Stellen Sie einen ExtraHop Flow Sensor mit AWS bereit

Veröffentlicht: 2024-06-03

In diesem Handbuch wird erklärt, wie die virtuelle ExtraHop-Durchflusssensor-Appliance (EFC 1291v) auf der Amazon Web Services (AWS) -Plattform bereitgestellt wird.

Der EFC 1291v ist so konzipiert, dass er eine Verbindung zu Reveal (x) 360 herstellt und flussbasierten Datenverkehr aus Ihrem Netzwerk sammelt. Die Paketanalyse ist nicht verfügbar.

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um eine EFC 1291v-Appliance in AWS bereitzustellen:

- Ein AWS-Konto
- Zugriff auf das Amazon Machine Image (AMI) der ExtraHop 1100v-Appliance
- Ein Produktschlüssel für eine EFC 1291v-Appliance
- Ein AWS-Instanztyp, der der VM-Größe der EFC-Appliance am ehesten entspricht, wie folgt:

Gerät	Unterstützter Instanztyp
Enthülle (x) EFC 1291v	c5.xlarge (4 vCPU und 8 GB RAM)

Überblick über die Bereitstellung

Für das Sammeln von Flow-Logs ist die folgende Konfiguration erforderlich.

1. Konfigurieren Sie eine IAM-Richtlinie und eine IAM-Rolle.
2. Stellen Sie die ExtraHop-Flow-Sensor-Instanz in AWS bereit.
3. Laden Sie eine von ExtraHop bereitgestellte Lambda-Funktion herunter und konfigurieren Sie sie. Die Lambda-Funktion wird immer dann ausgeführt, wenn neue Flow-Logs verfügbar sind, und leitet dann alle neuen Ereignisse an Ihren Sensor weiter. Weitere Informationen finden Sie in der folgenden AWS-Dokumentation: Verwenden von AWS Lambda mit Amazon Kinesis Firehose.
4. Aktivieren Sie die Veröffentlichung von VPC Flow Logs für eine Reihe von VPCs in Ihrer Umgebung.
5. Fügen Sie einen Lambda-Trigger hinzu.
6. Optional: Konfigurieren Sie Route 53.

