Déployez le capteur NetFlow ExtraHop EFC 1292v

Publié: 2024-04-10

Ce guide explique comment déployer l'appliance virtuelle à sonde NetFlow EFC 1292v.

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

Prérequis

Votre environnement doit répondre aux exigences suivantes pour déployer une sonde EFC 1292v :

- Accès à une sonde virtuelle (ExtraHop 1100v) sous Linux KVM ou VMware
- Une clé de produit EFC 1292v

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 Déployez la sonde ExtraHop avec 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 et objectif de flux**.
5. Désactivez toutes les interfaces restantes, car la sonde ne peut pas traiter les données NetFlow et Wire Data simultanément :
   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 **Handicap**.
   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 sensor before you can collect NetFlow records. The ExtraHop system 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.

Configure the flow type and UDP port

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **NetFlow**.
3. 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
4. From the Flow Type drop-down menu, select **NetFlow**.
5. Click the plus icon (**+**) to add the port.

Add approved networks

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **NetFlow**.
3. In the Approved Networks section, click **Add Approved Network**.
4. From the Flow Type drop-down menu, select **NetFlow**.
5. For IP address, type the IPv4 or IPv6 address.
6. For Network ID, type a name to identify this approved network.
7. Click **Save**.

Discover NetFlow devices

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

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. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **NetFlow**.
3. 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.
4. 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.