Stellen Sie einen ExtraHop-Sensor in AWS bereit

Veröffentlicht: 2024-02-12

Das folgende Verfahren führt Sie durch den Bereitstellungsprozess des Sensor-AMI zur Überwachung Ihrer Amazon Web Services (AWS) -Umgebung.

Nachdem Sie den Sensor in AWS bereitgestellt haben, konfigurieren Sie Spiegelung des AWS-Datenverkehrs oder RPCAP (RPCAP), um den Verkehr von Remote-Geräten an Ihren Sensor weiterzuleiten. Die AWS-Verkehrsspiegelung ist für alle Instance-Größen konfigurierbar und ist die bevorzugte Methode zum Senden von AWS-Verkehr an die EDA 6100v- und 8200v-Sensoren.

Wichtig: Um die beste Leistung bei der ersten Gerätesynchronisierung zu gewährleisten, schließen Sie alle Sensoren an die Konsole an und konfigurieren Sie dann die Weiterleitung des Netzwerkverkehrs zu den Sensoren.

Anforderungen an das System

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen virtuellen ExtraHop bereitzustellen Sensor in AWS:

- Ein AWS-Konto
- Zugriff auf das Amazon Machine Image (AMI) des ExtraHop-Sensors
- Die Sensor Produktschlüssel
- Ein AWS-Instanztyp, der dem virtuellen ExtraHop am ehesten entspricht Sensor Größe, wie folgt:

Sensoren	Empfohlener Instanztyp
Reveal (x) EDA 1100v	c5.xlarge (4 vCPU und 8 GB RAM)
EDA 6100 v	m5.4xlarge (16 vCPU und 64 GB RAM) c5.9xlarge (36 vCPU und 72 GB RAM) *
Enthülle (x) EDA 8200v	c5n.9xlarge (36 vCPU und 96 GB RAM)

Hinweis: Suchen Sie, wann immer möglich, nach Sensor innerhalb derselben Cluster-Platzierungsgruppe wie die Geräte, die den Datenverkehr weiterleiten. Diese bewährte Methode optimiert die Futterqualität, die Sensor erhält.

*Empfohlen, wenn der EDA 6100v nicht in derselben Cluster-Platzierungsgruppe wie der überwachte Verkehr bereitgestellt werden kann. Die c5.9xlarge-Instance hat höhere Kosten, ist jedoch in Umgebungen, in denen die Genauigkeit des Datenfeeds entscheidend ist, widerstandsfähiger.

Wichtig: AWS erzwingt ein Sitzungslimit von 10 Sitzungen für die VPC-Verkehrsspiegelung. Das Sitzungslimit kann jedoch erhöht werden für Sensoren läuft auf einem dedizierten C5-Host. Wir empfehlen den dedizierten c5-Host für EDA 8200v- und EDA 6100v-Instances, die ein größeres Sitzungslimit erfordern. Wenden Sie sich an den AWS-Support, um die Erhöhung des Sitzungslimits zu beantragen.

- (Optional) Eine Speicherfestplatte für Bereitstellungen, die Precision PCAP beinhalten. Anweisungen zum Hinzufügen einer Festplatte finden Sie in der AWS-Dokumentation.
  - Fügen Sie für den EDA 1100v eine Festplatte mit einer Kapazität von bis zu 250 GB hinzu.
  - Fügen Sie für die EDA 6100v und 8200v eine Festplatte mit einer Kapazität von bis zu 500 GB hinzu.

Erstellen Sie die ExtraHop-Instanz in AWS

Die Amazon Machine Images (AMIs) für ExtraHop-Sensoren sind verfügbar im AWS-Marktplatz. Sie können eine ExtraHop-Instance in AWS aus einem dieser AMIs erstellen.

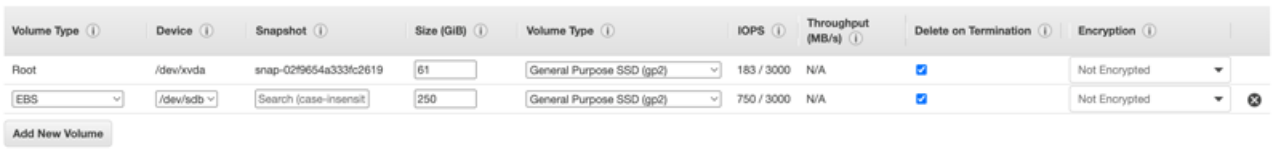
1. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei AWS an.
2. Klicken **EC2**.
3. Im linken Navigationsbereich unter **Bilder**, klicken **AMIs**.
4. Ändern Sie über der AMI-Tabelle die **Filtern** von **Gehört mir** zu **Private Bilder**.
5. Geben Sie in das Filterfeld `ExtraHop` und drücken Sie dann die EINGABETASTE.
6. Markieren Sie das Kästchen neben dem entsprechenden ExtraHop Sensor AMI und klick **Starten**.
7. Wählen Sie einen unterstützten Instance-Typ für Sensor Sie setzen ein.
8. Klicken **Weiter: Instanzdetails konfigurieren**.
9. Klicken Sie auf den **Netzwerk** Drop-down-Liste und wählen Sie eine der VPCs für Ihre Organisation aus.
10. Aus dem Verhalten beim Herunterfahren Dropdownliste, wählen **Stopp**.
11. Klicken Sie auf den **Vor versehentlicher Kündigung schützen** Checkbox.
12. Klicken Sie auf den **IAM-Rolle** Dropdownliste und wählen Sie eine IAM-Rolle aus.

