


PCAP konfigurieren

Veröffentlicht: 2024-04-09

Mit der Paketerfassung können Sie Datenpakete aus Ihrem Netzwerkverkehr sammeln, speichern und abrufen. Sie können eine Paketerfassungsdatei zur Analyse in einem Drittanbieter-Tool wie Wireshark herunterladen. Pakete können überprüft werden, um Netzwerkprobleme zu diagnostizieren und zu lösen und um sicherzustellen, dass die Sicherheitsrichtlinien eingehalten werden.

Durch Hinzufügen einer Paketerfassungsdiskette zum ExtraHop Sensor, können Sie die an Ihr ExtraHop-System gesendeten Rohdaten speichern. Diese Festplatte kann zu Ihrer virtuellen Festplatte hinzugefügt werden Sensor oder eine SSD, die in Ihrem physischen Gerät installiert ist Sensor.

Diese Anweisungen gelten nur für ExtraHop-Systeme, die über eine Precision Paket Capture Disk verfügen. Informationen zum Speichern von Paketen auf einer ExtraHop PacketStore-Appliance finden Sie in der [Anleitungen zur Bereitstellung von Packetstore](#).

-  **Wichtig:** Systeme mit selbstverschlüsselnden Festplatten (SEDs) können nicht für die Softwareverschlüsselung bei Paketerfassungen konfiguriert werden. Informationen zur Aktivierung der Sicherheit auf diesen Systemen finden Sie unter [Konfigurieren Sie selbstverschlüsselnde Festplatten \(SEDs\)](#).

Päckchen schneiden

Standardmäßig speichert der Packetstore ganze Pakete. Wenn Pakete noch nicht in Scheiben geschnitten sind, können Sie den Sensor so konfigurieren, dass er Pakete speichert, die auf eine feste Anzahl von Byte aufgeteilt sind, um den Datenschutz und das Lookback zu verbessern.


Weitere Informationen zur Konfiguration dieser Funktion in Ihrer laufenden Konfigurationsdatei erhalten Sie vom ExtraHop-Support.

PCAP aktivieren

Ihr ExtraHop-System muss für die PCAP lizenziert und mit einer dedizierten Speicherplatte konfiguriert sein. Körperlich Sensoren erfordern eine SSD-Speicherfestplatte und virtuelle Sensoren erfordern eine Festplatte, die auf Ihrem Hypervisor konfiguriert ist.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihr ExtraHop-System für Packet Capture lizenziert ist, indem Sie sich bei den Administrationseinstellungen anmelden und auf **Lizenz**. Packet Capture ist unter Funktionen aufgeführt und **Aktiviert** sollte erscheinen.

-  **Wichtig:** Der Erfassungsvorgang wird neu gestartet, wenn Sie die Paketerfassungsdiskette aktivieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Appliance-Einstellungen auf **Festplatten**.
3. Abhängig von deinem Sensor Typ- und Menüoptionen, konfigurieren Sie die folgenden Einstellungen.
 - Für physische Sensoren klicken Sie **Aktivieren** neben SSD Assisted Packet Capture, und klicken Sie dann auf **OK**.
 - Stellen Sie für virtuelle Sensoren sicher, dass `running` wird in der Spalte Status angezeigt und dass die Festplattengröße, die Sie für die PCAP konfiguriert haben, in der Spalte Größe angezeigt wird. klicken **Aktivieren** neben Triggered Packet Capture, und klicken Sie dann auf **OK**.

Nächste Schritte


Ihre Paketerfassungsdiskette ist jetzt aktiviert und bereit, Pakete zu speichern. Klicken **konfigurieren** wenn Sie die Festplatte verschlüsseln oder konfigurieren möchten **weltweite** oder **Präzisionspaket** erfasst.

Verschlüsseln Sie die Paketerfassungsdiskette

Festplatten zur Paketerfassung können mit 256-Bit-AES-Verschlüsselung gesichert werden.

Hier sind einige wichtige Überlegungen, bevor Sie eine Paketerfassungsdiskette verschlüsseln:

- Sie können eine Paketerfassungsdiskette nicht entschlüsseln, nachdem sie verschlüsselt wurde. Sie können die Verschlüsselung löschen, aber die Festplatte ist formatiert und alle Daten werden gelöscht.
- Sie können eine verschlüsselte Festplatte sperren, um jeglichen Lese- oder Schreibzugriff auf gespeicherte Paketerfassungsdateien zu verhindern. Wenn das ExtraHop-System neu gestartet wird, werden verschlüsselte Festplatten automatisch gesperrt und bleiben gesperrt, bis sie mit der Passphrase entsperrt werden. Unverschlüsselte Festplatten können nicht gesperrt werden.
- Sie können eine verschlüsselte Festplatte neu formatieren, aber alle Daten werden dauerhaft gelöscht. Sie können eine gesperrte Festplatte neu formatieren, ohne sie zuerst zu entsperren.
- Sie können alle Systemdaten sicher löschen (oder das System löschen). Anweisungen finden Sie in der [Medienleitfaden für ExtraHop Rescue](#).

