Analysieren Sie eine Paketerfassungsdatei

Veröffentlicht: 2023-09-13

Der Offline-Erfassungsmodus ermöglicht es Administratoren, eine mit einer Paketanalyse-Software wie Wireshark oder tcpdump aufgezeichnete Capture-Datei in das ExtraHop-System hochzuladen und zu analysieren.

Hier sind einige wichtige Überlegungen, bevor Sie den Offline-Aufnahmemodus aktivieren:

- Wenn die Erfassung in den Offline-Modus versetzt wird, wird der Systemdatenspeicher zurückgesetzt. Alle zuvor aufgezeichneten Metriken werden aus dem Datenspeicher gelöscht. Wenn das System in den Online-Modus versetzt wird, wird der Datenspeicher erneut zurückgesetzt.
- Im Offline-Modus werden keine Metriken von der Erfassungsoberfläche erfasst, bis das System wieder in den Online-Modus versetzt wird.
- Es werden nur Erfassungsdateien im PCAP-Format unterstützt. Andere Formate wie pcapng werden nicht unterstützt.

Stellen Sie den Offline-Aufnahmemodus ein

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Offline-Capture-Datei**.
4. Wählen **Upload** und dann klicken **Speichern**.
5. klicken **OK** um das Zurücksetzen des Datenspeichers zu bestätigen.
   Der Erfassungsvorgang wird gestoppt, der Erfassungsstatus wird auf Offline gesetzt und der Datenspeicher wird von allen Daten gelöscht. Wenn das System die Erfassung in den Offline-Modus versetzt hat, Offline-Capture-Datei Seite erscheint.
6. klicken **Wählen Sie Datei**, navigieren Sie zu der Capture-Datei, die Sie hochladen möchten, wählen Sie die Datei aus, und klicken Sie dann auf **Öffnen**.
7. klicken **Upload**.
   Das ExtraHop-System zeigt die Seite mit den Offline-Capture-Ergebnissen an , wenn die Capture-Datei erfolgreich hochgeladen wurde.
8. klicken **Ergebnisse ansehen** um die Paketerfassungsdatei so zu analysieren, als ob sich das System im Live-Capture-Modus befindet.

Bringen Sie das System in den Live-Aufnahmemodus zurück

1. In der Konfiguration des Systems Abschnitt, klicken **Aufnehmen (offline)**.
2. klicken **Capture neu starten**.
3. Wählen **Lebe**, und klicken Sie dann auf **Speichern**.

Das System entfernt die Leistungskennzahlen, die aus der vorherigen Erfassungsdatei gesammelt wurden, und bereitet den Datenspeicher für die Echtzeitanalyse über die Erfassungsoberfläche vor.