# RPCAP für einen ExtraHop-Packetstore konfigurieren

Veröffentlicht: 2024-09-26

Wenn Sie Ihren ExtraHop konfiguriert haben Sensor für RPCAP können Sie einen zweiten Feed von Paketen konfigurieren, der von Ihrer Remote-Umgebung an den ExtraHop-Paketspeicher weitergeleitet wird.

**Bevor Sie beginnen**

- Vervollständigen Sie die Verfahren in der Paketweiterleitung mit RPCAP Anleitung zur Konfiguration Ihres Sensor.
- Stellen Sie die Trace-Appliance bereit. (Sehen Sie sich unsere Bereitstellungsinhalte an.)
- Stellen Sie sicher, dass die niedrigsten Portnummern für beide identisch sind Sensoren und Paketshops.

## Überblick über die Bereitstellung

In den folgenden Schritten werden die wichtigsten Verfahren beschrieben, die für die Implementierung von RPCAP mit einer ExtraHop Trace-Appliance erforderlich sind.

1. Konfigurieren Sie zunächst die Trace-Appliance so, dass sie RPCAP-Verkehr akzeptiert, und fügen Sie Regeln für die Paketweiterleitung hinzu.
2. Als Nächstes laden Sie die rpcapd-Software herunter für die Discover-Appliance, die für Ihre Remote-Geräte gilt. (Linux und Windows werden beide unterstützt.)
3. Installieren Sie als Nächstes die rpcapd-Software auf jedem Linux- oder Windows-Gerät, von dem Sie den Datenverkehr weiterleiten möchten. Sie müssen die Konfigurationsdatei (rpcapd.ini) ändern, um Geräteschnittstellen anzugeben oder den Datenverkehr an die Discover-Appliances weiterzuleiten.
4. Wenn Ihre Umgebung über eine Firewall verfügt, öffnen Sie schließlich Ports an Ihrer Firewall für den erforderlichen RPCAP-Verkehr.

## RPCAP auf dem ExtraHop-System konfigurieren

Es wird empfohlen, eine zweite Schnittstelle nur für RPCAP zu konfigurieren, anstatt sowohl RPCAP als auch Management auf derselben Schnittstelle zu konfigurieren. Die Konfiguration einer dedizierten RPCAP-Schnittstelle erhöht die Wahrscheinlichkeit, dass alle Pakete erfolgreich an das ExtraHop-System weitergeleitet werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. Wählen Sie Schnittstelle 1, 2, 3 oder 4.

   Der ETA 1150v hat nur die Schnittstellen 1 und 2.
4. Aus dem Schnittstellenmodus Drop-down-Liste, wählen **Geschäftsleitung + RPCAP/ERSPAN/VXLAN/GENEVE Target**.
5. Konfigurieren Sie IPv4-Adressen für die Schnittstelle, indem Sie eine der folgenden Optionen wählen:
   - Geben Sie eine statische IPv4-Adresse in der **IPv4-Adresse** Feld, und geben Sie dann eine Netzmaske und eine Gateway-IP-Adresse IP-Adresse.
   - Aktivieren Sie dynamische IPv4-Adressen, indem Sie auf **DHCPv4 aktivieren**.

   **Hinweis** Sie können zwar IPv6-Adressen auf der Schnittstelle aktivieren, aber Sie können RPCAP-Pakete nicht über IPv6 weiterleiten. Sie müssen eine IPv4-Adresse auf der Schnittstelle konfigurieren, um RPCAP zu aktivieren. Weitere Informationen zur Konfiguration einer

Management + Capture-Schnittstelle finden Sie in Häufig gestellte Fragen zu ExtraHop Hardware.

6. klicken **Speichern**.

## Regeln für die Paketweiterleitung auf dem ExtraHop-System konfigurieren

Nachdem Sie die Schnittstelle als RPCAP-Ziel konfiguriert haben, müssen Sie Regeln für die Paketweiterleitung konfigurieren. Die Regeln für die Paketweiterleitung schränken ein, welcher Datenverkehr über RPCAP an das ExtraHop-System gesendet werden darf.

