

## Training – Day #2

15 June 2023 04:30

### Note :

- (1) Index name should be in lowercase. It will allow to create but "Add Data" will not push the data to splunk.
- (2) If Imported data is CSV type, then first column will be considered as Header/Feld Name.
- (3) **\_time** field will be taken **from file** or **at the time when file was imported** or we can define **custom** also.
- (4) Splunk has default settings to identify source type, but we can create our own source type from **Settings => Data => Source types**
- (5) Source-type details are mentioned in **props.conf**
- (6) While importing data, we can set Time for imported data.

The screenshot shows the 'Add Data' process in Splunk. The current step is 'Set Source Type'. A progress bar indicates the steps: Select Source (green), Set Source Type (green), Input Settings (white), Review (white), and Done (white). The main area displays a table of imported data from 'Sample\_tickets.csv'. The columns are \_time, active\_org, app\_family\_mots, and application\_name. There are three rows of data:

	_time	active_org	app_family_mots	application_name
1	6/6/23 5:17:00.000 AM	Org_1	Project 1	MSTR
2	6/6/23 5:17:00.000 AM	Org_1	Project 1	MSTR
3	6/6/23 5:17:00.000 AM	Org_1	Project 1	MSTR

Configuration options for the timestamp field are shown, including 'Extraction' set to 'Auto'. Other tabs like 'Delimited settings' and 'Advanced' are visible.

Download Data from => <https://1drv.ms/f/s!AuaadykgoOfEry6ikeBpOmerib7w?e=uOaI9U>

### Difference between Real-Time & Relative-Time search :

**Real-time search => Search at the time of insertion**, hence CPU utilization will be very high, so mostly we disable. Use real-time maximum for 1min to 2 min for security purpose.

**Relative time search => Search is happening after storage.**

### # Search Modes:

#### 3 types of Search mode:

- (1) **Fast Mode** : Searching speed will be very less as it **skip the extraction of filed**.
- (2) **Smart Mode** : Searching speed will be higher as it will **perform extraction** of filed. But I **cannot see data** for Even tab if used stats function and vice-versa
- (3) **Verbose Mode** : Searching speed will be very high as it will **perform extraction** of filed. But I **can switch** between Event/Pattern/Statistics pages

The screenshot shows the 'Smart Mode' dropdown in the search bar. It lists three modes: Fast Mode, Smart Mode, and Verbose Mode. Under Fast Mode, it says 'Field discovery off for event searches. No event or field data for stats searches.' Under Smart Mode, it says 'Field discovery on for event searches. No event or field data for stats searches.' Under Verbose Mode, it says 'All event & field data.'

### #table command:

| **table** <field1> <field2>

=> it will show data in tabular format for filed1 and filed2.

=> field name **is case-sensitive**.

=> if field name is wrong/case is wrong, **it will not give error. It will show the filed name with blank data.**

ticket_number	severity	current_ticket_state
INC000020685153	3	Closed
INC000020495065	4	Resolved
INC000020492348	3	Resolved
INC000020598590	3	Resolved

### #rename command:

Rename is only for search time, not permanent.

Events and Statistics tab will show renamed fields.

| rename <field1> as name\_1, <field2> as "name 1"

incident_number	severity	ticket state
INC000020685153	3	Closed
INC000020495065	4	Resolved
INC000020492348	3	Resolved
INC000020598590	3	Resolved
INC000020585083	3	Resolved
INC000020806534	3	Resolved

### #stats command:

Stats command will give statistical output. It is having 5 features :

- (1) **count**
- (2) **sum**
- (3) **avg**
- (4) **list** => list the fields
- (5) **values** => provide Unique values

#### (1) count

index="my\_idx" sourcetype="csv" | stats count | rename count as Total

OR

index="my\_idx" sourcetype="csv" | stats count as Total

**by** clause: will show count by grouping the fields.

index="my\_idx" sourcetype="csv" | stats count by current\_ticket\_state

current_ticket_state	count
Closed	29
Customer Hold	4
In Progress	15
On Hold	5
Pending	1
Resolved	45

index="my\_idx" sourcetype="csv" | stats count by current\_ticket\_state, severity

current_ticket_state	severity	count
Closed	2	7
Closed	3	16
Closed	4	6
Customer Hold	3	2
Customer Hold	4	2
In Progress	1	1

### (2, 3) sum() and avg()

for "sum" and "avg", we need numeric filed.

