

Training – Day #4

15 June 2023 04:33

#Knowledge-Objects

A user-defined entity that enriches the existing data in the Splunk platform.

You can use knowledge objects to get specific information about your data.

When you create a knowledge object, you can keep it private or you can share it with other users.

Knowledge managers manage how their organizations use knowledge objects in their Splunk Enterprise [deployments](#).

Splunk Enterprise knowledge objects include [saved searches](#), [event types](#), [tags](#), [field extractions](#), [lookups](#), [reports](#), [alerts](#), [data models](#), [workflow actions](#), and [fields](#).

From <<https://docs.splunk.com/Splexicon:Knowledgeobject>>

When you run a search, Splunk software runs several operations to derive knowledge objects and apply them to events returned by the search. **Splunk software performs these operations in a specific sequence.**

<https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/Searchtimeoperationssequence>

Search-time operation order	Operation name	Configurable in Splunk Web?	Location of file configuration
1	Role-based field filtering	No	<code>fieldfilter-<fieldname></code> in a stanza in the <code>authorize.conf</code> file.
2	Inline field extraction (no field transform)	Yes	<code>EXTRACT-<class></code> in a stanza in the <code>props.conf</code> file.
3	Field extraction that uses a field transform	Yes	<code>REPORT-<class></code> in a stanza in the <code>props.conf</code> file.
4	Automatic key-value field extraction	No	In stanzas in the <code>props.conf</code> file, where <code>KV_MODE</code> is set to a valid value other than <code>none</code> . If no <code>KV_MODE</code> value is specified for a stanza, it is set to <code>auto</code> by default.
5	Field aliasing	Yes	<code>FIELDALIAS-<class></code> in a stanza in the <code>props.conf</code> file.
6	Calculated fields	Yes	<code>EVAL-<fieldname></code> in a stanza in the <code>props.conf</code> file.
7	Lookups	Yes	<code>LOOKUP-<class></code> in a stanza in the <code>props.conf</code> file.
8	Event types	Yes	In a stanza in the <code>eventtypes.conf</code> file.
9	Tags	Yes	In a stanza in the <code>tags.conf</code> file.

#Calculated Fields:

Calculated fields are fields added to events at search time that **perform calculations with the values of two or more fields already present in those events**. Use calculated fields as a shortcut for performing repetitive, long, or complex transformations using the eval command.

<https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/definecalcfields#:~:text=Calculated%20fields%20are%20fields%20added,transformations%20using%20the%20eval%20command>.

We can **create a Template where we can define eval expression only once** and we have to attach that KB when any requirement is needed.

So if any change is required in expression, we have to do only on one place i.e. Template.

We can **apply Template on dataset based on (to be more precise on its attachment)**:

- (1) source
- (2) sourcetype
- (3) host

Add new

Fields > Calculated fields > Add new

Destination app: search

Apply to: sourcetype: named: splunkd_ui_access

Name: my_kb

Eval expression: round(bytes/1024, 3)." KB"

Cancel Save

Without Calculated Field:

```
index="_internal" sourcetype=splunkd_ui_access
| eval kb=round(bytes/1024, 3)." KB"
| table kb, bytes
```

New Search

Save As ▾ Create Table View Close

Last 24 hours ▾

48,156 events (6/7/23 4:00:00.000 AM to 6/8/23 4:04:18.000 AM) No Event Sampling ▾

Events Patterns Statistics (48,156) Visualization

20 Per Page ▾ Format Preview ▾

bytes	Count
418	0.408 KB
267	0.261 KB
418	0.408 KB
10140	9.902 KB
418	0.408 KB
5921	5.782 KB
418	0.408 KB

Create Calculate Filed:

Settings => Knowledge => Fields => Calculated Fields => New Calculated Fields

Add new

Fields > Calculated fields > Add new

Destination app: search

Apply to: sourcetype: named: splunkd_ui_access

Name: my_kb

Eval expression: round(bytes/1024, 3)." KB"

Cancel Save

Name of Calculated Fields will be => **<sourcetype/host/source>:EVAL-<Calculated Filed Name>**

Calculated fields

Fields > Calculated fields

Successfully saved "my_kb" in search.

