**Lab Exercise 2 - Creating an Index and Loading Data in Splunk**

**Objective**

This lab guides you through the process of creating a custom index in Splunk and uploading data into it for searching and analysis.

**Objectives**

1. Create a new index in Splunk.
2. Load data into the custom index.
3. Search and analyze the data in the created index.

**Pre-requisites**

* Access to a Splunk instance (Splunk Enterprise or Splunk Cloud).
* Administrator privileges on the Splunk instance.
* A sample dataset (e.g., web server logs or any CSV/JSON file).

**Steps**

**Step 1: Log in to Splunk**

1. Open the Splunk Web interface in your browser.
2. Log in with your Splunk credentials (admin privileges required).

**Step 2: Create a New Index**

1. Navigate to **Settings** > **Indexes**.
2. Click on **New Index**.
3. Provide the following details:
   * **Index Name**: custom\_index (or any name you prefer).
   * **Index Data Type**: Choose the default data type unless you need a specific type (e.g., metrics).
   * **Max Data Size**: Optional, specify limits for data storage.
4. Click **Save** to create the index.

**Step 3: Verify the Index**

1. In the **Indexes** list, confirm that your new index (custom\_index) is listed.
2. Note the Index Path for reference if needed.

**Step 4: Load Data into the Index**

1. Go to the **Settings** > **Add Data** menu.
2. Choose **Upload** for local file upload:
   * Click **Upload Files**.
   * Select the sample data file (e.g., sample\_logs.csv or web\_server.log).
   * Click **Next**.
3. Assign the data to your new index:
   * In the **Set Source Type** step, choose an appropriate source type (e.g., csv, access\_combined).
   * In the **Set Destination** step, select **custom\_index** as the index.
   * Click **Review** and then **Submit** to upload the data.

**Step 5: Verify Data Loading**

1. Navigate to the **Search & Reporting** app.
2. Run the following search query to verify data in your index:

index=custom\_index

1. Confirm that events from the uploaded file are displayed.

**Step 6: Perform Basic Analysis**

1. Filter events based on a keyword:

index=custom\_index error

1. Display specific fields using table:

index=custom\_index | table \_time host source

1. Generate a time-based chart:

index=custom\_index | timechart count by source

This lab exercise provides hands-on experience with index management and data ingestion in Splunk.