**index=\_internal | stats sum(bytes) as total\_bytes by sourcetype**

The screenshot shows a Splunk search interface with the following command in the search bar:

```
index=_internal | stats sum(bytes) as total_bytes by sourcetype
```

Below the search bar, it says "644,983 events (6/5/23 5:00:00.000 AM to 6/6/23 5:40:24.000 AM) No Event Sampling". The "Statistics (13)" tab is selected. The results table has columns for sourcetype and total\_bytes. The data includes:

sourcetype	total_bytes
mongod	NULL
python_upgrade_readiness_app	NULL
scheduler	NULL
secure_gateway_app_internal_log	NULL
splunk_archiver-too_small	NULL
splunk_assist_internal_log	NULL
splunk_python	NULL
splunk_search_messages	NULL
splunk_web_access	112885134
splunk_web_service	NULL

**fillnull** clause: will fill the null/blank values with "NULL"

**index=\_internal | stats sum(bytes) as total\_bytes by sourcetype | fillnull value=NULL total\_bytes**

The screenshot shows a Splunk search interface with the following command in the search bar:

```
index=_internal | stats sum(bytes) as total_bytes by sourcetype | fillnull value=NULL total_bytes
```

Below the search bar, it says "646,007 events (6/5/23 5:00:00.000 AM to 6/6/23 5:42:08.000 AM) No Event Sampling". The "Statistics (13)" tab is selected. The results table has columns for sourcetype and total\_bytes. The data includes:

sourcetype	total_bytes
mongod	NULL
python_upgrade_readiness_app	NULL
scheduler	NULL
secure_gateway_app_internal_log	NULL
splunk_archiver-too_small	NULL
splunk_assist_internal_log	NULL
splunk_python	NULL
splunk_search_messages	NULL
splunk_web_access	112885134
splunk_web_service	NULL

index=_internal   stats sum(bytes) as total_bytes by sourcetype   fillnull value="Data is empty" total_bytes	
154,744 of 154,744 events matched No Event Sampling ▾	
Events (154,744) Patterns Statistics (13) Visualization Job ▾	
20 Per Page ▾	✓ Format Preview ▾
sourcetype ↴	✓ total_bytes ↴
mongod	Data is empty
python_upgrade_readiness_app	Data is empty
scheduler	Data is empty
secure_gateway_app_internal_log	Data is empty
splunk_archiver-too_small	Data is empty
splunk_assist_internal_log	Data is empty
splunk_python	Data is empty
splunk_search_messages	Data is empty
splunk_web_access	90935605

**index=\_internal | stats avg(bytes) as total\_bytes by sourcetype | fillnull value=NULL total\_bytes**

index=_internal   stats avg(bytes) as total_bytes by sourcetype   fillnull value=NULL total_bytes	
648,015 events (6/5/23 5:00:00.000 AM to 6/6/23 5:44:26.000 AM) No Event Sampling ▾	
Events (648,015) Patterns Statistics (13) Visualization	
20 Per Page ▾	✓ Format Preview ▾
sourcetype ↴	✓ total_bytes ↴
mongod	NULL
python_upgrade_readiness_app	NULL
scheduler	NULL
secure_gateway_app_internal_log	NULL
splunk_archiver-too_small	NULL
splunk_assist_internal_log	NULL
splunk_python	NULL
splunk_search_messages	NULL
splunk_web_access	257141.53530751707

#### (4) list()

It will list all values. Values may be duplicate.

**index=\_internal | stats list(source)**

index=_internal   stats list(source)	
⚠ 'list' command: Limit of '100' for values reached. Additional values may ha	
✓ 655,286 events (6/5/23 5:00:00.000 AM to 6/6/23 5:54:19.000 AM) No	
Events (655,286)	Patterns Statistics (1) Visualization
20 Per Page ▾	✓ Format Preview ▾
list(source) ↴	
/home/ec2-user/splunk/var/log/splunk/splunkd_ui_access.log	

**index=\_internal | stats list(source) by sourcetype**

`index=_internal | stats list(source) by sourcetype`

567,428 of 567,428 events matched No Event Sampling ▾

Events (567,428) Patterns Statistics (13) Visualization

20 Per Page ▾ ✓ Format Preview ▾

sourcetype	list(source)
mongod	/home/ec2-user/splunk/var/log/splunk/mongod.log /home/ec2-user/splunk/var/log/splunk/mongod.log /home/ec2-user/splunk/var/log/splunk/mongod.log /home/ec2-user/splunk/var/log/splunk/mongod.log
python_upgrade_readiness_app	/home/ec2-user/splunk/var/log/splunk/eurareMOTE_SCAN_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log /home/ec2-user/splunk/var/log/splunk/jura_REMOTE_SCAN_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/pura_utils.log

### (5) values()

It will list Unique values.