Showing 1-4 of 4 items

Name	Field name	Eval expression	Owner
source::splunkd_ui_access : EVAL-ane_kb	ane_kb	round(bytes/1024,1)."KB"	user5
splunkd_ui_access : EVAL-boopash_kb	boopash_kb	round(bytes/1024,3)." KB"	user1
splunkd_ui_access : EVAL-my_kb	my_kb	round(bytes/1024, 3)." KB"	user2
splunkd_ui_access : EVAL-sp_kb	sp_kb	round(bytes/1024, 3)." KB"	user4

Search with template of created Calculated Fields:

```
index=_internal" sourcetype=splunkd_ui_access
| table my_kb, bytes
```

Note : No eval line is needed.

my_kb	bytes
0.640 KB	655
1.665 KB	1795
0.668 KB	684
2.076 KB	2126
0.774 KB	793

Permissions of Calculated Fields :

- (1) **Keep private** => Only creator can use and edit + **Default settings**
- (2) **This app only (search)** => **Give Permissions Based on Role + KB can be accessible from only search application**
- (3) **All apps (system)** => **Give Permissions Based on Role + KB can be accessible from all application**

Roles	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input checked="" type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>
viatris	<input type="checkbox"/>	<input type="checkbox"/>

Move => to move from one application to other application

#Tags:

<https://docs.splunk.com/Documentation/Splunk/9.0.4/SearchReference/Tags>

Tag is used to **Categorize** or **Identify** something.

In Splunk, we add **Tags to "Field Value"**.

How to create Tags:

Open Event Filed => Go to Field => Edit Tags=>

A screenshot of the Splunk interface showing a list of fields for an event. The 'severity' field is highlighted with a yellow box and has the value '3'. At the bottom right of the list, there is a blue button labeled 'Edit Tags'.

A screenshot of the 'Create Tags' dialog box. It shows a 'Field Value' input field containing 'severity=3' and a 'Tag(s)' input field containing 'my_sev_3_tag'. Below these fields are 'Cancel' and 'Save' buttons.

Run Query :

`index="my_idx" source="sample_tickets.csv" tag::severity="my_sev_3_tag"`

A screenshot of the search results. It shows a table with columns: 'Field Value', 'Time', and 'Details'. In the 'Field Value' column, there is a row with 'severity=3'. In the 'Details' column, there is a row for ticket number 58, which includes fields like 'Project', 'Org', 'Status', etc.

Field will be auto generated -

- (1) tag
- (2) tag-<field name>

Permissions:

A screenshot of the 'List by field value pair' table. It shows a list of 11 items, each with columns: 'Field value pair', 'Tag name', 'App', 'Sharing', 'Status', and 'Actions'. Some rows are highlighted with yellow boxes, such as 'severity=3' and 'my_sev_3_tag'.

Field value pair	Tag name	App	Sharing	Status	Actions
eventtype=Closed	Closed_Tickets	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
eventtype=Progress	Ticket_InProgress	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
eventtype=ticket_status	status	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
severity=3	normal	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
severity=3	normal	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
severity=3	my_sev_3_tag	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
severity=3	normal	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
severity=3	normal	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
severity=3	Normal	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
ticket_type=Incident	Problem	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete

How to Edit Condition of Tags:

Settings => Tags => List by tag name => click "Tag name" => Edit field value condition

List by tag name

Tags > List by tag name

Showing 1-11 of 11 items

App Search & Reporting (s...) Owner Any

Tag name	Field value pair
Closed_Tickets	eventtype=Closed
Normal	severity=3
Problem	ticket_type=Incident
Ticket_InProgress	eventtype=Progress
my_sev_3_tag	severity=3
normal	severity=3
normal	severity=3

