Automatisieren Sie die AWS-Verkehrsspiegelung mit CloudFormation

Veröffentlicht: 2024-07-02

Sie können die Datenverkehrsspiegelung für ExtraHop-Sensoren in AWS mit einer CloudFormation-Vorlage automatisieren, die im GitHub-Repo für ExtraHop-Codebeispiele öffentlich verfügbar ist. Die CloudFormation-Vorlage erstellt eine EventBridge-Regel und eine Lambda-Funktion, die zusammenarbeiten, um den Datenverkehr automatisch zu spiegeln. So funktioniert das System:

Die EventBridge-Regel wird ausgeführt, wenn eines der folgenden CloudTrail-Ereignisse eintritt:

- Schlagworte erstellen
- Schlagworte löschen
- Instanzen ausführen
- Traffic Mirror-Sitzung löschen

Die EventBridge-Regel startet dann die Lambda-Funktion. Die Lambda-Funktion erstellt oder löscht eine Traffic Mirror-Sitzung, die den Datenverkehr von einer EC2-Instance auf ein Traffic Mirror-Ziel spiegelt, das einem ExtraHop-Sensor zugeordnet ist. Die Lambda-Funktion bestimmt, wie die Spiegelsitzung auf der Grundlage von AWS-Tags erstellt wird, die auf EC2-Instances, Traffic-Mirror-Filter und Traffic-Mirror-Ziele angewendet werden.

Wenn das Ereignis createTags ist und einer EC2-Instance ein bestimmtes Tag hinzugefügt wurde, erstellt die Lambda-Funktion eine Traffic Mirror-Sitzung für die EC2-Instance. Wenn das Ereignis runInstances ist und die EC2-Instance ein bestimmtes Tag hat, erstellt die Lambda-Funktion eine Traffic Mirror-Sitzung für die EC2-Instance. Wenn das Ereignis deleteTrafficMirrorSession ist und eine zugeordnete EC2-Instance ein bestimmtes Tag hat, erstellt die Lambda-Funktion die Sitzung neu, um zu verhindern, dass Traffic Mirror-Sitzungen versehentlich oder böswillig gelöscht werden.

Wenn das Ereignis deleteTags ist und ein bestimmtes Tag aus einer EC2-Instance entfernt wurde, löscht die Lambda-Funktion eine Traffic Mirror-Sitzung.

Bevor Sie beginnen

- Erstellen Sie Verkehrsspiegelziele für jeden Ihrer ExtraHop-Sensoren.

  Die Traffic-Mirror-Ziele müssen einer der folgenden AWS-Ressourcen zugeordnet sein:

  - EC2-Instanz
  - Netzwerk-Load-Balancer
  - Gateway Load Balancer-Endpunkt
- Verkehrsspiegelfilter erstellen die bestimmen, welcher Verkehr auf Ihre Sensoren gespiegelt wird.

Stellen Sie die CloudFormation-Vorlage bereit

1. Gehe zum ExtraHop Code-Beispiele GitHub Repository und laden Sie das herunter `cloudformation_traffic_mirror/cloudformation_traffic_mirror.yml` Datei auf Ihrem lokalen Computer.
2. Navigieren Sie zur CloudFormation-Seite in AWS.
3. Erstellen Sie einen CloudFormation-Stack aus der heruntergeladenen CloudFormation-Vorlagendatei.

   Konfigurieren Sie die folgende Variable:

   Schlagwort Mirror

   Dieser Name identifiziert das spezifische Tag, das Sie zu Spiegeln und Filtern hinzufügen, um die Verkehrsspiegelung zu koordinieren. Notieren Sie den Wert dieser Variablen.

Weitere Informationen zur Konfiguration eines CloudFormation-Stacks finden Sie in der AWS-Dokumentation.

AWS-Ressourcen kennzeichnen

Die Lambda-Funktion erstellt Traffic Mirror-Sitzungen zwischen einer EC2-Instance und einem Traffic Mirror-Ziel. Um diesen Schritt zu vereinfachen, müssen Sie jeder Instanz, jedem Ziel und jedem Traffic Mirror-Filter dasselbe Tag hinzufügen.

Die folgende Tabelle zeigt beispielsweise eine Umgebung, in der der Name der TagMirror-Variablen lautet `EH-Mirror`. EC2-Instanzen `ec2-A` und `ec2-B` werden von dem Sensor überwacht, der zugeordnet ist mit `traffic-mirror-target-1`. Daten von `ec2-A` und `ec2-B` wird gefiltert nach `traffic-mirror-filter-1`. Ähnlich wie EC2-Instances `ec2-C` und `ec2-D` werden von dem Sensor überwacht, der zugeordnet ist mit `traffic-mirror-target-2`. Schließlich Daten von `ec2-C` und `ec2-D` wird gefiltert nach `traffic-mirror-filter-2`.

Tag-Schlüssel:Wert (Wird auf jede AWS-Ressource in einer Reihe angewendet)	EC2-Instanzname	Zielname des Verkehrsspiegels	V
`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. Markieren Sie jedes Verkehrsspiegelziel.
2. Markieren Sie jeden Verkehrsspiegelfilter.
3. Kennzeichnen Sie jede EC2-Instance.

Hinweis: Die EC2-Instance muss die Datenverkehrsspiegelung unterstützen. Weitere Informationen finden Sie in der AWS-Dokumentation zu den unterstützten Instanztypen.

Hinweis: Sie können mehrere EC2-Instances gleichzeitig taggen mit dem AWS-Tag-Editor.