`index=_internal | stats values(source)`

`index=_internal | stats values(source)`

280,800 of 280,800 events matched No Event Sampling ▾

Events (280,800) Patterns Statistics (1) Visualization

20 Per Page ▾ ✓ Format Preview ▾

values(source)
/home/ec2-user/splunk/var/log/splunk/eurareMOTE_LIST.log /home/ec2-user/splunk/var/log/splunk/eurareMAIL_NOTIFICATION_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/euramongoDB_TLS_DNS_VALIDATION.log /home/ec2-user/splunk/var/log/splunk/eurareAD_PROGRESS.log /home/ec2-user/splunk/var/log/splunk/eurareMOTE_SCAN_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/eurare_SCAN_APPS.log /home/ec2-user/splunk/var/log/splunk/eurare_SCAN_DEPLOYMENT.log /home/ec2-user/splunk/var/log/splunk/eurare_SEARCH_PEER_SSL_CONFIG.log /home/ec2-user/splunk/var/log/splunk/health.log /home/ec2-user/splunk/var/log/splunk/jurareMOTE_SCAN_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/jurare_SCAN_APPS.log /home/ec2-user/splunk/var/log/splunk/license_usage.log /home/ec2-user/splunk/var/log/splunk/metrics.log /home/ec2-user/splunk/var/log/splunk/mongod.log

`index=_internal | stats values(source) by sourcetype`

`index=_internal | stats values(source) by sourcetype`

✓ 658,222 events (6/5/23 5:00:00.000 AM to 6/6/23 5:57:42.000 AM) No Event Sampling ▾

Events (658,222) Patterns Statistics (13) Visualization

20 Per Page ▾ ✓ Format Preview ▾

sourcetype	values(source)
mongod	/home/ec2-user/splunk/var/log/splunk/mongod.log
python_upgrade_readiness_app	/home/ec2-user/splunk/var/log/splunk/eurareMOTE_LIST.log /home/ec2-user/splunk/var/log/splunk/eurareMAIL_NOTIFICATION_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/eurareMAIL_RECEIVERS_LIST.log /home/ec2-user/splunk/var/log/splunk/euramongoDB_TLS_DNS_VALIDATION.log /home/ec2-user/splunk/var/log/splunk/eurareAD_PROGRESS.log /home/ec2-user/splunk/var/log/splunk/eurareMOTE_LATEST_REPORT.log /home/ec2-user/splunk/var/log/splunk/eurareMOTE_SCAN_SCRIPTED_INPUT.log /home/ec2-user/splunk/var/log/splunk/eurare_SCAN_APPS.log /home/ec2-user/splunk/var/log/splunk/eurare_SCAN_DEPLOYMENT.log /home/ec2-user/splunk/var/log/splunk/eurare_SEARCH_PEER_SSL_CONFIG.log

NOTE : dedup will not work with list. Dedup will work with normal table.

index=\_internal | stats list(source) | stats count

406,607 of 406,607 events matched No Event Sampling

Events (406,607) Patterns Statistics (1) Visualization

20 Per Page ✓ Format Preview

count = 1

#### #eval command:

Eval command is **used to initialize some variable** and use that variable.

**index=\_internal | eval KB=bytes/1024 | table bytes, KB**

index=\_internal | eval KB=bytes/1024 | table bytes, KB

Last 24 hours ▾

636,754 of 636,754 events matched No Event Sampling

Events (636,754) Patterns Statistics (505,463) Visualization

20 Per Page ✓ Format Preview

bytes	KB
4	0.00390625
59	0.0576171875
1434	1.400398625
59	0.0576171875
1436	1.40234375
419	0.4091796875
419	0.4091796875
267	0.2607421875

To round to 2 decimal and concatenate/ add word

**index=\_internal | eval KB=round(bytes/1024, 2)." KB" | table bytes, KB**

index=\_internal | eval KB=round(bytes/1024, 2)." KB" | table bytes, KB

639,318 events (6/5/23 6:00:00.000 AM to 6/6/23 6:06:18.000 AM) No Event Sampling

Events (639,318) Patterns Statistics (639,318) Visualization

20 Per Page ✓ Format Preview

bytes	KB
59	0.06 KB
9724	9.50 KB
267	0.26 KB
267	0.26 KB
59	0.06 KB
418	0.41 KB
50	0.06 KB