Tag name	Field value pair
Closed_Tickets	eventtype=Closed
Normal	severity=3
Problem	ticket_type=Incident
Ticket_InProgress	eventtype=Progress
my_sev_3_tag	host=123, severity=3

#EventType:

<https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/Abouteventtypes>

(1) Condition of **Event Categorization based on "Search Query"**

How to create Event-Type:

Step #1 : Run your SPL :

```
index="my_idx" source="sample_tickets.csv" (current_ticket_state="Closed" OR current_ticket_state="Resolved")
```

Step #2: Save as "Event Type"

New Search

index="my_idx" source="sample_tickets.csv" (current_ticket_state="Closed" OR current_ticket_state="Resolved")

✓ 74 events (before 6/8/23 4:48:38.000 AM) No Event Sampling

Events (74) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

Save As ▾ Create Tab

Report Alert Existing Dashboard New Dashboard Event-Type

Save As Event Type

Name: my_event_type

Tags: Optional

Color: none

Priority: 10 (Lowest)

Date one: 2

one: 3

3: 4

4: 5

5: 6

6: 7

7: 8

8: 9

9: 10 (Lowest)

10: 11

11: 12

12: 13

13: 14

14: 15

15: 16

16: 17

17: 18

18: 19

19: 20

20: 21

21: 22

22: 23

23: 24

24: 25

25: 26

26: 27

27: 28

28: 29

29: 30

30: 31

31: 32

32: 33

33: 34

34: 35

35: 36

36: 37

37: 38

38: 39

39: 40

40: 41

41: 42

42: 43

43: 44

44: 45

45: 46

46: 47

47: 48

48: 49

49: 50

50: 51

51: 52

52: 53

53: 54

54: 55

55: 56

56: 57

57: 58

58: 59

59: 60

60: 61

61: 62

62: 63

63: 64

64: 65

65: 66

66: 67

67: 68

68: 69

69: 70

70: 71

71: 72

72: 73

73: 74

Save As Event Type

Name	my_event_type
Tags	Optional
Color	green
Priority	10 (Lowest)
Determines which style wins, when an event has more than one event type.	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Event types

Showing 1 of 1 item

App	Search & Reporting (s...)	Owner	Any	Visible in the App	my_eve	<input type="text"/>	<input type="button" value="Search"/>	25 per page	New Event Type					
Name	Search string					Tag(s)	Owner	App	Sharing	Status	Actions			
my_event_type	index="my_idx" source="sample_tickets.csv" (current_ticket_state="Closed" OR current_ticket_state="Resolved")					user2	search	Private	Permissions	Enabled	Disable	Clone	Move	Delete

Step #3 : Use Event Type to see the results

eventtype="my_event_type"

✓ 74 events (before 6/8/23 4:53:46.000 AM) No Event Sampling ▾

All time

Events (74) Patterns Statistics Visualization

Format Timeline ▾ 1 month per column

List 20 Per Page Next >

Time	Event
6/6/23 5:17:00.000 AM	Project 1,Org_1,,MSTR,Functionality,17-01-17 5:17,Closed,3498,Not Defined,240,10,17-01-17 5:17,17-01-17 5:17,BI Reports,,PROD MACHINE : laq0ndwpr01 : Job dat-lnh-rde-qjn558_rdn558opppsmdf.s failed with exit code 100,Not Defined,14-01-17 6:18,Not Defined,17-01-17 5:17,3,Net,Net,BI Data,INC0000207931 73,Remedy,Incident,14-01-17 6:18,SRVCAM-AM BI-Data host = ip-172-31-84-138.ec2.internal source = Sample_tickets.csv sourcetype = csv
6/5/23 11:43:00.000 AM	Project 1,Org_1,,MSTR,Access,14-05-16 11:43,Resolved,512398,Not Defined,Not Defined,10,25-01-16 8:59,13-01-17 5:17,BI Reports,owner_name2513,User confirmed that issue has been addressed.,Not Defined,16-03-16 4:24,16-03-16 4:24,14-05-16 11:43,2,Net,Net,BI Data,INC000019562669,Remedy,Service Request,16-03-16 4:24,SRVCAM-AM BI-Data host = ip-172-31-84-138.ec2.internal source = Sample_tickets.csv sourcetype = csv