Standardmäßig ist ein Eintrag für Port 2003 konfiguriert, der Datenverkehr von allen Schnittstellenadressen akzeptiert. Sie können den Standardeintrag für Ihre Umgebung ändern, den Standardeintrag löschen und weitere Einträge hinzufügen. Stellen Sie sicher, dass Sie Portnummern über 1023 angeben, um Konflikte mit reservierten Ports zu vermeiden. Es empfiehlt sich, diese Regeln zuerst festzulegen, damit das ExtraHop-System bereit ist, die weitergeleiteten Pakete zu empfangen, wenn Sie rpcapd auf Ihren Remote-Geräten konfigurieren.

Sie können bis zu 16 Regeln für die Paketweiterleitung im ExtraHop-System konfigurieren. Jede Regel muss einen einzigen TCP-Port haben, über den das ExtraHop-System die Paketweiterleitungsregeln an rpcapd-Geräte kommuniziert.

**Wichtig:** Die Informationen in der rpcapd-Konfigurationsdatei auf den Geräten , die Pakete weiterleiten, dürfen nicht den im ExtraHop-System festgelegten Regeln widersprechen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. In der RPCAP-Einstellungen Abschnitt, führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **2003** um den Standardeintrag zu öffnen.
   - klicken **Hinzufügen** um einen neuen Eintrag hinzuzufügen.

     **Wichtig:** Die Portnummern müssen 1024 oder höher sein.
4. In der RPCAP-Portdefinition hinzufügen Geben Sie im Abschnitt die folgenden Informationen ein:
   a) In der Hafen Feld, geben Sie den TCP-Port ein, der Informationen zu dieser Paketweiterleitungsregel übermittelt. Porteinträge müssen für jedes Schnittstellensubnetz auf demselben Server eindeutig sein.
   b) In der Schnittstellenadresse Feld, geben Sie die IP-Adresse oder den CIDR-Bereich der Schnittstelle auf dem Gerät ein, von dem das ExtraHop-System Datenverkehr empfangen soll. Beispielsweise leitet 10.10.0.0/24 den gesamten Datenverkehr auf dem System weiter, der Teil dieses CIDR-Bereichs ist, * ist ein Platzhalter, der dem gesamten Datenverkehr auf dem System entspricht, oder 10.10.0.5 sendet nur Verkehr auf der Schnittstelle, die der 10.10.0.5-IP-Adresse entspricht.

      **Hinweis:** Wenn eine Maschine über mehrere Schnittstellen verfügt und Sie in den Verkehrsregeln oder in der Datei rpcapd.ini keine Schnittstelle angeben, wählt das ExtraHop-System eine einzige Schnittstelle aus, von der der Datenverkehr weitergeleitet wird. Das ExtraHop-System wählt normalerweise die Schnittstelle mit dem Namen aus, der alphabetisch an erster Stelle steht. Wir empfehlen jedoch, dass Sie die Schnittstelle in den Verkehrsregeln angeben, um ein konsistentes Verhalten sicherzustellen. Wir empfehlen außerdem, die Schnittstelle nach Adresse und nicht nach Namen auszuwählen.
   c) In der Name der Schnittstelle Feld, geben Sie den Namen der Schnittstelle auf dem Gerät ein, die den Datenverkehr an das ExtraHop-System sendet. Zum Beispiel `eth0` in einer Linux-Umgebung oder `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}` in einer Windows-Umgebung.

d) In der Filter Feld, geben Sie die Ports für den Verkehr, den Sie an das ExtraHop-System weiterleiten möchten, in der Berkeley Packet Filter (BPF) -Syntax ein. Sie können beispielsweise eingeben `TCP-Anschluss 80` um den gesamten Verkehr auf TCP-Port 80 von Ihrem Remote-Netzwerkgerät an das ExtraHop-System weiterzuleiten. Weitere Hinweise zur BPF-Syntax finden Sie unter Pakete mit der Berkeley-Paketfilter-Syntax filtern.