    Hinweis: Wenn Sie einen Flusssensor (EFC 1291v) einsetzen, sollte dies die IAM-Rolle sein, die in der erstellt wurde Stellen Sie einen ExtraHop Flow Sensor mit AWS bereit Führer.
13. Wenn Sie in einer VPC gestartet sind und mehr als eine Schnittstelle haben möchten, scrollen Sie nach unten zu **Netzwerkschnittstellen** abschneiden und klicken **Gerät hinzufügen** um der Instanz zusätzliche Schnittstellen hinzuzufügen.

    Hinweis: Wenn Sie mehr als eine Schnittstelle haben, stellen Sie sicher, dass sich jede Schnittstelle in einem anderen Subnetz befindet.
14. Auf dem **Instanzdetails konfigurieren** Seite, klicken **Weiter: Speicher hinzufügen**. Die empfohlenen Speicherkapazitäten sind unten aufgeführt.

Fühler	Speicherkapazität
EDA 100 V	61 GiB
EDA 6100 v	1000 GiB
EDA 820 V	2000 GiB

15. Ändere das **Größe (GiB)** Feld für das Root-Volume auf den in der obigen Tabelle empfohlenen Wert für Ihren Sensor. Aus dem **Volume-Typ** Dropdownliste, wählen **Allzweck-SSD (gp2)**.
16. Optional: Fügen Sie ein neues Volume für eine Festplatte zur Erfassung von Präzisionspaketen hinzu.



17. Klicken **Weiter: Tag-Instanz**.
18. In der **Wert** Geben Sie in diesem Feld einen Namen für die Instanz ein.
19. Klicken **Weiter: Sicherheitsgruppe konfigurieren**.
20. Auf dem **Sicherheitsgruppe konfigurieren** Seite, folgen Sie dem unten stehenden Verfahren mit der folgenden Tabelle, um eine neue Sicherheitsgruppe zu erstellen oder Ports zu einer vorhandenen

Gruppe hinzuzufügen. Wenn Sie bereits eine Sicherheitsgruppe mit den erforderlichen Ports für ExtraHop haben, können Sie diesen Schritt überspringen.

a) Wählen Sie entweder **Erstellen Sie eine neue Sicherheitsgruppe** oder **Wählen Sie eine vorhandene Sicherheitsgruppe**. Wenn Sie eine vorhandene Gruppe bearbeiten möchten, wählen Sie die Gruppe aus, die Sie bearbeiten möchten. Wenn Sie eine neue Gruppe erstellen möchten, geben Sie ein **Name der Sicherheitsgruppe** und **Beschreibung**.

b) Klicken Sie auf den **Typ** Dropdownliste und wählen Sie eine Protokoll typ. Geben Sie die Portnummer in das **Portbereich** Feld.

c) Klicken Sie für jeden zusätzlichen Port, den Sie benötigen, auf **Regel hinzufügen** knopf. Klicken Sie dann auf **Typ** Dropdownliste, wählen Sie einen Protokolltyp aus und geben Sie die Portnummer in das **Portbereich** Feld.

Die folgenden Ports müssen für die ExtraHop AWS-Instanz geöffnet sein:

• **TCP-Ports 22, 80 und 443 für eingehende Nachrichten an das ExtraHop-System:** Diese Ports sind für die Verwaltung des ExtraHop-Systems erforderlich.

• **TCP-Port 443, ausgehend zu ExtraHop Cloud Services:** Fügen Sie die aktuelle IP-Adresse der ExtraHop Cloud Services hinzu. Weitere Informationen finden Sie unter Konfigurieren Sie Ihre Firewall-Regeln.

