Aufzeichnungen von ExtraHop an Splunk senden

Veröffentlicht: 2023-09-13

Sie können das ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Splunk-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen.

Bevor Sie beginnen

- Sie benötigen Version 7.0.3 oder höher von Splunk Enterprise und ein Benutzerkonto mit Administratorrechte.
- Sie müssen den Splunk HTTP Event Collector konfigurieren, bevor Ihr Splunk-Server ExtraHop-Datensätze empfangen kann . Sehen Sie die Splunk HTTP-Event-Collector Dokumentation für Anweisungen.

Hinweis: Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem Recordstore werden automatisch zum Splunk-Server umgeleitet. Es ist keine weitere Konfiguration erforderlich.

Aufzeichnungen von ExtraHop an Splunk senden

Führen Sie dieses Verfahren auf allen verbundenen ExtraHop-Systemen durch.

Wichtig: Wenn Ihr ExtraHop-System eine Konsole oder Reveal (x) 360 umfasst, konfigurieren Sie alle Sensoren mit denselben Recordstore-Einstellungen oder derselben Übertragungsverwaltung, um Einstellungen von der Konsole oder Reveal (x) 360 aus zu verwalten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Bereich Datensätze auf **Plattenladen**.
3. Wählen **Splunk als Recordstore aktivieren**.

   Hinweis: Wenn Sie von einem verbundenen ExtraHop-Recordstore zu Splunk migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
4. Füllen Sie im Abschnitt Record Ingest Target die folgenden Felder aus:

   • **Splunk-Ingest-Host:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.

   • **Port für den HTTP-Event-Collector:** Der Port, über den der HTTP Event Collector Datensätze sendet.

   • **HTTP-Event-Collector-Token:** Das Authentifizierungstoken, das Sie erstellt in Splunk für den HTTP Event Collector.
5. Füllen Sie im Abschnitt Record Query Target die folgenden Felder aus:

   • **Splunk-Abfragehost:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.

   • **REST-API-Port:** Der Port, über den Datensatzabfragen gesendet werden sollen.

   • **Methode der Authentifizierung:** Die Authentifizierungsmethode, die von Ihrer Version von Splunk abhängt.

   Für Splunk-Versionen nach 7.3.0 wählen Sie **Authentifizieren Sie sich mit Token**, und fügen Sie dann Ihr Splunk-Authentifizierungstoken ein. Anweisungen zum Erstellen eines Authentifizierungstokens finden Sie in der Splunk-Dokumentation.

Für Splunk-Versionen vor 7.3.0 wählen Sie **Authentifizieren Sie sich mit Benutzername und Passwort**, und geben Sie dann Ihre Splunk-Anmeldeinformationen Anmeldedaten .

6. Lösche das **Überprüfung des Zertifikats erforderlich** Kontrollkästchen, wenn für Ihre Verbindung kein gültiges SSL/TLS-Zertifikat erforderlich ist.

   Hinweis: Sichere Verbindungen zum Splunk-Server können verifiziert werden über vertrauenswürdige Zertifikate die Sie in das ExtraHop-System hochladen.

7. Geben Sie im Feld Indexname den Namen des Splunk-Indexes ein, in dem Sie Datensätze speichern möchten.

   Der Standardindex auf Splunk heißt `main`, wir empfehlen jedoch, dass Sie einen separaten Index für Ihre ExtraHop-Datensätze erstellen und den Namen dieses Indexes eingeben. Anweisungen zum Erstellen eines Indexes finden Sie in der Splunk-Dokumentation.

8. (zusätzlicher Sprung) Sensor nur) Klick **Verbindung testen** um zu überprüfen , ob das ExtraHop-System Ihren Splunk-Server erreichen kann.
9. klicken **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie nach gespeicherten Datensätzen im ExtraHop-System suchen, indem Sie auf **Rekorde** aus dem oberen Menü.

Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole verbunden mit Ihren ExtraHop-Sensoren können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen auf den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen über mehrere Sensoren hinweg auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Plattenläden von Drittanbietern konfiguriert und gelten nicht für den ExtraHop Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen auf der Sensor durch `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Bereich Datensätze auf **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Command-Appliance aus und klicken Sie dann auf **Übertragung**.

   Wenn Sie sich später entscheiden, die Einstellungen auf dem zu verwalten Sensor, wählen **dieses Discover-Gerät** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Übertragung**.