Analyse d'un fichier de capture de paquets

Publié: 2023-09-19

Le mode de capture hors ligne permet aux administrateurs de télécharger et d'analyser un fichier de capture enregistré par un logiciel d'analyse de paquets, tel que Wireshark ou tcpdump, dans le système ExtraHop.

Voici quelques considérations importantes à prendre en compte avant d'activer le mode de capture hors ligne :

- Lorsque la capture est définie en mode hors ligne, le magasin de données du système est réinitialisé. Toutes les mesures précédemment enregistrées sont supprimées du magasin de données. Lorsque le système est mis en mode en ligne, le magasin de données est à nouveau réinitialisé.
- En mode hors ligne, aucune mesure n'est collectée à partir de l'interface de capture jusqu'à ce que le système repasse en mode en ligne.
- Seuls les fichiers de capture au format pcap sont pris en charge. Les autres formats, tels que pcpapng, ne sont pas pris en charge.

Définir le mode de capture hors ligne

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Configuration du système, cliquez sur **Capture**.
3. Cliquez sur **Fichier de capture hors ligne**.
4. Sélectionnez **Télécharger**, puis cliquez sur **Enregistrer**.
5. Cliquez sur **OK** pour confirmer la réinitialisation du datastore.
   Le processus de capture est arrêté, l'état de la capture est défini sur hors ligne et le magasin de données est vidé de toutes ses données. Lorsque le système a défini la capture en mode hors ligne, la page Fichier de capture hors ligne s'affiche.
6. Cliquez sur **Choisir un fichier**, naviguez jusqu'au fichier de capture que vous souhaitez télécharger, sélectionnez le fichier, puis cliquez sur **Ouvrir**.
7. Cliquez sur **Télécharger**.
   Le système ExtraHop affiche la page Offline Capture Results (Résultats de la capture hors ligne) lorsque le fichier de capture est téléchargé avec succès.
8. Cliquez sur **Afficher les résultats** pour analyser le fichier de capture de paquets comme vous le feriez lorsque le système est en mode de capture en direct.

Remettre le système en mode de capture en direct

1. Dans la section Configuration du système, cliquez sur **Capture (hors ligne)**.
2. Cliquez sur **Redémarrer la capture**.
3. Sélectionnez **En direct**, puis cliquez sur **Enregistrer**.

Le système supprime les mesures de performance collectées dans le fichier de capture précédent et prépare le magasin de données pour une analyse en temps réel à partir de l'interface de capture.