• **(Optional) TCP/UDP-Ports 2003-2034, eingehend von der AWS-VPC zum ExtraHop-System :** Wenn Sie nicht konfigurieren AWS-Datenverkehrsspiegelung, müssen Sie einen Port (oder eine Reihe von Ports) öffnen, damit der Paketweiterleiter RPCAP-Verkehr von Ihren AWS-VPC-Ressourcen weiterleiten kann. Weitere Informationen finden Sie unter Paketweiterleitung mit RPCAP.

• **UDP-Port 53, ausgehend zu Ihrem DNS-Server:** UDP-Port 53 muss geöffnet sein, damit der Sensor eine Verbindung zum ExtraHop-Lizenzserver herstellen kann.

21. Klicken **Überprüfung und Markteinführung**.
22. Wählen **Marke Allzweck (SSD)...** und klicken **Weiter**.

    Hinweis: Wenn du auswählst **Marke Allzweck (SSD)...**, dann wird dieser Schritt bei nachfolgenden Instanzstarts nicht mehr angezeigt.
23. Scrollen Sie nach unten, um die AMI-Details, den Instance-Typ und die Sicherheitsgruppeninformationen zu überprüfen, und klicken Sie dann auf **Starten**.
24. Klicken Sie im Popup-Fenster auf die erste Dropdownliste und wählen Sie **Fahren Sie ohne Schlüsselpaar fort**.
25. Klicken Sie auf den **Ich gebe zu...** Checkbox und dann klicken **Instanz starten**.
26. Klicken **Instanzen anzeigen** um zur AWS-Managementkonsole zurückzukehren.

    In der AWS-Managementkonsole können Sie Ihre Instance auf der **Initialisieren** Bildschirm. Unter dem Tisch, auf dem **Beschreibung** Auf dieser Registerkarte finden Sie die IP-Adresse oder den Hostnamen für das ExtraHop-System, auf das von Ihrer Umgebung aus zugegriffen werden kann.
27. Registrieren Sie Ihr ExtraHop-System.

Die nächsten Schritte

- (Empfohlen) Konfigurieren Spiegelung des AWS-Datenverkehrs um den Netzwerkverkehr von Ihren EC2-Instances auf eine leistungsstarke ERSPAN/VXLAN/GENEVE-Schnittstelle auf Ihrem Sensor zu kopieren.

  Hinweis: Wenn Ihre Bereitstellung einen Durchsatz von mehr als 15 Gbit/s erfordert, teilen Sie Ihre Datenverkehrsspiegelungsquellen auf zwei leistungsstarke ERSPAN/VXLAN/GENEVE-Schnittstellen auf dem EDA 8200v auf.
- (Fakultativ) Weiterleiten von geneve-gekapseltem Datenverkehr von einem AWS Gateway Load Balancer.
- Überprüfen Sie die Checkliste für Sensor und Konsole nach der Bereitstellung.

Erstellen Sie ein Verkehrsspiegelziel

Führen Sie diese Schritte für jede ENI aus, die Sie erstellt haben.

1. Kehren Sie zur AWS-Managementkonsole zurück.
2. Klicken Sie im oberen Menü auf **Dienstleistungen**.
3. Klicken Sie im Abschnitt Networking & Content Delivery auf **VPC**.
4. Klicken Sie im linken Bereich unter Traffic Mirroring auf **Spiegelziele**.
5. Klicken **Verkehrsspiegelziel erstellen** und füllen Sie die folgenden Felder aus:

Option	Beschreibung
Namensschild	(Optional) Geben Sie einen beschreibenden Namen für das Ziel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für das Ziel ein.
Typ des Ziels	Wählen **Netzwerk-Schnittstelle**.
Ziel	Wählen Sie die ENI aus, die Sie zuvor erstellt haben.

6. Klicken **Erstellen**.

Notieren Sie sich die Ziel-ID für jede ENI. Sie benötigen die ID, wenn Sie eine Traffic Mirror-Sitzung erstellen.

Erstellen Sie einen Verkehrsspiegelfilter

Sie müssen einen Filter erstellen, um den Datenverkehr von Ihren ENI Traffic Mirror-Quellen zu Ihrem ExtraHop-System zuzulassen oder einzuschränken. Wir empfehlen die folgenden Filterregeln, um zu verhindern , dass doppelte Frames von Peer-EC2-Instances, die sich in einer einzelnen VPC befinden, auf die Sensor.

