Stellen Sie den ExtraHop Packetstore in AWS bereit

Veröffentlicht: 2024-07-17

In diesem Handbuch erfahren Sie, wie Sie das ExtraHop Packetstore AMI in Ihrer Amazon Web Services (AWS) -Umgebung starten.

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

- Ein AWS-Konto
- Zugriff auf das Amazon Machine Image (AMI) der ExtraHop Trace-Appliance
- Ein Extrahop Packetstore-Produktschlüssel
- Ein AWS-Instanztyp, der der Größe der Packetstore-VM am ehesten entspricht, wie folgt:

Paketshop	Unterstützte Instance-Typen
ETA 1150 v	m5.x groß, m5.2 x groß

Hinweis: Sie können die Größe Ihrer Instanz ändern, ohne den Packetstore erneut bereitzustellen. Sehen Sie die AWS-Dokumentation für Einzelheiten.

Bevor Sie beginnen
Die Amazon Machine Images (AMIs) von ExtraHop-Appliances werden nicht öffentlich geteilt. Bevor Sie mit dem Bereitstellungsverfahren beginnen können, müssen Sie Ihre AWS-Konto-ID an Ihren ExtraHop-Vertreter senden. Ihre Konto-ID wird mit dem ExtraHop AMI verknüpft.

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 Tabelle der AMIs den **Filter** von **Gehört mir** zu **Private Bilder**.
5. Geben Sie im Filterfeld Folgendes ein `ExtraHop` und drücken Sie dann die EINGABETASTE.
6. Markieren Sie das Kontrollkästchen neben dem ExtraHop Packetstore AMI und klicken Sie auf **Starten**.
7. Wählen Sie einen der folgenden unterstützten Instance-Typen aus:

Instanztyp	Einzelheiten
m5.x groß	Für die meisten Installationen empfohlen.
m 5.2 x groß	Wählen **m 5.2 x groß** wenn Sie einen höheren Durchsatz benötigen. Die Kosten für diese Instanz sind höher als für **m5.x groß**.

8. Klicken Sie auf **Netzwerk** Drop-down-Liste und wählen Sie die Standardeinstellung oder eine der VPCs für Ihre Organisation aus.
9. Optional: Klicken Sie auf **IAM-Rolle** Dropdownliste und wählen Sie eine IAM-Rolle aus.
10. Aus dem **Verhalten beim Herunterfahren** Drop-down-Liste, wählen **Stopp**.
11. Wählen Sie den **Vor versehentlicher Kündigung schützen** Checkbox.
12. klicken **Weiter: Speicher hinzufügen**.
13. In der Größe (GiB) Feld für die wurzel Volumen, geben Sie die Größe des Speichervolumens ein. Die minimale Packetstore-Größe beträgt 1000 GiB (1 TB) und die maximale Datenspeichergröße beträgt 2047 GiB (2 TB).
14. Aus dem Typ des Volumens Drop-down-Menü, wählen Sie entweder **magnetisch** oder **Allzweck-SSD (GP2)**. Wenn Sie eine Größe von mehr als 1024 GiB angeben, müssen Sie auswählen **Allzweck-SSD (GP2)**. GP2 bietet eine bessere Speicherleistung, allerdings zu höheren Kosten.

15. klicken **Weiter: Schlagworte hinzufügen**.
16. klicken **Tag hinzufügen**.
17. In der Wert Feld, geben Sie einen Namen für die Instanz ein.
18. klicken **Weiter: Sicherheitsgruppe konfigurieren**.
19. Wählen Sie eine vorhandene Sicherheitsgruppe aus oder erstellen Sie eine neue Sicherheitsgruppe mit den erforderlichen Ports.
20. klicken **Regel hinzufügen** und fügen Sie die folgenden Ports hinzu:

Typ	Portbereich
SSH	22
Benutzerdefiniertes TCP	443
Benutzerdefiniertes TCP	2003
Benutzerdefiniertes UDP	2003

Die TCP-Ports 22 und 443 sind für die Verwaltung des ExtraHop-Systems erforderlich. Für die Paketweiterleitung ist der TCP- und UDP-Port 2003 erforderlich.

