Automatisez la mise en miroir du trafic AWS avec CloudFormation

Publié: 2024-11-04

Vous pouvez automatiser la mise en miroir du trafic pour les capteurs ExtraHop dans AWS à l'aide d'un modèle CloudFormation accessible au public sur le référentiel GitHub d'exemples de code ExtraHop. Le modèle CloudFormation crée une règle EventBridge et une fonction Lambda qui fonctionnent ensemble pour refléter automatiquement le trafic. Voici comment fonctionne le système :

La règle EventBridge s'exécute lorsque l'un des événements CloudTrail suivants se produit :

- Créer des tags
- Supprimer les balises
- Exécuter des instances
- Supprimer la session Traffic Mirror

La règle EventBridge lance ensuite la fonction Lambda. La fonction Lambda crée ou supprime une session de miroir de trafic qui reflète le trafic d'une instance EC2 vers une cible de miroir de trafic associée à une sonde ExtraHop. La fonction Lambda détermine comment créer la session miroir en fonction des balises AWS appliquées aux instances EC2, des filtres de miroir de trafic et des cibles de miroir de trafic.

Si l'événement est CreateTags et qu'une balise spécifique a été ajoutée à une instance EC2, la fonction Lambda crée une session Traffic Mirror pour l'instance EC2. Si l'événement est RunInstances et que l'instance EC2 possède une balise spécifique, la fonction Lambda crée une session de miroir de trafic pour l'instance EC2. Si l'événement est DeleteTrafficMirrorSession et qu'une instance EC2 associée possède une balise spécifique, la fonction Lambda recrée la session pour empêcher la suppression accidentelle ou malveillante des sessions Traffic Mirror.

Si l'événement est DeleteTags et qu'une balise spécifique a été supprimée d'une instance EC2, la fonction Lambda supprime une session Traffic Mirror.

Avant de commencer

- Créez des cibles miroir de trafic pour chacun de vos capteurs ExtraHop.

  Les cibles du trafic miroir doivent être associées à l'une des ressources AWS suivantes :

  - Instance EC2
  - Équilibreurs de charge réseau
  - Point de terminaison Gateway Load Balancer
- Création de filtres de surveillance du trafic qui déterminent le trafic qui sera reflété par vos capteurs.

Déployez le modèle CloudFormation

1. Accédez au Exemples de code ExtraHop GitHub référentiel et téléchargez le `cloudformation_traffic_mirror/cloudformation_traffic_mirror.yml` fichier sur votre machine locale.
2. Accédez à la page CloudFormation dans AWS.
3. Créez une pile CloudFormation à partir du fichier modèle CloudFormation que vous avez téléchargé.

   Configurez la variable suivante :

   Tag : Miroir

   Ce nom identifie la balise spécifique que vous allez ajouter aux miroirs et aux filtres pour coordonner la mise en miroir du trafic. Enregistrez la valeur de cette variable.

   Pour plus d'informations sur la configuration d'une pile CloudFormation, consultez Documentation AWS.

Étiqueter AWS Resources

La fonction Lambda crée des sessions de miroir de trafic entre une instance EC2 et une cible de miroir de trafic. Pour faciliter cette étape, vous devez ajouter la même balise à chaque instance, cible et filtre miroir de trafic.

Par exemple, le tableau suivant illustre un environnement dans lequel le nom de la variable TagMirror est `EH-Mirror`. Instances EC2 `ec2-A` et `ec2-B` sont surveillés par la sonde associée à `traffic-mirror-target-1`. Données provenant de `ec2-A` et `ec2-B` est filtré par `traffic-mirror-filter-1`. De même, les instances EC2 `ec2-C` et `ec2-D` sont surveillés par la sonde associée à `traffic-mirror-target-2`. Enfin, les données provenant de `ec2-C` et `ec2-D` est filtré par `traffic-mirror-filter-2`.

Tag Clé : Valeur (Appliqué à chaque ressource AWS d'une ligne)	Nom de l'instance EC2	Nom de la cible Traffic Mirror	F
`EH-Mirror:sensor-1`	`ec2-A`	`traffic-mirror-target-1`	t
`EH-Mirror:sensor-1`	`ec2-B`	`traffic-mirror-target-1`	t
`EH-Mirror:sensor-2`	`ec2-C`	`traffic-mirror-target-2`	t
`EH-Mirror:sensor-2`	`ec2-D`	`traffic-mirror-target-2`	t

1. Marquez chaque cible du Traffic Mirror.
2. Marquez chaque filtre Traffic Mirror.
3. Marquez chaque instance EC2.

Note: L'instance EC2 doit prendre en charge la mise en miroir du trafic. Pour plus d'informations, consultez la documentation AWS sur les types d'instances pris en charge.

Conseil: Vous pouvez baliser plusieurs instances EC2 à la fois avec le Éditeur de balises AWS.