

Stellen Sie Reveal (x) 360-Sensoren für AWS bereit

Veröffentlicht: 2024-04-10

Veröffentlicht: 2024-04-10

Dieses Handbuch enthält Anweisungen zur Bereitstellung der von Extrahop verwalteten Reveal (x) 360-Sensoren und zur Konfiguration Ihrer AWS-Ressourcen (ENIs) zur Spiegelung des Datenverkehrs auf Reveal (x) 360-Sensoren.

Bevor Sie beginnen

- Machen Sie sich vertraut mit [So funktioniert die Datenverkehrsspiegelung in AWS](#).
- Sie müssen über ein AWS-Benutzerkonto verfügen, das in der Lage ist, eine IAM-Rolle zu erstellen und ENI-Ressourcen zu taggen.
- Identifizieren Sie die Instances in Ihrer VPC und die zugehörigen Netzwerkschnittstellen (Quell-ENIs), von denen Sie den Datenverkehr auf die Reveal (x) 360-Sensoren spiegeln möchten. Beachten Sie, dass Sie pro Sensor nur Schnittstellen aus einer Verfügbarkeitszone auswählen können. Für Umgebungen mit Schnittstellen in mehreren Verfügbarkeitszonen siehe [Implementieren Sie Reveal \(x\) 360-Sensoren für AWS in fortschrittlichen Umgebungen](#).
- Sie benötigen System- und Zugriffsadministrationsrechte, um Reveal (x) 360 zu konfigurieren.

In den folgenden Verfahren stellen Sie Reveal (x) 360-Sensoren bereit und spiegeln den Datenverkehr von einer Quell-ENI, die an Ihre EC2-Instances angeschlossen ist, auf eine Ziel-ENI, die an den Sensor angeschlossen ist, wider.



Hinweis Für diese Verfahren müssen Sie Einstellungen in Reveal (x) 360 und in der AWS-Managementkonsole konfigurieren. Daher ist es hilfreich, alle Benutzeroberflächen nebeneinander zu öffnen.

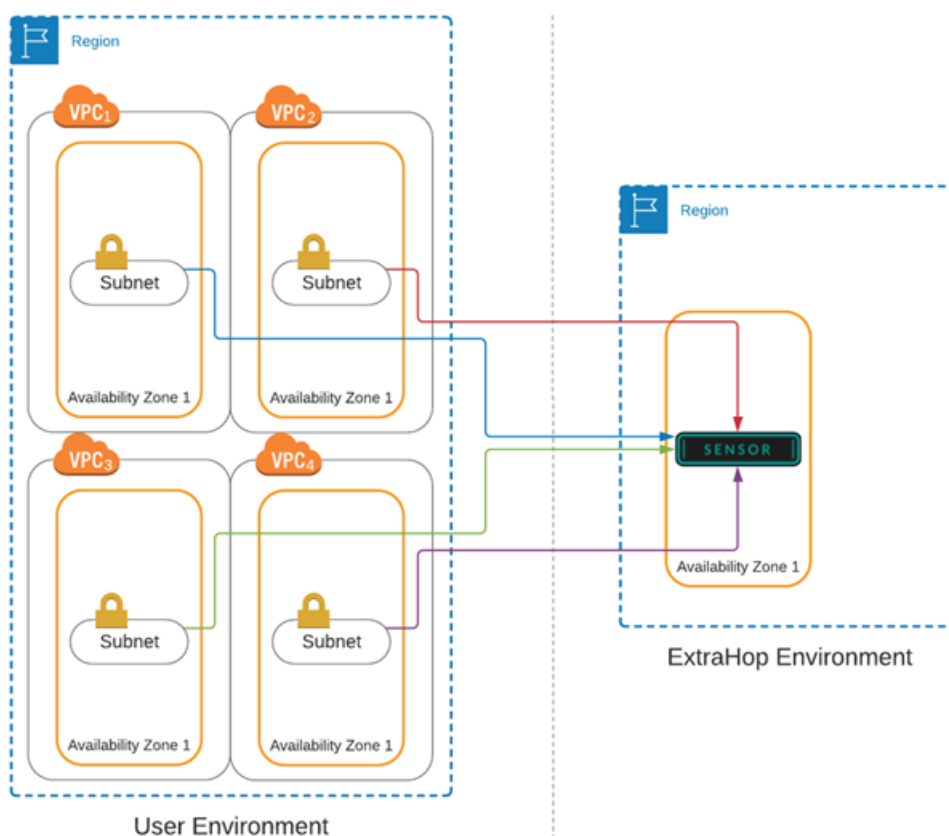


Hinweis Informationen zu selbstverwalteten Sensoren finden Sie unter [Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu Reveal \(x\) 360 her](#).