21. klicken **Überprüfung und Markteinführung**.
22. Wählen Sie die Startvolume-Option aus, die Sie in Schritt 14 ausgewählt haben, und klicken Sie dann auf **Weiter**.

> **Hinweis:** Wenn du wählst **Machen Sie General Purpose (SSD)... (empfohlen)**, Sie werden diesen Schritt bei nachfolgenden Instance-Starts nicht sehen.

23. Überprüfen Sie die AMI-Details, den Instance-Typ und die Sicherheitsgruppeninformationen, und klicken Sie dann auf **Starten**.
24. Klicken Sie im Popup-Fenster auf die erste Dropdownliste und wählen Sie **Ohne Schlüsselpaar fortfahren**.
25. Klicken Sie auf **Ich erkenne an...** Checkbox und dann klicken **Instances starten**.
26. klicken **Instanzen anzeigen** um zur AWS-Managementkonsole zurückzukehren.

    Von der AWS-Managementkonsole aus können Sie Ihre Instance auf der Initialisieren Bildschirm.

    Unter dem Tisch, auf dem **Beschreibung** Auf der Registerkarte finden Sie eine Adresse oder einen Hostnamen für das ExtraHop-System, auf das von Ihrer Umgebung aus zugegriffen werden kann.

Nächste Schritte

- Registrieren Sie Ihr ExtraHop-System
- Überprüfen Sie die Checkliste für die Rückverfolgung der Appliance nach der Bereitstellung.
- Verbinden Sie die Command and Discover-Appliances mit der Trace-Appliance.
- Konfigurieren Sie Remote Packet Capture (RPCAP), um den Datenverkehr von Remote-Geräten an Ihren virtuellen Packetstore weiterzuleiten. Weitere Informationen finden Sie unter RPCAP für einen ExtraHop-Packetstore konfigurieren.
- (Empfohlen) Konfigurieren Spiegelung des AWS-Datenverkehrs um Netzwerkverkehr von Ihren EC2-Instances auf eine RPCAP/ERSPAN/VXLAN/GENEVE-Schnittstelle in Ihrem Packetstore zu kopieren.

Erstellen Sie ein Traffic Mirror-Ziel

Führen Sie diese Schritte für jedes Elastic Netzwerk Interface (ENI) aus, das Sie erstellt haben.

1. Klicken Sie in der AWS-Managementkonsole im oberen Menü auf **Dienstleistungen**.
2. Klicken Sie **Netzwerke und Inhaltsbereitstellung** > **VPC**.
3. Klicken Sie im linken Bereich unter Traffic Mirroring auf **Ziele spiegeln**.

