Stellen Sie einen ExtraHop-Sensor auf AWS bereit

Veröffentlicht: 2024-08-08

Die folgenden Verfahren erklären, wie Sie einen virtuellen ExtraHop bereitstellen. Sensor in einer Amazon Web Services (AWS) -Umgebung. Sie müssen Erfahrung mit der Bereitstellung virtueller Maschinen in AWS innerhalb Ihrer virtuellen Netzwerkinfrastruktur haben.

Ein virtueller ExtraHop Sensor kann Ihnen helfen, die Leistung Ihrer Anwendungen in internen Netzwerken, im öffentlichen Internet oder einer virtuellen Desktop-Schnittstelle (VDI), einschließlich Datenbank- und Speicherebenen, zu überwachen. Das ExtraHop-System kann die Anwendungsleistung in geografisch verteilten Umgebungen wie Zweigstellen oder virtualisierten Umgebungen über den Verkehr zwischen virtuellen Rechnern überwachen.

Mit dieser Installation können Sie Netzwerkleistungsüberwachung, Netzwerkerkennung und -reaktion sowie Einbruchserkennung auf einem einzigen Gerät ausführen Sensor.

Wichtig: Das IDS-Modul benötigt das NDR-Modul. Bevor Sie das IDS-Modul auf diesem Sensor aktivieren können, müssen Sie die Sensor-Firmware auf Version 9.6 oder höher aktualisieren. Wenn das Upgrade abgeschlossen ist, können Sie die neue Lizenz auf den Sensor anwenden.

Hinweis: Wenn Sie das IDS-Modul auf diesem Sensor aktiviert haben und Ihr ExtraHop-System keinen direkten Zugang zum Internet und keinen Zugriff auf ExtraHop Cloud Services hat, müssen Sie IDS-Regeln manuell hochladen. Weitere Informationen finden Sie unter Laden Sie die IDS-Regeln über die REST-API in das ExtraHop-System hoch.

Nachdem Sie das bereitgestellt haben Sensor in AWS konfigurieren Spiegelung des AWS-Datenverkehrs oder RPCAP (RPCAP), um den Verkehr von Remote-Geräten an Ihre weiterzuleiten Sensor. Die AWS-Datenverkehrsspiegelung ist für alle Instanzgrößen konfigurierbar und ist die bevorzugte Methode, um AWS-Verkehr an die EDA 6100v und 8200v zu senden Sensor.

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:

- Sie müssen ein AWS-Konto haben.
- Sie müssen Zugriff auf das Amazon Machine Image (AMI) des ExtraHop haben Sensor.
- Du musst einen ExtraHop haben Sensor Produktschlüssel.
- Sie können optional eine Speicherfestplatte für Bereitstellungen konfigurieren, die eine präzise 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.

Anforderungen an virtuelle Maschinen

Sie müssen einen AWS-Instanztyp bereitstellen, der Ihrer virtuellen ExtraHop-Sensorgröße am ehesten entspricht und die folgenden Modulanforderungen erfüllt.

Fühler	Module	Empfohlener Instanztyp	Größe der Festplatte
EDA 1100 V	NDR, NPM	c5.xlarge (4 vCPUs und 8 GB RAM)	61 GB
EDA 6100 v	NDR, NPM	m5.4xlarge (16 vCPUs und 64 GB RAM) c5.9xlarge (36 vCPUs und 72 GB RAM)	1000 GB
EDA 6320v	NDR, NPM, Intrusion Detection System	m 5,8 x groß (32 vCPUs, 128 GB RAM)	1400 GB
EDA 8200 v	NDR, NPM	c5n.9xlarge (36 vCPUs und 96 GB RAM)	2000 GB

Hinweis: Durchsatz kann beeinträchtigt werden, wenn mehr als ein Modul auf dem Sensor aktiviert ist.

