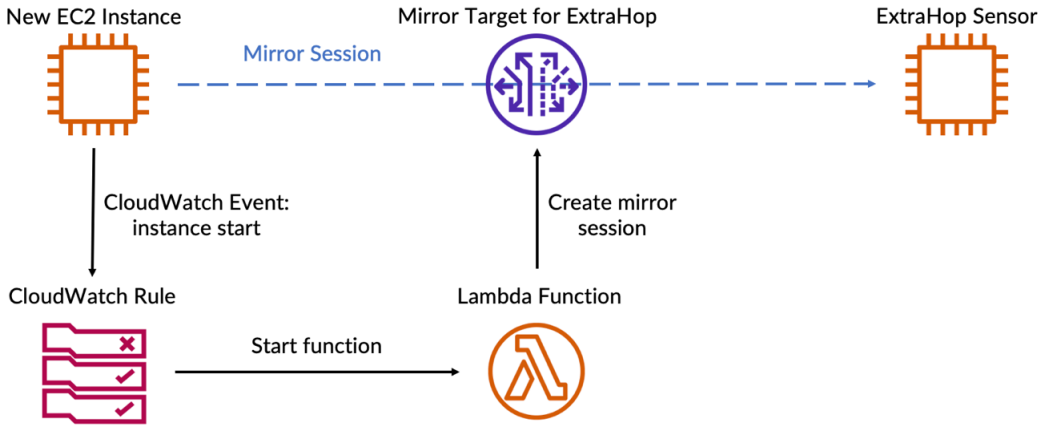
Automatisez la mise en miroir du trafic avec AWS Lambda

Publié: 2023-11-21

Vous pouvez configurer une fonction Lambda pour refléter automatiquement le trafic provenant des instances EC2 vers vos capteurs ExtraHop déployés dans AWS. Nous vous recommandons de configurer une forme d'automatisation pour vous assurer que toutes vos instances EC2 sont surveillées par le système ExtraHop .

Ce guide fournit des instructions pour configurer et installer un exemple de fonction Lambda disponible sur le référentiel ExtraHop GitHub. Voici comment fonctionne cette fonction :



Les étapes suivantes décrivent les différents processus décrits dans le schéma ci-dessus :

1. Chaque fois qu'une instance EC2 commence à s'exécuter, une règle CloudWatch exécute la fonction Lambda .
2. La fonction vérifie s'il existe une session miroir pour la nouvelle instance EC2.
3. S'il n'y a pas de session miroir pour l'instance, la fonction sélectionne la sonde ExtraHop vers laquelle elle reflétera le trafic.
    a. Tout d'abord, la fonction recherche les capteurs qui se trouvent dans la même zone de disponibilité que le miroir de trafic.

        Note: Si la fonction ne trouve aucun capteur dans la même zone de disponibilité, la variable LOCAL_ZONE_ONLY détermine si la fonction sélectionnera des capteurs en dehors de la zone de disponibilité. La mise en miroir du trafic entre les zones de disponibilité entraîne des frais supplémentaires par Go. Voir le Documentation AWS pour plus d' informations.
    b. Ensuite, la fonction filtre les capteurs avec des groupes de sécurité qui bloquent le trafic provenant de l'instance EC2.
    c. La fonction filtre ensuite les capteurs présents sur les VPC dotés de listes de contrôle d'accès bloquant le trafic provenant de l'instance EC2.
    d. Une fois que la fonction dispose d'une liste de capteurs valides, elle recherche la sonde ayant le plus petit nombre de sessions miroir afin de garantir une répartition uniforme des sessions miroir.
4. Enfin, la fonction crée une session miroir qui transfère le trafic de l' instance EC2 vers la sonde sélectionnée.

Avant de commencer

- Créez des cibles reflétant le trafic pour chacun de vos capteurs ExtraHop. Notez les identifiants des cibles ; vous devrez les ajouter au script.

- Création d'un filtre miroir de trafic qui détermine le trafic qui sera reflété par vos capteurs. Notez l'ID du filtre miroir ; vous devrez l'ajouter à une variable d'environnement dans la fonction Lambda.

Récupérez et installez l'exemple de script

1. Accédez à l'ExtraHop référentiel GitHub d'exemples de code et cliquez **miroir lambda_traffic_**.
2. Copiez le `lambda_traffic_mirror.py` fichier sur votre machine locale.
3. Ajoutez le `lambda_traffic_mirror.py` fichier vers un fichier zip avec le module Python netaddr.

   Le script importe le `netaddr` Module Python, qui n'est pas disponible pour les fonctions Lambda par défaut. Pour plus d'informations sur la création d'un fichier zip pour importer des bibliothèques tierces dans Lambda, consultez le Documentation AWS.
4. Dans AWS, créez une fonction Lambda.

   Pour plus d'informations sur la création de fonctions Lambda, consultez le Documentation AWS.
5. Sur la page de la fonction Lambda, cliquez sur **Actions** et sélectionnez **Téléchargez un fichier .zip** fichier.
6. Sélectionnez le fichier zip que vous avez créé.

Configuration de la fonction Lambda

Avant de pouvoir exécuter l'exemple de fonction Lambda, vous devez attribuer les autorisations nécessaires à la fonction et configurer la fonction pour référencer les informations de votre environnement AWS. Enfin, vous pouvez configurer une règle CloudWatch pour exécuter la fonction automatiquement.

1. Attribuez les autorisations suivantes à l'exemple de fonction Lambda :

   - Création de balises
   - Créer une session TrafficMirror
   - Décrire les instances
   - Décrire les interfaces réseau
   - Décrire les sessions TrafficMirror
   - Décrire les cibles du miroir de trafic
   - Décrire les groupes de sécurité
   - Décrire les ACL du réseau

   Pour plus d'informations sur la configuration des autorisations Lambda, consultez le didacticiel AWS ici.
2. Dans le `lambda_function.py` fichier, remplacez le `targets` variable d'environnement avec les identifiants des cibles du miroir de trafic pour vos capteurs ExtraHop.
3. Ajoutez l'ID du filtre miroir que vous avez créé en tant que variable d'environnement Lambda nommée `filter_id`.

   Pour plus d'informations sur les variables d'environnement Lambda, consultez Documentation AWS.
4. Configurez une règle CloudWatch pour démarrer la fonction Lambda chaque fois qu'une instance EC2 commence à s'exécuter.

   La règle CloudWatch doit s'exécuter selon le modèle d'événement suivant :

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EC2 Instance State-change Notification"
  ],
  "detail": {
```

```
    "state": [
      "running"
    ]
  }
}
```

Pour plus d'informations sur le démarrage de fonctions Lambda avec les règles CloudWatch, consultez le Documentation AWS.