Day - 6

23 December 2024 10:08

1. Field Summary.
2. Text function.
3. Conversion function.
4. Informational function.
5. Statistical function.
6. Multiku.
7. bin command.
8. xyseries.
9. untable.
10. foreach.
11. Date & time fun. (Strftime, strptime)
12. mvexpand.
13. Coalense.
14. Studio (Input filter)
15. MLTK Toolkit.

1 Studio Dashboard:-

1. Base Search
2. chain Search
3. Saved Search.
4. Geo Map
5. filter.
6. Visualization.

2. Text function:-

1. len → length of the string.
2. lower → string to the lower case.
3. upper → string to the upper case.
4. Ltrim → Trim the Certain value from the string from the left.
5. replace → Replace a certain value with other value.

Trim from the right side. the string.

6. rtrim → Trim from the right :-
7. trim → Trim a certain value from the string.

replace → <str>, <regex>, <replacement>

2. Information function:-

1. isbool - True/false
2. isdouble - Double Data Type
3. isint - Value is integer
4. isnull - The Value is their/Not
5. isnum - Value is Number.
6. isstr - Value is string/Not.
7. typeof(<value>) - Define the format of the string.

4. statistical Commands:-

1. stats
2. streamstats.
3. eventstats Command.

(5) Date & Time functions:-

(1) strptime → convert date & time value into epoch format

(2) strftime → Convert the epoc data into human readable format.

09-09-09 09:09

US → %m-%d-%y

EMEA → %y-%m-%d

APAC → %d-%m-%y

D_1 , D_2

$(D_2 - D_1)$ ✗

$(D_2$_time-epoc − D_1_time-epoc$)$ ✓

```
index=main source="Sample_tickets.csv"
| table time_submitted , last_resolved_date
| eval last_resolved_epoc = strptime(last_resolved_date, "%d-%m-%y %H:%M")
| eval time_submitted_epoc = strptime(time_submitted, "%d-%m-%y %H:%M")
| eval diff = last_resolved_epoc-time_submitted_epoc
| eval time_submitted_format = strftime(time_submitted_epoc, "%d-%B-%Y %A")
| eval diff_format = strftime(diff, "%d")
```

(6) xyseries:-

```
index=main source="Sample_tickets.csv"
| stats count by severity, current_ticket_state
| xyseries severity, current_ticket_state, count
| fillnull
```

(7) Untable Commands

```
index=main source="Sample_tickets.csv"
| stats count by severity, current_ticket_state
| xyseries severity, current_ticket_state, count
|untable severity, current_ticket_state, count
```

@Bin •

8 Bin Command:-

```
index=main source="Sample_tickets.csv"
| bin span=1mon _time
| stats count by _time, severity
```

9 mvexpand:-

```
| makeresults count=5
| streamstats count as counter
| eval field1 = "col1", field2="col2"
| mvcombine delim=";" counter
| mvexpand counter
```

10 FieldSummary:-

It will summarize the each & every field in the filtered dataset.

```
index=main source="data.csv"
| fieldsummary
```

11. Coalesce Command:-

A	B	C
a	x	
b	y	2
c	-	
d	v	w
e		

eval D = Coalesce(B, C)

A	D
	x

A	D
a	x
b	y
c	z
d	v
e.	w

eval D = Coalesce

(12) Foreach Command :-

Run the subseach that will run in the iteration.

```
| makeresults
| eval myfield1 = 5, myfield2 = 10
| foreach myfield*
    [ eval <<FIELD>> = '<<FIELD>>' + <<MATCHSTR>>]
```

(13) Splunk MLTK Toolkit :-

Machine learning → Dataset → Model
↓
To Train the dataset → Output → Data → predict

(1) Linear Regression.
(2.) Multi Linear Regression.

(1.) Linear Regression :-

Cost of My House ∝ Size of House
(Variable)

Cost of My House ∝

Cost ∝ Size (Variable)

Only one factor is involed in Prediction.

2. Multi linear Reg:-

Cost of Home = Size + Proximity + Age + Build Quality

Multiple factors involved for the Prediction.

Cost of My Car ∝ Age of Car → Single linear Regression

Cost of Car ∝ Age, Kms, Diesel/Petrol/CNG, Auto/Manual eee engine

↓

Multiple linear Regression.

Python] → ML Code/Algo.

R

Predit → LL

→ BJC

→ LLT

→ CLP

Dataset → Training Data (70%) → Model which is trained is Correct/Not.

→ Testdate

Dataset
100 erect

Test date
(30%)

Fustues Prediction.