Wenn sich Ihre AWS-Workloads in einer einzigen Availability Zone (AZ) befinden, können Sie den Datenverkehr von den Subnetzen in dieser AZ auf den ExtraHop-Sensor spiegeln, ohne dass Datenübertragungskosten anfallen.


Elastic Network Interfaces (ENIs) sind an EC2-Instances angehängt. Eine ENI kann so konfiguriert werden, dass sie den Netzwerkverkehr auf eine Spiegelzielschnittstelle spiegelt. Die Anzahl der Spiegelzielschnittstellen, die Sie an einen einzelnen Sensor anschließen können, hängt von der Größe des Sensorpakets ab.

Größe des Sensors	Anzahl der Spiegelzielschnittstellen
Extra klein, Premium oder Ultra	3
Small Premium oder Ultra	3
Mittlere Prämie	7



Rufen Sie Ihre Mandanten-ID ab


Ihre Mandanten-ID ist erforderlich, um eine IAM-Rolle zu erstellen und Ihre ENI-Ressourcen in AWS zu taggen. Rufen Sie die ID von der Reveal (x) 360-Administrationsseite ab, indem Sie die folgenden Schritte ausführen.

1. Melden Sie sich über die URL, die Sie in Ihrer Willkommens-E-Mail angegeben haben, bei der Reveal (x) 360-Konsole an. Sie können auch auf das Symbol Systemeinstellungen klicken.  und dann klicken **Die gesamte Verwaltung**.
2. klicken **Ziele spiegeln**.
3. Kopieren Sie die Mandanten-ID.

Erstellen Sie eine Zielnetzwerkschnittstelle (ENI)

Sie müssen für jedes Subnetz in Ihrer VPC, das Sie mit Reveal (x) 360 überwachen möchten, eine ENI erstellen. Ein einziger Reveal (x) 360-Sensor kann ENIs nur von einer Availability Zone aus überwachen.

Weitere Informationen finden Sie in der folgenden AWS-Dokumentation: [Eine Netzwerkschnittstelle erstellen](#).

-  **Wichtig:** Sie müssen eine Sicherheitsgruppe mit einer eingehenden Regel erstellen, die es ermöglicht, dass der VXLAN-gekapselte Datenverkehr über den UDP-Port 4789 von der Traffic-Spiegelquelle zum Traffic-Mirror-Ziel gesendet wird. Es darf keine Regeln für ausgehende Nachrichten geben. Lesen Sie die AWS-Dokumentation zu [eine Sicherheitsgruppe erstellen](#).

1. Melden Sie sich bei der Amazon EC2-Managementkonsole an über <https://console.aws.amazon.com/ec2/>.

2. Im linken Bereich unter Netzwerk und Sicherheit, klicken **Netzwerkschnittstellen**.
3. klicken **Netzwerkschnittstelle erstellen** und füllen Sie die folgenden Felder aus:
 - **Beschreibung:** Geben Sie eine Beschreibung ein. Der Beschreibungstext wird im Feld Beschreibung auf der Seite Mirror Target Interfaces angezeigt.
 - **Subnetz:** Wählen Sie ein Subnetz aus der Dropdownliste aus.
 - **Private IPv4-IP:** Wählen **Automatisch zuweisen**. Wählen Sie alternativ **Benutzerdefiniert** und geben Sie dann die primäre private IPv4-Adresse in das IPv4-Adressfeld Feld. Wenn dem Subnetz ein IPv6-CIDR-Block zugeordnet ist, können Sie optional eine IPv6-Adresse angeben.
 - **Elastischer Stoffadapter:** Markieren Sie nicht das Kontrollkästchen Elastic Fabric Adapter.
 - **Sicherheitsgruppen:** Wählen Sie die Sicherheitsgruppe aus, die Sie zuvor erstellt haben, um VXLAN-Verkehr in die ENI zuzulassen.
4. klicken **Tag hinzufügen**.
5. Typ `extrahop-tenant` in der Schlüssel Feld und geben Sie Ihre Mandanten-ID in das Wert Feld.
6. klicken **Erstellen**.

