Aufzeichnungen von ExtraHop an CrowdStrike Falcon LogScale senden

Veröffentlicht: 2024-01-31

Sie können Ihr ExtraHop Reveal (x) Enterprise-System so konfigurieren, dass Datensätze auf Transaktionsebene zur langfristigen Speicherung an ein CrowdStrike Falcon LogScale-Repository gesendet werden und diese Datensätze dann vom ExtraHop-System und der ExtraHop REST-API abgefragt werden.

Hier sind einige wichtige Überlegungen zur Aktivierung eines LogScale-Repositorys als Recordstore:

- Die Menge an Recordstore-Lookback, die abgefragt werden kann, wird bestimmt durch Einstellungen für die Datenspeicherung konfiguriert für Ihr LogScale-System.
- Sie können für jeden ExtraHop-Sensor ein separates LogScale-Repository aktivieren.
- Von einer ExtraHop-Konsole aus können Sie Datensätze aus LogScale-Repositorys auf allen verbundenen ExtraHop-Sensoren abfragen, sofern diese Repositorys derselben LogScale-Ansicht zugeordnet sind.
- Wenn alle ExtraHop-Sensoren Datensätze an dasselbe Repository senden, können Sie Recordstore-Einstellungen übertragen und verwalten Sie alle Sensoren von der ExtraHop-Konsole aus.
- Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem Recordstore werden automatisch zum LogScale-Repository umgeleitet. Es ist keine weitere Konfiguration erforderlich.

Aktiviere LogScale als Recordstore

Bevor Sie beginnen

- Ihr ExtraHop-System muss für den LogScale Recordstore lizenziert sein.
- Auf Ihrem ExtraHop-System muss die Reveal (x) Enterprise-Firmware-Version 9.5 oder höher ausgeführt werden.
- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Ihr ExtraHop-Benutzerkonto muss System- und Zugriffsadministrationsrechte.
- Ihr LogScale-System muss Version 1.111.0 oder höher haben.
- Ihr LogScale-Benutzerkonto muss über Administratorrechte verfügen.
- Sie müssen über ein LogScale-Ingest-Token verfügen, das einem Repository oder einem Organisationstoken zugeordnet ist, das die Berechtigung zum Ingest in allen Repositorys innerhalb der Organisation beinhaltet.
- Sie benötigen ein LogScale-View-Token, das die Zugriffsberechtigung zum Lesen von Daten beinhaltet.

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

   Wichtig: Wenn Sie von einem verbundenen ExtraHop-Recordstore zu LogScale migrieren, können Sie nicht mehr auf Datensätze zugreifen, die in diesem ExtraHop-Recordstore gespeichert sind.
4. In der Verschlucken Geben Sie in diesem Abschnitt die folgenden Informationen über das LogScale-Repository an, das Datensätze aus dem ExtraHop-System aufnehmen und speichern wird:
   - **Hostnamen aufnehmen:** Der Hostname des LogScale-Repositorys.
   - **Port aufnehmen:** Der Port, über den Datensätze an das Repository gesendet werden.
   - **Repository-Ingest-Token:** Das Authentifizierungstoken für die Aufnahme von Daten in LogScale.

© 2024ExtraHop Networks, Inc. Alle Rechte vorbehalten.

5. In der Abfrage Geben Sie in diesem Abschnitt die folgenden Details zum LogScale API-Server an, der Datensatzabfragen vom ExtraHop-System verarbeitet.
   - **API-Hostname:** Der Hostname des API-Servers.
   - **API-Anschluss:** Der Port, über den Datensatzabfragen an die API gesendet werden.
   - **Namen ansehen:** Der Name der LogScale-Ansicht, die mit dem Repository verbunden ist.
   - **Token anzeigen:** Das Authentifizierungstoken für Abfragen an das LogScale-Repository.
6. Optional: Wählen **Komprimiere ausgehende Datensatz-Payloads mit GZip** um die Größe aufgenommener Dateien zu reduzieren.
7. Klicken Sie **Verbindung testen** um zu überprüfen, ob Ihr Sensor mit dem LogScale-Repository kommunizieren kann.
8. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie Abfrage nach gespeicherten Datensätzen im ExtraHop-System durch Anklicken **Rekorde** aus dem oberen Navigationsmenü oder aus dem ExtraHop REST-API.

Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores 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 Abschnitt Datensätze auf **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

   Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.