Konfiguration einer IAM-Berechtigungsrichtlinie und einer IAM-Rolle

1. Erstelle eine IAM-Richtlinie über den JSON-Tab mit den folgenden Parametern:

```
{
    "Statement": [
        {
            "Action": [
                "ec2:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

2. Eine IAM-Rolle erstellen und fügen Sie die Genehmigungsrichtlinie bei.

   Das ExtraHop-System benötigt eine Instance-IAM-Rolle, um IP-Adressen von Flow-Logs mit Instances, Gateways und Lambdas zu korrelieren.

3. Klicken Sie auf **Vertrauensbeziehungen** klicken Sie auf die Registerkarte und bearbeiten Sie die Vertrauensrichtlinie so, dass sie wie folgt aussieht:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Setzen Sie das Sensor-AMI ein

1. Stellen Sie einen Reveal (x) EDA 1100V bereit, indem Sie den Stellen Sie einen ExtraHop-Sensor auf AWS bereit Führer.

   Der EDA 1100V ist ein Paketsensor, der bei Eingabe der Lizenz zu einem Flow-Log-Sensor wird. Der Sensor verarbeitet keine Pakete mehr.

   Hinweis: Sie können die Software Reveal (x) 1100v (BYOL) über den AWS Marketplace abonnieren.

2. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`. Der Benutzername ist eingerichtet und das Passwort ist die Zahlenfolge nach dem i- in der Instanz-ID.
3. Folgen Sie den Anweisungen, um die Lizenzvereinbarung zu akzeptieren, geben Sie den Produktschlüssel ein, ändern Sie die Standard-Setup- und Shell-Benutzerkontokennwörter, stellen Sie eine Verbindung zu ExtraHop Cloud Services her und stellen Sie eine Verbindung zu Reveal (x) 360 her.
4. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Die gesamte Verwaltung**.
5. In der Zugriffs-Einstellungen Abschnitt, klicken **API-Zugriff**.
6. In der Generieren Sie einen API-Schlüssel Abschnitt, geben Sie eine Beschreibung für den neuen Schlüssel ein und klicken Sie dann auf **Generieren**.
7. Generieren Sie das Flow Log-Geheimnis aus dem REST API Explorer.
   a) klicken **Öffnen Sie den ExtraHop API Explorer**.
   b) klicken **Geben Sie den API-Schlüssel ein** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das API-Schlüssel Feld.
   c) klicken **Autorisieren** und dann klicken **Schliessen**.
   d) klicken **ExtraHop** und dann klicken **BEITRAG /extrahop/flowlogs/secret**.
   e) klicken **Probiere es aus** und dann klicken **Anfrage senden**.
   f) Sehen Sie sich im Bereich Antworttext die an und Datensatz Sie sie auf `secret` Wert. Im nächsten Verfahren benötigen Sie das Geheimnis für die Umgebungsvariable EXTRAHOP_SECRET_KEY.

Lambda-Funktion konfigurieren

Eine von ExtraHop bereitgestellte Lambda-Funktion leitet neue Flow-Log-Ereignisse an den ExtraHop-Flow Fluss Sensor wann immer von einem Lambda-Trigger aufgerufen.

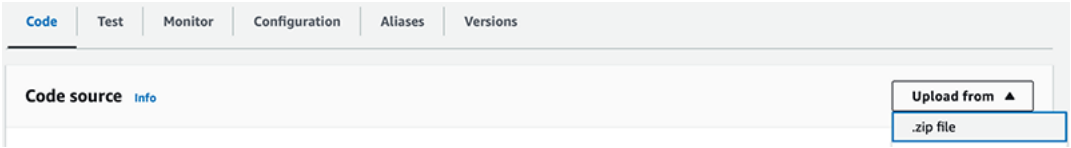
Weitere Informationen zum Erstellen von Lambda-Funktionen finden Sie in der AWS-Dokumentation.

Wichtig: Die Lambda-Funktion muss sich auf derselben VPC und demselben Subnetz wie der Flow-Log-Sensor Sensor. Die Funktion muss außerdem Teil einer Sicherheitsgruppe sein, die ausgehenden TCP-443-Verkehr zur Verwaltungsschnittstelle des Collectors zulässt.

