

Déployez le capteur NetFlow ExtraHop EFC 1292v

Publié: 2024-09-26

Ce guide explique comment déployer le système virtuel NetFlow EFC 1292v sonde.

L'EFC 1292v est conçu pour se connecter à RevealX 360 et RevealX Enterprise et collecter des enregistrements NetFlow depuis votre réseau. L'analyse des paquets n'est pas disponible.

Exigences du système

Votre environnement doit répondre aux exigences suivantes pour déployer une sonde virtuelle EFC 1292v sur Linux KVM ou VMware vSphere :

- Vous devez être familiarisé avec l'administration de Linux KVM ou de VMware VMWare.
- Vous devez disposer du fichier de déploiement ExtraHop, disponible sur [Portail client ExtraHop](#).
- Vous devez avoir un ExtraHop EFC 1292v sonde clé de produit.
- Vous devez effectuer la mise à niveau vers le dernier correctif pour l'environnement Linux KVM ou vSphere afin d'éviter tout problème connu.

Exigences relatives aux machines virtuelles

Vous devez configurer un hyperviseur qui correspond le mieux aux spécifications suivantes pour le réseau virtuel sonde.

Sonde	vCPU	RAM	Disque
1100 V	4	8 GO	46 GO

Vue d'ensemble du déploiement

La collecte des enregistrements NetFlow nécessite la configuration suivante.

- Déployez une instance de sonde ExtraHop sous Linux KVM ou VMware. Pour plus d'informations, voir [Déployer une sonde ExtraHop sur Linux KVM](#) ou [Déploiement de la sonde ExtraHop sur VMware](#).
- Configurez les interfaces.
- Configurez les paramètres NetFlow sur le système ExtraHop.

Configuration des interfaces

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface `<interface number>` page, à partir de **Mode d'interface** menu déroulant, sélectionnez **Gestion + Cible de flux**.
5. Désactivez toutes les interfaces restantes, car la sonde ne peut pas traiter simultanément les données NetFlow et Wire Data :
 - a) Dans le Interfaces section, cliquez sur le nom de l' interface que vous souhaitez configurer.
 - b) À partir du **Mode d'interface** menu déroulant, sélectionnez **Désactivé**.

- c) Répétez l'opération jusqu'à ce que toutes les interfaces supplémentaires soient désactivées.
6. Cliquez **Enregistrer**.

Configure NetFlow settings

You must configure port and network settings on the EFC 1292v NetFlow virtual sensor before you can collect NetFlow records. The EFC 1292v sensor supports the following flow technologies: Cisco NetFlow v5/v9 and IPFIX.

You must log in as a user with **System and Access Administration privileges** [↗](#) to complete the following steps.

Required NetFlow fields

ExtraHop parses only NetFlow v5 fields, and all v5 fields must be present in records sent to the sensor.


Field	Description
srcaddr	Source IP address
dstaddr	Destination IP address
nexthop	IP address of next hop router
input	SNMP index of input interface
output	SNMP index of output interface
dPkts	Packets in the flow
dOctets	Total number of Layer 3 bytes in the packets of the flow
First	SysUptime at start of flow
Last	SysUptime at the time the last packet of the flow was received
srcport	TCP/UDP source port number or equivalent
dstport	TCP/UDP destination port number or equivalent
tcp_flags	Cumulative OR of TCP flags
prot	IP protocol type (for example, TCP = 6; UDP = 17)
tos	IP type of service (ToS)
src_as	Autonomous system number of the source, either origin or peer
dst_as	Autonomous system number of the destination, either origin or peer
src_mask	Source address prefix mask bits
dst_mask	Destination address prefix mask bits

For more information, see [NetFlow V5 formats](#) [↗](#).

Configure the flow type and UDP port

1. In the Network Settings section, click **NetFlow**.
2. In the Ports section, from the Port field, type the UDP port number.

The default port for Net Flow is 2055. You can add additional ports as needed for your environment.

 **Note:** Port numbers must be 1024 or greater

3. From the Flow Type drop-down menu, select **NetFlow**.
4. Click the plus icon (+) to add the port.

Add approved networks

1. In the Network Settings section, click **NetFlow**.
2. In the Approved Networks section, click **Add Approved Network**.
3. From the Flow Type drop-down menu, select **NetFlow**.
4. For IP address, type the IPv4 or IPv6 address.
5. For Network ID, type a name to identify this approved network.
6. Click **Save**.

Discover NetFlow devices

You can configure the ExtraHop system to discover NetFlow devices by adding a range of IP addresses.




Note: ExtraHop systems do not support sampled NetFlow. Including sampled NetFlow in your traffic might result in inaccurate device metrics, but device discovery should still function as normal.

Here are some important considerations about Remote L3 Discovery:

- With NetFlow, devices that represent the gateways exporting records are automatically discovered. You can configure the ExtraHop system to discover devices that are representing the IP addresses observed in NetFlow records by adding a range of IP addresses.
- Exercise caution when specifying CIDR notation. A /24 subnet prefix might result in 255 new devices discovered by the ExtraHop system. A wide /16 subnet prefix might result in 65,535 new devices discovered, which might exceed your device limit.
- If an IP address is removed from the Device Discovery settings, the IP address will persist in the ExtraHop system as a remote L3 device as long as there are existing active flows for that IP address or until the capture is restarted. After a restart, the device is listed as an inactive remote L3 device.

1. In the Network Settings section, click **NetFlow**.
2. In the NetFlow Device Discovery section, type the IP address in the IP address ranges field.

You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.

 **Important:** Every actively-communicating remote IP address that matches the CIDR block will be discovered as a single device in the ExtraHop system. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.

3. Click the green plus icon (+) to add the IP address.

Next steps

You can add another IP address or range of IP addresses by repeating steps 3-4.