

Configuration d'une capture globale de paquets

Publié: 2023-09-19

Une capture globale de paquets recueille tous les paquets envoyés 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 la section Captures de paquets, cliquez sur **Capture de paquets globale**.
3. Dans la section Démarrer la capture globale de paquets, remplissez les champs suivants. Vous devez uniquement spécifier les critères que vous souhaitez pour la capture de paquets :
 - **Nom**: Un nom pour identifier la capture de paquets.
 - **Max Packets**: Le nombre maximum de paquets à capturer.
 - **Max Bytes**: Le nombre maximum d'octets à capturer.
 - **Durée maximale (millisecondes)**: La durée maximale de la capture de paquets en millisecondes. Nous recommandons la valeur par défaut de 1000 (1 seconde), ou de configurer jusqu'à 60000 millisecondes (1 minute).
 - **Snaplen**: Le nombre maximum d'octets copiés par trame. La valeur par défaut est de 96 octets, mais vous pouvez régler cette valeur sur un nombre compris entre 1 et 65535.
4. Cliquez sur **Start (Démarrer)**.
 -  **Conseil** Notez l'heure à laquelle vous démarrez la capture pour faciliter la localisation des paquets.
5. Cliquez sur **Arrêter** pour arrêter la capture de paquets avant que l'une des limites maximales ne soit atteinte.

Téléchargez votre capture de paquets.

- Sur les systèmes Reveal(x) Enterprise, cliquez sur **Paquets** dans le menu supérieur, puis sur **Télécharger PCAP**.
 - Pour vous aider à localiser votre capture de paquets, cliquez et faites glisser sur la chronologie de la requête de paquets pour sélectionner l'intervalle de temps où vous avez commencé la capture de paquets.
- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres système , cliquez sur **Toute l'administration**, puis cliquez sur **Afficher et télécharger des captures de paquets** dans la section Capture de paquets.