Date-Time function :

<https://docs.splunk.com/Documentation/SCS/current/SearchReference/DateandTimeFunctions>

**index=\_internal | eval KB=round(bytes/1024, 2) | eval date\_mon\_year=strftime(\_time, "%d:%m:%Y") | stats sum(KB) by date\_mon\_year**

index=\_internal | eval KB=round(bytes/1024, 2) | eval date\_mon\_year=strftime(\_time, "%d:%m:%Y") | stats sum(KB) by date\_mon\_year

Last 7 days ▾

1,007,915 events (5/30/23 6:00:00.000 AM to 6/6/23 6:12:49.000 AM) No Event Sampling

Events (1,007,915) Patterns Statistics (3) Visualization

20 Per Page ✓ Format Preview

date_mon_year	sum(KB)
04:06:2023	318567.91
05:06:2023	197502.44
06:06:2023	309377.80

OR

```
index="_internal" | eval KB=round(bytes/1024, 2) | eval date_mon_year=strftime(_time, "%D") |
stats sum(KB) by date_mon_year
```

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=\_internal | eval KB=round(bytes/1024, 2) | eval date\_mon\_year=strftime(\_time, "%D") | stats sum(KB) by date\_mon\_year
- Results Summary:** ✓ 1,008,574 events (5/30/23 6:00:00.000 AM to 6/6/23 6:13:38.000 AM) No Event Sampling
- Time Range:** Last 7 days
- Panel Tabs:** Events (1,008,574), Patterns, Statistics (3), Visualization
- Sort Options:** 20 Per Page ▾, Format, Preview ▾
- Table Headers:** date\_mon\_year, sum(KB)
- Data Rows:**

date_mon_year	sum(KB)
06/04/23	318567.91
06/05/23	197502.44
06/06/23	309766.74

### #eval with if-else

If going to use "dedup", use it as earliest as possible.

```
index="my_idx" sourcetype="csv" | dedup current_ticket_state | eval
state=if(current_ticket_state="Closed" OR current_ticket_state="Resolved", "Completed Ticket",
"Incomplete Ticket") | table current_ticket_state, state
```

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index="my\_idx" sourcetype="csv" | dedup current\_ticket\_state | eval state=if(current\_ticket\_state="Closed" OR current\_ticket\_state="Resolved", "Completed Ticket", "Incomplete Ticket") | table current\_ticket\_state, state
- Results Summary:** ✓ 6 events (before 6/6/23 6:19:25.000 AM) No Event Sampling
- Panel Tabs:** Events (6), Patterns, Statistics (6), Visualization
- Sort Options:** 20 Per Page ▾, Format, Preview ▾
- Table Headers:** current\_ticket\_state, state
- Data Rows:**

current_ticket_state	state
In Progress	Incomplete Ticket
Closed	Completed Ticket
Resolved	Completed Ticket
Pending	Incomplete Ticket
Customer Hold	Incomplete Ticket
On Hold	Incomplete Ticket

### #eval with case

In "case" statement, we can define multiple values.

```
Case(condition1,"<value1>,condition2,"<value2>"....1=1,"<default value>")
```

Case statement works from left to right=, hence 1=1 i.e. universal condition comes in last.

```
index="my_idx" sourcetype="csv" | dedup severity | eval sev=case(severity=1, "Critical", severity=2,
"High", severity=3, "Normal", 1=1, "Low") | table severity, sev
```

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index="my\_idx" sourcetype="csv" | dedup severity | eval sev=case(severity=1, "Critical", severity=2, "High", severity=3, "Normal", 1=1, "Low") | table severity, sev
- Results Summary:** ✓ 4 events (before 6/6/23 6:30:44.000 AM) No Event Sampling
- Panel Tabs:** Events (4), Patterns, Statistics (4), Visualization
- Sort Options:** 20 Per Page ▾, Format, Preview ▾
- Table Headers:** severity, sev
- Data Rows:**

severity	sev
3	Normal
2	High
4	Low
1	Critical

Sort +/-

In sort command + is default.

The top screenshot shows a search result for 4 events. The sort command is used with a plus sign (+) after severity, which means it sorts by severity in ascending order. The results are: 1 Critical, 2 High, 3 Low, 4 Low.

severity	sev
1	Critical
2	High
3	Low
4	Low

The bottom screenshot shows a search result for 4 events. The sort command is used with a minus sign (-) before severity, which means it sorts by severity in descending order. The results are: 4 Low, 3 Low, 2 High, 1 Critical.

severity	sev
4	Low
3	Low
2	High
1	Critical

### Top & Rare command

Top will give the top value.

