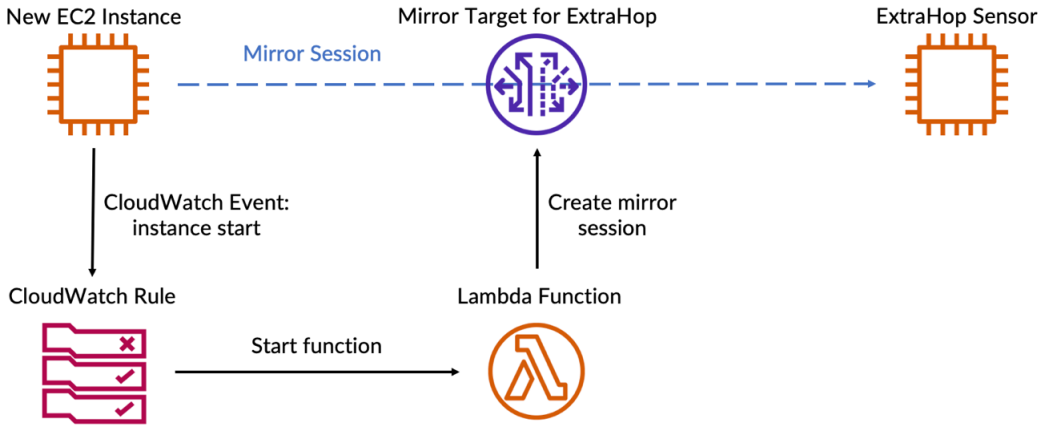
Automatisieren Sie die Datenverkehrsspiegelung mit AWS Lambda

Veröffentlicht: 2024-04-10

Sie können eine Lambda-Funktion so konfigurieren, dass der Datenverkehr von EC2-Instances automatisch auf Ihre in AWS bereitgestellten ExtraHop-Sensoren gespiegelt wird. Wir empfehlen Ihnen, irgendeine Form der Automatisierung zu konfigurieren, um sicherzustellen, dass alle Ihre EC2-Instances vom ExtraHop-System überwacht werden.

Dieses Handbuch enthält Anweisungen zur Konfiguration und Installation einer Lambda-Beispielfunktion, die im ExtraHop GitHub-Repository verfügbar ist. So funktioniert die Funktion:



Die folgenden Schritte skizzieren die einzelnen Prozesse, die in der obigen Abbildung beschrieben sind:

1. Jedes Mal, wenn eine EC2-Instance gestartet wird, führt eine CloudWatch-Regel die Lambda-Funktion aus.
2. Die Funktion überprüft, ob eine Spiegelsitzung für die neue EC2-Instance existiert.
3. Wenn es für die Instanz keine Spiegelsitzung gibt, wählt die Funktion aus, auf welchen ExtraHop-Sensor der Datenverkehr gespiegelt wird.
    a. Zunächst sucht die Funktion nach Sensoren, die sich in derselben Availability Zone wie der Traffic Mirror befinden.

        Hinweis: Wenn die Funktion keine Sensoren in derselben Availability Zone finden kann, bestimmt die Variable LOCAL_ZONE_ONLY, ob die Funktion Sensoren außerhalb der Availability Zone auswählt. Für die Spiegelung des Datenverkehrs zwischen Availability Zones fallen zusätzliche Gebühren pro GB an. Sehen Sie die AWS-Dokumentation für weitere Informationen.
    b. Als Nächstes filtert die Funktion Sensoren mit Sicherheitsgruppen heraus, die den Datenverkehr von der EC2-Instance blockieren.
    c. Anschließend filtert die Funktion Sensoren heraus, die sich auf VPCs mit ACLs befinden, die den Datenverkehr von der EC2-Instance blockieren.
    d. Sobald die Funktion über eine Liste gültiger Sensoren verfügt, sucht die Funktion nach dem Sensor mit der niedrigsten Anzahl von Spiegelsitzungen, um sicherzustellen, dass Spiegelsitzungen gleichmäßig verteilt sind.
4. Schließlich erstellt die Funktion eine Spiegelsitzung, die den Datenverkehr von der EC2-Instance an den ausgewählten Sensor weiterleitet.