Erstellen Sie eine IAM-Rolle in AWS

Mit der IAM-Rolle können Sie ExtraHop Zugriff auf die Traffic Mirror-Ziele gewähren, die Sie in AWS erstellt haben.

1. Kehren Sie zur AWS-Managementkonsole zurück.
2. In der Sicherheit, Identität und Compliance Abschnitt, klicken **ICH**.
3. Klicken Sie im linken Bereich auf **Rollen**.
4. klicken **Rolle erstellen**.
5. klicken **Ein anderes AWS-Konto**.
6. In der Geben Sie Konten an, die diesen Rollenabschnitt verwenden können, typ `895242732570` in der Konto-ID Feld.
7. Wählen Sie den **Externe ID erforderlich** Checkbox und gib deine Mandanten-ID in das Externe ID Feld.
8. klicken **Weiter: Berechtigungen**.
9. klicken **Richtlinie erstellen**. Die Seite Richtlinie erstellen wird in einem neuen Browserfenster oder einer neuen Registerkarte geöffnet.
10. Klicken Sie auf die Registerkarte JSON und fügen Sie den folgenden JSON-Text in das Feld ein, wobei der gesamte vorhandene Text ersetzt wird.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/extrahop-tenant": "<tenant-id>"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  }
]
}

```



Hinweis Die CreateNetworkInterfacePermission Mit diesem Parameter können Sie Ihr ENI an den Reveal (x) 360-Sensor anschließen.

11. Ersetze <tenant-id> mit Ihrer ExtraHop-Mandanten-ID.
12. klicken **Richtlinie überprüfen**.
13. Geben Sie einen Namen in das Politik Feld. Dieser Name kann eine beliebige Zeichenfolge sein.
14. klicken **Richtlinie erstellen**.
15. Nachdem die Richtlinie erstellt wurde, schließen Sie die **Richtlinien** Tabulatortaste und zurück zum Rolle erstellen Seite.
16. Klicken Sie auf das Aktualisierungssymbol . (Aktualisieren Sie die Browserseite nicht.)
17. In der Richtlinien filtern Feld, geben Sie den Namen der Richtlinie ein, die Sie erstellt haben.
18. Aktivieren Sie das Kontrollkästchen neben dem Richtliniennamen.
19. klicken **Weiter: Schlagworte**. Es müssen keine Tags eingegeben werden.
20. klicken **Weiter: Rückblick**.
21. In der Name der Rolle Feld, Typ ExtraHop-Vertrauen- <tenant-id>, wo <tenant-id> ist Ihre ExtraHop-Mandanten-ID. Wenn Ihre Mandanten-ID beispielsweise 12345abcd lautet, geben Sie ein ExtraHop-Trust-12345abcd.
22. klicken **Rolle erstellen**.

Fügen Sie Ihre AWS-Konten hinzu

Fügen Sie Ihre AWS-Kontoinformationen zum ExtraHop-System hinzu, um die Erkennung von Spiegelzielschnittstellen zu ermöglichen.

1. Kehren Sie zur Reveal (x) 360-Administrationsseite zurück.
2. klicken **AWS-Konten**.
3. klicken **Konto hinzufügen**.
4. Geben Sie einen Namen in das Name Feld zur Identifizierung des Kontos.
5. Geben Sie Ihre AWS-Konto-ID in das Konto-ID Feld.
6. klicken **Speichern**.
7. Wiederholen Sie die Schritte für jedes weitere AWS-Konto, für das Sie Spiegelzielschnittstellen haben.

Um ein Konto zu löschen, entfernen Sie alle mit dem Konto verbundenen Sensoren, wählen Sie den Kontonamen in der Kontenliste aus, und klicken Sie dann auf **Löschen**.

Nach Spiegelzielschnittstellen suchen

Nachdem Sie Ihre Ziel-ENIs in AWS markiert haben, müssen Sie in Reveal (x) 360 nach ihnen suchen, bevor sie an Ihre Sensor.