1. Laden Sie das herunter `exflowlogs-lambda.zip` Datei aus dem ExtraHop herunterlädt Seite.
2. Erstellen Sie in AWS eine Lambda-Funktion.
   - Die Funktion muss die folgenden Laufzeiteinstellungen haben:
     - Die Laufzeit muss **Amazon Linux 2**.
     - Der Handler muss `bootstrap`.
     - Die Architektur muss **arm64**.
   - Die Funktion muss eine Ausführungsrolle mit den folgenden Berechtigungen haben:

     • **CloudWatch-Protokolle:**
       - Log-Gruppe erstellen
       - Logstream erstellen
       - Ereignisse protokollieren

     • **EC2:**
       - Netzwerkschnittstelle erstellen
       - Netzwerkschnittstelle löschen
       - Netzwerkschnittstellen beschreiben
   - Sie müssen die Konnektivität zwischen Ihrer Lambda-Funktion und der VPC und dem Subnetz aktivieren, in denen sich Ihr Collector befindet. Die Funktion muss außerdem Teil einer Sicherheitsgruppe sein, die den Verkehr zwischen der Funktion und dem Collector ermöglicht.
   - Laden Sie das hoch `exflowlogs-lambda.zip` Datei.



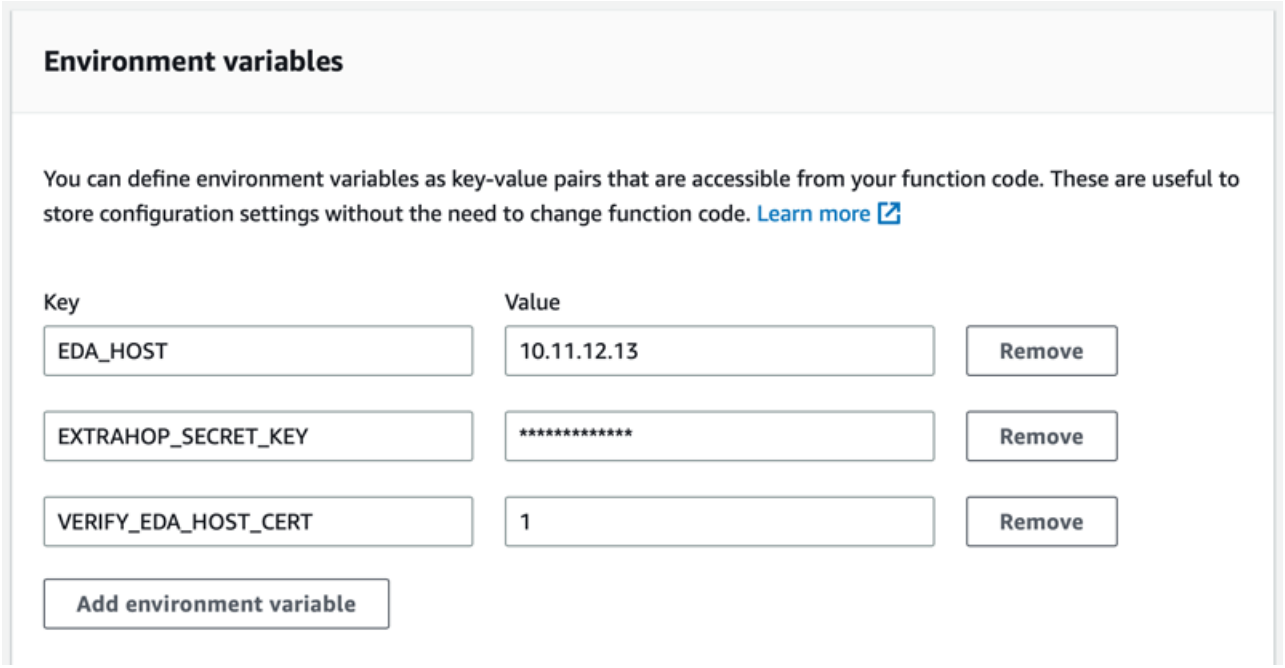
   - Auf dem **Kode** Tab, unter **Laufzeiteinstellungen**, setzen Sie den Handler-Wert auf `exflowlogs-lambda`.
   - Klicken Sie auf der Registerkarte Konfiguration auf **Allgemeine Konfiguration.**
     - Stellen Sie das Feld Speicher auf `128 MB`.
     - Setzen Sie das Feld Timeout auf `10 Sekunden`.
   - Klicken Sie **Funktions-URL** Die Funktions-URL ist erforderlich, wenn Sie Kinesis Firehose konfigurieren.
     - Wählen **KEINE** als Authentifizierungstyp.

       Hinweis Einstellung des Authentifizierungstyps auf **KEINE** erlaubt keinen öffentlichen Zugriff auf das Lambda, da die ressourcenbasierte Richtlinie der Funktion immer in Kraft ist und öffentlichen Zugriff gewähren muss, bevor die Funktions-URL Anfragen empfangen kann.
   - Klicken Sie **Umgebungsvariablen** und füge die folgenden Werte hinzu:

     • **EDA_HOST:** Die IP-Adresse oder der Hostname des VPC-Flow-Logs-Sensors.

     • **EXTRAHOP_SECRET_KEY:** Das Geheimnis, das Sie im vorherigen Verfahren über die ExtraHop REST-API generiert haben.

• **VERIFY_EDA_HOST_CERT:** Wenn der Sensor über das standardmäßige selbstsignierte Zertifikat verfügt, geben Sie an `0` um die Zertifikatsüberprüfung im Lambda-HTTP-Client zu deaktivieren. Andernfalls geben Sie an `1`.



Hinweis: Es kann bis zu 10 Minuten dauern, bis Geräte erkannt und Metriken aus Flow-Protokollen veröffentlicht werden.

Erstellen Sie einen Kinesis Firehose-Stream mit einem HTTP-Endpunkt

1. Navigieren Sie zum Amazon Kinesis-Dashboard.
2. Klicken Sie im linken Bereich auf **Lieferströme**.
3. klicken **Lieferstream erstellen**.
4. Wählen Sie die folgenden Quelle und Ziele aus:
   • **Quelle: Direktes PUT**
   • **Reiseziel: HTTP-Endpunkt**
5. Geben Sie einen eindeutigen Namen in das Feld Name des Lieferdatenstroms ein.
6. Geben Sie die folgenden Zieleinstellungen an:
   • **HTTP-Endpunktname: HTTP-Endpunkt**