Permissions:

Event types

Showing 1 of 1 item

App	Search & Reporting (s...)	Owner	Any	Visible in the App	my_eve	<input type="text"/>	<input type="button" value="Search"/>	25 per page	New Event Type					
Name	Search string					Tag(s)	Owner	App	Sharing	Status	Actions			
my_event_type	index="my_idx" source="sample_tickets.csv" (current_ticket_state="Closed" OR current_ticket_state="Resolved")					user2	search	Private	Permissions	Enabled	Disable	Clone	Move	Delete

#Lookups:

<https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/Aboutlookupsandfieldactions>

Lookup is a small static file.

Lookups enrich your **event data** by adding field-value combinations from lookup tables.

4 Type of lookup files :

- (1) CSV lookup
- (2) KV store lookup
- (3) Geospatial lookup

(4) External lookup

No license consumption as no index consumption. It will consume disk space on server.

How to use lookups?

Step #1 : Upload lookup in Splunk.

Settings => Lookups => Lookup Table files => Add =>

Note : Don't forget to put ".csv" in end of filename "Destination filename".

Add new

Lookups > Lookup table files > Add new

Destination app: search

Upload a lookup file: Choose File sample_lookup.csv

Select either a plaintext CSV file, a gzipped CSV file, or a KMZ/KML file. The maximum file size that can be uploaded through the browser is 500MB.

Destination filename*: my_sample_lookup.csv

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv". For a KMZ/KML file, we recommend a filename ending in ".kmz"?".km".

Cancel Save

Step #2 : List lookup by "|inputlookup" command

`/inputlookup my_sample_lookup.csv`

NEW Search...

/inputlookup my_sample_lookup.csv

99 results (before 6/8/23 5:09:58:000 AM) No Event Sampling ▾

Events Patterns Statistics (99) Visualization

20 Per Page ▾ Format Preview ▾

ticket_number	time_taken
INC000020793173	9hrs
INC000019343584	9hrs
INC000020793217	9hrs
INC000020793170	9hrs
INC000019866513	9hrs

Step #3 : Use lookup to enrich event by **2 ways**-

(1) using join

(2) using Lookup Definition => **More faster** than Join

Note : If field name are not same, then use "**rename**" command to create similar name.

(1) using join

```
index="my_idx" source="Sample_tickets.csv"
| table ticket_number, severity, current_ticket_state
| lookup my_sample_lookup.csv ticket_number OUTPUT time_taken as
time_consumed_enriched_from_lookup
```

New Search

Save As ▾

```
index="my_idx" source="Sample_tickets.csv"
| table ticket_number, severity, current_ticket_state
| lookup my_sample_lookup.csv ticket_number OUTPUT time_taken as time_consumed_enriched_from_lookup
```

✓ 99 events (before 6/8/23 5:16:28.000 AM) No Event Sampling ▾

Job ▾

Events Patterns Statistics (99) Visualization

20 Per Page ▾ Format Preview ▾

◀ Prev 1

ticket_number	severity	current_ticket_state	time_consumed_enriched_from_lookup
INC000020280565	3	Resolved	6hrs
INC000020425526	2	Resolved	6hrs
INC000019480506	4	Resolved	6hrs
INC000019482386	3	Resolved	6hrs
INC000020793157	3	Resolved	6hrs
INC000020793172	3	Closed	6hrs

