**How to Add Alerts in Splunk**

**Step 1: Run a Search Query**

1. Log in to your **Splunk Web Interface**.
2. Click on **Search & Reporting**.
3. In the search bar, enter a query to retrieve the data you want to monitor. Example:
4. source="138066\_1\_MOUNT BLUE1.xls" host="ip-172-31-28-3" sourcetype="mount"

| table \*

1. Click **Search** to ensure the query retrieves the expected results.

**Step 2: Save Search as an Alert**

1. Click on **Save As** (located at the top right of the search results).
2. Select **Alert**.
3. In the **Save As Alert** window, configure the following settings:
   * **Title:** Provide a meaningful name (e.g., "New Registration Alert").
   * **Description:** (Optional) Add a short description of the alert.
   * **Permissions:** Choose **Private** (only for you) or **Shared in App** (for others).
   * **Alert Type:** Choose **Scheduled** to run at a set interval or **Real-time** for immediate triggers.

**Step 3: Set Alert Conditions**

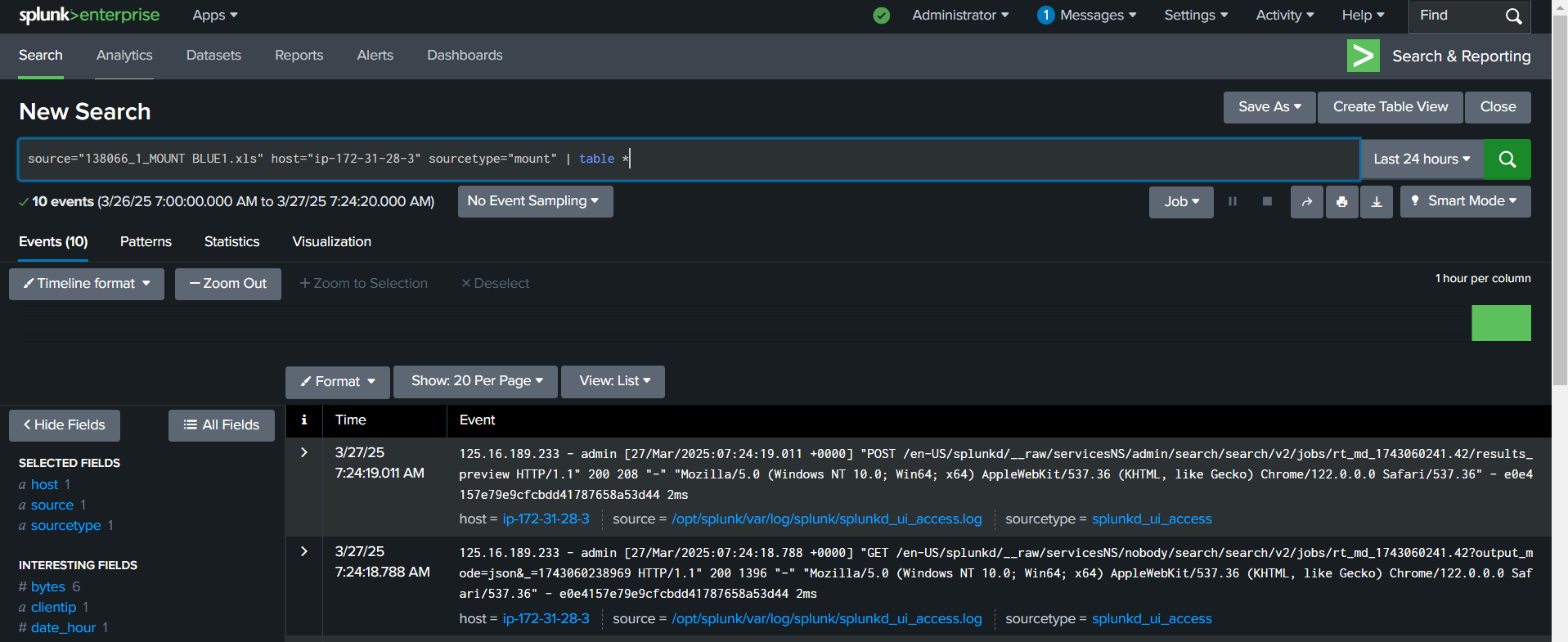
1. **Set the Time Range:** Select a relevant time range (e.g., **Last 24 hours**).
2. **Define a Schedule:**
   * Click on **Run on Cron Schedule**.
   * Enter a cron expression for scheduling (e.g., to run at 12:34 PM every day):
   * 34 12 \* \* \*
3. **Trigger Conditions:**
   * Select **Trigger alert when** → Number of Results > 0 (or another condition).

**Step 4: Add Actions (Log Event)**

1. Under **Trigger Actions**, click **Add Actions**.
2. Select **Log Event**.
3. In the **Event Text** box, enter a message (e.g., "New Registration Data Found").
4. Click **Save**.

**Step 5: Verify the Alert**

1. Go to **Settings → Searches, Reports, and Alerts**.
2. Find your alert and check its status.
3. To check logged events, run the following query in Search:
4. index=\_internal source="scheduler.log"
5. You should see an entry confirming that the alert was triggered.

  
  
  
A screenshot of a computer

AI-generated content may be incorrect.  
🡪>> Fill out these details and save them.  
🡪check in the alerts.