   • **HTTP-Endpunkt-URL:** Die URL der Lambda-Funktion
   • **Zugriffs-Schlüssel :** Das Geheimnis, das Sie im vorherigen Verfahren über die ExtraHop REST-API generiert haben.
   • **Kodierung von Inhalten: GZIP**
7. In der **Einstellungen sichern** Abschnitt, wählen Sie einen vorhandenen S3-Backup-Bucket aus oder erstellen Sie einen neuen Bucket.
8. klicken **Lieferstream erstellen**.

Erstellen Sie das VPC-Flow-Protokoll

Identifizieren Sie die VPCs, die Sie mit dem Fluss überwachen möchten Sensor.

- Wenn Ihre ExtraHop AWS-Bereitstellung ein Paket beinhaltet Sensoren, Sie sollten vermeiden, eine bestimmte VPC mit beiden Paket zu überwachen Sensor und ein Fluss protokolliert Sensor.
- Es ist zwar möglich, Protokolle für kleinere Einheiten wie einzelne Subnetze oder Schnittstellen zu senden, aber das Senden der gesamten VPC ermöglicht die beste Erkennung von Geräten.

1. Wählen Sie Ihre VPC aus.
2. Klicken Sie auf **Ablaufprotokolle** Tabulatortaste und dann klicken **Flow-Log erstellen**
3. Konfigurieren Sie die folgenden Einstellungen:

   • **Filter:** Akzeptieren

   • **Maximales Aggregationsintervall:** 1 Minute

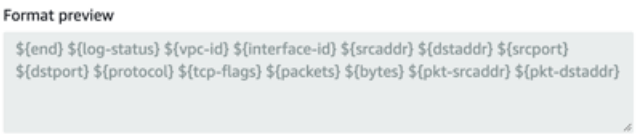
   • **Reiseziel:** Senden Sie über dasselbe Konto oder über ein anderes Konto an Kinesis Firehose

   • **Name des Kinesis Firehose-Lieferstreams:** Wählen Sie den Streamnamen aus, den Sie zuvor erstellt haben

   • **Format des Protokolldatensatzes:** Wählen **Benutzerdefiniertes Format** und wählen Sie dann die Protokollformatattribute in der folgenden Reihenfolge aus:

   - **Ende**
   - **Protokollstatus**
   - **vpc-id**
   - **Schnittstellen-ID**
   - **srcaddr**
   - **dstaddr**
   - **srcport**
   - **dstport**
   - **Protokoll**
   - **TCP-Flaggen**
   - **Pakete**
   - **Bytes**
   - **pkt-srcaddr**
   - **pkt-dstaddr**

Die Formatvorschau sollte der folgenden Abbildung ähneln.



Route 53-Protokolle konfigurieren (optional)

Amazon Route 53 bietet DNS-Abfrageprotokollierung, die für die Flow-Protokollkonfiguration nicht erforderlich ist, aber dringend empfohlen wird, wenn der Amazon DNS-Server konfiguriert ist.

Informationen zur Konfiguration von Route 53 zur Protokollierung von DNS-Abfragen, die ihren Ursprung in Ihren VPCs haben, finden Sie in der folgenden AWS-Dokumentation: Konfiguration der Resolver-Abfrageprotokollierung verwalten.

1. Gehen Sie zum Route 53-Dienst.
2. In der Resolver Abschnitt, klicken **Protokollierung von Abfragen**.
3. klicken **Abfrageprotokollierung konfigurieren**.
   a. Geben Sie einen Konfigurationsnamen für die Abfrageprotokollierung ein.
   b. Wählen **Kinesis Data Firehose-Lieferstream** als Ziel für Abfrageprotokolle.
   c. Wählen Sie den Kinesis Data Firehose-Lieferstream aus, den Sie zuvor erstellt haben.
   d. Klicken Sie im Abschnitt VPCs, für die Abfragen protokolliert werden sollen, auf **VPC hinzufügen**.
   e. Wählen Sie die VPCs aus, für die Sie Abfragen protokollieren möchten, und klicken Sie dann auf **Hinzufügen**.
   f. klicken **Abfrageprotokollierung konfigurieren**.