

Stellen Sie den ExtraHop EFC 1292v NetFlow Sensor bereit

Veröffentlicht: 2025-01-04

In diesem Handbuch wird erklärt, wie Sie den EFC 1292v NetFlow Virtual bereitstellen Sensor.

Der EFC 1292v wurde entwickelt, um eine Verbindung zu RevealX 360 und RevealX Enterprise herzustellen und NetFlow-Datensätze aus Ihrem Netzwerk zu sammeln. Eine Paketanalyse ist nicht verfügbar.

Anforderungen an das System

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen virtuellen EFC 1292v-Sensor auf Linux KVM oder VMware vSphere bereitzustellen:

- Sie müssen mit der Verwaltung von Linux KVM oder VMware vertraut sein.
- Sie benötigen die ExtraHop-Bereitstellungsdatei, die auf der [ExtraHop Kundenportal](#).
- Sie müssen einen ExtraHop EFC 1292v haben Sensor Produktschlüssel.
- Sie sollten ein Upgrade auf den neuesten Patch für die Linux-KVM- oder vSphere-Umgebung durchführen, um bekannte Probleme zu vermeiden.

Anforderungen an virtuelle Maschinen

Sie müssen einen Hypervisor bereitstellen, der den folgenden Spezifikationen für den virtuellen Computer am ehesten entspricht Sensor.

Fühler	vCPUs	RAM	Festplatte
1100 V	4	8 GB	46 GB

Überblick über die Bereitstellung

Das Sammeln von NetFlow-Datensätzen erfordert die folgende Konfiguration.

- Stellen Sie eine ExtraHop-Sensorinstanz in Linux KVM oder VMware bereit. Weitere Informationen finden Sie unter [Stellen Sie einen ExtraHop-Sensor auf Linux KVM bereit](#) oder [Stellen Sie den ExtraHop-Sensor auf VMware bereit](#).
- Schnittstellen konfigurieren.
- Konfigurieren Sie die NetFlow-Einstellungen auf dem ExtraHop-System.

Schnittstellen konfigurieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle `<interface number>` Seite, von der **Schnittstellen-Modus** Drop-down-Menü, wählen **Management + Flow-Ziel**.
5. Deaktivieren Sie alle verbleibenden Schnittstellen, da der Sensor NetFlow- und wire data nicht gleichzeitig verarbeiten kann:

- a) In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
 - b) Aus dem **Schnittstellen-Modus** Drop-down-Menü, wählen **Deaktiviert**.
 - c) Wiederholen Sie diesen Vorgang, bis alle zusätzlichen Schnittstellen deaktiviert sind.
6. Klicken Sie **Speichern**.

NetFlow-Einstellungen konfigurieren

Sie müssen die Port- und Netzwerkeinstellungen auf dem EFC 1292v NetFlow Virtual konfigurieren Sensor bevor Sie NetFlow-Datensätze sammeln können. Der EFC 1292v Sensor unterstützt die folgenden Flow-Technologien: Cisco NetFlow v5/v9 und IPFIX.

Sie müssen sich als Benutzer anmelden mit [System- und Zugriffsadministrationsrechte](#) um die folgenden Schritte abzuschließen.

Konfigurieren Sie den Flow-Typ und den UDP-Port

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **NetFlow**.
3. In der Häfen Abschnitt, aus dem Hafen Feld, geben Sie die UDP-Portnummer ein.
Der Standardport für Net Flow ist 2055. Sie können bei Bedarf weitere Ports für Ihre Umgebung hinzufügen.



Hinweis Die Portnummern müssen 1024 oder höher sein

4. Aus dem Durchflusstyp Drop-down-Menü, wählen **NetFlow**.
5. Klicken Sie auf das Plus-Symbol (+), um den Port hinzuzufügen.

Zulässige Netzwerke hinzufügen

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **NetFlow**.
3. In der Zulässige Netzwerke Abschnitt, klicken **Genehmigtes Netzwerk hinzufügen**.
4. Aus dem Durchflusstyp Drop-down-Menü, wählen **NetFlow**.
5. Für IP-Adresse, geben Sie die IPv4- oder IPv6-Adresse ein.
6. Für Netzwerk-ID, geben Sie einen Namen ein, um dieses zugelassene Netzwerk zu identifizieren.
7. Klicken Sie **Speichern**.

Entdecken Sie NetFlow-Geräte

Sie können das ExtraHop-System so konfigurieren, dass es NetFlow-Geräte erkennt, indem Sie eine Reihe von IP-Adressen hinzufügen.



Hinweis ExtraHop-Systeme unterstützen NetFlow mit Samples nicht. Wenn Sie NetFlow-Samples in Ihren Datenverkehr einbeziehen, kann dies zu ungenauen Gerätekennzahlen führen, aber die Geräteerkennung sollte weiterhin wie gewohnt funktionieren.

Hier sind einige wichtige Überlegungen zu Remote L3 Discovery:

- Mit NetFlow werden Geräte, die die Gateways darstellen, die Datensätze exportieren, automatisch erkannt. Sie können das ExtraHop-System so konfigurieren, dass Geräte erkannt werden, die die in NetFlow-Datensätzen beobachteten IP-Adressen repräsentieren, indem Sie einen Bereich von IP-Adressen hinzufügen.

- Seien Sie vorsichtig, wenn Sie die CIDR-Notation angeben. Ein /24-Subnetzpräfix kann dazu führen, dass 255 neue Geräte vom ExtraHop-System entdeckt werden. Ein breites /16-Subnetzpräfix kann dazu führen, dass 65.535 neue Geräte entdeckt werden, was Ihr Gerätelimit überschreiten könnte.
 - Wenn eine IP-Adresse aus den Gerät Discovery-Einstellungen entfernt wird, bleibt die IP-Adresse im ExtraHop-System als Remote-L3-Gerät bestehen, solange aktive Datenflüsse für diese IP-Adresse existieren oder bis die Erfassung neu gestartet wird. Nach einem Neustart wird das Gerät als inaktives Remote-L3-Gerät aufgeführt.
1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
 2. In der Netzwerkeinstellungen Abschnitt, klicken **NetFlow**.
 3. In der NetFlow-Geräteerkennung Abschnitt, geben Sie die IP-Adresse in das IP-Adressbereiche Feld. Sie können eine IP-Adresse oder eine CIDR-Notation angeben, z. B. `192.168.0.0/24` für ein IPv4-Netzwerk oder `2001:db8::/32` für ein IPv6-Netzwerk.
 - ⓘ **Wichtig:** Jede aktiv kommunizierende Remote-IP-Adresse, die dem CIDR-Block entspricht, wird im ExtraHop-System als einzelnes Gerät erkannt. Die Angabe breiter Subnetzpräfixe wie /16 kann dazu führen, dass Tausende von Geräten erkannt werden, wodurch Ihr Gerätelimit möglicherweise überschritten wird.
 4. Klicken Sie auf das grüne Plusymbol (+), um die IP-Adresse hinzuzufügen.

Nächste Schritte

Sie können eine weitere IP-Adresse oder einen weiteren IP-Adressbereich hinzufügen, indem Sie die Schritte 3 bis 4 wiederholen.