Bevor Sie beginnen

- Erstellen Sie Verkehrsspiegelziele für jeden Ihrer ExtraHop-Sensoren. Notieren Sie sich die IDs der Ziele. Sie müssen die IDs dem Skript hinzufügen.

- Erstellen Sie einen Verkehrsspiegelfilter das bestimmt, welcher Verkehr auf Ihre Sensoren gespiegelt wird. Notieren Sie sich die ID des Spiegelfilters. Sie müssen die ID zu einer Umgebungsvariablen in der Lambda-Funktion hinzufügen.

Rufen Sie das Beispielskript ab und installieren Sie es

1. Gehe zum ExtraHop Codebeispiele GitHub-Repository und klicken **Lambda-Traffic-Mirror**.
2. Kopiere das `lambda_traffic_mirror.py` Datei auf Ihrem lokalen Computer.
3. Füge die `lambda_traffic_mirror.py` Datei in eine Zip-Datei mit dem Python-Modul netaddr.

   Das Skript importiert die `netaddr` Python-Modul, das standardmäßig nicht für Lambda-Funktionen verfügbar ist. Informationen zum Erstellen einer Zip-Datei zum Importieren von Bibliotheken von Drittanbietern in Lambda finden Sie in der AWS-Dokumentation.
4. Erstellen Sie in AWS eine Lambda-Funktion.

   Weitere Informationen zum Erstellen von Lambda-Funktionen finden Sie in der AWS-Dokumentation.
5. Klicken Sie auf der Lambda-Funktionsseite auf **Aktionen** und wähle **Laden Sie eine ZIP-Datei hoch** datei.
6. Wählen Sie die Zip-Datei aus, die Sie erstellt haben.

Lambda-Funktion konfigurieren

Bevor Sie die Lambda-Beispielfunktion ausführen können, müssen Sie der Funktion die erforderlichen Berechtigungen zuweisen und die Funktion so konfigurieren, dass sie auf Informationen aus Ihrer AWS-Umgebung verweist. Schließlich können Sie eine CloudWatch-Regel so konfigurieren, dass die Funktion automatisch ausgeführt wird.

1. Weisen Sie der Lambda-Beispielfunktion die folgenden Berechtigungen zu:
   - Schlagworte erstellen
   - Traffic Mirror-Sitzung erstellen
   - Instanzen beschreiben
   - Netzwerkschnittstellen beschreiben
   - Beschreiben Sie TrafficMirror-Sitzungen
   - Beschreiben Sie Traffic Mirror Targets
   - Beschreiben Sie Sicherheitsgruppen
   - Netzwerk-ACLs beschreiben

   Informationen zur Konfiguration von Lambda-Berechtigungen finden Sie im AWS-Tutorial hier.
2. In der `lambda_function.py` Datei, ersetze die `targets` Umgebungsvariable mit den IDs der Traffic Mirror-Targets für Ihre ExtraHop-Sensoren.
3. Fügen Sie die ID des Spiegelfilters hinzu, den Sie als Lambda-Umgebungsvariable mit dem Namen erstellt haben `filter_id`.

   Weitere Informationen zu Lambda-Umgebungsvariablen finden Sie in der AWS-Dokumentation.
4. Konfigurieren Sie eine CloudWatch-Regel, um die Lambda-Funktion jedes Mal zu starten, wenn eine EC2-Instance ausgeführt wird.

   Die CloudWatch-Regel muss gemäß dem folgenden Ereignismuster ausgeführt werden:

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

```
  ],
  "detail": {
    "state": [
      "running"
    ]
  }
}
```

Weitere Informationen zum Starten von Lambda-Funktionen mit CloudWatch-Regeln finden Sie in AWS-Dokumentation.