(2) using lookup definitions

Settings => Lookups => Lookup Definitions => Add New

Add new

Lookups > Lookup definitions > Add new

Destination app	search
Name*	my_lookup_definition
Type	File-based
Lookup file*	my_sample_lookup.csv
Create and manage lookup table files.	
<input type="checkbox"/> Configure time-based lookup	
<input type="checkbox"/> Advanced options	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Lookup definitions

Lookups > Lookup definitions

Showing 1 of 1 item

Name	Type	Supported fields	Lookup file	Owner	App	Sharing	Status	Actions
my_lookup_definition	file	ticket_number,time_taken	my_sample_lookup.csv	user2	search	Private	Enabled Disable	Clone Move Delete

```
index="my_idx" source="Sample_tickets.csv"
| table ticket_number, severity, current_ticket_state
| lookup my_lookup_definition ticket_number OUTPUT time_taken as time_consumed_enriched_from_lookup
```

New Search

Job

```
index="my_idx" source="Sample_tickets.csv"
| table ticket_number, severity, current_ticket_state
| lookup my_lookup_definition ticket_number OUTPUT time_taken as time_consumed_enriched_from_lookup
```

✓ 99 events (before 6/8/23 5:28:36.000 AM) No Event Sampling ▾

Events Patterns Statistics (99) Visualization

20 Per Page ▾ Format Preview ▾

ticket_number	severity	current_ticket_state	time_consumed_enriched_from_lookup
INC000020280565	3	Resolved	6hrs
INC000020425526	2	Resolved	6hrs
INC000019480506	4	Resolved	6hrs
INC000019482386	3	Resolved	6hrs
INC000020793157	3	Resolved	6hrs
INC000020793172	3	Closed	6hrs
INC000020793149	3	Resolved	6hrs

#Automatic Lookup

Settings => Lookups => Automatic Lookup => Add New

Lookup input fields <field name of lookup> = <field name of index, need to mention if name is not same>

Lookup input fields ticket_number = [redacted]

Add new

Lookups > Automatic lookups > Add new

Destination app: search
Name: my_auto_lookup
Lookup table: my_lookup_definition
Apply to: source
named: Sample_tickets.csv
Lookup input fields: ticket_number
Lookup output fields: time_taken
time_taken_renamed_as_time_consumed
Overwrite field values
Cancel Save

Name of automatic lookup => <Apply to>::<Apply to Value>: LOOKUP <auto lookup name>

It will create lookup command with OUTPUTNEW.

Automatic lookups

Lookups > Automatic lookups

New Automatic Lookup

Successfully saved "my_auto_lookup" in search.					
Showing 1-3 of 3 items					
App	Search & Reporting (s...)	Owner	Any	Visible in the App	filter
Sample_tickets.csv : LOOKUP-brindha_auto_lookup	brindha_lookup ticket_number OUTPUTNEW time_taken AS time_consumed	user6	search	Private Permissions	Enabled Clone Move Delete
source:Sample_tickets.csv : LOOKUP-my_auto_lookup	my_lookup_definition ticket_number OUTPUTNEW time_taken AS time_taken_renamed_as_time_consumed	user2	search	Private Permissions	Enabled Clone Move Delete
source:sample_tickets.csv : LOOKUP-manoj_auto_lookup	manoj_lookup ticket_number OUTPUTNEW time_taken AS time_consumed	user7	search	Private Permissions	Enabled Clone Move Delete

Step #3: use the output field

```
index="my_idx" source="Sample_tickets.csv"
| table ticket_number, severity, current_ticket_state, time_taken AS
time_taken_renamed_as_time_consumed
```

New Search

Save As | Create Table View | All time

Events Patterns Statistics (99) Visualization

20 Per Page | Format Preview | < Prev 1 2 3 4 >

ticket_number	severity	current_ticket_state	time_taken	AS	time_taken_renamed_as_time_consumed
INC000020280565	3	Resolved			6hrs
INC000020425526	2	Resolved			6hrs
INC000019480506	4	Resolved			6hrs
INC000019482386	3	Resolved			6hrs
INC000020793157	3	Resolved			6hrs

#Lookup Editor Application

This application will make very easy to delete/modify any lookup file.