 **Wichtig:** Systeme mit selbstverschlüsselnden Festplatten (SEDs) können nicht für die Softwareverschlüsselung bei Paketerfassungen konfiguriert werden. Informationen zur Aktivierung der Sicherheit auf diesen Systemen finden Sie unter [Konfigurieren Sie selbstverschlüsselnde Festplatten \(SEDs\)](#).

1. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Sensortyp eine der folgenden Optionen aus.
 - Für virtuelle Sensoren klicken Sie auf **Konfigurieren** neben Triggered Packet Capture.
 - Für physische Sensoren klicken Sie auf **Konfigurieren** neben SSD Assisted Packet Capture.
3. Klicken **Festplatte verschlüsseln**.
4. Geben Sie einen Festplattenverschlüsselungsschlüssel aus einer der folgenden Optionen an:
 - Geben Sie eine Passphrase in die Felder Passphrase und Bestätigen ein.
 - Klicken **Wählen Sie Datei** und wählen Sie eine Verschlüsselungsschlüsseldatei aus.
5. Klicken **Verschlüsseln**.

Nächste Schritte

Sie können den Festplattenverschlüsselungsschlüssel ändern, indem Sie zur Seite Festplatten zurückkehren und auf **Konfigurieren** und dann **Festplattenverschlüsselungsschlüssel ändern**.

Formatieren Sie die Paketerfassungsdiskette

Sie können eine verschlüsselte Paketerfassungsdiskette so formatieren, dass alle Paketerfassungen dauerhaft entfernt werden. Durch das Formatieren einer verschlüsselten Festplatte wird die Verschlüsselung entfernt. Wenn Sie einen unverschlüsselten Paketerfassungsdatenträger formatieren möchten, müssen Sie den Datenträger entfernen und ihn dann erneut aktivieren.

 **Warnung:** Diese Aktion kann nicht rückgängig gemacht werden.

1. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Appliance-Plattform eine der folgenden Optionen aus.
 - Für virtuelle Sensoren klicken Sie **konfigurieren** neben Triggered Packet Capture.
 - Für physische Sensoren klicken Sie auf **konfigurieren** neben SSD Assisted Packet Capture.
3. klicken **Festplattenverschlüsselung löschen**.

4. klicken **Format**.

Entfernen Sie die Paketerfassungsdiskette

Wenn Sie eine Paketerfassungsdiskette ersetzen möchten, müssen Sie zuerst die Festplatte aus dem System entfernen. Wenn eine Paketerfassungsdiskette aus dem System entfernt wird, werden alle Daten auf der Festplatte dauerhaft gelöscht.

Um die Festplatte zu entfernen, muss eine Formatoption ausgewählt werden. Auf physischen Appliances können Sie die Festplatte nach Abschluss dieses Vorgangs sicher aus der Appliance entfernen.

1. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Appliance-Plattform eine der folgenden Optionen aus.
 - Für virtuelle Appliances klicken Sie auf **konfigurieren** neben Triggered Packet Capture.
 - Für physische Geräte klicken Sie auf **konfigurieren** neben SSD Assisted Packet Capture.
3. klicken **Festplatte entfernen**.
4. Wählen Sie eine der folgenden Formatoptionen aus:
 - **Schnelles Formatieren**
 - **Sicheres Löschen**
5. klicken **entfernen**.

Konfigurieren Sie eine globale PCAP

Eine globale PCAP sammelt jedes Paket, das an das ExtraHop-System gesendet wird, für die Dauer, die den Kriterien entspricht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Paketerfassungen auf **Globale Paketerfassung**.
3. In der Starten Sie die globale Paketerfassung Abschnitt, füllen Sie die folgenden Felder aus. Sie müssen nur die gewünschten Kriterien für die Paketerfassung angeben:
 - **Name:** Ein Name zur Identifizierung der PCAP.
 - **Max. Anzahl Pakete:** Die maximale Anzahl von Paketen, die erfasst werden sollen.
 - **Max. Byte:** Die maximale Anzahl von Byte, die erfasst werden sollen.
 - **Max. Dauer (Millisekunden):** Die maximale Dauer der PCAP in Millisekunden. Wir empfehlen den Standardwert 1000 (1 Sekunde) oder eine Konfiguration von bis zu 60000 Millisekunden (1 Minute).
 - **Snaps:** Die maximale Anzahl von Byte, die pro Frame kopiert werden. Der Standardwert ist 96 Byte, aber Sie können diesen Wert auf eine Zahl zwischen 1 und 65535 setzen.
4. klicken **Start**.



