Déployez le capteur NetFlow ExtraHop EFC 1292v

Publié: 2025-03-28

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 d'une 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 la **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**.

Configuration des paramètres NetFlow

Vous devez configurer les paramètres de port et de réseau sur le serveur virtuel NetFlow EFC 1292v sonde avant de pouvoir collecter des enregistrements NetFlow. L'EFC 1292v sonde prend en charge les technologies de flux suivantes : Cisco NetFlow v5/v9 et IPFIX.

Vous devez vous connecter en tant qu'utilisateur avec Privilèges d'administration du système et des accès pour effectuer les étapes suivantes.

Champs NetFlow obligatoires

ExtraHop analyse uniquement les champs NetFlow v5, et tous les champs v5 doivent être présents dans les enregistrements envoyés à la sonde.

Champ	Descriptif
srcaddr	adresse IP source
dstaddr	adresse IP de destination
prochaine étape	adresse IP du routeur Next Hop
entrée	Index SNMP de l'interface d'entrée
sortie	Indice SNMP de l'interface de sortie
DPCT	Paquets dans le flux
DocTets	Nombre total d'octets de couche 3 dans les paquets du flux
D'abord	SysUpTime au début du flux
Dernier	SysUpTime au moment où le dernier paquet du flux a été reçu
srcport	Numéro de port source TCP/UDP ou équivalent
dstport	Numéro de port de destination TCP/UDP ou équivalent
drapeaux TCP	OR cumulatif des indicateurs TCP
port	Type de protocole IP (par exemple, TCP = 6 ; UDP = 17)
jouets	Type de service IP (ToS)
src_as	Numéro de système autonome de la source, qu'il s'agisse d'origine ou d' homologue
dst_as	Numéro de système autonome de la destination, origine ou homologue
masque_src	Bits de masque de préfixe d'adresse source
masque_dst	Bits de masque de préfixe d'adresse de destination

Pour plus d'informations, voir Formats NetFlow V5.

Configurer le type de flux et le port UDP

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 **NetFlow**.

3. Dans le Ports section, de la Port dans ce champ, saisissez le numéro de port UDP.

   Le port par défaut pour Net Flow est `2055`. Vous pouvez ajouter des ports supplémentaires selon les besoins de votre environnement.

   Note: Les numéros de port doivent être de 1024 ou plus

4. À partir du Type de flux menu déroulant, sélectionnez **NetFlow**.
5. Cliquez sur l'icône plus (**+**) pour ajouter le port.

Ajouter des réseaux approuvés

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 **NetFlow**.
3. Dans le Réseaux approuvés section, cliquez sur **Ajouter un réseau approuvé**.
4. À partir du Type de flux menu déroulant, sélectionnez **NetFlow**.
5. Pour adresse IP, saisissez l'adresse IPv4 ou IPv6.
6. Pour ID réseau, saisissez un nom pour identifier ce réseau approuvé.
7. Cliquez **Enregistrer**.

Découvrez les appareils NetFlow

Vous pouvez configurer le système ExtraHop pour détecter les appareils NetFlow en ajoutant une plage d'adresses IP.

Note: Les systèmes ExtraHop ne prennent pas en charge le NetFlow échantillonné. L'inclusion d'un échantillon de NetFlow dans votre trafic peut entraîner des statistiques inexactes sur les équipements, mais la découverte des équipements devrait tout de même fonctionner normalement.

Voici quelques considérations importantes concernant Remote L3 Discovery :

- Avec NetFlow, les périphériques qui représentent les passerelles qui exportent des enregistrements sont automatiquement découverts. Vous pouvez configurer le système ExtraHop pour détecter les périphériques qui représentent les adresses IP observées dans les enregistrements NetFlow en ajoutant une plage d'adresses IP.
- Soyez prudent lorsque vous spécifiez la notation CIDR. Un préfixe de sous-réseau /24 peut entraîner la découverte de 255 nouveaux périphériques par le système ExtraHop. Un préfixe de sous-réseau /16 étendu peut entraîner la découverte de 65 535 nouveaux périphériques, ce qui peut dépasser la limite de votre équipement.
- Si une adresse IP est supprimée des paramètres Device Discovery, elle sera conservée dans le système ExtraHop en tant qu'équipement L3 distant tant qu'il existe des flux actifs pour cette adresse IP ou jusqu'à ce que la capture soit redémarrée. Après un redémarrage, l'équipement est répertorié comme un équipement distant L3 inactif.

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 **NetFlow**.
3. Dans le Découverte d'appareils NetFlow section, saisissez l' adresse IP dans Plages d'adresses IP champ.

   Vous pouvez spécifier une adresse IP ou une notation CIDR, telle que `192.168.0.0/24` pour un réseau IPv4 ou `2001:db8::/32` pour un réseau IPv6.

   Important: Chaque adresse IP distante communiquant activement qui correspond au bloc CIDR sera découverte en tant qu'équipement unique dans le système ExtraHop. La spécification de préfixes de sous-réseau étendus tels que /16 peut entraîner

la découverte de milliers de périphériques, ce qui peut dépasser la limite de votre équipement.

4. Cliquez sur l'icône verte plus (**+**) pour ajouter l' adresse IP.

Prochaines étapes

Vous pouvez ajouter une autre adresse IP ou une autre plage d'adresses IP en répétant les étapes 3 à 4.

Actions après le déploiement

Publié: 2025-03-28

- Passez en revue le Liste de contrôle après le déploiement des capteurs et des consoles et configurez des paramètres supplémentaires.
- Connexion à une sonde depuis une console RevealX Enterprise
- Connecter un stockage des paquets à RevealX Enterprise