Step 1: Log into Splunk

Log into your Splunk instance using a web browser.

Step 2: Search for Relevant Data

Use the Splunk search interface to find the data you want to analyze. You can do this by using the search command followed by your search query. For example:

```
source="/var/log/application.log" status=200.
```

This search will retrieve log entries from the specified source where the status is 200.

Step 3: Use the transaction Command

To group related events into transactions, use the transaction command in your search query. The transaction command requires you to specify a set of field-value pairs that define the transaction boundaries. For example:

```
source="/var/log/application.log" status=200 | transaction client_ip startswith="status=200" endswith="status=404"
```

Step 4: Display the Transaction Results

By default, Splunk will display the transaction results as a table. You can use the table command to format the output. For example:

```
source="/var/log/application.log" status=200 | transaction client_ip startswith="status=200" endswith="status=404" | table client_ip, duration, events
```

This will display a table with columns for client_ip, duration (time span of the transaction), and events (number of events in the transaction).

Step 5: Refine and Customize

You can further refine and customize your transaction analysis by adding additional commands to your search query. For example, you can use stats to calculate statistics on transaction durations or use eval to create calculated fields based on transaction data.

Here's an example of calculating the average duration of transactions:

```
source="/var/log/application.log" status=200 | transaction client_ip startswith="status=200" endswith="status=404" | stats avg(duration) as avg_duration
```

Step 6: Visualize the Results

If you want to create visualizations based on your transaction data, you can use Splunk's visualization tools. Click on the "Visualization" tab in Splunk and select the appropriate chart type (e.g., line chart, bar chart) to visualize your transaction data.