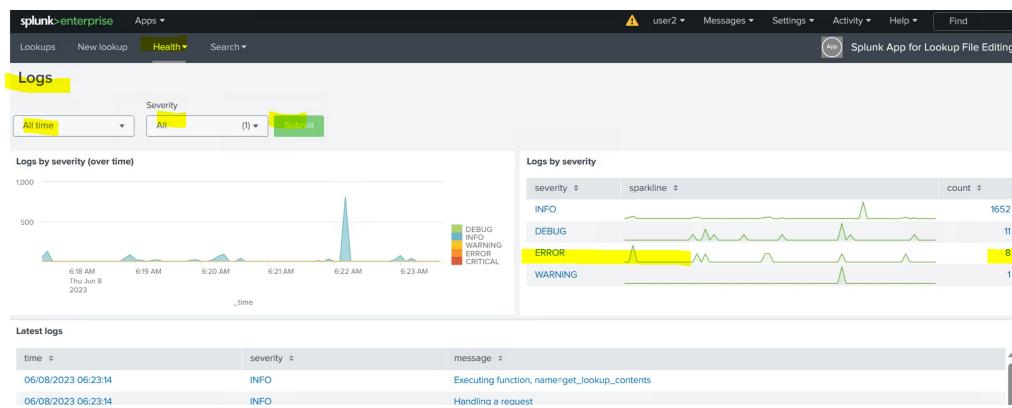
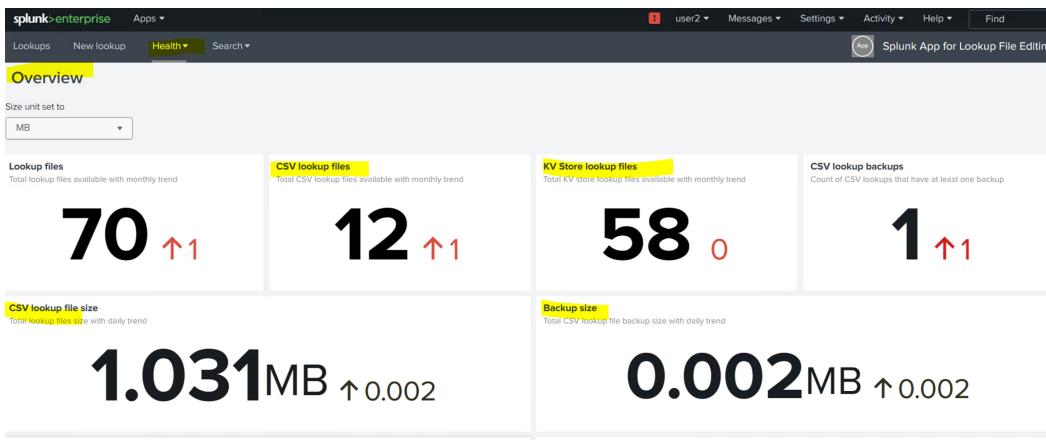
The screenshot shows a search results page for 'lookup' on a Splunk platform. The search bar at the top contains 'lookup'. Below it, there are several filters: 'CIM VERSION' (5.x, 4.x, 3.x), 'APP TYPE' (App, Add-on, Connector), and 'SUPPORT TYPE' (Developer Supported, Splunk Supported). The main results area shows one result: 'Splunk App for Lookup File Editing'. It includes a brief description, an 'Install' button, and a link to 'View on Splunkbase'. The page title is 'Not secure | 52.87.110.165:8000/en-US/manager/search/appsremote?offset=0&count=20'.

The screenshot shows the 'Lookup List' page in the Splunk interface. The URL is 'splunk>enterprise Apps > Lookups'. The search bar at the top has 'my_...' entered. A table below lists one entry: 'my_sample_lookup.csv' (CSV lookup, Search & Reporting app, owner user2, 0 backups). Action buttons for edit, search, and delete are shown. The page title is 'splunk>enterprise Apps > Lookups'.