Hinweis: Notieren Sie sich die Uhrzeit, zu der Sie mit der Erfassung beginnen, damit Sie die Pakete leichter finden können.

5. klicken **Stopp** um die Paketerfassung zu beenden, bevor eine der Höchstgrenzen erreicht ist.

Laden Sie Ihre PCAP herunter.

- Klicken Sie auf Reveal (x) Enterprise systems auf **Pakete** aus dem oberen Menü und dann klicken **PCAP herunterladen**.

Um Ihre PCAP zu finden, klicken und ziehen Sie auf die Zeitleiste der Paketabfrage, um den Zeitraum auszuwählen, in dem Sie die PCAP gestartet haben.

- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen , klicken Sie **Die gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Packet Capture.

Konfigurieren Sie eine präzise PCAP

Präzise Paketerfassungen erfordern ExtraHop-Trigger, mit denen Sie nur die Pakete erfassen können, die Ihren Spezifikationen entsprechen. Trigger sind hochgradig anpassbarer benutzerdefinierter Code, der bei definierten Systemereignissen ausgeführt wird.


Bevor Sie beginnen

Die Paketerfassung muss auf Ihrem ExtraHop-System lizenziert und aktiviert sein.

Es wird empfohlen, dass Sie sich mit dem Schreiben von Triggern vertraut machen, bevor Sie eine präzise PCAP konfigurieren. Hier sind einige Ressourcen, die Ihnen helfen sollen, mehr über ExtraHop-Trigger zu erfahren:

- [Trigger-Konzepte](#)
- [Einen Auslöser erstellen](#)
- [Trigger-API-Referenz](#)
- Gehen Sie durch: [Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren](#)

Im folgenden Beispiel erfasst der Auslöser einen HTTP-Flow mit dem Namen `HTTP host <hostname>` und stoppt die Erfassung, nachdem maximal 10 Pakete gesammelt wurden.

1. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Auslöser**.
2. klicken **Erstellen**.
3. Geben Sie einen Namen für den Auslöser ein und wählen Sie die Ereignisse `HTTP_REQUEST` und `HTTP_RESPONSE` aus.
4. Geben oder fügen Sie den folgenden Triggercode in den rechten Bereich ein.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Weisen Sie den Auslöser einem Gerät oder einer Gruppe von Geräten zu.





Warnung: Das Ausführen von Triggern auf nicht benötigten Geräten und Netzwerken erschöpft die Systemressourcen. Minimiere die Auswirkungen auf die Leistung, indem du einen Auslöser nur den spezifischen Quellen zuweist, aus denen du Daten sammeln musst.

6. Wählen **Auslöser aktivieren**.
7. klicken **Speichern**.

Nächste Schritte

Laden Sie die Paketerfassungsdatei herunter.

- Klicken Sie auf **Reveal (x) Enterprise systems** auf **Rekorde** aus dem oberen Menü. Wählen **Erfassung von Paketen** von der Art des Datensatzes Drop-down-Liste. Nachdem die mit Ihrer PCAP verknüpften Datensätze angezeigt wurden, klicken Sie auf das Paketsymbol , und klicken Sie dann auf **PCAP herunterladen**.
- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen , klicken **Gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Packet Capture.

Paketerfassungen anzeigen und herunterladen

Wenn Sie Paketerfassungen auf einer virtuellen Festplatte oder auf einer SSD-Festplatte in Ihrem Sensor, können Sie diese Dateien auf der Seite „Paketerfassungen anzeigen“ in den Administrationseinstellungen verwalten. Sehen Sie sich für Reveal (x) -Systeme und ExtraHop-Packetstores die Seite Pakete an.

Der Abschnitt Paketerfassungen anzeigen und herunterladen wird nur auf ExtraHop Performance-Systemen angezeigt. Auf Reveal (x) -Systemen werden präzise Paketerfassungsdateien gefunden, indem Datensätze nach dem Datensatztyp für die PCAP durchsucht werden.

- klicken **Einstellungen für die PCAP konfigurieren** um gespeicherte Paketerfassungen nach der angegebenen Dauer (in Minuten) automatisch zu löschen.
- Sehen Sie sich Statistiken über Ihre Paketerfassungsdiskette an.
- Geben Sie Kriterien an, um Paketerfassungen zu filtern und die Anzahl der in der Paketerfassungsliste angezeigten Dateien zu begrenzen.
- Wählen Sie eine Datei aus der Packet Capture-Liste aus und laden Sie die Datei herunter oder löschen Sie sie.



Hinweis Sie können keine einzelnen Paketerfassungsdateien aus Reveal (x) -Systemen löschen.