**Salesforce Data Collection via Elastic Integration**

This guide explains how to collect key operational events from Salesforce—including Login, Logout, and Apex activities—using Elastic’s integration. It covers the different methods available, required Salesforce permissions and licensing, and the steps to configure your Salesforce org for data collection.

**1. Overview of Data Streams**

The Elastic Salesforce integration enables you to collect several event types from your Salesforce instance. The main data streams include:

* **Login:**  
  Captures details about user logins (timestamps, IP addresses, user IDs, etc.) to monitor authentication activity.
* **Logout:**  
  Collects records of when users sign out, helping you track session durations and detect abnormal logout patterns.
* **Apex:**  
  Logs various events related to Apex code—such as callouts, execution times, database operations, and trigger invocations—for performance monitoring and debugging.
* **SetupAuditTrail (Optional):**  
  Tracks changes in the Salesforce Setup area over the last 180 days. (This stream may also be used for compliance monitoring.)

**Supporting Resources:**

* [Elastic Salesforce Integration Guide](https://www.elastic.co/guide/en/integrations/current/salesforce.html)
* [Salesforce Developer Documentation – EventLogFile Object](https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_eventlogfile.htm)

**2. Methods to Pull Salesforce Event Data**

There are multiple approaches to retrieve event data from Salesforce. The two primary methods include:

**A. Event Log Files (ELFs)**

**Description:**  
Salesforce automatically generates Event Log Files (ELFs) that capture a range of events—including logins, logouts, and Apex events. These files are accessible via the Salesforce REST API.

**How to Retrieve ELFs:**

1. **Query the EventLogFile Object:**  
   Use SOQL to select the desired fields from the EventLogFile object. For example:
2. SELECT Id, EventType, LogDate, LogFile
3. FROM EventLogFile
4. WHERE EventType IN ('Login', 'Logout', 'Apex')
5. **Download the Log File:**  
   Once you have the file ID, you can download the file (typically in CSV or JSON format) and parse it for detailed event data.

**Permissions & Licensing Considerations:**

* **API Enabled:**  
  The user account used for data collection must have the **API Enabled** permission.
* **Default Access:**
  + In Developer Edition orgs, all ELF types are available for free with a 1-day retention.
  + In Enterprise, Unlimited, and Performance editions, a limited subset (login, logout, API usage) is available without extra cost.
* **Extended Event Types & Retention:**  
  For access to a broader range of event types (like detailed Apex events) and longer retention (up to 365 days), you must subscribe to Salesforce Shield Event Monitoring.

**Supporting Resources:**

* [Salesforce Developer Documentation – EventLogFile Object](https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_eventlogfile.htm)
* [Trailhead: Get Started with Event Monitoring](https://trailhead.salesforce.com/content/learn/modules/event_monitoring/event_monitoring_intro)

**B. Real-Time Streaming (Platform Events)**

**Description:**  
Real-time streaming allows you to receive event data as it occurs rather than pulling historical batches. This is achieved via Salesforce’s Streaming API (using the CometD protocol) or Real-Time Event Monitoring.

**How to Retrieve Real-Time Data:**

1. **Streaming API (CometD):**
   * **Subscribe to Event Channels:**  
     Use a CometD client to subscribe to platform event channels such as:
     + /event/LoginPlatformEvent
     + /event/LogoutPlatformEvent
   * **Receive Events:**  
     As events are published, your client receives them in near real time, enabling immediate processing or alerting.

*Example (pseudocode):*

var client = new org.cometd.CometD();

client.configure({

url: 'https://yourInstance.salesforce.com/cometd/54.0',

requestHeaders: { Authorization: 'Bearer YOUR\_ACCESS\_TOKEN' }

});

client.handshake(function(handshakeReply) {

if (handshakeReply.successful) {

client.subscribe('/event/LoginPlatformEvent', function(message) {

console.log('Received login event:', message);

});

}

});

1. **Real-Time Event Monitoring API:**
   * Provides more immediate access to events, typically used when integrated with monitoring systems for alerting and analysis.

**Permissions & Licensing Considerations:**

* **Required Permissions:**  
  The integration user needs the **View Real-Time Event Monitoring Data** permission.
* **Additional Licensing:**  
  Real-time event streaming features usually require Salesforce Shield Event Monitoring (or a similar add-on), which adds cost compared to standard API access.