4. Klicken Sie **Verkehrsspiegelziel erstellen**.
5. Optional: Geben Sie im Feld Namens-Tag einen beschreibenden Namen für das Ziel ein.
6. Optional: Geben Sie im Feld Beschreibung eine Beschreibung für das Ziel ein.
7. Aus dem Typ des Ziels Wählen Sie in der Dropdownliste Netzwerkschnittstelle aus.
8. Aus dem Ziel Wählen Sie in der Dropdownliste die ENI aus, die Sie zuvor erstellt haben.
9. Klicken Sie **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 Verkehr von Ihren ENI-Traffic-Spiegelquellen 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 zu einem anderen im Subnetz gesendet wird oder ob der Verkehr an ein Gerät außerhalb des Subnetzes gesendet wird.
- Eingehender Verkehr wird nur gespiegelt auf Sensor wenn der Verkehr 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 erhalten 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**.
3. In der Namensschild Feld, geben Sie einen Namen für den Filter ein.
4. In der Beschreibung Feld, geben Sie eine Beschreibung für den Filter ein.
5. Unter Netzwerkdienste, wählen Sie **Amazon-DNS** Ankreuzfeld.
6. In der Regeln für eingehenden Verkehr Abschnitt, klicken **Regel hinzufügen**.
7. Konfigurieren Sie eine Regel für eingehenden Verkehr:
   a) In der Zahl Feld, geben Sie eine Zahl für die Regel ein, z. B. `100`.
   b) Aus dem Regelaktion Dropdownliste, wählen **ablehnen**.
   c) Aus dem Protokoll Dropdownliste, wählen **Alle Protokolle**.
   d) In der Quell-CIDR-Block Feld, geben Sie den CIDR-Block für das Subnetz ein.
   e) In der Ziel-CIDR-Block Feld, geben Sie den CIDR-Block für das Subnetz ein.
   f) In der Beschreibung Feld, geben Sie eine Beschreibung für die Regel ein.
8. Klicken Sie in den Abschnitten „Regeln für eingehenden Verkehr“ auf **Regel hinzufügen**.
9. Konfigurieren Sie eine zusätzliche Regel für eingehenden Datenverkehr:
   a) In der Zahl Feld, geben Sie eine Zahl für die Regel ein, z. B. `200`.
   b) Aus dem Regelaktion Dropdownliste, wählen **akzeptieren**.
   c) Aus dem Protokoll Dropdownliste, wählen **Alle Protokolle**.
   d) In der Quell-CIDR-Block Feld, Typ `0,0,0,0/0`.
   e) In der Ziel-CIDR-Block Feld, Typ `0,0,0,0/0`.
   f) In der Beschreibung Feld, geben Sie eine Beschreibung für die Regel ein.
10. Klicken Sie im Abschnitt Regeln für ausgehenden Datenverkehr auf **Regel hinzufügen**.

11. Konfigurieren Sie eine Regel für ausgehenden Datenverkehr:
    a) In der Zahl Feld, geben Sie eine Zahl für die Regel ein, z. B. `100`.
    b) Aus dem Regelaktion Dropdownliste, wählen **akzeptieren**.
    c) Aus dem Protokoll Dropdownliste, wählen **Alle Protokolle**.
    d) In der Quell-CIDR-Block Feld, Typ `0,0,0,0/0`.
    e) In der Ziel-CIDR-Block Feld, Typ `0,0,0,0/0`.
    f) In der Beschreibung Feld, geben Sie eine Beschreibung für die Regel ein.
12. Klicken Sie **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 Sitzung erstellen. Sensor.

Wichtig: Um zu verhindern, dass Spiegelpakete gekürzt werden, legen Sie den MTU-Wert der Traffic Mirror-Quellschnittstelle auf 54 Byte unter dem Ziel-MTU-Wert für IPv4 und 74 Byte unter dem MTU des Traffic Mirror-Zielwerts 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 **Spiegelsitzungen**.
2. Klicken Sie **Traffic Mirror-Sitzung erstellen**.
3. In der Namensschild Feld, geben Sie einen beschreibenden Namen für die Sitzung ein.
4. In der Beschreibung Feld, geben Sie eine Beschreibung für die Sitzung ein.
5. Aus dem Spiegelquelle Wählen Sie in der Dropdownliste die Quell-ENI aus.
   Die Quell-ENI ist normalerweise an die EC2-Instance angehängt, die Sie überwachen möchten.
6. Aus dem Spiegelziel Wählen Sie in der Dropdownliste die für die Ziel-ENI generierte Traffic Mirror-Ziel-ID aus.
7. In der Nummer der Sitzung Feld, Typ `1`.
8. Für die VNI-Feld, lass dieses Feld leer.
   Das System weist eine zufällige eindeutige VNI zu.
9. Für die Länge des Pakets Feld, lasse dieses Feld leer.
   Dies spiegelt das gesamte Paket wider.
10. Aus dem Filter Wählen Sie in der Dropdownliste die ID für den von Ihnen erstellten Traffic Mirror-Filter aus.
11. Klicken Sie **Erstellen**.