Default value of top is 10.

It will show 2 columns => count and percent columns

A search for '\_internal' using the top command. The results show 192,843 events matched. The Statistics tab is selected, showing a table with two columns: count and percent. The top values are: splunkd (count: 113861, percent: 67.518798), splunkd\_ui\_access (count: 32577, percent: 19.317939), splunkd\_access (count: 16714, percent: 9.911288), splunk\_assist\_internal\_log (count: 2636, percent: 1.563138), splunk\_web\_service (count: 818, percent: 0.485068), and splunk\_python (count: 818, percent: 0.485068).

	count	percent
splunkd	113861	67.518798
splunkd_ui_access	32577	19.317939
splunkd_access	16714	9.911288
splunk_assist_internal_log	2636	1.563138
splunk_web_service	818	0.485068
splunk_python	818	0.485068

Use limit to get top n values.

index=\_internal | top limit=3 sourcetype

A search for '\_internal' using the top command with limit=3. The results show 130,519 events matched. The Statistics tab is selected, showing a table with two columns: count and percent. The top 3 values are: splunkd (count: 80425, percent: 61.619381), splunkd\_ui\_access (count: 33082, percent: 25.346501), and splunkd\_access (count: 12502, percent: 9.578682).

	count	percent
splunkd	80425	61.619381
splunkd_ui_access	33082	25.346501
splunkd_access	12502	9.578682

Use limit=0, to get all values.

index=\_internal | top limit=0 sourcetype

All time

518,517 of 518,517 events matched No Event Sampling

Events (518,517) Patterns Statistics (13) Visualization

20 Per Page Preview

sourcetype	count	percent
splunkd	382992	79.652434
splunkd_access	50885	10.582764
splunkd_ui_access	33349	6.935730
splunk_assist_internal_log	8932	1.857625
secure_gateway_app_internal_log	2128	0.442569

Rare will give the bottom value

**index=\_internal | rare limit=3 sourcetype**

index=\_internal | rare limit=3 sourcetype

All time

✓ 1,028,399 events (before 6/6/23 6:42:22.000 AM) No Event Sampling

Events (1,028,399) Patterns Statistics (3) Visualization

20 Per Page Preview

sourcetype	count	percent
splunk_version	1	0.000097
splunkd_conf	1	0.000097
splunkd_stderr	1	0.000097

### Fields +/- command

+ is to add filed. Default

- - is to remove filed

**index=\_internal | rare limit=3 sourcetype | fields - percent**

index=\_internal | rare limit=3 sourcetype | fields - percent

All time

26,047 of 26,047 events matched No Event Sampling

Events (26,047) Patterns Statistics (3) Visualization

20 Per Page Preview

sourcetype	count
splunk_web_access	4
splunk_python	14
splunk_web_service	14

**index=\_internal | rare limit=3 sourcetype | fields - percent, - count**

New Search!

index=\_internal | rare limit=3 sourcetype | fields - percent, - count

All time

✓ 1,033,386 events (before 6/6/23 6:58:04.000 AM) No Event Sampling

Events (1,033,386) Patterns Statistics (3) Visualization

20 Per Page Preview

sourcetype
splunk_version
splunkd_conf
splunkd_stderr

### Chart command

chart count by X

chart count(Y) by X

Count/Y will be on Y-axis

X will be on X-axis

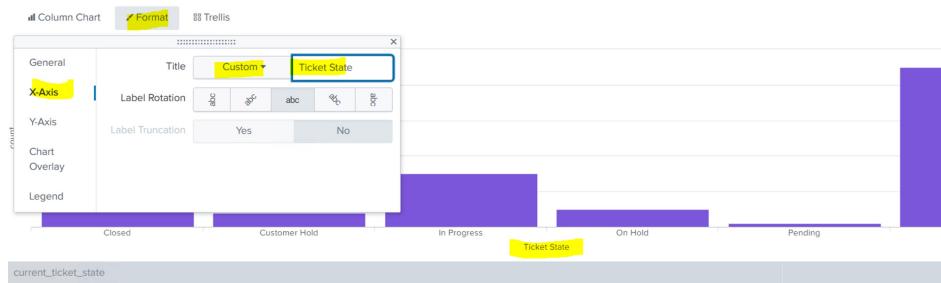
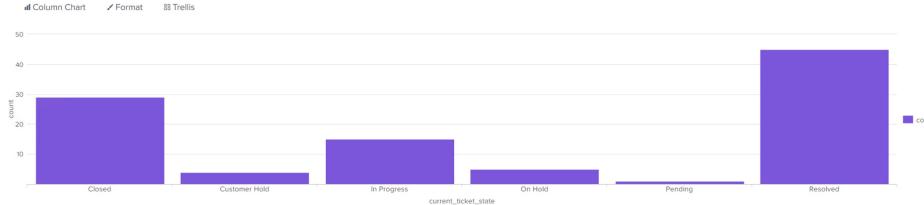
index="my\_idx" | chart count by current\_ticket\_state

