

Configuration d'une PCAP globale

Publié: 2024-07-18

Une PCAP globale collecte chaque paquet envoyé au système ExtraHop pendant la durée correspondant aux critères.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Captures de paquets section, cliquez sur **Capture globale de paquets**.
Lors de la configuration des captures de paquets, il vous suffit de spécifier les critères que vous souhaitez pour la capture de paquets.
3. Dans le Nom dans le champ, saisissez un nom pour identifier la capture de paquets.
4. Dans le Nombre maximum de paquets dans le champ, saisissez le nombre maximum de paquets à capturer.
5. Dans le Nombre maximum d'octets dans ce champ, saisissez le nombre maximum d'octets à capturer.
6. Dans le Durée maximale (millisecondes) champ, saisissez la durée maximale de la PCAP en millisecondes.

ExtraHop recommande la valeur par défaut de 1000 (1 seconde). La valeur maximale est de 60 000 millisecondes (1 minute).

7. Dans le Snäplen champ, saisissez le nombre maximum d'octets copiés par image.
La valeur par défaut est de 96 octets, mais vous pouvez définir cette valeur sur un nombre compris entre 1 et 65535.
8. Cliquez **Démarrer**.



Conseil Notez l'heure à laquelle vous commencez la capture pour faciliter la localisation des paquets.

9. Cliquez **Arrête** pour arrêter la capture de paquets avant que l'une des limites maximales ne soit atteinte.

Téléchargez votre capture de paquets.

- Sur les systèmes RevealX Enterprise, cliquez sur **Paquets** dans le menu supérieur, puis cliquez sur **Télécharger PCAP**.

Pour vous aider à localiser votre capture de paquets, cliquez et faites glisser le pointeur sur la chronologie de la requête par paquets pour sélectionner la plage de temps au cours de laquelle vous avez commencé la capture de paquets.

- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres du système , cliquez **Toute l'administration**, puis cliquez sur **Afficher et télécharger les captures de paquets** dans la section Capture de paquets.