Wichtig: AWS setzt ein Limit von 10 Sitzungen für die Virtual Private Cloud (VPC) - Datenverkehrsspiegelung durch. Das Sitzungslimit kann jedoch erhöht werden für Sensoren läuft auf einem dedizierten c5-Host. Wir empfehlen den c5 Dedicated Host für EDA 8200v- und EDA 6100v-Instances, die ein höheres Sitzungslimit erfordern. Wenden Sie sich an den AWS-Support, um die Erhöhung des Sitzungslimits zu beantragen.

Anforderungen an den Anschluss

Die folgenden Ports müssen für ExtraHop AWS-Instances geöffnet sein.

Hafen	Beschreibung
TCP-Ports 22, 80 und 443, die in das ExtraHop-System eingehen	Diese Ports werden benötigt, um das ExtraHop-System zu verwalten.
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 Firewallregeln.
UDP-Port 53 ausgehend zu Ihrem DNS-Server	Der UDP-Port 53 muss geöffnet sein, damit der Sensor eine Verbindung zum ExtraHop-Lizenzierungsserver herstellen kann.
(Optional) TCP/UDP-Ports 2003-2034, die von der AWS VPC in das ExtraHop-System eingehen	Wenn Sie nicht konfigurieren Spiegelung des AWS-Datenverkehrs, müssen Sie einen Port (oder eine Reihe von Ports) für den Paketweiterleiter öffnen, um den RPCAP-Verkehr von Ihren AWS-VPC-Ressourcen weiterzuleiten. Weitere Informationen finden Sie unter Paketweiterleitung mit RPCAP.

Erstellen Sie die ExtraHop-Instanz in AWS

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

1. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei AWS an.
2. Klicken Sie **EC2**.

3. Im linken Navigationsbereich unter Bilder, klicken **AMIs**.
4. Ändern Sie über der AMI-Tabelle das Filter von **Gehört mir** zu **Öffentliche Bilder**.
5. Geben Sie in das Filterfeld ein `ExtraHop` und drücken Sie dann ENTER.
6. Markieren Sie das Kästchen neben dem entsprechenden ExtraHop Sensor AMI und klick **Instance von AMI aus starten**.

   Weitere Informationen zur Auswahl eines virtuellen Sensor finden Sie unter Anforderungen an virtuelle Maschinen.Ω
7. In der Name Feld, geben Sie einen Namen zur Identifizierung des ExtraHop-Sensors ein.
8. In der Anwendungs- und Betriebssystem-Images (Amazon Machine Image) Abschnitt, überprüfen Sie das ausgewählte AMI.
9. In der Instanztyp Abschnitt, überprüfen Sie den ausgewählten Instanztyp.
10. In der Schlüsselpaar (Anmeldung) Abschnitt, wählen Sie ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues Schlüsselpaar.
11. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Bearbeiten**.
12. Aus dem VPC Wählen Sie in der Dropdownliste eine VPC aus.
13. Wählen Sie in der Dropdownliste Subnetz ein Subnetz aus.
14. Optional: Wenn Sie weitere Netzwerkschnittstellen hinzufügen möchten, wählen Sie in der Dropdownliste Öffentliche IP automatisch zuweisen die Option Deaktivieren aus.
15. Klicken Sie **Sicherheitsgruppe erstellen** oder **Wählen Sie eine vorhandene Sicherheitsgruppe**.

    Wenn Sie eine bestehende Gruppe bearbeiten möchten, wählen Sie die Gruppe aus, die Sie bearbeiten möchten. Wenn Sie eine neue Gruppe erstellen möchten, geben Sie einen Namen und eine Beschreibung der Sicherheitsgruppe ein.
16. In der Regeln für eingehende Sicherheitsgruppen Abschnitt, konfigurieren Sie alle erforderlichen Regeln.