**Supporting Resources:**

* [Trailhead: Get Started with Event Monitoring](https://trailhead.salesforce.com/content/learn/modules/event_monitoring/event_monitoring_intro)
* [Salesforce Shield Overview on Trailhead](https://trailhead.salesforce.com/content/learn/modules/shield_security)

**3. Salesforce Configuration & Setup**

**Step 1: Prepare Your Salesforce Environment**

* **User Permissions:**
  + Verify that the integration user has **API Enabled**.
  + For real-time streaming, also verify the **View Real-Time Event Monitoring Data** permission.
* **Connected App Creation:**
  + In Salesforce, navigate to **Setup > App Manager**.
  + Create a new connected app:
    - Enable OAuth Settings.
    - Set the Callback URL (typically your instance URL).
    - Select OAuth scopes such as “Manage user data via APIs” and “Perform requests at any time.”
    - Save and wait for changes to propagate.
  + Copy the **Consumer Key** and **Consumer Secret** for later use.

**Step 2: Data Extraction**

* **Using ELFs (Historical Data):**
  + Query the EventLogFile object via the REST API.
  + Example REST call (using curl):
  + curl https://yourInstance.salesforce.com/services/data/v54.0/query/?q="SELECT+Id,EventType,LogDate+FROM+EventLogFile+WHERE+EventType+IN+('Login','Logout','Apex')" \
  + -H "Authorization: Bearer YOUR\_ACCESS\_TOKEN"
* **Using Real-Time Streaming:**
  + Implement a CometD client in your preferred language.
  + Subscribe to the appropriate event channels and process events as they are published.

**Step 3: Data Processing & Integration**

* **Transformation & Storage:**
  + Parse the downloaded ELF files (CSV/JSON) or process the streaming data.
  + Map fields such as user ID, timestamp, IP address, and Apex metrics.
  + Ingest the data into your monitoring or analytics platform (e.g., Elasticsearch, Splunk).
* **Visualization:**
  + Build dashboards (using Kibana or another tool) to monitor login patterns, track session durations, and analyze Apex performance.

**Proof Link:**

* [Elastic Salesforce Integration Guide](https://www.elastic.co/guide/en/integrations/current/salesforce.html)

**4. Licensing Summary & Considerations**

* **Standard Salesforce Editions:**
  + Developer Edition: Full ELF access (all event types) free with 1-day retention.
  + Enterprise/Unlimited/Performance: Basic ELFs (login, logout, API usage) free with 1-day retention.
* **Salesforce Shield (Event Monitoring Add-On):**
  + Required to access extended event types (e.g., detailed Apex events) and to extend retention (up to 365 days).
  + Shield is an additional purchase (pricing is typically based on a percentage of your overall Salesforce contract).

**Supporting Resources:**

* [Trailhead: Get Started with Event Monitoring](https://trailhead.salesforce.com/content/learn/modules/event_monitoring/event_monitoring_intro)
* [Opt in for Event Log File Generation (Release Update)](https://help.salesforce.com/s/articleView?id=release-notes.rn_security_em_generate_event_log_files.htm&language=en_US&release=244&type=5)

**5. Summary of Implementation**

1. **Identify Data Needs:**
   * Decide which events (login, logout, Apex) you require.
2. **Set Up Salesforce:**
   * Ensure the integration user has the necessary permissions.
   * Create a Connected App for OAuth.
3. **Choose an Extraction Method:**
   * For historical analysis, use ELFs via the REST API.
   * For real-time monitoring, implement the Streaming API (CometD) subscription.
4. **Plan for Licensing:**
   * Determine if standard ELF access meets your needs.
   * If extended access or retention is required, plan to purchase Salesforce Shield Event Monitoring.
5. **Integrate with Your Analytics Platform:**
   * Parse, transform, and load the data into systems like Elasticsearch for dashboarding and alerting.

**6. Supporting Resources**

1. **Elastic Salesforce Integration Guide:**  
   <https://www.elastic.co/guide/en/integrations/current/salesforce.html>
2. **Salesforce Developer Documentation – EventLogFile Object:**  
   <https://developer.salesforce.com/docs/atlas.en-us.object_reference.meta/object_reference/sforce_api_objects_eventlogfile.htm>
3. **Trailhead: Get Started with Event Monitoring:**  
   <https://trailhead.salesforce.com/content/learn/modules/event_monitoring/event_monitoring_intro>
4. **Salesforce Shield Overview:**  
   <https://trailhead.salesforce.com/content/learn/modules/shield_security>
5. **Salesforce Help – Create a Connected App:**  
   <https://help.salesforce.com/s/articleView?id=sf.connected_app_create.htm&type=5>
6. **Opt in for Event Log File Generation (Release Update):**  
   <https://help.salesforce.com/s/articleView?id=release-notes.rn_security_em_generate_event_log_files.htm&language=en_US&release=244&type=5>