5. klicken **Speichern**, wodurch die Einstellungen gespeichert und die Erfassung neu gestartet werden.
6. Wiederholen Sie diese Schritte, um zusätzliche Regeln zu konfigurieren. Sie können bis zu 16 Regeln hinzufügen.

## Speichern Sie die laufende Konfigurationsdatei

Nachdem Sie die Schnittstelle konfiguriert und die Regeln für die Paketweiterleitung konfiguriert haben, müssen Sie die Änderungen in der laufenden Konfigurationsdatei speichern.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. klicken **Änderungen ansehen und speichern**.
4. Überprüfen Sie die Änderungen in der Aktuelle laufende Konfiguration (noch nicht gespeichert) Fensterscheibe.
5. klicken **Speichern**.
6. klicken **Erledigt**.

## Fügen Sie Einträge für die Trace-Appliance zu Ihren rpcapd-Linux-Geräten hinzu

Führen Sie die folgenden Schritte aus, um mit dem Senden von Paketen von Linux-Remotegeräten an die Trace-Appliance zu beginnen.

1. Öffnen Sie die rpcapd-Konfigurationsdatei (/opt/extrahop/etc/rpcapd.ini) in einem Texteditor. Die Konfigurationsdatei enthält Text, der dem folgenden Beispiel ähnelt:

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
UserName = rpcapd
```

2. Fügen Sie am Ende der Datei einen weiteren ActiveClient-Eintrag mit der IP-Adresse Ihrer Trace-Appliance und dem niedrigsten Port hinzu, mit dem Ihre Discover-Appliance konfiguriert ist . Im folgenden Beispiel lautet die IP-Adresse für die Discover-Appliance 10.0.0.100 und die IP-Adresse für die Trace-Appliance lautet 10.1.20.1, und beide Appliances hören den TCP-Port 2003 ab.

```
ActiveClient = 10.0.0.100,2003
ActiveClient = 10.1.20.1,2003
NullAuthPermit = YES
UserName = rpcapd
```

**Hinweis:** Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.

3. Starten Sie den RPCAP-Prozess neu, nachdem Sie die Konfigurationsdatei (rpcapd.ini) bearbeitet haben.

Für Beispielkonfigurationen, siehe die Anleitung Paketweiterleitung mit RPCAP.

## Fügen Sie Einträge für die Trace-Appliance zu Ihren rpcapd-Windows-Geräten hinzu

Führen Sie die folgenden Schritte aus, um mit dem Senden von Paketen von Windows-Remote-Geräten an die Trace-Appliance zu beginnen.

1. Öffnen Sie die rpcapd-Konfigurationsdatei (C:\Program Files\ rpcapd\ rpcapd.ini). Die Datei enthält Text ähnlich dem folgenden:

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
UserName = rpcapd
```

   **Hinweis** Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.

2. Fügen Sie am Ende der Datei einen weiteren ActiveClient-Eintrag mit der IP-Adresse Ihrer Trace-Appliance und dem niedrigsten Port hinzu, mit dem Ihre Discover-Appliance konfiguriert ist . Im folgenden Beispiel lautet die IP-Adresse für die Discover-Appliance 10.0.0.100 und die IP-Adresse für die Trace-Appliance lautet 10.1.20.1, und beide Appliances hören den TCP-Port 2003 ab.

```
ActiveClient = 10.0.0.100,2003
ActiveClient = 10.1.20.1,2003
NullAuthPermit = YES
UserName = rpcapd
```

3. Starten Sie den rpcapd-Prozess neu, nachdem Sie die Konfigurationsdatei (rpcapd.ini) bearbeitet haben.

Für Beispielkonfigurationen, siehe die Anleitung Paketweiterleitung mit RPCAP.