- Der gesamte ausgehender Datenverkehr wird gespiegelt auf Sensor, ob der Datenverkehr von einem Peer-Gerät an ein anderes im Subnetz gesendet wird oder ob der Datenverkehr an ein Gerät außerhalb des Subnetzes gesendet wird.
- Eingehender Verkehr wird nur gespiegelt auf Sensor wenn der Datenverkehr von einem externen Gerät stammt. Diese Regel stellt beispielsweise sicher, dass eine App-Serveranfrage nicht zweimal gespiegelt wird: einmal vom sendenden App-Server und einmal von der Datenbank , die die Anfrage empfangen hat.
- Regelnummern bestimmen die Reihenfolge, in der die Filter angewendet werden. Regeln mit niedrigeren Zahlen, z. B. 100, werden zuerst angewendet.

> **Wichtig:** Diese Filter sollten nur angewendet werden, wenn alle Instanzen in einem CIDR-Block gespiegelt werden.

1. Klicken Sie in der AWS-Managementkonsole im linken Bereich unter Traffic Mirroring auf **Spiegelfilter**.
2. klicken **Verkehrsspiegelfilter erstellen** und füllen Sie die folgenden Felder aus:

Option	Beschreibung
Namensschild	Geben Sie einen Namen für den Filter ein.
Beschreibung	Geben Sie eine Beschreibung für den Filter ein.
Netzwerkdienste	Wählen Sie den **Amazon-DNS** Checkbox.

3. In der Regeln für eingehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen** und füllen Sie dann die folgenden Felder aus:

Option	Beschreibung
Zahl	Geben Sie eine Zahl für die Regel ein, z. B. `100`.

Option	Beschreibung
Regelaktion	Wählen **ablehnen** aus der Dropdownliste.
Protokoll	Wählen **Alle Protokolle** aus der Dropdownliste.
CIDR-Quellblock	Geben Sie den CIDR-Block für das Subnetz ein.
CIDR-Zielblock	Geben Sie den CIDR-Block für das Subnetz ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.

4. In der Regeln für eingehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen** noch einmal und füllen Sie dann die folgenden Felder aus:

Option	Beschreibung
Zahl	Geben Sie eine Zahl für die Regel ein, z. B. `200`.
Regelaktion	Wählen **akzeptieren** aus der Dropdownliste.
Protokoll	Wählen **Alle Protokolle** aus der Dropdownliste.
CIDR-Quellblock	Typ `0.0.0.0/0`.
CIDR-Zielblock	Typ `0.0.0.0/0`.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.

5. In der Regeln für ausgehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen** und füllen Sie dann die folgenden Felder aus:

Option	Beschreibung
Zahl	Geben Sie eine Zahl für die Regel ein, z. B. `100`.
Regelaktion	Wählen **akzeptieren** aus der Dropdownliste.
Protokoll	Wählen **Alle Protokolle** aus der Dropdownliste.
CIDR-Quellblock:	Typ `0.0.0.0/0`.
CIDR-Zielblock:	Typ `0.0.0.0/0`.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.

6. klicken **Erstellen**.

Erstellen Sie eine Traffic Mirror-Sitzung

Sie müssen für jede AWS-Ressource, die Sie überwachen möchten, eine Sitzung erstellen. Sie können maximal 500 Traffic Mirror-Sitzungen pro erstellen Sensor.

Wichtig: Um zu verhindern, dass Spiegelpakete gekürzt werden, legen Sie den MTU-Wert der Traffic Mirror-Quellschnittstelle auf 54 Byte unter dem MTU-Zielwert des Traffic Mirrors für IPv4 und 74 Byte unter dem MTU-Zielwert des Traffic Mirrors für IPv6 fest. Weitere Informationen zur Konfiguration des Netzwerk-MTU-Werts finden Sie in der folgenden AWS-Dokumentation: Network Maximum Transmission Unit (MTU) für Ihre EC2-Instance.

1. Klicken Sie in der AWS-Managementkonsole im linken Bereich unter Traffic Mirroring auf **Spiegelsitzung**.
2. Klicken **Traffic Mirror-Sitzung erstellen** und füllen Sie die folgenden Felder aus:

Option	Beschreibung
Namensschild	(Optional) Geben Sie einen beschreibenden Namen für die Sitzung ein.

Option	Beschreibung
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Sitzung ein
Spiegelquelle	Wählen Sie die Quelle ENI aus. Die Quell-ENI ist normalerweise an die EC2-Instance angehängt , die Sie überwachen möchten.
Spiegelziel	Wählen Sie die Traffic Mirror-Ziel-ID aus, die für die Ziel-ENI generiert wurde.
Nummer der Sitzung	Typ `1`.
VNI	Lassen Sie dieses Feld leer.
Länge des Pakets	Lassen Sie dieses Feld leer.
Filtern	Wählen Sie im Dropdownmenü die ID für den Traffic Mirror-Filter aus, den Sie erstellt haben.

3. Klicken **Erstellen**.