The screenshot shows the details page for 'my_sample_lookup.csv'. The URL is 'splunk>enterprise Apps > Lookups / my_sample_lookup.csv'. It shows a table with four rows of data: ticket_number (INC000020793173, INC000019343584, INC000020793217, INC000020793170) and time_taken (9hrs, 9hrs, 9hrs, 9hrs). Buttons for 'Edit limit', 'Manage Backups', and 'Revert' are visible. The page title is 'splunk>enterprise Apps > Lookups / my_sample_lookup.csv'.

Create 2 kinds of lookup (1) CSV and (2) KV store

The screenshot shows the 'New lookup' creation process. The URL is 'splunk>enterprise Apps > Lookups > New lookup'. It has two sections: 'CSV lookup' (with a note about importing from Excel or CSV files) and 'KV store lookup' (with a note about large files). Buttons for 'Create CSV lookup' and 'Create KV store lookup' are at the bottom. The page title is 'splunk>enterprise Apps > Lookups > New lookup'.



#outputlookup command

It is used to **push data in an existing lookup**.

Default is **override the value**. So use append=true

```
| makeresults
| eval ticket_number=1, time_taken="40hrs"
| fields - _time
| outputlookup append=true my_sample_lookup.csv
```

New Search

```
| makeresults
| eval ticket_number=2, time_taken="60hrs"
| fields - _time
| outputlookup append=true my_sample_lookup.csv
```

1 result (6/7/23 6:00:00.000 AM to 6/8/23 6:33:41.000 AM) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

ticket_number	time_taken
2	60hrs

The screenshot shows a Splunk search interface with the command `| inputlookup my_sample_lookup.csv` at the top. Below it, a message indicates 101 results from 6/7/23 to 6/8/23. The Statistics tab is selected. A table displays ticket numbers (1, 2, INC000019298955, TNC000019231669) and their corresponding time taken (40hrs, 60hrs, 6hrs, 4hrs). The table has columns for ticket_number and time_taken.

ticket_number	time_taken
1	40hrs
2	60hrs
INC000019298955	6hrs
TNC000019231669	4hrs

#KV store lookup

Key Value paired

Used to store **Big files** which are **Dynamic** in nature.

Values are in Stack.

#Macros

Macros are like a function.

like define a function

Call a function

- Macro with no argument
- Macro with single argument
- Macro with multiple argument

How to create a macro ?

Settings => Advance search => Search macros => Add new

`index="my_idx" source="Sample_tickets.csv"`

`| stats count by severity`

Macro with no argument

Add new

Advanced search > Search macros > Add new

The screenshot shows the 'Add new' macro configuration dialog. The 'Destination app' is set to 'search'. The 'Name' field contains 'my_macro_with_noargument'. The 'Definition' field contains the search command: `index="my_idx" source="Sample_tickets.csv" | stats count by severity`. The 'Validation Expression' and 'Validation Error Message' fields are empty. At the bottom, there are 'Cancel' and 'Save' buttons.

Search macros

Advanced search » Search macros

Showing 1 of 1 item

Name	Definition	Arguments	Owner	App	Sharing	Status	Actions
my_macro_with_noargument	index="my_idx" source="Sample_tickets.csv" stats count by severity		user2	search	Private Permissions	Enabled Disable	Clone Move Delete

New Search Macro

Call a macro of no argument with tilde symbol `` :

'my_macro_with_noargument'