Wichtig: Das ExtraHop-System sucht nach Spiegelzielschnittstellen, indem es alle **unterstützte AWS-Regionen**. Es ist nicht möglich, das System so zu konfigurieren, dass das Scannen bestimmter Regionen umgangen wird. Wenn Sie den Zugriff auf eine dieser Regionen in Ihrer Umgebung einschränken, schlägt der Scanvorgang fehl. Wenden Sie sich an den ExtraHop-Support, wenn Sie nicht erfolgreich nach Spiegelzielschnittstellen suchen können.


1. Kehren Sie zur Reveal (x) 360-Administrationsseite zurück.
2. klicken **Ziele spiegeln**.
3. Auf dem Zielschnittstellen spiegeln Seite, klick **Scannen**.
Alle Schnittstellen, die Sie in AWS markiert haben, erscheinen im Zielschnittstellen spiegeln tabelle.


Tabelle 1: Unterstützte AWS-Regionen

Name der Region	Region
USA Ost (Ohio)	US-Ost-2
USA Ost (Nord-Virginia)	us-ost-1
USA West (Oregon)	US-West-2
USA West (Nordkalifornien)	us-west-1
Asien-Pazifik (Mumbai)	ap-Süd-1
Asien-Pazifik (Seoul)	ap-Nordost-2
Asien-Pazifik (Tokio)	ap-nordost-1
Asien-Pazifik (Sydney)	ap-Südost-2
Asien-Pazifik (Singapur)	ap-Southeast-1
Kanada (Zentral)	CA-Zentral-1
Europa (Frankfurt)	eu-central-1
Europa (Irland)	eu-west-1
Europa (London)	eu-west-2
Europa (Paris)	eu-west-3
Europa (Stockholm)	eu-nord-1
Südamerika (São Paulo)	sa-ost-1

Fügt Sensoren hinzu

Sie sind jetzt bereit hinzuzufügen Sensoren von der Reveal (x) 360 Administrationsseite.

-  **Wichtig:** Spiegelzielschnittstellen können dem Sensor nicht hinzugefügt oder daraus entfernt werden, nachdem der Sensor eingesetzt wurde. Wenn Sie das ENI, das der Sensor überwacht, ändern möchten, beenden Sie den Sensor und setzen Sie ein neues mit den gewünschten ENIs ein.

1. Klicken Sie auf der Reveal (x) 360 Administrationsseite auf **Sensoren einsetzen**.
2. Geben Sie einen eindeutigen Namen für Sensor in der Name Feld.
3. Wählen Sie ein Sensor Paket für Ihren Einsatz.
4. Wählen Sie eine Verfügbarkeitszonen-ID aus der Drop-down-Liste aus.
5. Aus dem Ziele spiegeln Wählen Sie in der Dropdownliste die Schnittstellen aus, die Sie an den neuen Sensor anschließen möchten. Nur die ENIs, die mit Ihrer Mandanten-ID gekennzeichnet wurden und sich in der ausgewählten Availability Zone befinden, werden in der Liste angezeigt.
6. klicken **Speichern**.
7. Optional: Wählen **Sitzungsschlüsselweiterleitung auf diesem Sensor aktivieren** wenn Sie Ihre Windows- und Linux-Server für die Weiterleitung von Sitzungsschlüsseln konfigurieren. Weitere Informationen finden Sie unter [Sitzungsschlüssel an von ExtraHOP verwaltete Sensoren weiterleiten](#) 

8. klicken **Sensor einsetzen**.

Wenn sich der Sensorstatus ändert von Ausstehend zu Laufend, Sie können Metriken, Erkennungen und Aufzeichnungen für Ihren AWS-Verkehr in Reveal (x) 360 anzeigen, indem Sie auf **Reveal (x) 360-Konsole** auf der Administrationsseite.

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 ausgehende 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**.

Sensorstatus anzeigen

1. Kehren Sie zur Reveal (x) 360-Administrationsseite zurück.
2. klicken **Sensoren** in der oberen rechten Ecke.
3. Finde deinen Sensor in der Tabelle und sieh dir die an Sensor Status.

Wenn der Sensor Wenn der Status von „Ausstehend“ zu „Wird ausgeführt“ geändert wird, können Sie Metriken, Erkennungen und Aufzeichnungen für Ihren AWS-Verkehr in Reveal (x) 360 anzeigen, indem Sie auf **Reveal (x) 360-Konsole** von der Administrationsseite.

Es kann einige Minuten dauern, bis Ihr Traffic im System erscheint.