    Weitere Informationen zu den Portanforderungen für ExtraHop-Systeme finden Sie unter Anforderungen an den Anschluss.

    a) Aus dem Typ Wählen Sie in der Dropdownliste einen Protokolltyp aus.
    b) In der Port-Bereich Feld, geben Sie die Portnummer ein.
    c) Für jeden weiteren benötigten Port klicken Sie auf **Sicherheitsgruppenregel hinzufügen**, und konfigurieren Sie dann den Typ- und Portbereich nach Bedarf.
17. Optional: Um zusätzliche Netzwerkschnittstellen zu einer Instanz in einer Virtual Private Cloud (VPC) hinzuzufügen, klicken Sie auf **Erweiterte Netzwerkkonfiguration**.

    a) klicken **Netzwerkschnittstelle hinzufügen**.
    b) Aus dem Netzwerk-Schnittstelle Wählen Sie in der Dropdownliste die Netzwerkschnittstelle aus, die Sie an die Instanz anhängen möchten.
    c) Aus dem Subnetz Dropdownliste, wählen Sie ein Subnetz aus.

    Hinweis: Wenn Sie mehr als eine Schnittstelle haben, stellen Sie sicher, dass sich jede Schnittstelle in einem anderen Subnetz befindet.
18. Ändern Sie im Abschnitt Speicher konfigurieren das GiB-Feld für das Root-Volume und wählen Sie **Allzweck-SSD (gp3)**.

    Weitere Informationen zur Auswahl einer Festplattengröße für die Speicherkapazität finden Sie unter Anforderungen an virtuelle Maschinen.
19. Optional: klicken **Neues Volumen hinzufügen** um ein Volume für eine präzise Paketerfassungsdiskette zu erstellen.
20. klicken **Erweiterte Details** um zusätzliche Einstellungen zu erweitern.
21. Optional: Klicken Sie auf IAM-Rolle Dropdownliste und wählen Sie eine IAM-Rolle aus.

    Hinweis: Wenn Sie einen ExtraHop-Flow-Sensor bereitstellen, sollte dies die IAM-Rolle sein, die in der Stellen Sie einen ExtraHop Flow Sensor mit AWS bereit Führer.

22. Aus dem Verhalten beim Herunterfahren Dropdownliste, wählen **Stopp**.
23. Aus dem Kündigungsschutz Dropdownliste, wählen **Aktiviere**.
24. Überprüfen Sie die AMI-Details, den Instance-Typ und die Sicherheitsgruppeninformationen und klicken Sie dann auf **Instanz starten**.
25. klicken **Alle Instanzen ansehen** um zur AWS-Managementkonsole zurückzukehren.

    Von der AWS Management Console aus können Sie Ihre Instance auf dem Initialisierungsbildschirm anzeigen. Unter dem Tisch, auf dem Beschreibung Auf der Registerkarte finden Sie die IP-Adresse oder den Hostnamen für das ExtraHop-System, auf das von Ihrer Umgebung aus zugegriffen werden kann.

Die nächsten Schritte

- Registrieren Sie Ihr ExtraHop-System.
- (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.
- Den Sensor konfigurieren.
- Überprüfen Sie die Checkliste für Sensor und Konsole nach der Bereitstellung.

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**.

Den Sensor konfigurieren

Bevor Sie beginnen
Bevor Sie den Sensor konfigurieren können, müssen Sie bereits eine Verwaltungs-IP-Adresse konfiguriert haben.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

   Der Standard-Anmeldename ist `setup` und das Passwort ist die VM-Instanz-ID.
2. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich dann an.
3. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, das Standard-Setup und die Passwörter für das Shell-Benutzerkonto zu ändern, eine Verbindung zu den ExtraHop Cloud Services herzustellen und eine Verbindung zu einer ExtraHop-Konsole herzustellen.

Nächste Schritte
Nachdem das System lizenziert ist und Sie sich vergewissert haben, dass Datenverkehr erkannt wird, führen Sie die empfohlenen Verfahren in der Checkliste nach der Bereitstellung.