New Search

my_macro_with_noargument

99 events (before 6/8/23 6:57:57.000 AM) No Event Sampling ▾

Events (99) Patterns Statistics (4) Visualization

20 Per Page ▾ Format Preview ▾

severity	count
1	3
2	16
3	58
4	22

'my_macro_with_noargument` | search severity=2

my_macro_with_noargument` | search severity=2

16 events (before 6/8/23 7:01:10.000 AM) No Event Sampling ▾

Events (16) Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

severity	count
2	16

Macro with single argument

Note: arguments are inside \$\$

index="my_idx" source="Sample_tickets.csv" current_ticket_state="Closed"
| stats count by severity, current_ticket_state

my_macro_with_single_argument(1)

Advanced search » Search macros » my_macro_with_single_argument(1)

Definition * Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg\$
 index="my_idx" source="Sample_tickets.csv" current_ticket_state="\$state\$"
 | stats count by severity, current_ticket_state

Arguments Use eval-based definition?

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '-' and '_' characters.
 state

Validation Expression Enter an eval or boolean expression that runs over macro arguments.

Validation Error Message Enter a message to display when the validation expression returns 'false'.

Cancel Save

ny_sev(1)

[Advanced search](#) » [Search macros](#) » my_sev()

Definition * Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$
index="my_idx" source="Sample_tickets.csv" severity=\$\$sev\$\$ | stats count by severity,

Arguments Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.
sev

Validation Expression Enter an eval or boolean expression that runs over macro arguments.
isnum(\$sev\$)

Validation Error Message Enter a message to display when the validation expression returns 'false'.
severity should be a number

Cancel Save

Call a macro of single argument

'my_macro_with_single_argument(Closed)'

severity	current_ticket_state	count
2	Closed	7
3	Closed	16
4	Closed	6

'my_sev(2)'

severity	current_ticket_state
2	Closed
2	In Progress
2	On Hold
2	Resolved

! Error in 'SearchParser': Encountered the following error while validating macro 'my_sev(a)': **severity should be a number.**

Validation : Isnum(\$sev\$) AND (\$sev\$ >0) AND (\$sev\$<5)

Validation Expression Enter an eval or boolean expression that runs over macro arguments.
isnum(\$sev\$) AND (\$sev\$=3)

Validation Error Message Enter a message to display when the validation expression returns 'false'.
severity should be a number and should be 3

! Error in 'SearchParser': Encountered the following error while validating macro 'my_sev(2)': **severity should be a number.**

Macro with multiple argument

```
index="my_idx" source="Sample_tickets.csv" severity=3 current_ticket_state="Closed"
| stats count by severity, current_ticket_state
```

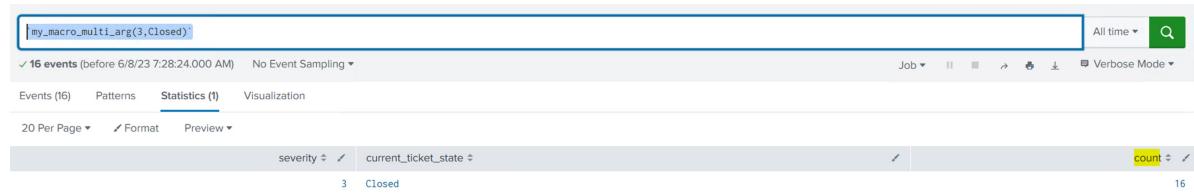
my_macro_multi_arg(2)

my_macro_multi_arg(2)

Advanced search > Search macros > my_macro_multi_arg(2)

The screenshot shows the 'Search macro' configuration page. The 'Definition' field contains the search command: `index="my_idx" source="Sample_tickets.csv" severity=sev current_ticket_state=$state$ | stats count by severity, current_ticket_state`. The 'Arguments' field contains `sev, state`. The 'Validation Expression' and 'Validation Error Message' fields are empty. At the bottom are 'Cancel' and 'Save' buttons.

'my_macro_multi_arg(3,Closed)'



Changing the argument order in "Arguments" :

The screenshot shows the 'Search macro' configuration page. The 'Arguments' field now contains `sev, state`. The 'Validation Expression' field is empty. At the bottom are 'Cancel' and 'Save' buttons.