index="my_idx"   chart count by current_ticket_state		All time	Search
Events (99) Patterns Statistics (6) Visualization		Job	Verbose Mode
20 Per Page			Format Preview
current_ticket_state	count	29	
Closed		4	
Customer Hold		15	
In Progress		5	
On Hold		1	
Pending		45	
Resolved			

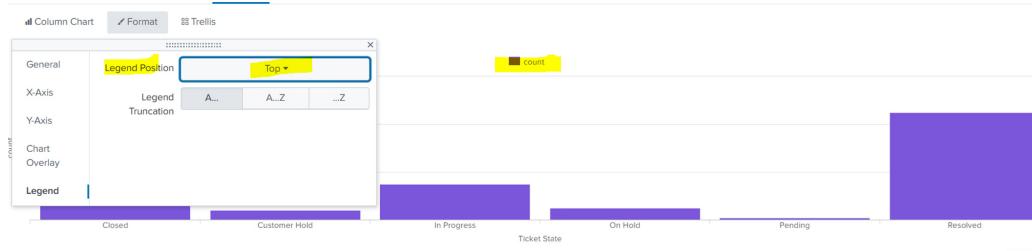
index="my\_idx" | chart count by current\_ticket\_state

✓ 99 events (before 6/6/23 7:01:16.000 AM) No Event Sampling ▾

Events (99) Patterns Statistics (6) Visualization



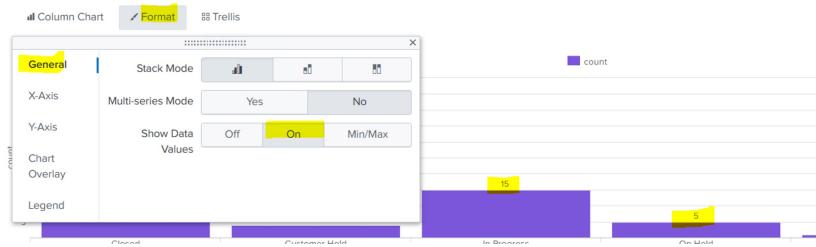
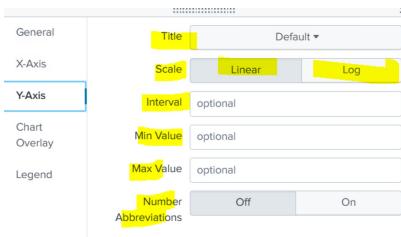
#### Legend Position:



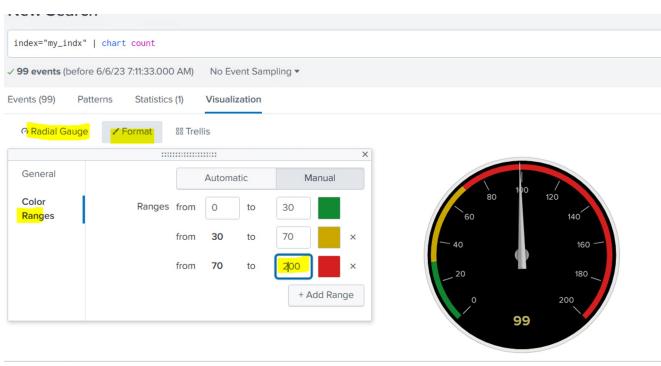
#### Format => X-axis Options:



#### Format => Y-axis options:



#### Radial Gauge:



#### Question :

Which query is most optimized ?

SPL 1 => index="my\_idx" | stats count as total by sourcetype

SPL 2 => index="my\_idx" | stats count by sourcetype | rename count as total

#### Answer :

SPL 1 will work faster as it will generate only 2 virtual table as rename is happening in 2ns step only.

